Inhaltsverzeichnis

1 Einführung

Full-spectrum, monitoring & compliance solution for servers and workstations.

Dies ist die offizielle Dokumentation für EventSentry, die umfassende Ressource, die alle Funktionen von EventSentry. Bitte beachten Sie, dass alle Themen direkt von der Verwaltungskonsole aus verlinkt sind und durch Klicken auf die Schaltfläche **Hilfe** in der gesamten Verwaltungskonsole aufgerufen werden können.

Für Erstbenutzer stehen auch andere Ressourcen zur Verfügung, die für den Einstieg in das Produkt hilfreich sein könnten:

- Online Training
- Web-Based Tutorials
- EventSentry Overview
- Best Practices

Andere Formate

Dieses Handbuch ist auch in den folgenden Formaten unter http://www.eventsentry.com/support/documentation erhältlich:

- Online (HTML)
- Microsoft Help Format (.chm)
- iPad / iBook

Support

Antworten auf die meisten Fragen finden Sie in den verschiedenen Bereichen auf der Produktwebsite http://www.eventsentry.com, einschließlich der Knowledge Base und der Foren. Wenn Sie eine Frage oder ein Problem mit EventSentry, dann versuchen Sie mit Hilfe der folgenden Ressourcen eine Antwort zu finden:

- Durchsuchen Sie **alle verfügbaren Ressourcen** online unter http://www.eventsentry.com
- Durchsuchen Sie die **KB** unter http://www.eventsentry.com/support/kb

E-Mail- und Telefon-Support ist auch für registrierte und Evaluierungsbenutzer verfügbar. Eine Liste der Support-Optionen finden Sie weiter unten:

- Füllen Sie unser Webformular aus
- Senden Sie eine E-Mail an support@netikus.net

Vielen Dank für die Nutzung von EventSentry!

Ihr **NETIKUS.**NET-Team.

1.1 Über

EventSentry, entwickelt von NETIKUS.NET ltd, ist ein WinXP - Windows 2003 - Windows Vista - Windows 2008 (R2) - Windows 7/8 - Windows 2012 (R2) - Windows 2019 Anwendungspaket, das aktiv das Ereignisprotokoll Ihres Servers (oder Ihrer Arbeitsstation), den Systemzustand und die Netzwerkgeräte überwacht.

Konfigurieren Sie EventSentry um Sie zu benachrichtigen, wenn wichtige Ereignisse, die Ihren Filterkriterien entsprechen, auftreten, oder um Ihre Ereignisprotokolle an einem zentralen Ort, wie z.B. einer zentralen ODBC-Datenbank, zu konsolidieren. Sie können auf verschiedene Arten aktiv benachrichtigt werden, einschließlich E-Mail, ASCII-Datei, Datenbank, Unix Syslog, SNMP, HTTP, Netzwerkmeldung, Prozess und mehr. Sie können auch Dienste, Festplattenplatz, Leistung, Prozesse und mehr überwachen. Der Heartbeat-Monitor prüft, ob Server und Netzwerkgeräte betriebsbereit sind.

EventSentry enthält auch einen Unix/Linux-Syslog/SNMP-Server, der eingehende Syslog-Pakete und SNMP-Traps entweder im Windows-Ereignisprotokoll oder in einer Datenbank protokolliert. Eine optionale NetFlow-Komponente visualisiert NetFlow- oder sFlow-Daten.

Wenn Sie EventSentry gekauft haben - Herzlichen Glückwunsch! Sie haben ein Softwareprodukt mit ausgezeichnetem Support und einem Team erhalten, das sich der Aufgabe verschrieben hat, die Log-, System- und Netzwerküberwachung so leistungsfähig wie möglich zu gestalten und gleichzeitig unser Produkt so einfach wie möglich zu bedienen.

Dieses Handbuch ist auch in den folgenden Formaten unter https://www.eventsentry.com/support/documentation erhältlich (Sie können auf den Text klicken, um die alternative Datei sofort herunterzuladen oder zu durchsuchen):

Online (HTML)
Microsoft Help Format (.chm)
Multimedia Help (.exe)

1.2 EventSentry Light

EventSentry Light ist die Freeware-Version von EventSentry und der Nachfolger von EventwatchNT, die eine EventSentry zeitlich unbegrenzte Evaluierung ermöglicht. EventSentry Light bietet nur einige wenige

Funktionen. Für EventSentry Light können wir keine Supportleistungen anbieten; bitte kaufen Sie EventSentry für erstklassigen Support.

Kurz gesagt, EventSentry Light hat die folgenden Einschränkungen:

- Keine Unterstützung für Datenbank- und Web Reports
- Es sind keine Sicherheits- und Compliance-Funktionen (Prozess, Anmeldung, Account Management, ...) verfügbar.
- Unterstützung nur über unsere Foren erhältlich (https://helpdesk.eventsentry.com)

Unten finden Sie einen **detaillierten Vergleich der Funktionen** von und EventSentry und EventSentry Light:

Feature Description	included in EventSentry Light
Actions	
SMTP Notification	yes
Syslog Notification	yes
SNMP Notification	yes
SNPP Notification	yes
Text File Notification (Plain Text, (X)HTML, CSV)	yes
Database Consolidation	**no**
Parallel Printer Notification	yes
Network Notification (aka "net send")	yes
Process Notification	yes
Sound Notification, Desktop Notification	yes
Jabber Notification	yes
Shutdown Notification, Service Control Notification	yes
HTTP Notification	yes
Filter (Event Log Monitoring) Options	
Event Log Packages	yes
Event Log Filters	yes
Filter Thresholds	yes
Filter Timers	yes
Monitor custom event logs	yes
Filtering based on Event log, severity, ID, source, category and text	yes
Filtering based on weekday and time of day	yes
Recurring Events	yes
Configure summary notifications	yes
Network Services	
Syslog Daemon	yes, no database logging
SNMP Trap Daemon	yes, no database logging
ARP Daemon	yes, no database logging
Log File Monitoring	

Monitor non-delimited text files	yes
Monitor delimited text files	**no**
Consolidate text files to database	**no**
System Health Features	
System Health Packages	yes
Service and Driver Monitoring	yes
Application Scheduler	yes
Event Log Backup / Clear	yes
Full event log detection	yes
Process Memory Monitoring	yes
Disk Space Monitoring	yes
Directory Size Monitoring	yes
Software/Hardware Inventory	yes, but no hardware inventory or uptime collection
Performance Monitoring	yes, but no history reports
File Change Monitoring	yes
NTP Monitoring	yes
Included Utilities	
Remote Update Utility	**no**
EventSentry Database Import Utility	**no**
Security & Compliance Features	
Process Tracking	**no**
Logon Tracking	**no**
Print Tracking	**no**
File Access Tracking	**no**
Account Management Tracking	**no**
Policy Change Tracking	**no**
General Features	
Groups	yes, max. 2
Process messages that occur during a server/workstation boot (Boot Scan)	yes
Resend messages if SMTP/ODBC/Syslog server is unavailable	yes, only SMTP
Remote service administration	**no**
Remote Update ((Un)Install,update,configure,control remote installations)	yes, up to two computers
Import & Link to Active Directory feature for remote update	**no**
Receive Syslog messages from remote Unix/Linux computers	yes, no database logging
Receive SNMP traps	yes, no database logging
View remote event logs in management application	yes
Import / Export configuration feature	yes
Custom Variable Support	yes
Heartbeat Monitoring	yes, without database logging

Environment Monitoring	yes, without database logging
Eligible for email and telephone support	**no**
Eligible for support at http://forums.netikus.net	yes

All configuration settings are retained when upgrading from EventSentry Light to EventSentry.

2 Installieren von EventSentry

Die Installation des EventSentry **Agenten**

- erfordert in den meisten Fällen keinen Neustart
- belegt **ungefähr 100Mb** Speicherplatz im Verzeichnis **`%SYSTEMROOT%\system32\eventsentry`**
- unterstützt das **MSI-Format** zur einfachen Active Directory-Integration

Sie können Remote-Agenten über die EventSentry Management-Konsole installieren und verwalten, indem Sie die Remote-Update-Funktion verwenden. Weitere Informationen finden Sie unter Verwaltung von Agenten.

Das Zielverzeichnis für die Dienste kann derzeit nicht geändert werden. Alle notwendigen EventSentry Servicedateien werden in das Verzeichnis %SYSTEMROOT% \system32\eventsentry kopiert.

2.1 Anforderungen

Hardware-Anforderungen

Alle EventSentry Komponenten, einschließlich der Agenten, erfordern einen Pentium IV oder höheren Prozessor mit SSE3-Unterstützung.

Betriebssystem-Plattformen

EventSentry läuft auf den folgenden Plattformen:

Operating System Version	Windows Editions	Run Installer	Monitor with Agent
Windows® NT 4 SP6	(Alle Versionen und Service Packs)	bis EventSentry v2.90	bis EventSentry v2.90
Windows® 2000	(Alle Versionen und Service Packs)	bis EventSentry v2.92	bis EventSentry v3.0.1
Windows® XP SP3	(Home, Professional) einschließlich x64-Editionen	bis EventSentry v3.3.1	Alle Versionen
Windows® Small Business Server 2003 SP2	(Alle Service Packs)	bis EventSentry v3.3.1	Alle Versionen
Windows® Server 2003 SP2	(all service packs), including x64 editions	bis EventSentry v3.3.1	Alle Versionen
Windows® Vista	(alle Editionen), einschließlich x64-Editionen	bis EventSentry v4.0.3	Alle Versionen
Windows® Server 2008 (R2)	(alle Editionen), einschließlich x64-Editionen	Alle Versionen	Alle Versionen
Windows® 7	(alle Editionen), einschließlich x64-Editionen	Alle Versionen	Alle Versionen
Windows® 8 & 8.1	(alle Editionen), einschließlich x64-Editionen	v2.93 und höher	Alle Versionen

Windows® Server 2012 (R2)	(alle Editionen), einschließlich x64-Editionen	v2.93 und höher	Alle Versionen
Windows® 10	(alle Editionen), einschließlich x64-Editionen	v3.2 und höher	Alle Versionen
Windows® Server 2016	(alle Editionen), einschließlich x64-Editionen	v3.3 und höher	Alle Versionen
Windows® Server 2019	(alle Editionen), einschließlich x64-Editionen	v3.5 und höher	EventSentry v3.5 und höher
Windows® 11	(alle Editionen), einschließlich x64-Editionen	v5.0 und höher	EventSentry v5.0 und höher
Windows® Server 2022	(alle Editionen), einschließlich x64-Editionen	v5.0 und höher	EventSentry v5.0 und höher
Windows® Server 2025	(alle Editionen), einschließlich x64-Editionen	v5.1 und höher	EventSentry v5.1 und höher

Siehe unten für Anforderungen an bestimmte Komponenten.

Hardware

Die folgenden **Mindestressourcenzuweisungen** (CPU-Kerne/Speicher) werden für die serverseitigen Komponenten von EventSentry empfohlen. Dies gilt **zusätzlich** zu den Kernanforderungen von Windows® Server. Je nach der Menge der empfangenen Daten können zusätzliche Ressourcen erforderlich sein.

Name der Komponente	# Anzahl der Kerne	Speicher (Mb)	Anmerkungen
Eingebaute PostgreSQL-Datenbank	4-8	4096-8192	Große Abfragen/Datenbanken können deutlich mehr Speicher benötigen
Network Services	1-2	256-512	Hohe NetFlow-Last kann mehr Kerne erfordern
Collector	1-2	256-512	
Web-Reports	1-2	512-1024	
Heartbeat-Monitor	1-2	128-256	Die Überwachung einer großen Anzahl von Hosts in kurzen Intervallen kann zusätzliche Kerne erfordern
ADMonitor	k.A.	k.A.	Keine signifikante Ressourcennutzung

Ein typischer EventSentry-Server, der **alle Komponenten** (einschließlich der Datenbank) nutzt, sollte über mindestens 4-8 Kerne und 8 GB Arbeitsspeicher verfügen (wobei die Ressourcennutzung durch Windows selbst bereits berücksichtigt ist). Zusätzlicher Speicher wird für größere Datenbanken empfohlen.

Berechtigungen

Die folgenden Berechtigungen sind für die Installation EventSentrymit der Setup-Anwendung erforderlich:

- Administrative Berechtigungen

oder

- Erlaubnis, Dienste zu schaffen und zu kontrollieren
- Erlaubnis, Dateien in %SYSTEMROOT%\SYSTEM32 zu schreiben
- Berechtigung zum Schreiben \Programmdateien-Verzeichnis

- Berechtigung zum Schreiben in den Registrierungsschlüssel HKEY_LOCAL_MACHINE\Software

> Die Installation von EventSentry auf einem Workstation-OS wie Windows 10 ist möglich, wird aber nicht empfohlen und für den produktiven Einsatz nicht unterstützt.

ADMonitor

Für die Arbeit von ADMonitor ist folgendes erforderlich:

- Der Host, auf dem ADMonitor installiert ist, muss Mitglied der Domäne sein, die er überwacht
- Das ADMonitor-Dienstkonto (**EventSentryADMonitor**) muss ein lokaler Administrator und Mitglied der Domänen-Administratorengruppe sein.
- Das ADMonitor-Dienstkonto (**EventSentryADMonitor**) muss Mitglied der **Enterprise** Admins-Gruppe sein, wenn eine Sub-Domäne überwacht wird.
- Die Gruppenrichtlinien-Verwaltungsfunktion muss installiert werden, um Gruppenrichtlinien-Änderungen zu überwachen
- Eingeschränkte Ueberwachung für "Account Management", "Directory Service Access" und "Active Directory Diagnostic Event Logging" ist erforderlich, um den Benutzer zu ermitteln, der eine Änderung vorgenommen hat (kann mit dem Administrator-Dienstprogramm konfiguriert werden)

Collector

Die folgenden Anforderungen werden für Hosts empfohlen, die den Collector-Dienst ausführen:

- Betriebssystem: Server-Betriebssystem, Windows 2012 R2 oder höher
- CPU: 4 oder mehr Kerne
- Speicher (RAM): Mindestens 512 Mb für den Collector verfügbar, 1 Gb oder mehr empfohlen

Network Services

Der Network Services-Dienst (zu dem der Syslog-, Snmp-, ARP- und NetFlow-Dämon gehört) erfordert mindestens eine 5-Host-Netzwerkgeräte-Lizenz, die NetFlow-Komponente erfordert mindestens eine NetFlow-Lizenz.

Für die in der EventSentry Light-Edition enthaltene Komponente "Netzwerkdienste", die nur 2 Remote-Hosts unterstützt und die Protokollierung eingehender Syslog- und/oder SNMP-Traps in einer Datenbank nicht unterstützt, ist keine Lizenz erforderlich.

NetFlow

Die folgenden Protokolle werden von der EventSentry NetFlow-Komponente unterstützt:

- NetFlow v1
- NetFlow v5
- NetFlow v9
- IPFIX
- sFlow

Agenten Management (Manuell oder MSI)

Agenten können entweder mit der Verwaltungskonsole oder mit MSI-Dateien installiert werden. Die folgenden Anforderungen müssen erfüllt sein, damit EventSentry-Agenten mit der Verwaltungskonsole bereitgestellt und verwaltet werden können:

- Die ADMIN$-Freigabe muss vorhanden sein, damit der Agent installiert werden kann.

- Die ADMIN$-Freigabe muss vorhanden sein, damit Konfigurationsaktualisierungen an die Agenten gepusht werden können. Wenn die ADMIN$-Freigabe vorhanden ist oder nicht vorhanden sein kann, können Sie stattdessen die ES$-Freigabe einrichten.
- Der **Client für Microsoft®-Netzwerke** muss installiert werden.

"Agent-Only" Installationsprogramme können von der Verwaltungskonsole generiert (erfordert kostenlose WiX-Software) und auf den Zielcomputern installiert oder bereitgestellt werden.

Der Collector (standardmäßig installiert) kann verwendet werden, um sowohl die Konfiguration als auch die Remote-Agenten auf dem neuesten Stand zu halten. Bei Verwendung des Collectors muss nur die Erstinstallation der Agenten durchgeführt werden (entweder mit Remote-Update oder einer MSI-Datei).

Web Reporting

Die EventSentry Web Reports unterstützen die folgenden Webbrowser:

- Mozilla Firefox 65 or higher
- Microsoft® Internet Explorer 11 or higher
- Microsoft® Edge (latest version)
- Google Chrome™ 72.0.3626 or higher
- Opera 58.0.3135.47 or higher
- Apple® Safari® 12.0.2 or higher

Ältere Versionen der oben aufgeführten Browser und nicht aufgeführte Browser funktionieren möglicherweise mit den EventSentry Web Reports, wurden jedoch nicht getestet.

Die EventSentry Web-Reports erforderen einen unterstützten Datenbankserver (siehe "Datenbank" unten) mit einer EventSentry Datenbank.

Anforderungen an die Datenbank

Siehe Datenbankanforderungen für weitere Informationen über ODBC-Treiber und unterstützte Datenbanken.

Hardware (optional)

Alle Sensoren, mit Ausnahme des reinen USB-Temperatur-/Feuchtesensors, sind erforderlich:

- Eine verfügbare serielle Schnittstelle (verwendet für die Datenerfassung)
- Ein verfügbarer USB-Anschluss (wird für die Stromversorgung verwendet)

Der reine USB-Sensor benötigt einen freien USB-Port sowie einen USB-zu-COM-Port-Treiber von FTDI Chip. Dieser Treiber ist im Unterverzeichnis "resources" des Hauptinstallationsverzeichnisses enthalten EventSentry.

2.1.1 Hardware-Spezifikationen für Sensoren

Hardware specifications for environment sensors manufactured by PCMeasure:

Sensor 30101 (temperature only)

Temperature Range	-30 to 100 degrees celsius
Absolute fail in this range	+/- 1,2 K
Non-linearity	0,4 K
Length	28 mm
Diameter	8,5 mm
Material	Ertacetal C
Cable	1,5 meters PVC, diameter 3,2 mm
Environment	for use in air

Sensor 30106 (temperature and humidity)

Temperature range	-30 to 80 degrees celsius
Absolute fail in this range	+/- 1,2 K
Non-linearity	0,4 K
Humidity range	0 to 100% relative humidity
Humidity accuracy	+/- 3.5% in range 20-80% humidity
Dimensions	60 x 58 x 25 mm
Environment	for us in air (inside)
Additional Information	Device has a Sub-D9 and USB connector and features a RJ 45 connector which supports an additional cable for a total lenght of up to 100 meters

2.1.2 Datenbanken

Datenbank-ODBC-Treiber

Wenn Daten in eine zentrale Datenbank konsolidiert werden, müssen die entsprechenden ODBC-Treiber für die Datenbank auf dem Host installiert werden wo EventSentry installiert ist (bei Verwendung des Collector), oder auf jedem Client, der in die Datenbank schreiben soll. Bei der Verwendung einer MSSQL-Server-Datenbank mit Windows® 2003 (oder neueren) Hosts ist keine Aktion erforderlich, aber weitere Informationen darüber, welche ODBC-Treiber installiert werden müssen, finden Sie in der folgenden Tabelle.

Database	Vista/2008, Win7/2008R2, Win 8/2012, Win 8.1/2012R2, Win 10/2016/2019/2022
PostgreSQL	inkludiert mit EventSentry Installation
Microsoft® SQL Server 2005-2022	im Lieferumfang des Betriebssystems enthalten, aber der neueste Treiber wird für serverseitige Komponenten empfohlen

Die Unterstützung für MySQL wird wahrscheinlich in zukünftigen Versionen von EventSentry beendet werden. Aktuellen Benutzern von MySQL wird empfohlen zu einer anderen Datenbank zu wechseln.

Datenbank-Unterstützungsebenen

EventSentry unterstützt 3 verschiedene Typen von SQL-Datenbankservern: PostgreSQL, Microsoft® SQL Server und MySQL (wird schrittweise eingestellt). EventSentry bietet je nach Typ und Version der Datenbank unterschiedliche Supportstufen. Diese verschiedenen Support-Level werden durch ihre jeweiligen Datenbank-Ebenen beschrieben, wie unten dargestellt:

Tier Level	Description
Tier 1 (recommended)	Die Datenbank wird vollständig unterstützt und wurde umfangreichen Tests unterzogen.
Tier 2	Die Datenbank wird unterstützt und hat grundlegende Tests durchlaufen.
Tier 3	Datenbank ist kompatibel mit EventSentry aber **nicht offiziell unterstützt** und nur minimal getestet. Benutzen Sie diese Datenbank nur wenn Sie Erfahrung mit ihr haben.

Datenbank (optional)

Ein Datenbankserver ist für die webbasierte Berichterstattung und bei der Konsolidierung von Ereignisprotokollen, Systemzustand und anderen Informationen in einer zentralen Datenbank erforderlich. Nicht alle Datenbanktypen und -versionen werden gleichwertig unterstützt, die Datenbank-Support-Ebene (siehe "Datenbank-Support-Ebenen" oben) beschreibt den Support-Level der Datenbank.

Datenbank	Supportstufe
PostgreSQL 9.1	3
PostgreSQL 9.6	2
PostgreSQL 14	1
Microsoft® SQL Server 2008 (32-bit or 64-bit)	2
Microsoft® SQL Server 2008 Express	2
Microsoft® SQL Server 2008 R2 (32-bit or 64-bit)	2
Microsoft® SQL Server 2008 R2 Express	2
Microsoft® SQL Server 2012	2
Microsoft® SQL Server 2012 Express	2
Microsoft® SQL Server 2014	1
Microsoft® SQL Server 2014 Express	1
Microsoft® SQL Server 2016	1
Microsoft® SQL Server 2016 Express	1
Microsoft® SQL Server 2017	1
Microsoft® SQL Server 2019	1
Microsoft® SQL Server 2022	1

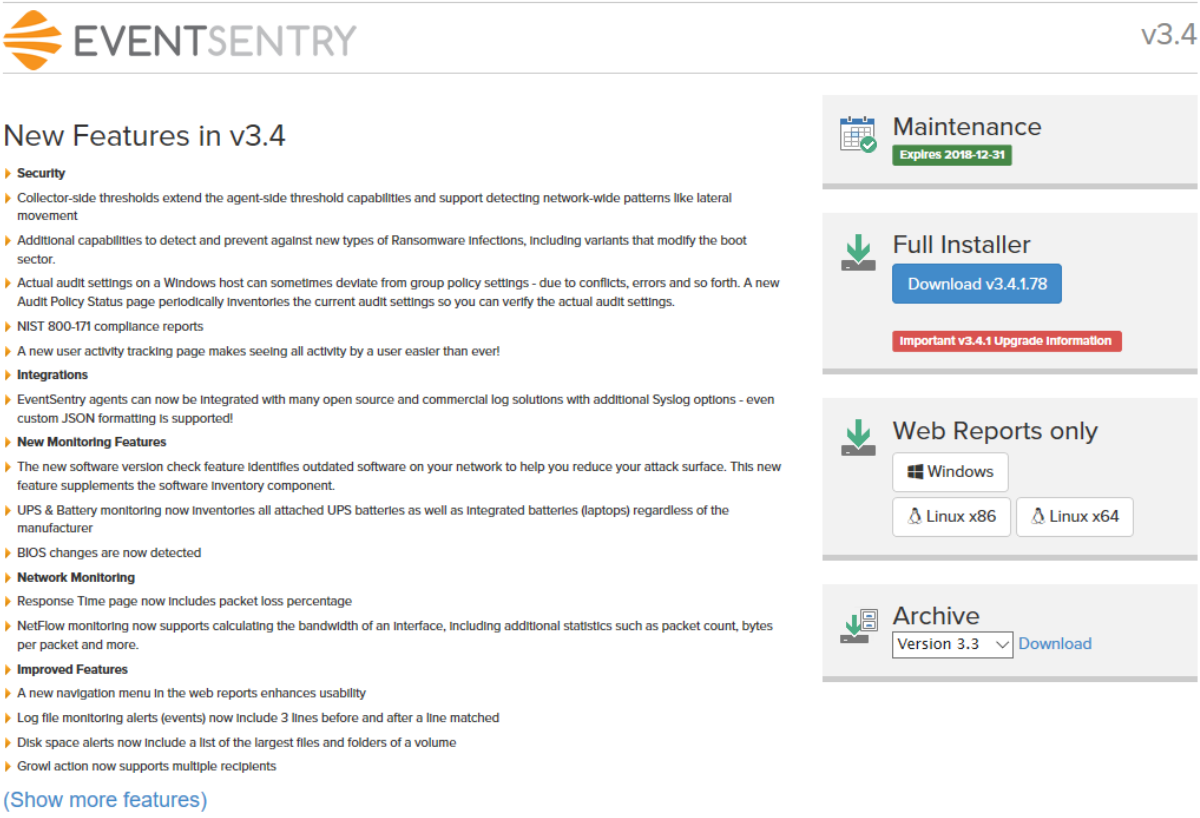
2.2 Erhalten von EventSentry

Um die neueste Version von EventSentry unserer Website zu erhalten, folgen Sie bitte den untenstehenden Schritten:

- Navigieren Sie zum Download-Bereich von http://www.eventsentry.com/ und folgen Sie dem Link **Jetzt herunterladen (nur für registrierte Benutzer)** oder rufen Sie den Kundenbereich unter https://store.netikus.net/customer/

- Folgen Sie den Anweisungen auf dieser Seite. Sie werden aufgefordert, sich mit Ihrer E-Mail-Adresse und Ihrem Passwort anzumelden.

- Sie werden ein Fenster ähnlich dem unten abgebildeten sehen. Klicken Sie auf **Download**, um die neueste Version herunterzuladen.



- Installieren Sie die Software. Das Setup-Programm aktualisiert die vorhandene Installation und erhält die Konfiguration.

2.3 EventSentry Lizenzieren

EventSentry erfordert eine gültige Lizenz, um zu laufen, derzeit haben wir Test- und Volllizenzen verfügbar. Für EventSentry Light ist derzeit keine Lizenz erforderlich.

Lizenzschlüssel können entweder aus einer Datei geladen werden (während der Installation und in der Verwaltungskonsole) oder in den Lizenzmanager in der Verwaltungskonsole eingefügt werden.

Da alle überwachten Rechner eine gültige Lizenz benötigen, können Sie mit Remote Update Lizenzinformationen an alle überwachten Rechner senden. Die Lizenzinformationen werden automatisch aktualisiert, wenn Sie die folgenden Fernaktualisierungsfunktionen ausführen:

- Konfiguration aktualisieren
- Upgrade-Agent(en)

Beachten Sie, dass Sie den Agenten neu starten müssen, um die Lizenzinformationen erneut einzulesen. Dies ist besonders wichtig, wenn Sie von einer Testlizenz zu einer Volllizenz wechseln.

Test-Lizenz

Eine Testlizenz erlaubt es Ihnen, EventSentry für einen begrenzten Zeitraum zu evaluieren, damit Sie feststellen können, ob sie Ihren Anforderungen an die Netzwerküberwachung entspricht. Der Testzeitraum beträgt derzeit 30 Tage und kann durch Kontaktaufnahme mit dem NETIKUS.NET-Vertrieb verlängert werden.

Sie können eine Probezeit beantragen, indem Sie zu http://www.eventsentry.com/downloads/trial navigieren und das Antragsformular für eine Probezeit ausfüllen.

Wenn Sie Ihre Evaluierung abgeschlossen haben, können Sie die Vollversion erwerben. Nach Abschluss Ihres Kaufs erhalten Sie einen Lizenzschlüssel zur dauerhaften Aktivierung Ihrer Testversion.

Vollständige Lizenz

Die Volllizenz erlaubt Ihnen die Nutzung EventSentry auf so vielen Computern, für die Sie Lizenzen erworben haben. Voll-Lizenzen laufen nicht ab, Support und Updates laufen jedoch ein Jahr nach dem ursprünglichen Kaufdatum ab.

Vollständige (Agenten-)Lizenzen

Vollständige Agentenlizenzen sind für jeden Host unter Microsoft Windows erforderlich, auf dem Sie das Ereignisprotokoll und/oder den Systemzustand überwachen möchten. Für die Überwachung der Ereignisprotokolle und des Systemzustands ist die Verwendung eines Agenten erforderlich, daher lautet der Lizenztyp **Agent**.

Netzwerkgeräte-Lizenzen

Sie können Lizenzen für Netzwerkgeräte verwenden, wenn Sie Hosts über die Heartbeat- oder Netzwerkdienste-Funktion überwachen, die Agenten jedoch **nicht** EventSentry auf diesen Computern installieren. Dies gilt sowohl für Unix/Linux-Computer als auch für Netzwerkgeräte wie Router, Switches usw..

Der Network Services Dienst erfordert mindestens eine 5-Host-Heartbeat-/Netzwerkgeräte-Lizenz.

Details zur Syslog- und SNMP-Lizenzierung

Wenn ein Netzwerkgerät Syslog- oder SNMP-Daten an EventSentry sendet, verwendet es eine Lizenz für **mindestens 24 Stunden** ab dem letzten Zeitpunkt, an dem das Gerät Daten gesendet hat. Wenn dieses Gerät 24 Stunden oder länger keine zusätzlichen Daten sendet, wird diese Lizenz anderen Netzwerkgeräten, die Daten senden, zur Verfügung gestellt.

NetFlow-Lizenzen
Die NetFlow-Komponente ist Teil der Netzwerkdienste, wird aber separat lizenziert. Um NetFlow nutzen zu können, muss für jeden installierten/aktivierten NetFlow-Collector eine NetFlow-Lizenz installiert werden. Wenn Sie z. B. 2 Router haben, die NetFlow-Daten an denselben EventSentry NetFlow-Collector senden, ist eine NetFlow-Lizenz erforderlich.

In den nächsten Kapiteln finden Sie Informationen und Screenshots zur korrekten Eingabe von Lizenzinformationen.

2.3.1 Entering a License

Wenn Sie EventSentry zum ersten Mal starten, dann sehen Sie den Lizenzierungsdialog, wie im folgenden Dialog dargestellt. Der Bereich **Informationen zur Testversion** zeigt an, wie viele Tage für die Evaluierung verbleiben (oder zeigt an, dass Sie die Vollversion ausführen), und Sie können mit der Schaltfläche **Lizenzen verwalten** eine neue Lizenz eingeben oder eine vorhandene Lizenz aktualisieren.

Wichtige Informationen über Lizenzen

1. Sie können nur maximal eine Testlizenz installieren.
2. Alle installierten Lizenzen müssen den **gleichen Organisationsnamen** haben.
3. Alle installierten Lizenzen müssen die gleiche Versionsnummer haben (siehe unten).
4. Sie müssen mindestens eine reguläre (Agenten-)Lizenz installiert haben, EventSentry funktioniert nicht, wenn Sie **nur** Lizenzen für Netzwerkgeräte oder NetFlow-Lizenzen installiert haben.

Versionsnummern und Ablaufdatum
Alle Lizenzen sind unbefristet und laufen nie ab, sondern funktionieren nur mit Versionen von EventSentry die vor dem Ablaufdatum der installierten Lizenzen veröffentlicht wurden.

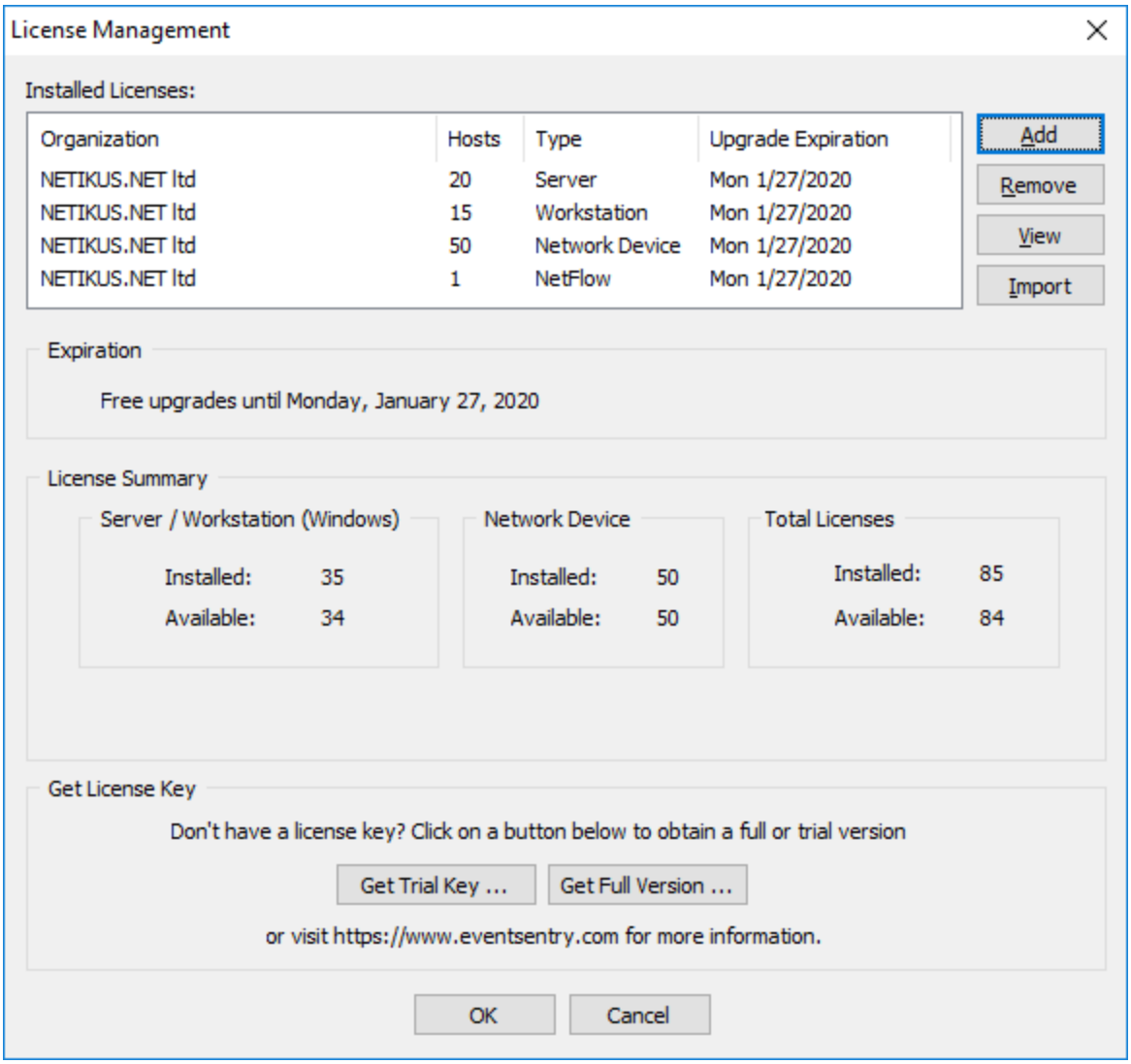
Beispiel
Sie können keine Version von EventSentry die am 1. Mai 2019 veröffentlicht wurde, wenn die installierten Lizenzen am 1. April 2019 ablaufen. Sie sind jedoch berechtigt, jede Version von EventSentry zu installieren, die am oder vor dem 1. April 2019 veröffentlicht wurde.

Das Ablaufdatum einer Lizenz spiegelt das Ende des Wartungsvertrags wider. Die Erneuerung der jährlichen Wartung und damit die Verlängerung des Wartungsablaufdatums führt dazu, dass neue Lizenzschlüssel generiert und an den Benutzer gesendet werden. Diese Lizenzschlüssel können einfach in die Verwaltungskonsole importiert werden.

Lizenzdialog ohne installierte Lizenz

Lizenzen verwalten

Nachdem Sie auf die Schaltfläche **Lizenzen verwalten** geklickt haben wird der Dialog Lizenzverwaltung angezeigt:



Das Dialogfeld Lizenzverwaltung listet alle installierten Lizenzen auf (bis zu 25 Lizenzen werden unterstützt) und zeigt die Gesamtzahl der installierten Lizenzen an, einschließlich der Anzahl der noch verfügbaren Lizenzen (*Total Available Licenses*).

Um eine neue Lizenz hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**. Um eine Lizenz zu entfernen, klicken Sie auf die Schaltfläche **Entfernen**. Sie können eine bereits installierte Lizenz anzeigen, indem Sie auf die Schaltfläche **Anzeigen** klicken.

Hinzufügen von Lizenzen

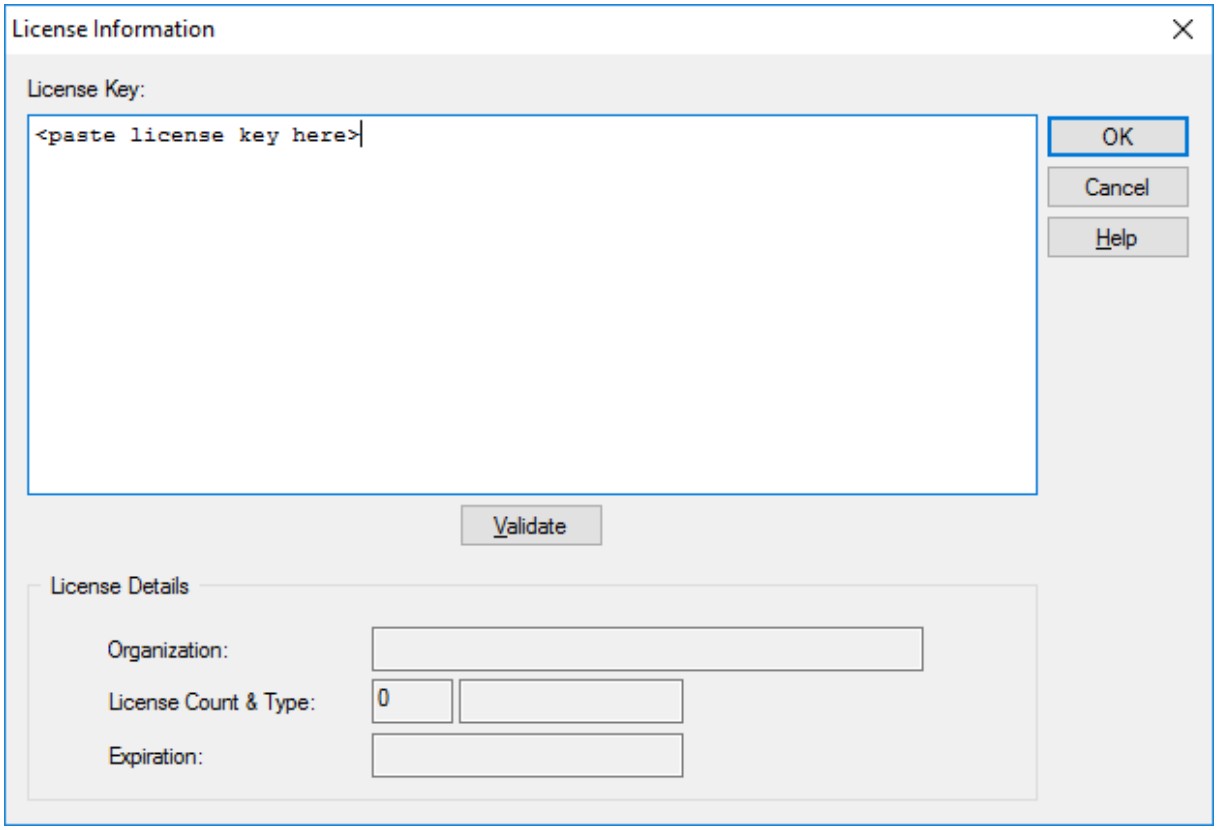
Lizenzen können entweder mit der Schaltfläche **Hinzufügen** einzeln hinzugefügt oder mit der Schaltfläche **Importieren** (empfohlen) in großen Mengen aus einer Datei importiert werden.

Importieren von Lizenzen

Wenn eine Lizenzdatei verfügbar ist, ist das Importieren der gesamten Datei mit allen in der Datei enthaltenen Lizenzschlüsseln der einfachste Weg, um Lizenzen hinzuzufügen. Lizenzdateien werden vom NETIKUS.NET Online Store immer dann versandt, wenn ein Wartungsvertrag verlängert oder neue Lizenzen erworben werden. Beim Importieren von Lizenzen werden **alle vorhandenen Lizenzen** durch die Lizenzen aus der Lizenzdatei **ersetzt**.

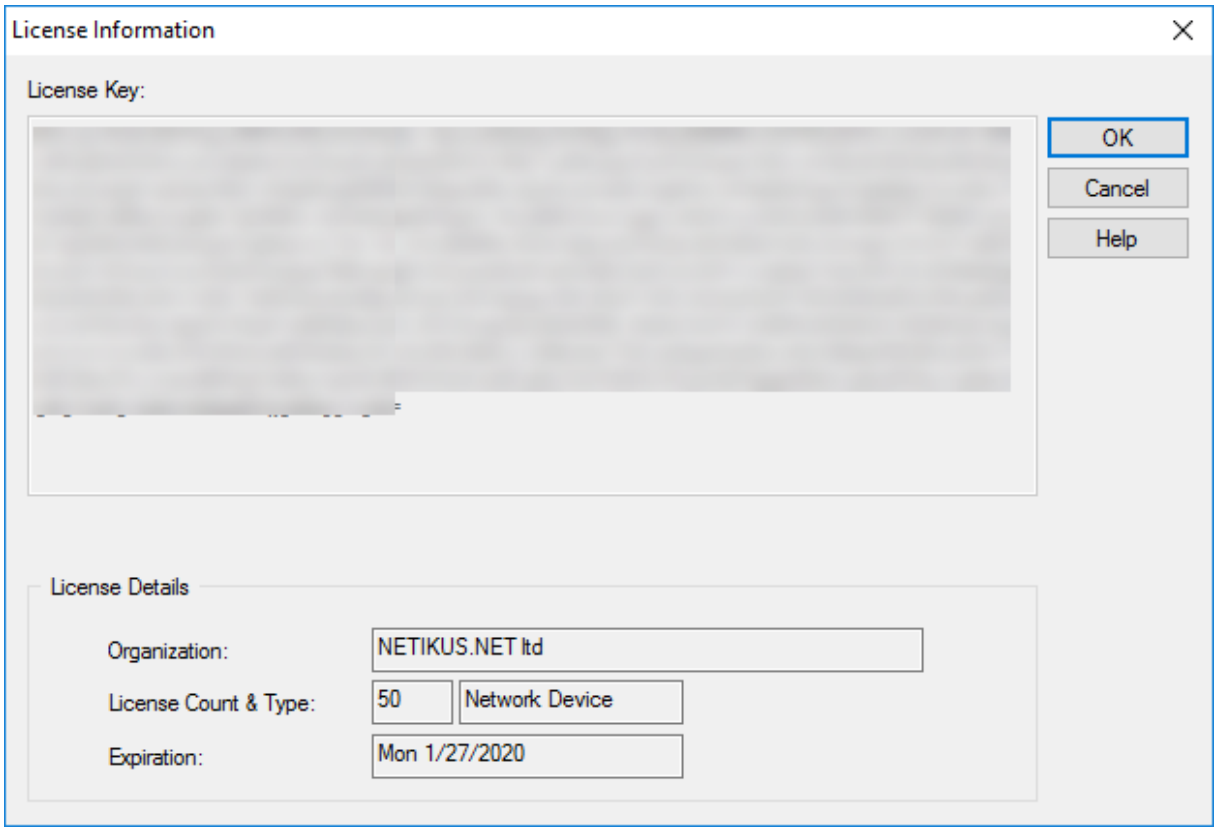
Hinzufügen einer Lizenz

Um eine einzelne Lizenz hinzuzufügen, klicken Sie auf die Schaltfläche Hinzufügen und fügen Sie den Lizenzschlüssel in das unten gezeigte Dialogfeld Lizenzinformationen ein.



Fügen Sie den gesamten Lizenzschlüssel **genau so ein, wie er in der E-Mail oder der Lizenzdatei erscheint.** Wenn der Schlüssel gültig ist, sollte er automatisch validiert und die Lizenzdetails unten ausgefüllt werden. Wenn Sie auf die Schaltfläche **Validate** klicken, wird manuell versucht, den Lizenzschlüssel zu validieren.

Ein validierter Lizenzschlüssel wird ähnlich wie der unten gezeigte Dialog angezeigt:



2.4 Lokale Installation (mit Installationsprogramm, Standard)

Zum Installieren EventSentry mit dem Installationsprogramm, führen Sie einfach das heruntergeladene Installationspaket aus, zum Beispiel eventsentry_v4_1_1_1_0_windows_setup.exe. Die folgenden optionalen Komponenten sind verfügbar:

Hilfe

Installiert die komplette Dokumentation sowie zusätzliche Handbücher im HTML-Format auf dem lokalen Rechner. Weitere Formate sind auch auf der Produktwebsite unter https://www.eventsentry.com/support/documentation verfügbar.

Eingebaute Datenbank

EventSentry unterstützt verschiedene Datenbanken, einschließlich der Standard-PostgreSQL-Datenbank, die mit dem Produkt ausgeliefert wird. Wählen Sie diese Komponente, um eine Instanz von PostgreSQL auf dem lokalen Computer zu installieren.

Bei der Auswahl dieser Komponente stehen die folgenden Optionen zur Verfügung:

Folder: Geben Sie an, wo die Datenbank gespeichert werden soll. **Wählen Sie ein Laufwerk/Verzeichnis mit ausreichendem Speicherplatz**.

Firewall: Geben Sie an, ob das Setup eine Firewall-Regel hinzufügen soll, um eingehenden Verkehr zur lokalen Datenbank (Port 5432) zuzulassen. Bei Verwendung des Collectors im Allgemeinen nicht erforderlich.

Admin Password: Geben Sie das Passwort für den administrativen Postgres-Benutzer an. Es wird dringend empfohlen, ein **sicheres** Passwort zu wählen.

Wählen Sie ein **sicheres** Passwort für den administrativen Postgres-Benutzer, er hat vollen Zugriff auf alle Daten.

Web Reports

Die Web Reports sind die Berichtsschnittstelle zur Datenbank. Die Web-Reports können entweder als Teil des Setups oder separat installiert werden (z.B. um sie auf einem anderen Host zu installieren). Wenn dieses Kästchen angekreuzt ist, werden die Web-Reports als Teil der Hauptinstallation installiert (standard).

Port:	Geben Sie den Standard-Port an, unter dem die Web Reports laufen sollen (standardmäßig 8080)
Service Port:	Geben Sie den Serviceport an, den die Web Reports verwenden sollen. Dieser Port ist nur auf dem lokalen Rechner zugänglich (standardmäßig 8081).
Firewall:	Geben Sie an, ob das Setup eine Firewall-Regel hinzufügen soll, um eingehenden Verkehr zu den Web Reports zuzulassen (standardmäßig Port 8080)

Wenn die Installation abgeschlossen ist, wird der Konfigurationsassistent gestartet und passt die Standardinstallation an. Er richtet die Standard-E-Mail-Benachrichtigung ein, schließt die Einrichtung der Datenbank ab und ermöglicht Ihnen die Konfiguration von Syslog- und SNMP- und anderen Funktionen.

2.5 Aktualisierung auf eine neue Version

EventSentry wird ständig weiterentwickelt und neue Versionen stehen für Sie zum Download auf unserer Website bereit. Bitte lesen Sie die nächsten Kapitel über die Aktualisierung EventSentry. EventSentry kommt mit kostenlosen Updates für ein Jahr, weitere Jahre Support und Updates sind gegen eine jährliche Gebühr erhältlich. Weitere Informationen zu den aktuellen Preisen finden Sie auf unserer Preisliste.

Wenn Sie EventSentry bereits installiert haben dann können Sie leicht nach einer neuen Version suchen, indem Sie zu Hilfe -> Nach Updates suchen navigieren oder http://www.eventsentry.com/downloads/version-history besuchen.

Wenn Sie ein registrierter Kunde mit einem aktiven Wartungsvertrag sind, finden Sie unter Getting EventSentry Anweisungen wie Sie die neueste Version herunterladen können.

2.5.1 Updating to v5.0

EventSentry v5.0 führt zwei wichtige Änderungen ein, die den Upgrade-Prozess im Vergleich zu früheren Upgrades komplexer machen, insbesondere für Benutzer, die die integrierte PostgreSQL-Datenbank verwenden.

Wenn Sie das neueste %PRODUCT%-Installationsprogramm ausführen, wird eine bestehende Installation auf die neueste Version 5.0 aktualisiert. Bevor Sie das Installationsprogramm ausführen, sollten Sie Ihre Einstellungen sichern (Home Export in der Konsole) und optional Ihre Datenbank sichern.

All server-side components of EventSentry, including the installer, built-in database and all utilities are now 64-bit. Agents are still available for 32-bit systems, but EventSentry can only be installed on 64-bit systems.

EventSentry now ships with the 64-bit version of PostgreSQL v14. This latest version of PostgreSQL includes a number of improvements that will make the built-in database faster and more reliable. Upgrading to v14 is not required but highly encouraged.

Several migration options will be available, see below for more details.

Clear text connections to the collector will be phased out in the next release of EventSentry. Users utilizing clear text connections with the collector need to migrate to TLS connections.

64-Bit Upgrade

Hauptdateien

Als Teil des Installationsprozesses werden alle Benutzerdaten (z. B. MIBs, Konfigurationssicherungen) aus dem bestehenden Installationsverzeichnis (z. B. **C:\Programme (x86)\EventSentry**) in das neue 64-Bit-Installationsverzeichnis (z. B. **C:\Programme\EventSentry**) verschoben. Alle benutzerdefinierten Verzeichnisse und Dateien, die sich im 32-Bit-Installationsverzeichnis befinden, sollten gesichert und manuell in das neue Installationsverzeichnis verschoben werden.

Nach dem Entfernen von Binär- und temporären Dateien (z. B. Installationsprogramme, Crash-Dumps) wird das 32-Bit-Installationsverzeichnis in das Zip-Archiv **backup_eventsentry_x86.zip** (im 64-Bit-Installationsordner) komprimiert.

ADMonitor

Da es sich bei den ADMonitor-Binärdateien der Version 4.2 und früher um 32-Bit-Programme handelt, die ebenfalls auf die 64-Bit-Plattform migriert wurden, werden alle mit ADMonitor verbundenen Daten ebenfalls in den 64-Bit-Installationsordner migriert. Alle 32-Bit-ADMonitor-Daten werden in das 64-Bit-Installationsverzeichnis verschoben und zu Sicherungszwecken komprimiert (im Unterverzeichnis **ADMonitor\backup** gespeichert).

PostgreSQL Upgrade

Wenn eine bestehende PostgreSQL 9.6 Datenbank erkannt wird, fragt das Installationsprogramm den Benutzer, ob die neuere v14 PostgreSQL Datenbank installiert werden soll.

Ein Upgrade von %PRODUCT% Version 3.2 oder früher, die noch PostgreSQL 9.1 verwendet, wird nicht unterstützt. Benutzer, die auf Version 5.0 upgraden möchten, sollten entweder zuerst auf %PRODUCT% 4.2 upgraden oder Support für weitere Optionen kontaktieren.

Bei der Installation von PostgreSQL v14 gibt es die folgenden zwei Möglichkeiten:

Option 1: Vorhandene Daten in PostgreSQL v9.6 archivieren, neue Daten in PostgreSQL v14 speichern

Bestehende Daten werden in PostgreSQL v9.6 beibehalten, aber alle neuen Daten werden in der aktualisierten v14-Datenbank gespeichert. Die bestehende v9.6-Datenbank wird weiterhin ausgeführt und ist über ein "Archiv"-Profil in den Webberichten zugänglich. Der Zugriff auf neue Daten erfolgt auf die gleiche Weise wie bisher. Dies ist der einfachste Ansatz mit der kürzesten Ausfallzeit und wird für große v9.6-Datenbanken empfohlen.

Option 2: Vorhandene Daten auf PostgreSQL v14 migrieren, v9.6 deaktivieren
Führt ein Skript aus, das die Daten aus der bestehenden v9.6-Datenbank in die aktualisierte v14-Datenbank kopiert und dabei das PostgreSQL-Dienstprogramm **pg_dumpall** verwendet. Die %PRODUCT%-Dienste werden während der Migration nicht verfügbar sein, und dieser Prozess ist potenziell zeitaufwändig (abhängig von der Hardware und der Größe der Datenbank). Da bei diesem Prozess Daten von einer Datenbank in die andere kopiert werden, wird freier Speicherplatz benötigt, der der Größe der bestehenden 9.6-Datenbank entspricht. Mit dieser Option entfällt die Notwendigkeit, die bestehende v9.6-Datenbank zu behalten, sie wird jedoch im Allgemeinen nur für kleinere Datenbanken empfohlen.

Das nachstehende Diagramm gibt einen Überblick über die Vor- und Nachteile der einzelnen Optionen:

	Option 1 (keine Datenmigration)	Option 2 (Datenmigration)
Beibehaltung der PostgreSQL v9.6-Datenbank für den Zugriff auf alte Daten	JA	NEIN
Möglichkeit, Suchvorgänge und Berichte mit alten und neuen Daten in Webberichten durchzuführen	NEIN	JA
Möglicherweise verlängerte Ausfallzeit von EventSentry	NEIN	JA
Potenzielles Fehlerrisiko bei der Datenmigration	NEIN	JA
Erfordert freien Speicherplatz auf der Grundlage der vorhandenen Datenbankgröße	NEIN	JA

Aktualisierung von v4.x
Keine spezifischen Anweisungen, Installationsprogramm ausführen.

Aktualisierung von v3.5
Führen Sie zuerst ein Upgrade auf v4.0 durch und folgen Sie dann den Upgrade-Anweisungen für v4.0.

Aktualisierung von v3.4
Ab Version 3.5 wird eine 64-Bit-Version des %PRODUCT% Heartbeat-Monitorsmitgeliefert . Der Konfigurationsassistent aktualisiert einen vorhandenen 32-Bit-Heartbeat-Dienst automatisch während des Post-Setup-Prozesses.

Aktualisieren von Version 3.3
Ab Version 3.4 wird eine 64-Bit-Version von Web Reports mitgeliefert. Das Installationsprogramm aktualisiert automatisch eine vorhandene 32-Bit-Installation von Web Reports, indem es die alte Version deinstalliert und die neue 64-Bit-Version während des Setups neu installiert. Eswird empfohlen, alle Konfigurationsdateien zu sichern, und einige Einstellungen müssen nach dem Upgrade möglicherweise manuell bearbeitet werden. Weitere Informationenfinden Sie in KB 370.

Aktualisierung von v3.2
Ein direkter Upgrade-Pfad von v3.2 wird nicht unterstützt. Um auf Version 5.0 zu aktualisieren, müssen die Benutzer zunächst auf Version 4.2 und dann auf Version 5.0 aktualisieren.

2.5.2 Updating to v4.2

Ausführen des neuesten Installationsprogrammes aktualisiert eine vorhandene auf die neuesten 4.2.x-Build. Bevor Sie das Installationsprogramm starten, sollten Sie Ihre Einstellungen sichern (Home > Export in der Konsole) und optional Ihre Datenbank sichern. Nachdem das Setup abgeschlossen ist und alle Dateien aktualisiert wurden, wird der Konfigurationsassistent alle konfigurierten Datenbanken auf das neueste Schema aktualisieren.

Zukünftige Versionen des EventSentry Installationsprogrammes unterstützt möglicherweise nur 64-Bit-Plattformen. 32-Bit-Plattformen können weiterhin mit dem Agenten überwacht werden, aber alle serverseitigen Komponenten werden nur 64-Bit-Systeme unterstützen. Es wird in Erwartung dieses Wandels empfohlen EventSentry nur auf 64-Bit-Plattformen zu installieren.

Die Unterstützung für MySQL wurde in v4.2 eingestellt. Gegenwärtigen Benutzern einer MySQL Datenbanken wird dringend empfohlen, zu einer anderen Datenbank zu wechseln. Weitere Informationen zu den unterstützten Datenbanktypen und -versionen finden Sie unter Datenbank.

Updating from v4.0 and v4.1

No specific instructions, run installer.

Updating from v3.5

No specific instructions, run installer.

Updating from v3.4

Version 3.5 and later ship with a 64-bit version of the EventSentry Heartbeat Monitor, the configuration assistant will automatically upgrade an existing 32-bit heartbeat service during the post-setup process.

Updating from v3.3

Version 3.4 and later ship with a 64-bit version of the Web Reports, the installer will automatically upgrade an existing 32-bit web reports installation by uninstalling the old and re-installing the new 64-bit version during setup. It is recommended to backup all configuration files and some settings may need to be edited manually after the upgrade, see KB 370 for more details.

Updating from v3.2

Version 3.3 introduced a number of important changes, including a new version of the built-in database. Click here for more information. Also see updating from v3.3 above.

Updating from v3.0 or v3.1

Version 3.2 introduced the new collector component, see Collector for more information. Also see updating from version 3.2 and v3.3 above.

Updating from v2.9x

When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to "Updating from v3.0" listed above.

2.5.3 Updating to v4.1

Ausführen des neuesten Installationsprogrammes aktualisiert eine vorhandene auf die neuesten 4.1.x-Build. Bevor Sie das Installationsprogramm starten, sollten Sie Ihre Einstellungen sichern (Home > Export in der Konsole) und optional Ihre Datenbank sichern. Nachdem das Setup abgeschlossen ist und alle Dateien aktualisiert wurden, wird der Konfigurationsassistent alle konfigurierten Datenbanken auf das neueste Schema aktualisieren.

Dieses Update fügt der Syslog-Tabelle zusätzliche Spalten hinzu, um die Bestätigung von Syslog-Meldungen zu unterstützen. Auf Installationen mit einer großen Menge an Syslog-Daten kann der Post-Update-Prozess je nach Datenbankleistung und Menge der vorhandenen Syslog-Daten viel länger als üblich dauern.

Zukünftige Versionen des EventSentry Installationsprogrammes unterstützt möglicherweise nur 64-Bit-Plattformen. 32-Bit-Plattformen können weiterhin mit dem Agenten überwacht werden, aber alle serverseitigen Komponenten werden nur 64-Bit-Systeme unterstützen. Es wird in Erwartung dieses Wandels empfohlen EventSentry nur auf 64-Bit-Plattformen zu installieren.

Die Unterstützung für MySQL wird in zukünftigen Versionen von EventSentry auslaufen. Gegenwärtigen Benutzern einer MySQL Datenbank wird dringend empfohlen, zu einer anderen Datenbank zu wechseln. Weitere Informationen zu den unterstützten Datenbanktypen und -versionen finden Sie unter Datenbank.

Updating from v4.0

No specific instructions, run installer.

Updating from v3.5

No specific instructions, run installer.

Updating from v3.4

Version 3.5 and later ship with a 64-bit version of the EventSentry Heartbeat Monitor, the configuration assistant will automatically upgrade an existing 32-bit heartbeat service during the post-setup process.

Updating from v3.3

Version 3.4 and later ship with a 64-bit version of the Web Reports, the installer will automatically upgrade an existing 32-bit web reports installation by uninstalling the old and re-installing the new 64-bit version during setup. It is recommended to backup all configuration files and some settings may need to be edited manually after the upgrade, see KB 370 for more details.

Updating from v3.2

Version 3.3 introduced a number of important changes, including a new version of the built-in database. Click here for more information. Also see updating from v3.3 above.

Updating from v3.0 or v3.1

Version 3.2 introduced the new collector component, see Collector for more information. Also see updating from version 3.2 and v3.3 above.

Updating from v2.9x

When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to "Updating from v3.0" listed above.

2.5.4 Updating to v4.0

Running the latest EventSentry installer will update an existing installation to the latest 4.0.x build. Prior to running the installer, you should back up your settings (Home > Export in the console) and optionally

back up your database. After the setup has completed and all files are updated the configuration assistant will update all configured databases to the latest schema.

Updating from v3.4

Version 3.5 and later ship with a 64-bit version of the EventSentry Heartbeat Monitor, the configuration assistant will automatically upgrade an existing 32-bit heartbeat service during the post-setup process.

Updating from v3.3

Version 3.4 and later ship with a 64-bit version of the Web Reports, the installer will automatically upgrade an existing 32-bit web reports installation by uninstalling the old and re-installing the new 64-bit version during setup. It is recommended to backup all configuration files and some settings may need to be edited manually after the upgrade, see KB 370 for more details.

Updating from v3.2

Version 3.3 introduced a number of important changes, including a new version of the built-in database. Click here for more information. Also see updating from v3.3 above.

Updating from v3.0 or v3.1

Version 3.2 introduced the new collector component, see Collector for more information. Also see updating from version 3.2 and v3.3 above.

Updating from v2.9x

When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to "Updating from v3.0" listed above.

2.5.5 Updating to v3.5

Running the latest EventSentry installer will update an existing 3.x installation to the latest 3.5.1 build. Prior to running the installer, you should back up your settings (Home > Export in the console) and back up your database. After the setup has completed and all files were updated, the configuration assistant will update all configured databases to the latest schema and update the local heartbeat agent (if installed) to 64-bit. See below for additional details.

Updating from v3.3 and later

Version 3.4 and later ship with a 64-bit version of the Web Reports, the installer will automatically upgrade an existing 32-bit web reports installation by uninstalling the old and re-installing the new 64-bit version during setup. It is recommended to backup all configuration files and some settings may need to be edited manually after the upgrade, see KB 370 for more details.

Updating from v3.2

Version 3.3 introduced a number of important changes, including a new version of the built-in database. Click here for more information. Also see updating from v3.3 above.

Updating from v3.0 or v3.1

Version 3.2 introduced the new collector component, see Collector for more information. Also see updating from version 3.2 and v3.3 above.

Updating from v2.9x

When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to "Updating from v3.0" listed above.

2.5.6 Updating to v3.4

Running the latest EventSentry installer will update an existing 3.x installation to the latest 3.4.1 build. Prior to running the installer, you should back up your settings (Home > Export in the console) and back up your database. After the setup has completed and all files were updated, the configuration assistant will update all configured databases to the latest schema. See below for additional details.

Updating from v3.3

Version 3.4 ships with a 64-bit version of the Web Reports, the installer will automatically upgrade an existing 32-bit web reports installation by uninstalling the old and re-installing the new 64-bit version during setup. It is recommended to backup all configuration files and some settings may need to be edited manually after the upgrade, see KB 370 for more details.

Updating from v3.2

Version 3.3 introduced a number of important changes, including a new version of the built-in database. Click here for more information. Also see updating from v3.3 above.

Updating from v3.0 or v3.1

Version 3.2 introduced the new collector component, see Collector for more information. Also see updating from version 3.2 and v3.3 above.

Updating from v2.9x

When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to "Updating from v3.0" listed above.

2.5.7 Updating to v3.3

Important Changes

EventSentry v3.3 introduces two major changes which impact the upgrade process more than previous updates:

- A new built-in database, PostgreSQL v9.6, ships with v3.3
- A 64-bit EventSentry agent is now available

PostgreSQL v9.6

Since (security) updates no longer available for the previously included PostgreSQL v9.1 database, EventSentry now ships with a newer version of PostgreSQL. Upgrading an existing database is not required, see KB article 332 which outlines all available upgrade options. For users utilizing the legacy built-in database, it is recommended to install the new v9.6 database, even if it will not be utilized immediately.

64-Bit Agent

A 64-bit agent is now available for hosts running a 64-bit version of Windows. A 64-bit agent makes it possible that 64-bit performance counters can be read from the agent, and that accessing 64-bit OS files (e.g. C:\Windows\System32) no longer requires disabling FS redirection. Please note that not all EventSentry components will be 64-bit, for example the management console is still a 32-bit process (although a 64-bit version is available).

Updating from v3.x

Running the latest EventSentry installer will update an existing 3.x installation to the latest 3.3.x build. Prior to running the installer, you should back up your settings (Home > Export in the console) and back up your database. After the setup has completed and all files were updated, the configuration assistant will update all configured databases to the latest schema. No further action is required.

Updating from v2.9x

When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to "Updating from v3.0" listed above.

2.5.8 Updating to v3.2

Updating from v3.0 and 3.1

Running the latest EventSentry installer will update an existing 3.0.1 or 3.1.1 installation to the latest 3.2.x build. Prior to running the installer, you should back up your settings (Home > Export in the console) and back up your database After the setup has completed and all files were updated, the configuration assistant will update all configured databases to the latest schema. No further action is required.

Important: Version 3.2 includes the new "collector" component which can either be activated during the upgrade with the configuration assistant or installed and configured after the upgrade is complete. See Collector for more information.

Updating from v2.9x

When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to "Updating from v3.0" listed above.

2.5.9 Updating to v3.1

Updating from v3.0

Running the latest EventSentry installer will update an existing 3.0.1 installation to the latest 3.1.x build. Prior to running the installer, you should back up your settings (Home > Export in the console) and back up your database. After the setup has completed and all files were updated, the configuration assistant will update all configured databases to the latest schema. No further action is required.

Updating from v2.9x

When updating from EventSentry v2.9x, refer to Updating to v3.0 for a list of major changes which affect an update to version 3.x. A configuration update (File -> Export) through the management console is recommended prior to upgrading. The update procedure is identical to "Updating from v3.0" listed above.

2.5.10 Updating to v3.0

The biggest change when updating to version 3.0 from any earlier version are the new web reports which no longer require IIS. The new web reports run on Windows, Linux and Apple OS X and utilize Java on the server side (included with the EventSentry installation). The new web reports also ship with their own web service. The existing web reports (referred to as the "Legacy Web Reports") will not be uninstalled by the 3.0 upgrade, refer to this KB article for instructions on how to uninstall.

Version 3.0 includes an improved filter scheduling feature, with the ability to setup more granular recurring & summary filters. We recommend that you review the "Hour/Day" tabs on all filters which have custom settings configured in that tab.

Web Reports

The new web reports include a variety of new functionality, including the following:

- UTC support for networks spanning multiple time zones
- Built-in web service which no longer relies on IIS
- Cross-platform capabilities for Linux and OS X support
- Ability to schedule & email reports
- Improved search capabilities for complex search queries
- PDF output

Java **is not required** on the client side - only on the host where the web reports are running.

SNMP Polling (Heartbeat Monitoring)

The heartbeat agent includes the ability to query SNMP counters from SNMP-enabled hosts through the existing performance monitoring feature. In addition to polling counters, the HB agent can also query disk space, uptime and basic hardware / OS information.

Ribbon (Management Console)

The management console offers a redesigned interface featuring the ribbon as well as updated icons throughout the interface. The following new features have also been added:

- Support to view application and services event logs with the build-in event viewer
- Better interface to configure day/time schedules, summary & recurring event filters
- Recurring events can now be configured to check minutely intervals
- Authentication has been redesigned so that credentials are created & applied to hosts or groups
- Misc usability improvements throughout the management console

Monitoring

- Log file monitoring supports sub folders
- Compliance "Logon By Type" tracking can exclude logons by computer accounts
- Event Log filters can override email subject & message body
- Packages can by dynamically assigned based on platform (32bit vs 64bit)
- Threshold filters can utilize insertion strings
- Disk space prediction feature (predicts when disk will be full)
- Identify reasons why hosts were shut down or rebooted
- Desktop notification supports Growl
- Network notification supports remote desktop services
- Application scheduler support process isolation
- New email format "HTML Modern"

Network Services

The network services include a new "ARP" daemon, which monitors network traffic and alerts users when new MAC addresses are found or MAC to IP associations change. The ARP daemon also keeps track of all significant MAC address changes and the current status of all MAC addresses and their IP associations can be reviewed through the web reports.

2.5.11 Updating from v2.7x to v2.90

Please follow these steps to update from EventSentry version 2.7x / 2.8x to version 2.90.

1. Just in case there are problems with the update, export the configuration using the File -> Export function of the management console.

2. Run the EventSentry 2.9x installer on the same machine where you previously ran the installer. You should not be prompted for license or setup information. The same setup options that were selected when you installed the previous version of EventSentry should be automatically selected. If not, then please ensure that the same settings are selected.

3. If you are currently using a **MSSQL or MySQL database** then make sure that you select the respective option on the **Custom Setup** page of the setup when you update. This ensures that all tables in the EventSentry database are updated, **a requirement** before you can update the agents.

If you are using Oracle or Access then you will need to run the Database Setup Wizard in order to update the current database to the latest standard. It is recommended that you run the Database Setup Wizard as soon as the installation is complete to avoid problems with the agents writing to the database.

4. A reboot is generally not required, but might be necessary depending on the OS you are using and other dynamic factors.

5. Once the setup is complete and the database has been updated (if the **ESObjectTracking** table exists in the EventSentry database then you know that you are database has been updated) you can start pushing out the updated agent.

Navigate to Remote -> Update Agent(s) to push the new agent to all remote monitored machines.

2.5.12 Updating from v2.60 to v2.70

This chapter contains very important information for users updating to version 2.7x from earlier versions of EventSentry. Read this chapter **carefully to avoid losing** parts of your configuration.

Local Filters

With the introduction of filter packages, the previously introduced Local Filters feature has become obsolete and will not be supported anymore. While local filters will be migrated to a "Local Filters Package" on the computer where you run the EventSentry setup, they will **be lost** on remote computers that are updated with the remote update feature.

Local filters from version 2.60 (and earlier) will be lost the first time you update the remote agents or push the configuration.

If you need to retain the local filters that you created on remote computer then you will have follow the steps below:

1. Connect to the remote computers that have local filters and note down the names and properties of these filters, including the computer name.
2. After you have migrated to version 2.70 create a filter package, for example "Custom Filters".
3. Add all the filters to this package, and make sure that enter the computer name where these filters are from in the Computer Name field. This will ensure that the filter will only be processed on that computer.
4. Make the package global or assign it to all computers that had local filters in version 2.60.

Global Filters

With the introduction of filter packages, the previously introduced Global Filters feature will not be available anymore, instead you can create **global packages** that will be processed on all computers. Global filters will be automatically migrated to a **Migrated Global Filters** package when updating to version 2.70.

Packages

Starting with version 2.70, filters are not organized through groups, global and local containers anymore. Instead, filters are organized into filter packages which are then assigned to either groups or computers. Filter packages can also be made global so that they apply to all computers, regardless of group membership.

Your configuration will of course be preserved, and all filters that previously belonged to a group will be automatically migrated to a package. For example, all filters from the SERVERS group will be migrated to **Migrated filters from SERVERS**. Health and tracking packages are now also organized using packages, and will migrated in a similar fashion.

We recommend that you review your configuration after the migration carefully and make adjustments as necessary. For example, you will almost always be able to consolidate your health packages into one or two packages.

Filter package order is not relevant for package/filter processing. Exclude filters will always be processed before include filters, regardless of their package order.

Database

Since new tables were added to the database it **is also necessary to update the database**. If you are using Microsoft® SQL Server, then you the database will be automatically updated during the installation, **make sure that you select the database feature** and provide login information.

If you are using MySQL, Oracle or Access then you will need to update the database using the Database Setup Wizard. Running the Database Setup Wizard after the installation has been updated will ensure that all necessary tables exist.

Upgrading from EventSentry v2.60 to v2.70 (or later)

1. Download the most current setup file and start the installation on the machine where the management console is installed. You will **not** have to apply any patches if you download the latest setup, which already has all patches incorporated into it.

2. The MSI installer will now automatically upgrade your existing installation. If the upgrade fails, uninstall version 2.60 (make sure you have a configuration backup) and then run the latest setup again. If your configuration was not preserved, import the previously exported configuration (File -> Import).

3. Perform a **Remote Update "Manage Agent(s)"** to update the service on the remaining computers, and ensure that "Always update configuration when updating remote agents" is checked in **Tools -> Options -> Remote Update**. Read the **Local Filters** section above as local filters on remote computers will be discarded when you update the configuration on remote hosts.

2.5.13 Updating from v2.50 to v2.60

Please follow the instructions below to update all EventSentry installations in your network. Always make sure that you **export the configuration** prior to any version upgrade.

Upgrading from EventSentry v2.50 to v2.60 (or later)

1. Download the most current setup file and start the installation on the machine where the management console is installed. You will **not** have to apply any patches if you download the latest setup, which already has all patches incorporated into it.

2. The MSI installer will now automatically upgrade your existing installation. If the upgrade fails, uninstall version 2.50 (make sure you have a configuration backup) and then run the latest setup again. If your configuration was not preserved, import the previously exported configuration (File -> Import).

3. Perform a **Remote Update "Manage Agent(s)"** to update the service on the remaining computers.

Upgrading from EventSentry v2.43 (or earlier) to v2.50 (or later)

1. Uninstall the currently installed version from the template (management) machine and make sure that you keep the configuration.

2. *MySQL and Oracle only:* Run the Database Setup Wizard to initialize the new EventSentry database.

3. *Optional:* Run the Database Migration Wizard to migrate data from the existing to the new database.

4. **Configure new features and save the configuration.** It is recommended that you change ODBC actions to use connection strings instead of System DSN names.

5. Perform a **Remote Update "Manage Agent(s)"** and update the service on the remaining computers.

Upgrading from EventSentry v2.x to v2.43 (or earlier)

1. Download the most current setup file (eventsentry_v2.XX_setup.exe). Run the setup on all template (management) machines. An uninstall of the current version is not required. A reboot is not required.

2. **Configure new features and save the configuration.**

3. Perform a **Remote Update "Update Configuration"** and update **all** settings.

4. Perform a **Remote Update "Manage Agent(s)"** and update the service on the remaining computers.

Upgrading from EventSentry v1.x to v2.30

1. If EventSentry Light v1.x was installed with the installer then uninstall it first.

2. Install the 2.x version of EventSentry on the management computer in your network; the existing service will be stopped and updated, the configuration will be preserved.

3. If applicable remove all left over files that belong to EventSentry v1.x (e.g. eventsentry_gui.exe)

4. Launch the management interface and verify that the configuration was converted correctly.

5. **Configure new features and save the configuration.**

6. Perform a **Remote Update "Update Configuration"** and update **all** settings.

7. Perform a **Remote Update "Manage Agent(s)"** and update the service on the remaining computers.

Users who installed EventSentry Light 1.x with the setup routine should completely uninstall EventSentry Light 1.x and perform a new installation from scratch. Note that this affects only computers where EventSentry Light version 1.x was setup with the installation routine.

2.5.14 Upgrading from EventSentry Light

If you have purchased EventSentry after evaluating EventSentry Light then you will need to upgrade all EventSentry Light installations.

To upgrade to EventSentry after using EventSentry Light you will need to upgrade one computer manually (**1. below**) and then, if you have multiple installations, perform a remote update (**2. below**). You can also update the service manually on each computer if you wish.

1. On the Local (template) Machine

1. If you are upgrading from EventSentry Light Version 1.x and ***installed it with the installer*** then you will need to **uninstall EventSentryLight v1.x first**. Otherwise just skip this step.
2. Install EventSentry with the setup program.

2. On Multiple Remote Machines

1. Make sure that the computer from which you are performing the remote update has the latest and full version of EventSentry installed (see above).
2. Add all the computers you wish to update to the remote update - either manually or by importing them.
3. Choose **Update** from the Manage Agent(s) submenu.
4. The service on the remote machines will be stopped, the service executable updated, and the service restarted. Please note that the service will only be restarted on the those computers where the service was running.

2.5.15 Upgrading from the EventSentry Trial Version

If you have purchased EventSentry after evaluating the trial version of EventSentry then you will need to update the license information on all EventSentry installations. A reboot is not necessary.

To upgrade to EventSentry after using the trial version of EventSentry you will need to upgrade one computer manually (**1. below**) and then, if you have multiple installations, perform a remote update (**2. below**). You can also update the licensing information manually on each computer if you wish.

1. On the Local Machine (Management Workstation)

1. Enter your full license by launching the **EventSentry License Management** which can be found in the Program Files folder.

2. On Multiple Remote Machines

1. Make sure that the computer from which you are performing has the full license configured.
2. Add all the computers you wish to update to the remote update.
3. Right-click the **Groups** node in the left pane and select **Remote Update -> Manage Agent(s) -> Update**. Alternatively you can also right-click the **Computers** node in a selected group and select **Manage Agent(s) -> Update**.
4. The service on the remote machines will be stopped, the service executable and license information updated, and the service restarted. Please note that the service will only be restarted on the those computers where the service was running.

2.5.16 Fortgeschrittene Benutzer

Die folgenden zwei Kapitel beschreiben, wie erweiterte Update-Funktionen durchgeführt werden, die normalerweise nur bei der Fehlerbehebung erforderlich sind. Die meisten Benutzer können diese Kapitel überspringen.

2.5.16.1 Manuelle Aktualisierung des Dienstes

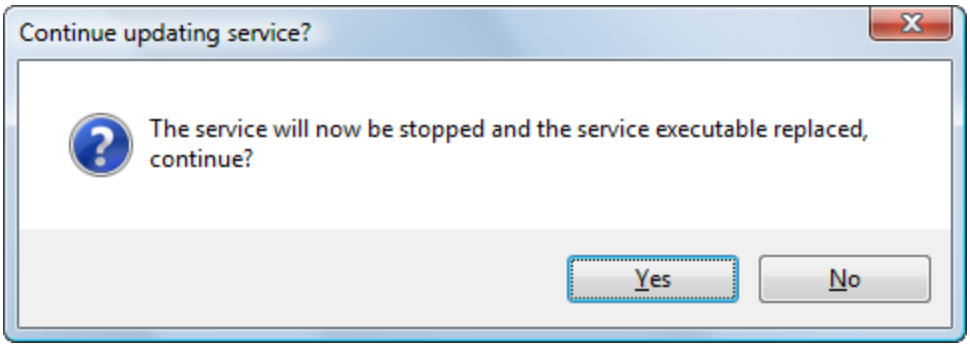
In diesem Abschnitt wird beschrieben, wie die EventSentry-Dienste manuell aktualisiert werden können.

Auf der lokalen Maschine

Der Dienst für den lokalen Agenten, den Heartbeat-Dienst, den Collector und/oder die Netzwerkdienste kann manuell aktualisiert werden. Je nachdem, für welche Komponente eine Aktualisierung erforderlich ist, klicken Sie auf eines der folgenden Symbole im linken Baum:

- Services
- Collector
- Heartbeat
- Network Services

Klicken Sie dann im Dialogfeld der Komponente auf die **Schaltfläche Aktualisieren**. Sie werden aufgefordert auf den Ordner zu zeigen, in dem sich die neue Version des Dienstes befinden wird.



Nachdem Sie das Dialogfenster mit **Ja** bestätigt haben, erscheint die

- der Dienst wird eingestellt
- die ausführbare Dienstdatei wird ersetzt
- und der Dienst wird neu gestartet (falls er vor der Aktualisierung lief)

Auf mehreren entfernten Rechnern

1. Stellen Sie sicher, dass auf dem Computer, von dem aus Sie das Remote-Update durchführen, die neueste Version des Dienstes installiert ist oder dass Sie Zugriff auf die neueste ausführbare Dienstdatei haben.
2. Fügen Sie alle Computer, die Sie aktualisieren möchten, in die entsprechende(n) Gruppe(n) ein.
3. Klicken Sie mit der rechten Maustaste auf "Computergruppen" oder die Gruppe, die ein Update erfordert, und wählen Sie "Agent(s) verwalten -> Upgrade".
4. Der Dienst auf den entfernten Rechnern wird angehalten, die ausführbare Dienstdatei aktualisiert und der Dienst neu gestartet. Bitte beachten Sie, dass der Dienst nur auf den Computern neu gestartet wird, auf denen der Dienst ausgeführt wurde.

2.5.16.2 Manuelle Aktualisierung der GUI und der Dokumentation

Dieser Abschnitt beschreibt, wie Sie die EventSentry-GUI, die Nachrichtendatei und die Dokumentation aktualisieren können.

Verwaltungskonsole(GUI)

Um die Verwaltungskonsolezu aktualisieren, ersetzen Sie eventsentry_gui.exe mit der aktualisierten Version des Archivs.

Nachrichtendatei

Um die Nachrichtendatei zu aktualisieren, ersetzen Sie %SYSTEMROOT% \system32\eventsentry_svc_x64.exe mit der aktualisierten Version des Archivs. Bitte beachten Sie, dass Sie alle Anwendungen, die das Ereignisprotokoll sperren, wie z.B. die Windows-Ereignisanzeige, schließen müssen, bevor Sie die Meldungsdatei ersetzen können.

Unter Windows Server 2003 müssen Sie den WinMgmt-Service vor dem Ersetzen stoppen/starten oder pausieren/fortsetzen eventsentry_svc_x64.exe. Starten Sie den Dienst neu, nachdem Sie die Datei aktualisiert haben.

Dokumentation

Um die Dokumentation zu aktualisieren, ersetzen Sie eventsentry_hlp.chm mit der aktualisierten Version des Archivs. Die Hilfedatei sollte sich immer im gleichen Verzeichnis wie die Verwaltungskonsole befinden eventsentry_gui.exe.

2.6 Verschieben von EventSentry auf einen neuen Server

Siehe KB 496 für Anweisungen zum Verschieben einer EventSentry-Installation auf einen neuen Server.

2.7 Agenten-Installation

Sie können den EventSentry Agenten auf verschiedenen Arten auf entfernten Rechnern installieren:

Fern-Update
Die **bevorzugte und einfachste** Methode zur Installation des EventSentry Agenten auf entfernten Computern ist die Verwendung von Remote-Update. Mit Remote-Update können Sie Agenten installieren, sie auf die neueste Version aktualisieren oder die neueste Konfiguration verschieben. Siehe unten, wenn Sie den Dienst "Collector" verwenden.

EventSentry MSI
Wenn die überwachten Computer Teil einer Active Directory-Umgebung sind oder wenn Sie eine andere Software einsetzen, die die Bereitstellung von MSI-Dateien unterstützt, können Sie eine EventSentry Agent MSI-Datei erstellen und den EventSentry Agent auf diese Weise bereitstellen. Diese Option ist vorzuziehen, wenn Sie keinen Zugriff auf die ADMIN$-Freigabe der überwachten Computer haben (das kostenlose WIX Toolset v3.x ist erforderlich, um 32-Bit-MSI-Pakete zu erstellen, 64-Bit-MSI-Installationspakete können nativ von der Management Console erstellt werden).

Collector
Sobald die Agenten verteilt sind (entweder über die Verwaltungskonsole oder mit MSI-Dateien), kann der Collector die Remote-Agenten auf die neueste Version patchen und auch automatisch die neueste Konfiguration übertragen (mehr Info).

Die standardmäßige Verwaltungsfreigabe **ADMIN$** (die das Verzeichnis **%SYSTEMROOT%** gemeinsam nutzt) muss vorhanden sein, damit die Agenten mit der Verwaltungskonsole installiert werden können.

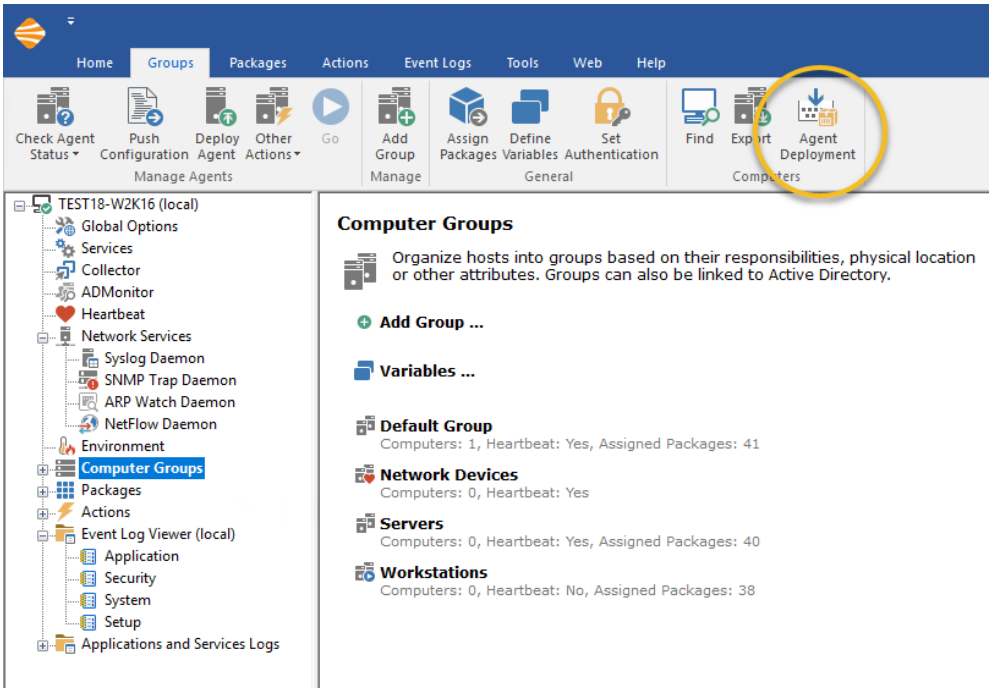
2.7.1 EventSentry-Agent MSI

In den meisten Fällen werden Sie zunächst die EventSentry Agent unter Verwendung der Fernaktualisierungsfunktion der Management-Konsole einsetzen, dies setzt jedoch voraus, dass die entfernten Hosts die SMB-Dateifreigabe aktiviert haben, dass die ADMIN$-Freigabe vorhanden ist und dass der Benutzer, der die Management-Konsole ausführt, Rechte zum Hinzufügen neuer Dateien zur entfernten ADMIN$-Freigabe hat.

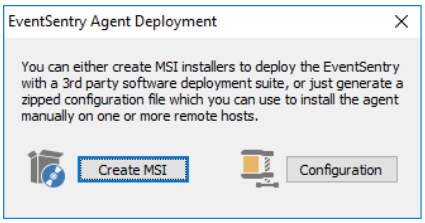
Wenn Ihre Netzwerkinfrastruktur diese Voraussetzungen nicht erfüllt oder wenn Sie es vorziehen, den Agenten über eine MSI-Datei bereitzustellen, können Sie die Anweisungen hier befolgen, um eine MSI-Datei vorzubereiten. Sie können dann jede Software, die in der Lage ist, MSI-Dateien zu installieren, verwenden, um den Agenten auf entfernten Rechnern zu installieren. Wenn die Agenten erfolgreich bereitgestellt wurden, können Sie die Management-Konsole verwenden, um Konfigurationsaktualisierungen nur unter Verwendung der ES$-Freigabe zu pushen, für die weder die ADMIN$-Freigabe noch administrative Berechtigungen erforderlich sind.

Führen Sie die folgenden Schritte aus, um eine 64-Bit-MSI-Datei zu generieren (WIX Toolset (v3) ist erforderlich, um neben 64-Bit-MSI-Installationsprogrammen auch ältere 32-Bit-MSI-Installationsprogramme zu erstellen):

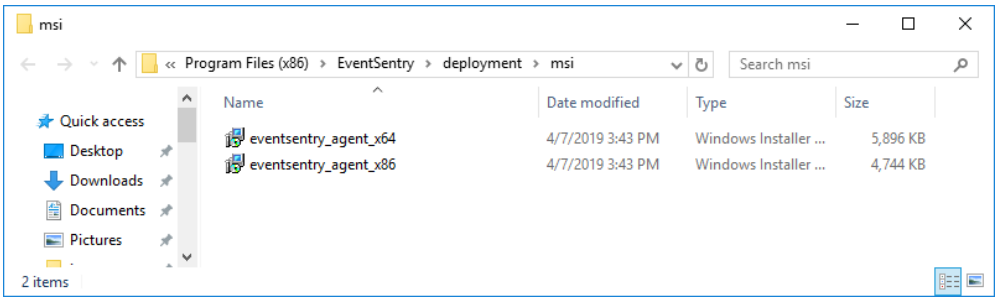
1. Öffnen Sie die Verwaltungskonsole und klicken Sie auf "Computer Groups".
2. Klicken Sie im Ribbon auf "Agent Deployment" auf der rechten Seite



3. Wählen Sie im daraufhin angezeigten Dialogfeld "Create MSI".



4. Wenn das WIX-Toolset nicht installiert ist, erzeugt die Verwaltungskonsole ein 64-Bit-MSI-Installationsprogramm und speichert es im Unterverzeichnis **deployment\msi** des EventSentry Installationsverzeichnisses.



2.8 Web Reports

Die Webberichte sind das Berichtswerkzeug für alle von %PRODUCT% gesammelten Daten und erfordern, dass eine oder mehrere %PRODUCT%-Datenbanken eingerichtet sind.

Die Webberichte können entweder als Teil der Hauptinstallation von %PRODUCT% installiert werden (empfohlen) oder aus dem Kundenbereich heruntergeladen und separat installiert werden. Wenn sie separat installiert werden, können sie entweder auf demselben Rechner installiert werden, auf dem das Haupt-Setup ausgeführt wurde, oder auf einem anderen Rechner. Das Standardinstallationsverzeichnis für die Webberichte ist **C:\Programme\EventSentry\WebReports**.

1a. Installation mit der Haupt EventSentry Installationsprogramm

Um die Web Reports mit dem Installer zu installieren, stellen Sie sicher, dass die Komponente "Web Reports" ausgewählt ist. Siehe Lokale Installation für weitere Einzelheiten zum Installationsprozess.

Sie können nun mit Ihrem Web-Browser zur Index-Seite navigieren, z.B. `http://yourserver:8080/`

2b. Installation mit dem separaten Webreport-Installationsprogramm

Um eine manuelle Installation der Webreports mit dem separaten Webreport-Installationsprogramm (z.B. eventsentry_webreports_v4_2_1_1_0_windows_setup.exe) durchzuführen, laden Sie das Installationsprogramm aus dem Kundenbereich herunter und führen Sie das Installationsprogramm einfach aus.

Das eigenständige Installationsprogramm kann unter Windows, Linux und/oder OS X ausgeführt werden. Die Web-Reports können auf jedem Host installiert werden, der direkten Zugriff auf die Datenbank hat.

Eine Installation neben einer bestehenden EventSentry Installation ist ebenfalls möglich, aber in diesem Fall wird empfohlen, das Hauptinstallationsprogramm auszuführen, das die Web Reports enthält. Wenn das Installationsprogramm für die Web-Reports zu einer vorhandenen EventSentry Installation hinzugefuegt wird, dann kann sie jederzeit deinstalliert werden.

3. Konfigurationsdateien

Alle Einstellungen in den Web Reports werden in XML-Konfigurationsdateien gespeichert.

 configuration.xml

Dies ist die Hauptkonfigurationsdatei für die Web Reports und wird bei der Produktinstallation automatisch konfiguriert. Die Datei enthält alle Profileigenschaften sowie globale Einstellungen für die Fehlerbehebung.

 preferences.xml

Diese Datei enthält sowohl alle globalen als auch benutzerspezifischen Einstellungen.

 reports.xml

Diese Datei enthält eine Liste aller verfügbaren Berichte.

 jobs.xml

Diese Datei enthält eine Liste aller konfigurierten Aufträge.

 users.xml

Steuert die Zugriffskontrolle und, wenn aktiviert, eine Liste aller Benutzer und Gruppen.

3 Verwaltungskonsole / Dienstprogramme

Sie können alle Aspekte von EventSentry über die Verwaltungskonsole konfigurieren. Die Verwaltungskonsole erstellt und verwaltet alle Registrierungsschlüssel, die die Konfiguration für die EventSentry Agenten.

Die Verwaltungskonsole ermöglicht es Ihnen auch, die Konfiguration auf entfernte Hosts zu übertragen und die EventSentry Agenten auf entfernten Computern zu installieren, Ereignisprotokolle anzuzeigen und vieles mehr.

Tastatur-Navigation
Die Managementkonsole kann mit der Tastatur navigiert werden.

- Um von der linken Baumansicht zum rechten Fensterbereich zu wechseln, nachdem ein Element mit ENTER ausgewählt wurde, drücken Sie die TAB-Taste.
- Um vom rechten Dialogfenster zur linken Baumansicht zurückzuschalten, drücken Sie die Tasten ALT+HOME.
- Alternativ können Sie STRG+1 drücken, um zur linken Baumansicht zu springen, und STRG+2, um zum rechten Fenster zu springen.
- Auf den Ribbon kann durch Drücken der ALT-Taste zugegriffen werden, während sich der Fokus in der linken Baumansicht befindet. Während Sie die ALT-Taste gedrückt halten, drücken Sie die gewünschte hervorgehobene Taste.

Anpassen der Verwaltungskonsole
Bitte klicken Sie hier, um Informationen darüber zu erhalten, wie die Verwaltungskonsole an Ihre Bedürfnisse angepasst werden kann.

Symbolleiste
Die Symbolleiste ermöglicht es Ihnen, verschiedene Aktionen schnell per Knopfdruck auszuführen, anstatt mit der rechten Maustaste auf Container klicken oder durch das Menü navigieren zu müssen. Siehe Symbolleiste für weitere Informationen.

Filter und Computer finden
Der "Finden-Dialog" ermöglicht es Ihnen, Filter oder Computer anhand von Suchkriterien zu finden, siehe Suchen für weitere Informationen.

3.1 Anpassung

Sie können viele Aspekte der Verwaltungskonsole anpassen, indem Sie im Menü **Extras** auf **Optionen** klicken. Alle Optionen sind in die folgenden Kategorien unterteilt:

Allgemein
Anpassen des Klickverhaltens und der Tray-Benachrichtigungen (mehr).

Willkommen & MyEventlog
Passen Sie das Aussehen des Begrüßungsbildschirms an, und legen Sie die Anmeldeinformationen für myeventlog.com fest (mehr).

Bestätigungen

Aktivieren/Deaktivieren bestimmter Bestätigungen (mehr).

Fernaktualisierung
Konfigurieren Sie globale Fern-Aktualisierungsoptionen (mehr).

Merkmale
Bestimmte Funktionen in der Verwaltungsanwendung ausblenden (mehr).

Web Reports & Proxy
Konfigurieren Sie die Web Reports, externe Suchlinks und Proxy-Einstellungen (mehr).

3.1.1 Allgemein

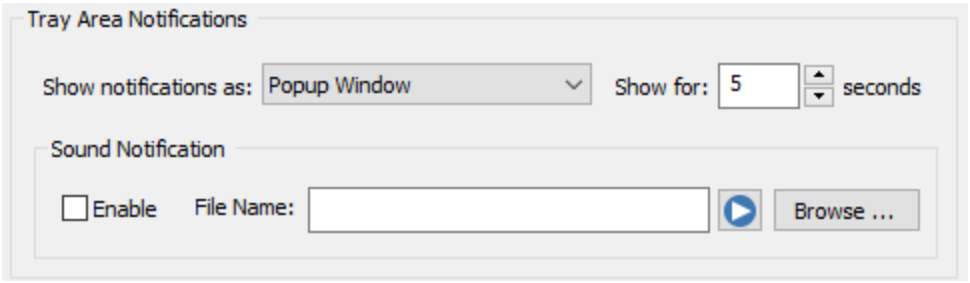
In Ablagefach minimieren
Wenn Sie die Anwendung minimieren, legen Sie sie in den Tray-Bereich, anstatt sie in die Taskleiste zu minimieren.

Doppelklicken Sie auf
Standardmäßig werden durch einen einzigen Linksklick auf die verschiedenen Objekte im linken Baumfenster die Objektdetails (wie z.B. Filtereinstellungen) in das rechte Fenster geladen. Sie können dieses Verhalten ändern, so dass statt eines einfachen Linksklicks ein Doppelklick erforderlich ist.

Nicht ausgewählte Gruppen automatisch zuklappen
Die Aktivierung dieser Funktion stellt sicher, dass die untergeordneten Elemente (Container) nur aus der Gruppe, die erweitert wurde, auf einmal sichtbar sind. Diese Funktion ist besonders nützlich, wenn Sie mehr als 2 Gruppen haben und vermeiden wollen, dass Sie nicht benötigte Gruppen zusammenklappen müssen, wenn Sie eine andere Gruppe erweitern.

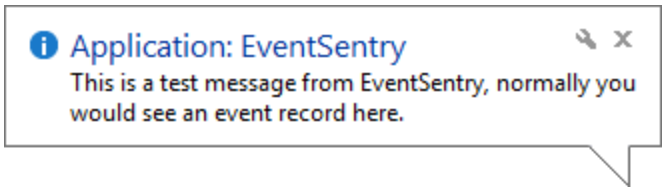
Wenn diese Funktion ausgewählt ist, werden jedes Mal, wenn Sie einen Gruppencontainer (z.B. *Standardgruppe*) expandieren, alle anderen Gruppen, die zu diesem Zeitpunkt expandiert sind, automatisch zugeklappt.

Benachrichtigungen in der Taskleiste
Diese Benachrichtigung ermöglicht es Ihnen, Ereignisprotokoll-Benachrichtigungen fast sofort auf Ihren Desktop zu erhalten. Beachten Sie, dass die GUI aktiv sein muss, damit Taskleistenbenachrichtigungen funktionieren.



Die Benachrichtigungen im Fachbereich können auf folgende Weise konfiguriert werden:

Ballon-Benachrichtigungen
Diese Benachrichtigungsart erfordert Windows 2000 oder höher und zeigt Ereignisprotokolldetails in einer Sprechblase an, wie in der Abbildung unten gezeigt:

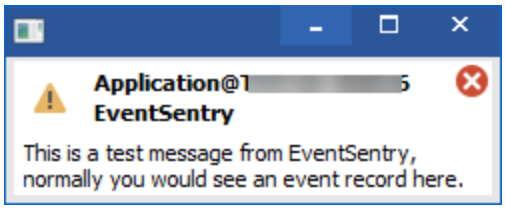


Das Symbol stellt den Schweregrad der Ereignisaufzeichnung dar. Die erste Zeichenfolge ist das Protokoll, in dem das Ereignis aufgetreten ist (in diesem Beispiel das Sicherheitsereignisprotokoll), und die zweite Zeichenfolge zeigt die Quelle des Ereignisprotokolls (in diesem Beispiel ebenfalls **Sicherheit**). Der Rest ist die eigentliche Meldung des Ereignisprotokolls mit maximal 255 Zeichen.

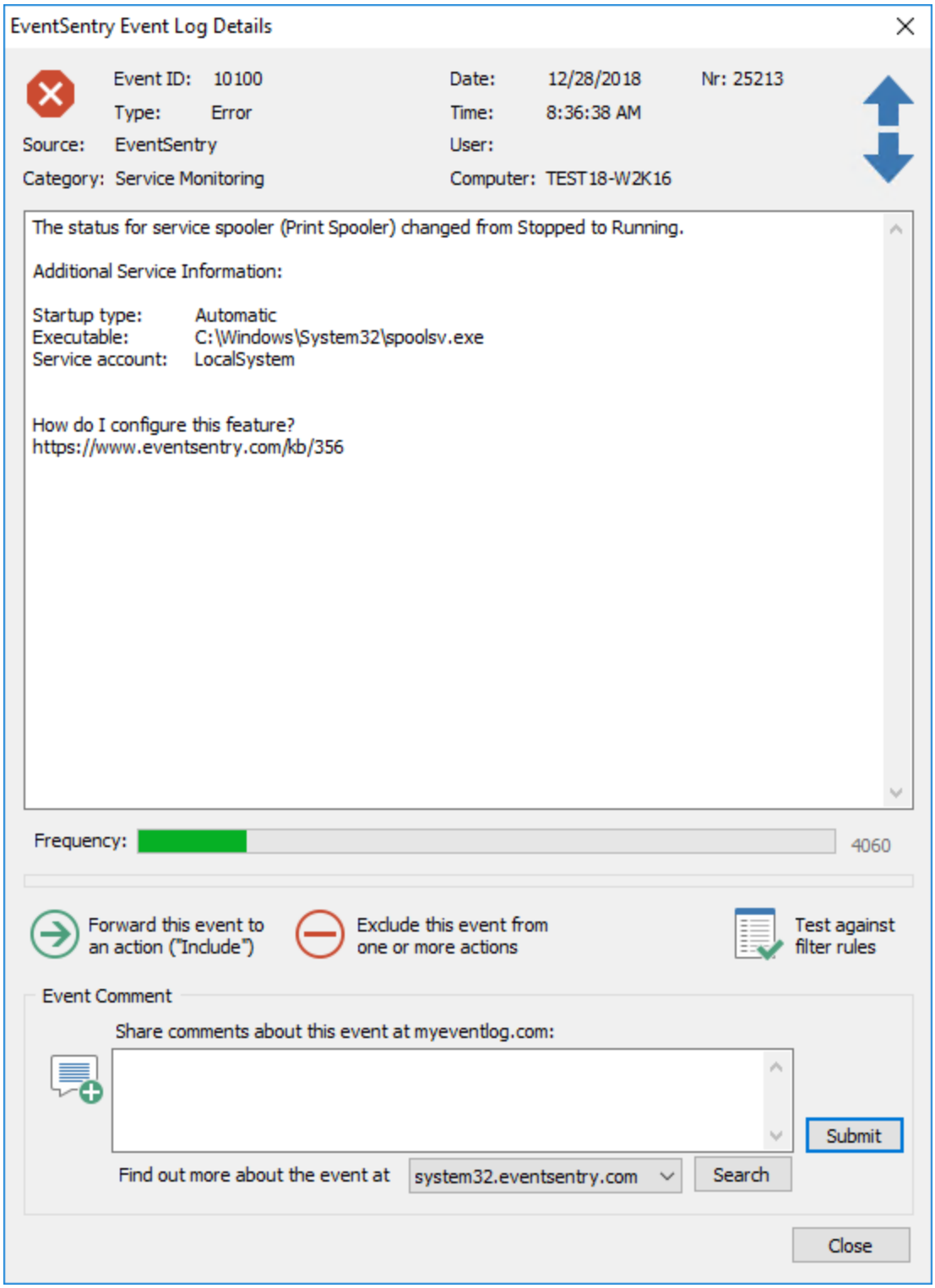
Popup-Fenster
Dieser Benachrichtigungstyp funktioniert mit Windows NT 4 und höher und zeigt Ereignisprotokolldetails in einem Popup-Fenster an, ähnlich wie die Windows Messenger-Anwendung. Dieser Benachrichtigungstyp ist am flexibelsten und nützlichsten, da er die folgenden zusätzlichen Funktionen bietet:

- Konfigurieren Sie, wie viele Sekunden das Fenster aktiv bleiben soll
- Bewegen Sie die Maus über das Fenster, um zu verhindern, dass es verschwindet
- Klicken Sie auf das Popup-Fenster, um die Details der Ereignisaufzeichnung anzuzeigen

Der folgende Screenshot zeigt eine typische Popup-Benachrichtigung:



Wenn Sie irgendwo in das Popup-Fenster klicken, werden die Details des Ereignisprotokolls angezeigt:

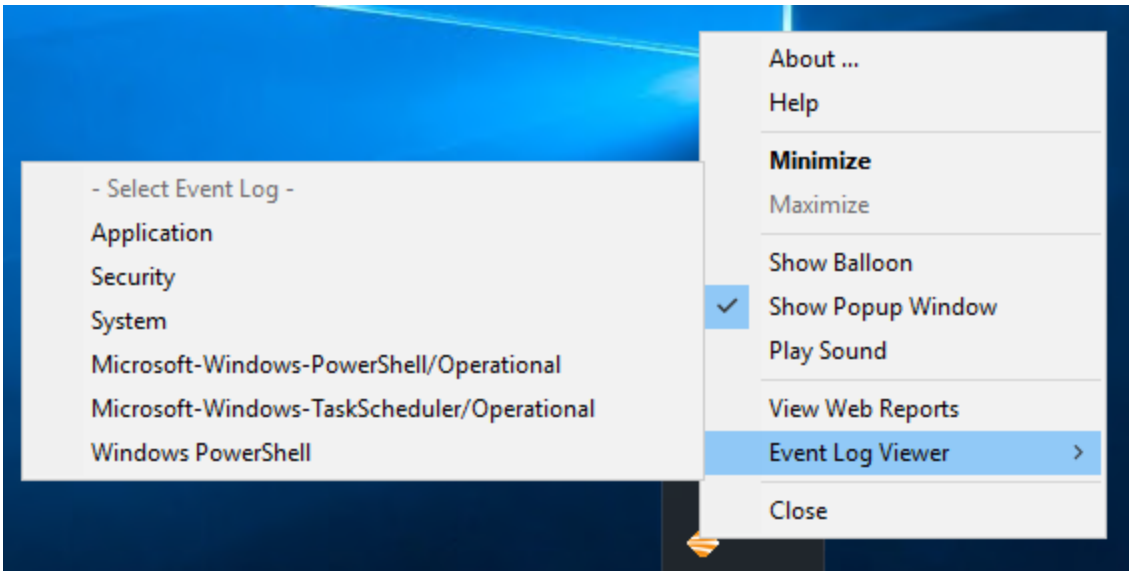


Ton-Benachrichtigung

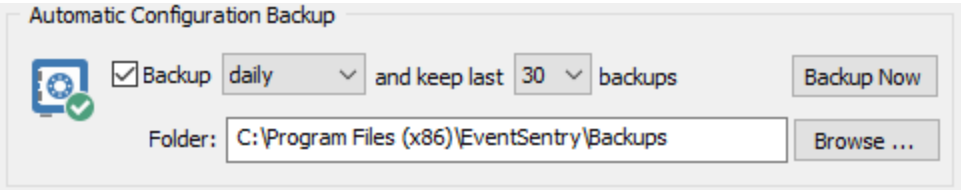
Zusätzlich zu oder anstelle der visuellen Benachrichtigungen können Sie sich auch durch eine Sounddatei im WAVE-Format benachrichtigen lassen. Wenn Sie keine Sounddatei angeben, wird stattdessen ein Standardton verwendet.

Klicken Sie auf **Aktivieren**, um die Tonbenachrichtigung zu aktivieren; klicken Sie auf das Symbol mit dem Lautsprecher, um den gewählten Ton zu hören.

Die Benachrichtigungen des Tray-Bereichs können auch konfiguriert werden, indem Sie mit der rechten Maustaste auf das Tray-Symbol klicken:



Automatische Konfigurationssicherung
Sie können die EventSentry-Konfiguration in regelmäßigen Abständen automatisch sichern, indem Sie diese Funktion aktivieren. Markieren Sie einfach das Kontrollkästchen "Backup-Konfiguration" und legen Sie ein Backup-Intervall fest (täglich, wöchentlich oder monatlich). Von nun an wird EventSentry bei jedem Start der Verwaltungsanwendung bei Bedarf automatisch ein Backup der Konfiguration im Unterverzeichnis "**Backups"** des Installationsverzeichnisses erstellen. Alte Konfigurations-Backups werden ebenfalls automatisch gemäß Ihren Einstellungen gelöscht.



Sie müssen die Verwaltungsanwendung öffnen, damit die Konfiguration gesichert werden kann. Der EventSentry-Agent sichert die Konfiguration nicht automatisch.

3.1.2 Version Check / Welcome

Versionsprüfung

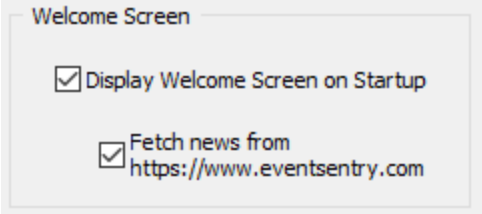
Um bei jedem Öffnen der Verwaltungskonsole automatisch nach einer **neuen Version** zu suchen, klicken Sie auf das Kontrollkästchen "Benachrichtigen Sie mich, wenn eine neue Version von EventSentry verfügbar ist". Dadurch wird automatisch die Funktion "Nach Updates suchen" aufgerufen und das Dialogfeld mit den Versionsinformationen angezeigt, wenn eine neue Version verfügbar ist.

Um automatisch nach **neuen Patches** zu suchen, aktivieren Sie das Kontrollkästchen "Benachrichtigen Sie mich, wenn ein neuer Patch verfügbar ist". Wenn Sie es vorziehen, nur benachrichtigt zu werden, wenn ein kritischer Patch veröffentlicht wurde, aktivieren Sie auch das Kontrollkästchen "Nur bei kritischen Patches benachrichtigen".

Aktivieren Sie die Online-Prüfung des Wartungsablaufs und den integrierten Patch-Download
Ermöglicht das automatische Herunterladen und Installieren von Patches von der Verwaltungskonsole aus.

Begrüßungsbildschirm

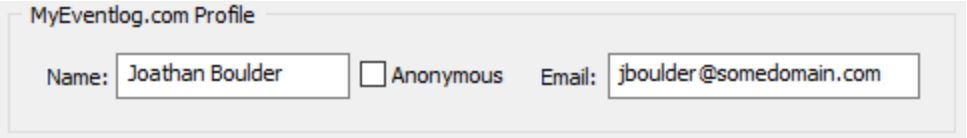
In diesem Abschnitt können Sie einige Aspekte des Begrüßungsbildschirms anpassen.



Begrüßungsbildschirm beim Start anzeigen
Durch Deaktivieren dieses Kontrollkästchens wird der Begrüßungsbildschirm beim Start der Verwaltungsschnittstelle nicht angezeigt. Der Begrüßungsbildschirm wird auch dann noch angezeigt, wenn Sie manuell auf das Symbol des Hauptrechners klicken.

Holen Sie sich Neuigkeiten von http://www.eventsentry.com
Wenn Sie dieses Kontrollkästchen deaktivieren, werden die aktuellen Nachrichten nicht aus dem Internet heruntergeladen. Deaktivieren Sie dieses Kontrollkästchen, wenn Ihr Computer nicht mit dem Internet verbunden ist, um eine Verzögerung beim Start der Anwendung zu vermeiden.

Wenn Ihr Rechner mit dem Internet verbunden ist, wird empfohlen, dieses Kontrollkästchen zu aktivieren, da Sie wichtige Informationen über neue Entwicklungen rund um EventSentry erhalten.



Ereignisprotokoll-Viewer

In diesem Abschnitt können Sie die Funktionen des Ereignisprotokoll-Viewers anpassen.

Sich an fernverbundene Ereignisprotokolle erinnern
Wenn Sie über die integrierte Ereignisprotokollanzeige eine Verbindung zu einem entfernten Ereignisprotokoll herstellen, **werden** diese verbundenen Ereignisprotokolle beim Neustart der EventSentry-Verwaltungskonsole standardmäßig **nicht** wieder geöffnet. Wenn Sie diese Option jedoch aktivieren, werden die entfernten Ereignisprotokolle gespeichert und automatisch wieder geöffnet.

EventSentry zum Standardhandler für Ereignisprotokoll-Sicherungsdateien machen
Zusätzlich zum Öffnen von entfernten Ereignisprotokollen können Sie auch Ereignisprotokolldateien öffnen, die zuvor gesichert wurden (z.B. durch die EventSentry-Ereignisprotokoll-Sicherungsfunktion oder durch die Windows-Ereignisanzeige). Wenn Sie diese Option aktivieren, registriert sich EventSentry selbst als Standardanwendung für .evt-Dateien, so dass Sie auf .evt-Dateien im Explorer doppelklicken und sie sofort in EventSentry anzeigen können.

Sie müssen sich abmelden und wieder anmelden, um auf die Ereignisprotokolldateien im Explorer doppelklicken zu können.

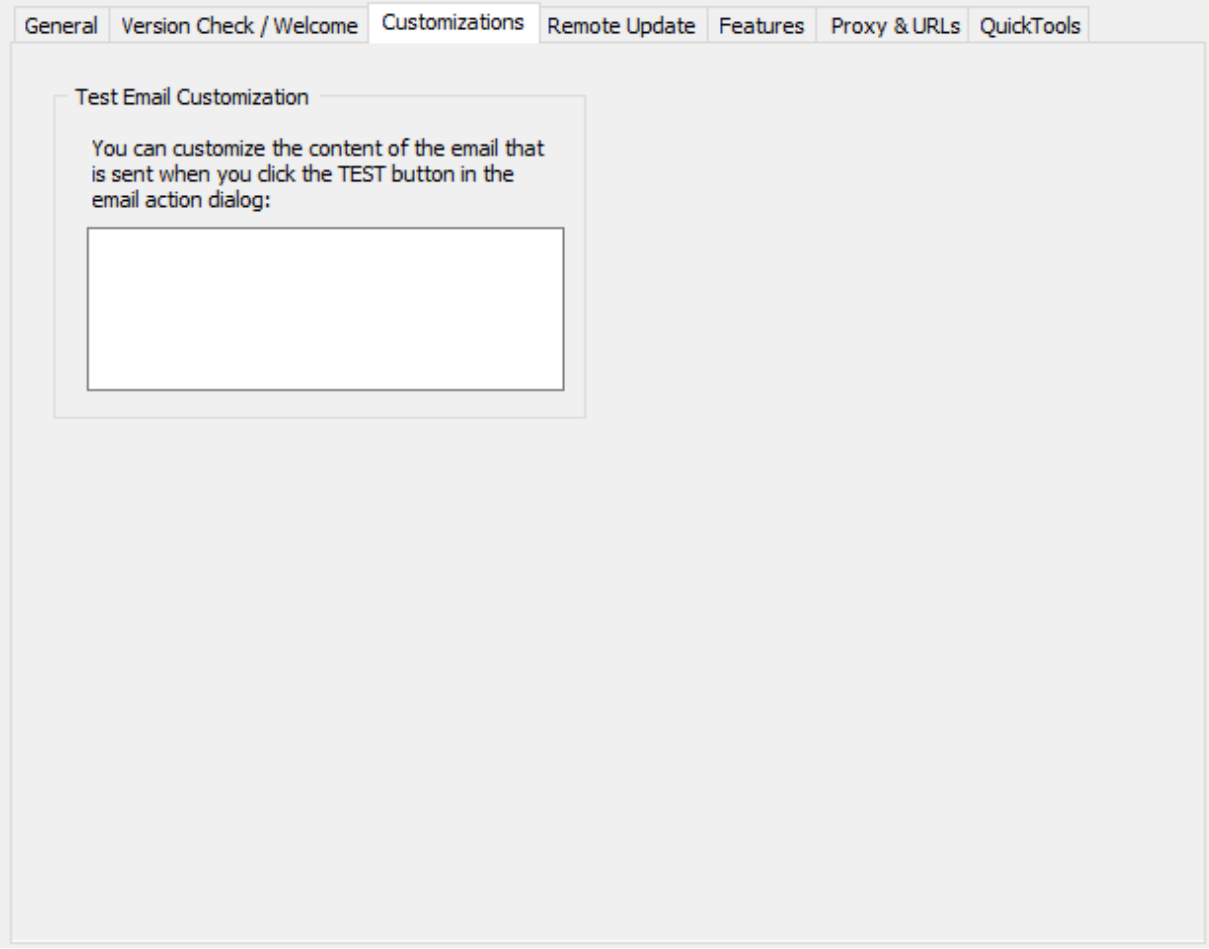
myeventlog.com
Sie können Kommentare zum Ereignisprotokoll direkt aus der Verwaltungsanwendung heraus an die Website myeventlog.com senden. Um das Einreichen von Kommentaren zu beschleunigen, können Sie hier Ihr Standardprofil einrichten.

Name (Autor)
Ihren vollständigen Namen. Wenn Sie das Kästchen "Anonym" ankreuzen, wird Ihr Name bei den von Ihnen eingereichten Kommentaren nicht angezeigt.

Ihre E-Mail-Adresse
Ihre E-Mail-Adresse wird zur eindeutigen Identifizierung Ihrer Einreichung verwendet. Bitte beachten Sie, dass Ihre E-Mail-Adresse **niemals** mit Ihren Beiträgen angezeigt wird.

3.1.3 Anpassungen

Um versehentliche Löschungen zu vermeiden, fordert EventSentry Sie vor Aktionen auf, z.B. bevor ein Filter oder eine Gruppe gelöscht wird. Der Screenshot unten zeigt die verfügbaren Bestätigungsoptionen:



Anpassung der Test-E-Mail

Wenn Sie im SMTP-Aktionsdialog auf die Schaltfläche **Test** klicken, sendet EventSentry eine Test-E-Mail an die konfigurierte(n) E-Mail-Adresse(n) in englischer Sprache. Der Inhalt dieser Test-E-Mail kann angepasst werden. Das Anpassen des Standardtextes kann hilfreich sein, um Verwirrung zu vermeiden oder eine Übersetzung in eine lokale Sprache bereitzustellen.

3.1.4 Remote Update

Threads

Geben Sie die Anzahl der Threads an, die von der Fernaktualisierungsfunktion verwendet werden sollen. Je mehr Threads Sie verwenden, desto schneller wird eine Fernaktualisierungsaktion ausgeführt.

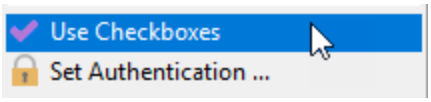
Für die meisten Netzwerke wird eine Anzahl von 5 Threads empfohlen, obwohl bei großen EventSentry-Installationen eine höhere Anzahl verwendet werden kann, um die für die Durchführung einer Aktion wie z.B. einer Konfigurationsaktualisierung erforderliche Zeit zu reduzieren.

CSV-Protokoll der Fernaktualisierungsergebnisse aufbewahren

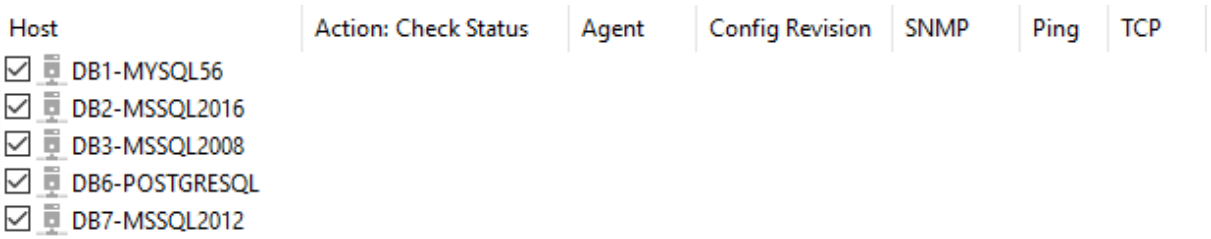
Protokolliert alle Remote-Update-Aktivitäten in einer CSV-Protokolldatei, jede Aktion erstellt eine separate Datei. Die Dateien werden im Unterverzeichnis "logs" des EventSentry-Installationsordners gespeichert, z.B. C:\Programme (x86)\EventSentry\logs. Um auf die Protokolldateien zuzugreifen, navigieren Sie entweder zu dem Ordner in Windows, oder klicken Sie mit der rechten Maustaste auf das Dialogfeld für die Fernaktualisierung und wählen Sie "Aktuelles Protokoll anzeigen" oder "Alle Protokolle durchsuchen". Ersteres ist nur verfügbar, nachdem eine Remote-Update-Aktion abgeschlossen ist.

Kontrollkästchen verwenden

Um selektiv nur ausgewählte Computer einer Gruppe zu aktualisieren, können Sie diese Option aktivieren. Anstatt die ausgewählte Aktion auf alle Computer der Gruppe(n) anzuwenden, wird dadurch neben jedem Computerobjekt ein Kontrollkästchen gesetzt, das Sie aktivieren/deaktivieren können. Sie können die Kontrollkästchen auch aktivieren/deaktivieren, indem Sie im Remote-Update mit der rechten Maustaste auf eine Gruppe klicken:

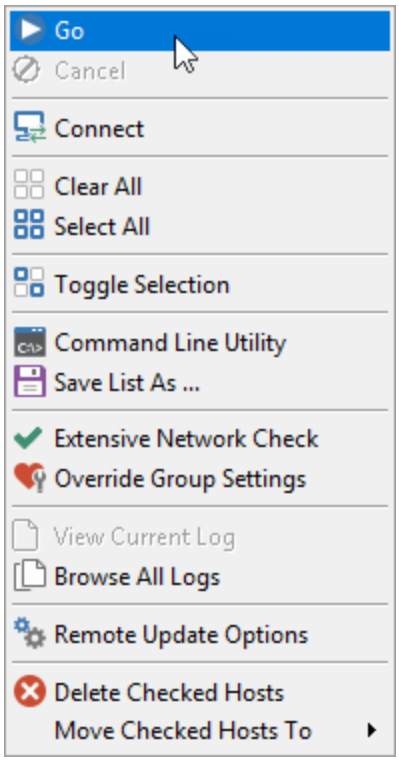


Nachdem Sie eine der Fern-Update-Optionen ausgewählt haben, sehen Sie eine Liste ähnlich der unten gezeigten:



Wenn Sie mit der Auswahl der richtigen Computerobjekte fertig sind, können Sie mit der rechten Maustaste irgendwo im rechten Fensterbereich klicken und im Menü **Go** wählen. Nur die ausgewählten Computerobjekte werden aktualisiert.

Die Aktivierung dieser Option ist erforderlich, um mehrere Computer auf einmal aus dem Fernupdate-Dialog zu verschieben oder zu löschen.



Sie können auch alle Computer löschen/überprüfen, indem Sie mit der rechten Maustaste klicken und entweder **Alle löschen** oder **Alle auswählen** aus dem Menü wählen.

Die Auswahl des Kontrollkästchens bleibt erhalten, wenn Sie Aktionen/Aktualisierungen auf derselben Gruppe durchführen.

Wenn Sie beispielsweise den EventSentry-Dienst auf ausgewählten Computern installieren und starten möchten, können Sie dies tun. Ihre Auswahl bleibt erhalten, solange Sie mit der rechten Maustaste auf dieselbe Gruppe im linken Fensterbereich klicken.

Beim Hinzufügen einzelner Computer zur Eingabe der IP-Adresse auffordern

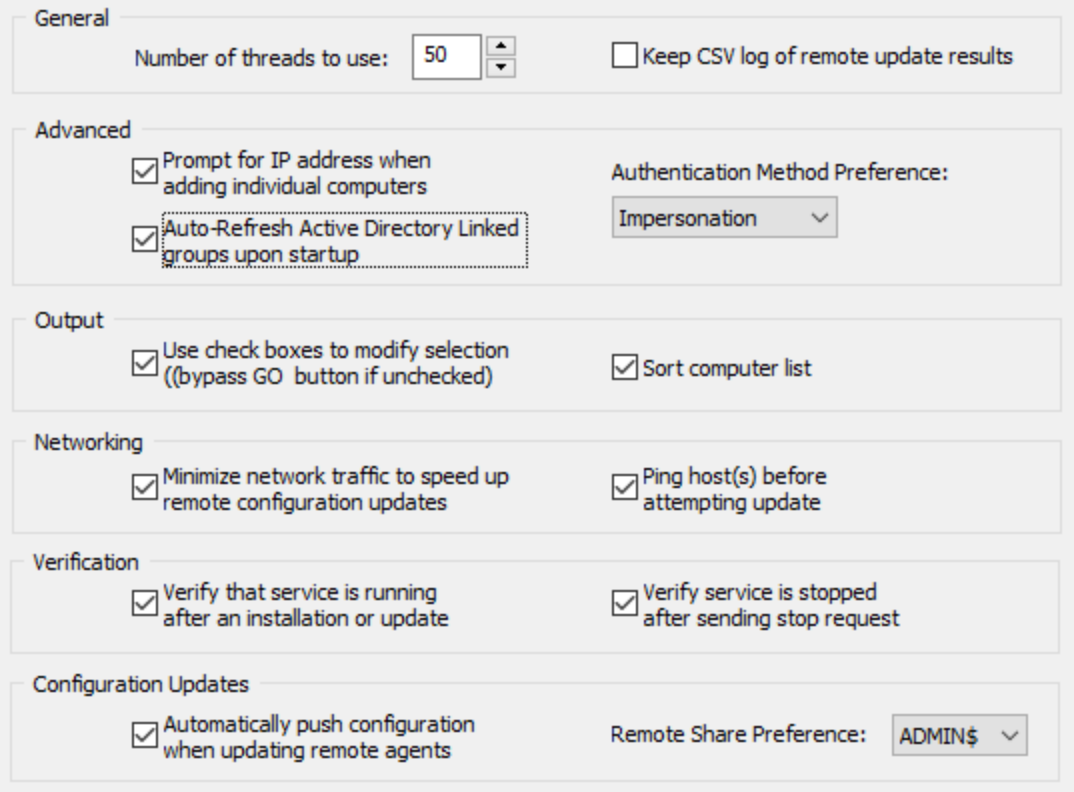
Sie können leicht zu merkende Aliase für die IP-Adresse in der Verwaltungsanwendung erstellen, wenn Sie Computer hinzufügen. Standardmäßig können Sie dem Container der Computer in einer Gruppe nur Hostnamen hinzufügen, aber bei der Aktivierung dieser Funktion können Sie optional auch eine IP-Adresse eingeben.

Auto-Aktualisierung von Active Directory Aktivierte Gruppen beim Start

Wenn diese Option aktiviert ist und Sie Gruppen haben, die mit Active Directory verknüpft sind, dann aktualisiert die Verwaltungskonsole bei jedem Öffnen der Verwaltungskonsole jede AD-fähige Gruppe mit AD. Wenn diese Option nicht angekreuzt ist, müssen Sie eine Remote-Update-Aktion (z.B. Agentenstatus prüfen) durchführen, um die Liste der Computer zu aktualisieren.

Authentifizierungsmethode Präferenz

Wenn alternative Anmeldeinformationen für Gruppen oder Computer verwendet werden, kann sich die Verwaltungskonsole entweder mittels Impersonation oder durch Verbindung mit der entfernten IPC$-Freigabe authentifizieren. Impersonation ist vorzuziehen, wird aber nicht immer unterstützt. Passen Sie diese Option an, wenn Sie Probleme bei der Authentifizierung mit Ferncomputern haben.



Computerliste sortieren

Wenn Sie dieses Kästchen ankreuzen, wird die Liste der Computer im Fernaktualisierungsfenster automatisch sortiert.

Netzwerkverkehr minimieren

Wenn Sie Hosts verwalten, die über mehrere Standorte über langsame Netzwerkverbindungen verteilt sind, empfiehlt es sich, diese Option zu aktivieren. Standardmäßig versucht EventSentry zu ermitteln, welche Art von Host auf dem Remote-Computer ausgeführt wird, und ruft auch den aktuellen Dienststatus vom Remote-Host ab, wenn die Konfiguration auf Remote-Hosts aktualisiert wird. Beide Funktionen erfordern zusätzlichen Netzwerkverkehr und führen zu einer langsameren Aktualisierung. Wenn Sie diese Option aktivieren, wird die Zeit, die benötigt wird, um die Konfiguration auf einen Remote-Host zu übertragen, erheblich verkürzt.

Diese Option wirkt sich nur auf die Aufgabe **Update-Konfiguration** aus, alle anderen entfernten Update-Optionen sind von dieser Einstellung nicht betroffen. Sie können den Remote-Service-Status, einschließlich der Version, jederzeit überprüfen, indem Sie die Aktion **Agentenstatus prüfen** ausführen.

Host(s) anpingen, bevor ein Update versucht wird

Durch Aktivieren dieser Option wird ein Ping an einen entfernten Host gesendet, bevor eine Fern-Aktualisierungsaktion versucht wird. Wenn diese Option aktiviert ist und ein Remote-Host nicht

erreichbar ist, versucht EventSentry nicht, ein Remote-Update durchzuführen und überspringt diesen Computer.

Überprüfen Sie, ob der Dienst nach einer Installation oder Aktualisierung läuft
Beim Installieren oder Aktualisieren eines Remote-Agenten startet das Remote-Update den Dienst auf dem Remote-Computer. Markieren Sie dieses Kästchen, um Remote Update anzuweisen, auf den erfolgreichen Start des Dienstes zu warten. Deaktivieren Sie das Kästchen, um die Installation / Aktualisierung von Remote-Agenten zu beschleunigen.

Überprüfen Sie, ob der Dienst nach dem Senden einer Stoppanforderung angehalten wurde
Wenn der EventSentry-Dienst auf Ferncomputern angehalten wird, kann Remote Update überprüfen, ob der Dienst tatsächlich erfolgreich angehalten wurde. Deaktivieren Sie dieses Kästchen, damit Remote Update einfach die Stoppanforderung sendet, ohne zu überprüfen, ob der Dienst erfolgreich gestoppt wurde.

Automatische Push-Konfiguration bei der Aktualisierung von Remote-Agenten
Wenn Sie diese Option wählen, wird die aktuelle Konfiguration auch auf den/die entfernten Host(s) ausgelagert, wenn ein Update des entfernten Agenten durchgeführt wird (Agent(s) verwalten -> Update).

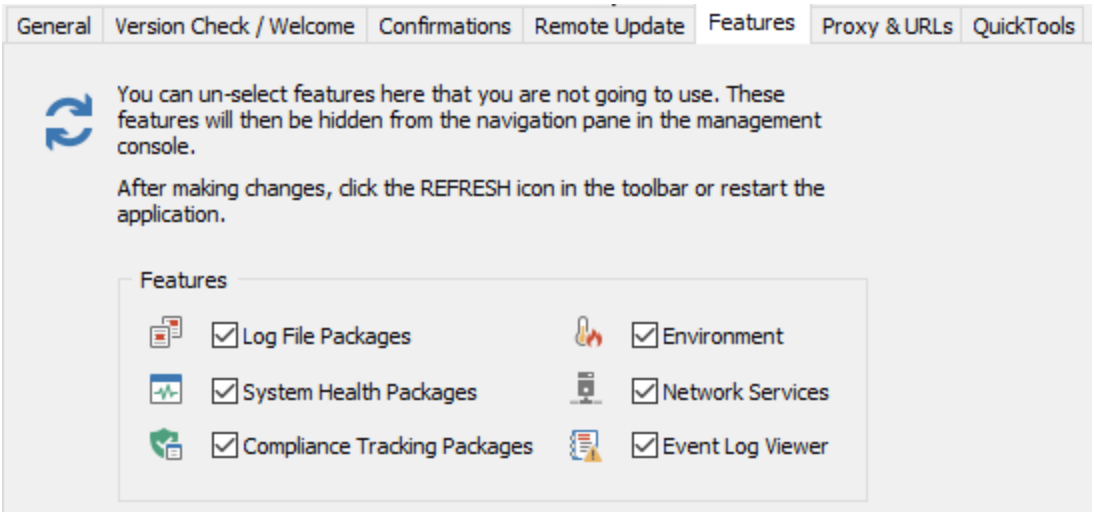
Präferenz für Remote Share
Standardmäßig sendet EventSentry Konfigurationsaktualisierungen über die ADMIN$-Freigabe an Remote-Agenten. Sie können jedoch auch die ES$-Freigabe einrichten, wenn die ADMIN$-Freigabe nicht verfügbar ist oder nicht verwendet werden kann. Wenn Sie also die ES$-Freigabe verwenden, empfiehlt es sich, diese Option auf **ES$** zu setzen, um Konfigurationsaktualisierungen zu beschleunigen.

3.1.5 Merkmale

Sie können bestimmte Feature-Container im Strukturfenster ausblenden, wenn Sie nicht alle Features von EventSentry verwenden. Dies kann die Navigation in der Verwaltungskonsole erleichtern, da weniger Container im Strukturfenster vorhanden sind.

Deaktivieren Sie einfach die Kontrollkästchen der Funktionen, die Sie ausblenden möchten, und sie werden nicht im Strukturfenster angezeigt, wenn Sie die Verwaltungskonsole neu starten.

Sie können auch die F5-Taste im Strukturfenster drücken oder mit der rechten Maustaste auf den Computercontainer klicken und Aktualisieren wählen, um die Struktur sofort **zu aktualisieren** und die ausgewählten Funktionen ein- oder auszublenden.

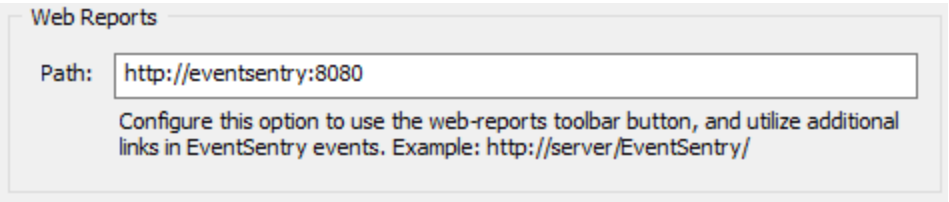


3.1.6 Web Reports & Proxy

Pfad zu Web Reports

Wenn Sie die Web Reports eingerichtet haben, empfiehlt es sich, den Pfad hier anzugeben. Nach der Konfiguration können Sie die Webschnittstelle in Ihrem Standard-Webbrowser anzeigen, indem Sie im ***Web -> Web Reports anzeigen*** wählen. Die Einstellung dieser Option ist auch für die Anzeige eines datenbankbasierten Heartbeat-Status innerhalb der EventSentry-GUI erforderlich.

Diese Einstellung ist auch notwendig, wenn die Heartbeat-Funktion in Verbindung mit einer Datenbank verwendet wird, so dass in der Verwaltungsanwendung automatisch die richtigen Webseiten angezeigt werden.



Benutzerdefinierte Such-URL

Mit der integrierten Ereignisanzeige können Sie die folgenden Websites nach Details zu einem Ereignisprotokolleintrag abfragen:

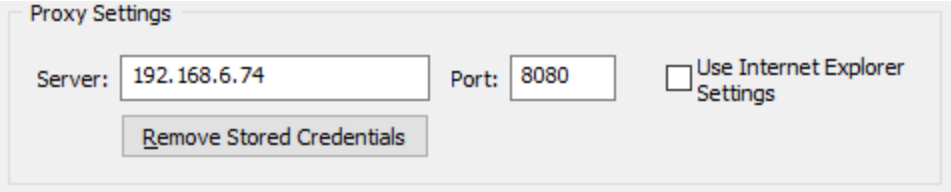
1. myeventlog.com (http://www.myeventlog.com/)
2. Google (http://www.google.com/)
3. Microsoft Knowledge Base (http://support.microsoft.com/)
4. Microsoft.com (http://www.microsoft.com/)
5. Eine benutzerdefinierte Suchseite

Die Optionen 1 - 4 können nicht geändert werden, Sie können jedoch Ihre eigene Suchseite in das Feld **Benutzerdefinierte Such-URL** eingeben. Sie können die Variablen **$EVENTID** und **$EVENTSOURCE** in der URL verwenden.

Proxy-Einstellungen

Die Nachrichten- und Feedback-Funktionen der Verwaltungskonsole arbeiten alle über das HTTP-Protokoll. Wenn Ihr Netzwerk einen Proxy-Server erfordert, können Sie hier den Proxy-Server und den Port angeben.

Wenn Sie Internet Explorer verwenden, können Sie einfach das Kontrollkästchen "Internet Explorer-Einstellungen verwenden" aktivieren, um EventSentry anzuweisen, automatisch die in Internet Explorer konfigurierten Proxy-Einstellungen zu verwenden.



3.1.7 QuickTools

Mit den QuickTools können Sie Befehlsdienstprogramme von der Verwaltungskonsole aus ausführen. Sie sind in die Computergruppen integriert und ermöglichen es Ihnen, jede beliebige Anwendung auf einem entfernten Computer mit nur einem Mausklick auszuführen. Sie können bis zu acht QuickTools konfigurieren, und jedes Tool kann dieselben Anmeldedaten verwenden, die für die Fern-Aktualisierung eingerichtet sind (falls sie für einen Computer oder eine Gruppe konfiguriert wurden). Die folgenden Optionen sind für jeden Eintrag verfügbar:

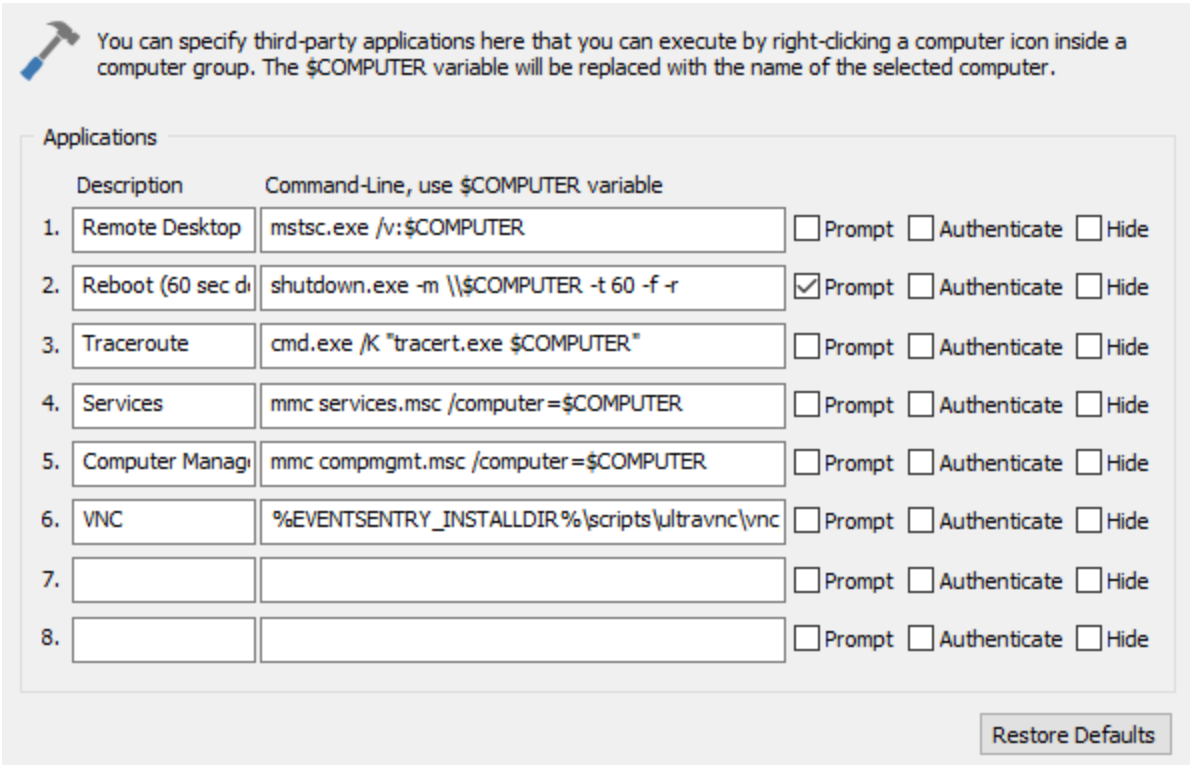
Name
Geben Sie einen beschreibenden Namen für das Werkzeug an. Dieser Name wird angezeigt, wenn Sie mit der rechten Maustaste auf ein Computerelement klicken.

Befehlszeile
Geben Sie die Befehlszeile für das Werkzeug an. Verwenden Sie die Variable **$COMPUTER**, die automatisch durch den Namen des ausgewählten Computers ersetzt wird.

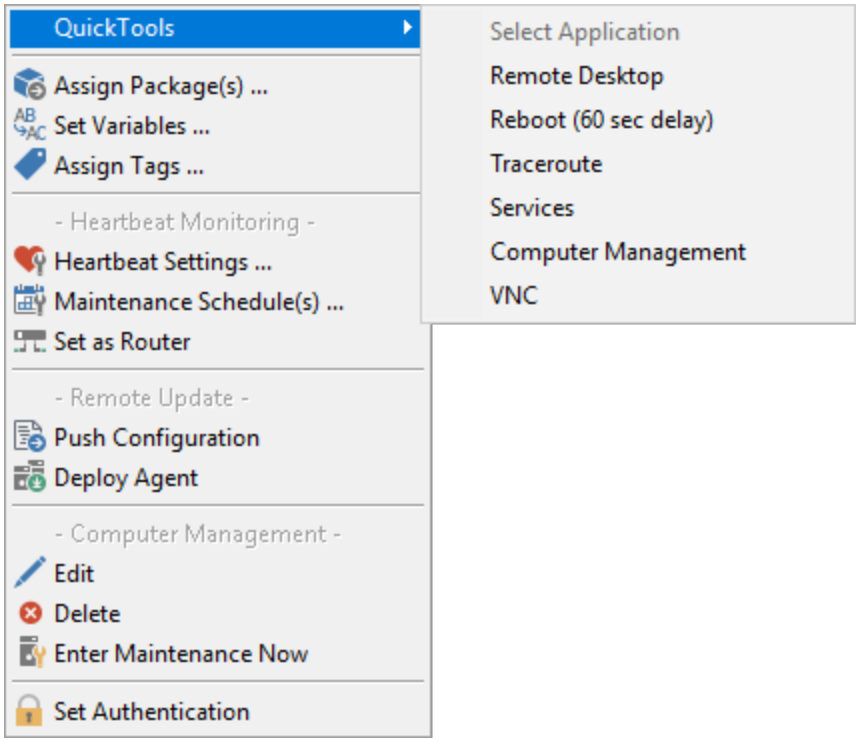
Prompt
Bei Tools die z.B. einem Neustart erzwingen, kann EventSentry einen Bestaetigungsdialog zeigen, bevor es das Tool ausführt.

Beglaubigen
Aktivieren Sie dieses Kontrollkästchen, wenn EventSentry sich *vor der* Ausführung des Tools authentifizieren soll. Die Anmeldeinformationen werden von der Gruppe oder dem Computer, falls konfiguriert, übernommen.

Ausblenden
Wenn Sie dieses Kästchen ankreuzen, werden alle Fenster ausgeblendet, die durch den direkt von der Managementkonsole ausgeführten Befehl geöffnet werden; das Erscheinen nachfolgender Fenster wird dadurch nicht verhindert. Dies kann z.B. nützlich sein, um ein Befehlszeilenfenster zu verbergen.

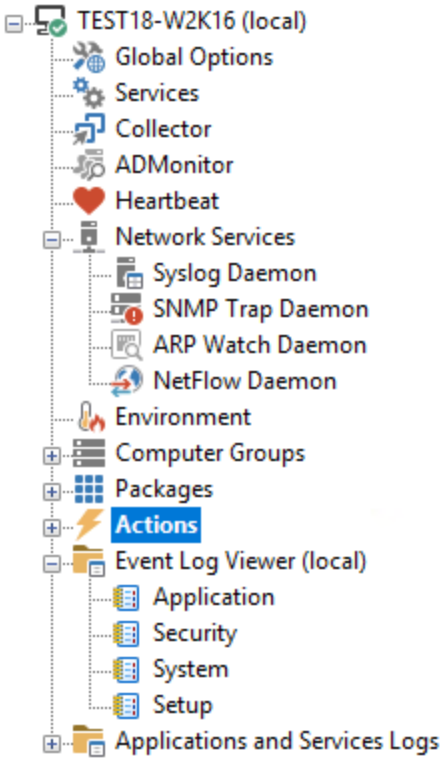


Um auf die QuickTools zuzugreifen, klicken Sie einfach mit der rechten Maustaste auf einen beliebigen Computer in einer Computergruppe und wählen Sie das Untermenü QuickTools:

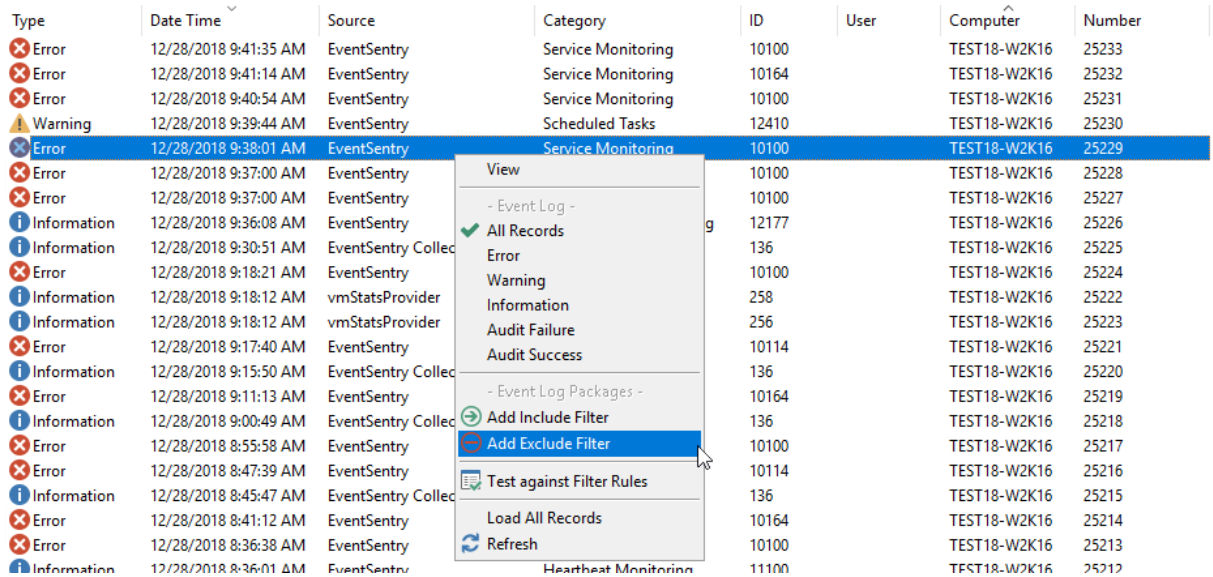


3.2 Event Log Viewer

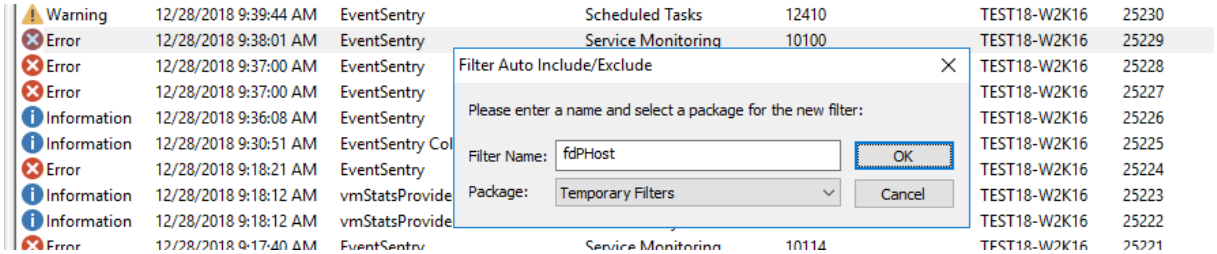
Die EventSentry-Benutzeroberfläche enthält eine sich selbst einstellende, integrierte Ereignisprotokollanzeige, mit der Sie grundlegende Ereignisprotokollfunktionen von EventSentry aus ausführen können. In den meisten Fällen müssen Sie keine weitere Ereignisprotokoll-Viewer-Anwendung öffnen. Sie können auch bis zu 15 Remote-Ereignisprotokolle, siehe Remote-Ereignisprotokolle ansehen für weitere Einzelheiten.



Automatisches Einschließen oder Ausschließen von Ereignissen durch einfaches Klicken der rechten Maustaste

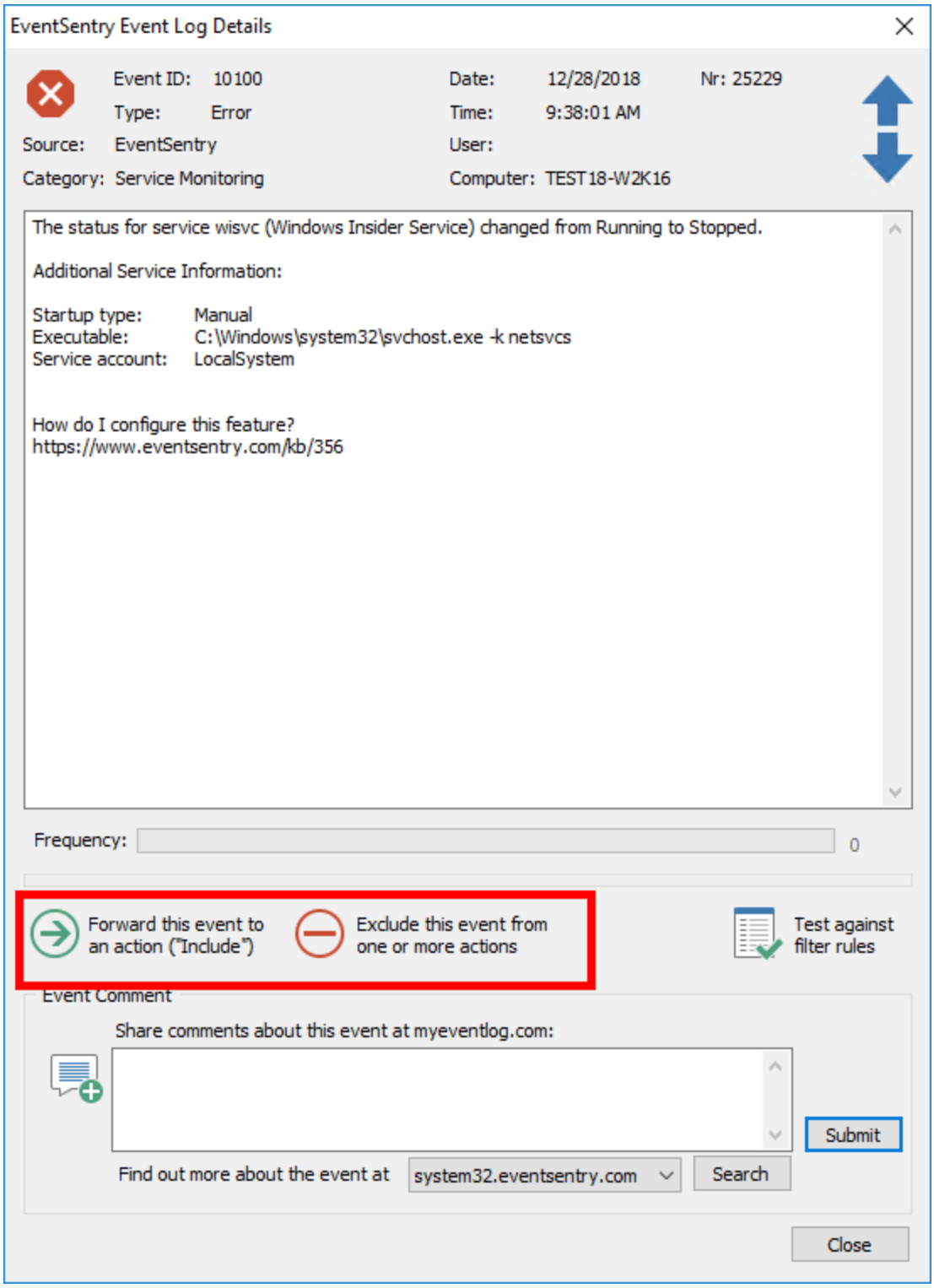


Anstatt Ein- oder Ausschlussfilter manuell einzurichten, können Sie sie einfach im **lokalen oder einem entfernten Ereignisprotokoll** lokalisieren, mit der rechten Maustaste anklicken und entweder "Einschlussfilter hinzufügen" oder "Ausschlussfilter hinzufügen" wählen. Daraufhin wird der folgende Dialog angezeigt



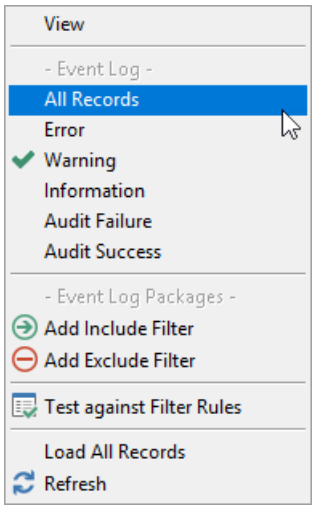
wo Sie einen Namen für den neuen Ereignisprotokollfilter angeben und ein Paket auswählen können, in dem der Filter erstellt werden soll.

Alternativ können Sie auch auf die Ein- und Ausschlussschaltflächen im Ereignisprotokoll-Detaildialog klicken:

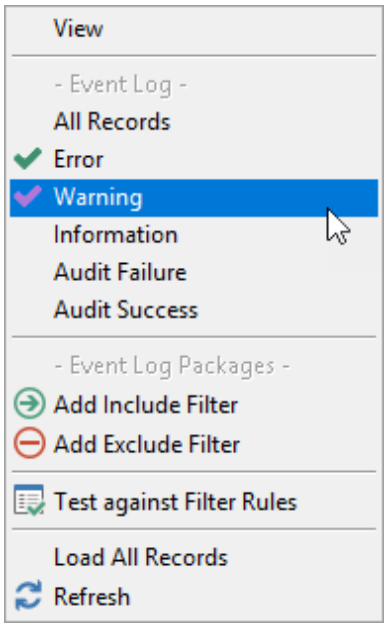


Ereignisse leicht filtern

Sie können Ereignisse auf einfache Weise anhand der Ereignisschwere herausfiltern. Klicken Sie einfach irgendwo mit der rechten Maustaste und wählen Sie den gewünschten Schweregrad aus:



Um zum Beispiel nur Warnungen zu sehen, wählen Sie "**Warnung**".



Um sowohl Fehler als auch Warnungen zu sehen, wählen Sie einfach "**Fehler**" zusätzlich zu Warnung.

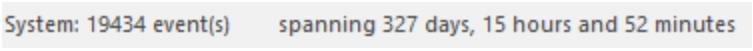
Um den Filter wieder zu deaktivieren, wählen Sie "**Alle Datensätze**". Diese Funktion ist zwar nicht so flexibel wie der Filtermechanismus des Ereignisbetrachters, der mit dem Betriebssystem ausgeliefert wird, aber sie macht die grundlegende Filterung viel einfacher zu verwenden. Wir werden in Zukunft weitere Filteroptionen hinzufügen.

Mehrere Ereignisprotokolle gleichzeitig anzeigen

Sie können die Ereignisprotokolle von (bis zu 15) entfernte Maschinen (weitere Informationen)

Zeitspanne anzeigen

Sie können sofort sehen, wie viele Ereignisprotokolleinträge vorhanden sind und wie lange sich ein Ereignisprotokoll erstreckt



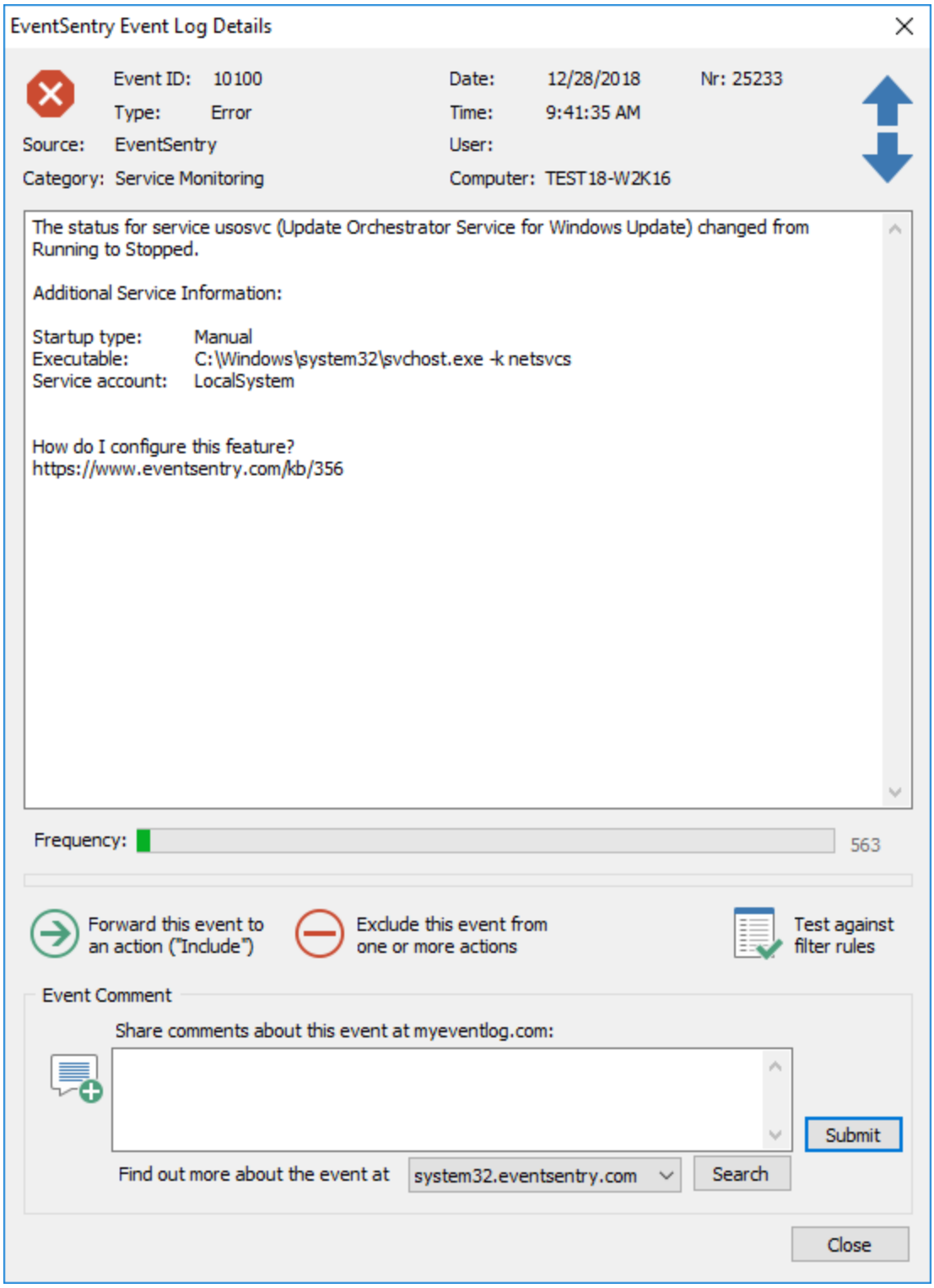
Event log summary information in the status bar

Automatisches Ausblenden von Spalten

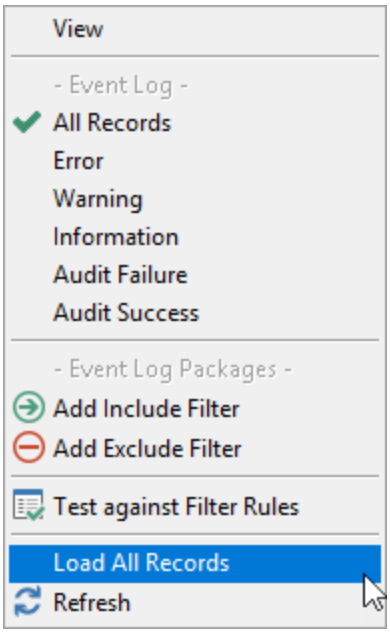
Wenn die Spalte **Kategorie** oder **Benutzer** leer ist, wird sie automatisch ausgeblendet.

Häufigkeit

Zeigen Sie die **Häufigkeit** eines Ereignisprotokolldatensatzes an (wie oft ein ähnlicher Ereignisdatensatz im Ereignisprotokoll erscheint). Diese Statistik wird zunächst für die ersten **3000** (oder weniger, wenn weniger Datensätze vorhanden sind) Ereignisaufzeichnungen berechnet und dann dynamisch berechnet, während Sie durch das Ereignisprotokoll blättern.



Wenn Sie genaue Statistiken sehen möchten, können Sie mit der rechten Maustaste auf einen beliebigen Ereignisprotokolleintrag klicken und im Menü **Alle Einträge laden** wählen.

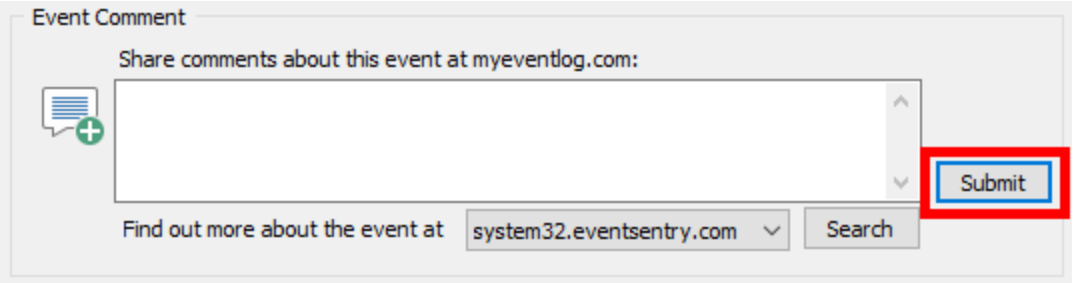


Die oben gezeigte Ereignisaufzeichnung trat im aktuellen Ereignisprotokoll **1806** Mal auf. Die Häufigkeit wird unter Berücksichtigung der **Ereignis-ID** und der **Ereignisquelle** berechnet.

*Manchmal können Ereignisdatensätze trotz einer eindeu tige **Ereignis-ID** eindeutige Einfügetexte enthalten. In diesem Fall ist die Häufigkeit nicht 100% genau.*

Automatische Übermittlung von Kommentaren

Sie können schnell und einfach Kommentare zu einem Ereignisprotokoll-Eintrag auf der Website **myeventlog.**com einreichen. Geben Sie einfach einen Kommentar in das Feld "Erweitert" ein und klicken Sie auf die Schaltfläche "Einreichen":



Weitere Informationen zu Ereignis-IDs finden Sie auf den Websites

Sie können die folgenden Websites über den Dialog EventSentry Event Log Details abfragen, um zusätzliche Informationen zu einem Ereignisprotokolleintrag zu erhalten:

1. MyEventlog.com (http://www.myeventlog.com/)
2. Google (http://www.google.com/)
3. Microsoft Knowledge Base (http://support.microsoft.com/)
4. Microsoft.com (http://www.microsoft.com/)
5. A custom search page

Spaltensortierung

Die Ausgabe kann durch Klicken auf die jeweilige Spaltenüberschrift sortiert werden.

3.2.1 Anzeigen von entfernten Ereignisprotokollen

Bis zu 15 Remote-Ereignisprotokolle können von der Verwaltungsanwendung aus eingesehen werden. Sie können den Remote-Computer auf drei Arten auswählen:

1. Manuelles Angeben eines Remote-Computers
Klicken Sie mit der rechten Maustaste auf das Objekt "Ereignisprotokollanzeige (lokal)" und wählen Sie "**Verbinden ...** ". Sie werden aufgefordert, einen entfernten Computernamen einzugeben.

2. Auswählen eines Computers aus einer Gruppe
Klicken Sie mit der rechten Maustaste auf das Objekt "Ereignisprotokollanzeige (lokal)" und wählen Sie einen Gruppennamen und einen Computernamen aus dem Menü aus.

3. Zuvor ausgewählter Computer
EventSentry speichert bis zu den letzten 3 Computern, mit denen Sie sich kürzlich erfolgreich verbunden haben, im Cache. Klicken Sie mit der rechten Maustaste auf das Objekt "Ereignisprotokollanzeige (lokal)" und wählen Sie einen dieser 3 (oder weniger) Computer aus.

Einschließen/Ausschließen von Ereignissen von Remote-Computern
Wenn Sie Ereignisse ein- oder ausschließen, indem Sie mit der rechten Maustaste auf Ereignisprotokolleinträge klicken, werden diese automatisch in der Gruppe angezeigt, in der sich dieser Computer befindet. Wenn Sie beispielsweise eine Verbindung zu dem Computer *CHEETAH* herstellen, der sich in der Gruppe *FILESERVERS* befindet, und ein bestimmtes Ereignis ausschließen, dann wird der resultierende Filter in der Gruppe *FILESERVERS* erstellt.

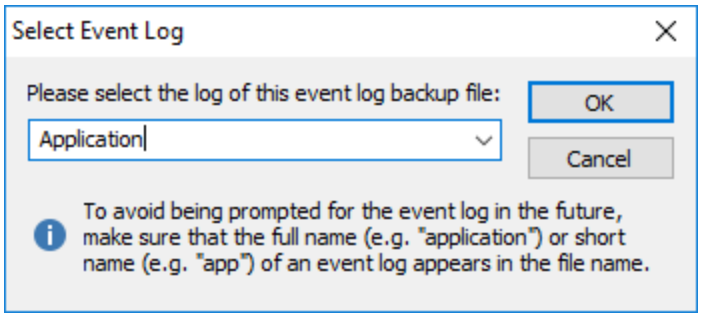
Verbindung zu trennen
Um die Verbindung zu einem entfernten Ereignisprotokoll zu trennen, klicken Sie einfach mit der rechten Maustaste auf das Ereignisprotokollobjekt des Computers und wählen Sie **Verbindung trennen**. Wenn Sie die Anwendung beenden, werden alle entfernten Ereignisprotokolle automatisch geschlossen. Beachten Sie, dass Verbindungen zu entfernten Ereignisprotokollen beim Neustart der Verwaltungsanwendung nicht automatisch wiederhergestellt werden.

3.2.2 Anzeigen von Ereignisprotokoll-Sicherungsdateien (.evtx)

Beginnend mit Version 2.70 von EventSentry haben Sie die Möglichkeit, Sicherungsdateien des Ereignisprotokolls zu öffnen. Ereignisprotokoll-Sicherungsdateien werden normalerweise mit dem Windows-Ereignisbetrachter, dem EventSentry Ereignisprotokoll-Sicherungsfunktion oder mit anderen Ereignisprotokoll-Verwaltungsanwendungen.

Um eine .evtx-Datei zu öffnen, klicken Sie mit der rechten Maustaste auf den Container "Ereignisprotokollanzeige (lokal)" und wählen Sie "Protokolldatei öffnen ...". Sie werden dann aufgefordert, nach einer .evtx-Datei zum Öffnen zu suchen.

Vermeiden einer Eingabeaufforderung für das Ereignisprotokoll
Damit ein zuvor gespeichertes Ereignisprotokoll korrekt angezeigt werden kann, muss eine Ereignisprotokoll-Verwaltungsanwendung wissen, aus welchem Ereignisprotokoll es ursprünglich exportiert wurde:



Sie können vermeiden, nach dem Ereignisprotokoll gefragt zu werden, indem Sie sicherstellen, dass der Dateiname entweder den vollständigen Namen oder eine Abkürzung des Ereignisprotokolls enthält, aus dem es exportiert wurde. EventSentry erkennt die folgenden Namen und Abkürzungen:

Vollständiger Name des Ereignisprotokolls	Abkürzung
Bewerbung	Anwendung
Sicherheit	sec
System	sys
DNS-Server	dns
Datei-Replikationsdienst	Vertreter
Verzeichnisdienst	

Wenn der Dateiname beispielsweise **fileserver_app_01122005.evtx** lautet, ordnet EventSentry diese Datei automatisch dem Ereignisprotokoll der Anwendung zu.

EventSentry erkennt benutzerdefinierte Ereignisprotokolle nicht automatisch. Wenn Sie also eine .evtx-Datei öffnen, die aus einem benutzerdefinierten Ereignisprotokoll exportiert wurde, müssen Sie entweder das benutzerdefinierte Ereignisprotokoll aus dem Dropdown-Menü auswählen oder den Namen manuell angeben.

Doppelklicken auf .evtx-Dateien im Explorer

Sie können EventSentry so konfigurieren, dass EventSentry der Standardhandler für .evtx-Dateien ist. Wenn diese Funktion aktiviert ist, können Sie im Windows-Explorer auf .evtx-Dateien doppelklicken, wodurch die .evtx-Datei automatisch in der EventSentry-Verwaltungskonsole angezeigt wird. Siehe Optionen für weitere Informationen.

3.3 Utilities

3.3.1 Agenten-Datenbank-Status-Dienstprogramm

Das Dienstprogramm für den Datenbankstatus der Agenten, es_db_agent_status.exe, fragt die Datenbank ab, um einen längeren Zeitraum der Datenbankinaktivität von einem oder mehreren Agenten zu erkennen. Durch Ausführen dieses Dienstprogramms wird sichergestellt, dass alle Agenten online sind und Daten in der Datenbank melden.

Das Dienstprogramm kann entweder bei Bedarf von der Befehlszeile aus ausgeführt werden oder regelmäßig mit einer Scheduling-Engine wie dem EventSentry-Anwendungs-Scheduler oder dem Windows Task-Scheduler geplant werden. Der Status der Agenten-Datenbank kann auch auf Anfrage über die Seite "Agentenstatus" im Wartungsmenü der Web Reports eingesehen werden.

Mithilfe von Befehlszeilenargumenten kann das Dienstprogramm entweder die Daten aller von einem Agenten verwendeten Funktionen untersuchen oder nur bestimmte Funktionen abfragen - z. B. nur Ereignisprotokolle.

Required Options

<SYSTEM DSN>	A System DSN pointing to the EventSentry database or, if an EventSentry agent is installed on the same machine where you are
<ACTION>	running the utility then you can specify the name of the EventSentry action instead of the DSN name.
<FEATURE>	The feature to verify, or **AllTables** to evaluate all features an agent is currently monitoring.
<MINUTES>	The maximum period of database inactivity, in minutes. If the most recent database entry from a host is older than <MINUTES>, the host will be listed as inactive.
<USER>	Specify a user that has permissions to query (SELECT) data, usually eventsentry_web
<PASS>	Password of <USER>

Optional Options

/V	Verbose output, useful when utilizing "AllTables" feature

Unter Windows Vista und höher muss das Programm von einer erhöhten Eingabeaufforderung ("Als Administrator ausführen") ausgeführt werden, wenn es auf eine EventSentry-Aktion verweist.

Beispiele

1. Stellen Sie eine Verbindung mit der Aktion "Primäre Datenbank" her und überprüfen Sie, ob alle Hosts in den letzten 30 Minuten Ereignisprotokolldaten gemeldet haben:
```
es_db_agent_status "Primary Database" EventLog 30 eventsentry_web 4h3Passw0rd
```

2. Stellen Sie eine Verbindung mit MyDSN System-DSN her und überprüfen Sie, ob alle Hosts die Leistung in den letzten 15 Minuten gemeldet haben:
```
es_db_agent_status MyDSN Performance 15 eventsentry_web #df2er
```

3. Stellen Sie eine Verbindung mit der MSSQL-Aktion her und überprüfen Sie, ob alle Hosts in den letzten 60 Minuten Daten für alle konfigurierten Features gemeldet haben:
```
es_db_agent_status MSSQL AllTables 60 dbreader MyP4ssw0rd!
```

4. Stellen Sie eine Verbindung zu der MySQL-Aktion her und überprüfen Sie, ob alle Hosts in den letzten 3 Stunden Ereignisprotokoll-, Syslog- & SNMP-Trap-Daten gemeldet haben:
```
es_db_agent_status MySQL EventLog,Syslog,Snmp 180 eventsentry_web thePa55w0rt
```

5. Stellen Sie eine Verbindung zur Aktion "Primäre Datenbank" her und überprüfen Sie, ob alle Hosts innerhalb der letzten 24 Stunden Ereignisprotokoll- und Anmeldeverfolgungsdaten gemeldet haben:
```
es_db_agent_status "Primary Database"  EventLog,LogonTracking 1440 eventsentry_web
datpa55w00rd
```

3.3.2 Konfigurations-Assistent

Der Konfigurationsassistent wird in der Regel nach der Ersteinrichtung und nach Hauptversions-Upgrades gestartet, wo er das Datenbankschema aktualisiert und neue Komponenten konfiguriert. Der Konfigurationsassistent wird auch zur Initialisierung neuer Datenbanken verwendet.

- Konfigurieren Sie eine neue SMTP-Aktion, wenn keine SMTP-Aktion aktuell eingerichtet ist
- Alle Datenbanken, die durch eine Aktion referenziert werden, auf das neueste Schema aktualisieren
- Einrichten einer neuen Datenbank, einschließlich Aktion, wenn derzeit keine Datenbankaktionen konfiguriert sind
- Einrichten und Konfigurieren einer individuellen Datenbank, wenn sie von einem Datenbank-Aktionsdialog in der Verwaltungskonsole gestartet wird
- Installieren & Konfigurieren des Heartbeat-Agenten
- Installieren & Konfigurieren der Network Services
- Installieren & Konfigurieren der ADMonitor-Komponente

The configuration assistant is automatically launched after every installation / upgrade.

Voraussetzungen

Der Konfigurationsassistent befindet sich im Unterverzeichnis **config_assistant** und benötigt zur Ausführung die folgenden Dateien:

- es_config_assistant.exe
- Qt5Core.dll
- Qt5Gui.dll
- Qt5Xml.dll
- Qt5Widgets.dll
- msvcp140.dll
- concrt140.dll
- vccorlib140.dll
- vcruntime140.dll
- schema.xml
- platforms\qwindows.dll

Command-Line Parameters

The utility supports a single command line parameter, "/initdb", which needs to be followed by the name of a database action. For example:

```
es_config_assistant.exe /initdb "Primary Database"
```

Dadurch wird entweder die Datenbank, auf die die Aktion "Primäre Datenbank" verweist, initialisiert oder die bestehende Datenbank auf das neueste Schema aktualisiert.

3.3.3 Datenbank Purge Utility

Das Dienstprogramm zum löschen von Daten in der Datenbank wird als Teil der **Web Reports** installiert und befindet sich im Unterordner "Database Wizards" des Installationsordners %PRODUCT%.

Required Options

<SYSTEM DSN>	Ein System-DSN
	oder,
<ACTION>	

	Wenn %PRODUCT% auf demselben Rechner installiert ist, auf dem Sie es_db_purge.exe ausführen, können Sie den Namen der %PRODUCT%-Aktion anstelle des DSN-Namens angeben.
<FEATURE>	Wenn Sie mit diesem Dienstprogramm Datensätze löschen, müssen Sie angeben, aus welcher Funktion (z. B. **EventLog** oder **Performance**) die Daten tatsächlich gelöscht werden sollen. Nachstehend finden Sie eine Liste der verfügbaren Funktionen. Sie können jeweils nur eine Funktion auswählen
<DAYS/HOURS>	Löscht Datensätze, die älter sind als die angegebene Anzahl von Tagen (Standard) oder Stunden. Geben Sie Tage an, indem Sie ein "d" an die Zahl anhängen, geben Sie Stunden an, indem Sie ein "h" an die Zahl anhängen.
<USER>	Geben Sie einen Benutzer an, der die Berechtigung hat, Daten zu löschen
<PASS>	Kennwort von <USER>

Optional Options

/count	Zeigt an, wie viele Datensätze gelöscht werden sollen
/test	Daten nicht tatsächlich löschen, sondern nur zeigen, wie viele Datensätze davon betroffen wären
/shrinkdb	Verkleinern der Datenbank (nur MSSQL) nach Löschung
/shrinklog	Verkleinern von Datenbankprotokolldateien (nur MSSQL) nach Löschung
/shrinkindexes	Verkleinern von Indizes (nur PostgreSQL) nach dem Löschen, kann erhebliche Mengen an temporärem Speicherplatz erfordern
/log:<FILENAME>	Protokollierung aller durchgeführten Aktionen in einer Protokolldatei
/host:<HOSTNAME>	Nur von HOSTNAME protokollierte Daten löschen. Wenn angegeben, werden keine NetFlow- oder ADMonitor-Daten gelöscht.
/utc	Die Daten in der Datenbank werden mit einem UTC-Zeitstempel geschrieben, der bei der Übergabe eines Aktionsnamens automatisch erkannt wird.

Unter Windows Vista und höher muss das Purge Tool über eine erweiterte Eingabeaufforderung ("Als Administrator ausführen") ausgeführt werden, wenn es auf eine EventSentry-Aktion verweist.

Beispiele

1. Löschen Sie **alle Daten** aus der "Primärdatenbank", die älter als 90 Tage sind.
```
es_db_purge.exe "Primary Database" All Tables 90d postgres postgrespw
```

2. Delete **all event log data** from the "Archive Database" action which is older than 366 days
```
es_db_purge.exe "Archive Database" EventLog 366d postgres postgrespw
```

3. Ermitteln Sie, wie viele Syslog-Daten **älter als 30 Tage** sind
```
es_db_purge.exe "Primary Database" Syslog 30d /test postgres postgrespw
```

4. Löschen von Ereignisprotokolldaten nur von Host **DC03**, die älter als 90 Tage sind
```
es_db_purge.exe "Primary Database" EventLog 90d /host:DC03 postgres
postgrespw
```

Planung

Wir empfehlen, dass Sie das Dienstprogramm, z.B. über den EventSentry Application Scheduler (oder den Windows-Aufgabenplaner), regelmäßig, **mindestens jedoch** monatlich, ausführen. Dadurch wird sichergestellt, dass sich in Ihrer Datenbank keine unnötigen Daten ansammeln.

Die folgende Tabelle erläutert alle unterstützten Feature-Namen. Sie können auch das AllTables-Schlüsselwort verwenden, um Daten aus allen Tabellen zu bereinigen.

Feature Name	Explanation
EventLog	Event log records
Diskspace	Disk space data
Performance	Performance data
ProcessTracking	Compliance: Process tracking data
LogonTracking	Compliance: Console Logon tracking data
PrintTracking	Compliance: Print tracking data
HeartbeatHistory	Heartbeat history
HeartbeatPing	Heartbeat ping history
ServiceHistory	Service history
SoftwareHistory	Software history
EnviroTempHumid	Temperature and humidity (if available) data
EnviroMotion	Motion data
Nessus	Nessus data
Syslog	Syslog data
Snmp	Snmp data
FileMonitoring	File Change monitoring data
LogFileDelimited	Data from delimited log files
LogFileNondelimited	Data from non-delimited log files
FileAccess	File Access Tracking data
RegistryTracking	Registry tracking data
UptimeHistory	Uptime history
ActionHistory	Action trigger history
ReportHistory	Report history
AccountMgmtUser	Compliance: Account Management Tracking (Users)
AccountMgmtGroup	Compliance: Account Management Tracking (Groups)
AccountMgmtComputer	Compliance: Account Management Tracking (Computer)
LogonAuthFailure	Compliance: Network Logon (Failure)
LogonAccountAuth	Compliance: Network Logon (Domain Account Authentication)
LogonByType	Compliance: Network Logon (Logon By Type)
PolicyChange	Compliance: Policy Change Tracking
LargeFiles	Disk Space data (large files only)
ScheduledTasks	Scheduled Tasks inventory data
NetFlow	NetFlow data
ADMonitor	ADMonitor object changes
ADMonitorGroupPolicy	ADMonitor group policy changes
SysmonNetwork	Sysmon network data
ValidationScripts	Validation script data
PermissionStatus	Permission Inventory data

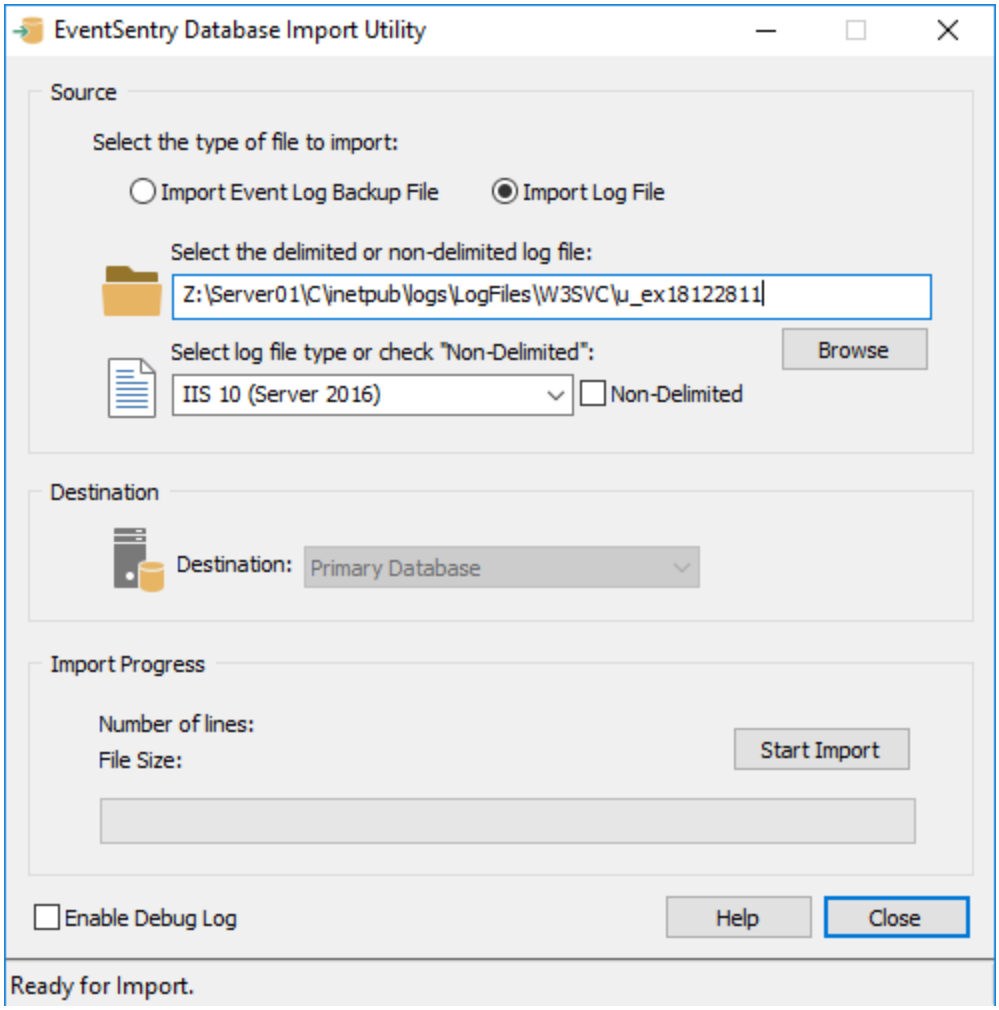
3.3.4 Log Import Utility

Mit dem EventSentry-Log-Import-Dienstprogramm können Sie zuvor gesicherte Ereignisprotokolldateien (.evtx) oder Protokolldateien (z. B. IIS, DHCP usw.) in eine EventSentry-Datenbank importieren, so dass sie in den webbasierten Berichten durchsuchbar sind.

Vorteile

Das EventSentry-Dienstprogramm zum Importieren von Ereignisprotokollen ist nützlich für Administratoren, die alle ihre Ereignisprotokolle regelmäßig automatisch mit EventSentry sichern, jedoch mit begrenzter Datenbankspeicherung. Mit dem Dienstprogramm können die gesicherten .evtx-Dateien jederzeit in die Datenbank importiert werden. Sie können das Dienstprogramm auch verwenden, um EVTX-Dateien zu importieren, die vor der Verwendung von EventSentry gesichert wurden.

Sie können das Dienstprogramm auch verwenden, um abgegrenzte und nicht abgegrenzte Protokolldateien in die EventSentry-Datenbank zu importieren. Da das Dienstprogramm Befehlszeilenparameter unterstützt und geräuschlos ausgeführt werden kann, ist es besonders nützlich für den Import von Protokolldateien auf einer geplanten Basis.



Starten Sie das Dienstprogramm auf einem Computer, auf dem Sie EventSentry installiert haben, mit der Setup-Anwendung, einschließlich der Komponente Verwaltungskonsole. Sie können das

Dienstprogramm dann entweder über das Startmenü (Start -> Programme -> EventSentry -> EventSentry Datenbank-Import-Dienstprogramm) oder durch Auswahl von "Tools -> Utilities -> Database Import Utility" starten.

Wenn Sie eine Ereignisprotokoll-Rückdatei importieren, können Sie auch mit der rechten Maustaste auf den Container "Event Log Viewer (Local)" in der Management-Konsole klicken und "Import Log File to Database" wählen.

Importieren von Ereignisprotokoll-Sicherungsdateien

Wählen Sie die Sicherungsdatei des Ereignisprotokolls (.evtx) und wählen Sie den Typ des Ereignisprotokolls, den die Datei enthält. Wenn der Dateiname entweder die Zeichenfolgen "app", "sec", "sys", "dns", "rep" oder "dir" enthält, erkennt EventSentry das Ereignisprotokoll automatisch und wählt das Ereignisprotokoll voraus. Es ist wichtig, sicherzustellen, dass die Ereignisprotokollauswahl korrekt ist, damit das Datenbankimport-Dienstprogramm weiß, wie Ereignisprotokoll-IDs in echte Meldungen übersetzt werden können.

Einschränkungen

Wenn die Gesamtzahl der von Ihnen erworbenen EventSentry-Lizenzen weniger als 10 beträgt, muss der Computer, von dem Sie die Ereignisprotokoll-Sicherungsdatei importieren, in einer EventSentry-Gruppe vorhanden sein. Wenn der Computer nicht vorhanden ist, müssen Sie den Computer über die Verwaltungskonsole zu einer Gruppe hinzufügen und das Dienstprogramm neu starten.

Importieren von getrennten und nicht getrennten Protokolldateien

Wählen Sie eine abgegrenzte oder nicht abgegrenzte Protokolldatei zum Importieren aus. Wenn Sie eine abgegrenzte Protokolldatei importieren, muss eine Protokolldatei-Definition vorhanden sein, damit die Datei korrekt importiert werden kann. Wenn keine Definition vorhanden ist, müssen Sie das Dienstprogramm schließen und zuerst eine Protokolldatei-Definition erstellen.

Das Datenbankimport-Dienstprogramm aktualisiert automatisch die Werte "Anzahl der Zeilen" und "Dateigröße" im Abschnitt "Importfortschritt", nachdem eine Datei mit der Schaltfläche "Durchsuchen" ausgewählt wurde. Das Dienstprogramm erkennt auch automatisch, ob eine Datei ein Unix-Zeilentrennzeichen enthält, und importiert diese Dateien ebenfalls korrekt.

Ziel

Wählen Sie die Datenbankbenachrichtigungsaktion, in die Sie die Daten schreiben möchten. Wenn Ihre EventSentry-Installation nur eine Datenbankbenachrichtigungsaktion enthält, wird diese automatisch ausgewählt, und das Pulldown-Menü wird deaktiviert.

Import-Fortschritt

Wenn Sie sich vergewissert haben, dass Ihre Auswahl korrekt ist, können Sie auf die Schaltfläche "Import starten" klicken, um den Import zu starten. In diesem Bereich wird Ihnen auch die Größe der zu importierenden Ereignisprotokoll-Sicherungsdatei und die Anzahl der in der Ereignisprotokoll-Sicherungsdatei enthaltenen Ereignisprotokolleinträge angezeigt.

Der Fortschrittsbalken zeigt Ihnen an, wie viele Daten bisher importiert wurden, und Sie können den Import jederzeit abbrechen.

Command-Line Options

Das EventSentry-Datenbankimport-Dienstprogramm unterstützt die folgenden Befehlszeilenoptionen:

Command-Line Option	Explanation	Example

/file:	The event log backup (.evtx) or log file to import	/file:server01_app_072006 .evtx
/action:	The name of the EventSentry action to write the data to	/action:mssql
/eventlog:	The name of the event log contained in the event log backup file	/eventlog:Security
/filedefinition:	Name of an EventSentry log file definition	/filedefinition:IIS
/nondelimited	Indicate that the file to import is a non-delimited log file	
/unix	Force utility to use a Unix line terminator	
/debug	Enable debug logging to %SYSTEMROOT% \system32\eventsentry	/debug
/?	shows supported command-line options	/?

Um beispielsweise das Sicherheitsereignisprotokoll aus der Datei DBSRV01_SEC-062006.evtx automatisch in der Aktion Primäre Datenbank aufzuzeichnen, führen Sie den folgenden Befehl aus:

```
 eventsentry_db_import.exe /file:"c:\logs\DBSRV01_SEC-
062006.evtx" /eventlog:Security /action:"Primary Database"
```

Wenn Sie mehrere Protokolldateien in die mssql-Aktion importieren müssen, dann können Sie z.B. eine Batch-Datei erstellen:

```
 eventsentry_db_import.exe /file:DBSRV01_SEC-
062006.evtx /eventlog:Security /action:mssql
 eventsentry_db_import.exe /file:DBSRV01_SEC-
072006.evtx /eventlog:Security /action:mssql
 eventsentry_db_import.exe /file:DBSRV01_SEC-
082006.evtx /eventlog:Security /action:mssql
```

Um eine IIS-Protokolldatei, bei der es sich um eine "delimited" Protokolldatei handelt, in die Datenbank zu importieren, führen Sie den folgenden Befehl aus:

```
 eventsentry_db_import.exe /file:ex070828.log /filedefinition:"IIS 6" /action:mssql
```

3.3.5 Event Message Browser

Mit dem integrierten Ereignisnachrichten-Browser können Sie alle verfügbaren Ereignisnachrichten anzeigen, die auf Ihrem System protokolliert werden können. Sie können einfach ein Ereignisprotokoll (z.B. **Anwendung**) und eine der verfügbaren Ereignisquellen aus diesem Protokoll (z.B. **ntbackup**) auswählen und dann alle verfügbaren Ereignis-IDs aus dieser Quelle überprüfen.

Allgemein

Wenn der Ereignisnachrichten-Browser aus dem Filterdialog gestartet wird, können Sie die grundlegenden Ereigniseigenschaften auf den Filter anwenden. Zusätzlich können Sie das ausgewählte Ereignis auch im Ereignisprotokoll erzeugen, indem Sie auf die Schaltfläche **Test** klicken.

Der Ereignisnachrichten-Browser kann aus dem Filterdialog durch Klicken auf die Schaltfläche **Suchen** oder über das Menü unter **Tools -> Utilities -> Event Message Browser**.

Insertion Strings / Creating Test Events

Die meisten Ereignismeldungen verwenden sogenannte Einfügungszeichenketten, die durch das Prozentzeichen gefolgt von einer Zahl angegeben werden. Beispielsweise könnte eine Ereignisnachricht im Ereignisnachrichten-Browser die Zeichenfolge **%1** enthalten, die zur Laufzeit durch Nutzdaten ersetzt wird. Zum Beispiel die Ereignisnachricht (Ereignis-ID **10100** von **EventSentry**):

```
The status for service %1 (%2) changed from %3 to %4.
```

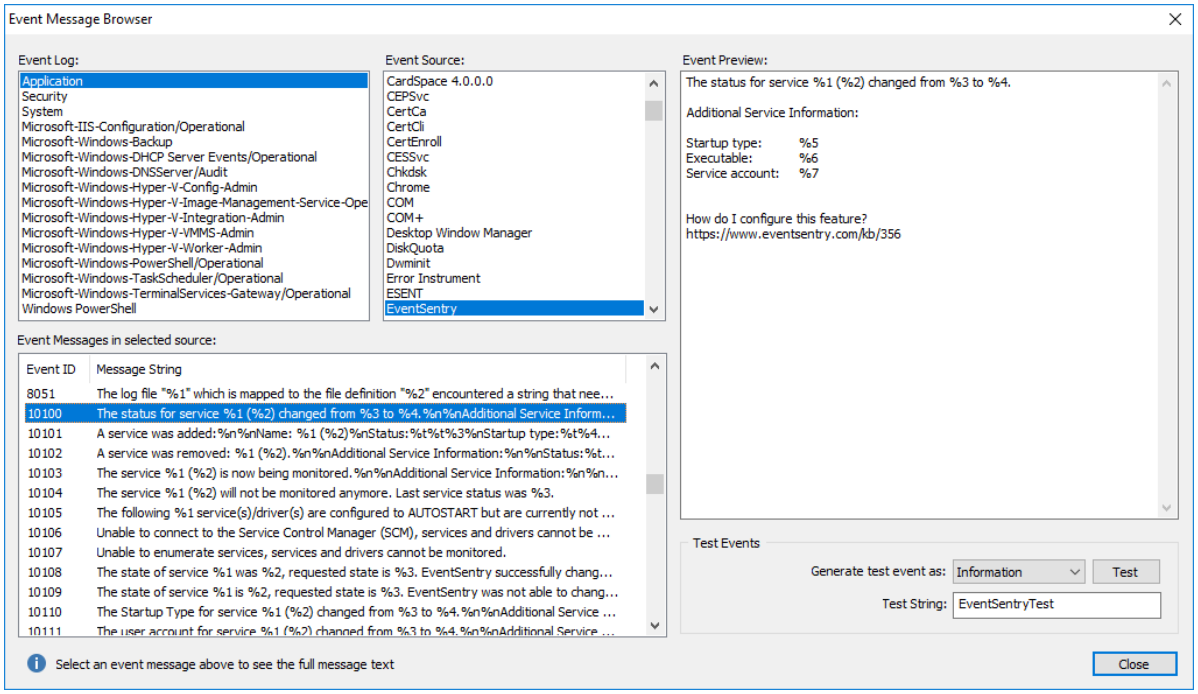
sieht im Ereignisprotokoll ähnlich aus wie unten:

```
The status for service Winmgmt (Windows Management Instrumentation)
changed from Running to Stopped.
```

da EventSentry den Einfügetext %1, %2, %3 und %4 durch Daten ersetzt, die für die aktuelle Operation relevant sind. Bei der Erstellung eines Testereignisses über den Ereignismeldungs-Browser werden die Einfügezeichenfolgen alle durch den im Feld **Testzeichenfolge** angegebenen Text ersetzt, bei dem es sich standardmäßig um *EventSentryTest* handelt.

> ⚠ Sie können derzeit mit dem Ereignismeldungs-Browser keine Test-Ereignisse im Ereignisprotokoll **Sicherheit** erstellen.

Der untenstehende Screenshot zeigt den Ereignismeldungs-Browser, in dem das obige Ereignis angezeigt wird:



3.3.6 Protokoll-Parser (Collector)

Der Protokoll-Parser kann die vom EventSentry-Collector generierten Speicherabbilddateien oder die vom Agent generierte temporäre Datei zur Fehlerbehebung untersuchen. Die Ausführung des Protokoll-Parser-Dienstprogramms sollte nur unter den folgenden Umständen erforderlich sein:

1. Der Collector protokollierte das Ereignis 142 oder 143

2. Die temporäre Datei, die vom Agenten erzeugt wird, während ein Collector offline ist und untersucht werden muss

Das Protokoll-Parser-Dienstprogramm (protocol_parser.exe) befindet sich im Unterverzeichnis "resources" des EventSentry-Installationsverzeichnisses.

Collector-Veranstaltung 142 & 143
Wenn der Collector ein Paket nicht erfolgreich parsen kann, protokolliert er Ereignis 142 und/oder 143 und überträgt den Paketinhalt in eine Datei mit der Endung **.dump** im Verzeichnis %SYSTEMROOT\system32\eventsentry\temp\collector. Übergeben Sie einfach den Dateinamen als Parameter an das Protokoll-Parser-Dienstprogramm.

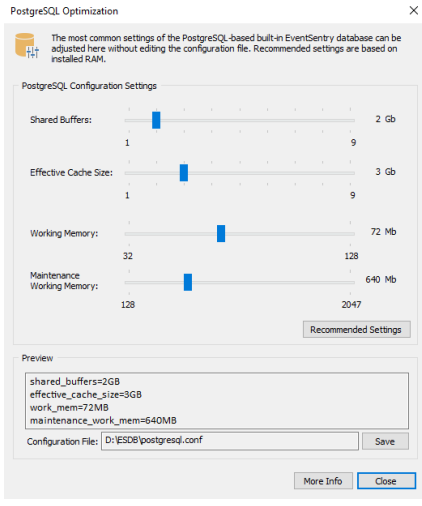
Sicherungsdatei des Agenten
Der Agent protokolliert alle zwischengespeicherten Daten in der Datei **%SYSTEMROOT\SysWOW64\eventsentry\temp\eventsentry_collector.client_backup.tmp**, wenn ein Collector nicht verfügbar ist, wenn die zwischengespeicherten Daten nicht im Speicher abgelegt werden können oder wenn der Agent angehalten wird. Übergeben Sie einfach den Dateinamen als Parameter an das Protokoll-Parser-Dienstprogramm.

3.3.7 Remote Update Utility

Siehe "Automatisieren der Fern-Aktualisierung" für weitere Informationen über das Fern-Aktualisierungsprogramm eventsentry_upd.exe.

3.3.8 Built-In Database PostgreSQL Optimization

Da die integrierte PostgreSQL-Datenbank nicht standardmäßig auf Leistung optimiert ist, ist es in der Regel notwendig, einige der Konfigurationseinstellungen zu ändern, um eine bessere Leistung der Datenbank zu erreichen. Alle Einstellungen für die integrierte Datenbank können durch Bearbeiten der PostgreSQL-Konfigurationsdateien geändert werden, aber die wichtigsten leistungsbezogenen Einstellungen können auch in der Verwaltungskonsole angepasst werden, ohne dass Konfigurationsdateien direkt bearbeitet werden müssen.



Der PostgreSQL-Optimierungsdialog kann aufgerufen werden über:

- Ribbon: Tools -> Utilities -> Built-In Database Optimization
- Datenbank-Aktionsdialog (nur PostgreSQL-Aktionen mit lokaler Datenbank)

Das Dialogfeld ermöglicht die Anpassung ausgewählter Konfigurationseinstellungen, die sich alle auf verschiedene Aspekte der Datenbankleistung auswirken. Wenn Sie den Mauszeiger über die Hebel bewegen, wird ein Tooltip mit einer Beschreibung der einzelnen Parameter angezeigt.

Konfigurationsdatei gefunden
Wenn der Dialog von einem Host aus gestartet wird, auf dem die EventSentry-Datenbank lokal ausgeführt wird, versucht die Verwaltungskonsole, die Konfigurationsdatei **(**standardmäßig **postgresql_eventsentry.conf** oder **postgresql.conf**) zu analysieren und die aktuellen Einstellungen für die aufgeführten Konfigurationsparameter zu lesen. Die zutreffende Konfiguration wird

im Feld "Konfigurationsdatei" angezeigt, wenn eine Datei erfolgreich erkannt wurde.

Wenn Sie auf "Recommended Settings" klicken, werden die Konfigurationseinstellungen auf der Grundlage des installierten RAMs angepasst. Durch Klicken auf die Schaltfläche "Save" wird die aktive Konfigurationsdatei gespeichert.

Keine Konfigurationsdatei(en) gefunden
Wenn keine Konfigurationsdateien gefunden werden, wählt der Dialog die empfohlenen Einstellungen auf der Grundlage des derzeit verfügbaren Arbeitsspeichers aus und zeigt eine Vorschau der Konfigurationsparameter im Abschnitt "Preview" an. Diese Konfigurationsparameter können dann in eine beliebige PostgreSQL-Konfigurationsdatei eingefügt werden.

Weitere Informationen zur Optimierung der Leistung der integrierten PostgreSQL-Datenbank finden Sie unter KB article 232.

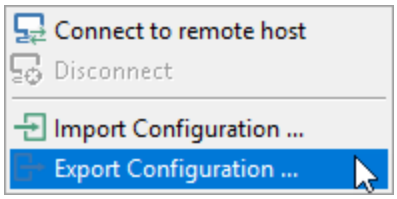
Der **EventSentry-Datenbankdienst** muss immer neu Konfigurationseinstellungen wirksam werden.

3.4 Exportieren, Importieren und Speichern der Konfiguration

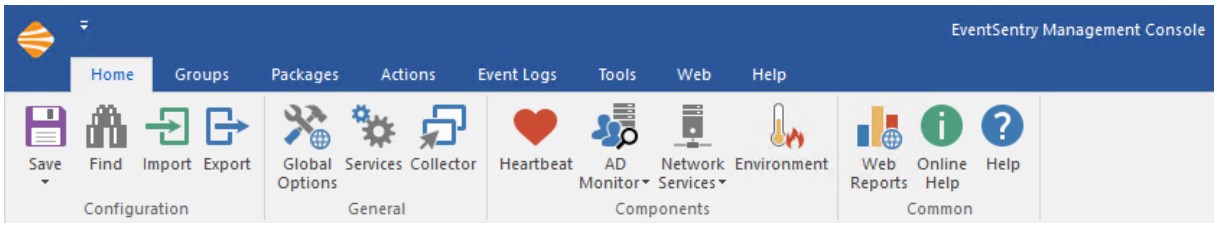
Die gesamte EventSentry-Konfiguration wird in der Registry gespeichert und kann einfach exportiert / importiert werden. Dies kann nützlich sein, wenn Sie mehrere Installationen von EventSentry hinter einer Firewall haben. Es wird dringend empfohlen, die Konfiguration regelmäßig zu Sicherungszwecken zu exportieren. Alternativ können Sie die Konfiguration zu Dokumentationszwecken auch als HTML-Datei speichern.

Diese Funktion wird nur unterstützt wenn die Konsole mit dem lokalen Rechner verbunden ist.

Exportieren
Um die Konfiguration in eine **.**reg-Registrierungsdatei zu exportieren, klicken Sie entweder mit der rechten Maustaste auf das Computerobjekt und wählen Sie **Export Configuration**



oder wählen Sie auf der Registerkarte **Home** die Option **Export**.



Sie werden dann aufgefordert, einen Dateinamen anzugeben, unter dem die Konfiguration gespeichert werden soll. Diese Datei kann dann auf einen anderen Computer importiert werden, auf dem ebenfalls EventSentry ausgeführt wird.

Importieren

Um die Konfiguration auf einen Zielcomputer zu importieren, müssen Sie zunächst die zuvor erstellte **.**reg-Datei auf den Zielcomputer übertragen. Es gibt dann 2 Optionen:

- Öffnen Sie die EventSentry-GUI und klicken Sie, wie oben unter **Exportieren** beschrieben, entweder mit der rechten Maustaste auf das Computerobjekt und wählen Sie **Konfiguration importieren** oder wählen Sie **Import** aus dem Menü **Datei**. Die GUI wird geschlossen, damit die Änderung wirksam wird.

- Doppelklicken Sie im Explorer auf die **.**reg-Datei, um sie in die Registrierung zu importieren. Bitte beachten Sie, dass die GUI (eventsentry_gui.exe) geschlossen sein muss, wenn Sie die Konfiguration importieren, da die importierten Einstellungen sonst von der GUI überschrieben werden könnten.

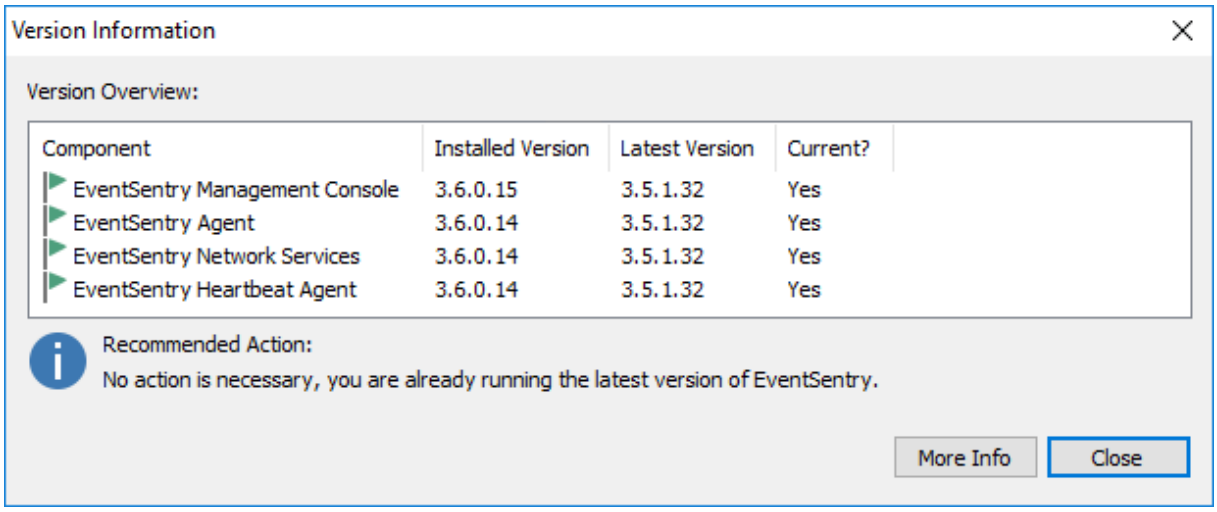
Speichern der Konfiguration

Um die gesamte EventSentry-Konfiguration in einer HTML-Datei zu speichern, wählen Sie auf der Registerkarte Home die Option "Save as Html". Alle Konfigurationsoptionen, mit Ausnahme der GUI-Einstellungen aus den Tools -> Options Dialogen, werden dann in die angegebene Datei geschrieben, die in jedem gängigen Webbrowser wie Internet Explorer, Firefox und Chrome geöffnet werden kann. Bitte beachten Sie, dass **Sie** die Konfiguration **nicht** zu einem späteren Zeitpunkt aus einer .html-Datei importieren **können**; dies ist nur möglich, wenn Sie die Konfiguration **exportieren** (siehe oben).

3.5 Auf neue Versionen prüfen

Neben der Überprüfung auf die neueste Version von EventSentry auf der Produkt-Website können Sie auch die Verwaltungskonsole verwenden, um einfach festzustellen, ob Sie die neueste Version von EventSentry verwenden, und alle anwendbaren Patches herunterladen.

Um nach einer neuen Version oder einem Patch zu suchen, navigieren Sie zur **Help -> Check for Updates**, die einen Dialog ähnlich dem unten gezeigten anzeigt:



Der Dialog **Versionsinformationen** zeigt Ihnen die drei Hauptkomponenten von EventSentry und ob sie aktuell sind oder nicht. Wenn die Spalte "Aktuell" "Ja" anzeigt und ein grünes Kontrollkästchen neben der Komponente angezeigt wird, dann ist diese auf dem neuesten Stand und keine Aktion erforderlich.

Die Aktualisierungsfunktion erkennt Folgendes:

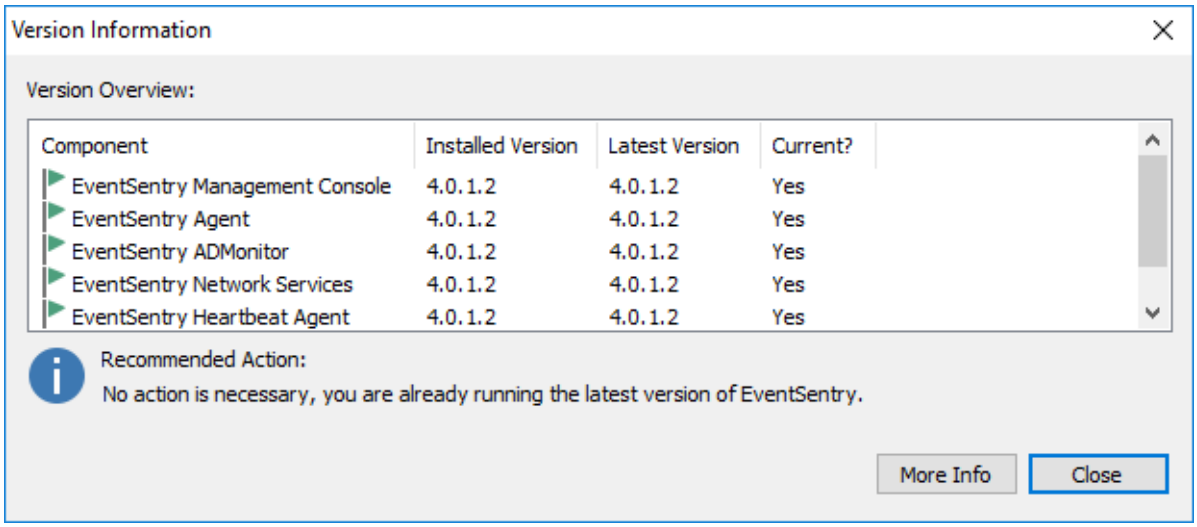
- Patch-Verfügbarkeit: Sie verwenden die neueste Version, aber es wurde ein Patch veröffentlicht, der bestimmte Probleme behebt.
- Neue Version verfügbar: Sie benutzen nicht die neueste Version
- Up-To-Date: Sie verwenden die neueste Version

Patch-Verfügbarkeit

Wenn ein Patch für EventSentry veröffentlicht wurde, können Sie diese Funktion verwenden, um den Patch automatisch herunterzuladen und zu installieren. Das folgende Dialogfeld zeigt eine Installation, die Version 3.0.0.16 ausführt, wobei jedoch die neueste Version 3.0.0.25 verfügbar ist (die auch eine kritische Korrektur enthält). Die **empfohlene Aktion** ist daher, den neuesten Patch herunterzuladen und zu installieren, um die Installation auf den neuesten Stand zu bringen.

Wenn Sie sich für die Online-Prüfung des Wartungsablaufs entschieden haben und über einen aktiven Wartungsvertrag oder eine aktive Testversion verfügen, können Sie das neueste Installationsprogramm direkt über die Verwaltungskonsole herunterladen. Die Online-Wartungsprüfung kann unter Tools -> Options -> Version Check / Welcome -> "Enable online maintenance expiration check and integrated patch download" aktiviert werden. Wenn Sie sich von der Online-Wartungsprüfung abgemeldet haben oder keinen aktiven Wartungsvertrag haben, dann können Sie den neuesten Installer aus dem Kundenbereich herunterladen.

Klicken Sie auf die Schaltfläche **Download & Patch installieren**, um den Download des Patches zu starten. Heruntergeladene Installationsprogramme werden im Unterverzeichnis **Patches** Ihrer EventSentry-Installation gespeichert, z.B. `C:\Program Files\EventSentry\Patches`.



Verfügbarkeit der neuen Version

Wenn eine neue Version für EventSentry veröffentlicht wurde, dann zeigt die **Empfohlene Aktion** an, dass Sie eine neue Version herunterladen und installieren können, und es wird eine Schaltfläche **Download** angezeigt. Da das Herunterladen einer neuen Version einen aktuellen Wartungsvertrag erfordert, gelangen Sie durch Klicken auf den Download-Button zu unserer Software-Update-Seite, auf der Sie sich mit Ihrer registrierten E-Mail-Adresse und Ihrem Passwort anmelden müssen.

Weitere Informationen zur Aktualisierung auf die neueste Version finden Sie in den Unterkapiteln von Auf eine neue Version aktualisieren.

Automatische Prüfung auf neue Versionen

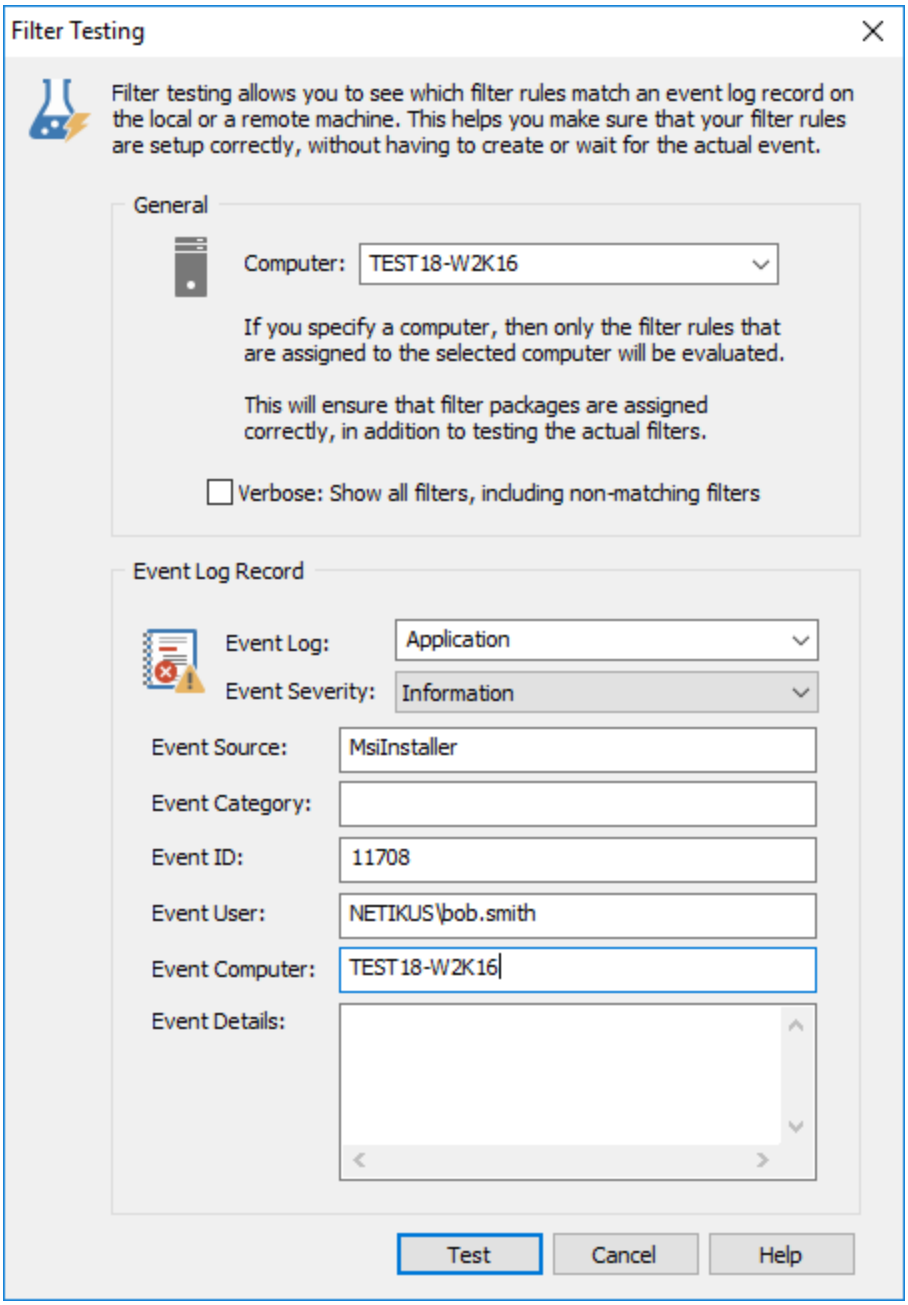
Zusätzlich zum Aufrufen der Funktion **Nach Updates suchen** über das Hilfemenü können Sie EventSentry so konfigurieren, dass bei jedem Start der Verwaltungskonsole automatisch nach neuen Versionen und Patches gesucht wird.

Sie können diese Funktion konfigurieren, indem Sie zu **Tools -> Options -> Version Check / Welcome** navigieren, weitere Informationen finden Sie hier.

3.6 Testen von Ereignisprotokoll-Filterregeln

Mit dem Dienstprogramm zum Testen von Filterregeln können Sie Ihre Filterregeln gegen tatsächliche Ereignisprotokollereignisse testen, ohne tatsächlich auf Ereignisse warten zu müssen. Das Tool ist auch in die integrierte Ereignisprotokollanzeige integriert und zeigt Ihnen an, welche Filterregeln dem Ereignis entsprechen würden, einschließlich der Aktion, die ausgelöst würde.

Auf diese Weise lässt sich leicht sicherstellen, dass die Filterregeln für Ihr Ereignisprotokoll korrekt eingerichtet sind.



Starten des Filterregeltests

Sie können das Dienstprogramm entweder über das Hauptmenü starten, indem Sie zu **Tools -> Utilities -> Filter Rules Test Utility** navigieren, oder Sie können auf das Werkzeug zugreifen, indem Sie mit der rechten Maustaste auf ein Ereignis aus dem integrierten Ereignisprotokoll-Viewer klicken und "Test gegen Filterregeln" wählen. Letzteres ist im Allgemeinen einfacher, da alle Ereigniseigenschaften automatisch in den Abschnitt "Ereignisprotokollaufzeichnung" eingetragen werden.

Computer

Da Ereignisprotokollfilter Computern und Gruppen zugewiesen werden, können verschiedenen Computern unterschiedliche Regeln zugewiesen sein. Daher muss EventSentry wissen, welche Filterregeln geladen und gegen welche Regeln getestet werden sollen. Wenn Sie hier keinen Computernamen angeben, wird der Ereignisprotokolleintrag gegen **alle** Filterregeln getestet.

Ausführlich: Alle Filter anzeigen, auch nicht übereinstimmende

Wenn Sie diese Option markieren, können Sie genau sehen, warum ein Filter **nicht** mit Ihrem Ereignis übereinstimmt. Standardmäßig zeigt das Tool nur die erste Filterregel an, die mit dem im Abschnitt "Ereignisprotokollaufzeichnung" angegebenen Ereignis übereinstimmt. Das bedeutet, dass, wenn ein Ereignis z.B. mit einem Ausschluss- **und** einem Einschlussfilter übereinstimmt, nur der Ausschlussfilter ohne die Option "Ausführlich" angezeigt wird.

Filter, die nicht mit dem Ereignis übereinstimmen, werden nicht angezeigt. Wenn Sie beispielsweise eine Fehlersuche durchführen müssen, warum ein von Ihnen erstellter Filter nicht mit einem bestimmten Ereignis übereinstimmt und dieses nicht verarbeitet, dann zeigt Ihnen diese Option alle nicht übereinstimmenden Filter an und gibt an, warum sie nicht mit dem Ereignis übereinstimmten.

Ereignisprotokoll-Aufzeichnung

Geben Sie so viele Eigenschaften aus dem eigentlichen Ereignis wie möglich an. Sie sind verpflichtet, mindestens die

- Ereignisprotokoll
- Ereignis-Schweregrad
- Ereignis-Quelle
- Ereignis-ID

Anzeigen der Ergebnisse

Klicken Sie auf die Schaltfläche TEST, um die Ergebnisse des Tests anzuzeigen. Die Ergebnisse sehen ähnlich aus wie auf dem unten gezeigten Screenshot, wenn Sie das Kontrollkästchen "Verbose" nicht markieren:

Filter Name	Package	Match Reason	Actions
Email Critical Events	Email Notification		Default Email
Consolidate Non-Security...	Database Consolidation		Primary Datab...

Beachten Sie, dass "Match Reason" leer ist, wenn der Abgleichsfilter keine Quelle, Kategorie, Ereignis-ID oder Ereignisdetail konfiguriert hat. Andernfalls zeigt die Spalte an, welche Felder des Filters mit dem Ereignis übereinstimmten.

Wenn Sie die Option "Ausführlich" wählen, dann sieht die Ausgabe etwas anders aus und enthält zusätzliche Spalten:

Filter Name	Package	Match?	Reason	Actions
Bit Defender/Digital Signi...	AntiVirus Software	No	Severity	Default Email
Bit Defender/No CD-ROM	AntiVirus Software	No	Severity	Default Email
G Data/G Data: Scan Audi...	AntiVirus Software	No	Severity	Default Email
G Data/G Data: System Int...	AntiVirus Software	No	Severity	Default Email
Malwarebytes/Web Prote...	AntiVirus Software	No	Severity	Default Email
McAfee/McAfee: Port Blo...	AntiVirus Software	No	Severity	Default Email
McAfee/Unsigned code w...	AntiVirus Software	No	Severity	Default Email
Sophos/Sophos: Checksu...	AntiVirus Software	No	Severity	Default Email
Sophos/Sophos: EM Library	AntiVirus Software	No	Severity	Default Email
Sophos/Sophos: Perfmon	AntiVirus Software	No	Severity	Default Email
Sophos/Sophos: Service A...	AntiVirus Software	No	Severity	Default Email
Sophos/Sophos: Service R...	AntiVirus Software	No	Event Log	Default Email
Symantec/Symantec: Def ...	AntiVirus Software	No	Severity	Default Email
Symantec/Symantec: Extr...	AntiVirus Software	No	Severity	Default Email
Symantec/Symantec: File ...	AntiVirus Software	No	Severity	Default Email
Symantec/Symantec: No ...	AntiVirus Software	No	Severity	Default Email
Symantec/Symantec: Thr...	AntiVirus Software	No	Severity	Default Email
Trend Micro/TrendMicro: ...	AntiVirus Software	No	Severity	Default Email
Trend Micro/TrendMicro: ...	AntiVirus Software	No	Severity	Default Email
Event 4656	Common 2008-2016 Audit...	No	Severity	Default Email
Event 4656 WinSXS	Common 2008-2016 Audit...	No	Severity	Default Email
Event 4673-4674	Common 2008-2016 Audit...	No	Severity	Default Email

Die Liste enthält nun alle Filter, und nicht übereinstimmende Filter zeigen an, warum sie nicht mit dem übergebenen Ereignis übereinstimmten. Beispielsweise stimmten die meisten Ausschlussfilter im obigen Screenshot nicht mit dem Ereignis überein, weil der im Filter gewählte Schweregrad nicht mit dem Ereignisschweregrad übereinstimmte.

Sie können auf einen Filter in der Liste doppelklicken, um die Filterdetails zu finden und zu bearbeiten.

3.7 Wizards

Beginnend mit Version 2.72 enthält die Verwaltungskonsole jetzt einen Assistenten, der neuen Benutzern hilft, allgemeine Aufgaben leichter zu erledigen und das Konzept der EventSentryschnelleren Verständlichkeit zu verstehen.

Auf die Assistenten kann über die Menüoption **Assistenten** zugegriffen werden, und die folgenden Assistenten sind derzeit verfügbar.

Einrichtung eines Ereignisprotokoll-Filters

Dieser Assistent führt Sie durch die Erstellung eines Basisfilters und unterstützt auch die folgenden erweiterten Eigenschaften:

- Tag/Zeit-Beschränkungen
- Zusammenfassung Filter
- Filter für wiederkehrende Ereignisse

Da der Assistent für die Einrichtung des Ereignisprotokollfilters hauptsächlich von neuen Benutzern verwendet werden soll, werden erweiterte Filteroptionen wie Schwellenwerte, Zeitgeber und benutzerdefinierte Ereignisprotokolle vom Assistenten für die Einrichtung des Ereignisprotokollfilters nicht unterstützt und müssen direkt am Filter konfiguriert werden.

Datenbank-Konsolidierung

Der Assistent für die Datenbankkonsolidierung führt Sie durch den Prozess der Einrichtung der Datenbankkonsolidierung, falls er nicht schon während des Installationsprozesses eingerichtet wurde. Dieser Assistent erstellt eine Aktion (er initialisiert jedoch nicht die Datenbank, sondern gibt Anweisungen), ermöglicht es Ihnen, die Arten von Ereignissen festzulegen, die Sie für die Konsolidierung planen, und gibt Ihnen die Möglichkeit, Systemzustands- und/oder Tracking-Daten in der Datenbank zu sammeln.

Weitere Assistenten sind für die Zukunft geplant, und Sie sind herzlich eingeladen, uns Vorschläge für neue Assistenten zu schicken. **Bitte beachten Sie auch unsere Tutorials unter http://www.eventsentry.com -> Support.**

3.8 Toolbar (Legacy)

Die Legacy-Symbolleiste wird entweder angezeigt, wenn der Ribbon deaktiviert ist (Tools -> Options -> General) oder wenn die Verwaltungskonsole auf einem Rechner mit Windows XP oder Windows 2003 läuft. Die Symbolleiste ermöglicht es Ihnen, verschiedene Aktionen schnell mit einem Klick auf die Schaltfläche auszuführen, anstatt mit der rechten Maustaste auf Container zu klicken oder durch das Menü zu navigieren.

 Bringt Sie auf den Startbildschirm

 Stellt den Baum im linken Fensterbereich wieder her (aktualisiert)

 Sichert die Konfiguration

 Schneidet die aktuelle Auswahl aus, nur gültig mit Computer-, Filter- und Aktionselementen

 Kopiert die aktuelle Auswahl, nur gültig mit Filter- und Aktionselementen

 Fügt das zuvor kopierte/ausgeschnittene Element ein

 Erlaubt Ihnen, nach Filtern oder Computern zu suchen

 Lädt die neuesten Pakete von www.eventsentry.com herunter.

 Schickt die neueste Konfiguration an alle Computer in allen Gruppen

 Startet die Fern-Aktualisierung, wenn "Use Checkboxes" konfiguriert ist

 Zeigt die Web Reports an, falls konfiguriert

 Öffnet http://www.eventsentry.com in Ihrem Standardbrowser

 Öffnet die EventSentry Willkommens-Assistent

 Navigiert zum EventSentry Knowledge Base

 Öffnet diese Hilfedatei

3.9 Suchen

Manchmal ist es schwierig zu wissen, ob es bereits einen Filter für ein bestimmtes Ereignis gibt, oder herauszufinden, zu welcher Gruppe ein Computer gehört.

Mit dem Finden-Dialog können Sie auf einfache Art und Weise nach Filtern und Computer suchen. Sie können den Suchdialog auf drei Arten erreichen:

- Drücken von CTRL+F
- Wählen Sie **Find** aus dem Menü **Edit**
- Drücken der Schaltfläche **Find** in der Symbolleiste

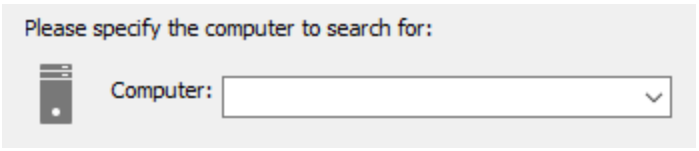
Nachdem das Dialogfeld **Suchen** angezeigt wurde, wählen Sie entweder die Registerkarte **Filter** oder **Computer**.

Filter

Wählen Sie diese Registerkarte, um nach Filtern mit bestimmten Eigenschaften zu suchen, z.B. können Sie alle Filter anzeigen, bei denen die Ereignisquelle auf "NETLOGON" eingestellt ist. Sie können auch alle Filter anzeigen, die einem bestimmten Computer oder einer bestimmten Gruppe zugeordnet sind. Weitere Informationen finden Sie unter Suchen nach Filtern.

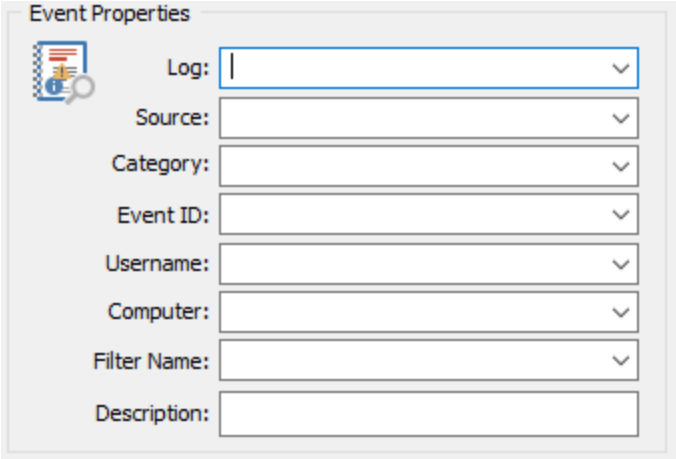
Computer

Wählen Sie diese Registerkarte, um einen Computer in Ihren konfigurierten Gruppen zu finden. Geben Sie einfach den Computernamen in das Feld **Computer** ein und klicken Sie auf **Find**. Der Computer wird in der Baumstruktur ausgewählt, falls er existiert.



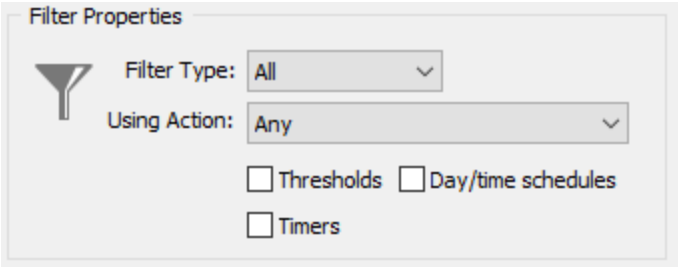
3.9.1 Filter suchen

Wenn Sie eine große Anzahl von Paketen und Filtern haben, kann es schwierig sein, einen Filter unter allen Paketen zu finden. Mit der Suchfunktion können Sie nach Filtern suchen, die auf den meisten Ereigniseigenschaften eines Filters basieren, einschließlich



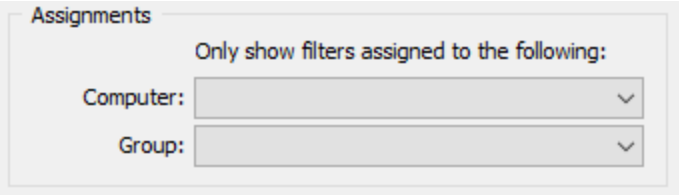
- Protokoll
- Quelle
- Kategorie
- ID
- Benutzername
- Computer
- Name des Filters
- Beschreibung

Sie können auch nach Filtern suchen, die auf allgemeinen Eigenschaften basieren:

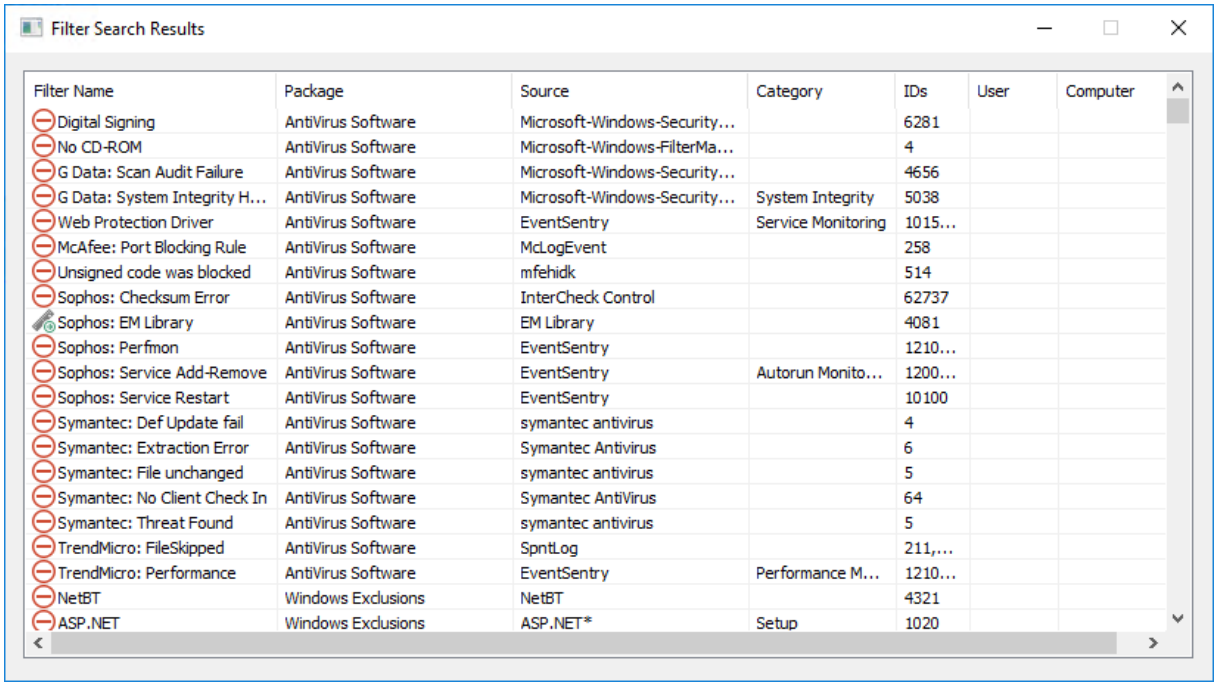


- zugewiesene Aktionen
- Filtertyp (einschließen oder ausschließen)
- Filter mit Schwellenwerten
- Filter mit Zeitplänen
- Filter mit Zeitschaltuhren

Schließlich können Sie nur Filter anzeigen, die einem bestimmten Computer oder einer bestimmten Gruppe zugeordnet sind:



Nachdem Sie die Filtereigenschaften ausgewählt und auf die Schaltfläche **Suchen** geklickt haben, wird eine Liste von Filtern, die Ihren Suchkriterien entsprechen, angezeigt, die Ihnen die gebräuchlichsten Eigenschaften eines Filters anzeigt:



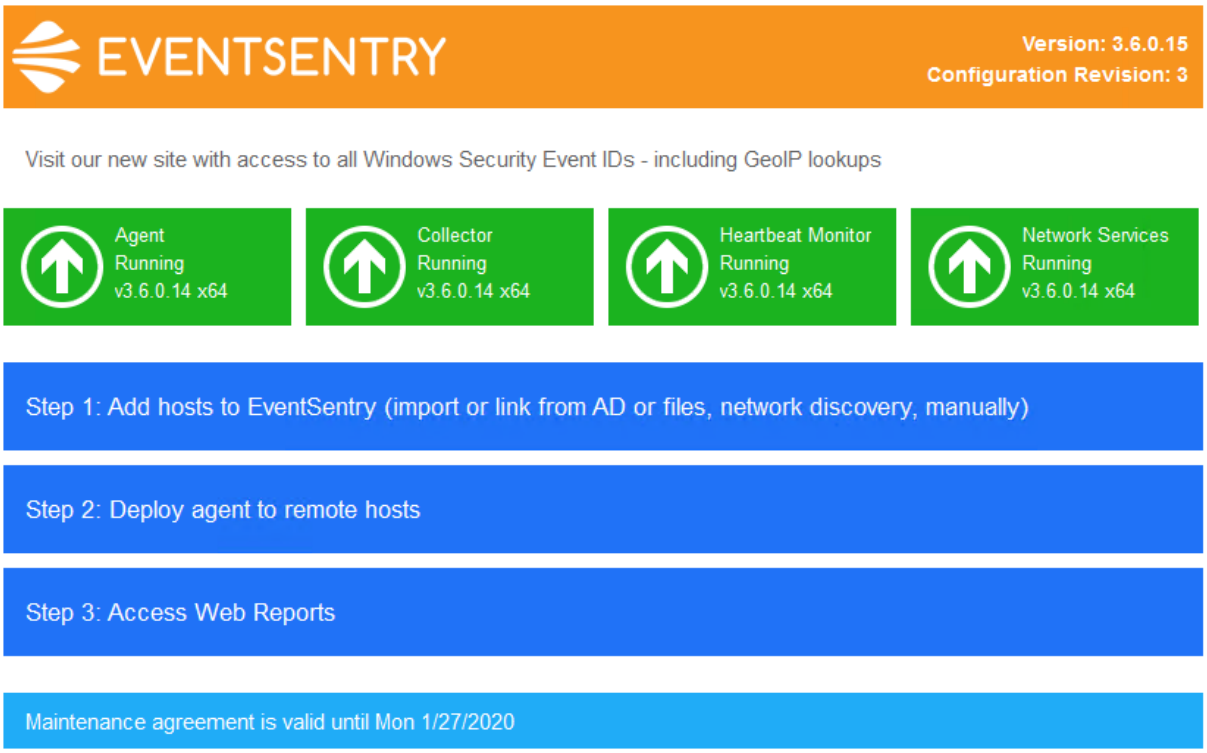
Filter Name	Package	Source	Category	IDs	User	Computer
Digital Signing	AntiVirus Software	Microsoft-Windows-Security...		6281		
No CD-ROM	AntiVirus Software	Microsoft-Windows-FilterMa...		4		
G Data: Scan Audit Failure	AntiVirus Software	Microsoft-Windows-Security...		4656		
G Data: System Integrity H...	AntiVirus Software	Microsoft-Windows-Security...	System Integrity	5038		
Web Protection Driver	AntiVirus Software	EventSentry	Service Monitoring	1015...		
McAfee: Port Blocking Rule	AntiVirus Software	McLogEvent		258		
Unsigned code was blocked	AntiVirus Software	mfehidk		514		
Sophos: Checksum Error	AntiVirus Software	InterCheck Control		62737		
Sophos: EM Library	AntiVirus Software	EM Library		4081		
Sophos: Perfmon	AntiVirus Software	EventSentry		1210...		
Sophos: Service Add-Remove	AntiVirus Software	EventSentry	Autorun Monito...	1200...		
Sophos: Service Restart	AntiVirus Software	EventSentry		10100		
Symantec: Def Update fail	AntiVirus Software	symantec antivirus		4		
Symantec: Extraction Error	AntiVirus Software	Symantec Antivirus		6		
Symantec: File unchanged	AntiVirus Software	symantec antivirus		5		
Symantec: No Client Check In	AntiVirus Software	Symantec AntiVirus		64		
Symantec: Threat Found	AntiVirus Software	symantec antivirus		5		
TrendMicro: FileSkipped	AntiVirus Software	SpntLog		211,...		
TrendMicro: Performance	AntiVirus Software	EventSentry	Performance M...	1210...		
NetBT	Windows Exclusions	NetBT		4321		
ASP.NET	Windows Exclusions	ASP.NET*	Setup	1020		

Um alle Filterdetails anzuzeigen, doppelklicken Sie einfach auf einen Filter aus der Liste, der den Filter im linken Baumfenster lokalisiert und die Filterdetails im rechten Fensterbereich anzeigt.

4 Arbeiten mit EventSentry

4.1 Begrüßungsbildschirm

Der Begrüßungsbildschirm wird im **Detailbereich** angezeigt, nachdem Sie die EventSentry-Verwaltungskonsole gestartet haben. Um den Begrüßungsbildschirm manuell anzuzeigen, klicken Sie auf das Root-Element im Baumverzeichnis links.



Kopfzeile

Oben rechts in der orangefarbenen Kopfzeile wird die Version der Verwaltungskonsole sowie die Konfigurationsrevision angezeigt. Die Konfiguration ist einfach eine inkrementelle Nummer, die bei jedem Speichern der Konfiguration um eins erhöht wird.

Nachrichten

Zeigt das neueste Nachrichten-Update über EventSentry an. Wenn Sie auf den Link klicken, öffnet sich ein Webbrowser und navigiert zu der entsprechenden Webseite.

Dienst-Status

Die grünen Kacheln unter den neuesten Nachrichten zeigen den Status aller installierten Dienste, einschließlich ihrer Version. Sofern nicht eine benutzerdefinierte Binärdatei vom Support herausgegeben wurde, sollten alle Komponenten dieselbe Version ausführen, wie oben gezeigt.

Schritte

Zeigt die empfohlenen Schritte an, die nach der Installation von EventSentry durchzuführen sind.

Wartungsvertrag

Zeigt den aktuellen Status des Wartungsvertrags an, wenn Sie die Vollversion von EventSentry verwenden.

Alle Kacheln sind anklickbar (mit Ausnahme der obersten orangefarbenen Kachel)

4.2 Collector

Der EventSentry Collector, eingeführt in Version 3.2, ermöglicht eine 3-Schichten-Architektur zwischen einer Aktion (z.B. Datenbank, E-Mail-Server) und den EventSentry-Agenten. Wenn er aktiviert ist, bietet der Collector eine Funktionalität ähnlich wie ein Proxy-Server (wenn auch mit wesentlich mehr Funktionalität) und kommuniziert mit einer unterstützenden EventSentry-Aktion im Namen eines Remote-Agenten. Der Collector unterstützt sowohl Komprimierung als auch sichere TLS-Verschlüsselung.

Der Collector kann während der Installation aktiviert werden (Standardverhalten) oder nach einer Installation oder einem Upgrade konfiguriert werden. Eine Aktion wird unter den folgenden Umständen über einen Collector geleitet:

- Ein Collector wird in den "Collector"-Einstellungen konfiguriert (und ausgeführt)
- Die Aktion kann durch einen Collector geleitet (siehe "Unterstützte Aktionen") und für die Verwendung eines Collectors konfiguriert werden

Es ist möglich und wird unterstützt, nur einige Aktionen über einen Collector zu leiten, andere Aktionen jedoch für eine direkte Kommunikation (zwischen Agent und Aktion) zu konfigurieren.

Unterstützte Plattformen

Der Collector ist als 64-Bit (x64) und 32-Bit (x86) Binärdatei verfügbar. Die 64-Bit-Binärdatei wird empfohlen und standardmäßig auf 64-Bit-Betriebssystemen installiert.

Unterstützte Aktionen

Die folgenden Aktionen können über einen Collector geleitet werden:

- Datenbank
- E-Mail (SMTP)
- Syslog
- Datei

Alle anderen Aktionen kommunizieren entweder direkt mit der entfernten Aktion (z.B. HTTP-Aktion) oder werden lokal ausgeführt (z.B. Prozess-Aktion).

Unterstützte Komponenten

Die folgenden Komponenten können derzeit den Collector nutzen, alle anderen Komponenten kommunizieren weiterhin direkt mit ihren jeweiligen Aktionen:

- Agents
- Heartbeat Service
- Network Services

Vorteile

Die Verwendung des Collectors bietet folgenden Vorteile:

1. Die Kommunikation zwischen den Agenten und dem Collector kann für mehr Privatsphäre verschlüsselt werden, was für Hosts, die Daten über ein unsicheres Netzwerk übertragen (z.B. Laptops), nützlich ist.
2. Die Kommunikation zwischen den Agenten und dem Collector kann komprimiert werden, um den Bandbreitenverbrauch zu reduzieren
3. Die Sicherheit kann erhöht werden, indem Aktionen, wie z.B. ein Datenbank- oder E-Mail-Server, so eingeschränkt werden, dass nur der Collector und nicht alle Agenten darauf zugreifen können.
4. Datenbank: Alle Daten werden vom Agenten zwischengespeichert, wenn der Collector vorübergehend nicht verfügbar ist. Nur Ereignisprotokolldaten werden im Cache gespeichert, wenn **kein** Collector verwendet wird, während die Datenbank nicht verfügbar ist.
5. Datenbank: Obwohl automatisch von den EventSentry-Agenten verwaltet, müssen ODBC-Treiber nicht auf den Agenten installiert werden.
6. Datenbank: Die Anmeldedaten für die Datenbank müssen nicht an die Agenten übermittelt werden, da sie nicht direkt mit der Datenbank verbunden sind.
7. Agentenverwaltung: Der Collector kann automatisch Konfigurations- und Agent-Updates an entfernte Agenten übertragen.

Nachteile

In einigen Fällen kann die traditionelle Methode, bei der die Agenten direkt mit einer Aktion kommunizieren, vorzuziehen sein. Der Collector bietet in den folgenden Szenarien wenig Nutzen:

1. Die gesamte Installation erstreckt sich nur über einen einzigen Host
2. Die Agenten haben eine direkte Verbindung mit der Datenbank oder dem E-Mail-Server
3. Daten, die vom Agenten an die Aktion gesendet werden, werden bereits über ein sicheres Netzwerk übertragen
4. Daten, die vom Agenten an die Aktion gesendet werden, werden bereits über ein schnelles Netzwerk übertragen, wo die Komprimierung wenig oder keinen Nutzen bringt
5. Die Aktion (z.B. Datenbank) ist zuverlässig und hat keine oder nur geringe Ausfallzeiten
6. Die Installation und/oder Wartung eines oder mehrerer Collectors ist nicht wünschenswert

Redundanz

Da der Collector ein potenzieller Single Point of Failure (SPOF) ist, bietet EventSentry die folgenden Funktionen, um eine maximale Verfügbarkeit zu gewährleisten:

- Agenten speichern alle Daten in einem persistenten lokalen Cache, wenn sie den Collector nicht erreichen können. Die Daten werden erneut übermittelt, sobald der Collector erreichbar ist.
- Der Collector speichert alle Daten im Cache, wenn er eine Aktion (z.B. Datenbank, E-Mail-Server) nicht im Speicher erreichen kann, und wird auf die Festplatte gespült, wenn der Collectordienst beendet wird. Zwischengespeicherte Daten werden in temporäre Dateien ausgelagert, wenn der In-Memory-Cache (auch als Warteschlange bezeichnet) entweder eine harte Grenze überschreitet oder aufgrund früherer Nutzung ungewöhnlich hoch ist.
- Der Collector protokolliert Ereignis ID 210, wenn das Auslagern beginnt, gefolgt von Ereignis 214, wenn das Auslagern deaktiviert wird. Der Collector benötigt mindestens 500 MB freien Speicherplatz auf dem Laufwerk %SYSTEMROOT%, um das Paging auf der Festplatte zu unterstützen.
- Mehrere Collectors können für zusätzliche Redundanz konfiguriert werden.

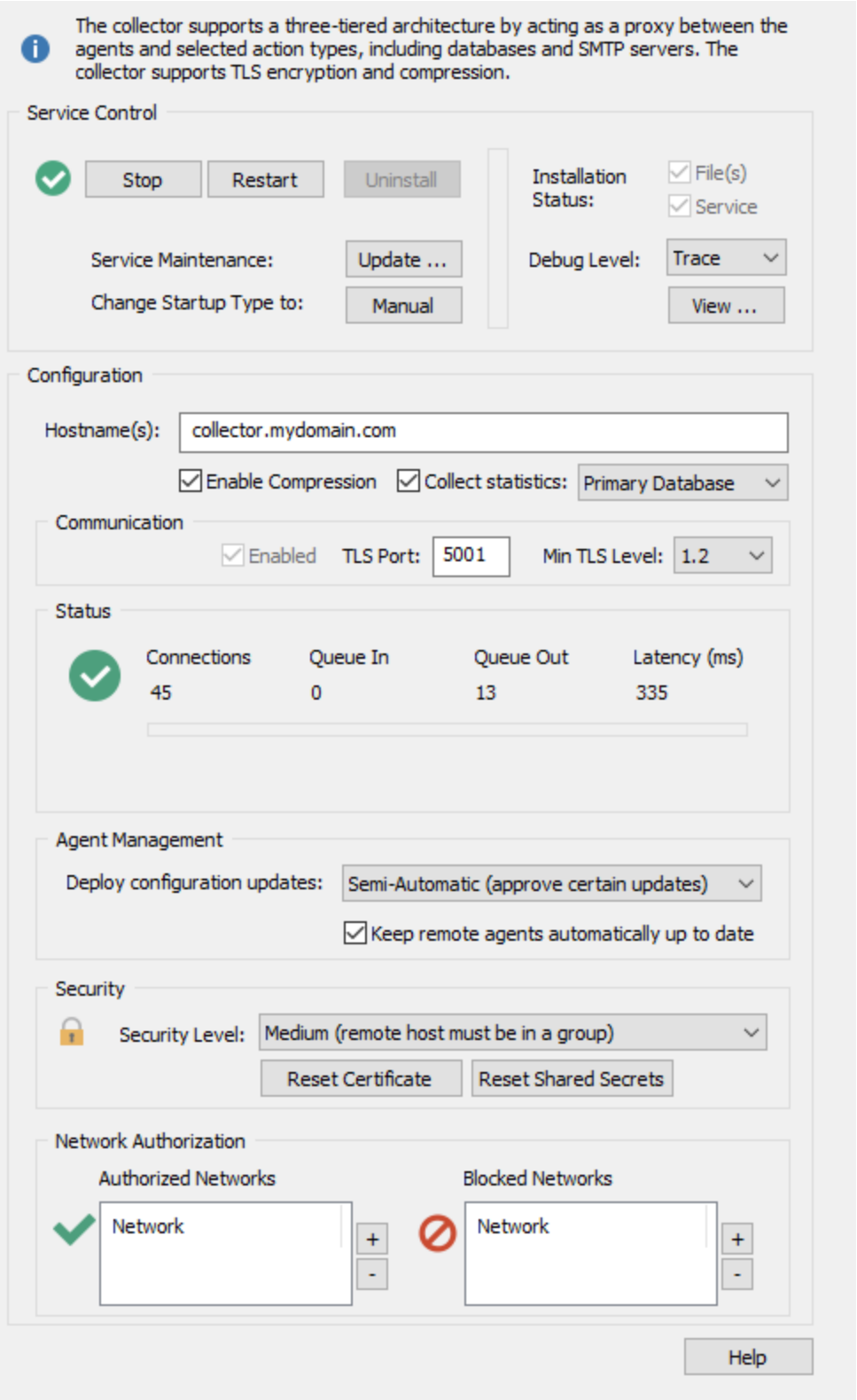
Leistung

Der Collectordienst ist so konzipiert, dass er sowohl eine große Anzahl von Kunden als auch große Datenmengen in Echtzeit unterstützt. Für Datenbankaktionen verwendet der Collector mehrere (~20)

gleichzeitige DB-Verbindungen, um einen hohen Durchsatz zu gewährleisten. Der aktuelle Status des Collectors kann in den Web Reports unter dem Menüabschnitt Werkzeuge/Wartung ("Collector Status") eingesehen werden, wenn "Collect Statistics" aktiviert ist.

4.2.1 Konfiguration

Die Konfiguration des Collectors erfolgt über die Schaltfläche "Collector" im Navigationsbaum und Ribbon ("Home -> Allgemein") der Verwaltungskonsole. Das Collectorsymbol in der Baumansicht wird farbig angezeigt, wenn der Collectordienst ("EventSentryCollector") ausgeführt wird, oder grau, wenn der Collector entweder nicht installiert ist oder nicht ausgeführt wird.



Hostname
Gibt den Host-Namen an, mit dem sich die Remote-Agenten verbinden werden. Dies sollte entweder ein Host-Name sein, der von allen Hosts aufgelöst werden kann, oder eine IP-Adresse. Wenn der Collector

sowohl vom internen LAN als auch von Remote-Clients, die sich durch eine Firewall verbinden, kontaktiert werden soll, kann Split DNS konfiguriert werden.

Mehrere Collectors können mit einem Komma getrennt werden, siehe "Mehrere Collectors" für weitere Informationen.

Komprimierung aktivieren
Komprimiert alle Daten, bevor sie an den Collector übertragen werden, wodurch der gesamte Bandbreitenverbrauch des Agenten reduziert wird. Der Komprimierungsfaktor hängt von den gesammelten Daten ab und liegt in der Regel zwischen 15 und 25% (wodurch die Menge der übertragenen Daten um etwa 20% reduziert wird). Die Aktivierung der Komprimierung wird in den meisten Fällen empfohlen und ist standardmäßig aktiviert.

Sammeln von Statistiken
Sammelt die folgenden grundlegenden Leistungsstatistiken in der Datenbank, siehe Collectorstatus für weitere Informationen.

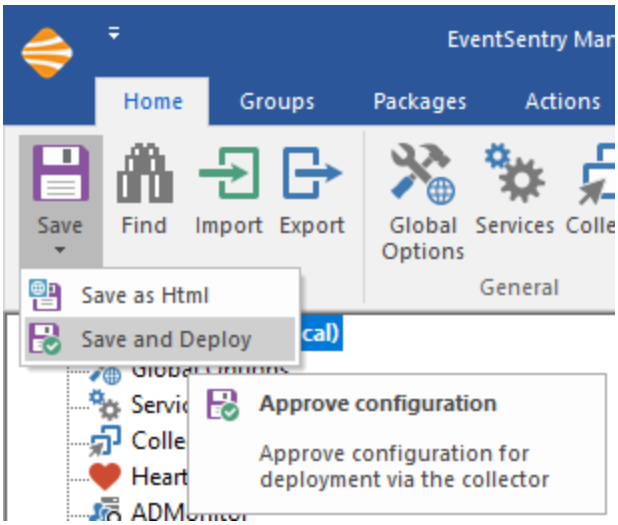
Aktivieren der Cleartext-Kommunikation
Übermittelt alle Daten, einschließlich der Protokollinhalte, im Klartext über den ausgewählten TCP-Port. Die Daten werden kodiert, aber nicht verschlüsselt. Eine Kommunikation im Klartext ist nicht empfohlen.

Verschlüsselte Kommunikation aktivieren
Übermittelt alle gesammelten Daten über einen sicheren TLS-Kanal. Verschlüsselte Kommunikation wird bevorzugt, wenn sowohl Klartext als auch Verschlüsselung aktiviert sind.

Konfigurationsaktualisierungen bereitstellen
Anstatt Konfigurationsaktualisierungen manuell von der Verwaltungskonsole mit Remote-Update zu pushen, kann der Collector Konfigurationsaktualisierungen automatisch an alle verbundenen Agenten senden. Dies ist besonders nützlich für Clients, die nicht permanent mit dem Netzwerk verbunden sind, in dem sich die Verwaltungskonsole befindet, z.B. Laptops.

Automatisch
Jedes Mal, wenn die Konfiguration in der Verwaltungskonsole gespeichert wird, verteilt der Collector sie automatisch an alle verbundenen Remote-Agenten.

Semi-Automatisch
Verteilt eine aktualisierte Konfiguration nur dann automatisch, wenn die Konfiguration mit der Option "Save and Deploy" gespeichert wird. Durch einfaches Klicken auf die Schaltfläche "Speichern" wird die Konfiguration lokal gespeichert, aber nicht netzwerkweit verteilt.



Wenn eine Konfigurationsaktualisierung genehmigt wird, entweder manuell oder automatisch, kann es mehrere Minuten dauern bis der Agent die neue Konfiguration geladen hat.

Agenten, die auf Hosts laufen, auf denen EventSentry mit dem Setup installiert wurde (betrifft normalerweise nur einen Host), akzeptiert keine Fernkonfigurationsaktualisierungen und lädt stattdessen die Konfiguration direkt aus der Registrierung.

Remote-Agenten auf dem neuesten Stand halten
Anstatt Remote-Agenten jedes Mal manuell zu aktualisieren, wenn ein Patch oder ein Versions-Update installiert wird, kann der Collector einen aktualisierten Agenten an alle verbundenen Hosts pushen. Sobald der Remote-Agent eine aktualisierte Agenten-Binärdatei empfängt, wird er automatisch aktualisiert und neu gestartet. Diese Funktion funktioniert nur für Agenten mit v3.3.x oder höher.

Es kann bis zu 10 Minuten dauern, bis ein Agenten-Update vom Collector gesendet wird, wenn ein Remote-Agent mit einem veralteten Agenten erkannt wird.

Agentenverwaltungsfunktionen funktionieren nur über sichere Verbindungen.

Weitere Informationen finden Sie unter Collector-Sicherheitskonfiguration.

4.2.1.1 Sicherheit

Der Collector ist so konzipiert, dass er eine sichere und zuverlässige Datenübertragung zwischen den EventSentry Agenten und den Collector. Die meisten der unten aufgeführten Sicherheitseinstellungen gelten nur, wenn die TLS-Kommunikation aktiviert ist.

TLS-Verschlüsselung
Zertifikate für die TLS-Kommunikation werden automatisch vom Collector erstellt, wenn der Dienst zum ersten Mal gestartet wird. Zertifikate werden mit einer Bitlänge von 2048 Bit (1024 Bit auf Windows Server 2003) unter Verwendung von SHA256 als Signaturalgorithmus erstellt.

Chiffren

Der/die Agent(en) und der Collector handeln auf beiden Hosts die sicherste verfügbare Chiffre aus. Die verwendete Chiffre hängt sowohl vom Betriebssystem als auch von der Schannel-Konfiguration unter Windows ab (sowohl auf dem Client (Agent) als auch auf dem Server (Collector)).

Es wird empfohlen, den Collector möglichst auf der neueren Windows-Version (2012 oder höher) laufen zu lassen, um sicherzustellen, dass die sichersten Chiffren zur Verfügung stehen.

Standardmäßige Sicherheitsfunktionen

Die folgenden Sicherheitsfunktionen sind immer aktiviert, unabhängig von der unten gewählten Sicherheitsstufe.

Shared Secret

Wenn ein EventSentry Agent sich zum ersten Mal mit einem Collector verbindet, generiert er eine eindeutige ID sowie ein gemeinsames Passwort, das er über einen verschlüsselten TLS-Kanal an den Collector sendet. Der Collector speichert dann das gemeinsame Geheimnis lokal und ordnet es der eindeutigen ID des entfernten Hosts zu. Sobald das "shared secret" mit dem entfernten Host assoziiert ist, werden nur noch Verbindungsversuche akzeptiert, die mit dem lokal gespeicherten gemeinsamen Geheimnis übereinstimmen. Dadurch wird sichergestellt, dass ein entfernter Host nicht imitiert werden kann.

Zertifikatsvalidierung (Agenten)

Wenn ein Agent zum ersten Mal eine Verbindung zu einem Collector herstellt, lädt er das Zertifikat des Remote-Hosts herunter und speichert es lokal im Cache. Bei allen zukünftigen Verbindungsversuchen mit demselben Collector wird das vom Collector vorgelegte Zertifikat mit dem lokal zwischengespeicherten Zertifikat verglichen. Die Verbindung wird vom Agenten abgebrochen, wenn die Zertifikate nicht übereinstimmen.

Sicherheitsebenen

Der Collector unterstützt 3 verschiedene Sicherheitsstufen sowie Zugriffslisten auf IP-Ebene, um sicherzustellen, dass sich nur autorisierte Hosts mit dem Collector verbinden können. Die Sicherheitsstufen sind kumulativ: Eine **mittlere** Sicherheitsstufe erfordert, dass Prüfungen von der Basissicherheitsstufe durchlaufen werden, eine **hohe** Sicherheitsstufe erfordert, dass Prüfungen sowohl von der Basis- als auch von der mittleren Sicherheitsstufe durchlaufen werden.

Netzwerkbasierte Berechtigungen (autorisierte und gesperrte Netzwerke) werden immer ausgewertet, bevor eine weitere Prüfung auf Basis der Sicherheitsstufe durchgeführt wird.

Grundlegend

Ermöglicht jedem EventSentry-Agenten mit einer gültigen gemeinsamen geheimen Verbindung.

Medium

Der Remote-Hostname (der vom Agenten in einer Autorisierung gesendet wird, die auf dem Hostnamen des Agenten basiert) muss sich in einer EventSentry-Gruppe befinden, damit eine Verbindung hergestellt werden kann.

Hoch

Ein Reverse-IP-Lookup des verbindenden Hosts muss zu einem Host in einer Gruppe aufgelöst werden. Wenn z. B. ein Host mit der IP-Adresse 192.168.1.50 eine Verbindung herstellt, versucht der Collector,

eine umgekehrte IP-Abfrage durchzuführen und dann den resultierenden Hostnamen in einer Gruppe zu finden.

Zertifikat zurücksetzen
Das Zurücksetzen des Collectorzertifikats ist nur unter den folgenden Umständen erforderlich:

- Das Zertifikat wurde kompromittiert und muss ersetzt werden
- Das Zertifikat muss durch ein anderes Zertifikat ersetzt werden
- Die entfernten Hosts haben ein anderes Zertifikat für den Collector-Host zwischengespeichert und lehnen den Collector ab

Beim Zurücksetzen des Zertifikats werden die folgenden Aktionen durchgeführt:

1. Das bestehende Zertifikat wird umbenannt (um das Zertifikat zu erhalten)
2. Wenn der EventSentry Collector neu gestartet wird, wird ein neues Zertifikat erstellt
3. Remote-Agenten werden bis zu 1 Woche lang befugt sein, ein neues Zertifikat zu akzeptieren.

Nach dem Klicken auf die Schaltfläche "Zertifikat zurücksetzen" müssen die folgenden Aktionen durchgeführt werden:

1. Die Konfiguration muss an alle entfernten Hosts übertragen werden
2. Der EventSentry Collector-Dienst muss neu gestartet werden

"Shared Secret" zurücksetzen
Das Zurücksetzen gemeinsam genutzter Geheimnisse ist nur dann erforderlich, wenn ein entfernter EventSentry-Agent neu installiert wird, ohne zuvor aus der Konfiguration entfernt worden zu sein. Durch Klicken auf die Schaltfläche "Reset Shared Secrets" wird die gesamte lokale Datenbank mit gemeinsam genutzten Geheimnissen gelöscht und neue gemeinsam genutzte Geheimnisse von allen entfernten Hosts akzeptiert, so als ob sie sich zum ersten Mal verbinden würden.

Netzwerk-Autorisierung
Autorisierte und gesperrte Netzwerke können für beide angegeben werden:

- nur bestimmten Hosts oder Subnetzen Zugang gewähren
- bestimmte Hosts oder Subnetze blockieren
- beides

Autorisierte Netzwerke
Gibt alle autorisierten Netzwerke an. Autorisiert alle Subnetze/Hosts, wenn leer. Blockierte Netzwerke haben Vorrang vor autorisierten Netzwerken.

Blockierte Netzwerke
Gibt alle Subnetze/Hosts an, die keine Verbindung herstellen dürfen. Blockierte Hosts haben immer Vorrang vor autorisierten Hosts.

4.2.2 Mehrere Collector

Trotz der im Collector und in den Agenten vorhandenen Redundanzfunktion kann es aus folgenden Gründen vorteilhaft sein, mehr als einen Collector einzurichten:

- Die Ressourcenauslastung des Hosts, auf dem der Kollektor läuft, ist zu hoch
- Isolierung zwischen Hosts ist erwünscht
- Kollektoren sind aufgeteilt und mit verschiedenen Datenbanken verbunden

- Ein längerer/regelmäßiger Ausfall des primären Kollektors ist geplant oder zu erwarten.

Die folgenden Schritte beschreiben, wie Sie einen zusätzlichen Collector einrichten und konfigurieren.

1. Bestimmen eines Hosts
Wählen Sie einen Host, der über genügend Speicher- und CPU-Ressourcen verfügt, um den Collectordienst auszuführen. Windows 2012 und höher wird bevorzugt, da es eine bessere Sicherheit bietet, wenn sich moderne Clients verbinden. Ein Host mit einer schnellen Verbindung zur Back-End-EventSentry-Datenbank sollte bevorzugt werden.

2. Konfigurieren von EventSentry
Öffnen Sie auf dem Host, auf dem EventSentry installiert ist, die Verwaltungskonsole und klicken Sie auf das Symbol "Collector". Fügen Sie im Feld "Hostname(n)" ein Komma und den Hostnamen des neuen Collectors an, z. B.

esmain.yourcompany.com,esbackup.yourcompany.com

3. Erhöhte Sicherheit
Wenn eine oder mehrere Datenbankaktionen, die vom Collector verwendet werden sollen, für erhöhte Sicherheit konfiguriert sind, muss der für den Backup-Collector vorgesehene Host als vertrauenswürdiger Host konfiguriert werden.

4. Push-Konfiguration/Bereitstellungsagent
Wenn auf dem Host, der für den Backup-Collector bestimmt ist, bereits ein EventSentry-Agent ausgeführt wird, drücken Sie einfach die Konfiguration, andernfalls stellen Sie einen Agenten mit Fernaktualisierung bereit. Dies ist erforderlich.

5. Erforderliche Dateien kopieren
Kopieren Sie aus dem EventSentry-Installationsverzeichnis (normalerweise C:\Programme\EventSentry) die folgenden Dateien (und/oder Verzeichnisse) in ein beliebiges temporäres Verzeichnis auf dem Remote-Host. Zu diesem Zweck verwenden wir das Verzeichnis **C:\EventSentry**.

64-bit
- eventsentry_gui_x64.exe
- es_collector_svc_x64.exe
- Qt5Core.dll
- concrt140.dll
- msvcp140.dll
- vccorlib140.dll
- vcruntime140.dll

Beispiel: Sie sollten die Datei C:\EventSentry\x64\Qt5Core.dll haben.

6. Registrierung und Installation des Collector-Dienstes
Starten Sie die Verwaltungskonsole (eventsentry_gui[_x64].exe) und navigieren Sie zum Collector-Dialogfeld. Das Hostnamenfeld sollte die in Schritt (2) eingegebenen korrekten Informationen enthalten. Falls nicht, versuchen Sie, die Konfiguration erneut zu verschieben und optional den EventSentry-Agentendienst neu zu starten.

Klicken Sie dann auf die Schaltfläche "Installieren" und zeigen Sie auf das temporäre Verzeichnis.

7. Anpassen

Es wird nicht empfohlen, die "Kommunikations"-Einstellungen des Collectors zu ändern, da sie mit den Einstellungen des primären Collectors übereinstimmen sollten. Die "Netzwerkautorisierung"-Einstellungen können auf einem Backup-Collector angepasst werden, wenn nur ausgewählten Subnetzen der Zugriff gestattet werden soll.

8. Aktivierung
Der Backup-Collector wird aktiviert, indem der Dienst mit der Schaltfläche "Start" gestartet wird. Die Konfiguration muss auch von dem Host, auf dem EventSentry installiert ist (nicht vom Backup-Collector), an alle Remote-Hosts übertragen werden, damit die Remote-Hosts den Backup-Collector kennen.

9. Wartung
Die vom Collector verwendete Binärdatei, **es_collector_svc.exe** bzw. **es_collector_svc_x64.exe**, muss auf jedem aufgeführten Backup-Collector manuell aktualisiert werden, wenn ein Patch oder eine neue Version von EventSentry installiert wird. Beenden Sie einfach den EventSentryCollector-Dienst auf einem Backup-Collector, ersetzen Sie die Binärdatei durch die neueste Version aus dem Installationsverzeichnis und starten Sie den EventSentryCollector-Dienst neu.

Wenn mehrere Collectors konfiguriert sind, versucht ein Agent immer nacheinander, eine Verbindung zu den aufgelisteten Collectors herzustellen, beginnend mit dem ersten aufgelisteten Host. Wenn eine Verbindung mit einem Backup-Collector hergestellt wird, kommuniziert der Agent weiterhin mit diesem Collector, bis die Verbindung unterbrochen oder der Agent neu gestartet wird.

4.3 Pakete

EventSentry ermöglicht Ihnen die Konfiguration von Filter-, Gesundheits-, Sicherheits- und Compliance- sowie Validierungsskripten-Paketen. Ein Paket enthält eine Reihe von Anweisungen (z.B. Ereignisprotokollfilter, Speicherplatzeinstellungen, Einstellungen für die Dienstüberwachung usw.), die dann angewendet werden können auf

- Alle Computer
- Computer in einer bestimmten Gruppe
- Computer, die bestimmten Kriterien entsprechen (Betriebssystem, Plattform, Betrieb eines Dienstes)
- Nur einzelne Computer

Weitere Informationen zu Paketen finden Sie unter Paketoptionen.

Paket-Typen
EventSentry wird mit 5 verschiedenen Pakettypen geliefert:

1.  **Ereignisprotokoll-Pakete**
   Enthalten einen oder mehrere Include-Filter, Exclude-Filter und Ordner. Weitere Informationen finden Sie unter "Ereignisprotokoll-Überwachung".

2.  **Log-Datei-Pakete**
   Enthalten Optionen zum Überwachen einer oder mehrerer Dateien und zum Konsolidieren und/oder Protokollieren von geparstem Text im Ereignisprotokoll.

3.  **System Health-Pakete**

System Health Pakete können die folgenden Objekte enthalten:

- Dienst Überwachung
- Festplattenspeicher-Überwachung
- Ordner-Überwachung
- Leistungsüberwachung
- Software/Hardware-Bestandsaufnahme
- Prozessüberwachung
- Anwendungs-Scheduler
- Sicherung des Ereignisprotokolls
- Datei-Überwachung
- Aufgabenplanung
- NTP
- System Status Tray App

Bitte beachten Sie, dass ein Gesundheitspaket nur maximal ein Objekt jedes Typs enthalten darf, z. B. können Sie nicht zwei Dienstüberwachungsobjekte zu demselben Gesundheitspaket hinzufügen.

4.  **Sicherheits- und Compliance-Pakete**
Sicherheits- und Compliance-Pakete können die folgenden Objekte enthalten:

- Prozesse
- Konsolen-Anmeldungen
- Netzwerk-Anmeldungen
- Kontoführung
- Dateizugriff
- Änderungen von Richtlinien (Policy Changes)
- Druckaktivität

Bitte beachten Sie, dass ein Tracking-Paket nur maximal ein Objekt jedes Typs enthalten darf, z.B. können Sie nicht zwei Prozess Objekte zum gleichen Paket hinzufügen.

5.  **Pakete mit Validierungsskripten**
Enthält ein Skript-Objekt, das die Planung eines oder mehrerer Validierungsskripte entweder nach Tag oder Namen ermöglicht.

4.3.1 Paket-Optionen

Jedes Paket, egal um welchen Typ es sich handelt, enthält die folgenden Konfigurationsoptionen.

Sie können Paketoptionen anzeigen und bearbeiten, indem Sie entweder **mit der rechten Maustaste auf ein Paket klicken** und "**Bearbeiten**" wählen oder indem Sie mit der linken Maustaste auf ein Paket klicken und auf "**Paketoptionen bearbeiten**" auf dem rechten Bildschirm klicken.

 **Aktiviertes Paket**
Sie können Pakete aktivieren/deaktivieren, um alle in ihnen enthaltenen Überwachungsoptionen zu aktivieren oder zu deaktivieren. Deaktivierte Pakete werden mit einem roten x im Baum angezeigt.

 **Globales Paket**

Anstatt ein Paket allen Gruppen oder Computern zuzuweisen, können Sie ein Paket global machen. Globale Pakete gelten für alle Computer, unabhängig von ihrer Gruppenzugehörigkeit. Sobald ein Paket globalisiert wurde, kann es nicht mehr Gruppen oder Computern zugeordnet werden.

Paket für Filterverkettung

Gibt ein Paket an, das für die Filterverkettung konfiguriert ist.

Beschreibung

Geben Sie eine Beschreibung für ein Paket ein, um das Paket, seinen Inhalt und/oder seinen Zweck kurz zu beschreiben.

Paket-Zuordnungen

Sie können ein Paket entweder einem Computer oder Gruppen zuweisen oder ein Paket so konfigurieren, dass es global ist und somit für jeden Computer in Ihrer Konfiguration gilt. Markieren Sie das Kontrollkästchen "Globales Paket", um ein Paket global zu machen, oder klicken Sie auf die Schaltfläche "Zuweisen", um dieses Paket einem oder mehreren Computern zuzuweisen.

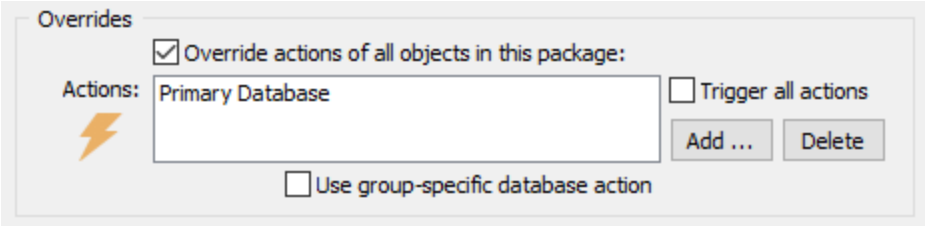
Sie können auch mit der rechten Maustaste auf ein Paket klicken, um die Paketzuordnungen zu konfigurieren.

Übersteuert

Viele Funktionen in EventSentry sind an eine bestimmte Aktion gebunden. Anstatt jeden Filter, Gesundheitszustand oder jede Verfolgungsfunktion für die Verwendung einer bestimmten Aktion zu konfigurieren, können Sie die Benachrichtigung stattdessen auf Paketebene einstellen. Wenn Sie eine Benachrichtigung auf Paketebene festlegen, können Sie die Aktion(en) für die einzelnen Elemente innerhalb des Pakets nicht festlegen.

Um Aktionen auf Paketebene festzulegen, markieren Sie das Kontrollkästchen "Aktionen aller Objekte in diesem Paket überschreiben" und füllen Sie die Liste "Aktionen" aus. Bitte beachten Sie, dass nur Ereignisprotokollpakete mehr als eine Aktion enthalten dürfen, Health- und Security/Compliance-Pakete dürfen nur eine Aktion in der Liste haben.

Gruppenspezifische Datenbankaktion verwenden: Wenn in den Gruppeneigenschaften konfiguriert, wird diese Datenbank dynamisch zur Liste der Aktionen **hinzugefügt**. Die Liste der Aktionen sollte leer sein, wenn nur die gruppenspezifische Aktion für das Paket verwendet werden soll.



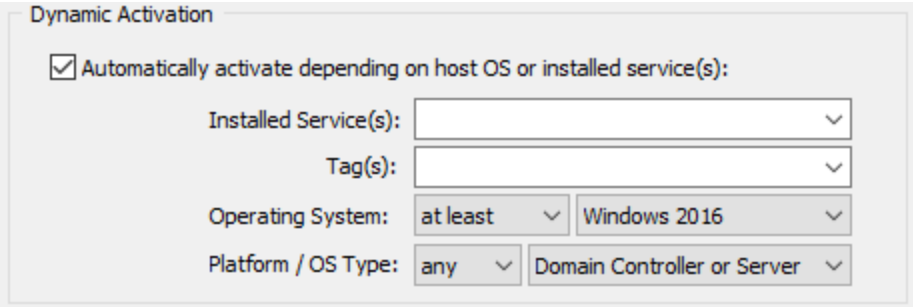
Ereignisprotokollpakete bieten weitere Paketoptionen, die im Kapitel Ereignisprotokollpakete erläutert werden.

Pakete, die für die dynamische Aktivierung konfiguriert wurden, müssen weiterhin Gruppen oder Computern zugewiesen werden, **nicht zugewiesene Pakete werden nicht aktiviert.**

Dynamische Aktivierung

Sie können ein Paket von der Existenz eines bestimmten Windows-Dienstes oder der installierten Version von Windows abhängig machen. Beispielsweise können Sie ein Paket nur aktivieren, wenn der "mysql"-Dienst installiert ist, oder auf Computern mit Windows Server 2008 oder höher. Es ist wichtig zu beachten, dass die dynamische Aktivierung **keine Pakete zuordnet**, so dass die dynamische Aktivierung immer noch die Zuordnung des Pakets erfordert. Im Allgemeinen wird empfohlen, Pakete, die die dynamische Aktivierung verwenden, global zu machen.

Alle Bedingungen müssen erfüllt sein (in einer UND-ähnlichen Weise), wenn mehrere Bedingungen konfiguriert sind (z.B. Betriebssystem und Plattform).



Aktivieren auf Basis des installierten Dienstes

Um ein Paket nur dann zu aktivieren, wenn ein oder mehrere Dienste installiert sind, geben Sie die **Namen der Dienstschlüssel** in das Feld "Installierte(r) Dienst(e)" ein. Trennen Sie mehrere Dienstschlüsselnamen durch ein Komma. Wenn mehrere Dienste aufgeführt sind, reicht es aus, wenn nur einer der aufgeführten Dienste installiert ist.

> Geben Sie immer den **Dienstschlüsselnamen** an, nicht den Anzeigenamen des Dienstes.

Aktivieren basierend auf einem zugewiesenen Tag

Pakete können auf Hosts aktiviert werden, denen ein bestimmtes Tag zugewiesen ist (entweder direkt oder implizit durch die Gruppe); trennen Sie mehrere Tags durch ein Komma. Wenn mehrere Tags aufgelistet sind, reicht es aus, wenn auf einem Ziel-Host nur eines der aufgelisteten Tags zugewiesen ist.

Aktivieren auf der Grundlage des Betriebssystems

Um ein Paket nur für ein bestimmtes Betriebssystem oder einen Bereich von Betriebssystemen zu aktivieren, wählen Sie den Vergleichstyp (maximal, gleich, mindestens) sowie ein Betriebssystem aus. Wenn Sie z.B. "mindestens Windows Vista" wählen, dann wird das Paket auf allen Computern aktiviert, auf denen Windows Vista oder später läuft.

Aktivieren auf der Grundlage der Plattform

Um ein Paket nur für eine bestimmte Plattform (z.B. 64-Bit) zu aktivieren, wählen Sie die Plattform aus der Liste aus oder setzen Sie die Option auf "beliebig", damit das Paket auf allen Plattformen aktiviert wird.

Aktivieren basierend auf dem OS-Typ

Ein Paket kann aktiviert werden, je nachdem, ob es sich um einen Domänencontroller, einen Server, eine Workstation (Client) oder eine Kombination handelt.

Sortieren von Paketen

Es spielt keine Rolle, in welcher Reihenfolge sich Ihre Pakete befinden. Die Reihenfolge der Pakete hat keinen Einfluss auf die Funktionalität von EventSentry. Sie können die Pakete jedoch alphabetisch (entweder aufsteigend oder absteigend) sortieren, indem Sie mit der rechten Maustaste auf den jeweiligen Pakettypecontainer klicken und "Pakete sortieren" wählen.

4.3.2 Pakete zuweisen

Pakete müssen zugewiesen werden, bevor sie von einem Computer verwendet werden können. Sie können den folgenden Bereichen zugeordnet werden:

- Alle Computer (= global)
- Eine oder mehrere Gruppen
- Ein oder mehrere Computer

Mit der EventSentry-Verwaltungskonsole können Sie Pakete **entweder durch Rechtsklick auf die eigentlichen Pakete** oder durch **Rechtsklick auf die Gruppen- oder** Computerobjekte zuweisen. Dadurch erhalten Sie mehr Flexibilität beim Konfigurieren und Arbeiten mit Paketen.

Pakete können auch automatisch zugewiesen werden, entweder in Abhängigkeit von einem oder mehreren installierten Dienst(en) oder in Abhängigkeit vom Betriebssystem des überwachten Hosts.

Pakete als global einstellen

Sie können ein Paket als global konfigurieren und auf alle Computer anwenden:

- Klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie "Global".
- Klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie "Bearbeiten", wodurch Sie zu den Paketoptionen gelangen. Aktivieren Sie dort das Kontrollkästchen "Global Package", wodurch das Paketsymbol entsprechend geändert wird.
- Klicken Sie mit der rechten Maustaste auf den Container "Computer Groups" und wählen Sie "Assign Package(s) ...". Von diesem Dialog aus können Sie die "**Global**"-Flagge für mehr als ein Paket auf einmal umschalten.

Klicken Sie hier für weitere Informationen.

Pakete zu Gruppen zuordnen

Klicken Sie hier für weitere Informationen.

Zuweisen von Paketen zu Computern

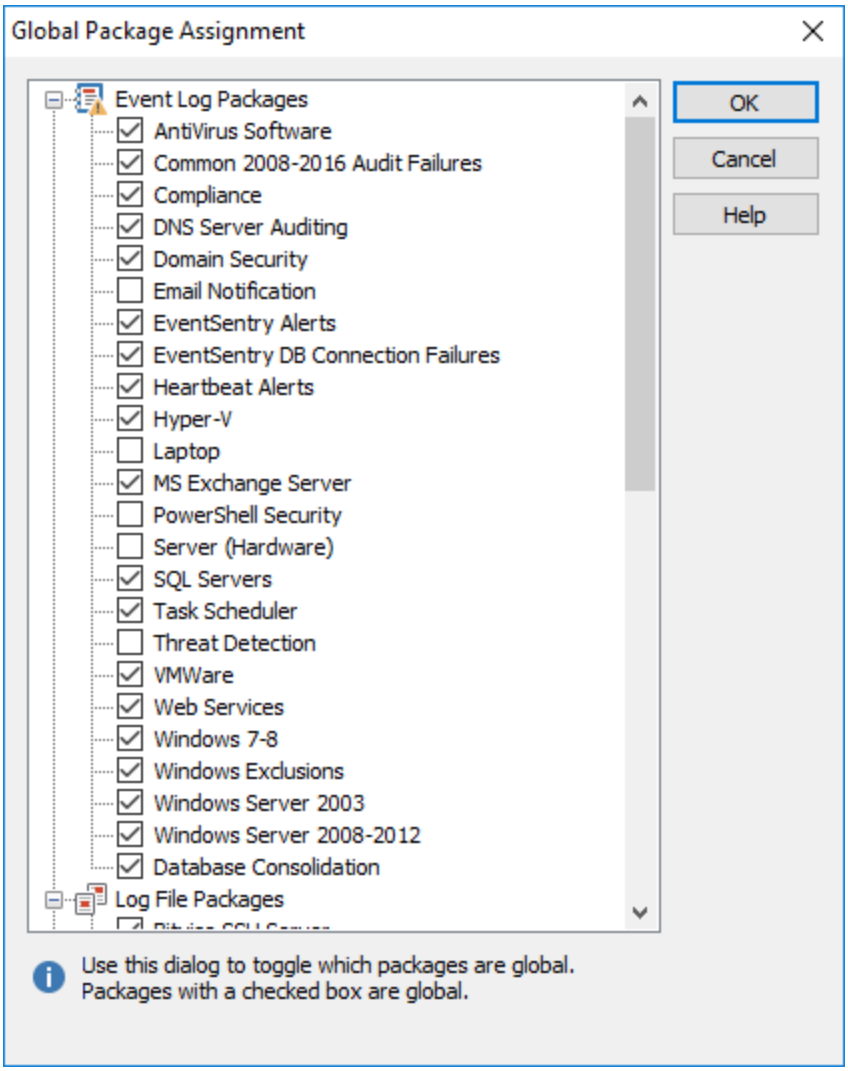
Klicken Sie hier für weitere Informationen.

Nicht zugewiesene Pakete

Nicht zugewiesene Pakete erscheinen in der Paketliste grau und werden vom EventSentry-Agenten nicht geladen.

4.3.2.1 Pakete als global festlegen

Mit dem Dialogfeld "Globale Paketzuordnung" können Sie mehr als ein Paket gleichzeitig zu einem globalen Paket konfigurieren. Wenn Sie mit der rechten Maustaste auf den Container "Computer Groups" klicken und "Assign Package(s)..." wählen, wird das folgende Dialogfeld angezeigt:

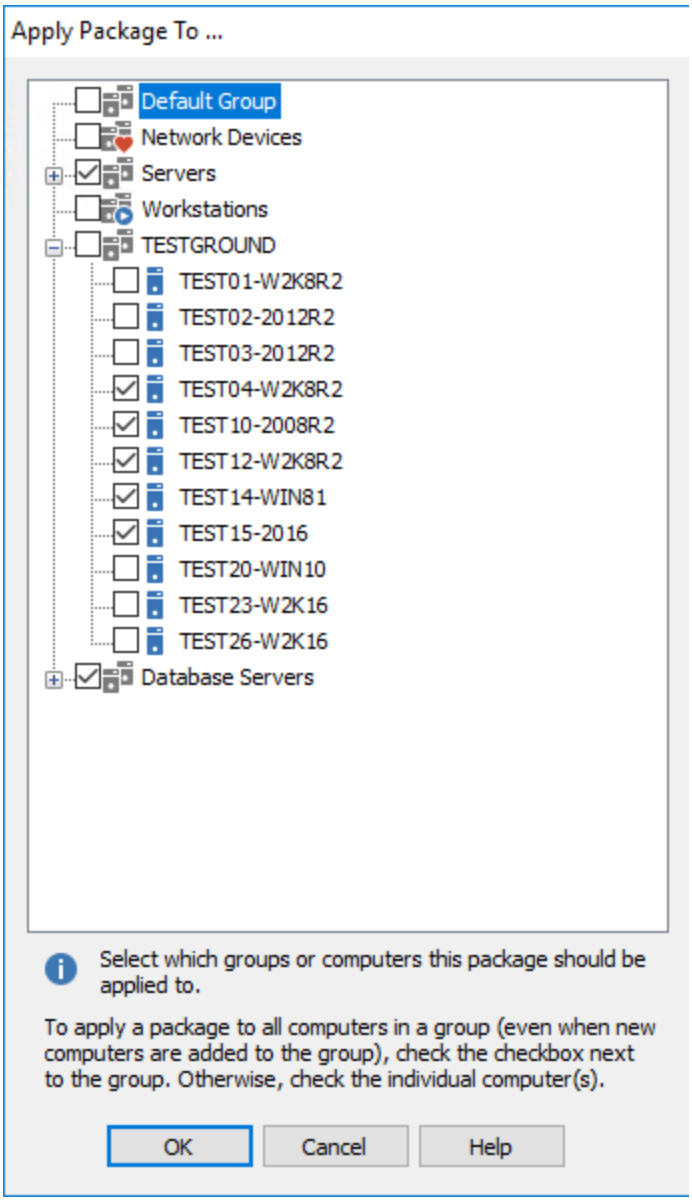


Alle Pakete mit einem markierten Kontrollkästchen sind globale Pakete, andere Pakete sind reguläre Pakete, die bereits einer Gruppe oder einem Computer zugeordnet sind oder einer Gruppe oder einem Computer zugeordnet werden müssen. Um ein Paket zu einem globalen Paket zu machen, kreuzen Sie einfach das Kontrollkästchen an, um das globale Kennzeichen zu löschen und ein Paket zu einem zuweisbaren Paket zu machen, löschen Sie einfach das Kontrollkästchen.

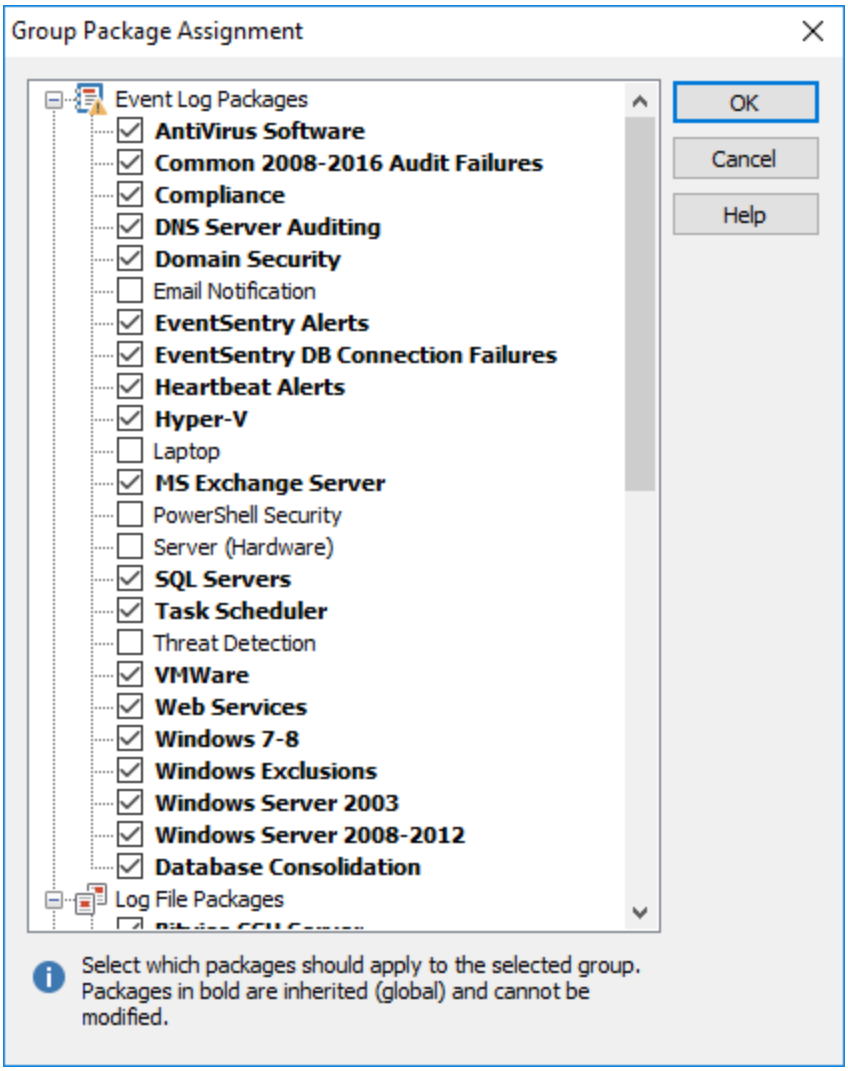
4.3.2.2 Zuweisen zu Gruppen

Sie können ein Paket auf zwei Arten einer Gruppe zuordnen:

1. Klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie "Assign ...", wodurch das Dialogfeld "Apply Package To ..." (Paket anwenden auf ...) angezeigt wird. Wählen Sie dort die Gruppe(n) aus, auf die das Paket angewendet werden soll, und klicken Sie auf OK. Diese Option ist vorzuziehen, wenn Sie ein Paket mehr als einer Gruppe zuweisen müssen.



2. Klicken Sie mit der rechten Maustaste auf die Gruppe, auf die das Paket angewendet werden soll, und wählen Sie "Assign Package(s) ...", was Sie zum Dialogfeld "Package Assignments" bringt. Wählen Sie dort alle Pakete aus, die auf die ausgewählte Gruppe angewendet werden sollen. Diese Option ist vorzuziehen, wenn Sie einer Gruppe mehr als ein Paket zuweisen müssen.

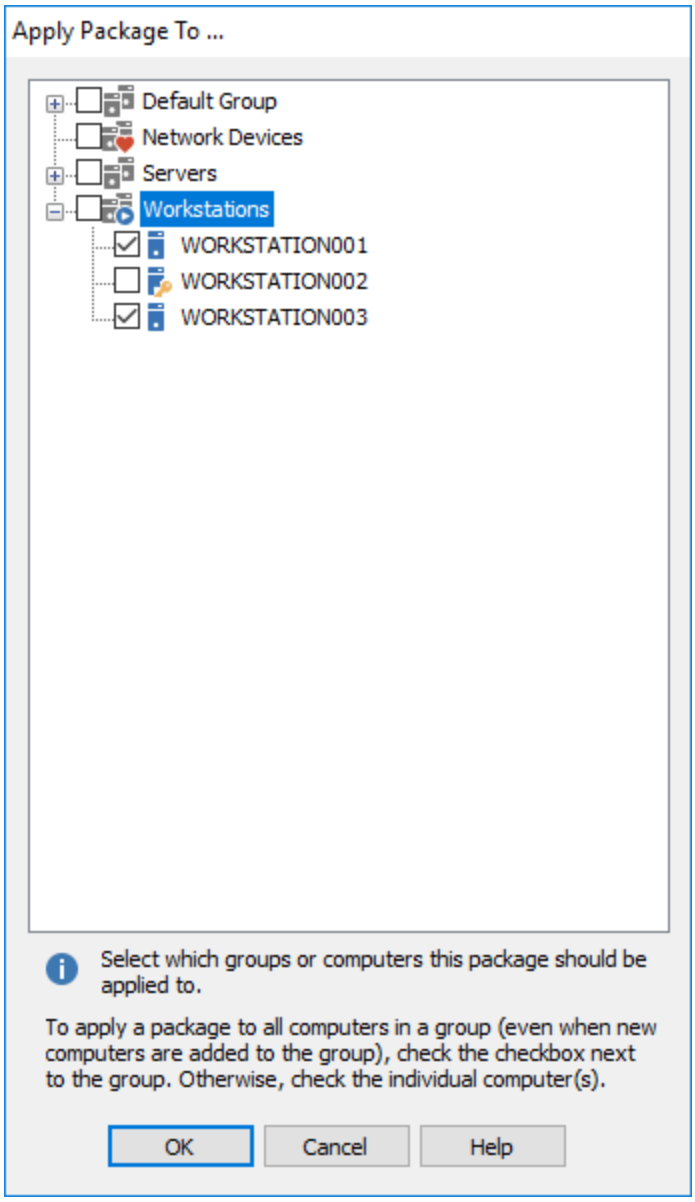


Bitte beachten Sie, dass globale Pakete in der Paketliste fett erscheinen und nicht zugewiesen/nicht zugewiesen werden können.

4.3.2.3 Zuweisen zu Computern

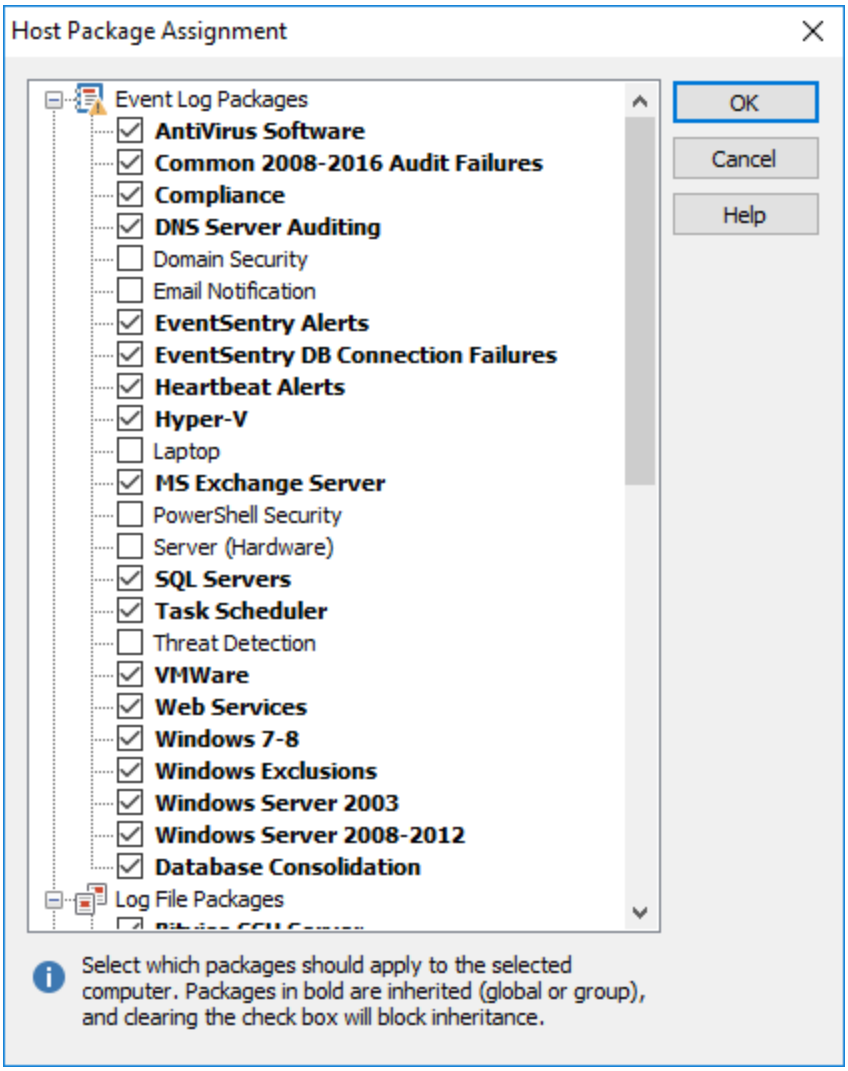
Sie können ein Paket auf zwei Arten einem Computer zuweisen:

1. Klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie "Assign ...", wodurch das Dialogfeld "Apply Package To ..." (Paket anwenden auf ...) angezeigt wird. Wählen Sie dort den/die Computer aus, auf den/die das Paket angewendet werden soll, und klicken Sie auf OK. Diese Option ist vorzuziehen, wenn Sie ein Paket mehr als einem Computer zuweisen müssen.



Bitte beachten Sie, dass globale Pakete und Pakete, die der Gruppe zugeordnet sind, in der der Computer Mitglied ist, fett dargestellt werden. Sie können die Paketvererbung blockieren, indem Sie das Kontrollkästchen eines fett dargestellten Pakets deaktivieren. Klicken Sie hier für weitere Informationen.

2. Klicken Sie mit der rechten Maustaste auf den Computer, auf den das Paket angewendet werden soll, und wählen Sie "Assign Package(s) ...", wodurch Sie zum Dialogfeld "Package Assignments" gelangen. Wählen Sie dort alle Pakete aus, die auf den ausgewählten Computer angewendet werden sollen. Diese Option ist vorzuziehen, wenn Sie einem Computer mehr als ein Paket zuweisen müssen.



4.3.2.3.1 Sperren der Paketvererbung

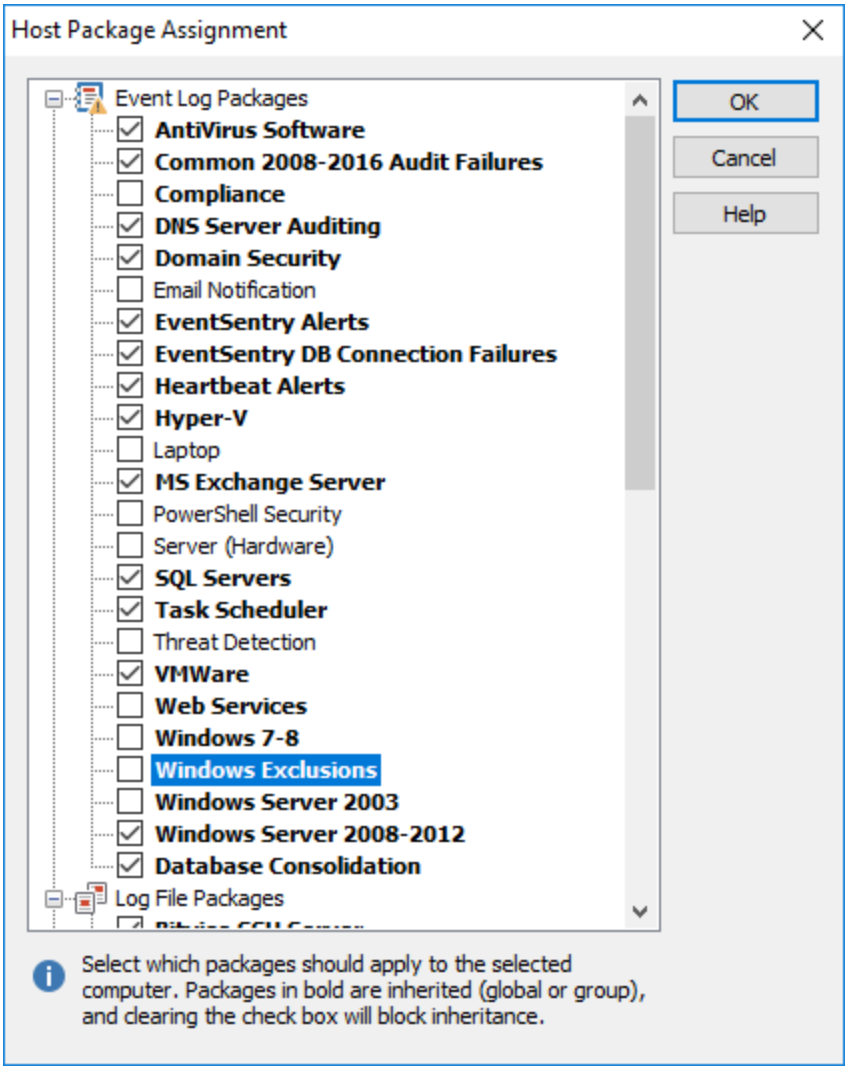
Ab Version 2.90 ist es möglich, einen oder mehrere Computer von globalen oder Gruppenpaket-Zuweisungen auszuschließen.

Dies ist z. B. nützlich, wenn Sie ein globales Paket haben, das auf 99 % aller Computer zutrifft, oder ein einer Gruppe zugeordnetes Paket, das mit einer geringen Anzahl von Ausnahmen auf alle Computer in der Gruppe zutrifft.

Es ist zwar möglich, die globalen oder gruppenbasierten Zuweisungen zu ändern, indem das Paket Computern direkt zugewiesen wird, doch besteht dabei die Gefahr, dass neuen Computern nicht das richtige Paket zugewiesen wird. Stattdessen können Sie die globalen oder gruppenbasierten Zuweisungen beibehalten und die Computer, denen Sie das Paket nicht zuweisen möchten, einfach ausschließen.

Um die Vererbung für eine globale oder gruppenbasierte Paketzuordnung zu blockieren, erweitern Sie die Container **Computergruppen** und navigieren Sie zu dem Computer, für den Sie die Vererbung blockieren möchten. Klicken Sie mit der rechten Maustaste auf den Computer und wählen Sie **Assign Package(s)...** . Das daraufhin angezeigte Dialogfeld zeigt Ihnen alle Pakete an, die diesem Computer

zugeordnet sind, wobei vererbte Pakete fett dargestellt werden. Um die Vererbung zu blockieren, deaktivieren Sie einfach das Kontrollkästchen neben dem (fettgedruckten) geerbten Paket, wie unten für das Paket **Services for Vista Win2k8** gezeigt:



Blockieren der Vererbung

Denken Sie daran, dass blockierte Pakete mit dem Computerobjekt verknüpft sind und auch dann blockiert bleiben, wenn das geerbte Paket auf global oder gruppenbasiert umgeschaltet wird.

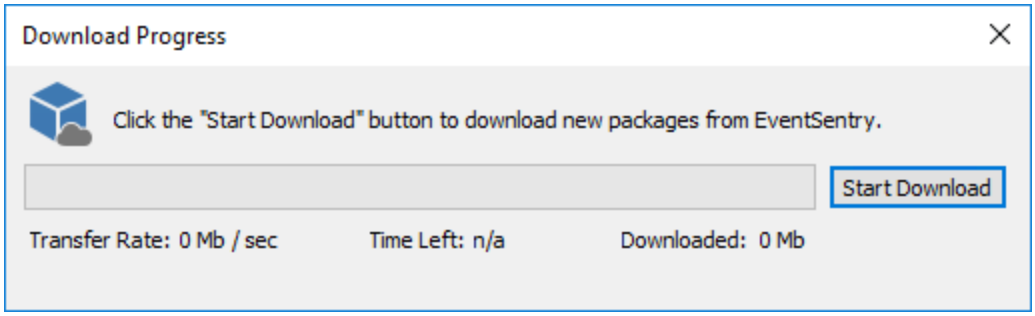
4.3.3 Herunterladen von Paketen

NETIKUS.NET bietet einen Standardsatz von Filter- und Health-Paketen, die ständig aktualisiert und verbessert werden, um gemeinsame Filter- und Service-Einstellungen anzubieten.

Ein Standardsatz von Filter- und Health-Paketen wird bei der ersten Installation automatisch konfiguriert EventSentryund Sie können die neuesten aktuellen Pakete erhalten, indem Sie sie von unserer Website direkt von der Verwaltungskonsole herunterladen.

1. Herunterladen neuer Pakete

Um die neuesten Pakete herunterzuladen, wählen Sie **Download Latest Packages** ... aus dem Menü Extras, klicken Sie auf das Symbol in der Symbolleiste oder klicken Sie mit der rechten Maustaste auf den Paket-Container und wählen Sie **Download Latest Packages** ..., wodurch der folgende Dialog angezeigt wird:



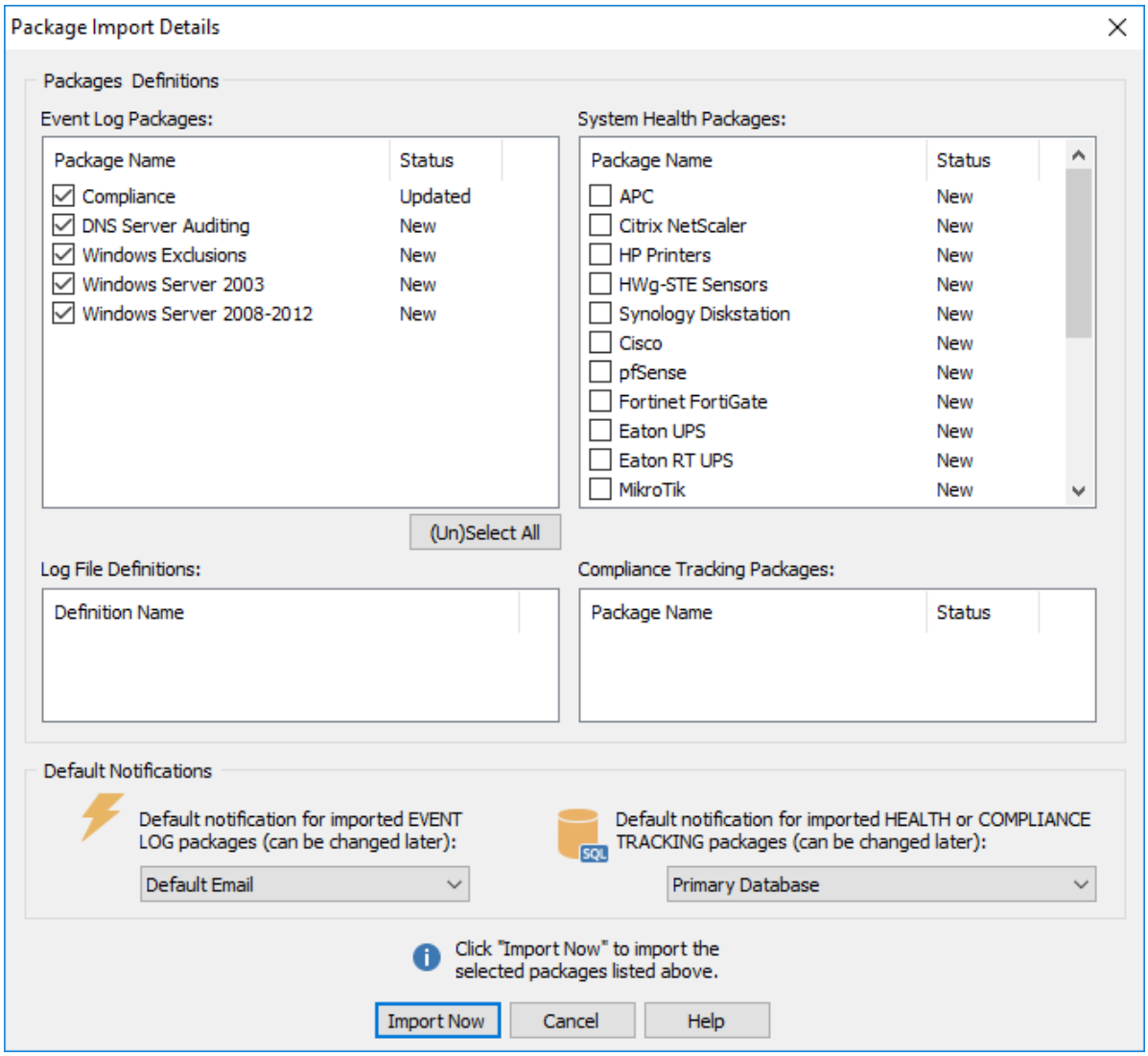
Wenn Sie das Kontrollkästchen **Do not merge downloaded packages ...** markieren, werden neue Filter in aktualisierten Paketen nicht mit Ihren aktuellen Paketen zusammengeführt, und Sie können nur vollständig neue Pakete installieren.

Die Paketdatei wird heruntergeladen, nachdem Sie auf die Schaltfläche **Download starten** und auf die Schaltfläche **Weiter** klicken, um auszuwählen, welche Pakete importiert werden sollen.

2. Auswahl der zu importierenden Pakete

Sobald die Paketdatei heruntergeladen worden ist, wird EventSentry bestimmen welche Pakete neu sind und welche Pakete seit dem letzten Download aktualisiert wurden.

Sie können im Dialogfeld **Paketimportdetails** auswählen, welche Pakete Sie importieren möchten. Wenn Sie es vorziehen, ein bestimmtes Paket nicht zu installieren, können Sie einfach das Kontrollkästchen neben dem Namen des Pakets deaktivieren.



Da alle Filter mindestens eine Aktion erfordern um mit ihnen verknüpft zu werden, müssen Sie eine bestehende Aktion im Standardbenachrichtigungs-Container auswählen. Sie können diese Einstellung nach dem Import ändern oder erweitern, indem Sie mit der rechten Maustaste auf das/die importierte(n) Paket(e) klicken und **Bearbeitungsoptionen** wählen.

Beim Import von Health-Paketen wird außerdem empfohlen, eine Standardbenachrichtigung vom Datenbanktyp auf Paketebene anzugeben.

3. Post-Import-Anpassungen

Sie können heruntergeladene Pakete (und Filter) bearbeiten, nachdem Sie sie importiert haben, z.B. um die Beschreibung zu ändern oder Benachrichtigungen hinzuzufügen/zu ändern.

Es wird jedoch nicht empfohlen, in Paketen enthaltene Filter umzubenennen oder zu löschen, da diese Filter beim nächsten Herunterladen von Paketen wieder importiert werden.

Proxy-Server

Alle Funktionen in EventSentry die Dateien herunterladen oder Inhalte über HTTP übermitteln, unterstützen einen Proxy-Server. Wenn Ihr Netzwerk die Verwendung eines Proxy-Servers für die HTTP-

Kommunikation erfordert, finden Sie unter Web Reports & Proxy weitere Informationen zur Konfiguration dieser Funktion.

4.3.4 (Auf-)Verbergen von Paketen

Sie können Pakete ausblenden an denen Sie nicht interessiert sind. Wenn Sie EventSentry z.Bsp. nur verwenden um Server zu überwachen, dann können Sie das Laptops-Paket ausblenden. Versteckte Pakete sind noch aktiv und werden verarbeitet, werden aber in der Verwaltungskonsole nicht angezeigt. Diese Funktion ist besonders nützlich, wenn Sie Pakete aus dem Web herunterladen.

Verstecken vs. Löschen

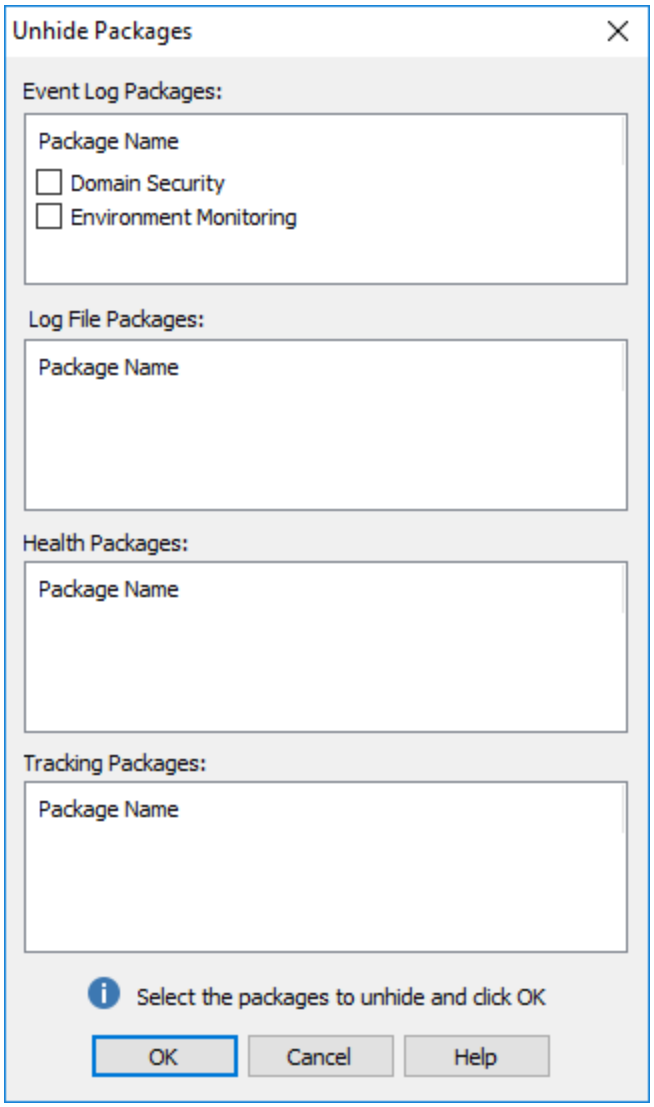
Wenn Sie ein zuvor heruntergeladenes Paket aus Ihrer Konfiguration löschen, werden Sie beim nächsten Herunterladen von Paketen aus dem Web aufgefordert, dieses Paket erneut zu importieren. Wenn Sie das Paket jedoch ausblenden, werden Sie in Zukunft nicht mehr aufgefordert, das Paket zu importieren (es sei denn, es wurde aktualisiert), da das Paket technisch noch installiert ist.

Ausblenden eines Pakets

Um ein Paket auszublenden, klicken Sie mit der rechten Maustaste auf den Paketcontainer und wählen Sie Ausblenden. Das Paket verschwindet sofort aus der Liste. Das Paket wird weiterhin zugewiesen, es sei denn, Sie heben die Zuweisung auf.

Ausblenden eines oder mehrerer Pakete

Um ein weiteres Paket einzublenden, klicken Sie mit der rechten Maustaste auf den Container "Packages" und wählen Sie "Unhide Packages", wodurch das folgende Dialogfeld angezeigt wird:



Wählen Sie das (die) Paket(e) aus, das (die) Sie einblenden möchten, und klicken Sie auf OK. Die Pakete erscheinen nun wieder in der Baumstruktur.

4.4 Aktionen

Mit einer Aktion (bis zu 128 können angelegt werden) legen Sie fest, wie Sie benachrichtigt werden, wenn ein relevantes Ereignis eintritt. Die folgenden Benachrichtigungsarten werden derzeit unterstützt:

- E-Mail (SMTP)
- Datenbank
- HTTP
- Datei (einschließlich einfacher Text, (X)HTML- und CSV-Dateien)
- Syslog (UDP / TCP)
- SNMP-Fallen
- Netzwerk-Nachricht
- Prozess
- Ton
- Schreibtisch

- Dienst
- Herunterfahren/Neustart
- Geschnatter
- Parallele Schnittstelle (ASCII-fähige Matrixdrucker)

Die SMTP-, HTTP-, Syslog-TCP- und Datenbankbenachrichtigungen unterstützen lokales Caching, das eine fehlgeschlagene Aktion erneut benachrichtigen kann (z.B. wenn der SMTP-Server vorübergehend nicht erreichbar ist), wenn sie wieder verfügbar ist. Alle Aktionen, die vom Collector unterstützt werden, unterstützen auch das lokale Caching.

4.4.1 Aktionen verwalten

So aktivieren/deaktivieren Sie eine Aktion

Aktionen können aktiviert und/oder deaktiviert werden, indem Sie mit der rechten Maustaste auf das entsprechende Aktionssymbol im linken Navigationsbaum klicken. Diese Funktion ist praktisch, wenn Sie in Filtern von der Funktion "**apply to all actions**" Gebrauch machen. Anstatt mehrere Filter zu ändern, können Sie Aktionen einfach deaktivieren oder wieder aktivieren, indem Sie das Kontrollkästchen deaktivieren oder ankreuzen.

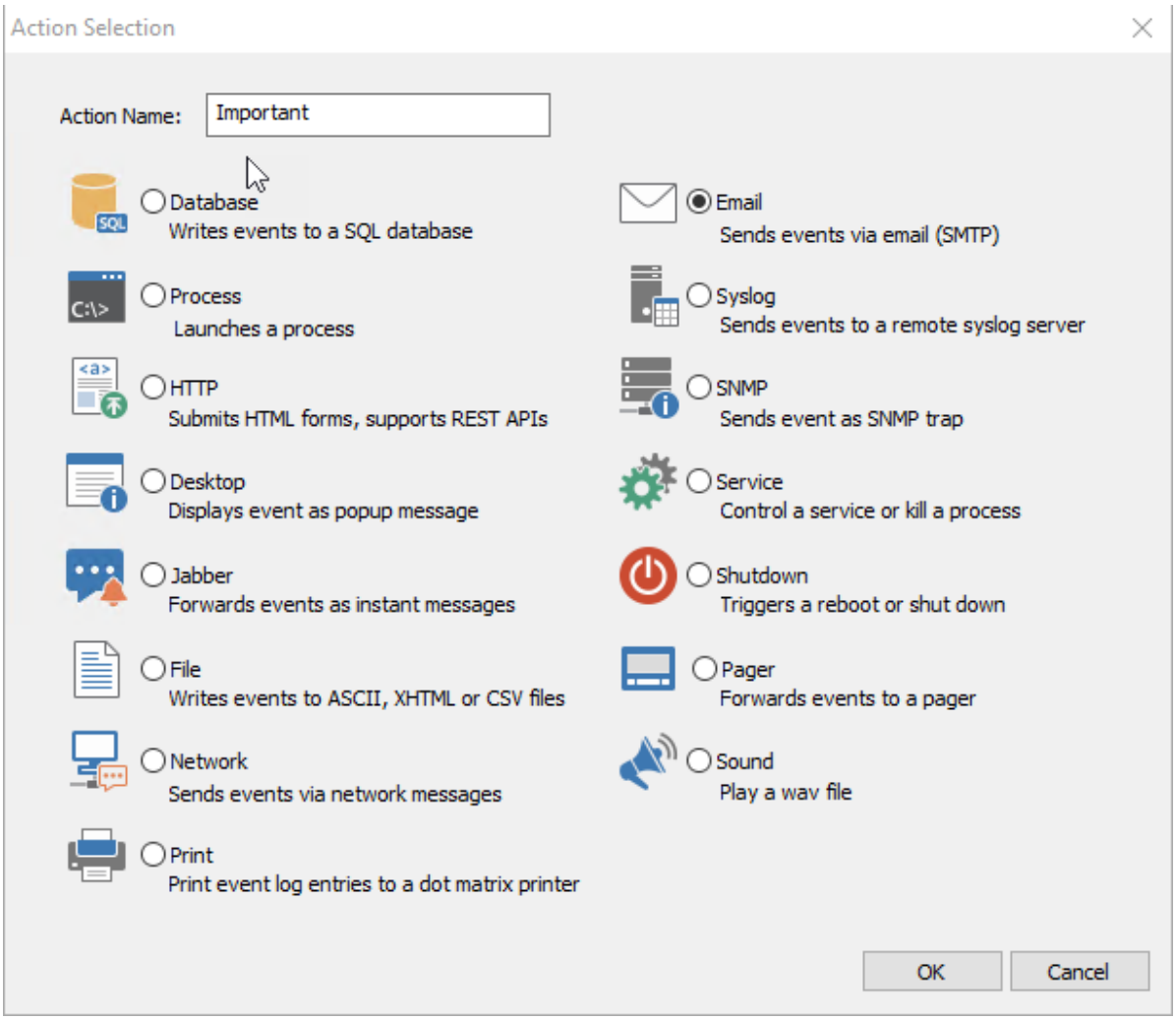
Collector verwenden

Die Aktivierung von "**Use Collector**" leitet eine Aktion durch einen der konfigurierten Collectors. Nur ausgewählte Aktionen können durch den Collector geleitet werden.

So fügen Sie eine neue Aktion hinzu

- Klicken Sie mit der rechten Maustaste auf Aktionen im linken Fensterbereich und wählen Sie Aktion hinzufügen; Sie werden aufgefordert, den Namen der Aktion einzugeben.
- Verwenden Sie den Ribbon, um eine neue Aktion hinzuzufügen (es wird der Dialog "Aktionsauswahl" angezeigt)
- Verwenden Sie den Ribbon, aber klicken Sie auf den Abwärtspfeil der Schaltfläche "Aktion hinzufügen", um einen Aktionstyp zum Hinzufügen auszuwählen

Der Aktionstyp (z.B. E-Mail) kann nach dem Anlegen einer Aktion nicht mehr geändert werden.



Aktionen bearbeiten

- Klicken Sie mit der linken Maustaste (oder doppelklicken Sie, siehe Benutzerfreundlichkeit) auf das Aktionselement im linken Fensterbereich
- Klicken Sie mit der rechten Maustaste auf das Aktionsobjekt und wählen Sie Bearbeiten

Die Aktionsdetails werden dann in den rechten Fensterbereich geladen und das aktive Aktionsobjekt im linken Fensterbereich wird fett dargestellt. Bitte beachten Sie, dass Sie den Aktionstyp einer bestehenden Aktion nicht ändern können.

Aktionen löschen

- Klicken Sie mit der rechten Maustaste auf die Aktion und wählen Sie Löschen aus dem Menü
- Wählen Sie die Aktion aus und wählen Sie "Löschen" im Ribbon
- Wählen Sie das Aktionsobjekt aus und drücken Sie die Taste Entf auf der Tastatur

Wenn ein oder mehrere Filter auf die Aktion verweisen, die gelöscht wurde, dann wird die gelöschte Aktion aus der Aktionsliste des Filters entfernt. Ein Filter wird deaktiviert, wenn die gelöschte Aktion die einzige Aktion dieses Filters war.

Filter finden, die eine Aktion referenzieren

Sie können eine Liste aller Filter anzeigen, die sich entweder direkt oder indirekt (ein Filter, der so konfiguriert ist, dass er alle Aktionen auslöst) auf eine Aktion beziehen. Klicken Sie mit der rechten Maustaste auf die betreffende Aktion und wählen Sie "Show Filters" -> "(Directly) Referencing this action".

So benennen Sie eine Aktion um

- Klicken Sie mit der rechten Maustaste auf die Aktion und wählen Sie Umbenennen aus dem Menü
- Wählen Sie die Aktion aus und drücken Sie die Taste F2 auf der Tastatur (funktioniert nur, wenn die Benutzerfreundlichkeit auf Doppelklick eingestellt ist)
- Klicken Sie 1-2 Sekunden lang mit der linken Maustaste auf das Aktionsobjekt

Aktion kopieren / duplizieren

1. Klicken Sie auf das Aktionsobjekt im linken Fensterbereich und vergewissern Sie sich, dass es ausgewählt ist
2. Klicken Sie auf das Kopiersymbol in der Symbolleiste oder wählen Sie Kopieren aus dem Menü Bearbeiten
3. Klicken Sie auf das Einfügen-Symbol in der Symbolleiste oder wählen Sie Einfügen aus dem Menü Bearbeiten

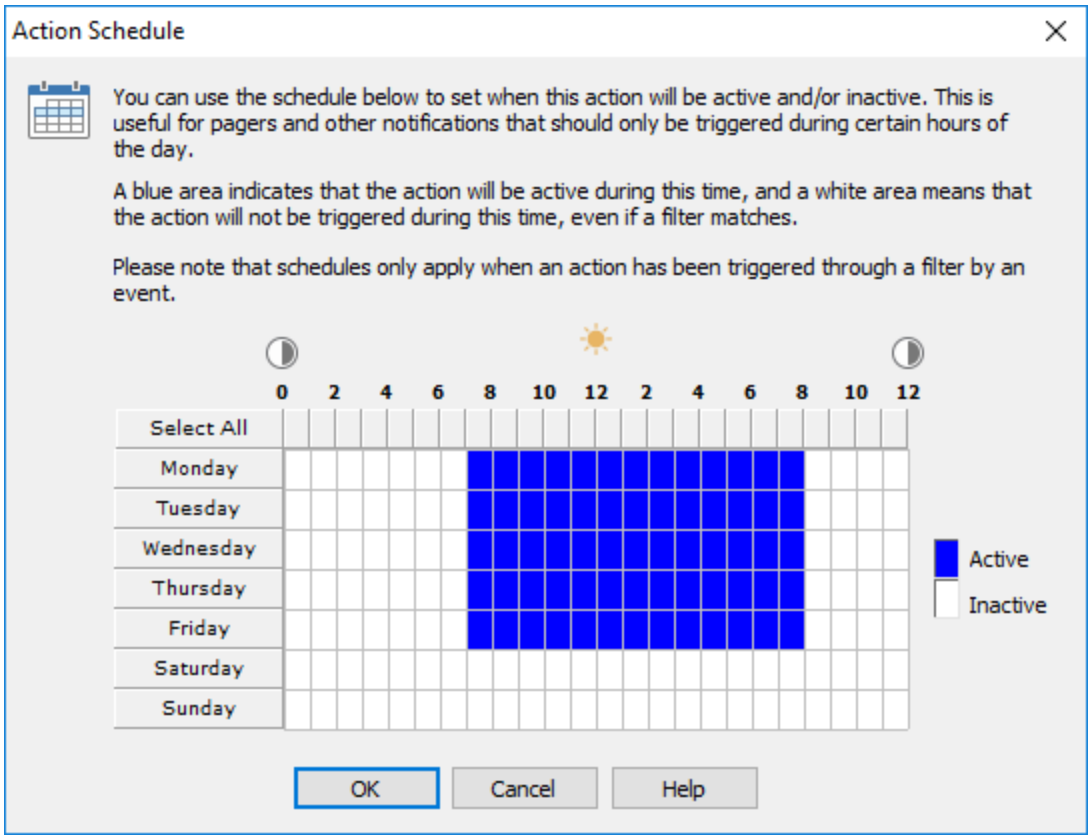
Wenn ein Aktionsobjekt mit dem gleichen Namen bereits existiert, wird dem Namen "Kopie von" vorangestellt. Bitte beachten Sie, dass Aktionsobjekte nicht ausgeschnitten und eingefügt werden können.

Aktionsreihenfolge ändern

Sie können die Reihenfolge der Aktionen ändern, indem Sie Aktionen per Drag & Drop an eine andere Position unter dem Actions-Container ziehen.

4.4.2 Zeitplan

Ein Aktionszeitplan aktiviert oder deaktiviert eine Aktion basierend auf der Tageszeit und/oder dem Wochentag. Dies ist ähnlich wie bei Filterzeitplänen, aber die Einstellung des Zeitplans bei der Aktion kann vorzuziehen sein, wenn Sie viele Filter haben, die die Aktion auslösen (wodurch doppelte Einstellungen auf mehreren Filtern vermieden werden).



Um einen Zeitplan festzulegen, klicken Sie auf die Schaltfläche **Zeitplan** und wählen Sie aus, während welcher Stunden die Aktion aktiv sein soll. Blaue Kästchen zeigen aktive Stunden an, während weiße Kästchen inaktive Stunden anzeigen. Sie können auf einen Wochentag oder eine Stunde des Tages klicken, um mehrere Kästchen auf einmal umzuschalten.

Denken Sie daran, dass ein Aktionszeitplan unabhängig von dem Filter, der ihn auslöst, wirksam ist und Ereignisse, die außerhalb des konfigurierten Zeitplans liegen, verworfen werden.

4.4.3 Aktions-Optionen

Für Aktionen können unabhängig von ihrem Typ mehrere generische Optionen festgelegt werden.

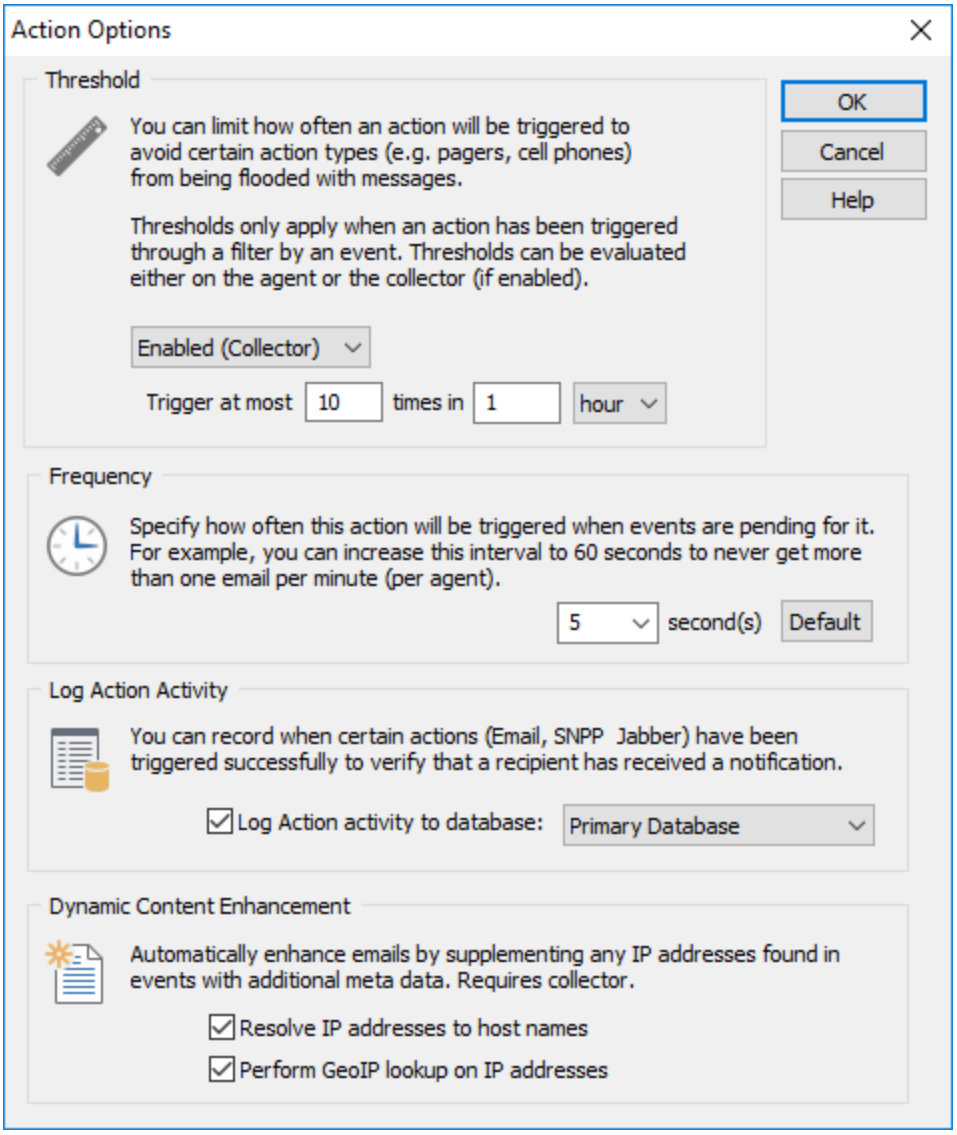
Schwellenwerte
Aktions-Schwellenwerte können begrenzen, wie oft eine Aktion ausgelöst wird. Schwellenwerte können auch mit Filtern kontrolliert werden, was im Allgemeinen vorzuziehen ist.

Häufigkeit
Anstatt dass eine Aktion sofort ausgelöst wird, wenn ein passendes Ereignis eintritt, kann die Häufigkeit einer Aktion angepasst werden.

Aktion Aktivität
Durch das Aktivieren einer Aktionsauslöser-Historie wird verfolgt, wann eine Aktion ausgelöst wurde, einschließlich Zustellinformationen wie Empfänger.

Dynamische Inhaltsverbesserung

Verbessert E-Mails, indem dynamische Daten in E-Mails, derzeit IP-Adressen, durch zusätzliche Informationen wie Geolokalisierung oder Hostnamen ergänzt werden.



4.4.3.1 Schwellenwerte

Sie können die Anzahl der Ereignisse, die an eine Aktion weitergeleitet werden, mit Hilfe von Filterschwellenwerten begrenzen, was in den meisten Szenarien gut funktioniert und eine Menge erweiterter Konfigurationseinstellungen für Schwellenwerteinstellungen bietet (z.B. Ereignisprotokollprotokollierung usw.).

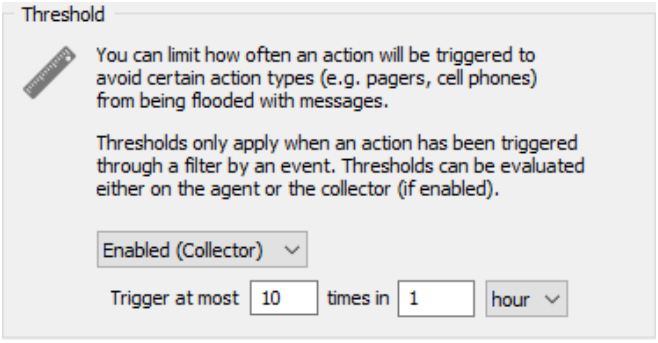
In einigen Fällen könnte es wünschenswerter sein, stattdessen eine Beschränkung auf eine Aktion anzuwenden. Dies ist nützlich, wenn Sie eine große Anzahl von Filtern haben, die Ereignisse an eine Aktion senden (und es zeitaufwändig wäre, für alle diese Filter Schwellenwerte festzulegen), oder wenn Sie eine Aktion (z.B. einen Pager) haben, bei der Sie sicherstellen müssen, dass nur eine begrenzte Anzahl von Ereignissen an die Aktion weitergeleitet wird.

Durch das Festlegen von Grenzen für Aktionen können Sie sicherstellen, dass die Aktion höchstens die festgelegte Anzahl von Zeitpunkten im konfigurierten Zeitraum ausgelöst wird, unabhängig davon, wie

viele Ereignisse von einem oder mehreren Filtern an die Aktion übergeben werden. Klicken Sie auf die Schaltfläche **Optionen**, um einen Aktionsgrenzwert festzulegen.

Aktionsgrenzwerte können entweder auf dem Agent oder auf dem Collector (wenn ein Collector aktiviert ist) ausgewertet werden. Wenn auf "Enabled (Collector)" gesetzt, ist der Schwellenwert global und gilt für alle vom Collector gesendeten E-Mails. So würde ein Grenzwert von "10 pro 1 Stunde" dazu führen, dass nicht mehr als 10 E-Mails in einer Stunde gesendet werden. Wenn derselbe Schwellenwert für "Aktiviert (Agent)" konfiguriert ist, wird der Schwellenwert auf dem Agenten ausgewertet und bedeutet, dass von jedem Agenten nicht mehr als 10 E-Mails gesendet werden - was dazu führen könnte, dass mehr als 10 E-Mails von mehreren Agenten gesendet werden.

Es ist wichtig zu verstehen, dass sich eine Aktionsgrenze nicht auf die Anzahl der Ereignisse bezieht, sondern auf die Anzahl der Auslösungen der Aktion. Wenn Sie z.B. ein Limit für eine E-Mail-Aktion festlegen, dann gilt das Limit für die **Anzahl der E-Mails**, nicht für die Anzahl der Ereignisse innerhalb der E-Mails. Daher funktioniert die Funktion zur Begrenzung von Aktionen je nach Art der ausgelösten Aktion unterschiedlich. Weitere Einzelheiten zur Funktionsweise des Aktionslimits für verschiedene Aktionstypen finden Sie in der unten stehenden Liste:



Aktionstyp	Pro Ereignis	Pro Auslöser (Detail)
E-Mail (SMTP)	-	Ja (per E-Mail)
Pager (SNPP)	-	Ja (pro Verbindung zum SNPP-Server)
Datenbank	-	Ja (pro Verbindung zum Datenbankserver)
Syslog	-	Ja (pro Verbindungen zum Syslog-Server)
Datei	Ja	-
Parallel	Ja	-
Netzwerk-Nachricht	Ja	-
Prozess	Ja	-
Sound	Ja	-
Desktop	Ja	-
Jabber	Ja	-
SNMP	Ja	-
Dienst	Ja	-
Herunterfahren	Ja	-

Aktionsgrenzwerte mit Collector

Beachten Sie bei der Verwendung von Aktionsschwellenwerten mit Collector folgendes:

- Collector-seitige Aktions-Schwellenwerte werden derzeit nur für die SMTP-Aktion unterstützt.
- Wenn eine E-Mail die letzte E-Mail ist, bevor der Schwellenwert überschritten wird, beginnt der Betreff der E-Mail mit **[THRESHOLD REACHED]**, um anzuzeigen, dass einige E-Mails unterdrückt werden können.

Häufigkeit

Standardmäßig leiten die E-Mail-, Pager- und Datenbankaktionen Ereignisse alle 5 Sekunden an den konfigurierten Server weiter. Dieses Intervall kann zum Zweck der Aggregation von Ereignissen erhöht werden. Anstatt beispielsweise 3 E-Mails innerhalb einer Minute zu erhalten, die jeweils ein einzelnes Ereignis enthalten, können Sie jede Minute eine E-Mail erhalten, die alle drei Ereignisse enthält. Diese Funktion ist vor allem für die E-Mail- und Datenbankaktion nützlich.

4.4.3.2 Häufigkeit

Die Aktionshäufigkeit (oder das Polling-Intervall) gibt an, wie oft Ereignisse, die einer Aktion unterbreitet wurden, von dieser Aktion verarbeitet (und an ihr jeweiliges Ziel gesendet) werden. Wenn die Aktionshäufigkeit für eine E-Mail beispielsweise auf 60 Sekunden eingestellt ist, wird der EventSentry Agent nie mehr als eine E-Mail pro Minute senden, da die Ereignisse im Wesentlichen gruppiert werden. 3 Ereignisse, die im Abstand von 5 Sekunden stattfinden, werden alle in einer E-Mail versendet.

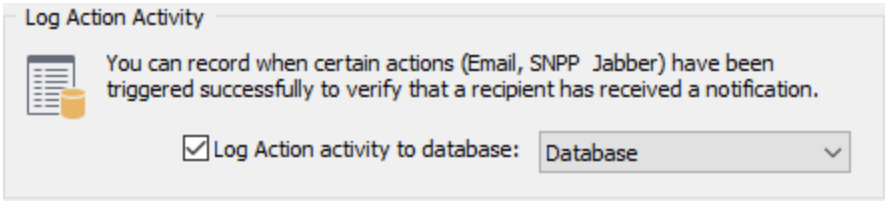
Die Aktionshäufigkeit gilt für die folgenden Aktionstypen:

- E-Mail
- Datenbank
- Syslog
- HTTP
- Netzwerk
- SNPP

4.4.3.3 Aktion Aktivität

Sie können verfolgen, wann immer eine bestimmte Aktion ausgelöst wird, indem Sie in einem Aktionsdialogfeld auf die Schaltfläche **Optionen** klicken. Die Trigger-History-Funktion ist derzeit für alle Aktionen mit geringem Volumen verfügbar, einschließlich E-Mail, Jabber und SNPP.

Wenn aktiviert, zeichnet EventSentry jedes Mal auf, wenn die Aktion ausgelöst wird, einschließlich des Zeitstempels sowie der Empfängerinformationen der Aktion. Der Verlauf der Aktionsauslösung kann mit Hilfe der Web Reports auf der Seite "Ereignissuche -> Aktionsverlauf" überprüft werden.



Die unten aufgeführten Felder werden in der Historie aufgezeichnet:

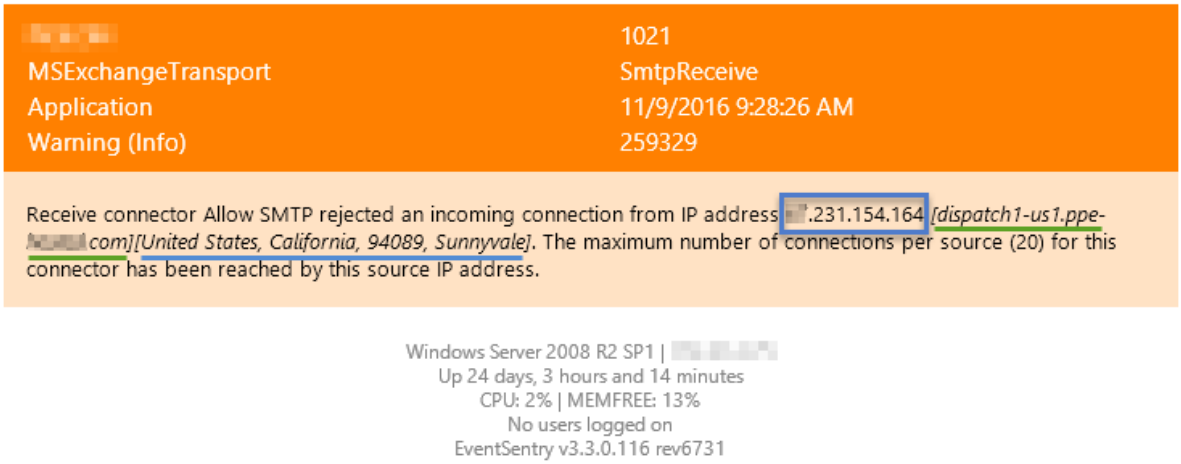
- Source Computer
- Action Name
- Action Type
- Action Recipients
- Filter Package Name
- Filter Name
- Event Number
- Event ID

- Event Log
- Event Source
- Event ID

4.4.3.4 Dynamische Inhaltsverbesserung

EventSentry kann automatisch IP-Adressen aus jedem Ereignis extrahieren und die IP-Adressen durch **Reverse-Lookup-** und/oder **Geo-IP-Lookup-Daten** ergänzen. Durch die Angabe von Geolokalisierung und/oder Hostnamen in der E-Mail wird die Nutzbarkeit von E-Mail-Benachrichtigungen für den Empfänger erheblich verbessert, ohne dass dieser manuelle Nachschlagen durchführen muss.

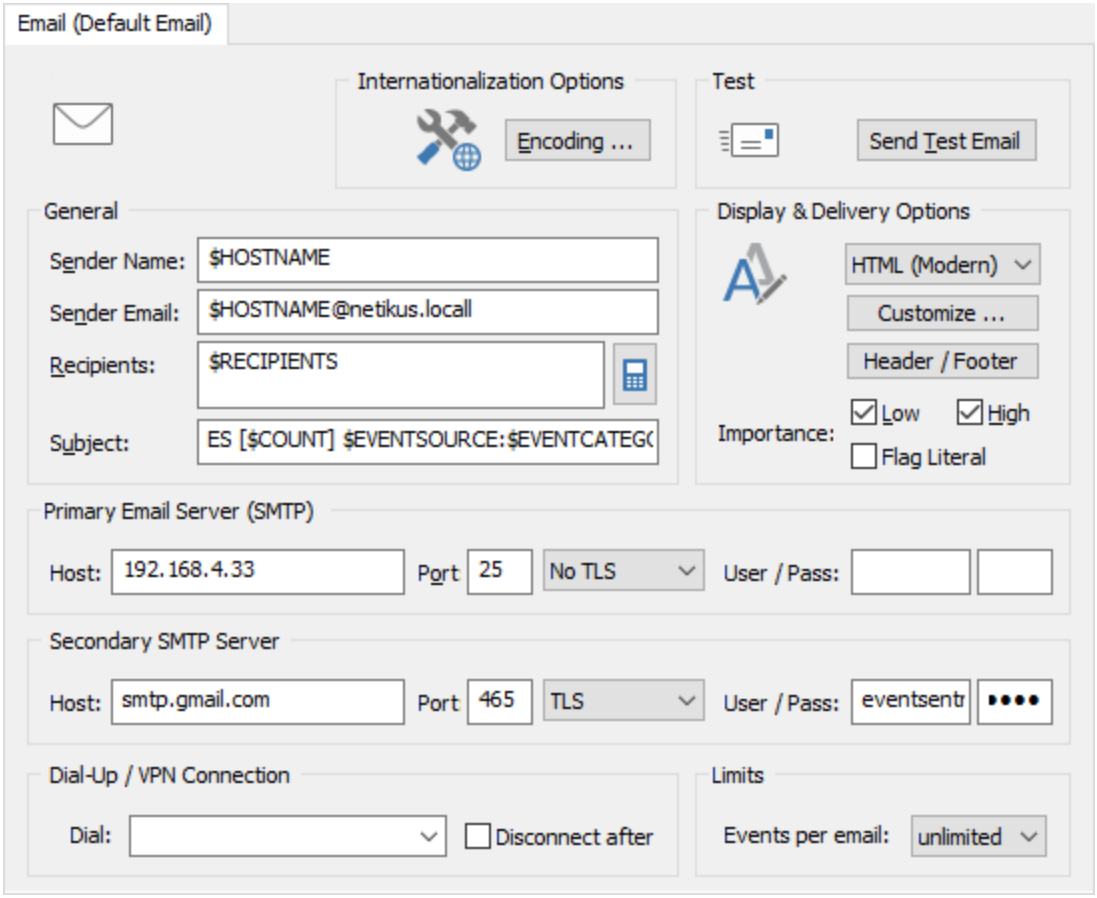
Die Abbildung unten zeigt eine E-Mail-Benachrichtigung, die eine IP-Adresse (blaues Rechteck) enthält, die durch die Bereitstellung von zusätzlichem Kontext erweitert wurde. Unmittelbar nach der IP-Adresse folgt ein Reverse-Lookup (grüne Linie) sowie die Geolokalisierung der IP-Adresse (blaue Linie).



Diese Funktion ist derzeit nur für E-Mail-Aktionen verfügbar, die den Collector verwenden. Sowohl Reverse-Lookups als auch Geoip-Lookups werden auf dem Collector, nicht auf dem Agent ausgeführt.

4.4.4 Email (SMTP)

Eine SMTP-Aktion leitet Ereignisprotokollmeldungen per E-Mail weiter. Die E-Mail-Aktion unterstützt mehrere Formate, Backup-SMTP-Server, SSL-Authentifizierung, Variablen und mehr.



Absender Name

Dieser Wert erscheint als Absendername der E-Mail (nicht die E-Mail-Adresse). Dies ist normalerweise der Hostname des Computers. Wenn Sie planen, eine SMTP-Aktion auf mehrere Hosts zu replizieren, können Sie hier die Variable **$HOSTNAME** verwenden. Um mehr über Variablen zu erfahren, klicken Sie hier.

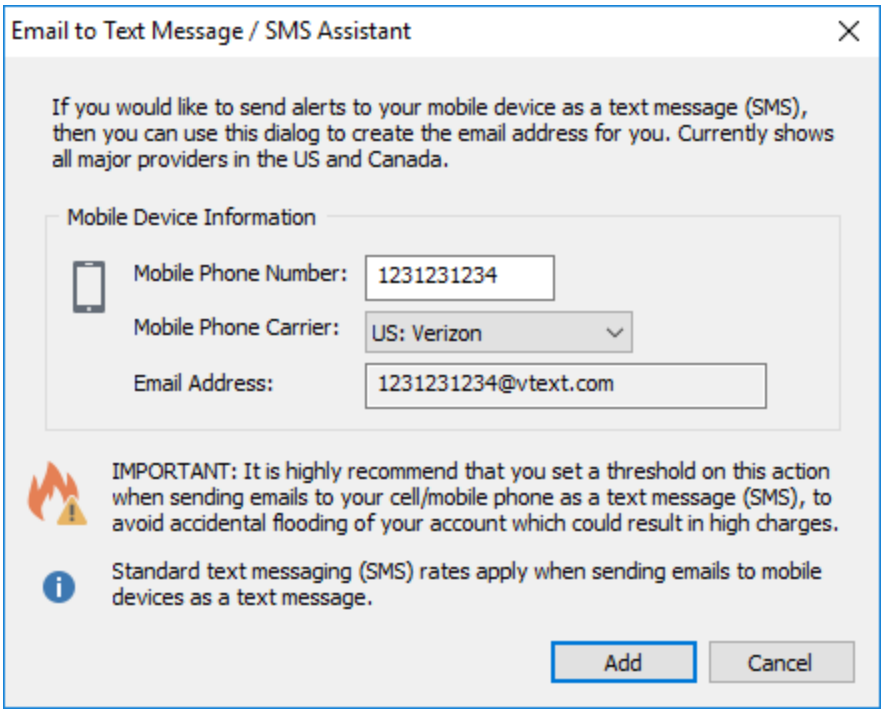
Absender E-Mail

Die E-Mail-Adresse, unter der diese E-Mail gesendet wird. Wenn Sie andere Personen als sich selbst benachrichtigen, sollten Sie wahrscheinlich sicherstellen, dass Antworten auf E-Mails, die von EventSentry irgendwo ankommen.

Empfänger

Eine durch Komma getrennte Liste der E-Mail-Adressen des Empfängers. Die Gesamtlänge aller Empfänger (einschließlich der Kommas) darf 512 Zeichen nicht überschreiten. Wenn eine der E-Mail-Adressen vom Server zurückgewiesen wird, wird die E-Mail nicht gesendet und ein Fehler wird im Ereignisprotokoll protokolliert.

Wenn Sie beabsichtigen, eine Textnachricht über ein E-Mail-Gateway an ein Mobiltelefon zu senden, können Sie auf das Mobiltelefonsymbol neben dem Empfängerfeld klicken. Die meisten Mobilfunkanbieter bieten solche Gateways für den Absender kostenlos an, auch wenn für den Empfänger in der Regel Standard-SMS-Tarife gelten. Der Helferdialog erstellt die korrekte E-Mail-Adresse für Sie. Wenn Ihr Anbieter nicht aufgeführt ist, müssen Sie sich an Ihren Anbieter wenden, um die korrekte E-Mail-Adresse zu erhalten.



Bitte zögern Sie nicht, unserem Support-Team weitere Mobilfunkanbieter zur Aufnahme in eine zukünftige Version von EventSentry vorzuschlagen.

Wie im Dialog angegeben, wird dringend empfohlen, dass Sie einen Schwellenwert für jede Aktion anwenden, die Nachrichten an ein Mobiltelefon / Handy sendet, bei der Gebühren pro Nachricht anfallen könnten.

Betreff

Der Betreff der E-Mail. Die Variablen **$LOG** und **$COUNT** werden unterstützt. Um mehr über Variablen zu erfahren, klicken Sie hier.

Dynamischer Text im Betreff

Wenn mindestens ein Ereignis der aktuellen E-Mail vom Agenten gespoolt wurde, weil der SMTP-Server vorübergehend nicht verfügbar war, wird der Text **[BACKUP]** automatisch zum Betreff hinzugefügt. Wenn mindestens ein Ereignis der aktuellen E-Mail aus einem Ereignisprotokoll-Rescan stammt (z.B. das Ereignis trat ein, während der Agent nicht lief), dann wird der Text **[RESCAN]** automatisch zum Betreff hinzugefügt.

Wenn für die Aktion ein collector-seitiger Schwellenwert konfiguriert ist und eine E-Mail die letzte E-Mail vor Überschreiten des Schwellenwerts ist, wird der Betreff so geändert, dass er mit dem Text **[THRESHOLD REACHED]** beginnt, um anzuzeigen, dass einige E-Mails unterdrückt werden können.

(Primärer) SMTP-Server und -Port

Der Hostname oder die IP-Adresse des SMTP-Servers und der Port, auf dem der angegebene SMTP-Server auf eingehende Anfragen lauscht. Der Port ist standardmäßig auf **25** eingestellt.

(Sekundär-)SMTP-Server und -Port

Sie können einen sekundären SMTP-Server (einschließlich Port- und Authentifizierungsinformationen) angeben, der kontaktiert wird, wenn der primäre SMTP-Server nicht verfügbar ist. EventSentry verbindet sich immer mit dem primären SMTP-Server, bevor es den sekundären SMTP-Server ausprobiert.

SMTP-Authentifizierung Benutzername/Passwort

Wenn Ihr SMTP-Server eine Authentifizierung erfordert, geben Sie hier Benutzername und Passwort an. Sie können einen Benutzernamen und ein Passwort sowohl für den primären als auch für den sekundären Server angeben.

Derzeit werden die Authentifizierungsprotokolle Klartext (AUTH LOGIN) und MD5 (CRAM MD-5) unterstützt.

TLS

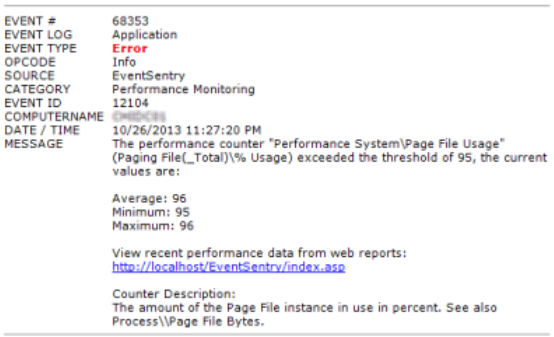
Setzen Sie diese Option entweder auf **TLS** oder **TLS (überprüfen)** , wenn der Server, zu dem Sie eine Verbindung herstellen, eine TLS-Verbindung unterstützt oder erfordert. Wenn Sie diese Option auf **TLS (überprüfen)** setzen, wird nur eine Verbindung zu SMTP-Remote-Servern hergestellt, die über ein gültiges TLS-Zertifikat verfügen; wenn Sie diese Option auf **TLS** setzen, akzeptiert **TLS** alle Remote-Zertifikate, auch selbstsignierte.

Stil

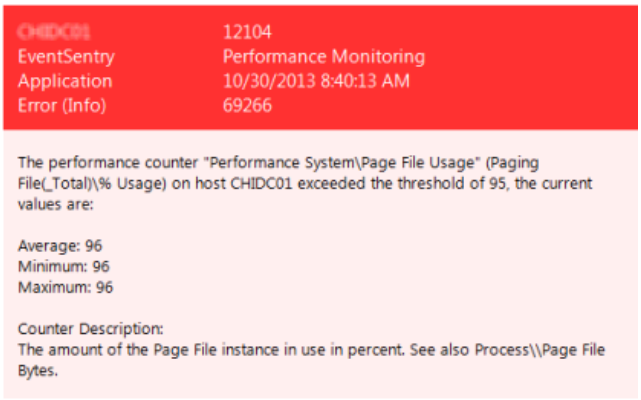
Sie können E-Mails entweder als einfachen Text, im HTML-Format oder in Miniaturgröße erhalten.

Einfacher Text: Sendet E-Mails ohne jegliche Formatierung.

HTML-E-Mail (Legacy & Modern): HTML-E-Mails können sowohl im Legacy als auch im modernen Format verschickt werden. Das Legacy-Format ist das ursprüngliche HTML-Format, das moderne HTML-Format wurde mit Version 3.0 eingeführt. Wenn Sie die Option HTML (Legacy) verwenden, können Sie auch die in den HTML-E-Mails verwendete Schriftart und -größe konfigurieren; die Standardeinstellung ist **Verdana** mit **11px**.



HTML (Legacy)



HTML (Modern)

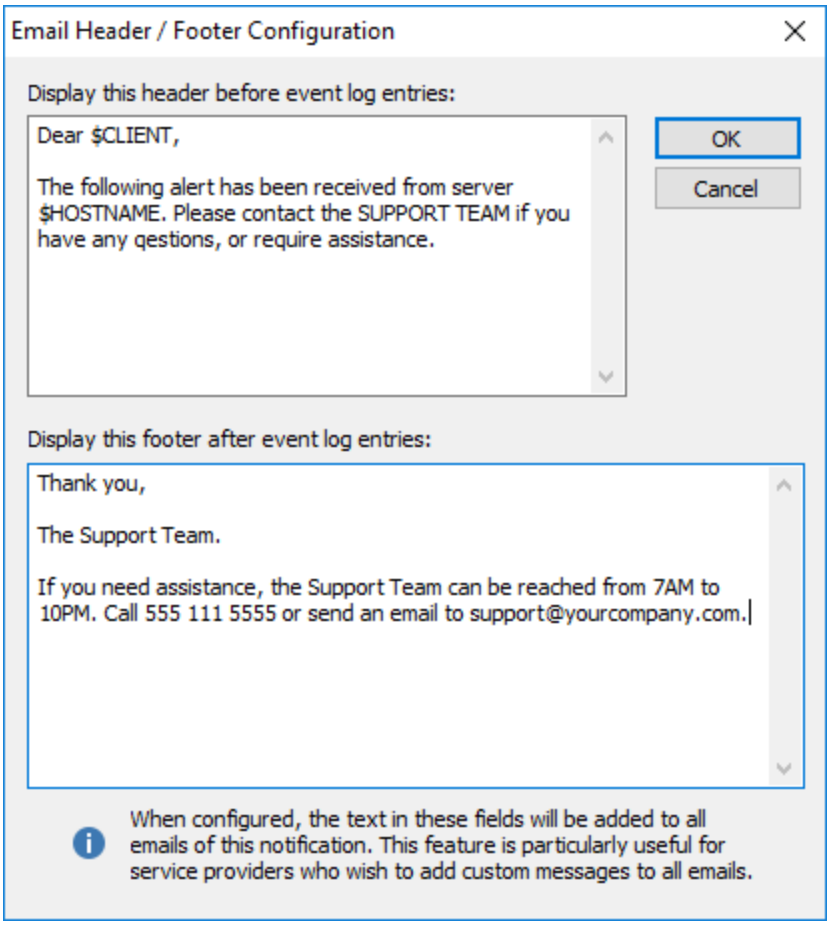
E-Mails, die im HTML-Format gesendet werden, enthalten auch einen einfachen Text für nicht HTML-fähige E-Mail-Clients.

Anzeige- und Zustelloptionen

Es ist möglich, den Inhalt und das Aussehen von E-Mail-Aktionen anzupassen, einschließlich der Eigenschaften des Ereignisprotokolls, die in von EventSentry gesendeten E-Mails enthalten sind.

Kopfzeile/Fußzeile

Sie können optional eine Kopf- und/oder Fußzeile zu jeder ausgehenden E-Mail mit dieser Benachrichtigung hinzufügen. Diese Funktion ist besonders nützlich für Dienstanbieter, die zusätzliche Informationen zu den an ihre Kunden gesendeten E-Mails hinzufügen möchten. Sowohl die Kopf- als auch die Fußzeile können bis zu 1024 Zeichen enthalten, mit einem Maximum von 2048 Zeichen nach variabler Erweiterung.



Hohe und niedrige Priorität

Die meisten E-Mail-Clients unterstützen ein Prioritaetsattribut, welche die Wichtigkeit einer E-Mail anzeigen. Diese Funktion ist nützlich, um sofort festzustellen, ob eine von EventSentry gesendete E-Mail wichtig ist oder nicht.

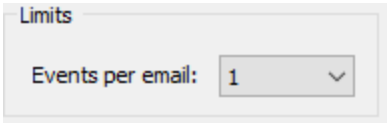
Hohe Bedeutung:	E-Mails werden mit dem Kennzeichen für hohe Wichtigkeit gesendet, wenn mindestens ein Ereignisprotokolleintrag in der E-Mail entweder ein **Fehler** oder ein **Audit-Fehler** ist.
Geringe Bedeutung:	E-Mails werden mit dem Kennzeichen für geringe Bedeutung versandt, wenn eine E-Mail nur **Informations-** oder Audit-Erfolgsmeldungen enthält.

Priorität Wörtlich

Wird in Kombination mit den Flags **Hohe und Niedrige Wichtigkeit** verwendet. Wenn die Option "**Flag Literal"** aktiviert ist, wird eine E-Mail unabhängig vom E-Mail-Inhalt immer mit hoher oder niedriger Wichtigkeit gesendet.

Max. Anzahl von Ereignissen pro E-Mail

Standardmäßig würde EventSentry so viele Ereignisdatensätze enthalten, wie in einer E-Mail gescannt wurden (eine E-Mail könnte mehr als 5 Ereignisdatensätze enthalten, wenn diese in kurzer Zeit eintraten). Diese Option ist besonders nützlich für Mobiltelefone, bei denen Ereignisaufzeichnungen nach der ersten nicht mehr gelesen werden können. Setzen Sie diese Option auf **unbegrenzt**, um das Standardverhalten wiederherzustellen, andernfalls auf die maximale Anzahl von Ereignisdatensätzen, die jede E-Mail enthalten sollte.



Dial-Up-Verbindung

Sie können eine bestehende RAS- (einschließlich VPN-) Verbindung auswählen, und EventSentry wählt diese Verbindung vor dem Senden der E-Mail an, wenn der SMTP-Server nicht kontaktiert werden konnte. Die RAS-Verbindung wird nach dem Senden der E-Mails aufgelegt, wenn die Option "**Auflegen nach**" aktiviert ist.

Sie können die grundlegenden Ereigniseigenschaften aus einer E-Mail direkt in das Dialogfeld **"General Filter"** einfügen, um auf einfache Weise einen Ein-/Ausschlussfilter auf der Grundlage einer erhaltenen E-Mail zu erstellen.

Wählen Sie einfach das Ereignis in der E-Mail aus und kopieren Sie es in die Zwischenablage. Erstellen Sie dann einen Filter (oder öffnen Sie einen vorhandenen Filter), klicken Sie auf ein beliebiges Textfeld und drücken Sie STRG+V. Die Tastaturkombination ist notwendig, ein Rechtsklick & Einfügen funktioniert nicht. Klicken Sie hier für weitere Informationen.

4.4.4.1 Fehlerbehebung E-Mail (SMTP)

Lösungen für häufige Probleme mit der SMTP-Aktion:

- Vergewissern Sie sich, dass der primäre (und ggf. der sekundäre) Hostname korrekt eingegeben wurde, einschließlich des Ports (standardmäßig 25). Vergewissern Sie sich auch, dass der Host, auf dem EventSentry installiert ist, den angegebenen Hostnamen erreichen kann.
- Sie können mehrere Empfänger durch ein Komma (,) trennen, achten Sie darauf, dass in diesem Feld keine Leerzeichen enthalten sind.
- Stellen Sie sicher, dass der angegebene SMTP-Server Nachrichten von der angegebenen Absender-E-Mail-Adresse und dem Computer, auf dem EventSentry installiert ist, akzeptiert.
- Diese Aktion protokolliert im Falle eines Fehlers die folgenden Ereignisse im Anwendungsereignisprotokoll mit der **EventSentry** Ereignisquelle:

Ereignis-IDs	Ereignis-ID	Problem
	500	Es konnte keine Verbindung zum angegebenen SMTP-Server hergestellt werden.
	501	Während der SMTP-Kommunikation ist ein Fehler aufgetreten.

	502	Verbindung zum primären SMTP-Server nicht möglich, Backup-Host wird versucht.

4.4.4.2 Anzeige- und Zustelloptionen

Stil / Anpassen

Das Erscheinungsbild von E-Mails kann angepasst werden, indem die in HTML-E-Mails verwendete Schriftart und Größe gewählt wird, indem ausgewählt wird, welche Ereigniseigenschaften in der E-Mail enthalten sein sollen, oder indem die in der E-Mail angezeigte Textmenge insgesamt minimiert wird.

Einfacher Textstil

E-Mails werden in einfachem ASCII-Text gesendet. Wenn Sie auf die Schaltfläche **Anpassen** klicken, können Sie auswählen, welche Felder eines Ereignisses in der E-Mail enthalten sein sollen. Sie können die Ausgabe beispielsweise so anpassen, dass nie die Ereignisnummer oder nie die Ereigniskategorie angezeigt wird.

HTML (Legacy) Stil

Verwenden Sie die **HTML-Schriftartoptionen**, um die Schriftart und Schriftgröße der von EventSentry erzeugten E-Mails anzupassen. Wie beim reinen Textstil können Sie durch Klicken auf die Schaltfläche **Anpassen** auswählen, welche Felder eines Ereignisses in der E-Mail enthalten sein sollen.

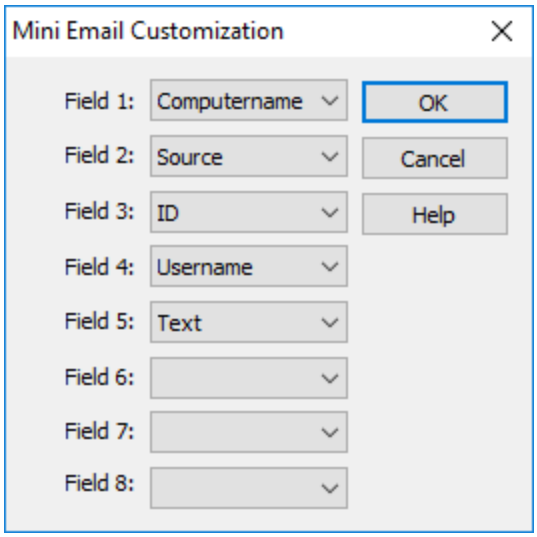
HTML-Stil (modern)

Schriftart und Schriftgrößenanpassung werden in diesem Stil nicht unterstützt, Ereignisfelder können umgeschaltet werden. Da dieser Stil zwei Felder pro Zeile anzeigt (z.B. Quelle & Kategorie), wird ein Feld nur dann ausgeblendet, wenn beide Felder in der Zeile nicht angekreuzt sind. Daher hat das bloße Deaktivieren des Kontrollkästchens "Ereigniskategorie" keine Wirkung, da die Ereignisquelle angezeigt wird.

Das Anpassen der Felder, die in einer E-Mail angezeigt/in einer E-Mail enthalten sind, kann die Kopieren/Einfügen-Funktionalität im Filterdialog unterbrechen.

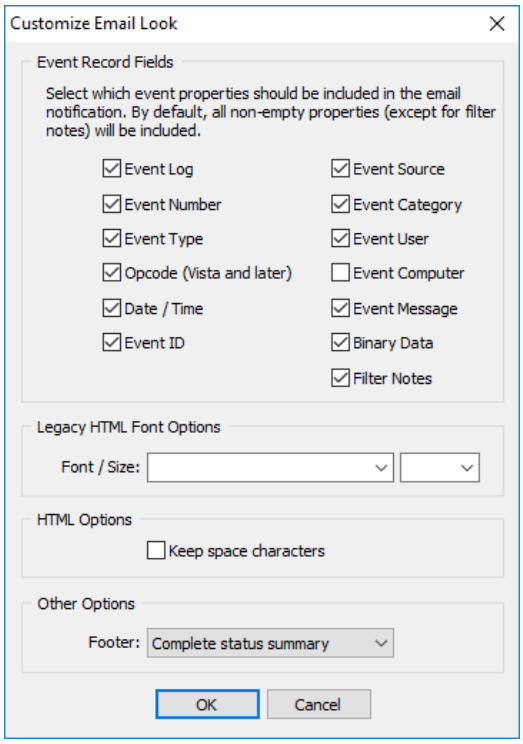
Miniatur-Stil

Wenn Sie vorhaben, über ein Mobiltelefon oder einen Pager benachrichtigt zu werden, sollten Sie dieses Kästchen ankreuzen. Es sendet kleine E-Mails, die nur die wichtigsten Informationen enthalten. Sie können das Aussehen der "**Miniatur**"-E-Mail anpassen, indem Sie auf die Schaltfläche "**Anpassen**" klicken. *Die Option **Maximale Anzahl von Ereignissen pro E-Mail** könnte ebenfalls von Interesse sein.*



Anpassung

Sie können anpassen, welche Eigenschaften des Ereignisprotokolls (z. B. Protokoll, Quelle, Kategorie usw.) in den von EventSentry gesendeten E-Mails enthalten sein sollen. Standardmäßig werden alle Eigenschaften mit Ausnahme der "Filternotizen" einbezogen.



Wenn Sie das Kontrollkästchen "EventSentry-Version einschließen" aktivieren, wird die aktuelle Version des EventSentry-Agenten in der E-Mail angezeigt. Dies ist eine einfache und unaufdringliche Methode, um zu überprüfen, ob der Agent auf einem bestimmten Rechner die neueste Version ausführt.

Leerzeichen beibehalten

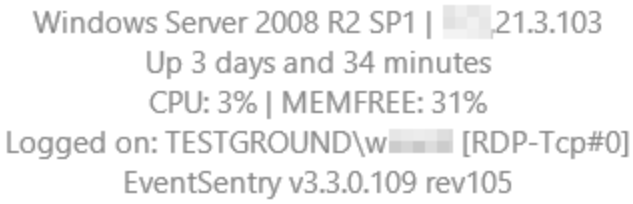
Wenn dieses Kontrollkästchen aktiviert ist, werden Leerzeichen von Ereignissen in HTML-E-Mails beibehalten.

Fußzeile

E-Mails können die folgenden Arten von automatischen Fußzeilen enthalten:

- Keine Fußzeile
- Nur Agentenversion: Zeigt die Version des Agenten an, der auf dem Host läuft, der das/die Ereignis(e) erzeugt hat.
- Vollständige Statuszusammenfassung: Enthält die Version des Agenten sowie die folgenden Angaben:

1. Betriebssystem
2. Die IP-Adresse
3. Laufzeit
4. CPU & Memory Utilization
5. Angemeldete(r) Benutzer, falls vorhanden



Beispiel für eine vollständige Statuszusammenfassung

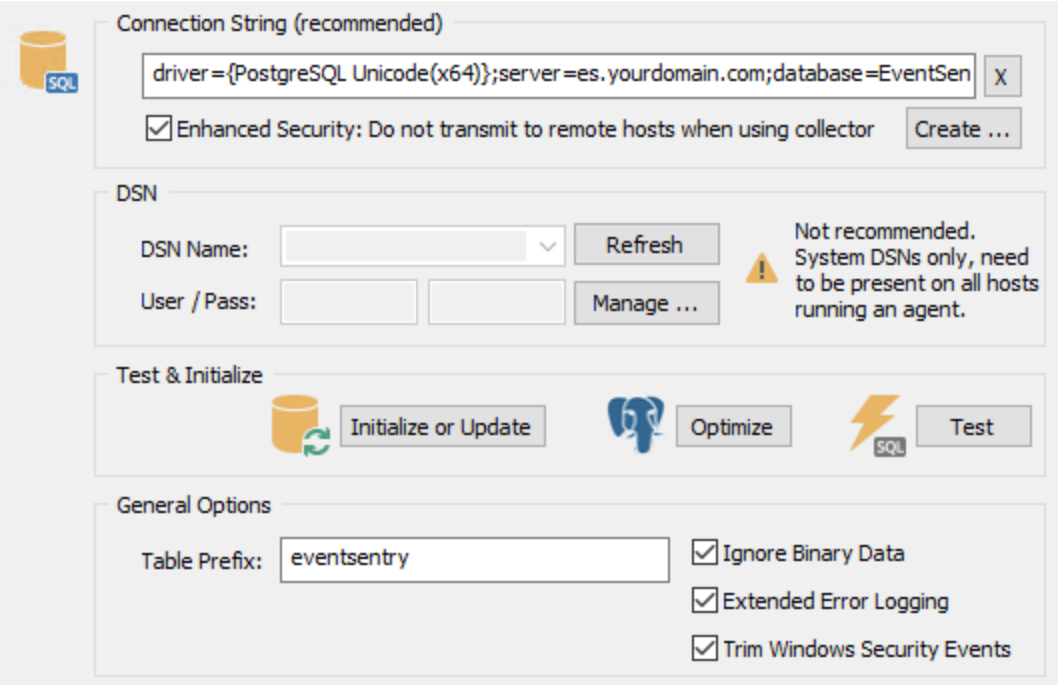
E-Mails, die über einen Collector gesendet werden und Ereignisse von mehr als einem Host enthalten, enthalten eine separate Statuszusammenfassung für jeden Host, der in dieser E-Mail enthalten ist.

4.4.5 Datenbank

EventSentry kann Ereignisprotokollaufzeichnungen über ODBC an jeden unterstützten Datenbankserver senden. "Connection Strings" sind der empfohlene Weg, um die Aktion auf eine Datenbank zu verweisen.

Unter Schritte zur Ereignisprotokollkonsolidierung finden Sie Informationen darüber, wie Sie Ereignisprotokollsätze konsolidieren.

Verwenden Sie das Datenbank-Import-Dienstprogramm, um archivierte Ereignisprotokollsicherungen (.evt/.evtx) oder Protokolldateien in eine Datenbank zu importieren.



Connection Strings

Anwendungen können entweder Connection Strings oder einen System-DSN (Datenquellenname) verwenden, um eine Verbindung zu einer Datenbank herzustellen. Ersteres ist einfacher zu implementieren, da Sie nicht auf jedem Host eine DSN erstellen (und warten) müssen.

Um einen Connection String zu erstellen, verweisen Sie entweder auf Ihre:

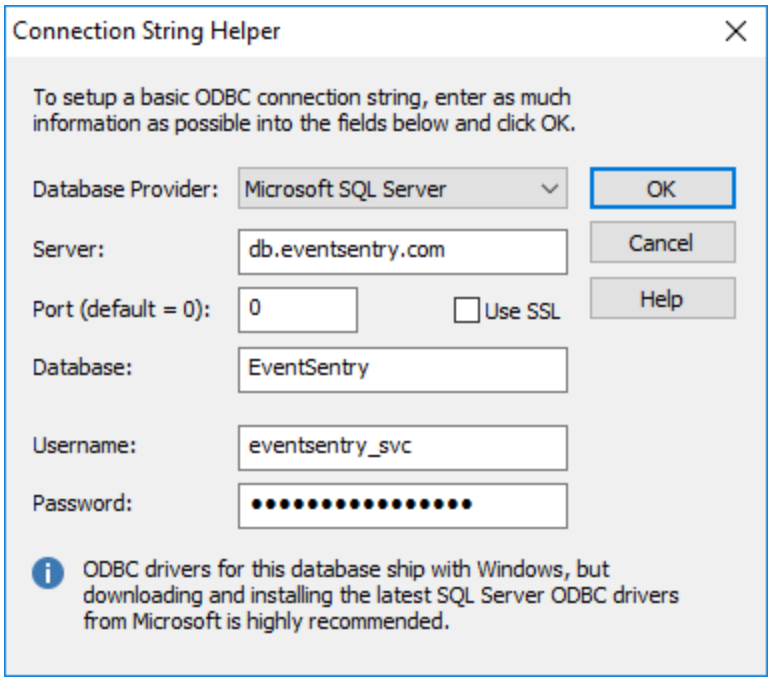
- Dokumentation von Datenbankanbietern
- Eine Online-Ressource (z.B. http://www.connectionstrings.com)
- Verwenden Sie den integrierten Connection String Helper, indem Sie auf **Create** klicken

Der **Connection String Helper** richtet automatisch einen Connection String für unterstützte Datenbanken ein, Sie müssen nur die erforderlichen Parameter angeben. Wenn zusätzliche Informationen benötigt werden oder die Verbindung nicht funktioniert, bearbeiten Sie bitte die generierte Zeichenfolge im ODBC-Haupt-Dialogfeld manuell.

Erhöhte Sicherheit

Durch Aktivieren dieses Kontrollkästchens wird verhindert, dass die Details der Verbindung (z.Bsp. Passwort) an die Remote-Agenten übertragen werden. Dieses Kontrollkästchen sollte **nur aktiviert werden, wenn ein Collector konfiguriert ist**, da die Remote-Agenten sonst keine Verbindung zur Datenbank herstellen können.

Wenn auf einem oder mehreren Remote-Hosts ein anderer EventSentry-Dienst als der Überwachungs-Agent (z. B. Heartbeat-Agent, Netzwerkdienst) ausgeführt wird, müssen die Hosts, auf denen diese Dienste ausgeführt werden, als "Trusted Host" (vertrauenswürdiger Host) konfiguriert werden. "Trusted Hosts" erhalten die vollständigen Connection String-Details, auch wenn erhöhte Sicherheit aktiviert ist. Um einen Host als vertrauenswürdig zu konfigurieren, klicken Sie mit der rechten Maustaste auf das Host-Element in der Computergruppe, klicken Sie auf "Bearbeiten" und aktivieren Sie das Kontrollkästchen "Trusted Host".



Nachdem Sie eine Verbindung zu Ihrem Datenbankserver eingerichtet haben, klicken Sie auf die Schaltfläche **Initialize or Update Database**, um die Datenbank und das Schema zu erstellen.

DSN-Name

Als Alternative zu Verbindungszeichenketten können Sie auch System-DSN-Namen verwenden, um eine Verbindung zu einer Datenbank herzustellen. Geben Sie den Namen eines **System-DSN** ein. Weitere Informationen zu DSN-Namen finden Sie unter Best Practices. Der hier angegebene DSN-Name muss **auf jedem Host**, der diese Aktion verwendet, **vorhanden sein** (siehe auch: Fehlerbehebung).

Sie können nicht sowohl einen DSN als auch einen Connection String angeben.

Benutzername/Passwort

Wenn Ihre Datenquelle ein Login erfordert, geben Sie Benutzername und Passwort an. Für weitere Informationen über Benutzername und Passwörter lesen Sie bitte auch Best Practices.

Verwalten von ODBC

Wenn Sie auf diese Schaltfläche klicken, wird der **Datenquellen-Administrator** aufgerufen, eine integrierte Anwendung, die mit Windows geliefert wird und Ihnen die Konfiguration von System- und Benutzer-DSNs ermöglicht. Beachten Sie, dass diese Schaltfläche nur aktiv ist, wenn Sie mit dem lokalen Rechner verbunden sind.

Datenbank initialisieren oder aktualisieren

Startet den Konfigurations-Assistenten, der entweder eine neue Datenbank erstellt oder eine bestehende Datenbank auf das neueste Schema (gemäß schema.xml) aktualisiert. Das Starten des Konfigurations-Assistenten ist nur erforderlich, wenn eine neue EventSentry-Aktion erstellt wird oder wenn der Konfigurations-Assistent bei einem Upgrade eine weitere Datenbank nicht aktualisiert hat.

PostgreSQL Optimization

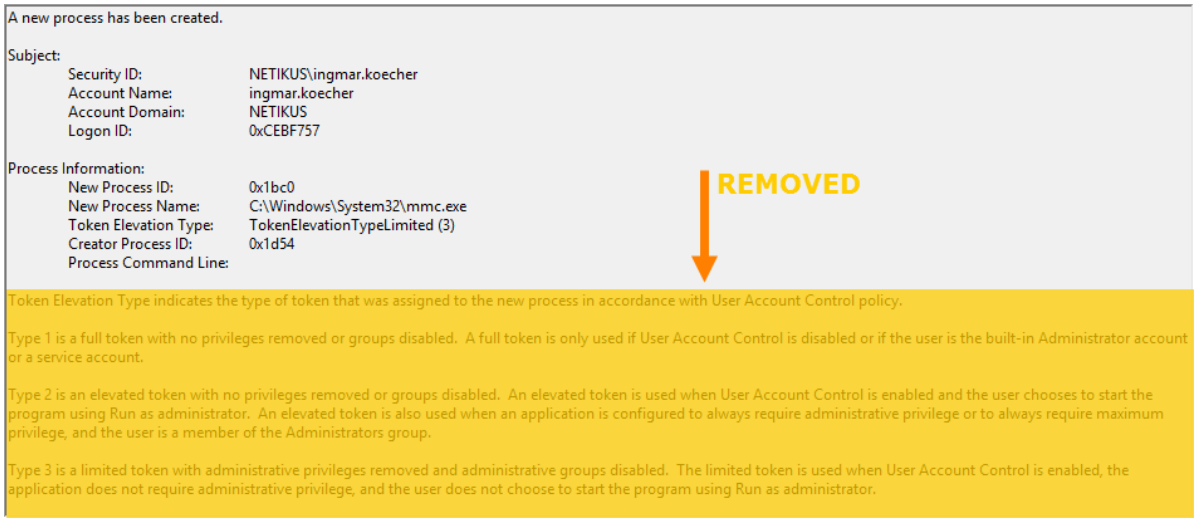
Startet den PostgreSQL-Optimization Dialog, der die Optimierung der integrierten Datenbank vereinfacht.

Allgemeine Optionen

Binäre Daten ignorieren
Einige Ereignisse, normalerweise entweder aus dem Anwendungs- oder Systemereignisprotokoll, sind mit Binärdaten verknüpft. Wenn Sie nicht daran interessiert sind, Binärdaten in der Datenbank zu konsolidieren, können Sie dieses Kontrollkästchen aktivieren.

Erweiterte Fehlerprotokollierung
Standardmäßig protokolliert der EventSentry-Agent nur verbindungsbezogene Datenbankprobleme im Ereignisprotokoll. Wenn Sie die erweiterte Fehlerprotokollierung aktivieren, werden die meisten Datenbankfehler periodisch im Ereignisprotokoll protokolliert.

Trimmen von Windows-Sicherheitsereignissen
Viele Windows-Sicherheitsereignisse enthalten nach den Ereignisdetails nicht unbedingt notwendige Beschreibungen. Diese Beschreibungen sind für alle Ereignisse der gleichen Ereignis-ID identisch und können beträchtlichen Platz in einer Datenbank beanspruchen. Wenn Sie diese Option aktivieren, werden diese Beschreibungen automatisch aus dem Ereignis entfernt, bevor sie in der Datenbank protokolliert werden. Die Ereignisbeschreibungen bleiben für alle anderen Benachrichtigungsarten, z.B. E-Mail, bestehen. Der untenstehende Screenshot zeigt, welche Art von Informationen aufgrund des Windows-Sicherheitsereignisses 4688, das protokolliert wird, wenn ein neuer Prozess gestartet wird, aus dem Ereignis entfernt wird:



Immer binäre Daten anhängen - NUR FÜR REGISTRIERENDE UND ERWEITERTE BENUTZER
In einigen Fällen, insbesondere bei der Verarbeitung großer Mengen an **großen**, **eindeutigen** und **sich nicht wiederholenden** Binärdaten, können die EventSentry-Agenten eine erhebliche Belastung für den Datenbankserver darstellen, wenn die Größe der ESEventlogData-Tabelle zu groß wird. Alle Binärdaten werden in dieser Nachschlagetabelle gespeichert, und der Agent versucht, vorhandene Zeilen in dieser Tabelle wiederzuverwenden, wenn er auf doppelte Binärdaten stößt, was im Allgemeinen der Fall ist.

Wenn Sie große Mengen an eindeutigen Binärdaten erwarten, können Sie dieses Problem vermeiden, indem Sie verhindern, dass der EventSentry-Agent Binäreinträge wiederverwendet und stattdessen Binärdaten an die Tabelle **ESEventlogData** anhängt. Dadurch wird dem Datenbankserver weniger Arbeit

aufgebürdet, da die Tabelle **ESEventlogData** nicht mehr so oft abgefragt werden muss (sie muss nach wie vor für jeden Binäreintrag einmal abgefragt werden).

Um diese Option zu aktivieren:

- Deaktivieren Sie das Kontrollkästchen "Ignoriere Binärdaten", wenn es markiert ist
- Schließen Sie die Verwaltungskonsole
- Starten Sie **regedit.exe** und navigieren Sie zu der Registrierung der Aktion, für die Sie diese aktivieren möchten:

`HKEY_LOCAL_MACHINE\Software\WOW6432Node\netikus.net\EventSentry\Targets\MY DATABASE`

wobei **MYDATABASE** der Name Ihrer Datenbankaktion ist. Fügen Sie dort einen neuen DWORD-Wert mit dem Namen **ODBC_AlwaysAppendBinaryData** hinzu und setzen Sie den Wert auf **1**.

Klicken Sie hier, um einen Eintrag der Häufig gestellten Fragen zu dieser Aktion anzuzeigen.

4.4.5.1 Einrichten der Datenbank

EventSentry verwendet eine Reihe von Tabellen, in denen Ereignisprotokoll-, Systemzustands-, Protokolldatei- und "Sicherheit & Konformität"-Informationen gespeichert werden.

Die Datenbank wird nach der Installation durch den Konfigurationsassistenten automatisch eingerichtet. Sie können den Konfigurationsassistenten auch jederzeit ausführen, um eine vorhandene Datenbank auf das neueste Schema zu aktualisieren. Sie können den Konfigurationsassistenten auch aus dem Aktionsdialog heraus starten, indem Sie auf die Schaltfläche "Initialize or Update Database" klicken.

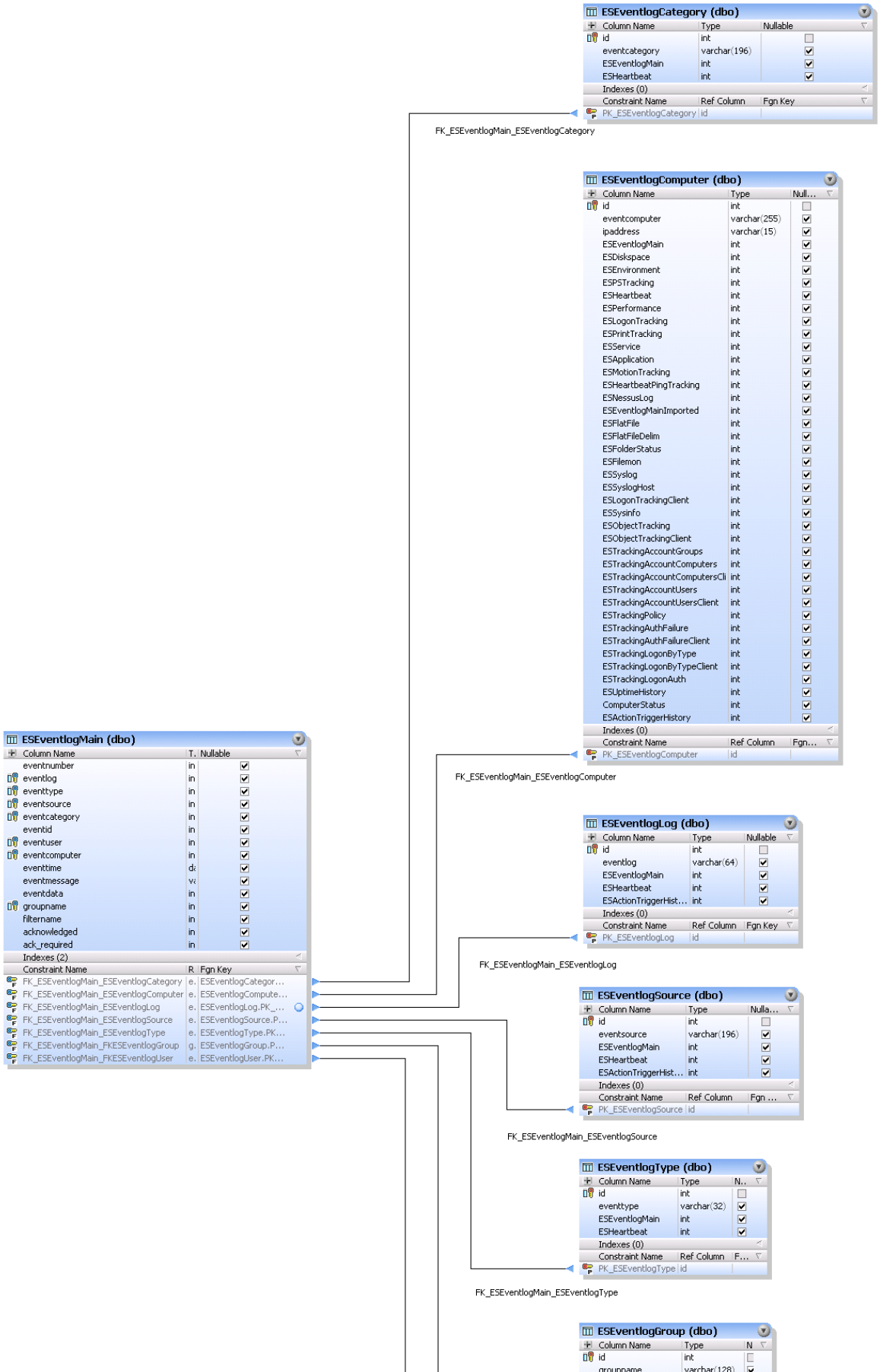
Informationen zur Sicherheit: Sowohl der Benutzername als auch das Passwort werden derzeit im Klartext in die Registry geschrieben. Standardmäßig sind aber die EventSentry Registrierungsschlüssel **nur für Administratoren zugänglich**.

4.4.5.2 Datenbank-Schema

Die EventSentry Datenbank verwendet Dutzende von Tabellen, um alle gesammelten Informationen zu speichern, und fast alle Tabellen sind miteinander verknüpft.

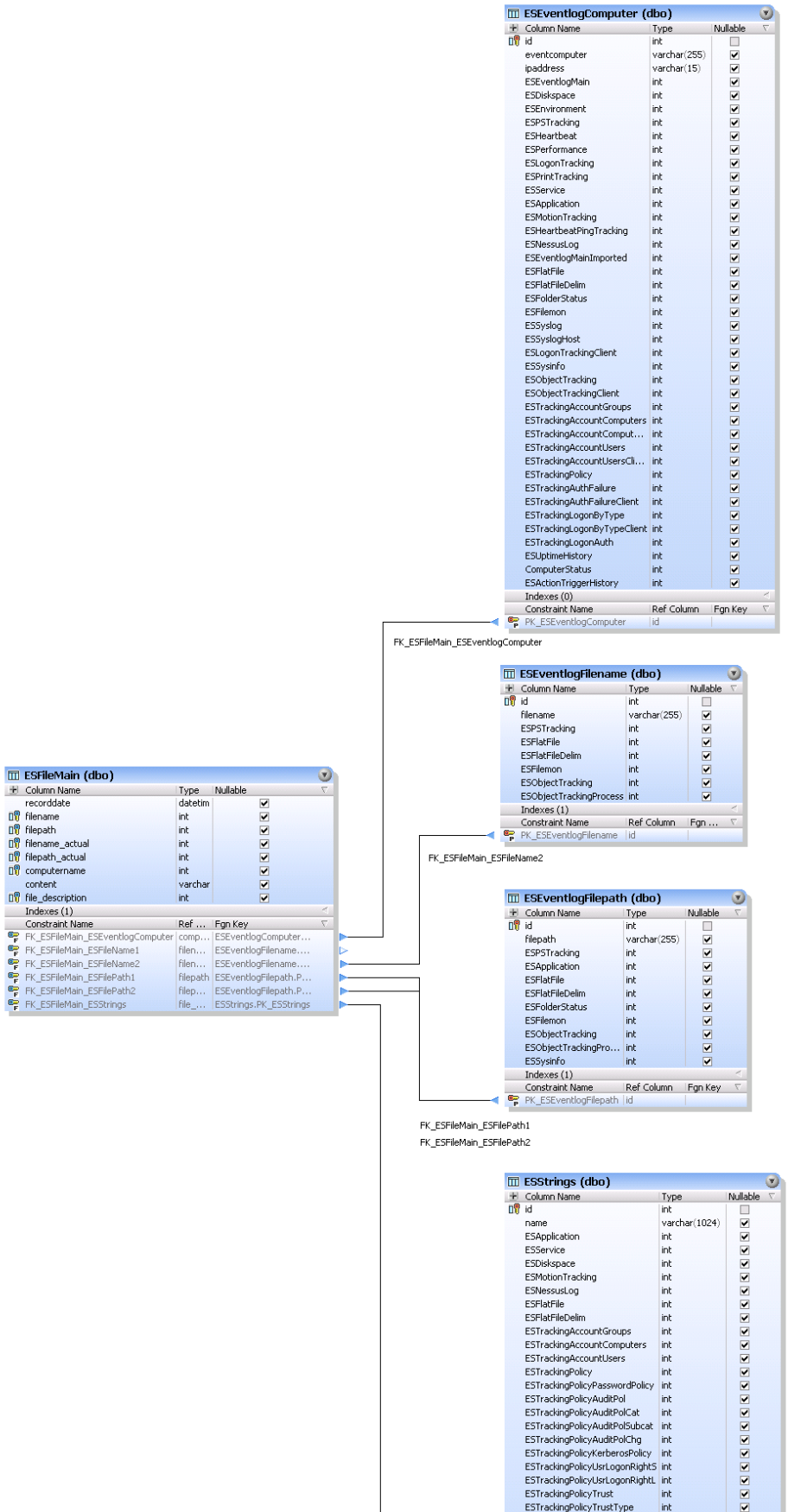
Wenn Sie beabsichtigen, (Berichts-)Anwendungen von Drittanbietern zu verwenden, um Informationen aus unserer Datenbank zu lesen, dann ist es wichtig, diese Beziehungen zu verstehen. Auf den folgenden Seiten finden Sie eine grafische Darstellung aller Tabellen und ihrer Beziehungen.

4.4.5.2.1 Event Log Consolidation

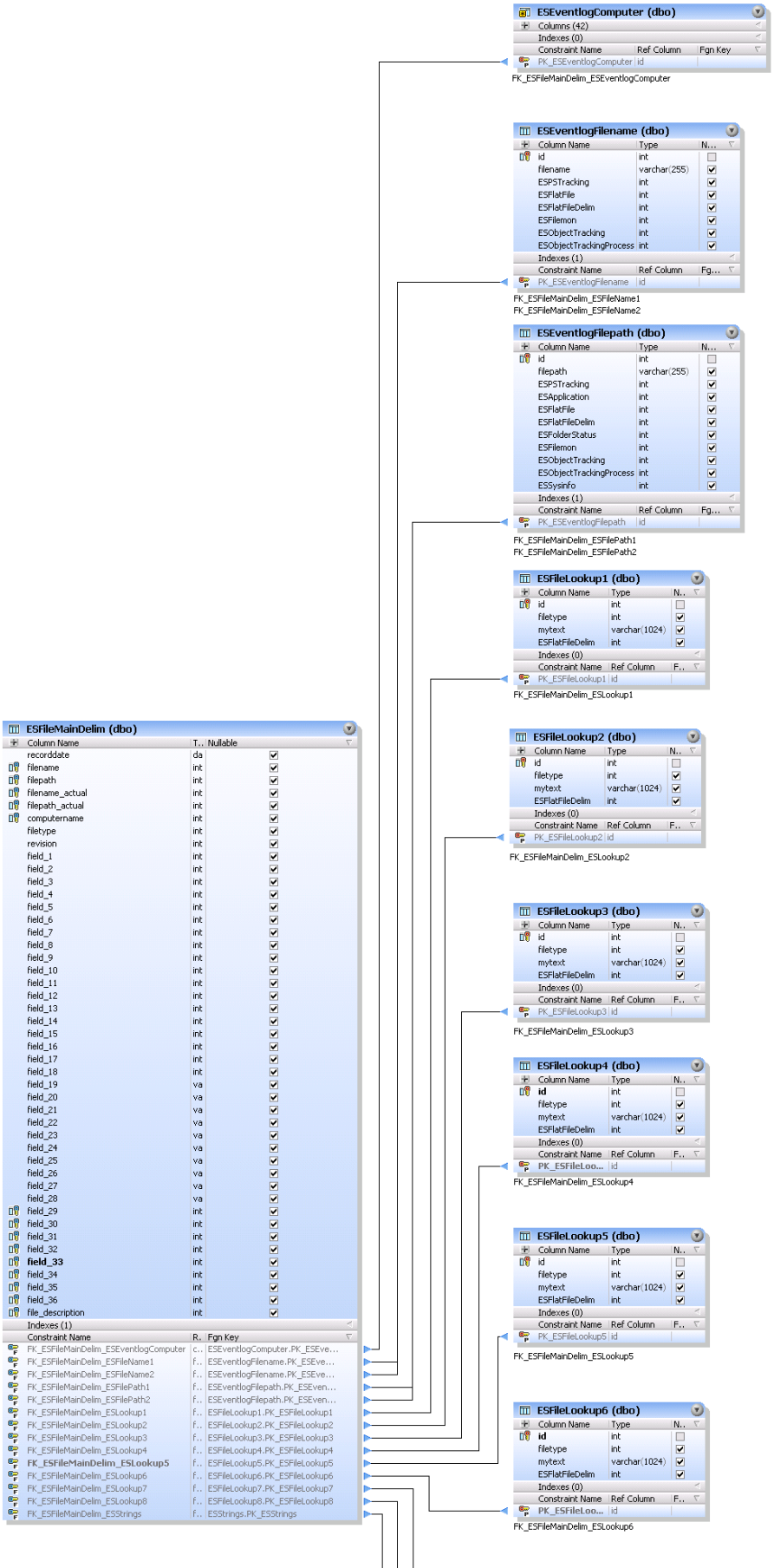


4.4.5.2.2 Log File Monitoring

4.4.5.2.2.1 Non-Delimited Log Files

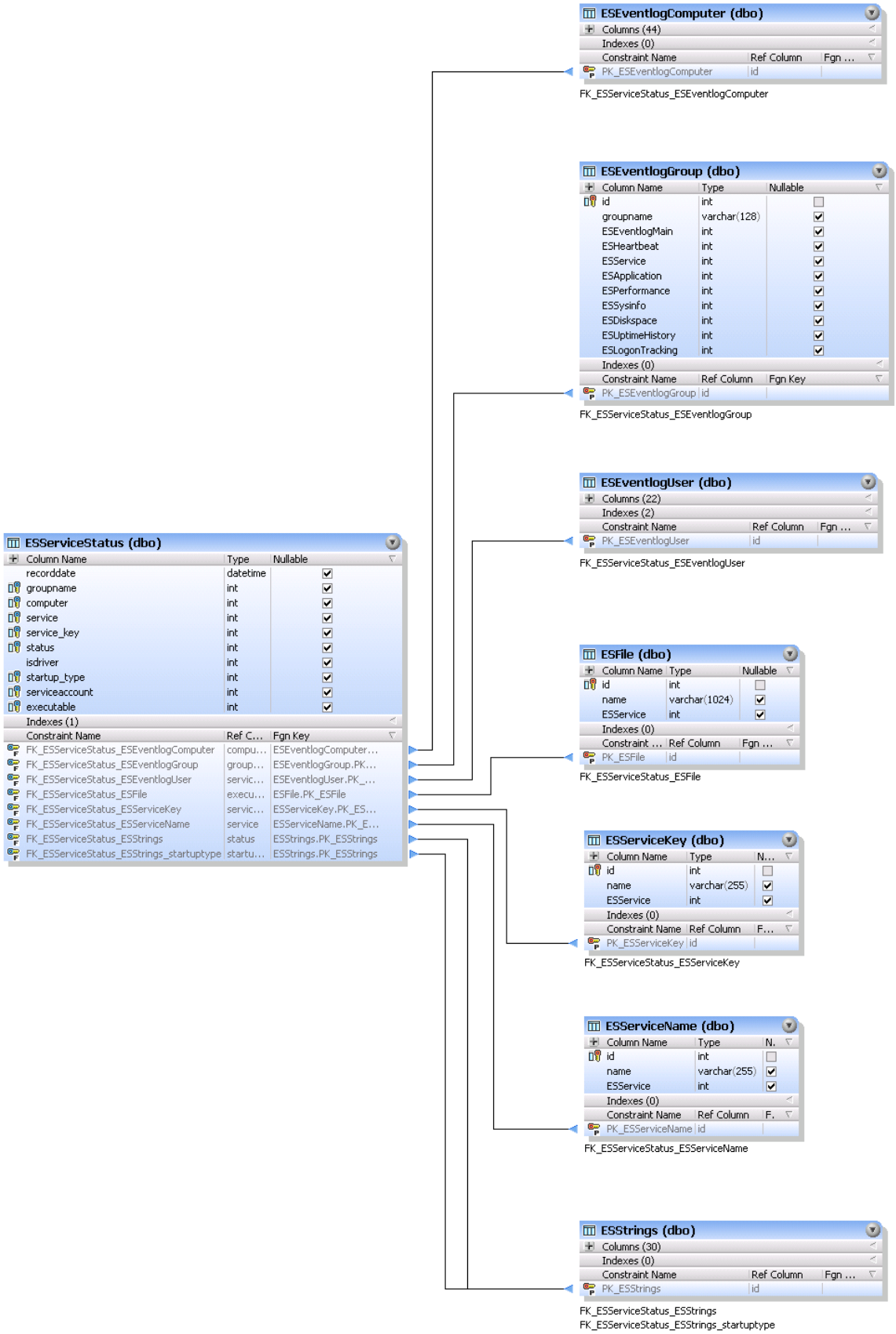


4.4.5.2.2.2 Delimited Log Files

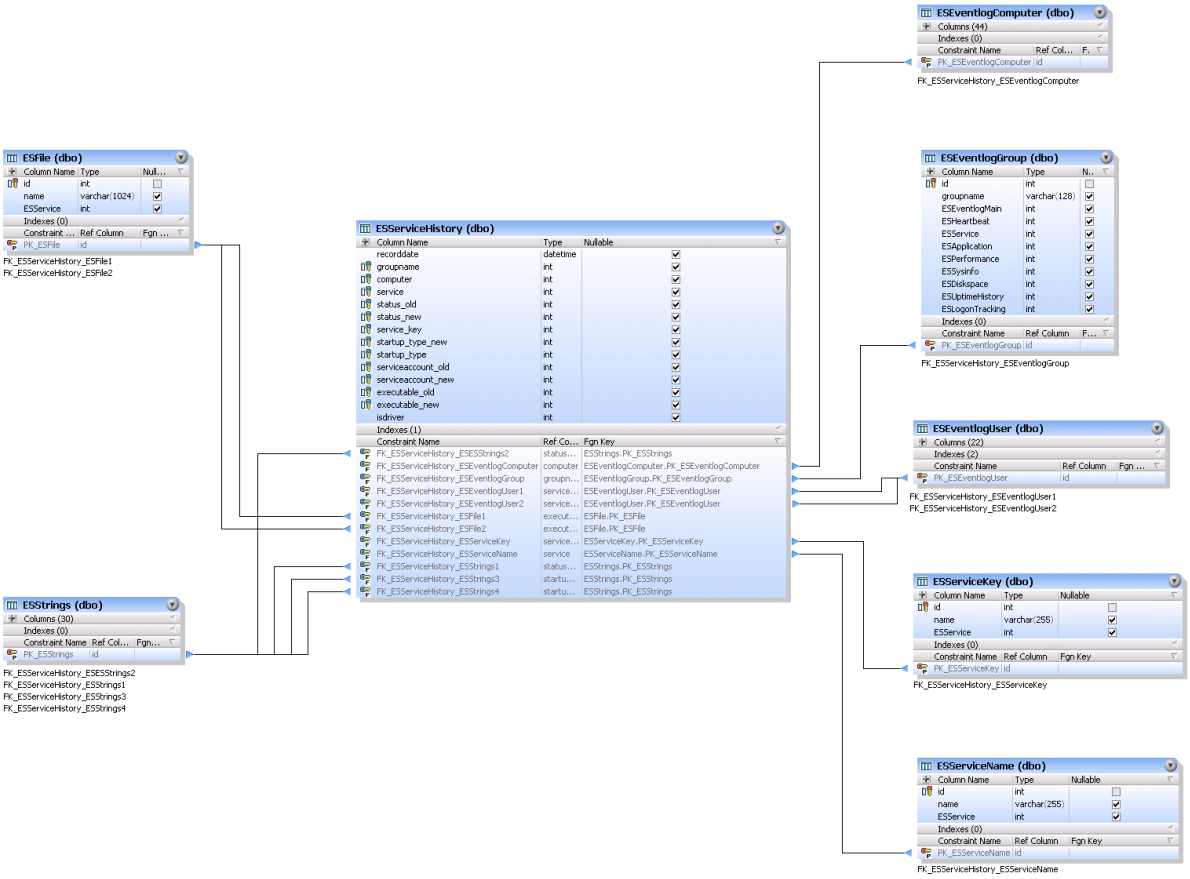


4.4.5.2.3 Service Monitoring

4.4.5.2.3.1 Service Status

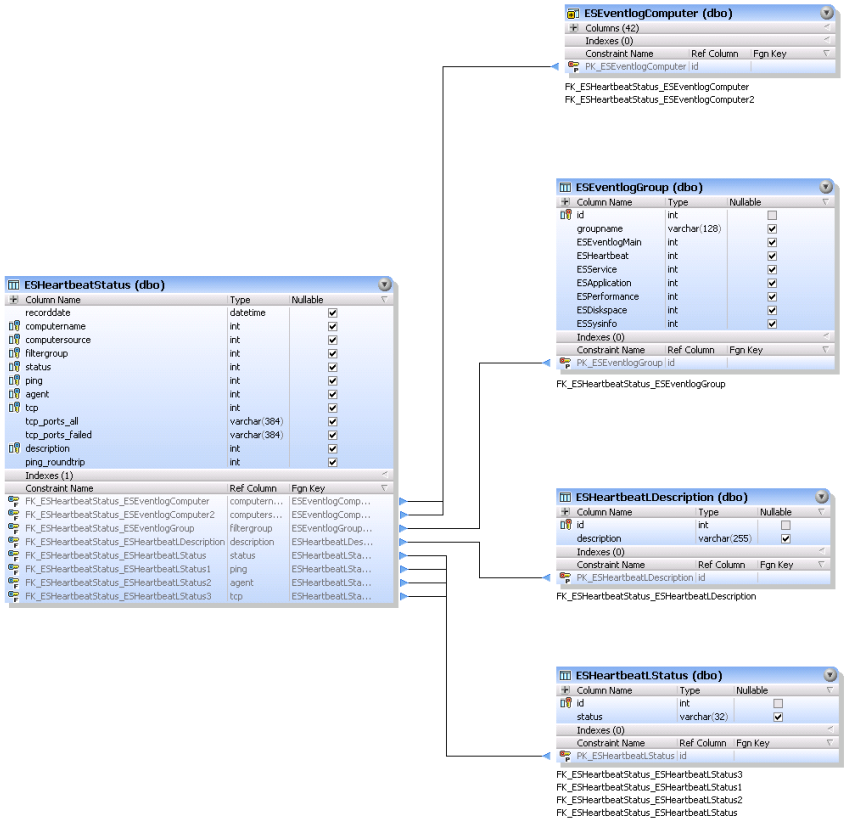


4.4.5.2.3.2 Service History



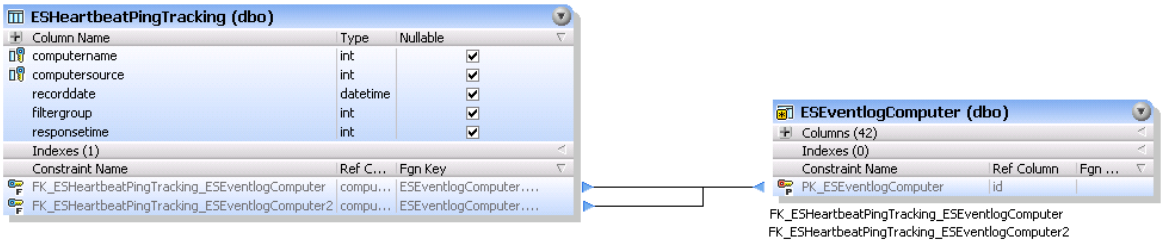
4.4.5.2.4 Heartbeat Monitoring

4.4.5.2.4.1 Heartbeat Status

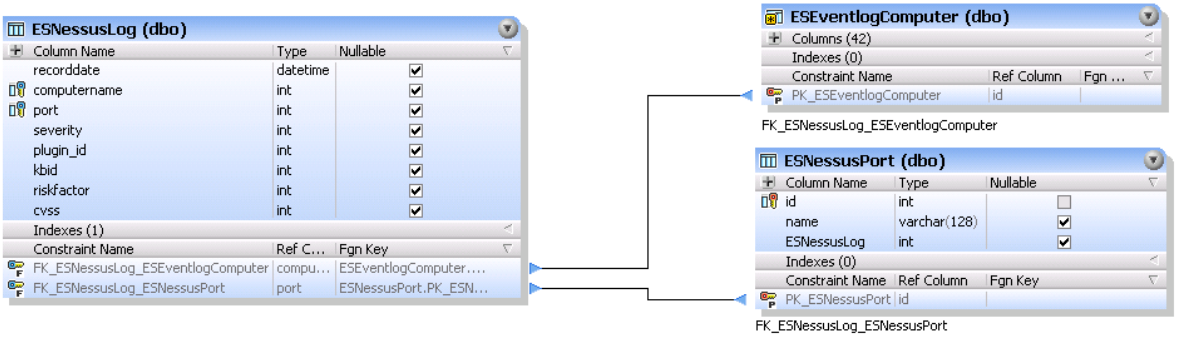


4.4.5.2.4.2 Heartbeat History

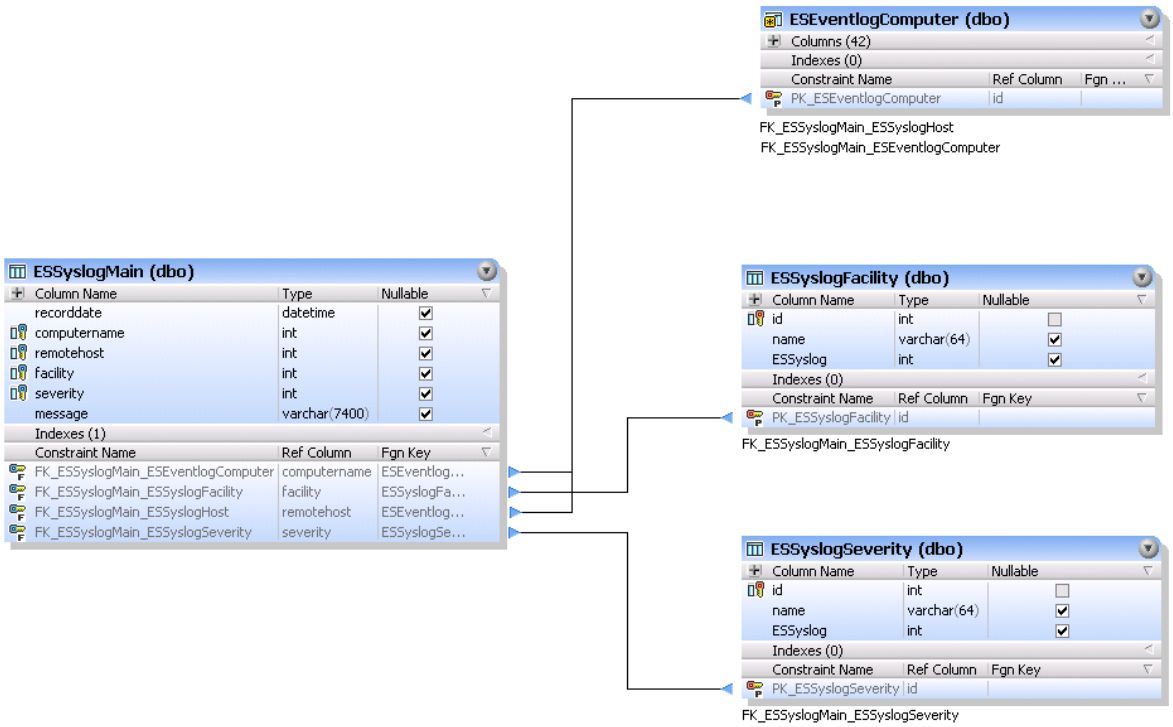
4.4.5.2.4.3 Heartbeat Response Times



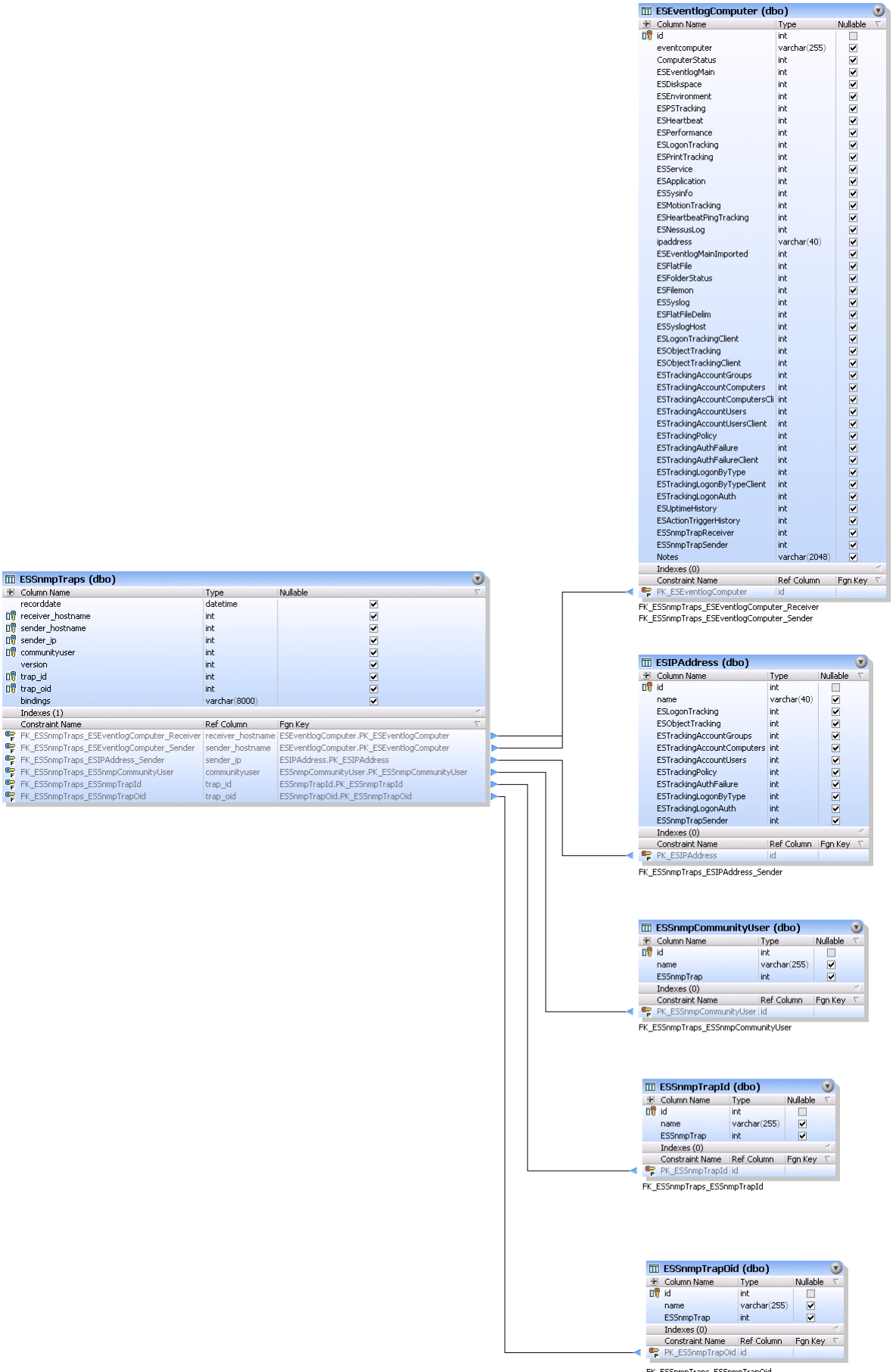
4.4.5.2.5 Nessus



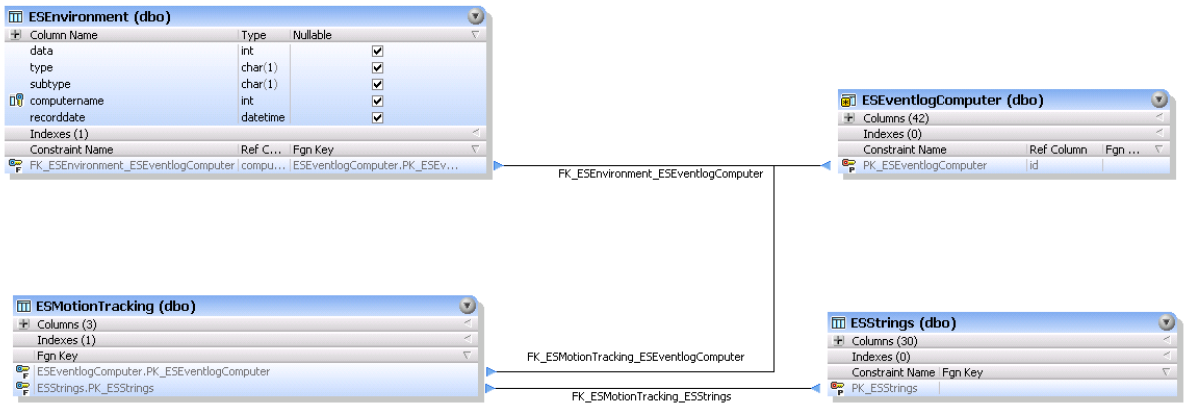
4.4.5.2.6 Syslog



4.4.5.2.7 Snmp

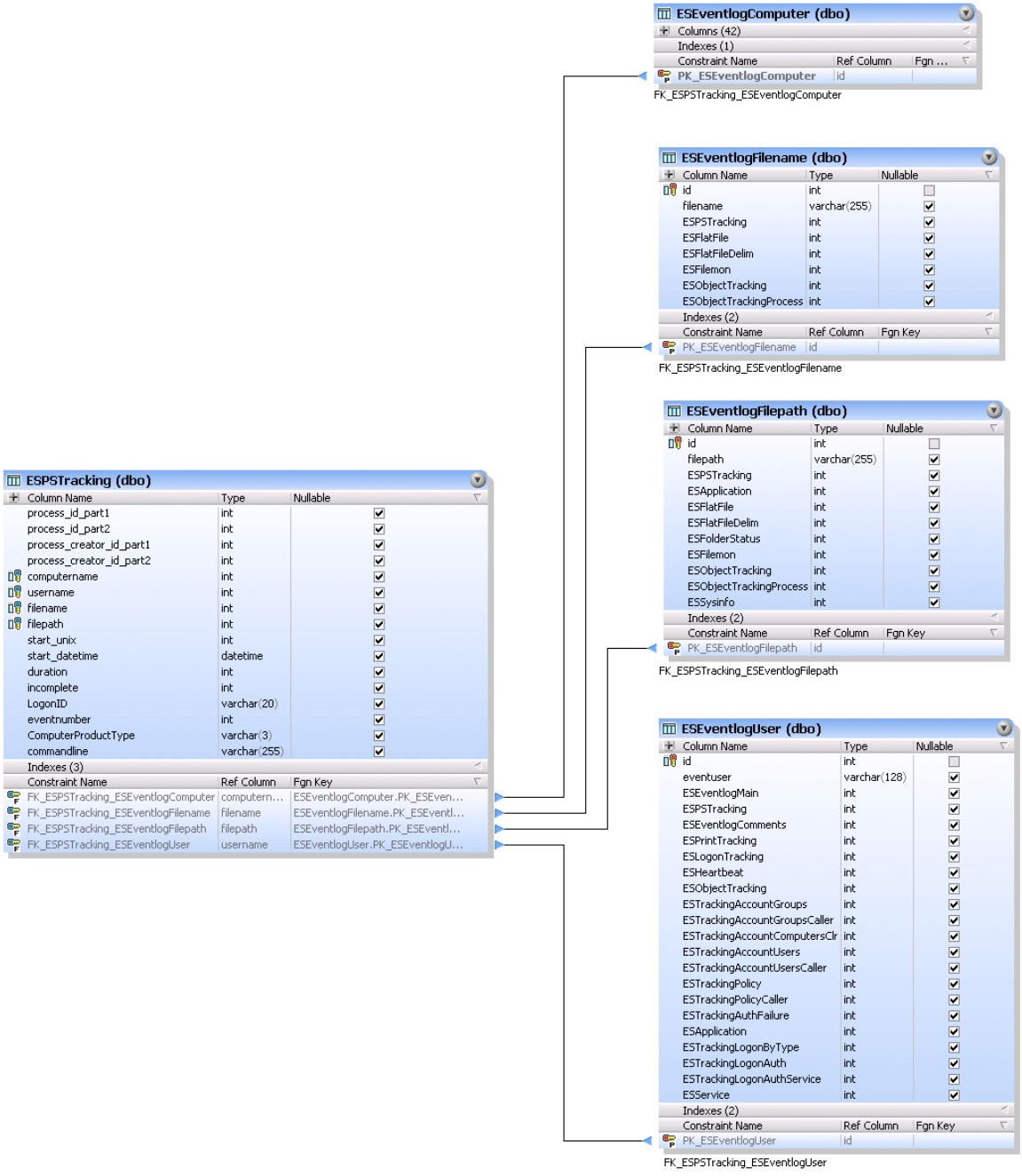

ESEventlogComputer (dbo)
Column Name Type Nullable
id int
eventcomputer varchar(255)
ComputerStatus int
ESEventlogMain int
ESDiskspace int
ESEnvironment int
ESPSTracking int
ESHeartbeat int
ESPerformance int
ESLogonTracking int
ESPrintTracking int
ESService int
ESApplication int
ESSysinfo int
ESMotionTracking int
ESHeartbeatPingTracking int
ESNessusLog int
ipaddress varchar(40)
ESEventlogMainImported int
ESFlatFile int
ESFolderStatus int
ESFilemon int
ESSyslog int
ESFlatFileDelim int
ESSyslogHost int
ESLogonTrackingClient int
ESObjectTracking int
ESObjectTrackingClient int
ESTrackingAccountGroups int
ESTrackingAccountComputers int
ESTrackingAccountComputersCli int
ESTrackingAccountUsers int
ESTrackingAccountUsersClient int
ESTrackingPolicy int
ESTrackingAuthFailure int
ESTrackingAuthFailureClient int
ESTrackingLogonByType int
ESTrackingLogonByTypeClient int
ESTrackingLogonAuth int
ESUptimeHistory int
ESActionTriggerHistory int
ESSnmpTrapReceiver int
ESSnmpTrapSender int
Notes varchar(2048)
Indexes (0)
Constraint Name Ref Column Fgn Key
PK_ESEventlogComputer id
FK_ESSnmpTraps_ESEventlogComputer_Receiver
FK_ESSnmpTraps_ESEventlogComputer_Sender
ESSnmpTraps (dbo)
Column Name Type Nullable
recorddate datetime
receiver_hostname int
sender_hostname int
sender_ip int
communityuser int
version int
trap_id int
trap_oid int
bindings varchar(8000)
Indexes (1)
Constraint Name Ref Column Fgn Key
FK_ESSnmpTraps_ESEventlogComputer_Receiver receiver_hostname ESEventlogComputer.PK_ESEventlogComputer
FK_ESSnmpTraps_ESEventlogComputer_Sender sender_hostname ESEventlogComputer.PK_ESEventlogComputer
FK_ESSnmpTraps_ESIPAddress_Sender sender_ip ESIPAddress.PK_ESIPAddress
FK_ESSnmpTraps_ESSnmpCommunityUser communityuser ESSnmpCommunityUser.PK_ESSnmpCommunityUser
FK_ESSnmpTraps_ESSnmpTrapId trap_id ESSnmpTrapId.PK_ESSnmpTrapId
FK_ESSnmpTraps_ESSnmpTrapOid trap_oid ESSnmpTrapOid.PK_ESSnmpTrapOid
ESIPAddress (dbo)
Column Name Type Nullable
id int
name varchar(40)
ESLogonTracking int
ESObjectTracking int
ESTrackingAccountGroups int
ESTrackingAccountComputers int
ESTrackingAccountUsers int
ESTrackingPolicy int
ESTrackingAuthFailure int
ESTrackingLogonByType int
ESTrackingLogonAuth int
ESSnmpTrapSender int
Indexes (0)
Constraint Name Ref Column Fgn Key
PK_ESIPAddress id
FK_ESSnmpTraps_ESIPAddress_Sender
ESSnmpCommunityUser (dbo)
Column Name Type Nullable
id int
name varchar(255)
ESSnmpTrap int
Indexes (0)
Constraint Name Ref Column Fgn Key
PK_ESSnmpCommunityUser id
FK_ESSnmpTraps_ESSnmpCommunityUser
ESSnmpTrapId (dbo)
Column Name Type Nullable
id int
name varchar(255)
ESSnmpTrap int
Indexes (0)
Constraint Name Ref Column Fgn Key
PK_ESSnmpTrapId id
FK_ESSnmpTraps_ESSnmpTrapId
ESSnmpTrapOid (dbo)
Column Name Type Nullable
id int
name varchar(255)
ESSnmpTrap int
Indexes (0)
Constraint Name Ref Column Fgn Key
PK_ESSnmpTrapOid id

4.4.5.2.8 Environment Monitoring

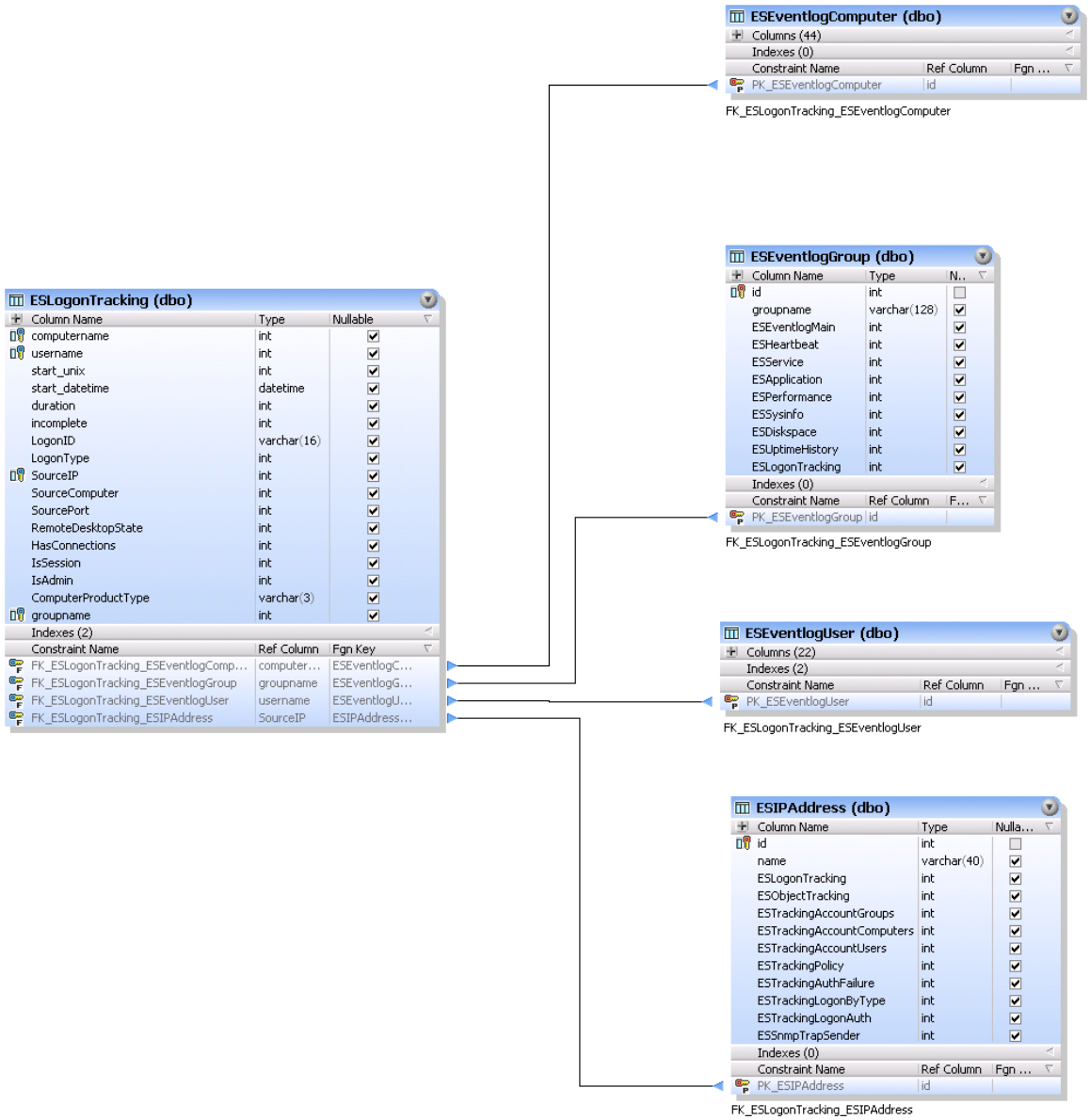


4.4.5.2.9 Compliance Tracking

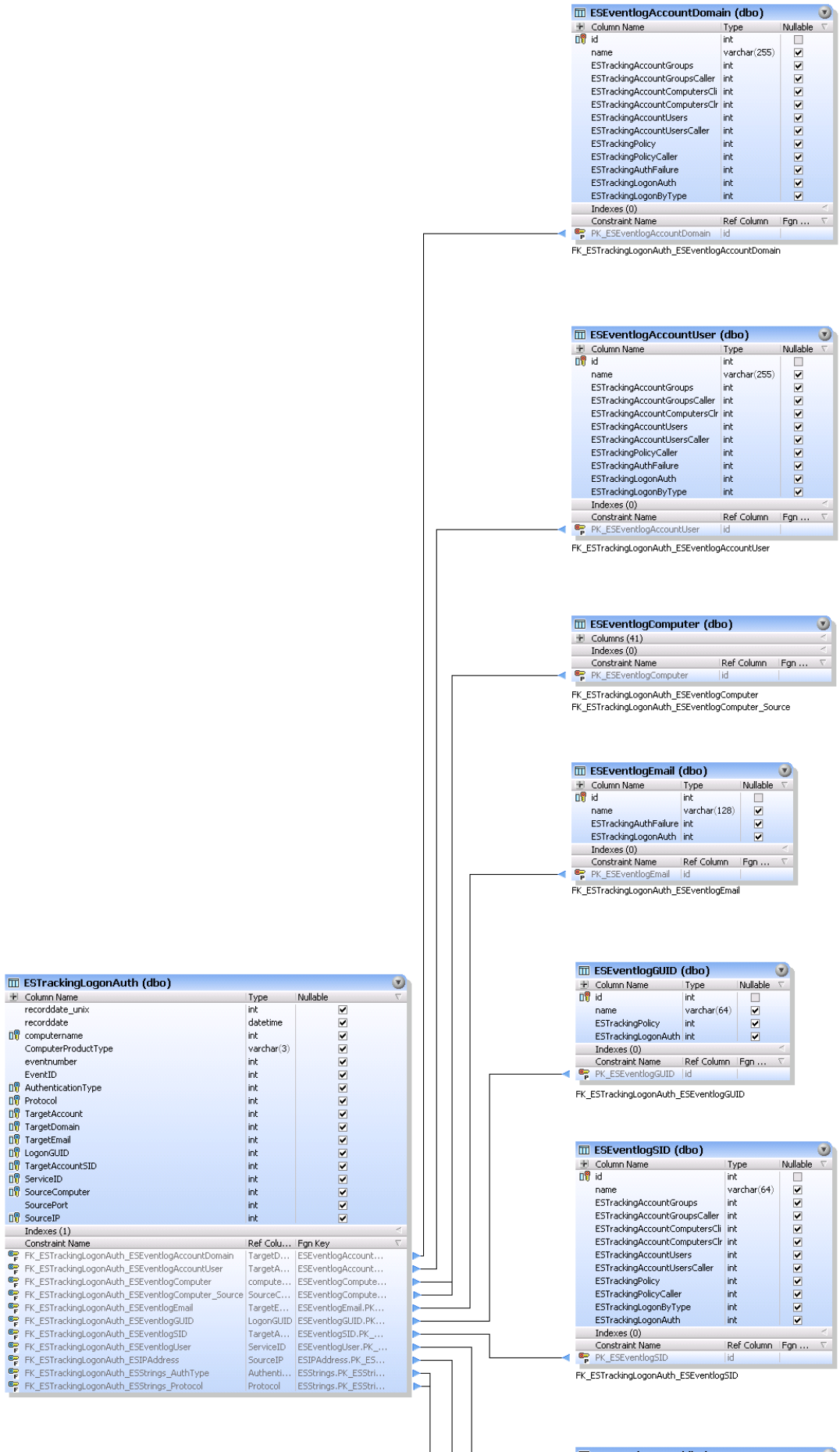
4.4.5.2.9.1 Process Tracking



4.4.5.2.9.2 Logon Tracking

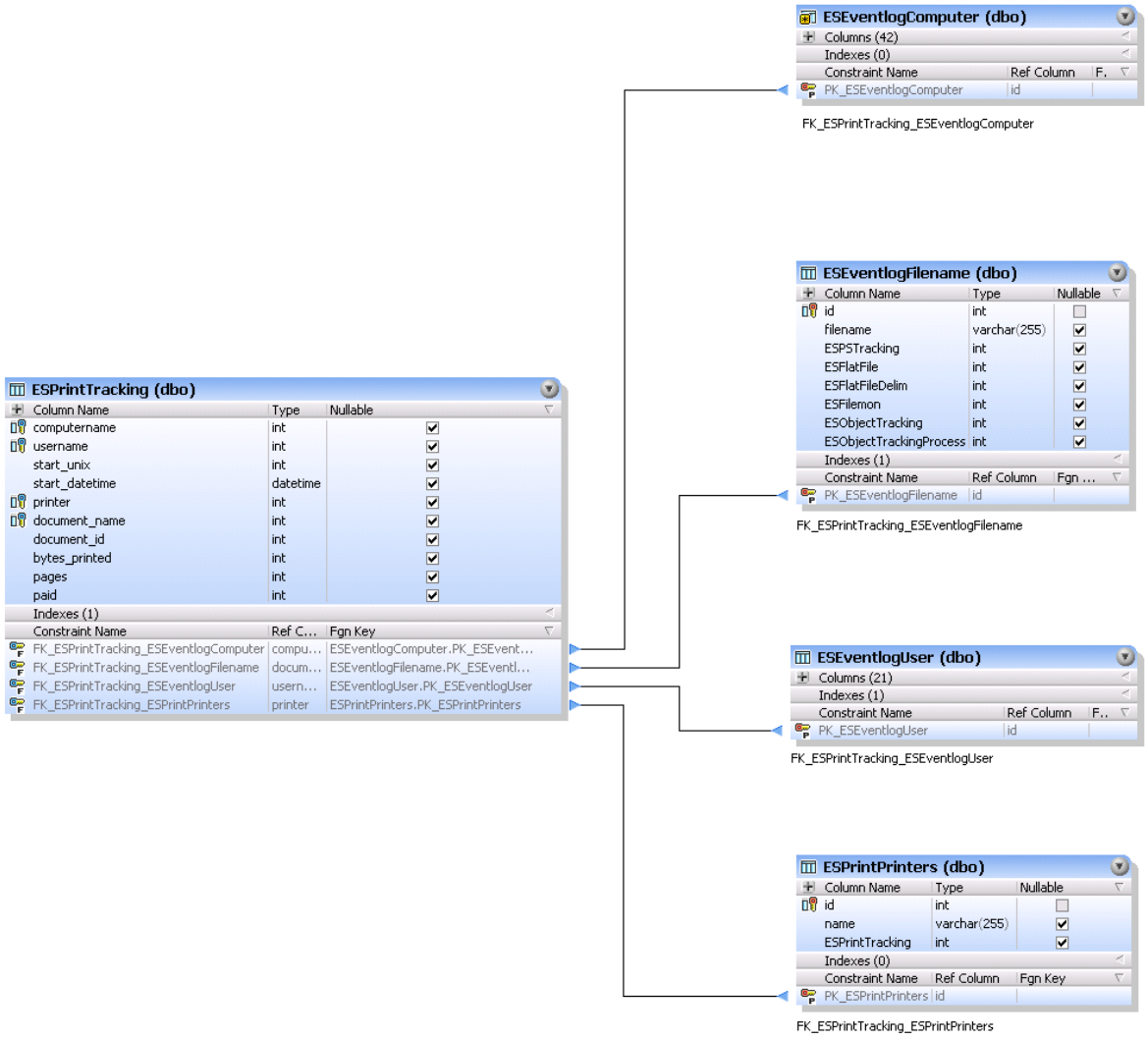



ESEventlogAccountDomain (dbo)
Column Name Type Nullable
id int
name varchar(255)
ESTrackingAccountGroups int
ESTrackingAccountGroupsCaller int
ESTrackingAccountComputersCli int
ESTrackingAccountComputersClr int
ESTrackingAccountUsers int
ESTrackingAccountUsersCaller int
ESTrackingPolicy int
ESTrackingPolicyCaller int
ESTrackingAuthFailure int
ESTrackingLogonAuth int
ESTrackingLogonByType int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogAccountDomain id
FK_ESTrackingAuthFailure_ESEventlogAccountDomain
ESEventlogAccountUser (dbo)
Column Name Type Nullable
id int
name varchar(255)
ESTrackingAccountGroups int
ESTrackingAccountGroupsCaller int
ESTrackingAccountComputersClr int
ESTrackingAccountUsers int
ESTrackingAccountUsersCaller int
ESTrackingPolicyCaller int
ESTrackingAuthFailure int
ESTrackingLogonAuth int
ESTrackingLogonByType int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogAccountUser id
FK_ESTrackingAuthFailure_ESEventlogAccountUser
ESTrackingAuthFailure (dbo)
Column Name Type Nullable
recorddate_unix int
recorddate datetime
computername int
ComputerProductType varchar(3)
eventnumber int
eventid int
Protocol int
AuthenticationType int
SourceComputer int
SourceIP int
SourcePort int
TargetAccount int
TargetDomain int
TargetAccountID int
FailureReason int
FailureReasonNum int
Indexes (1)
Constraint Name Ref Colu... Fgn Key
FK_ESTrackingAuthFailure_ESEventlogAccountDomain TargetD... ESEventlogAcco...
FK_ESTrackingAuthFailure_ESEventlogAccountUser TargetA... ESEventlogAcco...
FK_ESTrackingAuthFailure_ESEventlogComputer compute... ESEventlogCom...
FK_ESTrackingAuthFailure_ESEventlogComputer_Source SourceC... ESEventlogCom...
FK_ESTrackingAuthFailure_ESEventlogUser TargetA... ESEventlogUser...
FK_ESTrackingAuthFailure_ESIPAddress SourceIP ESIPAddress.PK...
FK_ESTrackingAuthFailure_ESStrings_AuthType Authenti... ESStrings.PK_ES...
FK_ESTrackingAuthFailure_ESStrings_FailureReason FailureR... ESStrings.PK_ES...
FK_ESTrackingAuthFailure_ESStrings_Protocol Protocol ESStrings.PK_ES...
ESEventlogComputer (dbo)
Columns (41)
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogComputer id
FK_ESTrackingAuthFailure_ESEventlogComputer
FK_ESTrackingAuthFailure_ESEventlogComputer_Source
ESEventlogUser (dbo)
Column Name Type Nullable
id int
eventuser varchar(128)
ESEventlogMain int
ESPSTracking int
ESEventlogComments int
ESPrintTracking int
ESLogonTracking int
ESHeartbeat int
ESObjectTracking int
ESTrackingAccountGroups int
ESTrackingAccountGroupsCaller int
ESTrackingAccountComputersClr int
ESTrackingAccountUsers int
ESTrackingAccountUsersCaller int
ESTrackingPolicy int
ESTrackingPolicyCaller int
ESTrackingAuthFailure int
ESApplication int
ESTrackingLogonByType int
ESTrackingLogonAuth int
ESTrackingLogonAuthService int
Indexes (1)
Constraint Name Ref Column Fgn ...
PK_ESEventlogUser id
FK_ESTrackingAuthFailure_ESEventlogUser
ESIPAddress (dbo)
Column Name Type Nullable
id int
name varchar(15)
ESLogonTracking int
ESObjectTracking int
ESTrackingAccountGroups int
ESTrackingAccountComputers int
ESTrackingAccountUsers int
ESTrackingPolicy int
ESTrackingAuthFailure int
ESTrackingLogonByType int
ESTrackingLogonAuth int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESIPAddress id
FK_ESTrackingAuthFailure_ESIPAddress
ESStrings (dbo)
Columns (30)

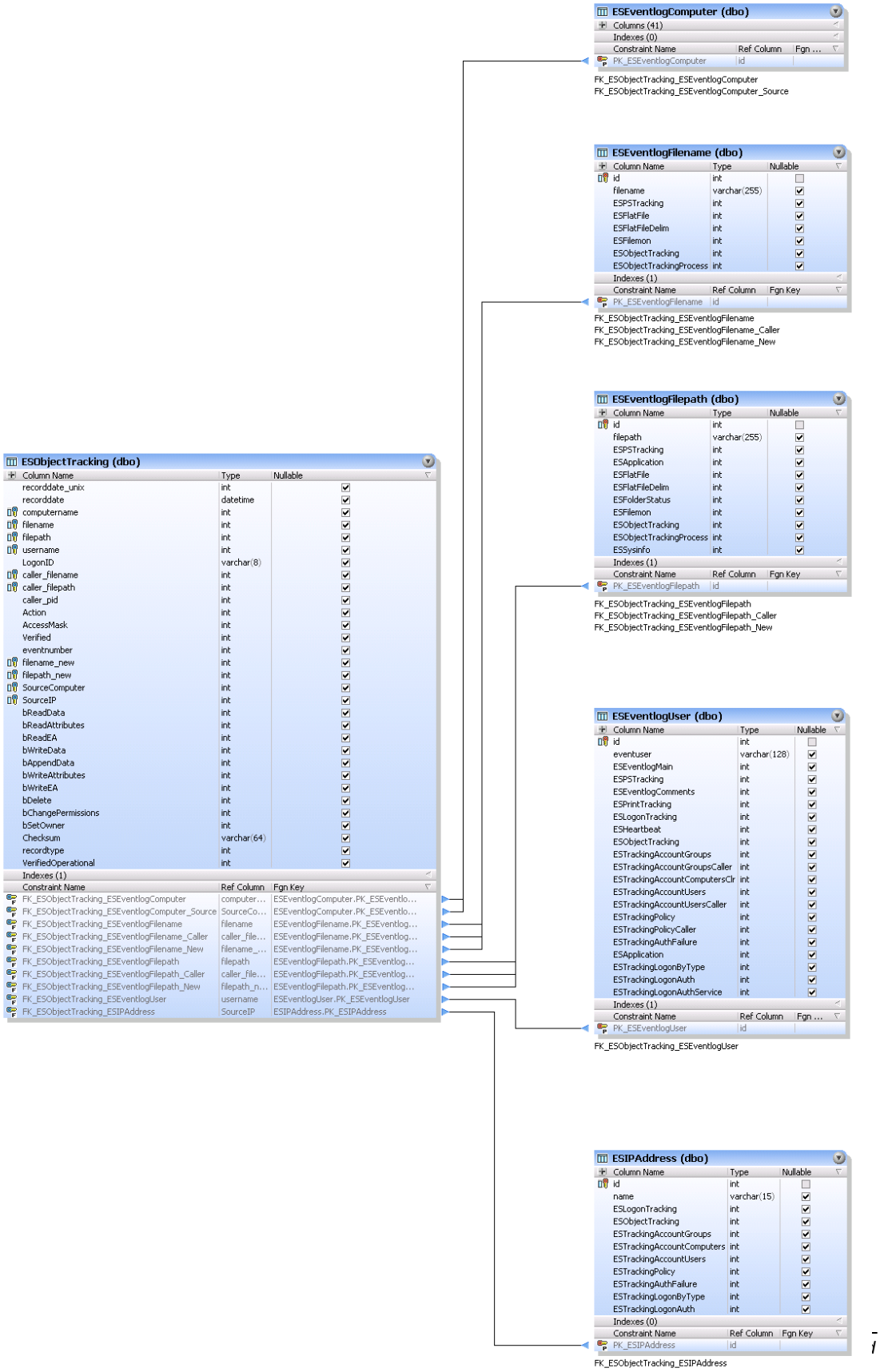

ESEventlogAccountDomain (dbo)
Column Name Type Nullable
id int
name varchar(255)
ESTrackingAccountGroups int
ESTrackingAccountGroupsCaller int
ESTrackingAccountComputersCli int
ESTrackingAccountComputersClr int
ESTrackingAccountUsers int
ESTrackingAccountUsersCaller int
ESTrackingPolicy int
ESTrackingPolicyCaller int
ESTrackingAuthFailure int
ESTrackingLogonAuth int
ESTrackingLogonByType int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogAccountDomain id
FK_ESTrackingLogonAuth_ESEventlogAccountDomain
ESEventlogAccountUser (dbo)
Column Name Type Nullable
id int
name varchar(255)
ESTrackingAccountGroups int
ESTrackingAccountGroupsCaller int
ESTrackingAccountComputersClr int
ESTrackingAccountUsers int
ESTrackingAccountUsersCaller int
ESTrackingPolicyCaller int
ESTrackingAuthFailure int
ESTrackingLogonAuth int
ESTrackingLogonByType int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogAccountUser id
FK_ESTrackingLogonAuth_ESEventlogAccountUser
ESEventlogComputer (dbo)
Columns (41)
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogComputer id
FK_ESTrackingLogonAuth_ESEventlogComputer
FK_ESTrackingLogonAuth_ESEventlogComputer_Source
ESEventlogEmail (dbo)
Column Name Type Nullable
id int
name varchar(128)
ESTrackingAuthFailure int
ESTrackingLogonAuth int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogEmail id
FK_ESTrackingLogonAuth_ESEventlogEmail
ESTrackingLogonAuth (dbo)
Column Name Type Nullable
recorddate_unix int
recorddate datetime
computername int
ComputerProductType varchar(3)
eventnumber int
EventID int
AuthenticationType int
Protocol int
TargetAccount int
TargetDomain int
TargetEmail int
LogonGUID int
TargetAccountSID int
ServiceID int
SourceComputer int
SourcePort int
SourceIP int
Indexes (1)
Constraint Name Ref Colu... Fgn Key
FK_ESTrackingLogonAuth_ESEventlogAccountDomain TargetD... ESEventlogAccount...
FK_ESTrackingLogonAuth_ESEventlogAccountUser TargetA... ESEventlogAccount...
FK_ESTrackingLogonAuth_ESEventlogComputer compute... ESEventlogCompute...
FK_ESTrackingLogonAuth_ESEventlogComputer_Source SourceC... ESEventlogCompute...
FK_ESTrackingLogonAuth_ESEventlogEmail TargetE... ESEventlogEmail.PK...
FK_ESTrackingLogonAuth_ESEventlogGUID LogonGUID ESEventlogGUID.PK...
FK_ESTrackingLogonAuth_ESEventlogSID TargetA... ESEventlogSID.PK_...
FK_ESTrackingLogonAuth_ESEventlogUser ServiceID ESEventlogUser.PK_...
FK_ESTrackingLogonAuth_ESIPAddress SourceIP ESIPAddress.PK_ES...
FK_ESTrackingLogonAuth_ESStrings_AuthType Authenti... ESStrings.PK_ESStri...
FK_ESTrackingLogonAuth_ESStrings_Protocol Protocol ESStrings.PK_ESStri...
ESEventlogGUID (dbo)
Column Name Type Nullable
id int
name varchar(64)
ESTrackingPolicy int
ESTrackingLogonAuth int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogGUID id
FK_ESTrackingLogonAuth_ESEventlogGUID
ESEventlogSID (dbo)
Column Name Type Nullable
id int
name varchar(64)
ESTrackingAccountGroups int
ESTrackingAccountGroupsCaller int
ESTrackingAccountComputersCli int
ESTrackingAccountComputersClr int
ESTrackingAccountUsers int
ESTrackingAccountUsersCaller int
ESTrackingPolicy int
ESTrackingPolicyCaller int
ESTrackingLogonByType int
ESTrackingLogonAuth int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogSID id
FK_ESTrackingLogonAuth_ESEventlogSID


ESEventlogAccountDomain (dbo)
Column Name Type Nullable
id int
name varchar(255)
ESTrackingAccountGroups int
ESTrackingAccountGroupsCaller int
ESTrackingAccountComputersCli int
ESTrackingAccountComputersClr int
ESTrackingAccountUsers int
ESTrackingAccountUsersCaller int
ESTrackingPolicy int
ESTrackingPolicyCaller int
ESTrackingAuthFailure int
ESTrackingLogonAuth int
ESTrackingLogonByType int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogAccountDomain id
FK_ESTrackingLogonByType_ESEventlogAccountDomain
ESEventlogAccountUser (dbo)
Column Name Type Nullable
id int
name varchar(255)
ESTrackingAccountGroups int
ESTrackingAccountGroupsCaller int
ESTrackingAccountComputersClr int
ESTrackingAccountUsers int
ESTrackingAccountUsersCaller int
ESTrackingPolicyCaller int
ESTrackingAuthFailure int
ESTrackingLogonAuth int
ESTrackingLogonByType int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogAccountUser id
FK_ESTrackingLogonByType_ESEventlogAccountUser
ESEventlogComputer (dbo)
Columns (41)
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogComputer id
FK_ESTrackingLogonByType_ESEventlogComputer
FK_ESTrackingLogonByType_ESEventlogComputer_Source
ESTrackingLogonByType (dbo)
Column Name Type Nullable
recorddate_unix int
recorddate datetime
computername int
ComputerProductType varchar(3)
eventnumber int
EventID int
LogonAction int
LogonType int
TargetAccount int
TargetDomain int
TargetAccountID int
TargetAccountSID int
LogonProcess int
LogonID varchar(16)
SourceIP int
SourceComputer int
SourcePort int
FailureReason int
Indexes (1)
Constraint Name Ref Column Fgn Key
FK_ESTrackingLogonByType_ESEventlogAccountDomain TargetDo... ESEventlogAccountDomain.PK_ESEv...
FK_ESTrackingLogonByType_ESEventlogAccountUser TargetAcc... ESEventlogAccountUser.PK_ESEven...
FK_ESTrackingLogonByType_ESEventlogComputer computer... ESEventlogComputer.PK_ESEventlo...
FK_ESTrackingLogonByType_ESEventlogComputer_Source SourceCo... ESEventlogComputer.PK_ESEventlo...
FK_ESTrackingLogonByType_ESEventlogSID TargetAcc... ESEventlogSID.PK_ESEventlogSID
FK_ESTrackingLogonByType_ESEventlogUser TargetAcc... ESEventlogUser.PK_ESEventlogUser
FK_ESTrackingLogonByType_ESIPAddress SourceIP ESIPAddress.PK_ESIPAddress
FK_ESTrackingLogonByType_ESStrings_FailureReason FailureRe... ESStrings.PK_ESStrings
FK_ESTrackingLogonByType_ESStrings_LogonProcess LogonPro... ESStrings.PK_ESStrings
FK_ESTrackingLogonByType_ESStrings_LogonType LogonType ESStrings.PK_ESStrings
ESEventlogSID (dbo)
Column Name Type Nullable
id int
name varchar(64)
ESTrackingAccountGroups int
ESTrackingAccountGroupsCaller int
ESTrackingAccountComputersCli int
ESTrackingAccountComputersClr int
ESTrackingAccountUsers int
ESTrackingAccountUsersCaller int
ESTrackingPolicy int
ESTrackingPolicyCaller int
ESTrackingLogonByType int
ESTrackingLogonAuth int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogSID id
FK_ESTrackingLogonByType_ESEventlogSID
ESEventlogUser (dbo)
Column Name Type Nullable
id int
eventuser varchar(128)
ESEventlogMain int
ESPSTracking int
ESEventlogComments int
ESPrintTracking int
ESLogonTracking int
ESHeartbeat int
ESObjectTracking int
ESTrackingAccountGroups int
ESTrackingAccountGroupsCaller int
ESTrackingAccountComputersClr int
ESTrackingAccountUsers int
ESTrackingAccountUsersCaller int
ESTrackingPolicy int
ESTrackingPolicyCaller int
ESTrackingAuthFailure int
ESApplication int
ESTrackingLogonByType int
ESTrackingLogonAuth int
ESTrackingLogonAuthService int
Indexes (1)
Constraint Name Ref Column Fgn ...
PK_ESEventlogUser id
FK_ESTrackingLogonByType_ESEventlogUser
ESIPAddress (dbo)
Column Name Type Nullable
id int
name varchar(15)
ESLogonTracking int
ESObjectTracking int
ESTrackingAccountGroups int
ESTrackingAccountComputers int

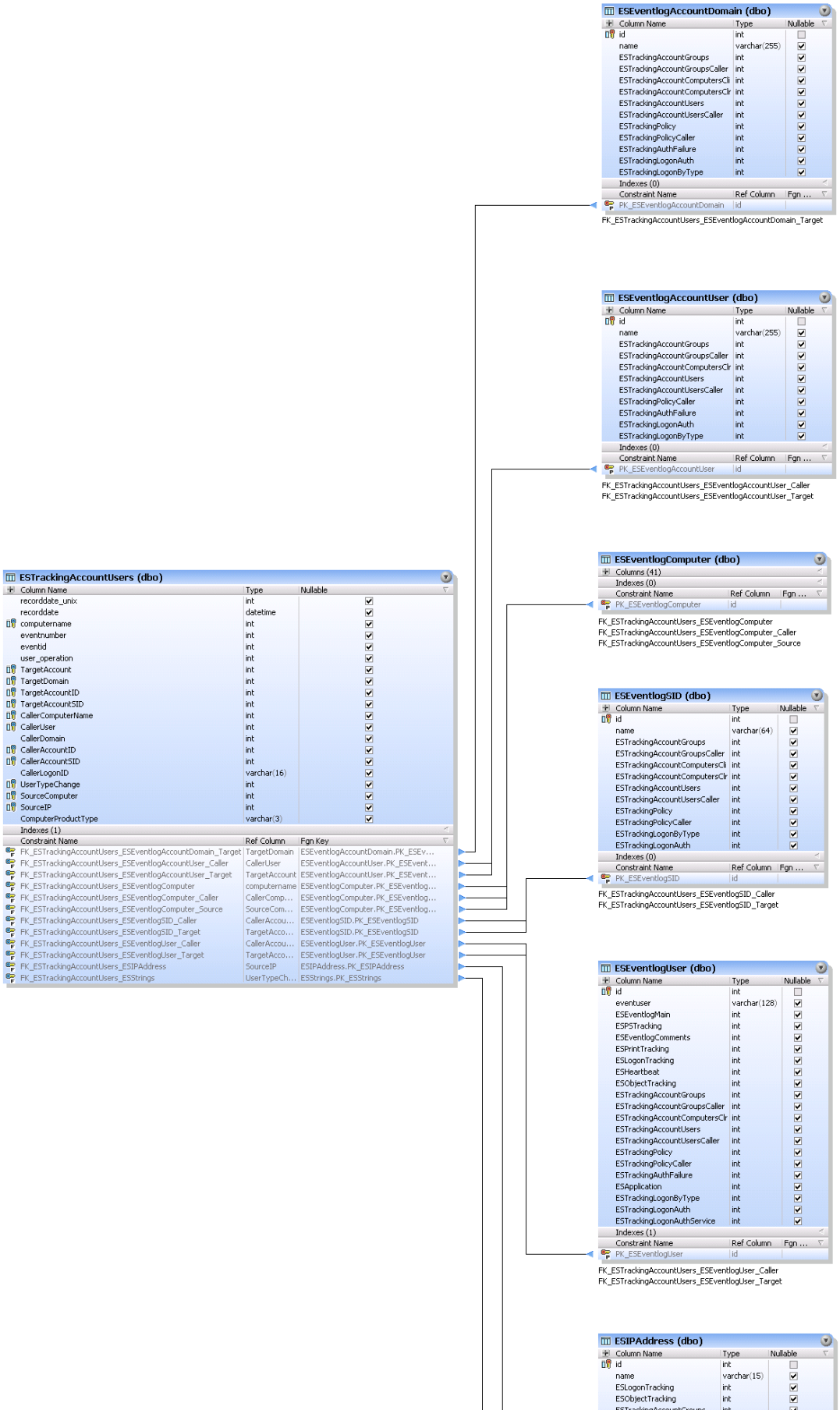
4.4.5.2.9.3 Print Tracking

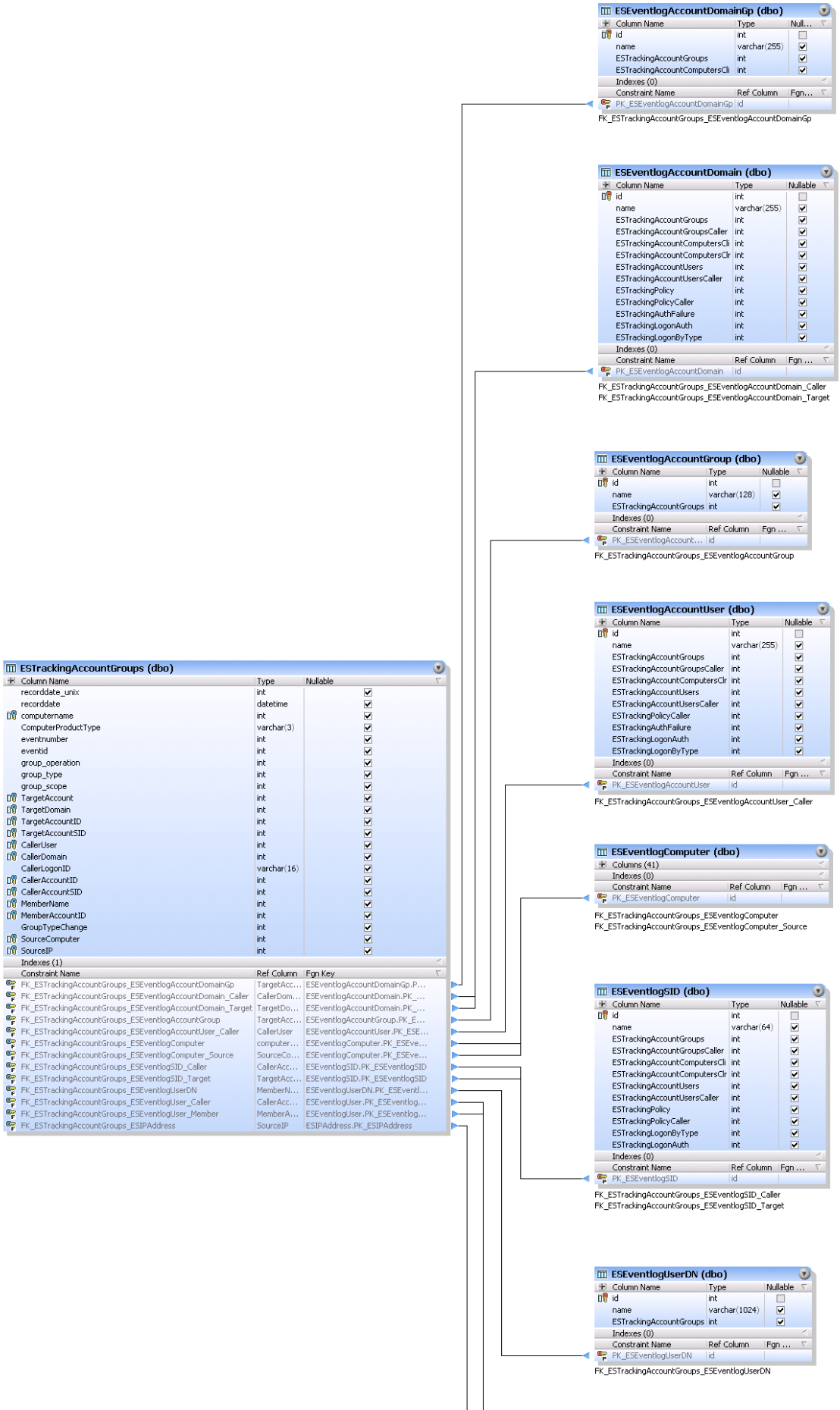


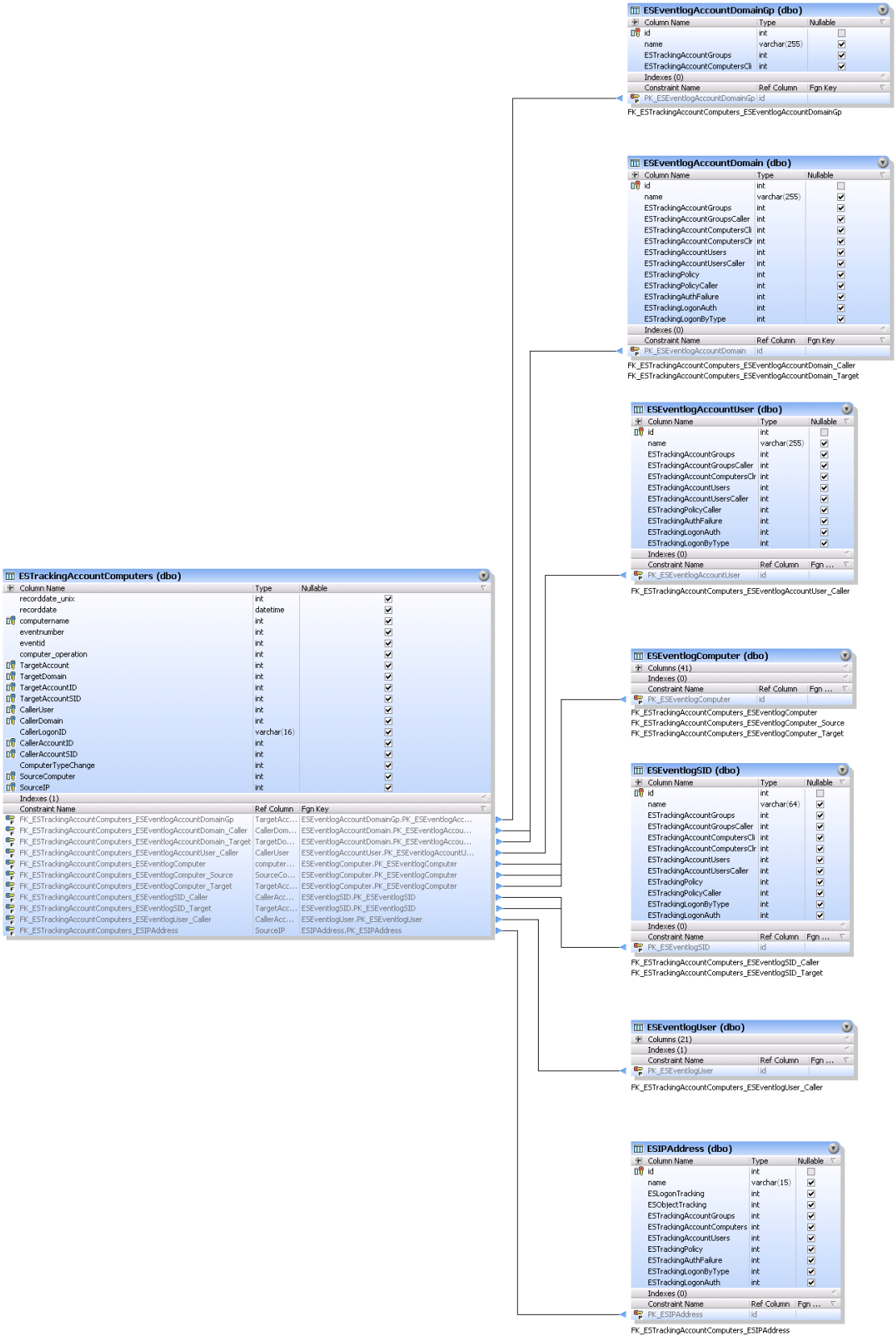
4.4.5.2.9.4 File Access Tracking



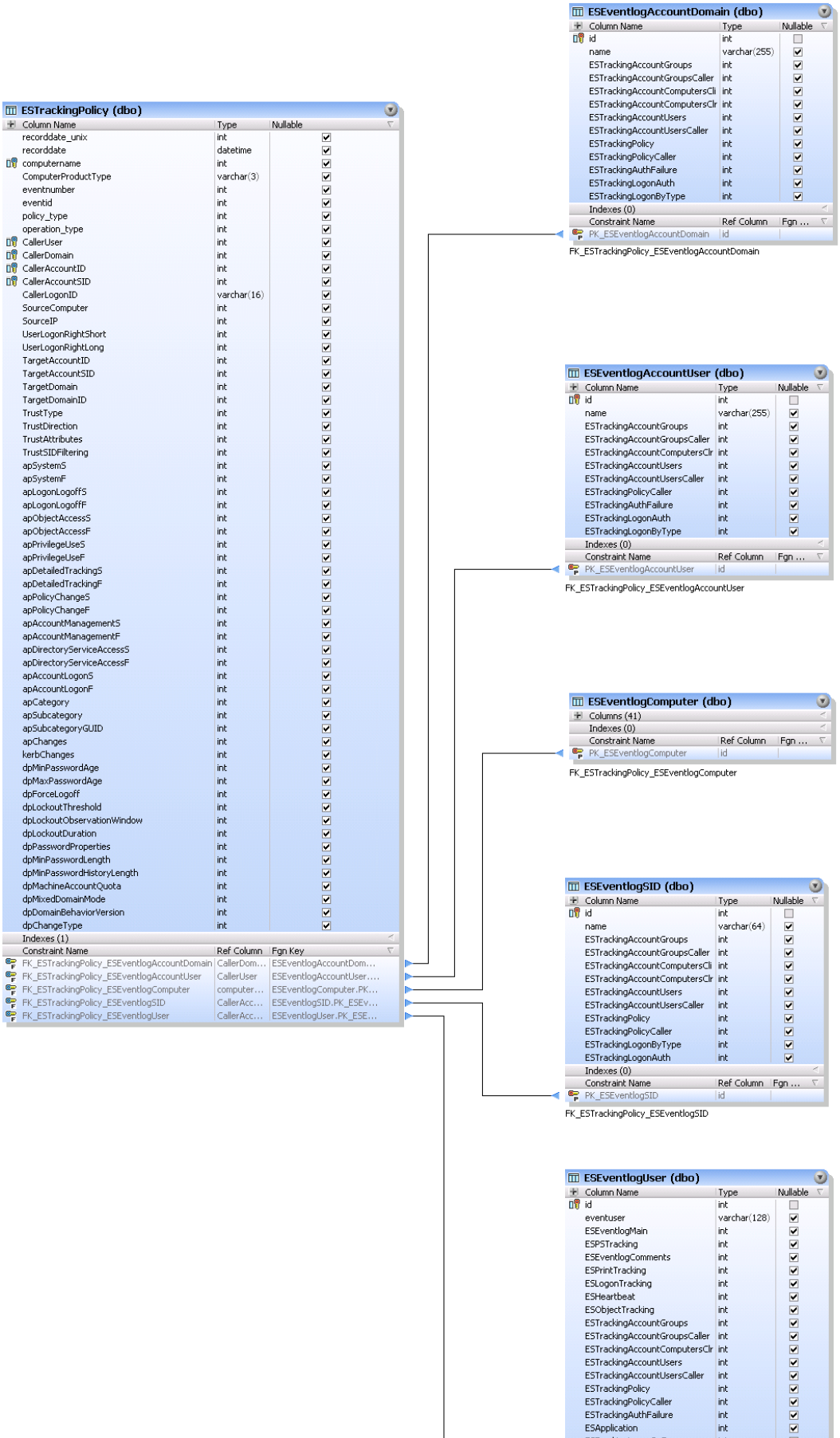
4.4.5.2.9.5 Account Management




ESEventlogAccountDomainGp (dbo)
Column Name Type Null...
id int
name varchar(255)
ESTrackingAccountGroups int
ESTrackingAccountComputersCli int
Indexes (0)
Constraint Name Ref Column Fgn...
PK_ESEventlogAccountDomainGp id
FK_ESTrackingAccountGroups_ESEventlogAccountDomainGp
ESEventlogAccountDomain (dbo)
Column Name Type Nullable
id int
name varchar(255)
ESTrackingAccountGroups int
ESTrackingAccountGroupsCaller int
ESTrackingAccountComputersCli int
ESTrackingAccountComputersClr int
ESTrackingAccountUsers int
ESTrackingAccountUsersCaller int
ESTrackingPolicy int
ESTrackingPolicyCaller int
ESTrackingAuthFailure int
ESTrackingLogonAuth int
ESTrackingLogonByType int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogAccountDomain id
FK_ESTrackingAccountGroups_ESEventlogAccountDomain_Caller
FK_ESTrackingAccountGroups_ESEventlogAccountDomain_Target
ESEventlogAccountGroup (dbo)
Column Name Type Nullable
id int
name varchar(128)
ESTrackingAccountGroups int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogAccount... id
FK_ESTrackingAccountGroups_ESEventlogAccountGroup
ESEventlogAccountUser (dbo)
Column Name Type Nullable
id int
name varchar(255)
ESTrackingAccountGroups int
ESTrackingAccountGroupsCaller int
ESTrackingAccountComputersClr int
ESTrackingAccountUsers int
ESTrackingAccountUsersCaller int
ESTrackingPolicyCaller int
ESTrackingAuthFailure int
ESTrackingLogonAuth int
ESTrackingLogonByType int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogAccountUser id
FK_ESTrackingAccountGroups_ESEventlogAccountUser_Caller
ESTrackingAccountGroups (dbo)
Column Name Type Nullable
recorddate_unix int
recorddate datetime
computername int
ComputerProductType varchar(3)
eventnumber int
eventid int
group_operation int
group_type int
group_scope int
TargetAccount int
TargetDomain int
TargetAccountID int
TargetAccountSID int
CallerUser int
CallerDomain int
CallerLogonID varchar(16)
CallerAccountID int
CallerAccountSID int
MemberName int
MemberAccountID int
GroupTypeChange int
SourceComputer int
SourceIP int
Indexes (1)
Constraint Name Ref Column Fgn Key
FK_ESTrackingAccountGroups_ESEventlogAccountDomainGp TargetAcc... ESEventlogAccountDomainGp.P...
FK_ESTrackingAccountGroups_ESEventlogAccountDomain_Caller CallerDom... ESEventlogAccountDomain.PK_...
FK_ESTrackingAccountGroups_ESEventlogAccountDomain_Target TargetDo... ESEventlogAccountDomain.PK_...
FK_ESTrackingAccountGroups_ESEventlogAccountGroup TargetAcc... ESEventlogAccountGroup.PK_E...
FK_ESTrackingAccountGroups_ESEventlogAccountUser_Caller CallerUser ESEventlogAccountUser.PK_ESE...
FK_ESTrackingAccountGroups_ESEventlogComputer computer... ESEventlogComputer.PK_ESEve...
FK_ESTrackingAccountGroups_ESEventlogComputer_Source SourceCo... ESEventlogComputer.PK_ESEve...
FK_ESTrackingAccountGroups_ESEventlogSID_Caller CallerAcc... ESEventlogSID.PK_ESEventlogSID
FK_ESTrackingAccountGroups_ESEventlogSID_Target TargetAcc... ESEventlogSID.PK_ESEventlogSID
FK_ESTrackingAccountGroups_ESEventlogUserDN MemberN... ESEventlogUserDN.PK_ESEventl...
FK_ESTrackingAccountGroups_ESEventlogUser_Caller CallerAcc... ESEventlogUser.PK_ESEventlog...
FK_ESTrackingAccountGroups_ESEventlogUser_Member MemberA... ESEventlogUser.PK_ESEventlog...
FK_ESTrackingAccountGroups_ESIPAddress SourceIP ESIPAddress.PK_ESIPAddress
ESEventlogComputer (dbo)
Columns (41)
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogComputer id
FK_ESTrackingAccountGroups_ESEventlogComputer
FK_ESTrackingAccountGroups_ESEventlogComputer_Source
ESEventlogSID (dbo)
Column Name Type Nullable
id int
name varchar(64)
ESTrackingAccountGroups int
ESTrackingAccountGroupsCaller int
ESTrackingAccountComputersCli int
ESTrackingAccountComputersClr int
ESTrackingAccountUsers int
ESTrackingAccountUsersCaller int
ESTrackingPolicy int
ESTrackingPolicyCaller int
ESTrackingLogonByType int
ESTrackingLogonAuth int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogSID id
FK_ESTrackingAccountGroups_ESEventlogSID_Caller
FK_ESTrackingAccountGroups_ESEventlogSID_Target
ESEventlogUserDN (dbo)
Column Name Type Nullable
id int
name varchar(1024)
ESTrackingAccountGroups int
Indexes (0)
Constraint Name Ref Column Fgn ...
PK_ESEventlogUserDN id
FK_ESTrackingAccountGroups_ESEventlogUserDN

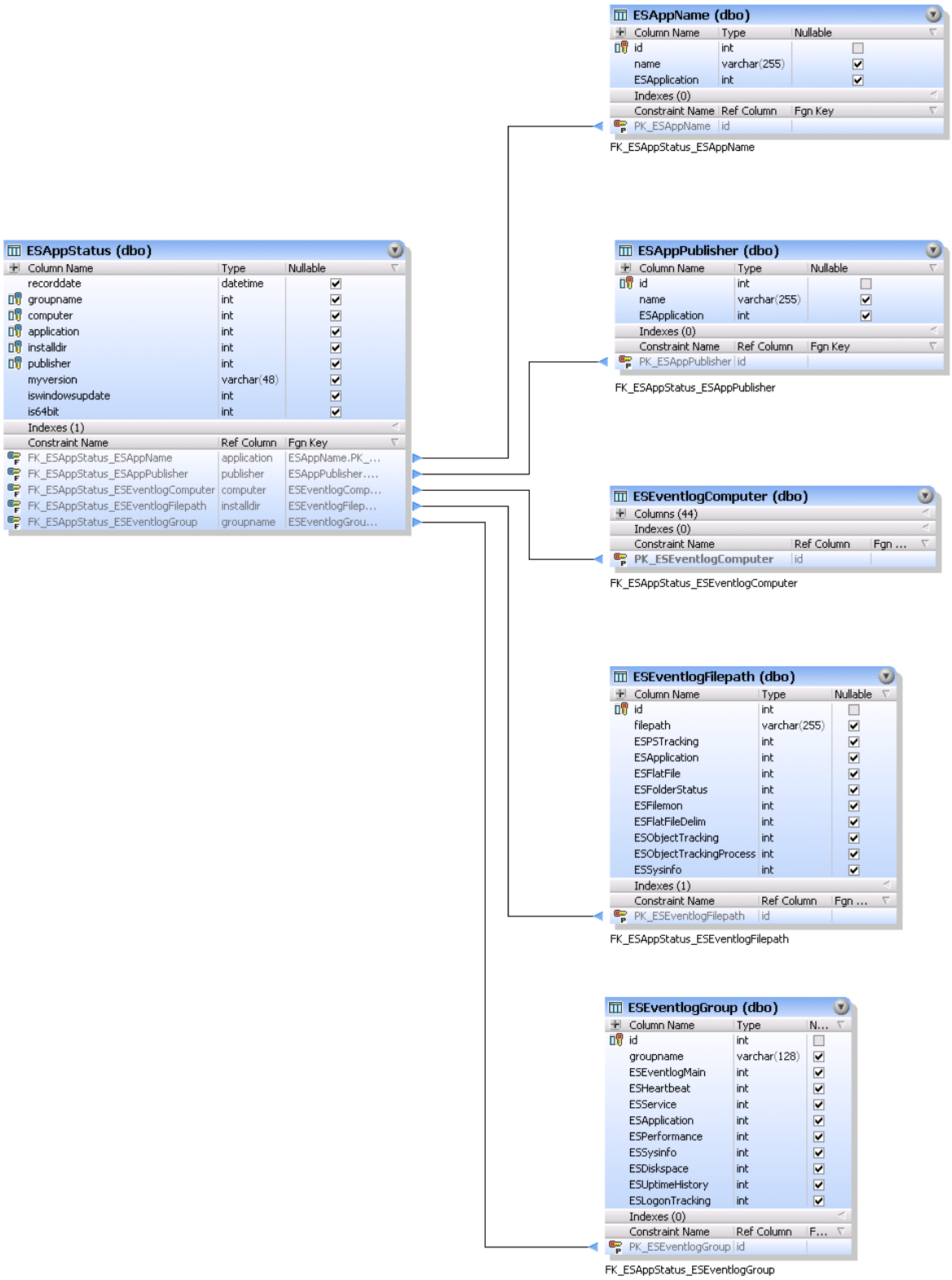


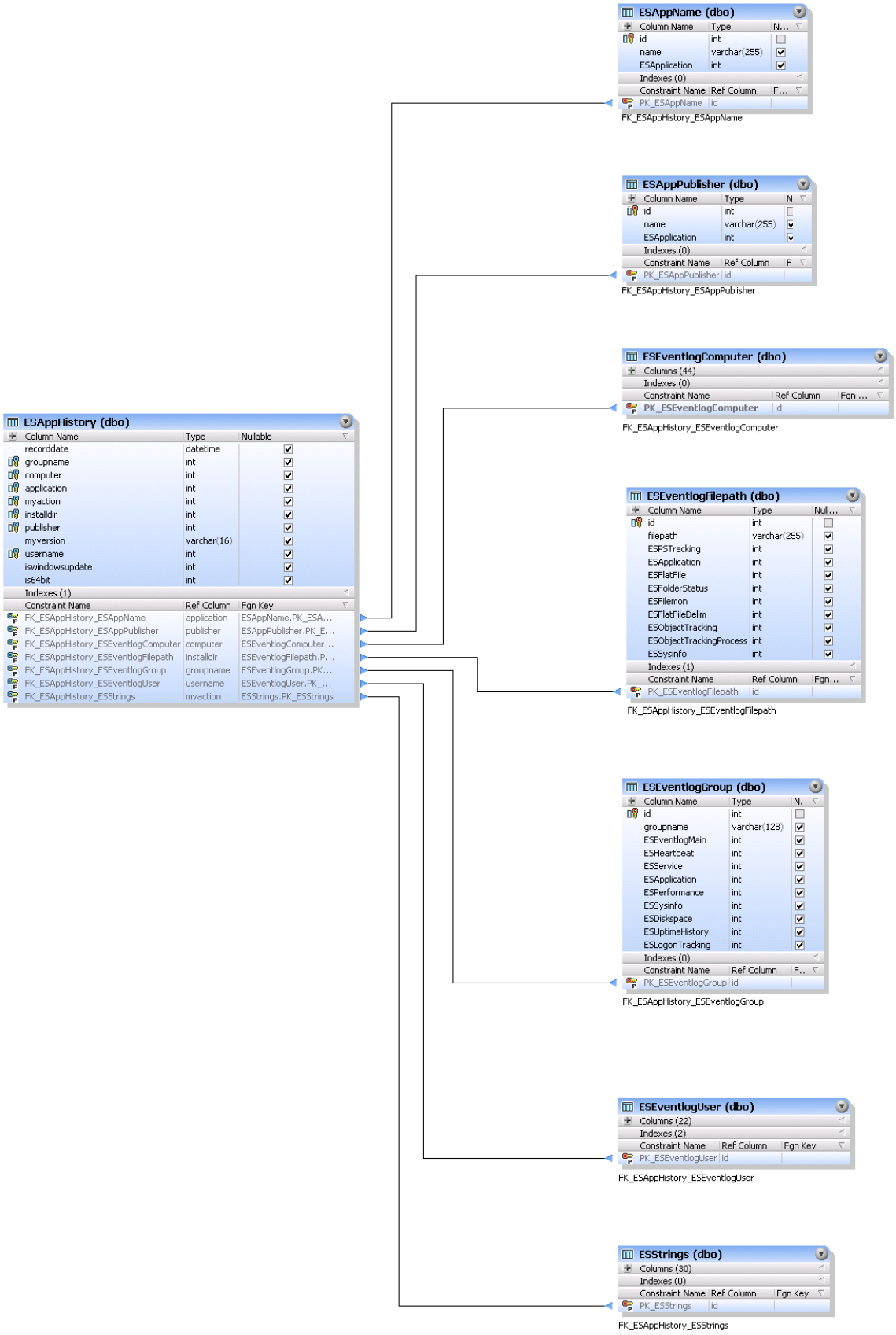
4.4.5.2.9.6 Policy Change Tracking



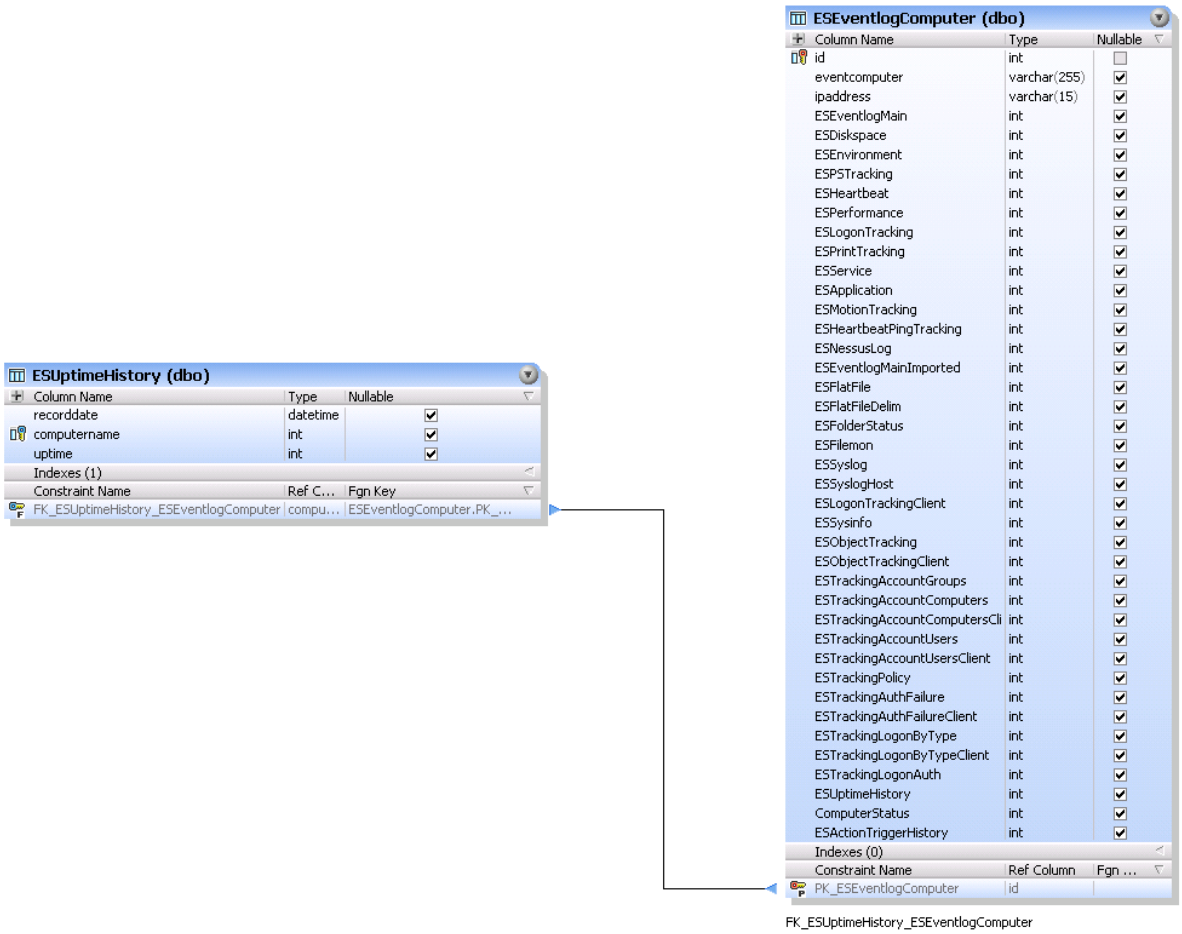
4.4.5.2.10 Inventory

4.4.5.2.10.1 Software Monitoring

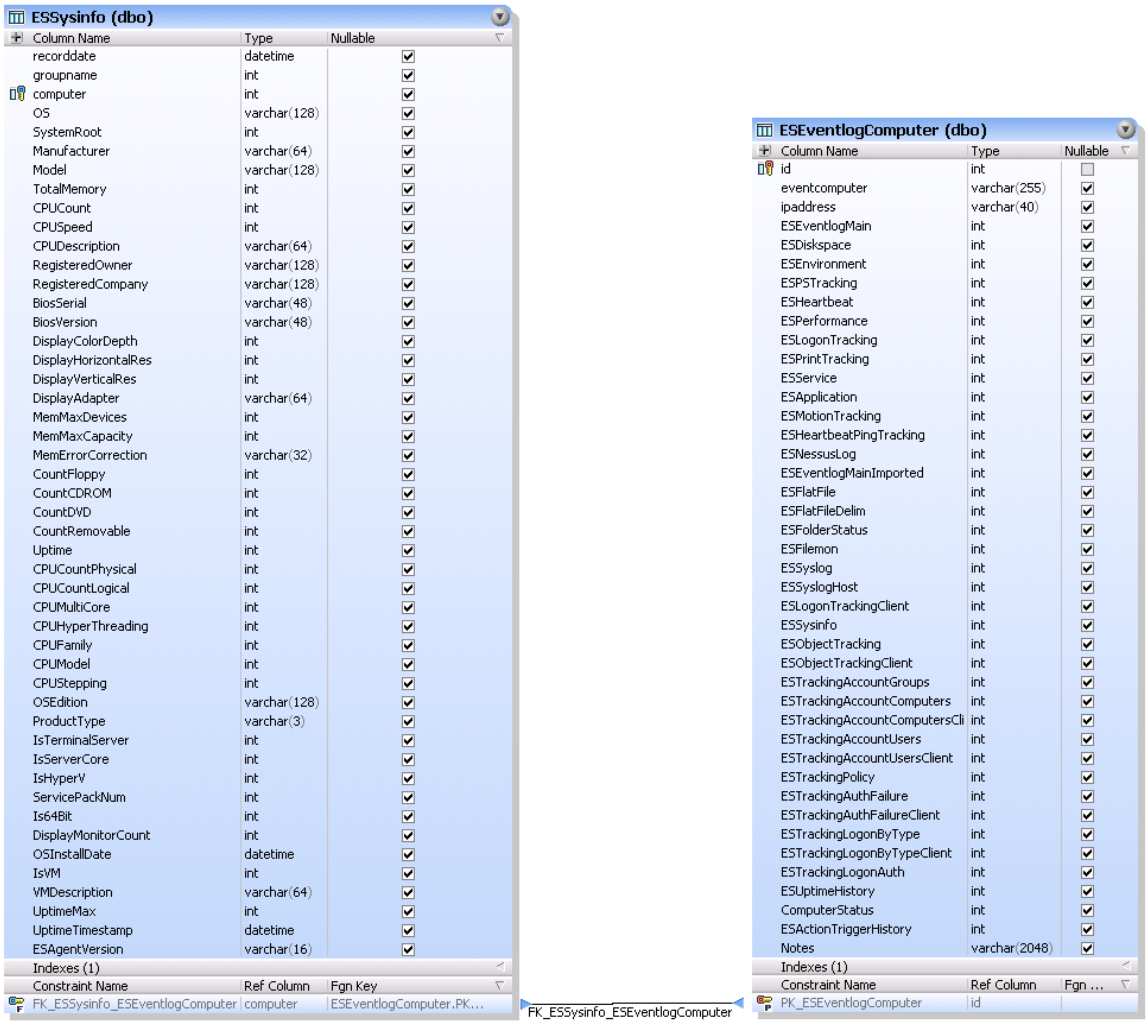




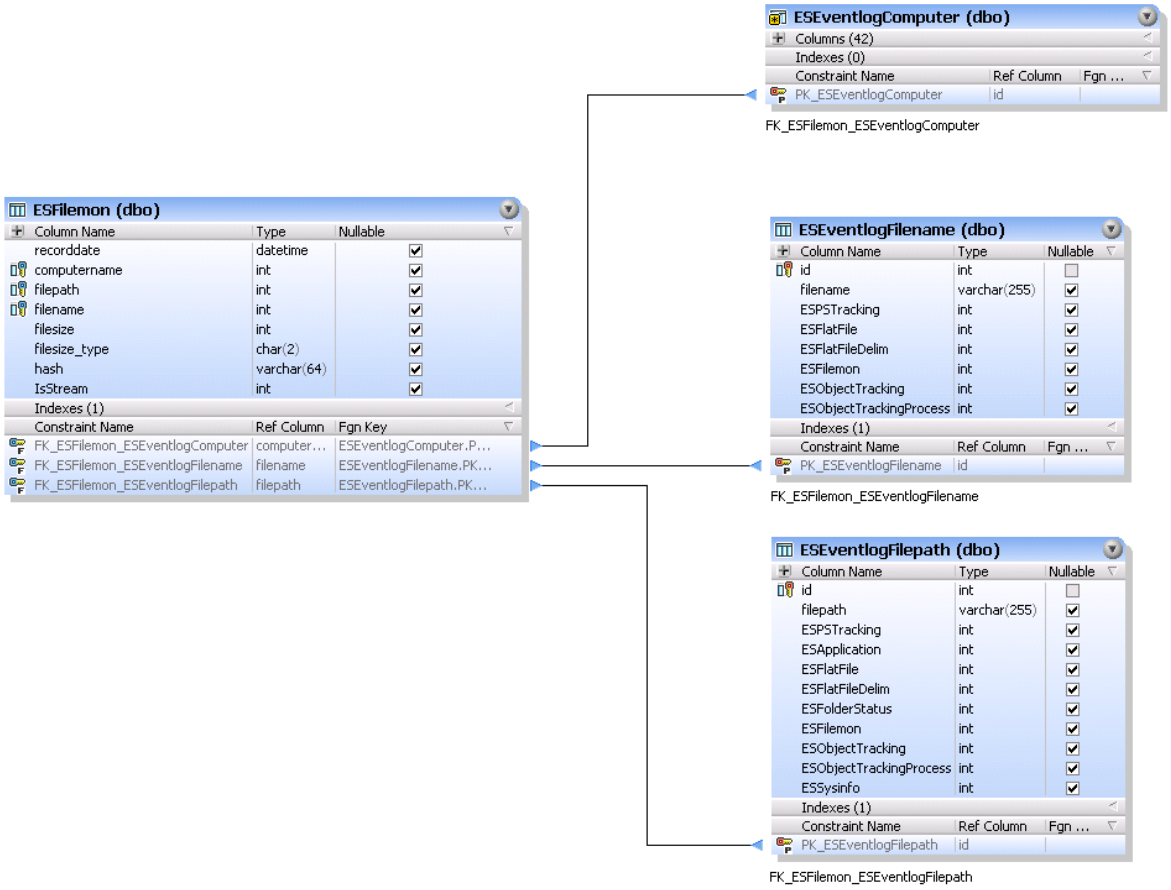
4.4.5.2.10.2 Uptime Monitoring



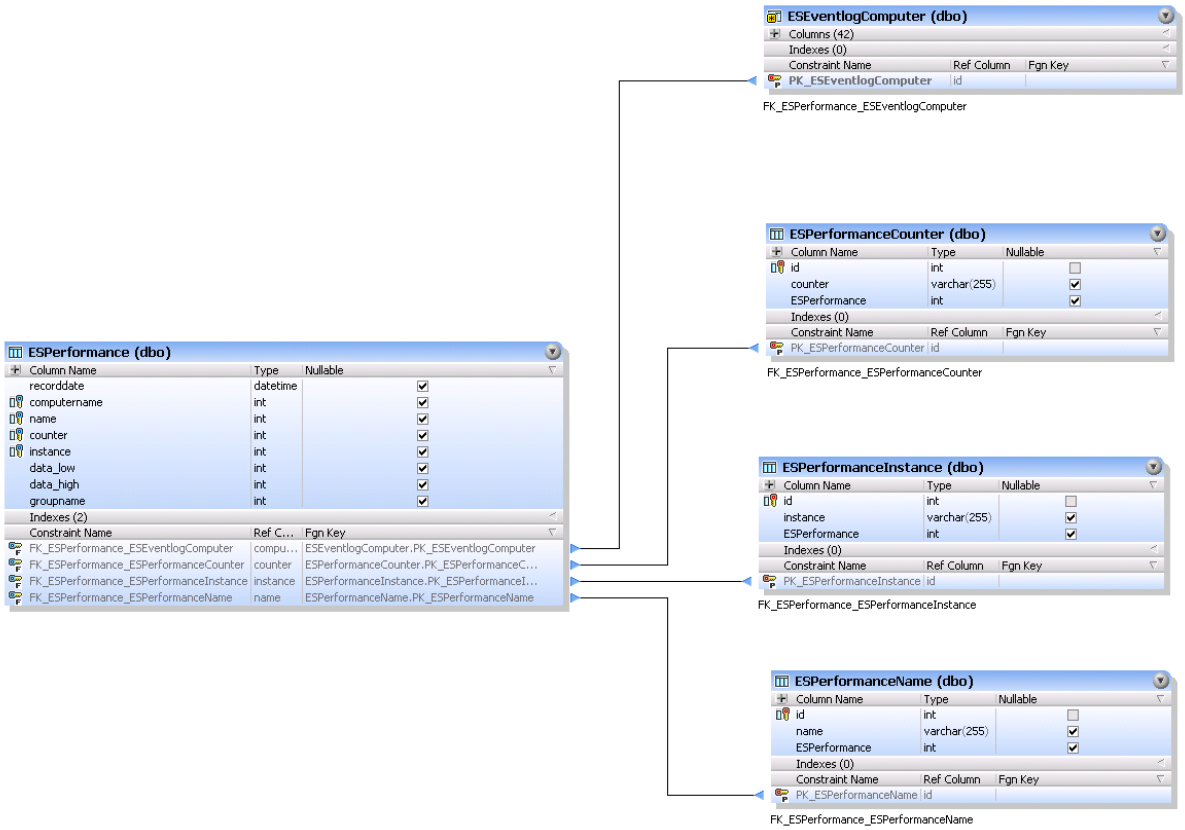
4.4.5.2.10.3 Hardware Inventory



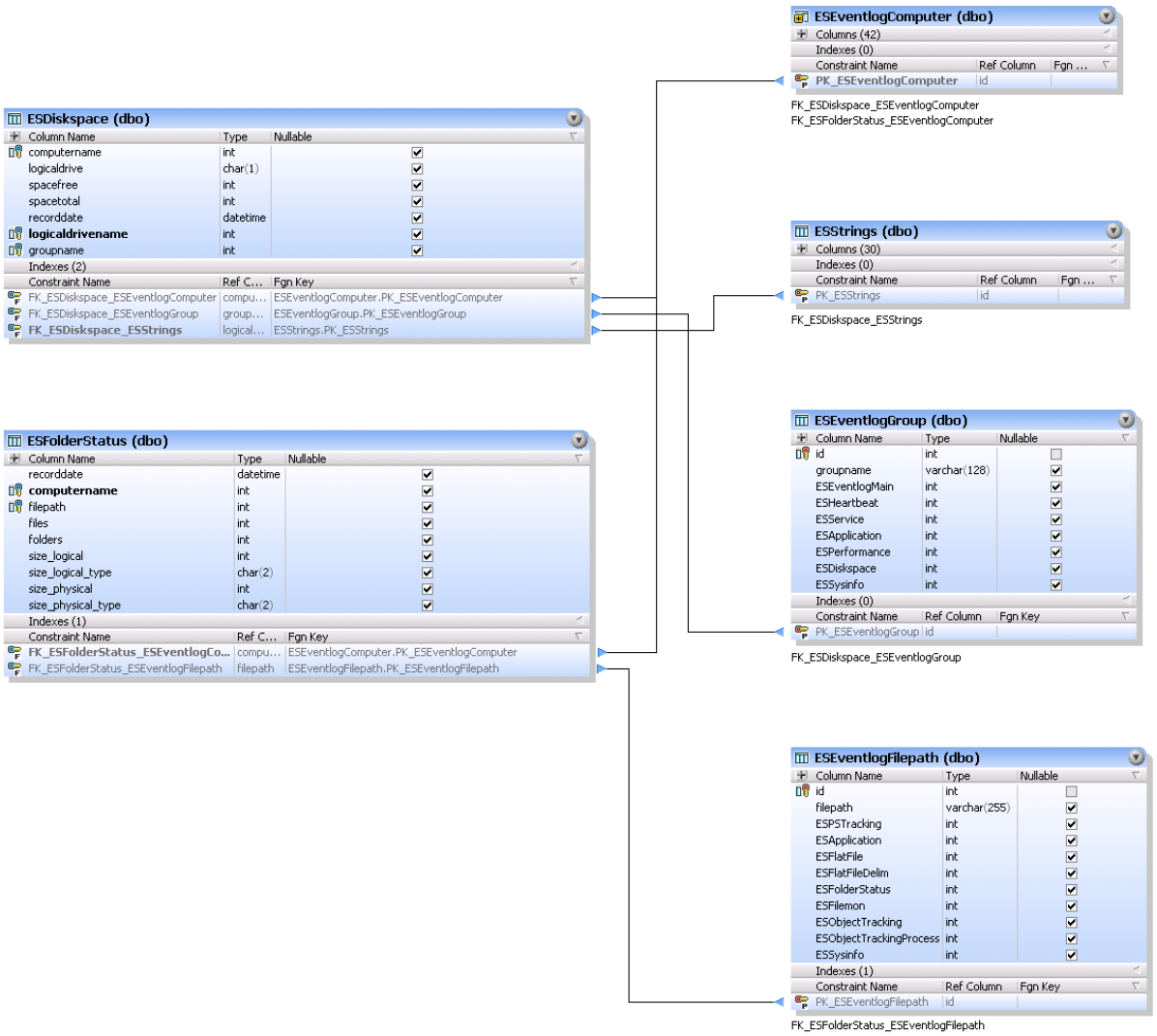
4.4.5.2.11 File Monitoring



4.4.5.2.12 Performance Monitoring



4.4.5.2.13 Disk Space Monitoring



4.4.5.3 Schritte zur Ereignisprotokoll-Konsolidierung

Bitte befolgen Sie die unten aufgeführten Schritte, um Ereignisprotokolleinträge in einer zentralen Datenbank zu konsolidieren. Je nach der von Ihnen verwendeten Datenbank müssen Sie möglicherweise zusätzliche Schritte durchführen.

Installieren eines Datenbankservers

Wenn Sie nicht die integrierte Datenbank verwenden und nicht bereits eine Datenbank wie PostgreSQL or MSSQL laufen haben, müssen Sie einen Datenbankserver in Ihrem Netzwerk einrichten. Die EventSentry-Website enthält Leitfäden, die den Einrichtungsprozess unterstützen (siehe http://www.eventsentry.com/support/documentation), sowie einen Setup-Assistenten für MS SQL Server Express, der unter http://www.eventsentry.com/downloads heruntergeladen werden kann.

Einrichten einer Datenbank während der Installation

Eine EventSentry-Datenbank wird automatisch mit dem Konfigurationsassistenten eingerichtet, nachdem der Installationsvorgang abgeschlossen ist. Der schnellste Weg, eine EventSentry-Datenbank einzurichten, ist die Auswahl der Eingebauten Datenbank während der Installation.

Konfigurieren der Konsolidierung und Bereitstellen von Agenten

1. Erstellen/konfigurieren Sie die ODBC-Aktion in EventSentry und konfigurieren Sie sie so, dass sie entweder eine Verbindungszeichenfolge (empfohlen) oder einen System-DSN verwendet. Testen Sie die ODBC-Aktion.

2. Klicken Sie auf die Schaltfläche "Datenbank initialisieren / aktualisieren", um die Datenbank für die Verwendung mit EventSentry einzurichten.

3. Optional: Wenn Sie einen System-DSN verwenden, stellen Sie sicher, dass der angegebene *ODBC-System-DSN* auf allen Rechnern vorhanden ist, die in die Datenbank schreiben werden. Wir empfehlen die Verwendung von EventSentry Admin Assistant, wenn Sie einen System-DSN-Namen auf mehrere Computer ausrollen müssen.

4. Erstellen Sie einen oder mehrere Include-Filter, die Ereignisprotokollinformationen sammeln und sie an die ODBC-Aktion (Datenbank) weiterleiten. Die Ereignisprotokoll-Konsolidierung beginnt erst, wenn die Ereignisprotokoll-Filter ordnungsgemäß eingerichtet sind.

5. Verwenden Sie Remote Update, um die aktualisierten Filter und Aktionen an alle Hosts zu senden, die den EventSentry-Agenten ausführen (nicht erforderlich wenn der Collector aktiviert ist).

6. Richten Sie die Web Reports so ein, dass die Datenbank über einen Webbrowser abgefragt werden kann.

4.4.5.4 Fehlerbehebung in Datenbanken

Lösungen für häufige Probleme mit der Datenbankaktion:

- Wenn Sie DSN-Namen verwenden (nicht empfohlen), stellen Sie sicher, dass der von Ihnen angegebene DSN-Name ein **System-DSN** ist. Benutzer-DSN-Namen werden nicht unterstützt.

- Der von Ihnen angegebene DSN-Name muss mit einem vorhandenen System-DSN übereinstimmen, der auf die richtige Datenbank verweist. Diese Datenquellennamen (DSN) müssen auf jedem Computer eingerichtet werden, auf dem der EventSentry-Agent/Dienst installiert ist. Sie können den EventSentry-Administrationsassistenten verwenden, um Datenquellennamen einfach auf mehrere Computer auszurollen.

- Verwenden Sie Verbindungszeichenfolgen anstelle von System-DSNs, um zu vermeiden, dass der DSN auf Zielcomputern eingerichtet werden muss.

- Stellen Sie sicher, dass alle erforderlichen **ODBC-Treiber** für Ihren Datenbankserver korrekt auf dem Host installiert sind, auf dem EventSentry installiert ist. Microsoft Windows 2000 und höher wird mit standardmäßig installierten SQL Server-Treibern ausgeliefert. Alle anderen Treiber müssen manuell installiert werden.

- Die Datenbank muss wie im vorigen Kapitel beschrieben eingerichtet und initialisiert werden.

- Diese Aktion protokolliert die folgenden Ereignisse mit der **EventSentry-Ereignisquelle** im Falle eines Fehlers im Anwendungsereignisprotokoll:

Ereignis-IDs	Ereignis-ID	Problem
	530	Eine bestimmte Funktion kann keine Verbindung mit der Datenbank herstellen.
	531	Bei der Verbindung mit der angegebenen Datenbank ist ein Fehler aufgetreten.
	532	Die folgenden Fehler oder Warnungen sind innerhalb der letzten 5 Minuten bei der Kommunikation mit der Datenbank aufgetreten:

4.4.5.5 Web Reports

Die Webberichte sind das Berichtswerkzeug für alle von %PRODUCT% gesammelten Daten und erfordern, dass eine oder mehrere %PRODUCT%-Datenbanken eingerichtet sind.

Die Webberichte können entweder als Teil der Hauptinstallation von %PRODUCT% installiert werden (empfohlen) oder aus dem Kundenbereich heruntergeladen und separat installiert werden. Wenn sie separat installiert werden, können sie entweder auf demselben Rechner installiert werden, auf dem das Haupt-Setup ausgeführt wurde, oder auf einem anderen Rechner. Das Standardinstallationsverzeichnis für die Webberichte ist **C:\Programme\EventSentry\WebReports**.

1a. Installation mit der Haupt EventSentry Installationsprogramm

Um die Web Reports mit dem Installer zu installieren, stellen Sie sicher, dass die Komponente "Web Reports" ausgewählt ist. Siehe Lokale Installation für weitere Einzelheiten zum Installationsprozess.

Sie können nun mit Ihrem Web-Browser zur Index-Seite navigieren, z.B. `http://yourserver:8080/`

2b. Installation mit dem separaten Webreport-Installationsprogramm

Um eine manuelle Installation der Webreports mit dem separaten Webreport-Installationsprogramm (z.B. eventsentry_webreports_v4_2_1_1_0_windows_setup.exe) durchzuführen, laden Sie das Installationsprogramm aus dem Kundenbereich herunter und führen Sie das Installationsprogramm einfach aus.

Das eigenständige Installationsprogramm kann unter Windows, Linux und/oder OS X ausgeführt werden. Die Web-Reports können auf jedem Host installiert werden, der direkten Zugriff auf die Datenbank hat.

Eine Installation neben einer bestehenden EventSentry Installation ist ebenfalls möglich, aber in diesem Fall wird empfohlen, das Hauptinstallationsprogramm auszuführen, das die Web Reports enthält. Wenn das Installationsprogramm für die Web-Reports zu einer vorhandenen EventSentry Installation hinzugefuegt wird, dann kann sie jederzeit deinstalliert werden.

3. Konfigurationsdateien

Alle Einstellungen in den Web Reports werden in XML-Konfigurationsdateien gespeichert.

configuration.xml
Dies ist die Hauptkonfigurationsdatei für die Web Reports und wird bei der Produktinstallation automatisch konfiguriert. Die Datei enthält alle Profileigenschaften sowie globale Einstellungen für die Fehlerbehebung.

preferences.xml
Diese Datei enthält sowohl alle globalen als auch benutzerspezifischen Einstellungen.

reports.xml

Diese Datei enthält eine Liste aller verfügbaren Berichte.

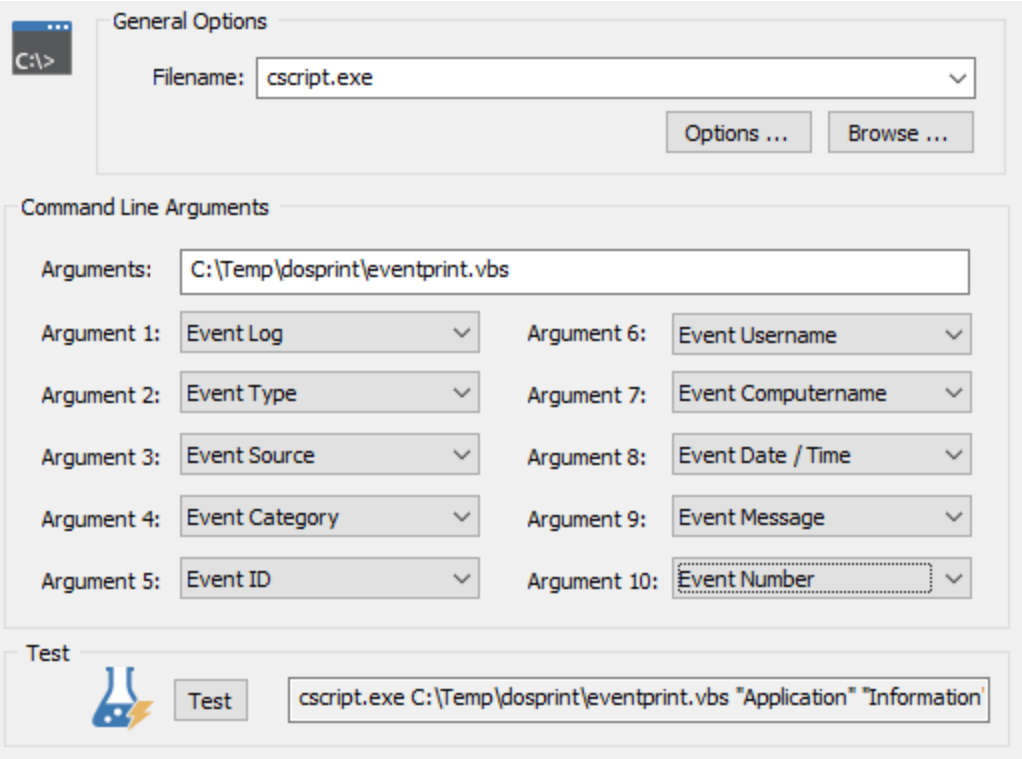
 jobs.xml
Diese Datei enthält eine Liste aller konfigurierten Aufträge.

 users.xml
Steuert die Zugriffskontrolle und, wenn aktiviert, eine Liste aller Benutzer und Gruppen.

4.4.6 Prozess

EventSentry kann jeden externen Prozess starten und Kommandozeilenargumente an den Prozess übergeben. Prozesse können entweder auf dem Desktop sichtbar sein oder im Hintergrund laufen.

Wenn diese Benachrichtigung ausgelöst wird, protokolliert EventSentry ein Ereignis im Ereignisprotokoll, das anzeigt, ob der Prozess erfolgreich gestartet wurde oder nicht.



Dateiname

Geben Sie im Feld Dateiname die auszuführende Datei an. Sie können entweder ein vorhandenes Skript angeben oder mit der Schaltfläche "**Browse**" auswählen oder mit dem Dropdown-Menü ein eingebettetes Skript auswählen. Eingebettete Skripte werden mit dem @-Symbol vor der Datei angegeben.

Kommandozeilen-Argumente

Benutzerdefinierte Argumente können an den Prozess übergeben werden. Sie können in diesem Feld auch Variablen verwenden, z.B. Einfügetext ($STR1, $STR2, ...).

Laufzeit-Argument 1 .. 10

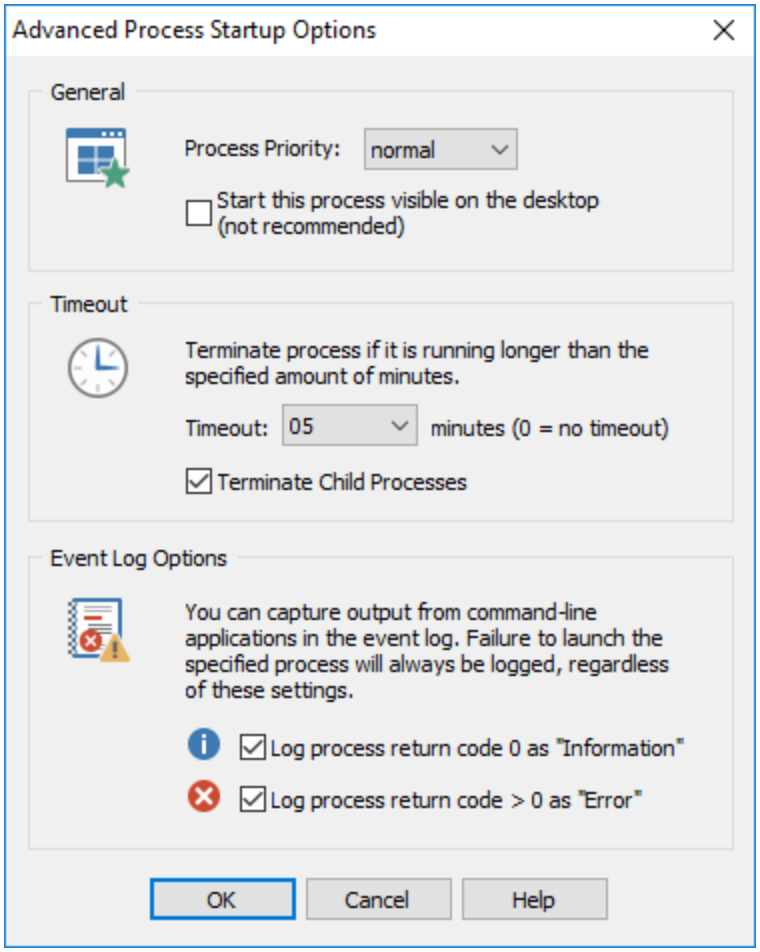
Hier können Sie die Details der Ereignisaufzeichnung an den Prozess übergeben. Alle Argumente sind in Anführungszeichen eingeschlossen, nur die ersten 768 Zeichen der eigentlichen Ereignismeldung werden an den Prozess übergeben.

Die Befehlszeile für den obigen Screenshot könnte wie folgt aussehen:

```
cscript.exe c:\temp\dosprint\eventprint.vbs "Application" "Warning"
"EventSentry" "Service Monitoring" 10100 "" "DBSERVER" "7/27/2008 3:15:23
PM" "The status of service MySQL (MySQL) changed from Running to Stopped.
```

Siehe Optionen für weitere Konfigurationsoptionen.

4.4.6.1 Optionen



Prozess-Priorität
Die Priorität des Prozesses; standardmäßig **normal**.

Diesen Prozess auf dem Desktop starten (sichtbar)
Wenn Sie dieses Kästchen ankreuzen, ist der Prozess sichtbar, wenn Sie auf dem Computer angemeldet sind. Wenn dieses Kästchen nicht angekreuzt ist, ist der Prozess unsichtbar.

Auszeit
Beendet den Prozess nach der gewählten Anzahl von Minuten. Setzen Sie diese Option auf **00**, wenn der Prozess nie beendet werden soll.

Beenden Sie Child-Prozesse: Beendet rekursiv alle Child-Prozesse, die durch den Prozess gestartet wurden.

Ereignisprotokoll-Optionen

Ähnlich wie der Application Scheduler kann der Agent ein Ereignis im Ereignisprotokoll protokollieren, basierend auf dem Rückgabecode (ERRORLEVEL), den der Prozess zur Verfügung stellt. Dies ist vor allem für Konsolenprozesse und Skripte nützlich.

Protokolliert den Rückgabecode 0:
Protokolliert ein Informationsereignis, wenn der Prozess mit dem Returncode 0 beendet wurde.

Rückgabecode >0 protokollieren:
Protokolliert ein Fehlerereignis, wenn der Prozess mit einem Rückkehrcode größer als 0 beendet wurde (was normalerweise auf einen Fehler hindeutet).

4.4.6.2 Fehlerbehebung von Prozessen

Lösungen für Probleme mit der Prozess Aktion:

- Das LocalSystem-Konto (oder das Konto, unter dem der EventSentry Dienst läuft) benötigt die Erlaubnis, die in **Dateiname** angegebene Datei auszuführen.
- Die angegebene ausführbare Datei muss auf jedem Computer vorhanden sein, der diese Benachrichtigungsaktion verwendet.
- Gestartete Prozesse **sind auf dem Desktop nicht sichtbar**, es sei denn, das Kontrollkästchen "Diesen Prozess auf dem Desktop starten" ist aktiviert.
- Diese Aktion protokolliert im Falle eines Fehlers die folgenden Ereignisse im Anwendungsereignisprotokoll mit der **EventSentry** Ereignisquelle:

Ereignis-IDs	Ereignis-ID	Problem / Beschreibung
	561	Der Prozess konnte nicht eingeleitet werden.
	562	Der Prozess überschritt die maximale Laufzeit und konnte nicht beendet werden.
	563	Der Prozess überschritt die maximale Laufzeit und wurde erfolgreich beendet.

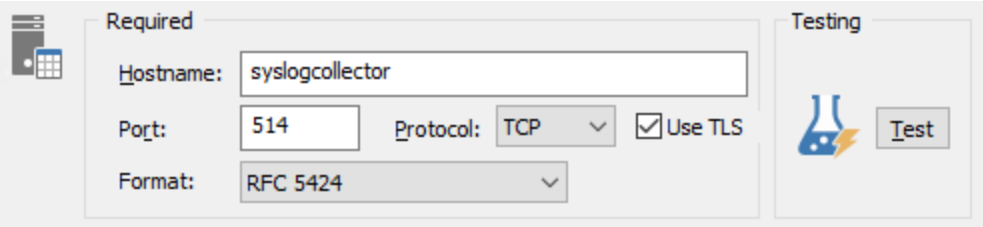
4.4.6.3 Ereignisprotokoll

Die folgenden Ereignisse werden von dieser Funktion protokolliert, wenn ein Prozess erfolgreich gestartet wurde:

Ereignis-IDs	Ereignis-ID	Problem / Beschreibung
	560	Der Prozess wurde erfolgreich gestartet (protokolliert, nachdem der Prozess korrekt beendet wurde).
	564	Der Prozess wurde erfolgreich gestartet.

4.4.7 Syslog

Sie können Ereignisprotokollaufzeichnungen entweder über das UDP- oder TCP-Protokoll an entfernte Unix/Linux-Syslog-Server senden. Ereignisprotokollaufzeichnungen können in einer Vielzahl von Formaten gesendet werden, einschließlich Snare, Graylog, CEF und anderen.



Hostname
Die IP-Adresse oder der Hostname des entfernten Syslog-Servers.

Anschluss
Der Port, auf dem der Remote-Syslog-Server auf eingehende Anforderungen lauscht, standardmäßig 514.

Protokoll
Das zu verwendende Protokoll, entweder UDP oder TCP. Die meisten Hosts verwenden das UDP-Protokoll.

TLS verwenden
TLS-Verschlüsselung verwenden, wenn vom entfernten Syslog-Server unterstützt, erfordert TCP.

Format
Das Format, in dem Ereignisprotokollaufzeichnungen gesendet werden. Das "EventSentry"-Format ist unten dargestellt.

Direkt (ohne Collector):
hostname: optional prefix[timestamp-eventnumber]
ID=eventid:eventlog:eventsource:eventcategory:severity:eventuser:eventmessage:binarydata

Indirekt (mit Collector):
hostname: optional prefix[timestamp-eventnumber]
ID=eventid:eventcomputer:eventlog:eventsource:eventcategory:severity:eventuser:eventmessage

Event-Kategorie, Event-Benutzer und Binärdaten sind nur enthalten, wenn sie im Event-Datensatz vorhanden sind. Carriage Returns im Ereignisprotokolldatensatz werden automatisch entfernt.

Weitere unterstützte Formate sind Snare, RFC 5424, Graylog (GELF), CEF, Nagios Log Server sowie ein benutzerdefiniertes JSON-Format.

Kritikalität (nur Snare-Format)
Wenn das "Snare"-Format gewählt wird, konfigurieren Sie eine Kritikalität.

Präfix
Sie können jeder Syslog-Nachricht, die von EventSentry versendet wird, einen Textstring voranstellen lassen. Geben Sie die Zeichenfolge einfach in das Feld **Präfix** ein.

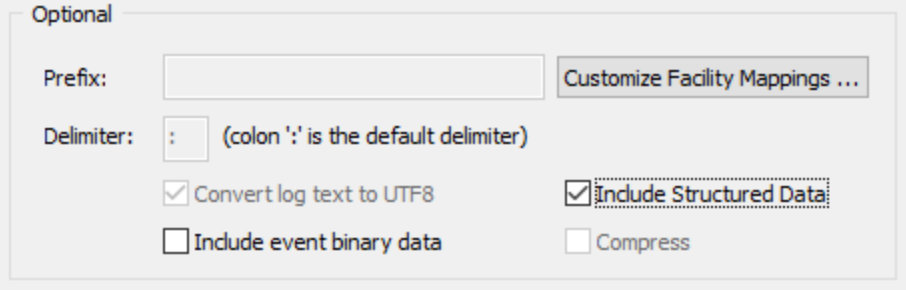
Begrenzer
Standardmäßig werden alle Felder aus dem Ereignisprotokoll mit einem Doppelpunkt (:) verkettet, aber es kann ein anderes Trennzeichen angegeben werden.

Protokolltext in UTF8 konvertieren
Konvertiert die Ereignisprotokollnachricht in das UTF8-Format.

Einschließen von Ereignis-Binärdaten
Schließt Ereignis-Binärdaten, falls vorhanden, in die Syslog-Nachricht ein.

Strukturierte Daten einbeziehen (nur RFC 5424)
Enthält Schlüsselereignisfelder als strukturierte Daten zusätzlich zur Syslog-Meldung.

komprimieren
Komprimiert Daten, nur Unterstützung für das GELF-Format über UDP



Testen Sie
Senden einer Syslog-UDP-Nachricht an den entfernten Host

Die meisten Syslog-Dämonen auf Unix/Linux-Servern akzeptieren standardmäßig keine entfernten Syslog-Pakete. Bitte lesen Sie die entsprechenden Man Pages, wenn Sie nicht wissen, wie Sie diese Funktion aktivieren können. Auf den meisten Linux-Distributionen müssen Sie dem Syslog-Daemon beim Start entweder die Option **-r** oder **-x** übergeben.

4.4.7.1 Fehlerbehebung Syslog

Solutions for common problems with the Syslog action:

- Make sure that the syslog server you are sending to is configured to accept remote connections
- Make sure that the syslog server you are sending to is configured to use the same protocol and port as specified in **Protocol** and **Port**. This is usually the **UDP** protocol with port **514** but can be different.
- This action logs the following events to the application event log with the **EventSentry** event source in case of an error:

Event IDs

Event ID	Problem / Description
520	A TCP connection could not be established with the remote host.
521	A UDP socket could not be created.

4.4.8 SNMP

Sie können v1-, v2c- oder v3-SNMP-Traps an eine SNMP-Verwaltungsstation senden.

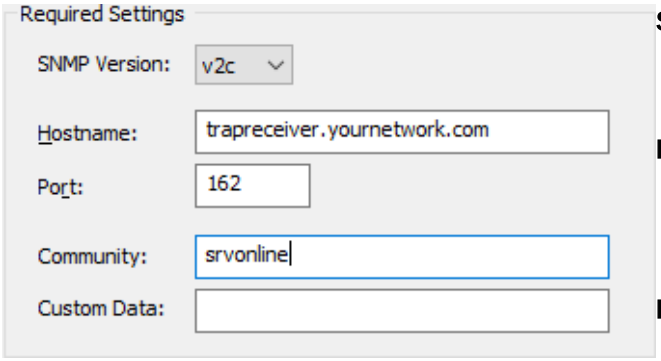
MIB
Damit Traps in Ihrem SNMP-Verwaltungssystem korrekt angezeigt werden, müssen Sie eine der beiden MIBs, die mit EventSentry ausgeliefert werden, importieren/zusammenstellen:

- EventSentryV1.mib
- EventSentryV2cV3.mib

Diese Dateien werden im Unterverzeichnis "Mibs" des Installationsverzeichnisses von EventSentry installiert (standardmäßig `C:\Programme\EventSentry\Mibs`). Abhängig von der Version des Traps, den Sie senden, müssen Sie eine der beiden Dateien importieren:

Version 1: EventSentryV1.mib
Version 2c & 3: EventSentryV2cV3.mib

Allgemeine Einstellungen



SNMP-Version
Die Version, mit der der SNMP-Trap gesendet wird.

Hostname
Der Hostname oder die IP-Adresse des Rechners, auf dem die SNMP-Verwaltungsanwendung ausgeführt wird.

Hafen
Der zu verwendende UDP-Port, standardmäßig 162.

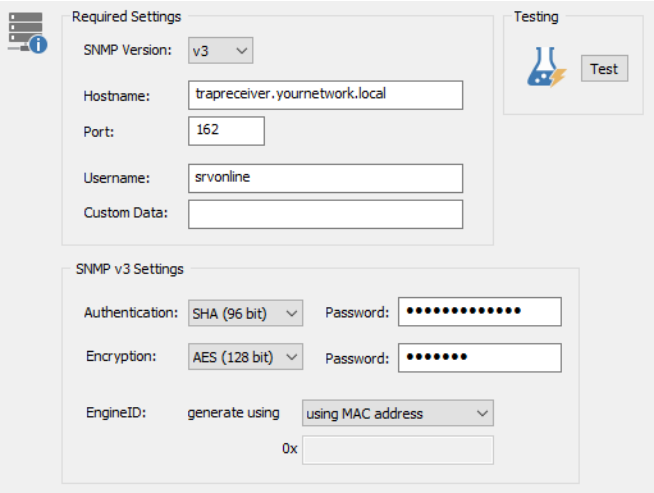
Testen Sie
Sendet einen Test-Trap an die konfigurierte Verwaltungsstation.

SNMP v1/v2c-Einstellungen

Gemeinschaft
Die SNMP-Community.

SNMP v3-Einstellungen

Wenn die empfangende Verwaltungsstation v3-SNMP-Traps unterstützt, konfigurieren Sie einige der erweiterten SNMP-Optionen, wie z. B. Authentifizierung und Verschlüsselung, die nur in SNMP v3-Traps verfügbar sind.



Authentifizierung (Datenintegrität)
Wählen Sie einen der verfügbaren Authentifizierungsmechanismen (MD5 (96 Bit) oder SHA (96 Bit)) oder wählen Sie "Keine", wenn keine Authentifizierung/Datenintegrität erwünscht ist. Bei Auswahl der Authentifizierung muss ein Passwort eingegeben werden.

Verschlüsselung (Datenschutz)
Wählen Sie einen der verfügbaren Verschlüsselungsalgorithmen (DES, 3DES oder AES (128 Bit)) oder wählen Sie "Keine", wenn keine Verschlüsselung gewünscht wird. Bei Auswahl der Verschlüsselung muss ein Passwort eingegeben werden.

EngineID
SNMPv3 erfordert eine EngineID, die eine eindeutige Kennung für eine SNMP-Engine (wie z.B. EventSentry) ist. EventSentry kann die Engine ID entweder automatisch generieren, indem es entweder die MAC- oder IP-Adresse einer Netzwerkschnittstelle verwendet, oder Sie können die Engine ID manuell angeben. Bei Multi-Homed-Hosts wird die MAC- oder IP-Adresse der Schnittstelle, die den Trap sendet, verwendet, wenn die Engine-ID automatisch generiert wird.

4.4.8.1 Fehlerbehebung bei SNMP

Lösungen für häufige Probleme mit der SNMP-Aktion:

- Stellen Sie sicher, dass Sie die EventSentry MIB auf dem Zielhost importieren. Die Datei *EventSentryV1.mib* befindet sich im Unterverzeichnis Mibs des Installationsverzeichnisses.

- Stellen Sie sicher, dass die SNMP-Verwaltungskonsole SNMP v1-Traps unterstützt.

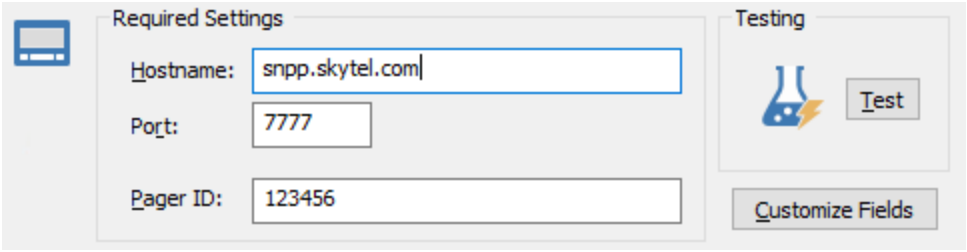
- Diese Aktion protokolliert im Falle eines Fehlers die folgenden Ereignisse im Anwendungsereignisprotokoll mit der **EventSentry**Ereignisquelle:

Ereignis-IDs	Ereignis-ID	Problem / Beschreibung
	590	Ein Trap konnte nicht gesendet werden.

4.4.9 Pager (SNPP)

Sie können die Ereignisprotokollnachricht an Ihren Pager weiterleiten, wenn Ihr Provider das SNPP-Protokoll unterstützt. Das SNPP-Protokoll ist eine vereinfachte Version des SMTP-Protokolls und ermöglicht es Ihnen, Nachrichten über TCP/IP über das Internet an den Pager zu senden.

Um herauszufinden, ob Ihr Provider SNPP unterstützt, sollten Sie die Website Ihres Providers überprüfen oder http://www.notepage.net/snpp.htm besuchen. Dort finden Sie eine Liste der meisten Paging-Provider in den USA einschließlich ihrer SNPP-Server-Details.

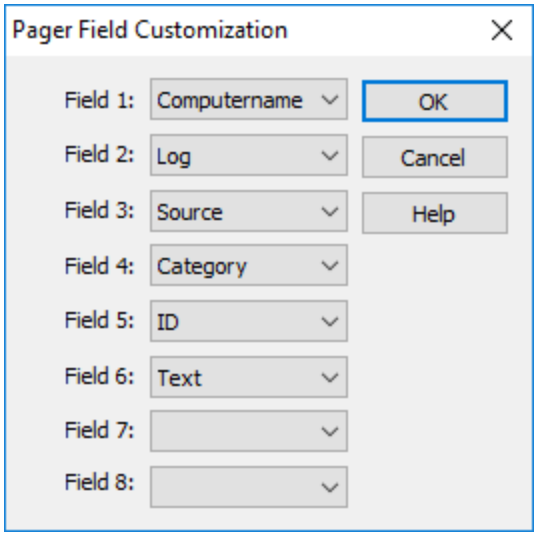


Hostname
Den Host-Namen des SNPP-Servers Ihres Providers. Erkundigen Sie sich bei Ihrem Provider, ob er seinen Kunden SNPP anbietet und was sein SNPP-Server ist, oder besuchen Sie http://www.notepage.net/snpp.htm.

Anschluss
Der TCP-Port, auf dem der SNPP-Server lauscht, normalerweise 7777 oder 444.

Pager-ID
Die Nummer des Pagers.

Felder anpassen
Sie können konfigurieren, welche Ereignisdetails an den Pager gesendet werden, indem Sie auf die Schaltfläche **Felder anpassen** klicken. Diese Funktion ist identisch mit der Funktion **Mini anpassen**, die in der E-Mail-Aktion zu finden ist:



Wählen Sie aus, welche Felder in welcher Reihenfolge Sie an den Pager gesendet haben möchten, und klicken Sie auf **OK**.

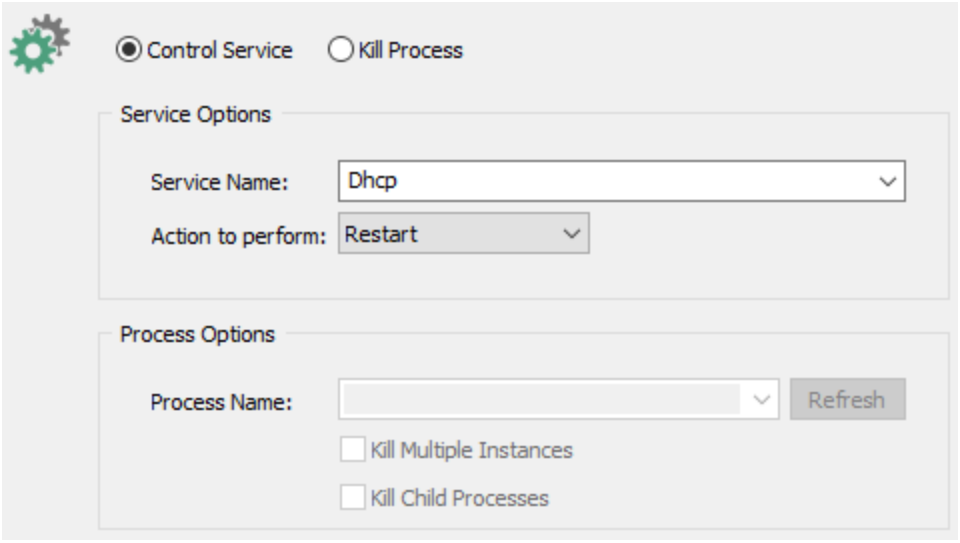
4.4.9.1 Fehlerbehebung SNPP

Diese Aktion protokolliert die folgenden Ereignisse mit der **EventSentry-Ereignisquelle** im Falle eines Fehlers im Anwendungsereignisprotokoll:

	Ereignis-ID	Problem / Beschreibung
Ereignis-IDs	600	Eine Verbindung mit dem entfernten SNPP-Host konnte nicht hergestellt werden.
	601	Eine Nachricht an den angegebenen Pager-Empfänger konnte nicht gesendet werden.
	602	Die Nachricht konnte nicht gesendet werden.

4.4.10 Service & Prozesssteuerung

EventSentry kann als Reaktion auf einen Ereignisprotokolleintrag einen Dienst steuern oder einen Prozess beenden.



Modus der Dienststeuerung

Name des Dienstes
Name des Dienstes, der kontrolliert werden soll.

Durchzuführende Aktion
Die Art der Aktion, die auf dem Dienst ausgeführt werden soll (Start, Stop, Neustart, Fortsetzen, Pause werden unterstützt).

Prozess-Kill-Modus

Prozess Name
Name des Prozesses, der beendet werden soll. Sie können hier Einfügetext wie **$STR1**, **$STR2** usw. verwenden. Dieses Feld akzeptiert PIDs sowohl in dezimaler als auch in hexadezimaler Darstellung sowie Prozessnamen, so dass es leicht direkt mit Ereignissen wie der Ereignis-ID 4688 verknüpft

werden kann. Bitte beachten Sie, dass das Pulldown-Menü nur Prozesse auf dem lokalen Rechner auflistet.

Mehrere Instanzen töten
Standardmäßig wird nur der erste gefundene Prozess, der mit dem angegebenen Namen übereinstimmt, beendet. Wenn Sie dieses Kontrollkästchen aktivieren, werden alle Prozesse beendet, die dem unter **Prozessname** angegebenen Namen entsprechen.

Kindliche Prozesse töten
Beendet rekursiv alle untergeordneten Prozesse des *Prozessnamens* , die durch den Prozess gestartet wurden.

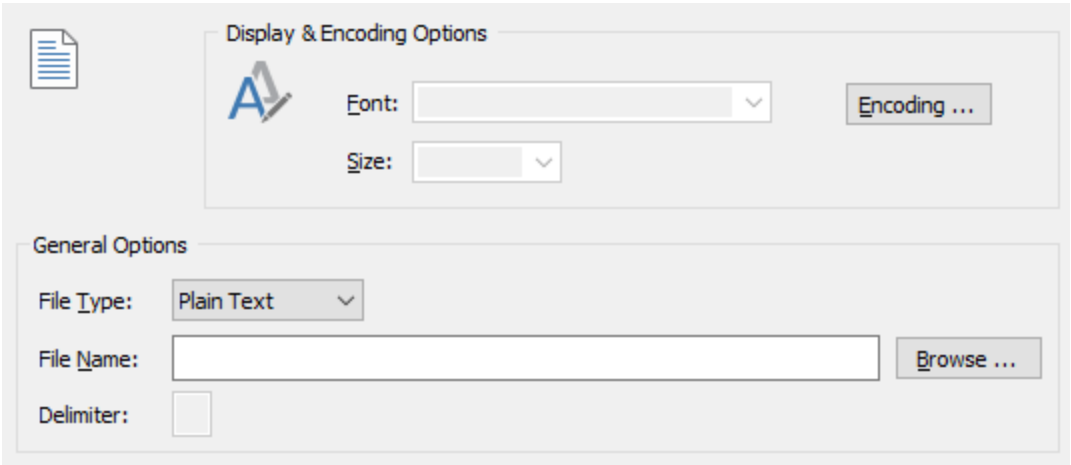
4.4.10.1 Fehlerbehebung Service Dienststeuerung

Diese Aktion protokolliert die folgenden Ereignisse mit der **EventSentry-Ereignisquelle** im Falle eines Fehlers im Anwendungsereignisprotokoll:

	Ereignis-ID	Problem / Beschreibung
Ereignis-IDs	611	Es konnte keine Verbindung zum SCM (Service Control Manager) hergestellt werden.
	612	Der angeforderte Dienst konnte nicht geöffnet werden.
	613	Der Befehl zur Steuerung des Anforderungsdienstes konnte nicht gesendet werden.
	614	Der Dienst konnte nicht wieder aufgenommen werden, weil er nicht gestoppt werden konnte.
	615	Dienststeuerungsbefehl wurde erfolgreich gesendet, der Dienst befand sich jedoch nicht im gewünschten Zustand.
	617	Der angegebene Prozess konnte nicht beendet werden.

4.4.11 Datei

EventSentry kann Ereignisprotokollaufzeichnungen in ASCII-, XHTML- oder CSV-Dateien schreiben (anhängen). Geben Sie einfach den Dateinamen und die Art der Ausgabe (ASCII, XHTML oder CSV) an, die Sie wünschen.



Dateiname

Der Name der Ausgabedatei. Die Datei wird erstellt, falls sie noch nicht existiert; das Verzeichnis wird **nicht** automatisch erstellt und muss bereits existieren. Dieses Feld unterstützt Laufzeitvariablen, um mehr über Variablen zu erfahren, klicken Sie hier.

Wenn Sie **XHTML** als Dateityp wählen und eine vorhandene Aktionsdatei haben (die nicht von EventSentry erstellt wurde), dann wird die angegebene Datei überschrieben.

Begrenzer
Geben Sie ein Trennzeichen an, das Standard-Trennzeichen ist ein Komma.

Dateityp
Das gewünschte Ausgabeformat: **Einfaches**, **(X)HTML** oder **CSV**.

*Wenn Sie die **Option (X)HTML** verwenden, können Sie auch die in den (X)HTML-E-Mails verwendete Schriftart und Größe konfigurieren. Die Standardeinstellung ist **Verdana** mit **11px**.*

Klicken Sie hier, um einen Eintrag der Häufig gestellten Fragen für diese Aktion anzuzeigen.

4.4.11.1 Fehlerbehebung bei Dateien

Lösungen für häufige Probleme mit der Dateiaktion:

- Standardmäßig ist EventSentry aufgrund von Berechtigungsproblemen **nicht** in der Lage, in eine Datei zu schreiben, die sich auf einem Remote-Server (freigegebenes Laufwerk) befindet. Der EventSentry-Dienst läuft unter dem LocalSystem-Benutzerkonto, einem Konto, das normalerweise keine Berechtigungen auf Remote-Computern hat. Eine Lösung für dieses Problem finden Sie in den FAQs zur Fehlerbehebung.

- Das Verzeichnis für den **Dateinamen** muss existieren und wird nicht von EventSentry erstellt. Der Dateiname selbst wird jedoch bei Bedarf erstellt.

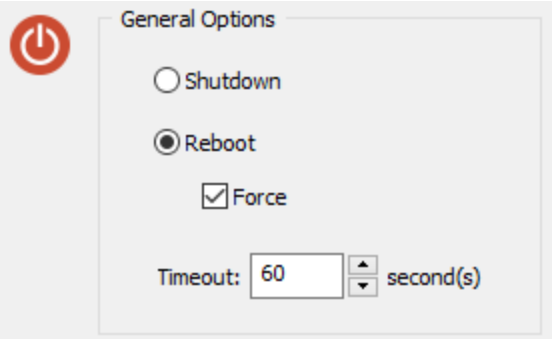
- Diese Aktion protokolliert die folgenden Ereignisse mit der **EventSentry-Ereignisquelle** im Falle eines Fehlers im Anwendungsereignisprotokoll:

 Ereignis-IDs	Ereignis-ID	Problem / Beschreibung
	510	Die angeforderte Datei konnte nicht geöffnet/erstellt werden.

Außerdem ist es im Allgemeinen nicht empfehlenswert, einen Dateinamen für mehrere Installationen von EventSentry aufgrund möglicher Zeitprobleme zu verwenden. Wenn mehr als eine Instanz von EventSentry gleichzeitig versucht, in die Datei zu schreiben, könnten einige Ereignisaufzeichnungen übersprungen werden oder die Datei beschädigt werden.

4.4.12 Herunterfahren/Neustart

EventSentry kann einen Computer neu starten oder herunterfahren.



Kraft
Eine Anwendung mit ungespeicherten Änderungen kann verhindern, dass der Computer neu gestartet oder heruntergefahren wird. Aktivieren Sie dieses Kontrollkästchen, um das Schließen von Anwendungen zu erzwingen.

Auszeit
Geben Sie die Anzahl der Sekunden an EventSentry sollte warten, bevor der Computer neu gestartet oder neu gebootet wird.

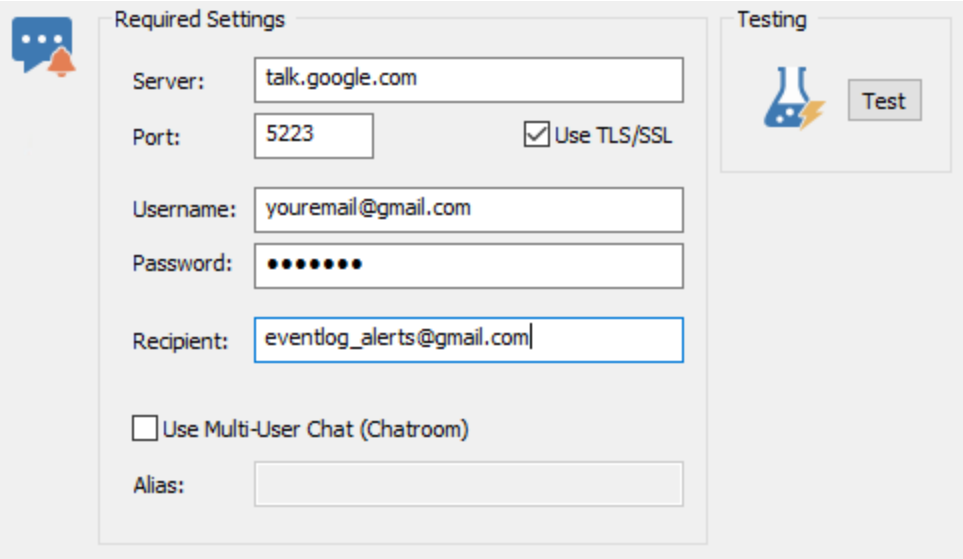
4.4.12.1 Fehlerbehebung beim Herunterfahren/Reboot

Diese Aktion protokolliert die folgenden Ereignisse im Anwendungsereignisprotokoll mit der **EventSentry** Ereignisquelle im Falle eines Fehlers:

Ereignis-IDs	Ereignis-ID	Problem / Beschreibung
	620	Ein Herunterfahren/Neustart des Systems konnte nicht eingeleitet werden.

4.4.13 Jabber

Sie können Ereignisprotokollmeldungen als Instant Messages über das Jabber-Protokoll weiterleiten. EventSentry unterstützt sowohl Klartext als auch durch TLS/SSL verschlüsselte Nachrichten. Geben Sie einfach einen Server, eine Anmeldung und einen Empfänger an, und EventSentry benachrichtigt Sie sofort über kritische Ereignisprotokollmeldungen.



Server
Der Hostname oder die IP-Adresse des Jabber-Servers.

Hafen
Geben Sie den TCP-Port des Jabber-Servers an.

TLS/SSL verwenden
Markieren Sie dieses Kästchen, wenn der Server TLS/SSL erfordert oder unterstützt.

Benutzername
Die Jabber-ID, die erforderlich ist, um sich am Jabber-Server anzumelden. Erkundigen Sie sich bei Ihrem Server-Administrator, um die korrekte Anmeldung zu bestimmen.

Kennwort
Das Passwort für "Benutzername".

Empfänger
Der Empfänger, der die Sofortnachricht auf dem Jabber-Server erhalten soll. Dies kann auch ein Chat-Raum sein (siehe unten).

Mehrbenutzer-Chat (Chat-Raum) verwenden
Markieren Sie dieses Kästchen, um Jabber-Nachrichten an einen Chat-Raum statt direkt an einen anderen Benutzer zu senden

Alias
Die meisten Chat-Räume erfordern einen Alias, geben Sie ihn hier an.

4.4.13.1 Jabber Fehlerbehebung

Lösungen für gemeinsame Probleme mit der Jabber-Aktion:

- Stellen Sie sicher, dass Sie das richtige Login verwenden. Logins für Jabber variieren und können ein Benutzername oder eine E-Mail-Adresse sein.

- Wenn Ihr Server TLS/SSL erfordert (z.B. talk.google.com), dann stellen Sie sicher, dass Sie das Kontrollkästchen "TLS/SSL verwenden" aktivieren.

- Diese Aktion protokolliert im Falle eines Fehlers die folgenden Ereignisse im Anwendungsereignisprotokoll mit der **EventSentry** Ereignisquelle:

 Ereignis-IDs	Ereignis-ID	Problem / Beschreibung
	630	Eine Verbindung zum Jabber/XMPP-Host konnte nicht hergestellt werden.
	631	Eine Nachricht konnte nicht an den Chat-Raum gesendet werden.

4.4.14 Http

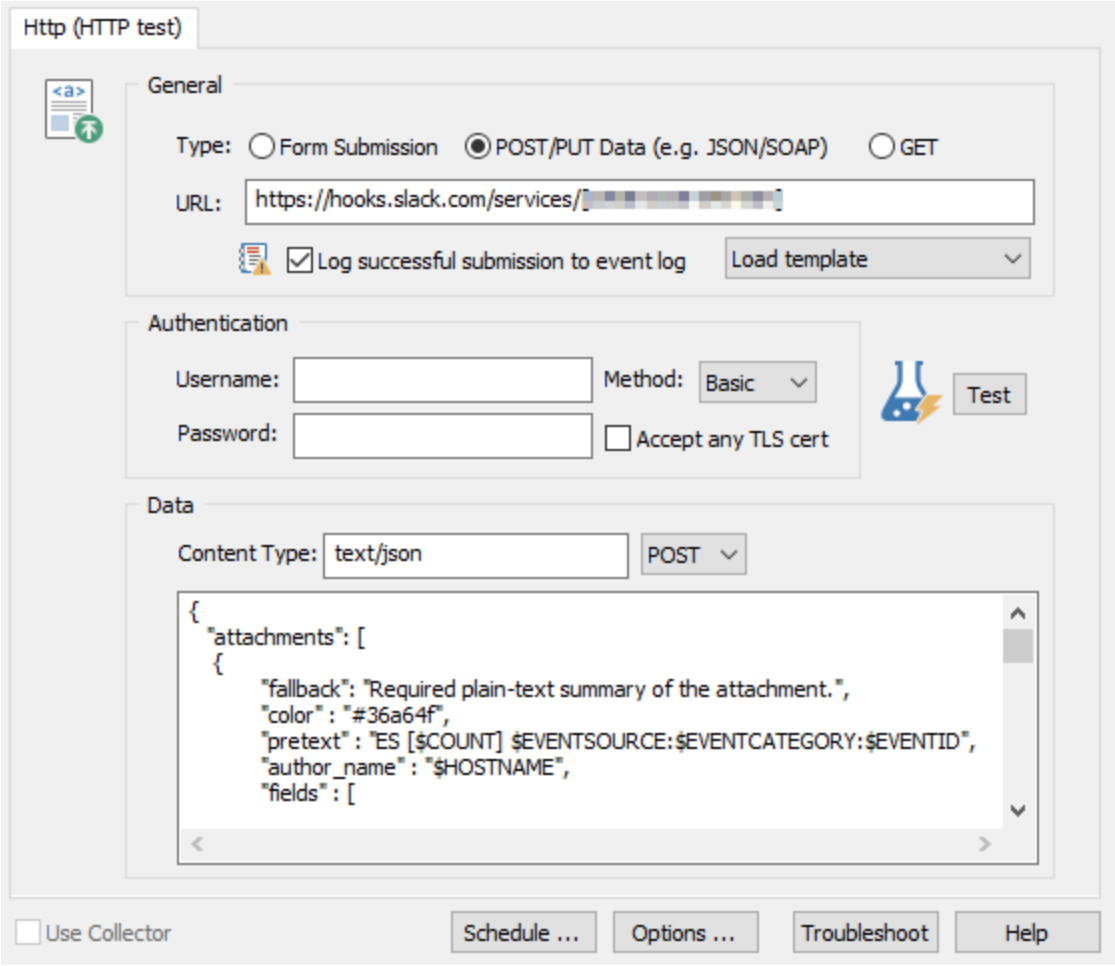
Die HTTP-Aktion kann auf verschiedene Weise mit öffentlichen HTTP-basierten APIs wie Ticketing-Systemen, Collaboration Suites und Hardware-Geräten interagieren:

- Ein Formular einreichen
- POST-Daten
- PUT-Daten
- GET-Anfrage

Die HTTP-Aktion unterstützt sowohl HTTP als auch HTTPS, Authentifizierung (Basic, Digest und NTLM) und ermöglicht die Übermittlung von bis zu 20 Formularelementen. Formularelemente können entweder statische Informationen oder dynamische Informationen durch die Verwendung von Variablen enthalten.

Beachten Sie, dass die HTTP-Aktion nicht nur durch Ereignisse ausgelöst werden kann (wie alle anderen Aktionen auch), sondern auch durch das System Tray Utility, um die Erstellung von Support-Tickets im webbasierten Ticketing-System zu erleichtern.

Die HTTP-Aktion kann entweder so konfiguriert werden, dass Daten an ein HTTP-basiertes Formular (oder Seiten, die Daten vom Formulartyp erwarten) übermittelt werden, indem **Formularübermittlung** als Typ ausgewählt wird, oder dass benutzerdefinierte Daten über eine POST- oder PUT-Anforderung übermittelt werden, indem **POST/PUT-Daten** ausgewählt werden. Lesen Sie die API-Dokumentation, um festzustellen, welcher Typ korrekt funktioniert.



Vorlage laden

Wenn Sie Ereignisdaten an einen unter Vorlagen aufgeführten Webdienst übermitteln, wählen Sie einfach die Vorlage aus, und alle erforderlichen Formularfelder werden automatisch vorgeladen. Benutzerspezifische Felder (z.B. API-Schlüssel) müssen manuell konfiguriert werden und sind mit Text in .

Um einen neuen Webdienst vorzuschlagen, der in die Liste der Vorlagen aufgenommen werden soll, senden Sie einfach eine E-Mail an unser Support-Team.

URL

Die URL der Webseite, die das einzureichende Formular enthält. Dieses Feld unterstützt Variablen.

Authentifizierung

Authentifizierungsverfahren: Basic Authentication, Digest und NTLM sind unterstützte Authentifizierungsmethoden.

Benutzername/Passwort: Die Authentifizierungsdaten.

Es wird empfohlen, nur die Basis-Authentifizierung zu verwenden, wenn ein Formular über eine sichere Webseite (https://.....) eingereicht wird.

Proxy Server
Wenn auf die angegebene Webseite über einen Proxy-Server zugegriffen werden muss, kann ein Proxy-Server mit der HTTP-Aktion verknüpft werden. Durch Klicken auf die Schaltfläche "Einstellungen" im Bereich "Proxy" wird ein Dialog angezeigt, in dem die Proxy-Einstellungen konfiguriert werden können. Wenn Sie das Kontrollkästchen "Proxy verwenden" aktivieren, werden die Proxy-Server-Einstellungen aktiviert.

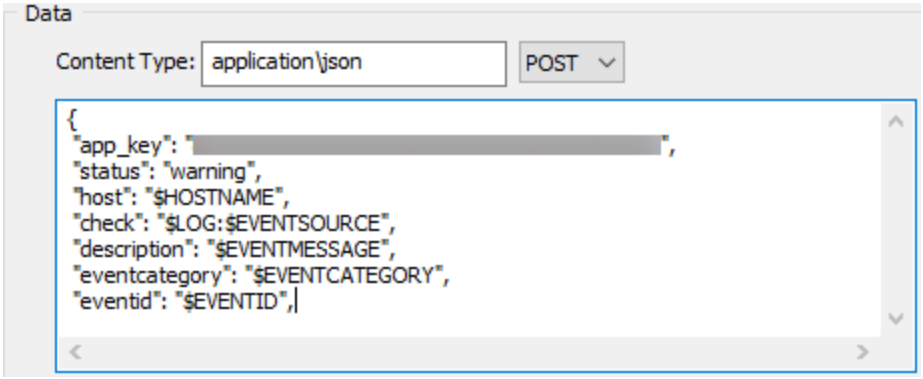
Formular-Übermittlung: Formular-Felder
Es können bis zu 20 Formularfelder angegeben werden, die eingereicht werden sollen. Sie können entweder dynamische Informationen unter Verwendung einer der unterstützten Variablen einbeziehen oder statische Informationen für die Formularfelder angeben.

Der "Name des Formularelements" ist der Name des Formularelements, während "Wert" sich auf den Inhalt des Wertes des Formularelements bezieht. Informationen darüber, welche Variablen unterstützt werden, finden Sie im Kapitel "Variablen".

POST/PUT-Daten
Für APIs, die POST- oder PUT-Anforderungen erwarten, müssen der Inhaltstyp, der Übermittlungstyp (POST/PUT) und die Daten definiert werden. Die gleichen Variablen, die in den Formularfeldern unterstützt werden, werden auch im Datenfeld unterstützt.

Nach UTF8 konvertieren: Konvertiert dynamische Daten aus Variablen (z.B. $EVENTSOURCE, $EVENTMESSAGE ...) vor der Übertragung nach UTF8.

Ein typischer POST/PUT-Aufbau ist in der Abbildung unten dargestellt:



GET
Übermittelt eine HTTP-GET-Anfrage an die angegebene URL. Die von der Webseite zurückgegebenen Daten sind im Ereignis 642 verfügbar, das protokolliert wird, wenn die HTTP(S)-GET-Anfrage erfolgreich war.

4.4.14.1 Fehlerbehebung HTTP

Bei Formulareinreichungen lädt der HTTP die Webseite, die das Formular enthält, vor dem Einreichen nicht herunter. Daher müssen alle notwendigen Formularfelder in der Liste angegeben werden (z.B. Felder *vom Typ input type="submit"*).

Beispielsweise werden HTML-basierte Formulare manchmal über eine Submit-Schaltfläche (<input type="submit" name="NameOfButton" value="SomeValue">) eingereicht. Wenn dies der Fall ist, muss

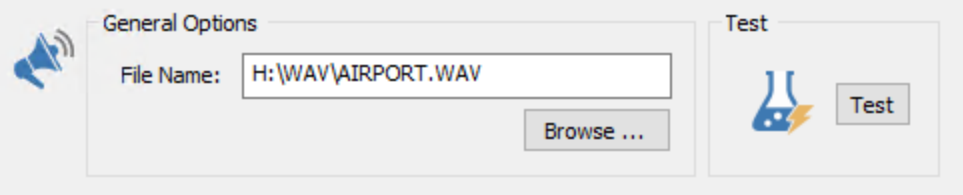
das Name/Wert-Paar für den Submit-Button ("NameOfButton"/"SomeValue" für das vorherige Beispiel) in der Aktion angegeben werden.

Diese Aktion protokolliert die folgenden Ereignisse im Ereignisprotokoll der Anwendung mit der **EventSentry** Ereignisquelle:

Ereignis-IDs	Ereignis-ID	Problem / Beschreibung
	640	Das webbasierte Formular kann nicht eingereicht werden.
	642	Aktion wurde erfolgreich ausgelöst.

4.4.15 Ton

EventSentry kann eine wav-Datei abspielen, um anzuzeigen, dass ein Ereignis eingetreten ist. Diese Sounddatei wird unabhängig von der Verwaltungskonsole abgespielt, die ebenfalls einen Sound abspielen kann, wenn ein Ereignis eingetreten ist.



Dateiname
Der Dateiname der abzuspielenden wav-Datei. Damit dies funktioniert, muss im Computer eine Soundkarte installiert sein.

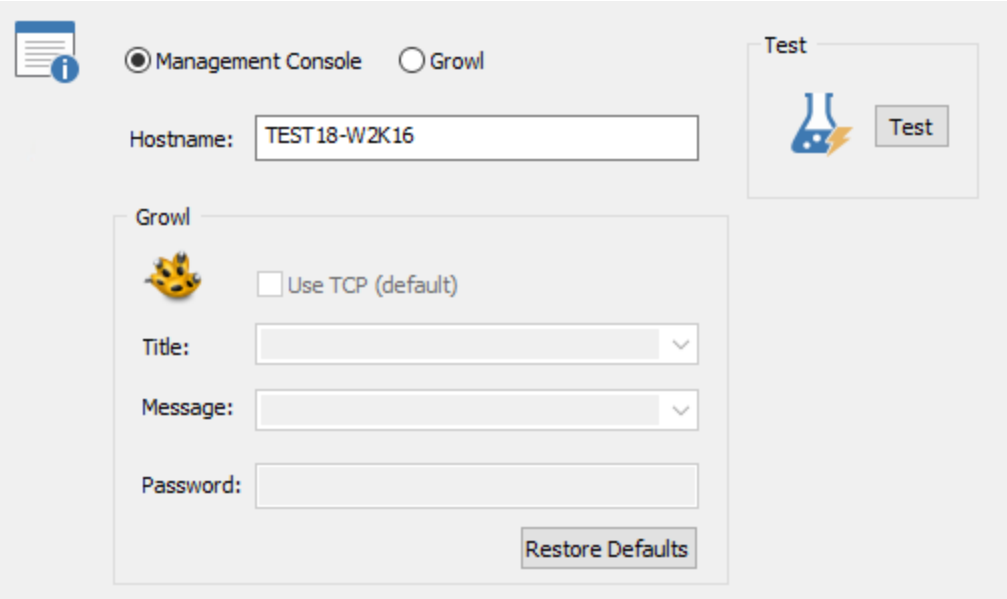
Test
Klicken Sie auf die Schaltfläche "**Test**", um die Sounddatei abzuspielen.

4.4.15.1 Fehlerbehebung Ton

Zur Zeit sind keine Informationen zur Fehlerbehebung verfügbar.

4.4.16 Desktop

Leitet ein Ereignis entweder an eine lokale/ferne Instanz der Verwaltungskonsole oder an eine Instanz von Growl weiter.



Verwaltungskonsole
Der empfangende Host muss die Verwaltungskonsole laufen haben und muss so konfiguriert werden (Extras - Optionen - Allgemein), dass entweder ein Pop-up-Fenster oder eine Sprechblasenmeldung angezeigt wird. Die Verwaltungskonsole kann auch so konfiguriert werden, dass sie eine WAV-Datei abspielt.

> Da die Desktop-Aktion Windows-Mailslots zum Senden von Nachrichten über das Netzwerk verwendet, die **keine Verschlüsselung oder Authentifizierung unterstützen**, wird empfohlen **keine sicherheitsempfindlichen Informationen** über diese Benachrichtigung **zu senden**. Es wird auch empfohlen, sicherheitsempfindliche Nachrichten, die über die Desktop-Aktion von entfernten Hosts empfangen werden, zu verifizieren, da sie gefälscht werden könnten.

Growl
Leitet eine Veranstaltung an einen Gastgeber weiter, bei dem Growl läuft. Eine oder mehrere Variablen können in den Feldern "Titel" und "Nachricht" verwendet werden, die verfügbaren Variablennamen können durch Klicken auf den Pfeil in der Dropdown-Steuerung angezeigt werden. Ein Passwort ist nur dann erforderlich, wenn der Host, auf dem Growl läuft, ein Passwort verlangt. "TCP verwenden" wird für die meisten Szenarien empfohlen. **Netzwerk-Benachrichtigungen zulassen** muss im Dialogfeld **Growl-Sicherheit** aktiviert werden.

Hostname
Geben Sie den Hostnamen an, an den die Nachrichten gesendet werden sollen.

Test
Sendet eine Testnachricht.

4.4.16.1 Troubleshooting desktop notifications

Lösungen für häufige Probleme mit der Desktop-Aktion:

- Die Verwaltungsanwendungen müssen aktiv und korrekt konfiguriert sein, damit diese Aktion ordnungsgemäß funktioniert. Weitere Informationen finden Sie auf der vorherigen Seite.
- Stellen Sie sicher, dass die Desktop-Benachrichtigungen (entweder als Sprechblase oder Popup-Fenster) in den *Allgemeinen Optionen* der Verwaltungsanwendung aktiviert sind.
- Stellen Sie sicher, dass Growl läuft und so konfiguriert ist, dass es Netzwerknachrichten akzeptiert. Wenn ein Passwort konfiguriert ist, stellen Sie sicher, dass das Passwort übereinstimmt.

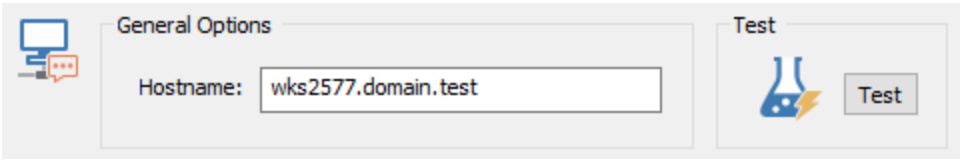
Diese Aktion protokolliert im Falle eines Fehlers die folgenden Ereignisse im Anwendungsereignisprotokoll mit der EventSentry Ereignisquelle:

Ereignis-IDs	Ereignis-ID	Problem / Beschreibung
	580	Ein Mailslot konnte nicht erstellt werden.
	581	Die Aktion "%1" konnte keine Benachrichtigung an den (entfernten) Growl-Hörer senden. Stellen Sie sicher, dass auf dem entfernten Rechner Growl läuft, Netzwerknachrichten akzeptiert und keine Firewall den Verkehr blockiert.

4.4.17 Netzwerk-Nachricht

Sendet eine Netzwerknachricht, ähnlich dem Befehlszeilen-Dienstprogramm "msg.exe", an einen Remote-Host über die Remote Desktop Services API. Wenn "Remotedesktopdienste verwenden" nicht angekreuzt ist, wird eine Nachricht über den "Messenger"-Dienst gesendet.

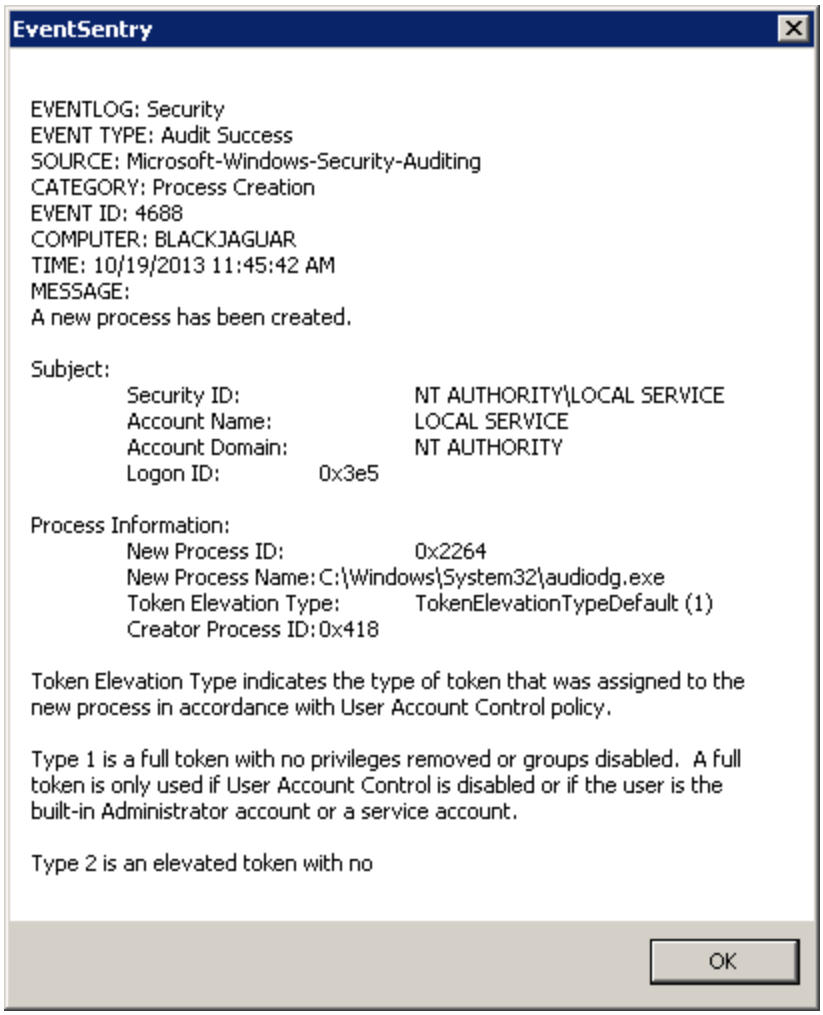
Der Host, der die Nachricht sendet, muss dazu berechtigt sein, siehe Voraussetzungen für weitere Informationen.



Wenn der Host, der die Nachricht empfängt, unter Windows 2003 oder höher läuft, sollte "Remotedesktopdienste verwenden" immer markiert sein.

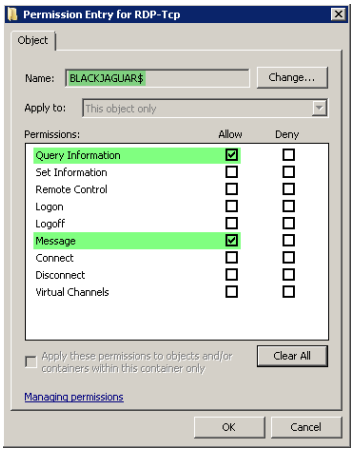
Hostname
Host welcher die Nachricht erhält. Der Remote-Host muss den "Messenger"-Dienst ausführen, wenn "Remotedesktopdienste verwenden" nicht angekreuzt ist.

Test
Klicken Sie auf diese Schaltfläche, um eine Testnachricht an den Remote-Host zu senden.



4.4.17.1 Voraussetzungen

Wenn "Remotedesktopdienste verwenden" aktiviert ist (Standardeinstellung), ist es wichtig, dass der Agent die Erlaubnis hat, die Nachricht an den entfernten Host zu senden, der die Nachricht empfängt. Das Konto, das versucht, die Nachricht zu senden, benötigt die Berechtigungen "Informationen abfragen" und "Nachricht" (siehe Bild unten).



Wenn der EventSentry Agent unter dem LocalSystem-Konto ausgeführt wird, benötigt das Computerkonto (z.B. SERVER05$) diese Berechtigungen. Wenn der EventSentry Agent so umkonfiguriert wurde, dass er unter einem bestimmten Benutzerkonto läuft, dann benötigt dieses Benutzerkonto die Berechtigungen "Abfrage von Informationen" und "Nachricht".

Befolgen Sie diese Anweisungen, um einen Benutzer oder ein Computerkonto zum Senden von Nachrichten zu autorisieren:

1. Melden Sie sich bei dem Rechner an, der die Nachrichten empfangen soll
2. Öffnen Sie "Ferndesktop-Sitzungs-Host-Konfiguration" unter "Verwaltungswerkzeuge\Ferndesktop-Dienste".

3. Klicken Sie im Hauptschmerz unter "Verbindungen" mit der rechten Maustaste auf "RDP-Tcp" und wählen Sie "Eigenschaften".
4. Klicken Sie auf die Registerkarte "Sicherheit".
5. Klicken Sie auf "Hinzufügen", und fügen Sie den Benutzer oder das Computerkonto zur Liste hinzu.
6. Vergewissern Sie sich, dass der Benutzer in der Benutzerliste ausgewählt ist, und klicken Sie unten rechts auf "Erweitert".
7. Wählen Sie das soeben hinzugefügte Benutzerkonto aus und klicken Sie auf "Bearbeiten".
8. Stellen Sie sicher, dass nur "Query Information" und "Message" auf "Allow" gesetzt sind, wie im Screenshot dargestellt.
9. Schliessen Sie alle Dialoge mit "OK".
10. In den meisten Fällen ist es notwendig, den Rechner neu zu starten, auf dem die Berechtigungen vorgenommen wurden.

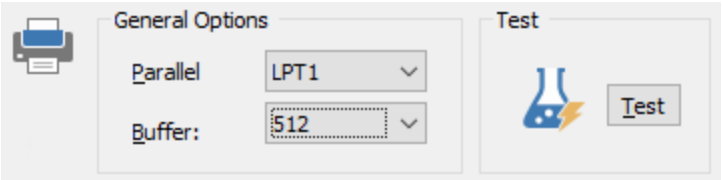
Diese Aktion protokolliert die folgenden Ereignisse im Anwendungsereignisprotokoll mit der EventSentry Ereignisquelle im Falle eines Fehlers:

Ereignis-IDs	Ereignis-ID	Problem/Beschreibung
	550	Eine "net send" Nachricht konnte nicht gesendet werden.

4.4.18 Parallel-Drucker

EventSentry kann Ereignisprotokolleinträge auf einem Drucker ausdrucken, der in der Lage ist, ASCII-Zeichen zu interpretieren, die an den Parallelport gesendet werden. Die meisten Matrixdrucker auf dem Markt unterstützen dies.

Ein Beispiel für das Drucken von Ereignisprotokolleinträgen ist das Drucken von Auditfehlern des Sicherheitsereignisprotokolls. Schließen Sie einen Matrixdrucker an einen unternehmenskritischen Server an und drucken Sie **Audit-Fehler** auf den Matrixdrucker. In diesem Fall gehen selbst dann keine Informationen verloren, wenn es einem Angreifer gelingt, die Protokolldateien aus der Ferne zu löschen.



Hafen
Die Anschlüsse, an die der Drucker angeschlossen ist, werden unterstützt: **LPT1**, **LPT2** oder **LPT3**.

Puffer-Länge
Wenn der Drucker offline ist, dann EventSentry puffert bis zu Ereignisprotokolleinträgen der **Pufferlänge**. Die Puffergröße kann zwischen **256** und **32768** liegen.

Um zu testen, ob Ihr Drucker ordnungsgemäß funktioniert, schließen Sie ihn einfach an den ausgewählten parallelen Anschluss an und drücken Sie auf **Test**. Wenn der Drucker eine Testzeile druckt, können Sie diesen Drucker verwenden.

EventSentry kann nur dann auf den parallelen Anschluss drucken, wenn keine andere Anwendung den ausgewählten Anschluss verwendet. Darüber hinaus müssen Sie

sicherstellen, dass kein installierter Windows-Drucker für die Verwendung des gewählten Druckeranschlusses konfiguriert ist. Andernfalls empfängt und verarbeitet der Spoolerdienst EventSentry. Der Drucker druckt eine Testlinie aus, die nicht die gewünschten Ergebnisse liefert.

4.4.18.1 Fehlerbehebung bei Parallеldruckern

Zur Zeit sind keine Informationen zur Fehlerbehebung verfügbar.

4.5 Computer-Gruppen

Computergruppen ermöglichen es Ihnen, Server und Workstations in Gruppen zu kategorisieren, so dass Sie große Mengen von Servern und Workstations einfacher verwalten können. EventSentry benötigt mindestens eine Gruppe, um ordnungsgemäß zu funktionieren, und der lokale Computer wird immer automatisch der ersten verfügbaren Gruppe hinzugefügt, wenn er in einer anderen Gruppe nicht vorhanden ist.

Gruppentypen

Es gibt drei verschiedene Arten von Gruppen, die Sie in EventSentry erstellen können:

 Remote-Update Only Group
Verwaltet entfernte EventSentry-Agenten (z. B. Agenten installieren, Agenten aktualisieren usw.).

 Heartbeat-Enabled Windows Group (default)
Verwaltet Remote-Agenten (genau wie die Gruppe "Nur Remote-Update"), überwacht aber auch die Betriebszeit und Verfügbarkeit (Hosts und Agenten).

 Active-Directory Linked Group
Mit Active Directory (AD) verknüpfte Gruppen können entweder eine "Remote-Update Only"- oder eine "Heartbeat-Enabled Windows"-Gruppe sein, aber die Gruppenzugehörigkeit ist direkt mit einer OU oder Gruppe in Active Directory verknüpft (weitere Informationen).

 Heartbeat-Only Group
Dieser Gruppentyp ist nur für die Überwachung von Hosts ohne Verwendung eines Agenten durch PING- und TCP-Prüfungen vorgesehen. Dieser Gruppentyp ist nützlich zur Überwachung von Unix-basierten Computern, Routern, Druckern, Switches usw.

Standarddatenbank für Gruppen

Einer Gruppe kann eine Standarddatenbankaktion zugewiesen werden, auf die dann in einem Paket dynamisch verwiesen werden kann. Auf diese Weise kann für jede Gruppe eine eigene Datenbank konfiguriert werden, die von Agenten dynamisch genutzt werden kann, ohne dass eine Duplizierung von Paketen erforderlich ist.

Verwalten von Gruppen

Hinzufügen einer Gruppe
Sie können eine neue Gruppe hinzufügen, indem Sie mit der rechten Maustaste auf "Computergruppen" klicken und "Gruppe hinzufügen" wählen.

Löschen einer Gruppe
Sie können eine Gruppe löschen, indem Sie mit der rechten Maustaste auf den Gruppencontainer klicken und "Löschen" wählen. Alle Informationen, einschließlich aller Paketzuordnungen, werden **permanent entfernt**, sobald Sie die Konfiguration speichern.

Umbenennen einer Gruppe
Sie können eine Gruppe umbenennen, indem Sie mit der rechten Maustaste auf den Gruppencontainer klicken und "Umbenennen" wählen oder indem Sie die Gruppe auswählen und die Taste F2 auf Ihrer Tastatur drücken.

Pakete zuweisen
Sie können Pakete entweder einer **Gruppe** oder einem Computer zuweisen. Um ein Paket einer Gruppe zuzuweisen, klicken Sie mit der rechten Maustaste auf die Gruppe und wählen Sie "**Assign Package(s)**". ". Um ein Paket einem Computer zuzuordnen, klicken Sie mit der rechten Maustaste auf den Computer, und wählen Sie "**Assign Package(s)**". ".

Hinzufügen von Computern
Sie können Computer, die überwacht werden sollen, entweder manuell hinzufügen oder sie mit Hilfe des Import-Assistenten importieren. Klicken Sie hier für weitere Informationen.

Zusätzliche Authentifizierung einstellen
Wenn Sie Ihre aktuellen Anmeldedaten nicht zur Verwaltung von Remote-Computern verwenden können, können Sie mit dem Authentifizierungsmanager Anmeldedaten zuweisen.

Der von Ihnen eingegebene Benutzername und das Passwort werden in der Registrierung verschlüsselt und können nur von dem Benutzer entschlüsselt werden, der sie verschlüsselt hat. Wenn sich z.B. **Admin1** an einem Computer anmeldet und einen Benutzernamen/ein Passwort für eine Gruppe oder einen Computer festlegt und **Admin2** sich am selben Computer anmeldet, dann kann Admin2 den von **Admin1** eingegebenen Benutzernamen und das Passwort nicht sehen.

Um zuvor festgelegte Anmeldedaten zu entfernen, befolgen Sie dasselbe Verfahren, klicken Sie stattdessen jedoch auf die Schaltfläche "**Remove Authentication**".

Wenn Sie beabsichtigen, den Status des EventSentry-Agenten auf Computern in einer Gruppe zu überwachen, in der Sie **die Authentifizierung festlegen**, dann lesen Sie bitte diesen Hinweis.

Verwalten von EventSentry-Agenten
Sie können Remote Update verwenden, um Remote-Agenten zu verwalten (Agenten installieren, Agenten aktualisieren, die neueste Konfiguration verschieben usw.).

Verwendung von Variablen
Sie können überall in EventSentry Variablen verwenden, um die Konfiguration und Verwaltung des Produkts zu erleichtern. Variablen werden erstellt und definiert, indem Sie mit der rechten Maustaste auf den Container **Computer Groups** klicken, und können auf der Ebene der einzelnen Gruppen überschrieben werden. Weitere Informationen finden Sie unter "Variablen".

4.5.1 Hinzufügen von Hosts

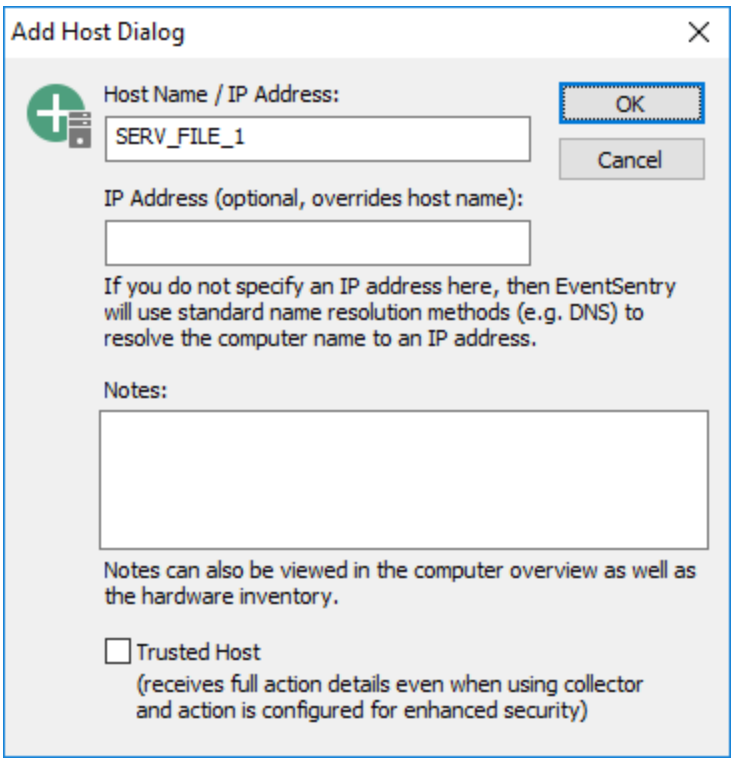
Computer können auf verschiedene Weise zu einer Gruppe hinzugefügt werden:

- Manuell
- Aus einer Textdatei importiert
- Importiert aus der Netzwerkumgebung
- Aus einem Netzwerkscan importiert

- Aus Active Directory importiert
- Verknüpft mit einer Active Directory OU oder Gruppe

Computer einzeln hinzufügen

Klicken Sie mit der rechten Maustaste auf eine Gruppe und wählen Sie **"Add Computer / IP Address ..."**. Wenn EventSentry so konfiguriert ist, dass Sie beim Hinzufügen von Computern nach einer IP-Adresse gefragt werden (Tools -> Options -> Remote Update), dann wird Ihnen der folgende Dialog angezeigt:



Wenn Sie in diesem Dialogfeld im Feld "IP-Adresse (optional)" eine IP-Adresse angeben, fügt EventSentry den Hostnamen zum Gruppencontainer hinzu, stellt jedoch immer eine Verbindung zur IP-Adresse des Remote-Hosts her, anstatt eine Verbindung über den Hostnamen herzustellen. Wenn Sie lieber mit IP-Adressen arbeiten, können Sie auch einfach die IP-Adresse in das Feld "Computername / IP-Adresse" eingeben.

Wenn EventSentry nicht so konfiguriert ist, dass Sie zur Eingabe einer IP-Adresse aufgefordert werden, werden Sie aufgefordert, den Hostnamen oder die IP-Adresse einzugeben.

Hinweise

Sie können auch Notizen für einen Computer eingeben, die dann unter "Inventar - Computer" in den Web Reports sichtbar sind.

Trusted Host

Vertrauenswürdige Hosts erhalten vollständige Aktionsdetails (z. B. Datenbankverbindungszeichenfolge), selbst wenn eine Aktion für erhöhte Sicherheit konfiguriert ist. Ein Host sollte als vertrauenswürdiger Host konfiguriert werden, wenn:

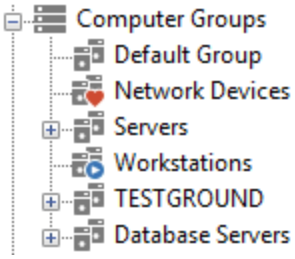
- Ein Collector ist aktiviert und in Verwendung
- Eine Aktion ist für erhöhte Sicherheit konfiguriert

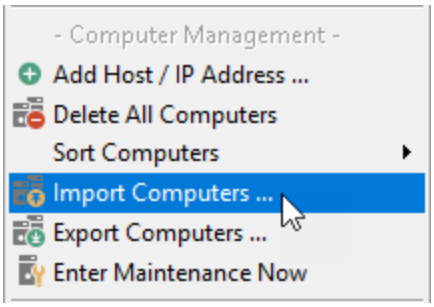
- Der Host führt entweder den Heartbeat-Dienst, den Netzwerkdienste-Dienst oder ein anderes EventSentry-Dienstprogramm (z. B. Datenbank-Import, Bereinigungsdienstprogramm) aus, das vollständige Angaben zu einer bestimmten Aktion erfordert.

Es wird empfohlen keine FQDN-Namen zu verwenden wenn Sie Computer hinzufügen, die nicht mit einer Active Directory-Domäne verbunden sind. Andernfalls können Probleme mit Paketzuweisungen auftreten.

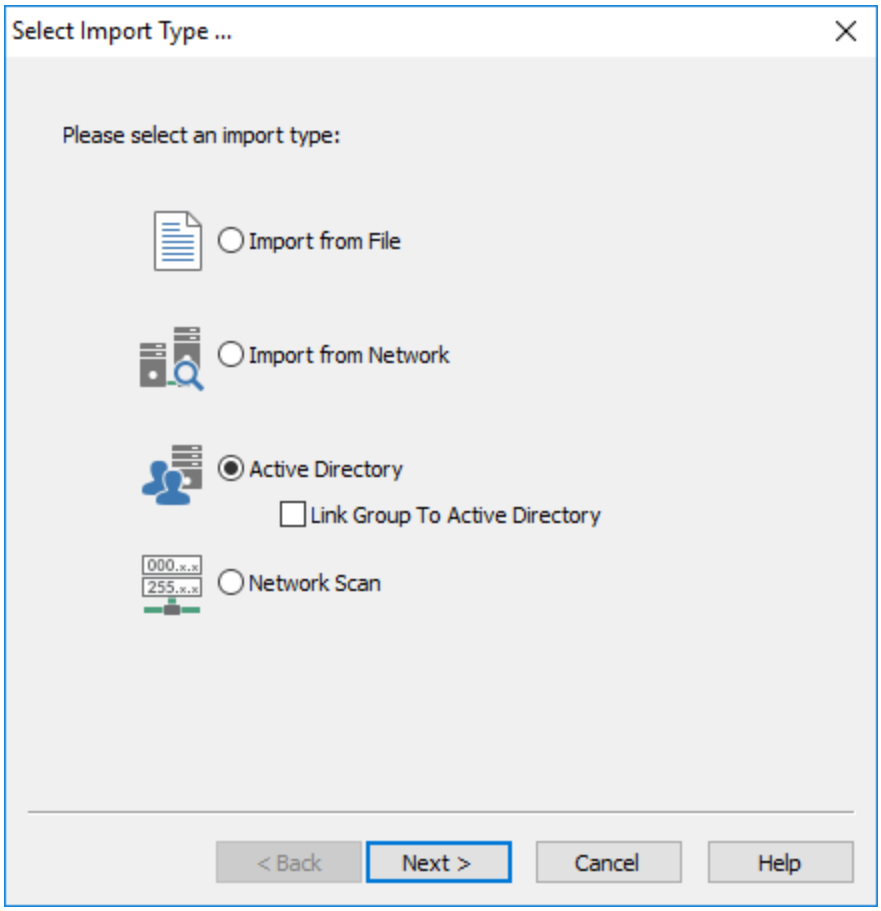
Importieren

Um den Importvorgang zu starten, klicken Sie mit der rechten Maustaste auf einen Gruppencontainer und wählen Sie "**Computer importieren ...**". ".





Dadurch wird der **Import-Assistent** wie unten dargestellt gestartet. Wählen Sie eine Importart und klicken Sie auf **Next**.

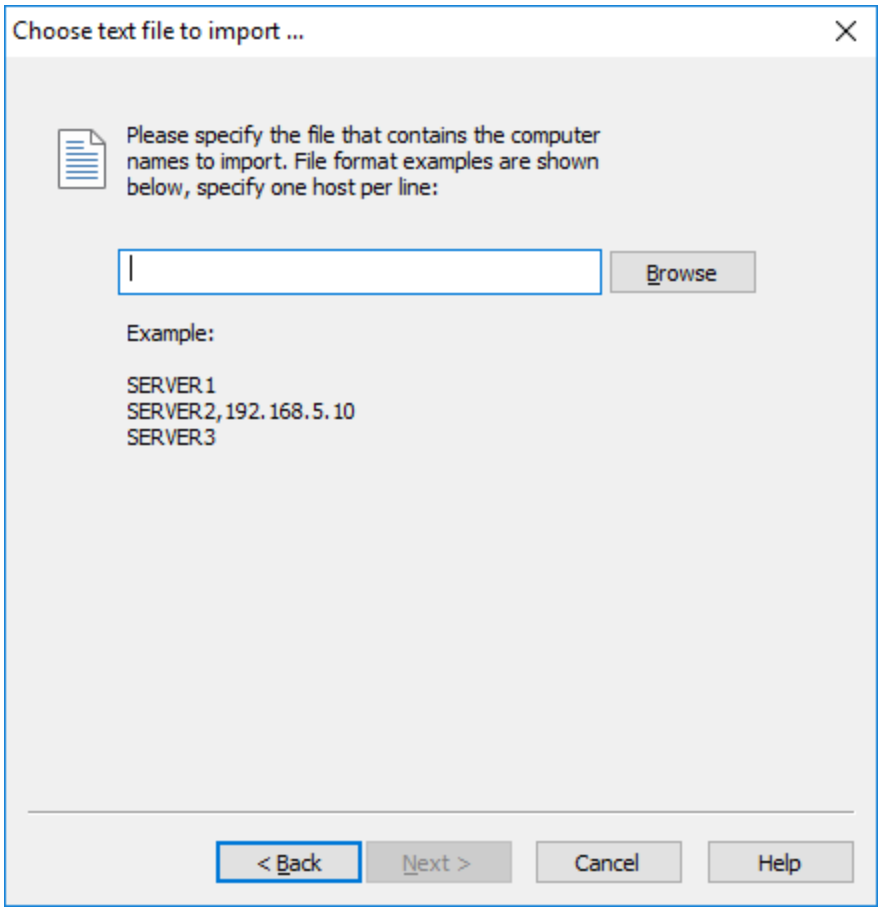


Klicken Sie auf die untenstehenden Links, um weitere Informationen zu einer bestimmten Importart zu erhalten:

- Importieren aus einer Textdatei
- Import aus der Netzwerkumgebung
- Importieren aus Active Directory
- Link zu Active Directory

4.5.1.1 Aus Textdatei importieren

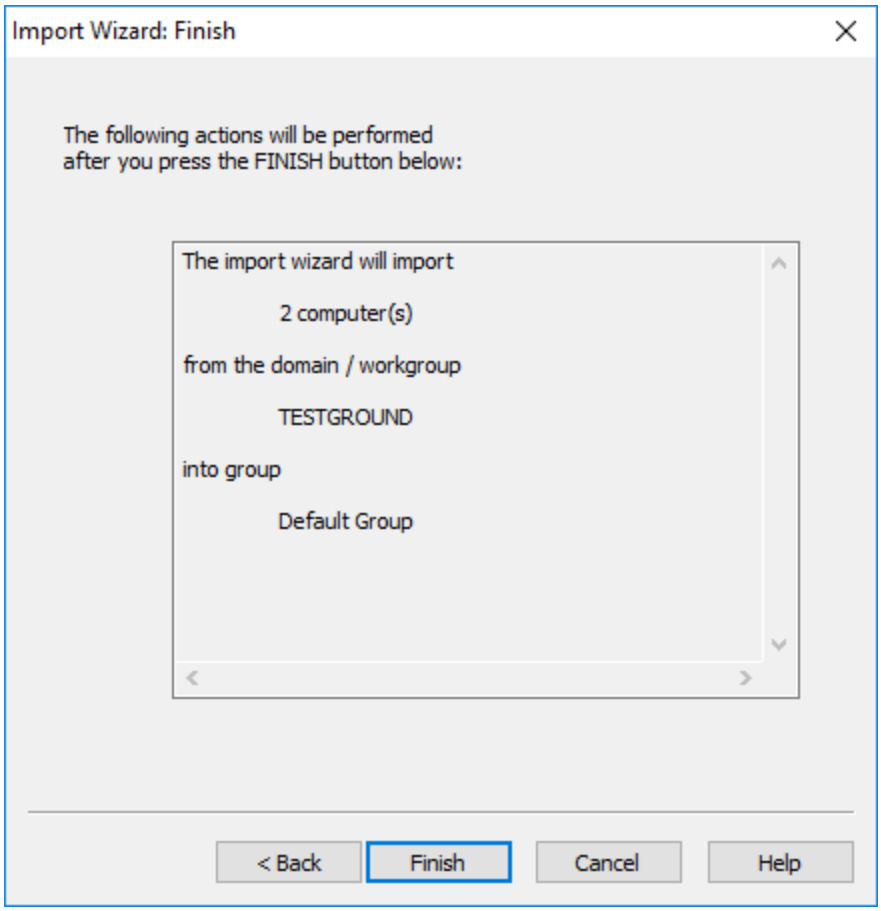
Nach Auswahl der Importmethode **Import aus Datei** wird Ihnen das unten gezeigte Dialogfeld angezeigt:



Beim Importieren werden alle in der Importdatei angegebenen Computer zur aktuellen Liste der Computer hinzugefügt, die Datei sollte pro Zeile einen Computernamen enthalten. Vorhandene Computer werden nicht aus der Liste entfernt.

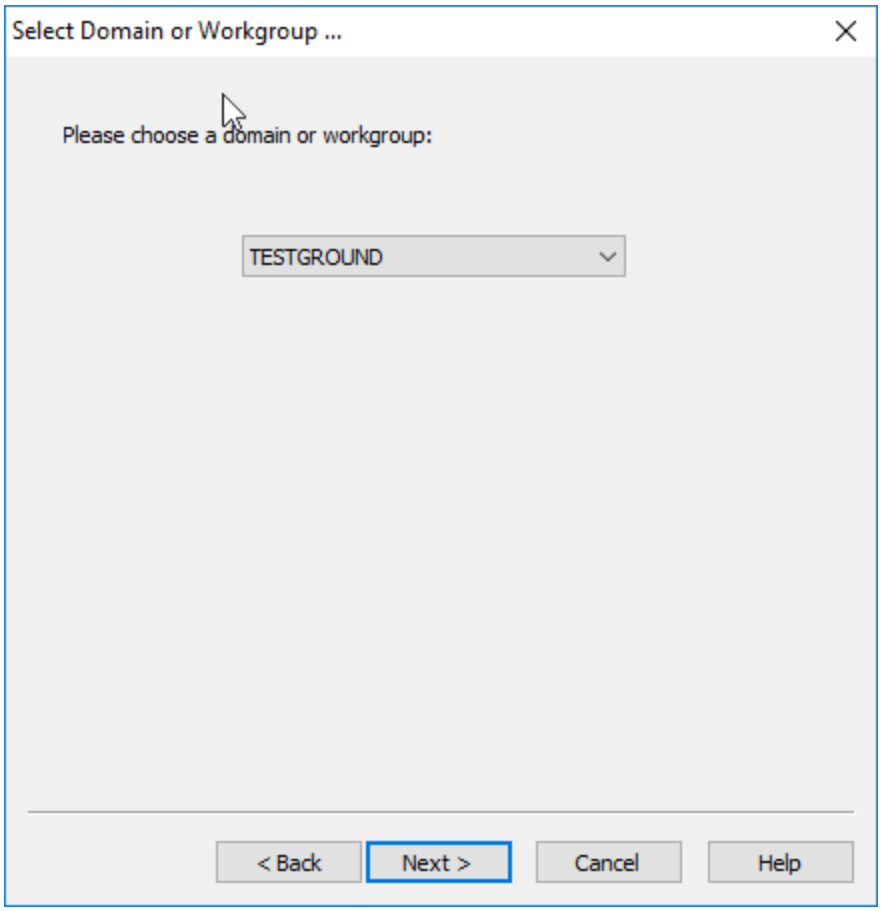
Hinweis: Wenn die Importdatei keine Gruppenzuweisungen enthält (siehe Dateiformat in "Exportieren"), werden alle Computer der Datei zur aktuell ausgewählten Gruppe hinzugefügt. Wenn die Datei Gruppenzuweisungen enthält, werden nur Computer aus übereinstimmenden Gruppen importiert.

Nachdem Sie die zu importierende Datei ausgewählt haben, klicken Sie auf **Weiter**, um den Zusammenfassungsbildschirm anzuzeigen:

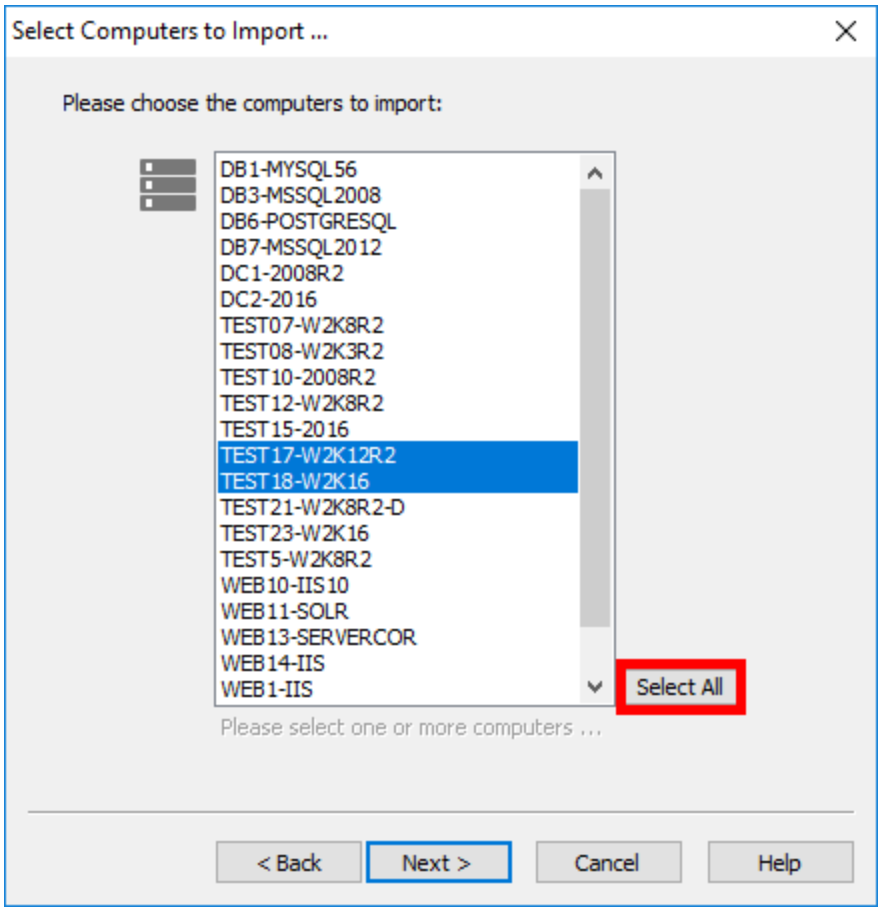


4.5.1.2 Import aus Netzwerkumgebung

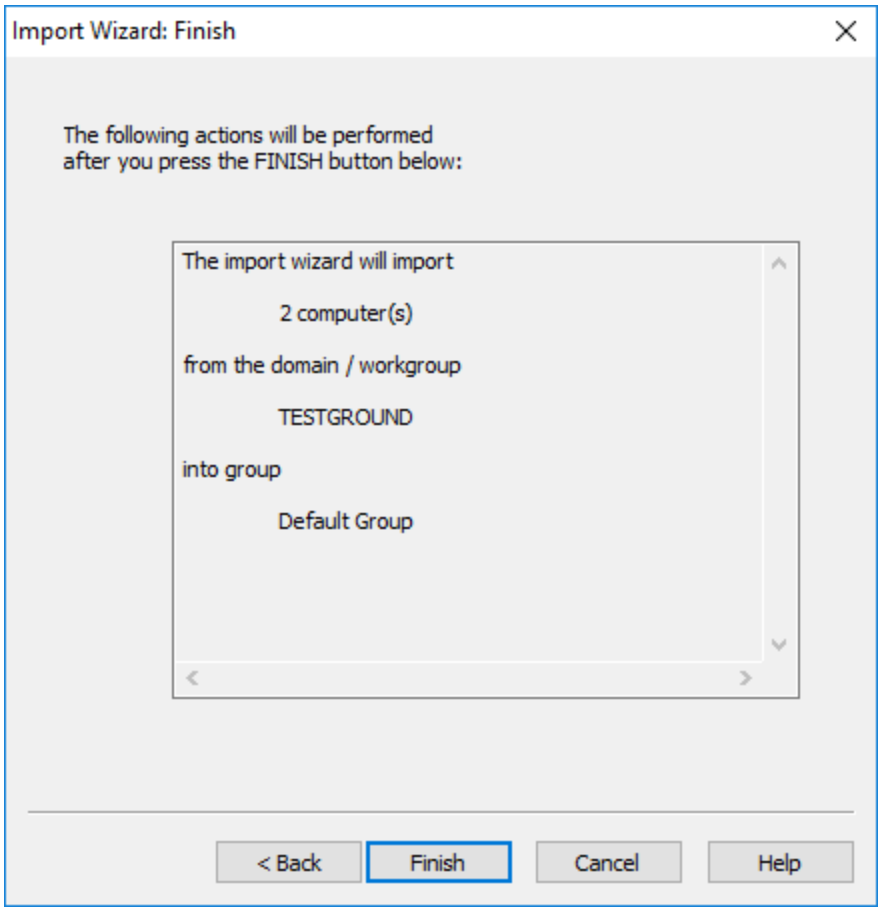
Nachdem Sie die Importmethode **Import aus Netzwerk** gewählt haben, wird Ihnen das unten gezeigte Dialogfeld angezeigt:



Wählen Sie eine Domäne und klicken Sie dann auf **Weiter**, um die einzelnen Computer auszuwählen:

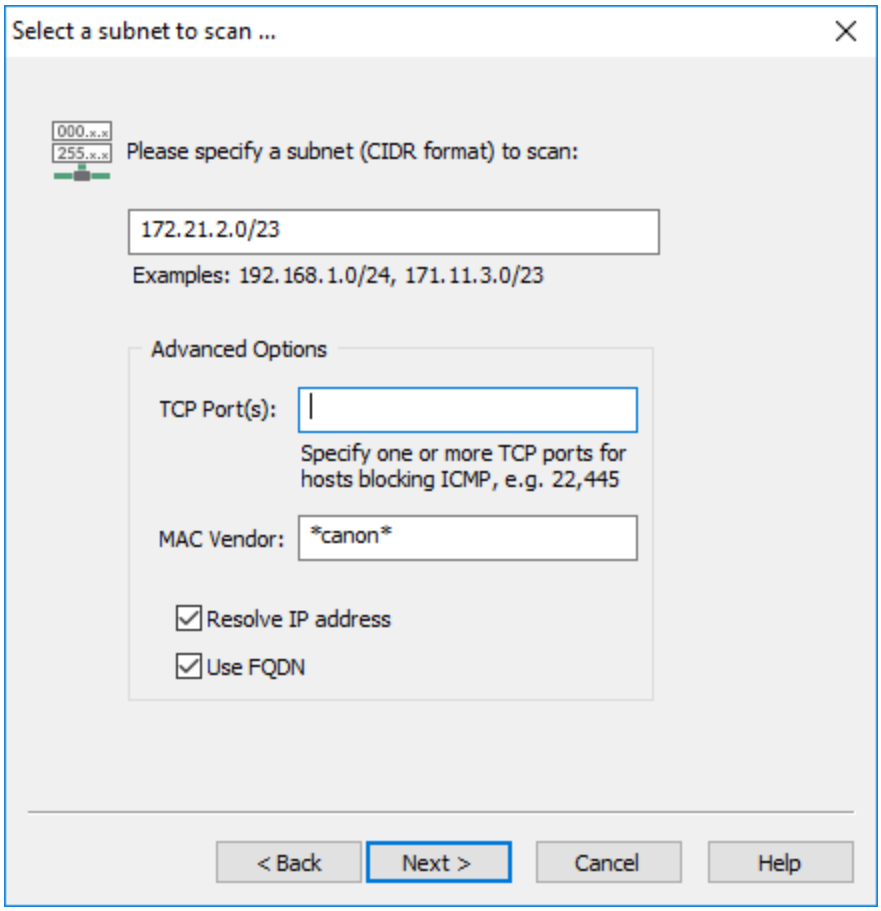


Wenn Sie auf einen Computernamen klicken, wird der Name in der Liste entweder aus- oder abgewählt. Um alle Computer auszuwählen, klicken Sie auf die Schaltfläche **Alle auswählen**. Wenn Sie fertig sind, klicken Sie auf **Weiter**, um den Zusammenfassungsbildschirm wie unten dargestellt anzuzeigen. Klicken Sie auf Fertig stellen, um den Importvorgang zu starten.



4.5.1.3 Netzwerk-Scan

Mehrere Hosts können schnell aus einem Netzwerkscan (Discovery) importiert werden. Ein Netzwerk-Scan ist auf ein bestimmtes Subnetz gerichtet und startet einen Multi-Threaded-Scan aller verfügbaren IP-Adressen im angegebenen Adressbereich.



Teilnetz
Gibt das zu scannende Subnetz im CIDR-Format an.

TCP-Port(s)
Ermöglicht die Entdeckung von Hosts, die nicht auf Ping-Anfragen (ICMP) antworten, sondern auf einem TCP-Port lauschen. Standardmäßig werden Hosts durch Ping (ICMP)-Anforderungen entdeckt, aber wenn dies nicht gelingt, können sie auch über einen oder mehrere TCP-Ports entdeckt werden. Wenn ein oder mehrere TCP-Ports konfiguriert sind, EventSentry versucht zunächst, die IP-Adresse zu pingen, und versucht, wenn keine Antwort eingeht, eine TCP-Verbindung zu den aufgeführten TCP-Ports herzustellen. Mehrere TCP-Ports müssen durch ein Komma getrennt werden.

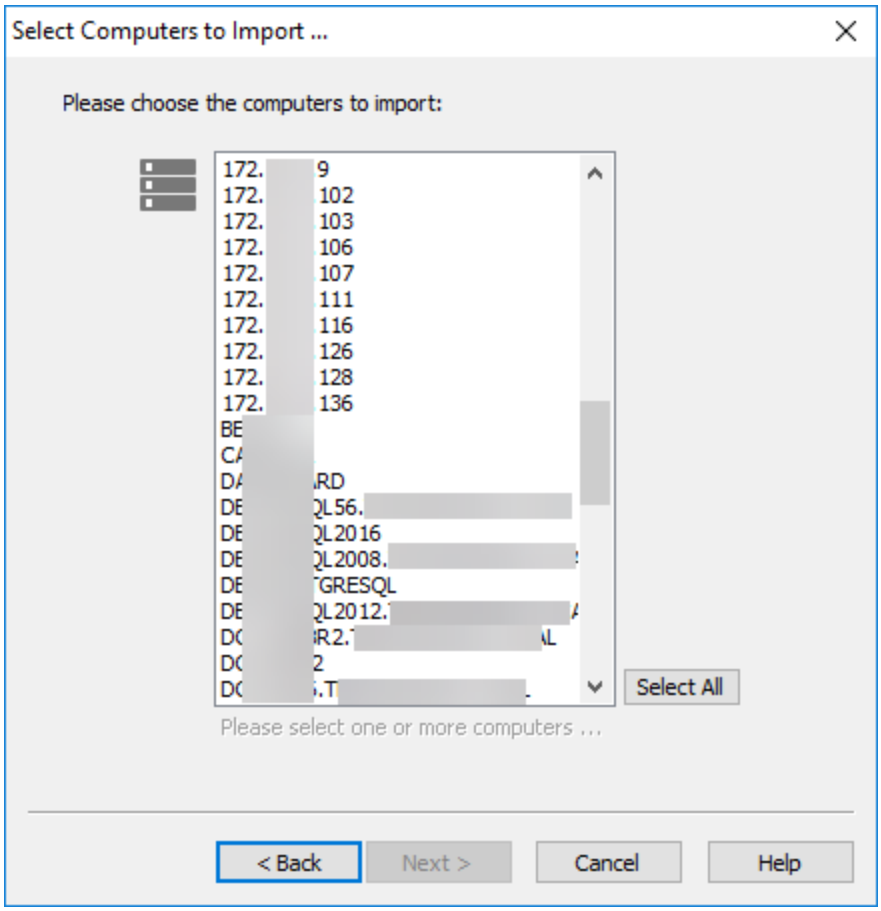
Die Auflistung eines oder mehrerer TCP-Ports verlangsamt die Geschwindigkeit des Netzwerkscans.

MAC-Anbieter
Wenn angegeben, werden nur Hosts importiert, bei denen der Hersteller der Netzwerkkarte mit dem angegebenen Zeichenfolgenmuster übereinstimmt (Wildcards werden unterstützt). Um z. B. nur DELL-Geräte zu importieren, geben Sie **dell** oder ***dell*** an. Beachten Sie, dass MAC-Adressen, die nicht ordnungsgemäß in der MAC-Herstellerdatenbank registriert sind, nicht importiert werden.

IP-Adresse auflösen

Löst entdeckte IP-Adressen in einen Hostnamen auf (empfohlen). Durch die Auswahl dieser Option wird die Scan-Geschwindigkeit leicht reduziert.

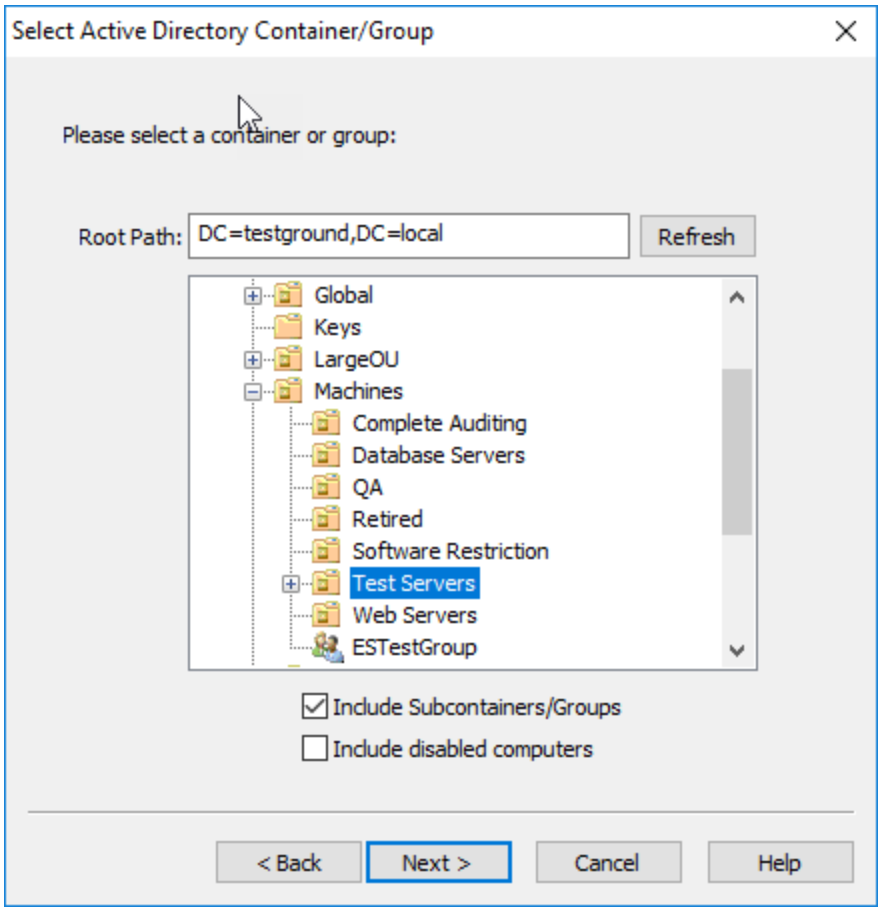
FQDN verwenden
Gibt bei der Auflösung von IP-Adressen die Hostnamen im FQDN-Format zurück.



4.5.1.4 Importieren aus Active Directory

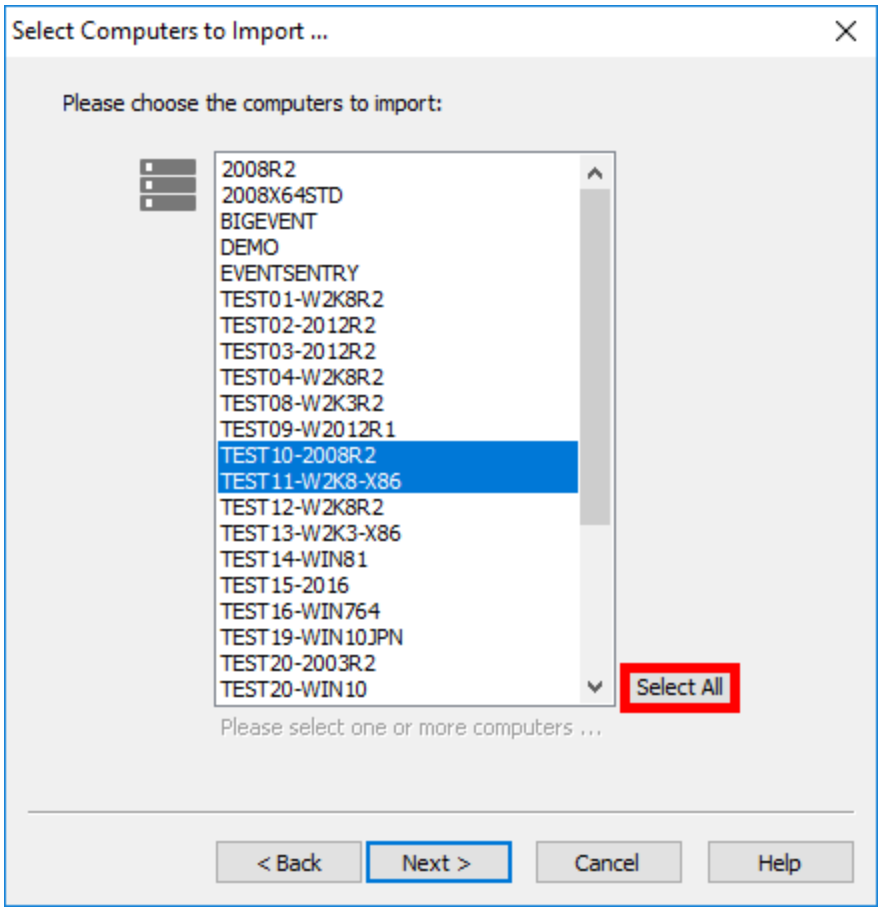
Mit der Active Directory-Funktion können Sie entweder Computer aus Active Directory importieren (durch Angabe einer OU oder Gruppe) oder die Gruppe dauerhaft mit Active Directory verknüpfen, das die Computer aus Active Directory abruft, anstatt sie in EventSentry zu speichern.

Nach der Auswahl der Importmethode von **Active Directory** wird Ihnen ein Dialog angezeigt, der ähnlich wie der unten gezeigte aussieht:

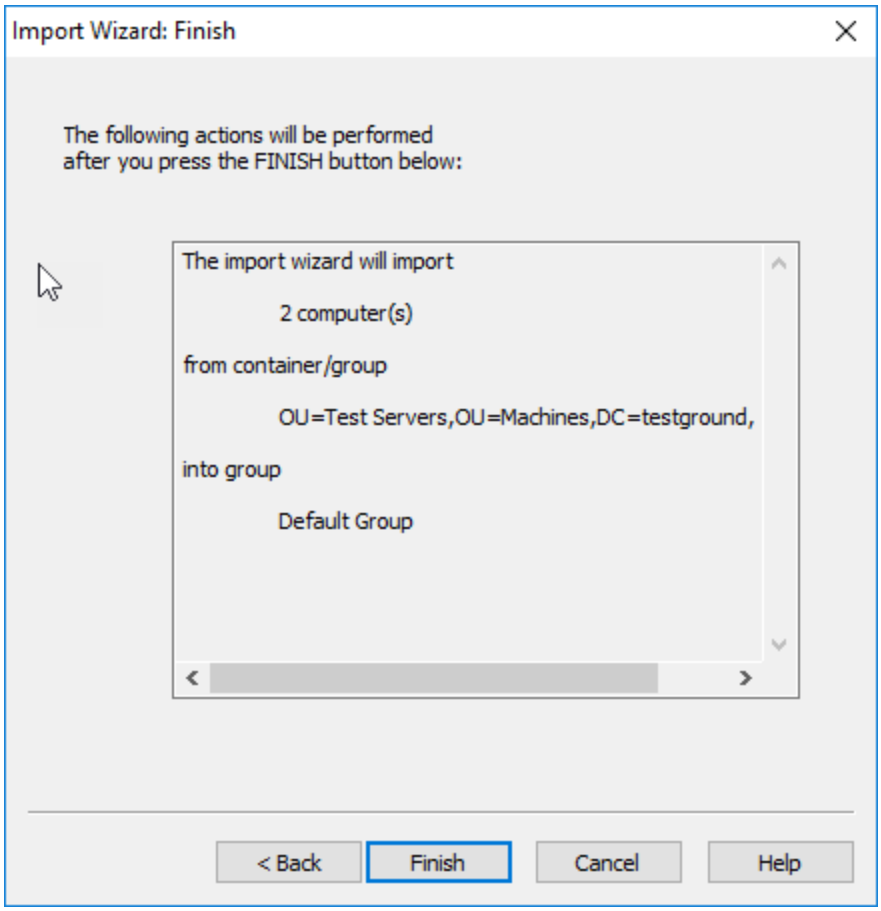


Wählen Sie den Container oder die Organisationseinheit, von der Sie Computer importieren möchten, und klicken Sie auf **Weiter**. Sie können auch das Kontrollkästchen "**Include Subcontainers/Groups**" aktivieren, um Computer aus Untercontainern einzubeziehen, oder das Kontrollkästchen "**Include disabled computers**" aktivieren, um auch deaktivierte Computer zu importieren, die standardmäßig übersprungen werden.

Nachdem Sie auf **Weiter** geklickt haben, können Sie die Computernamen, die importiert werden sollen, anzeigen und einzelne Computer auswählen oder die Auswahl aufheben:



Um alle Computer zu importieren, klicken Sie einfach auf **Alle auswählen**. Wenn Sie erneut auf **Weiter** klicken, wird ein Zusammenfassungsbildschirm angezeigt:



Klicken Sie auf **Fertig stellen**, um alle ausgewählten Computer zu importieren.

4.5.1.5 Verknüpfung mit Active Directory

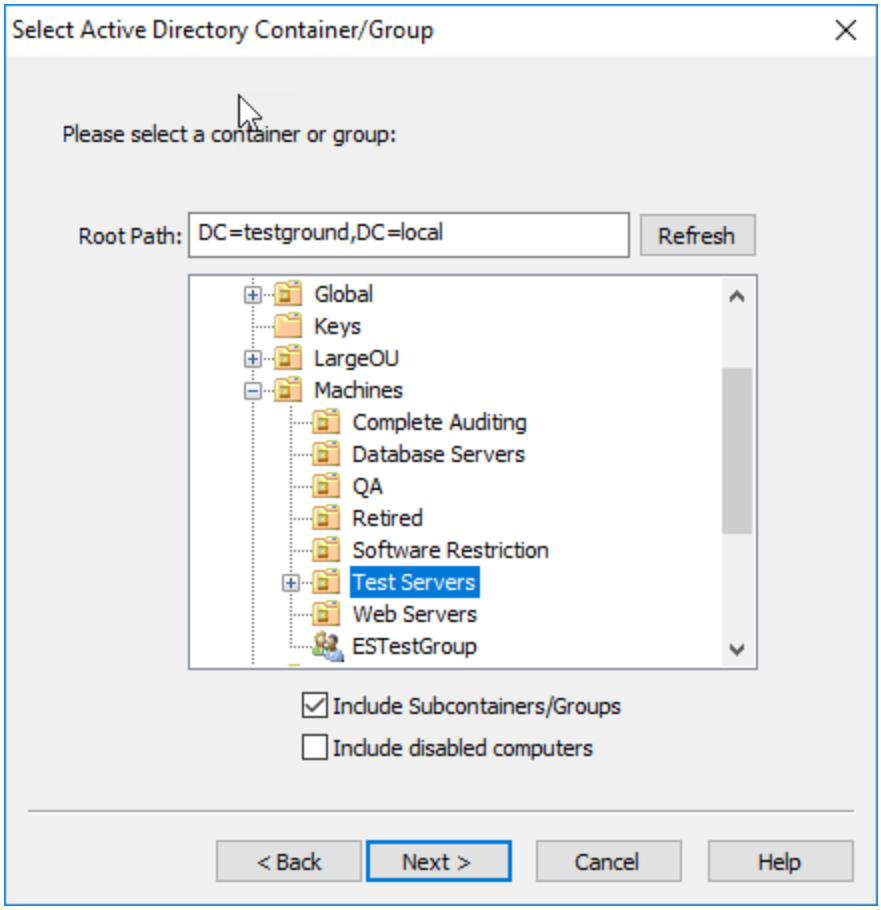
Wenn Sie über eine funktionierende Active Directory-Infrastruktur verfügen, können Sie Gruppen mit Active Directory verknüpfen, anstatt die Computer zu importieren. Auf diese Weise müssen Sie die Computer nur einmal, nämlich in Active Directory, verwalten.

Jedes Mal, wenn Sie eine Remote-Update-Aktion in einer verknüpften Gruppe durchführen, werden die Computernamen aus Active Directory und nicht aus der lokalen Konfiguration abgerufen. Sie können nur einige Gruppen mit Active Directory verknüpfen, es ist nicht erforderlich, alle Gruppen mit Active Directory zu verknüpfen.

Um eine Gruppe mit Active Directory zu verknüpfen, klicken Sie mit der rechten Maustaste auf das Element **Computer** in der gewünschten Gruppe und wählen Sie "**Mit Active Directory verknüpfen**". Sie können beim Importieren aus Active Directory auch das Kontrollkästchen "**Link Group To Active Directory**" aktivieren.

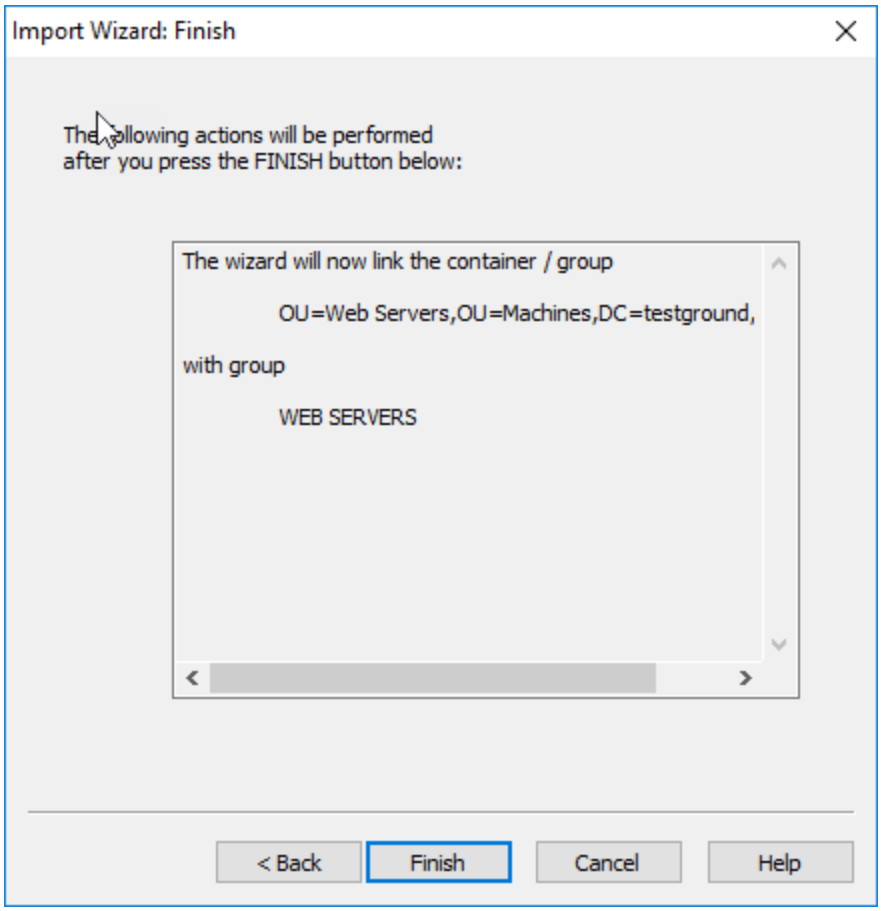
Denken Sie daran, dass EventSentry die Computer in der Gruppe nicht automatisch aktualisiert, wenn sich die Quell-OU oder -Gruppe in Active Directory ändert. Sie müssen eine Remote-Update-Aktion durchführen (z.B. Status prüfen), um eine Aktualisierung der Computerliste auszulösen.

Nachdem Sie im Assistenten auf **Weiter** geklickt haben, wird Ihnen ein Dialog ähnlich dem unten gezeigten angezeigt:



Wählen Sie im Dialog "**Select Active Directory Container/Group**" die **OU** oder **Gruppe** in Active Directory, mit der Sie eine Verknüpfung herstellen möchten. Um den Baum einer anderen Active Directory-Domäne anzuzeigen, geben Sie einfach einen Pfad in das Feld "**Root Path**" ein und klicken Sie auf die Schaltfläche "**Refresh**".

Wenn Sie fertig sind, klicken Sie auf **Weiter**, und der Bestätigungsdialog wird angezeigt:



Sobald eine Gruppe mit Active Directory verknüpft ist, sehen Sie keine Computer mehr unter dem Computer-Objekt. Alle Remote-Update-Aktionen werden auf alle Computer der Active Directory OU/Gruppe, mit der Sie verknüpft sind, angewendet.

AutoSortieren

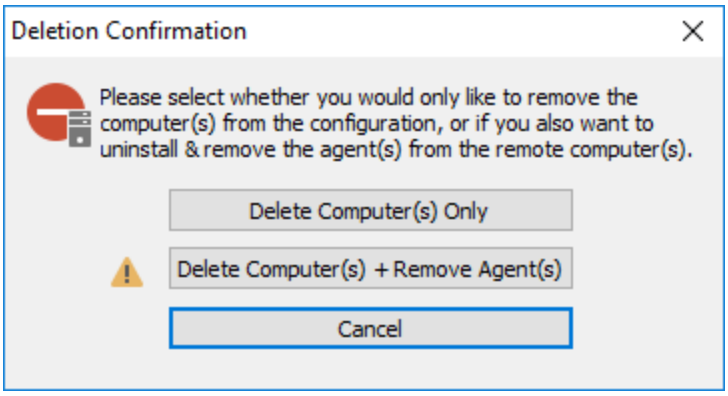
Sie können mit der rechten Maustaste auf einen Gruppencontainer klicken und **AutoSort** wählen, um die aus Active Directory abgerufenen Computer automatisch alphabetisch zu sortieren.

> ⚠ Alle vorhandenen Computer einer Gruppe werden entfernt, wenn Sie eine Gruppe mit Active Directory verknüpfen.

4.5.2 Löschen und Verschieben von Hosts

Löschen eines einzelnen Hosts

Hosts können einzeln gelöscht werden, indem Sie "Löschen" entweder aus dem Kontextmenü oder aus dem Ribbon wählen. Beim Löschen eines einzelnen Hosts gibt die Verwaltungskonsole eine Abfrage aus, ob der Agent vom entfernten Host installiert werden soll (beim Löschen von Hosts aus einer Gruppe, die Agenten enthält) oder ob der Host einfach aus der Verwaltungskonsole entfernt werden soll.



Beachten Sie, dass ein Agent auch jederzeit manuell über die Systemsteuerung von einem überwachten Host entfernt werden kann, deinstallieren Sie einfach die Anwendung "EventSentry Agent". Hosts können nicht aus Gruppen entfernt werden, die mit Active Directory verknüpft sind.

Mehrere Hosts löschen

Mehrere Hosts können über die Fernaktualisierungsfunktion gelöscht werden, wenn die Funktion "Kontrollkästchen verwenden" in den Fernaktualisierungsoptionen aktiviert ist. So löschen Sie mehrere Hosts:

1. Stellen Sie sicher, dass "Kontrollkästchen verwenden" aktiviert ist.
2. Wählen Sie eine Gruppe aus, aus der mehrere Computer gelöscht werden sollen.
3. Wählen Sie "Status prüfen" entweder aus der Multifunktionsleiste oder indem Sie mit der rechten Maustaste auf die Gruppe klicken.
4. Optional: Sortieren Sie die Computer in der Ergebnisliste.
5. Markieren Sie die Hosts, die gelöscht werden sollen. Klicken Sie mit der rechten Maustaste auf den Hauptbereich, um alle Hosts zu löschen/auszuwählen, und schalten Sie die Kontrollkästchen mit der Menüoption "Auswahl umschalten" um.
6. Klicken Sie mit der rechten Maustaste auf den Hauptbereich und wählen Sie "Deleted checked hosts", um die Hosts aus der Gruppe zu löschen.
7. Überprüfen Sie, ob die Computer korrekt entfernt wurden, und speichern Sie die Konfiguration.

Das Löschen von Hosts über diese Methode führt nicht zur Deinstallation von Remote-Agenten.

Verschieben eines einzelnen Hosts

Ein einzelner Host kann verschoben werden, indem das Computersymbol von einer Gruppe in eine andere gezogen wird.

Verschieben mehrerer Hosts

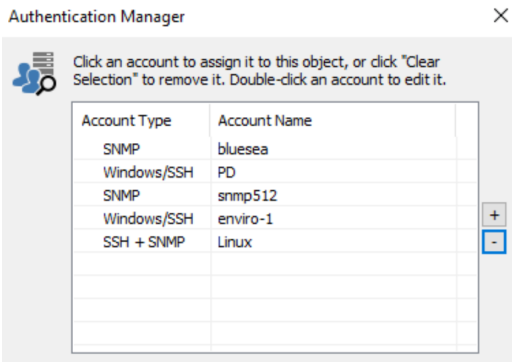
Mehrere Hosts können über die Fernaktualisierungsfunktion verschoben werden, wenn die Funktion "Kontrollkästchen verwenden" in den Fernaktualisierungsoptionen aktiviert ist. So verschieben Sie mehrere Hosts:

1. Stellen Sie sicher, dass "Use Checkboxes" aktiviert ist.
2. Wählen Sie eine Gruppe aus, aus der mehrere Computer verschoben werden sollen.
3. Wählen Sie "Status prüfen" entweder aus der Multifunktionsleiste oder indem Sie mit der rechten Maustaste auf die Gruppe klicken.
4. Optional: Sortieren Sie die Computer in der Ergebnisliste.
5. Markieren Sie die Hosts, die verschoben werden sollen. Klicken Sie mit der rechten Maustaste auf den Hauptbereich, um alle Hosts zu löschen/auszuwählen, und schalten Sie die Kontrollkästchen mit der Menüoption "Toggle Selection" um.

6. Klicken Sie mit der rechten Maustaste auf den Hauptbereich, wählen Sie "Move Checked Hosts To" und wählen Sie eine Gruppe, in die die Hosts verschoben werden sollen.
7. Überprüfen Sie, ob die Computer korrekt verschoben wurden, und speichern Sie die Konfiguration.

4.5.3 Authentifizierung

Custom Windows, SSH and SNMP credentials can be managed by the Authentication Manager and



- set globally
- applied to a group
- applied to a computer

Apply custom credentials is necessary under the following conditions:

- The currently-logged on user does not have permission to install and/or update agents on remote hosts
- The user account under which the heartbeat agent is running under does not have permission to query the EventSentry service status on remote hosts
- Remote hosts use SNMP v3 authentication or SNMP v1/v2c authentication with a community other than "public"
- Remote hosts support SSH

Credentials in the authentication manager are used by the management console when accessing remote hosts through remote update or the event viewer and by the Heartbeat Agent when polling the remote agent status or retrieving SNMP information. Since all credentials configured in the authentication manager are encrypted, **it is required that the heartbeat agent service run under the the same Windows account under which the credentials are entered in the management console.**

Important Info for Windows Credentials & Heartbeat Monitoring
Windows credentials entered will be encrypted in the registry, and can only be decrypted by the user who encrypted them. E.g., if user Bulls\DerrickR configures credentials for hosts, then the EventSentry Heartbeat Monitor service needs to also run under the Bulls\DerrickR user account.

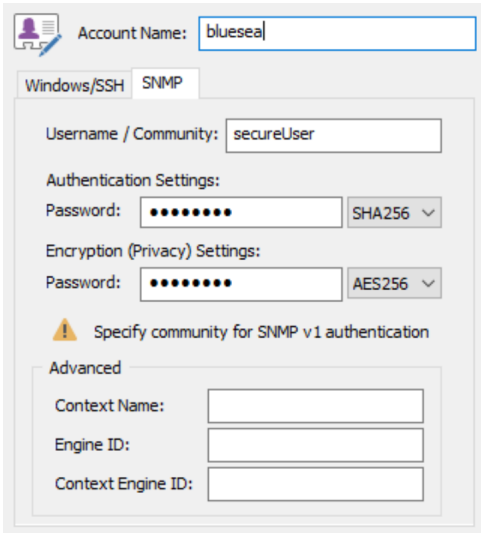
Note that the Heartbeat Agent, when utilizing the collector, does not need to utilize Windows credentials.

The authentication manager is accessible via Tools -> Options, or by selecting

- computer groups
- any group
- any host

and clicking "Set Authentication" in the ribbon or the context menu.

Adding Accounts



EventSentry supports Windows, SSH and SNMP accounts, both of which are identified by a unique "Account Name" which identifies the credentials. The "Account Name" and the actual user name can be the same, but an account name must be unique. Account names are case sensitive. An account is added by clicking the **+** icon in the authentication manager.

Windows / SSH

Specify a valid user name, including the domain when necessary (Windows only), as well as a password.

EventSentry automatically determines whether to use Windows or SSH credentials depending on the group / host type.

LAPS Support

Windows credentials can be configured to use LAPS by checking the "Use LAPS" check box. LAPS is only utilized by the management console (for agent management), the heartbeat agent does not have the ability to dynamically retrieve LAPS passwords from AD.

SNMP

For SNMP v1 and v2c only a community needs to be specified.

For SNMP v3, a user name and either Authentication, Encryption or both Authentication and Encryption can be specified.

Assigning Credentials

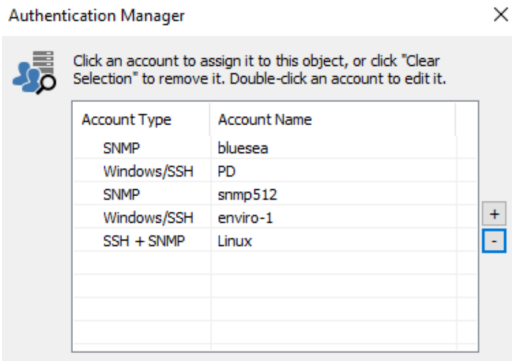
Credentials can be assigned to the selected entity by either selecting an account name from the list or by adding a new account to the authentication manager with the **+** icon. A green check mark next to an account name indicates that the account is assigned to the currently selected entity.

Removing Credentials

Credentials can be removed from a selected entity by clicking "Set Authentication" in the ribbon or the context menu and subsequently clicking "Clear Selection" in the authentication manager.

----------OLD_TEXT----------

Benutzerdefinierte Windows- und SNMP-Zugangsdaten können vom Authentication Manager verwaltet werden und



- global gesetzt
- auf eine Gruppe angewendet
- auf einen Computer angewendet

Die Anwendung benutzerdefinierter Berechtigungsnachweise ist unter den folgenden Bedingungen erforderlich:

- Der aktuell angemeldete Benutzer hat nicht die Berechtigung, Agenten auf entfernten Hosts zu installieren und/oder zu aktualisieren
- Das Benutzerkonto, unter dem der Heartbeat-Agent läuft, hat nicht die Berechtigung, den EventSentry Dienststatus auf entfernten Hosts abzufragen
- Entfernte Hosts verwenden SNMP v3-Authentifizierung oder SNMP v1/v2c-Authentifizierung mit einer anderen als der "öffentlichen" Community

Die Berechtigungsnachweise im Authentifizierungsmanager werden von der Verwaltungskonsole beim Zugriff auf entfernte Hosts über Remote-Update oder den Ereignisbetrachter und vom Heartbeat-Agenten beim Abfragen des Remote-Agentenstatus oder beim Abrufen von SNMP-Informationen verwendet. Da alle im Authentifizierungsmanager konfigurierten Anmeldedaten verschlüsselt sind, **ist es erforderlich, dass der Heartbeat-Agentendienst unter demselben Windows-Konto läuft, unter dem die Anmeldedaten in der Verwaltungskonsole eingegeben werden.**

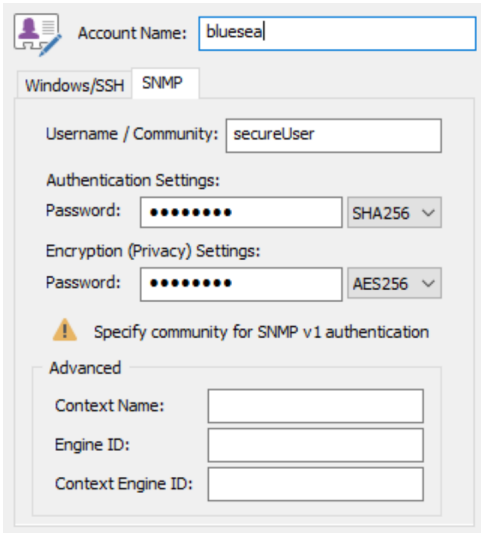
Wichtige Informationen zur Herzschlagüberwachung
Der von Ihnen eingegebene Benutzername und das Passwort werden in der Registrierung verschlüsselt und können nur von dem Benutzer entschlüsselt werden, der sie verschlüsselt hat. Wenn z.B. der Benutzer Bulls\DerrickR Zugangsdaten für Hosts konfiguriert, dann muss der EventSentry Heartbeat Monitor-Dienst auch unter dem Bulls\DerrickR-Benutzerkonto laufen.

Der Authentifizierungsmanager ist zugänglich über Tools -> Options oder durch Auswahl von

- Computergruppen
- irgendeine Gruppe
- jeder Host

und klicken Sie auf "Set Authentication" im Ribbon oder Kontextmenü.

Hinzufügen von Konten



EventSentry unterstützt Windows- und SNMP-Konten, die beide durch einen eindeutigen "Kontonamen" identifiziert werden, der die Anmeldedaten beschreibt. Der "Kontoname" und der tatsächliche Benutzername können identisch sein, aber ein Kontoname muss eindeutig sein. Bei Kontonamen wird zwischen Groß- und Kleinschreibung unterschieden. Ein Konto wird durch Klicken auf das +-Symbol im Authentifizierungsmanager hinzugefügt.

Fenster
Geben Sie einen gültigen Benutzernamen, gegebenenfalls einschließlich der Domäne, sowie ein Passwort an.

SNMP
Für SNMP v1 und v2c muss nur eine Community angegeben werden.

Für SNMP v3 können ein Benutzername und entweder Authentifizierung, Verschlüsselung oder sowohl Authentifizierung als auch Verschlüsselung angegeben werden.

Berechtigungsnachweise zuweisen

Berechtigungsnachweise können der ausgewählten Entität entweder durch Auswahl eines Kontonamens aus der Liste oder durch Hinzufügen eines neuen Kontos zum Authentifizierungsmanager mit dem Symbol **+** zugewiesen werden. Ein grünes Häkchen neben einem Kontonamen zeigt an, dass das Konto der aktuell ausgewählten Entität zugeordnet ist.

Entfernen von Berechtigungsnachweisen

Berechtigungsnachweise können von einer ausgewählten Entität entfernt werden, indem Sie auf "Set Authentication" in der Multifunktionsleiste oder im Kontextmenü und anschließend auf "Clear Selection" im Authentifizierungsmanager klicken.

4.5.4 Computer exportieren

Je nachdem, ob Sie mit der rechten Maustaste auf eine **Gruppe** oder den Knoten **Remote Update** geklickt haben, werden beim Exportieren entweder alle Computer aus der ausgewählten Gruppe oder aus allen Gruppen in die angegebene Textdatei geschrieben.

Entfernen von Computern aus der Liste

Sie können einzelne Computer, alle Computer aus einer Gruppe oder alle Computer aus allen Gruppen entfernen:

Einzelner Computer
Klicken Sie mit der rechten Maustaste auf einen Computer und klicken Sie auf **Löschen** oder wählen Sie ein Computerobjekt aus und drücken Sie die Entf-Taste auf der Tastatur.

Alle Computer aus der Gruppe
Klicken Sie mit der rechten Maustaste auf eine Gruppe und wählen Sie **Alle löschen.**

Alle Computer aus allen Gruppen:

Klicken Sie mit der rechten Maustaste auf den Knoten **Remote Update** und wählen Sie **Alle löschen.**

Dateiformat

Die für Importe und Exporte verwendete Textdatei sollte auf das folgende Format konfiguriert werden:

```
[Gruppenname1]
computer1
computer2
computer3
[Gruppenname2]
computer10
computer11
[Gruppenname3]
computer700
computer701
```

Namen in Klammern beschreiben den Beginn einer neuen Gruppe, während Namen allein Computernamen angeben. Um ein Beispiel für eine solche Textdatei zu sehen, fügen Sie einfach ein paar Computer zur Computerliste hinzu und exportieren Sie sie in eine Textdatei. Diese Datei können Sie dann als Vorlage für zukünftige Importe verwenden.

4.5.5 Variablen

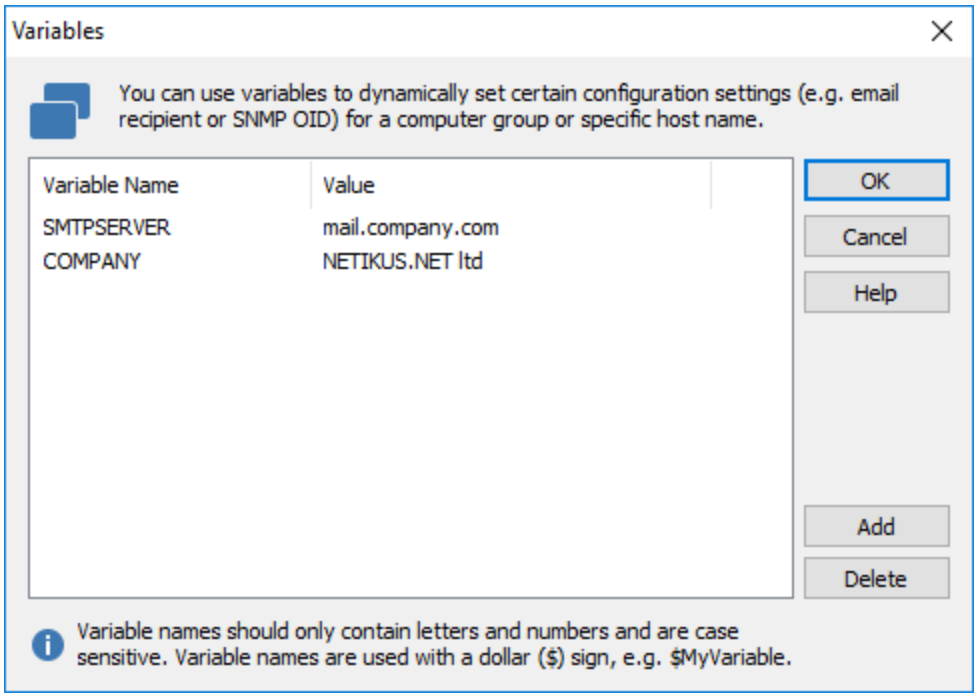
Variablen erlauben es Ihnen, flexiblere Konfigurationen zu erstellen, wenn Objekte wie z.B. Aktionen die meisten, aber nicht alle Konfigurationswerte gemeinsam haben.

EventSentry unterstützt Laufzeit- und benutzerdefinierte Variablen. **Laufzeitvariablen** werden während der Laufzeit festgelegt (z.B. $HOSTNAME, $LOG, usw.), während **benutzerdefinierte Variablen** von Ihnen definiert werden.

Variablennamen unterscheiden Groß- und Kleinschreibung und beginnen immer mit dem Dollarzeichen **$**.

Benutzerdefinierte Variablen definieren

Sie definieren benutzerdefinierte Variablen global, indem Sie mit der rechten Maustaste auf das Objekt "**Gruppen**" klicken und "**Variablen definieren**" wählen. Dann wird Ihnen das Dialogfeld *"Variablen"* angezeigt:



Variablen sollten mit einem Standardwert initialisiert werden, der dann gruppenweise überschrieben werden kann. Benutzerdefinierte Variablen können in bestimmten Filter- und Aktionsfeldern verwendet werden, siehe "Benutzerdefinierte Variablen" für weitere Informationen.

Um den Standardwert einer bereits definierten Variable zu ändern, doppelklicken Sie darauf. Um bereits definierte Variablen zu entfernen, wählen Sie die Variable aus und klicken Sie auf "Löschen".

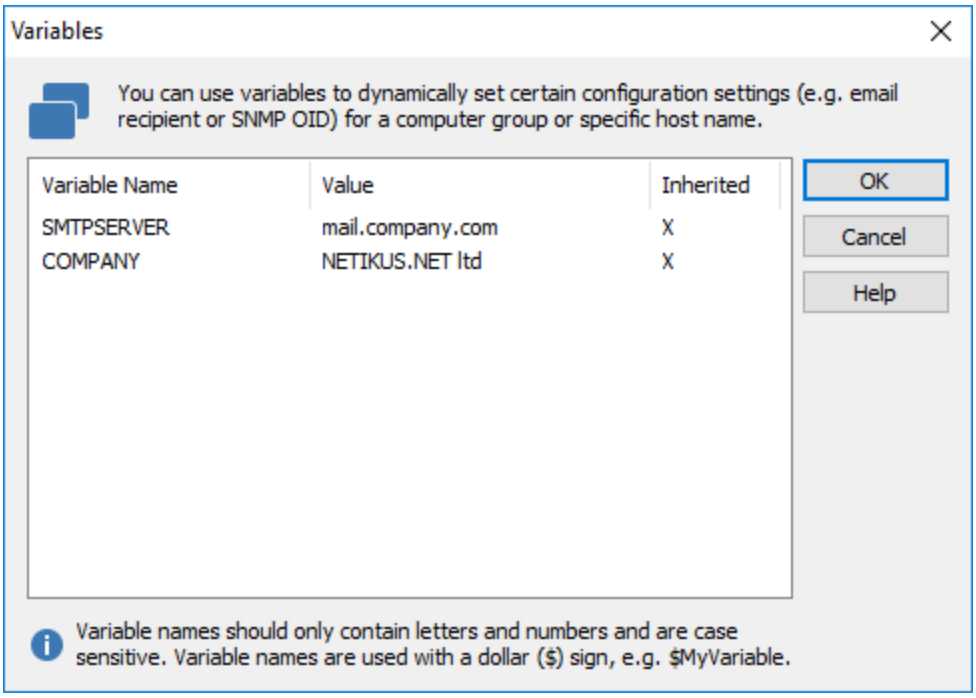
Variablennamen werden referenziert, indem das Dollarzeichen ($) vorangestellt wird, wie es in einigen Programmiersprachen verwendet wird. Um zum Beispiel die oben gezeigte Variable SMTPSERVER im Feld SMTP-Server einer SMTP-Aktion zu verwenden, muss $SMTPSERVER geschrieben werden.

> Benutzerdefinierte Variablen können einen beliebigen Namen haben, dürfen aber nur Buchstaben enthalten. Zahlen und Sonderzeichen werden im Namen einer benutzerdefinierten Variable nicht unterstützt.

Vorgabewerte überschreiben

Sie können die Standardwerte der Variablen auf einer **Pro-Gruppe oder auf einer** Pro-Computer-Basis außer Kraft setzen. Im obigen Beispiel können Sie leicht verschiedene SMTP-Server für verschiedene Gruppen angeben, ohne dass Sie mehrere SMTP-Aktionen erstellen müssen.

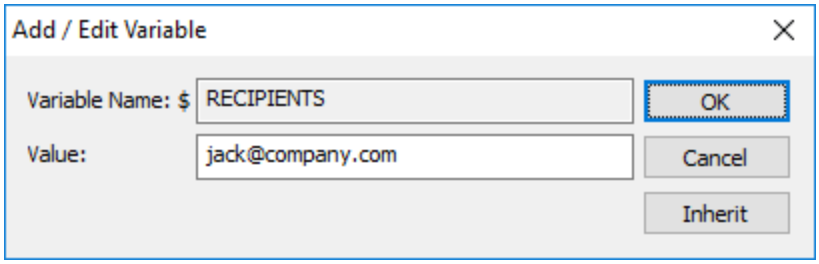
Um Variablen zu überschreiben, klicken Sie mit der rechten Maustaste auf die Gruppe oder den Computer, für den Sie die Variable überschreiben möchten, und wählen Sie "Variable(n) setzen". Sie werden ein ähnliches, wenn auch etwas anderes Dialogfeld angezeigt bekommen:



Wie Sie sehen können, sind die Schaltflächen "Hinzufügen" und "Löschen" nicht mehr vorhanden, da Sie Variablen nur definieren können, wenn Sie mit der rechten Maustaste auf das Objekt "Gruppen" klicken. In einer bestimmten Gruppe können Sie nur die Werte ändern (=übersteuern).

Im obigen Bildschirmfoto wurde der Standardwert für die SMTPSERVER-Variable in mail2.netikus.net geändert. Die Variable COMPANY wurde jedoch nicht geändert, was durch das X in der Spalte Vererbt angezeigt wird.

Um eine Variable außer Kraft zu setzen, doppelklicken Sie auf den Namen und geben Sie einen neuen Variablenwert ein. Zuvor angepasste Variablen können auf ihren Standardwert zurückgesetzt werden, indem Sie einfach auf die Schaltfläche "Vererben" klicken oder das Feld "Wert" löschen.



4.5.5.1 Unterstützte Variablen und Felder

Laufzeit-Variablen

Laufzeitvariablen sind Variablen, die sich während der Laufzeit ändern können oder die von dem verarbeiteten Ereignisprotokoll abhängen. Diese Variablen werden in den folgenden Feldern unterstützt:

Bei E-Mail-Aktionen spiegeln Ereignisvariablen (z.B. $EVENTID) immer den Wert des ersten in der E-Mail enthaltenen Ereignisses wider (da E-Mails mehrere Datensätze enthalten können).

	Email				File	Syslog	SNMP Trap	Desktop (Growl)	Process Action	Event Log Backup	Service / Process	HTTP
	Sender Name Sender Email	Subject	Header & Footer	Email Msg Override	File Name	Prefix	Custom Data	Title Message	Command Line Arguments	File Name	Service Name Process Name	All Form Fields
$HOSTNAME $HOSTNAMEFQDN $HOSTNAMEALIAS	X	X	X	X	X					X		X
$EVENT... VARIABLES (1)		X	X	X	X	X	X	X	X			X
$STR1 .. $STR28 $STRelementName	X	X	X	X				X	X		X	X
DATE / TIME VARIABLES (2)					X				X	X		
$LOG										X		
$COUNT		X										
$IPADDRESS		X	X	X			X		X			X
$LICENSEE		X	X									

Bei E-Mail-Aktionen kann die Variable $LOG im Betreff auf "Various" aufgelöst werden, wenn die E-Mail Ereignisse aus mehreren Ereignisprotokollen enthält.

Event Variables (1)
$GROUP
$FILTER
$PACKAGE
$NOTES
$EVENTLOG
$EVENTTYPE
$EVENTSOURCE
$EVENTCATEGORY
$EVENTID
$EVENTUSER
$EVENTDATETIME
$EVENTDATETIMEISO8601
$EVENTNUMBER
$EVENTCOMPUTER
$EVENTMESSAGE

Date / Time Variables (2)

$DAY
$MONTH
$YEAR
$HOUR
$MINUTE

$IPADRESSE: Wird entweder zu der IP-Adresse aufgelöst, die einem Host-Eintrag in einer Gruppe zugeordnet ist, oder - falls dort nicht festgelegt - zu der IP-Adresse der Schnittstelle mit der schnellsten Netzwerkverbindung auf dem System.

Einfügetext-Variablen

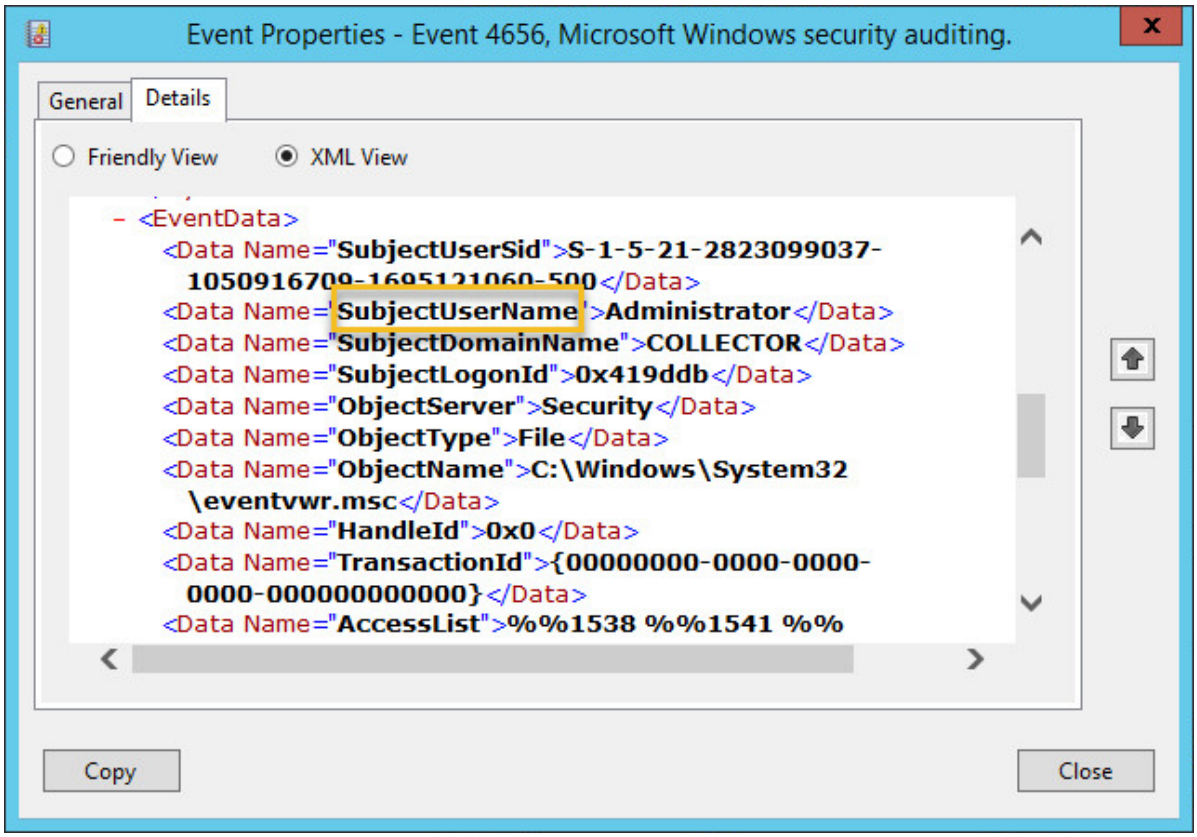
Die meisten Windows-Ereignisse basieren auf Vorlagen und enthalten dynamische Werte, die gewöhnlich "Einfügetext", "Insertion Strings" oder "Ereignis-Metadaten" genannt werden. Diese Einfügetexte werden als Variablen in EventSentry und kann bei den meisten Aktionen verwendet werden.

Einfügetexte-Variablen beginnen immer mit **$STR** und werden sowohl in numerischer (z.B. **$STR2**) als auch in textueller Form (z.B. **$STRIpAddress**) unterstützt. Die Sequenznummer eines Einfügetexts kann mit dem Event Message Browser identifiziert werden, wobei Einfügetexte mit Prozentzeichen gefolgt von einer Zahl, z.B. %1, %2 usw., gekennzeichnet werden.

Einfügetexte werden mit der Variablen **$STRx** angegeben, wobei **x** durch die Nummer aus dem Einfügetext ersetzt wird. Um z.B. den 3. Einfügetext eines Ereignisses in einem E-Mail-Betreff anzuzeigen, könnte **$STR3** in den E-Mail-Betreff der Aktion aufgenommen werden. Die obige Tabelle listet auf, welche Felder Variablen für Einfügetexte unterstützen.

Einfügetexte in ihrer Textform werden ebenfalls durch die Variable **$STRx** angegeben, wobei **x** durch den Namen des Metadatenelements ersetzt wird. Beispielsweise würde $STRSubjectUserName auf den Inhalt des Feldes **SubjectUserName** aufgelöst. Datenelementnamen finden Sie in der Windows-Ereignisanzeige entweder im Register "Freundliche Ansicht" oder im Register "XML-Ansicht" der Ereignisdetails.

Bei Variablennamen wird zwischen Groß- und Kleinschreibung unterschieden - nur **$STRSubjectUserName** würde im Beispiel unten zum **Administrator** aufgelöst, $STRSUBJECTUSERNAME nicht!



Benutzerdefinierte Variablen

Benutzerdefinierte Variablen können einen beliebigen Namen haben, dürfen aber nur Buchstaben enthalten. Zahlen und Sonderzeichen werden im Namen einer benutzerdefinierten Variable nicht unterstützt. Benutzerdefinierte Variablen werden in den folgenden Feldern unterstützt:

Backup Event Logs

Backup File ("File")

Log File Monitoring

File Path

Filters

Source
Category
Username
Computer
Advanced: Email Subject Override
Advanced: Email Content Override

SMTP Notification

Sender Name
Sender Email
Recipients
Subject
Primary (incl. User & Pass)
Secondary (incl. User & Pass)

Dial
Header & Footer
Character Set

HTTP

Form fields
HTTP Content Type (PUT/POST)
HTTP Content Data (PUT/POST)

Database Notification

DSN Name
Table Name
Username
Password

Syslog

Host Name
Custom data

SNMP + SNPP Notification

Host Name

File

File Name
Character Set

Network Message

NetBIOS Name

Process

Process Name
Arguments

XMPP

Chat room

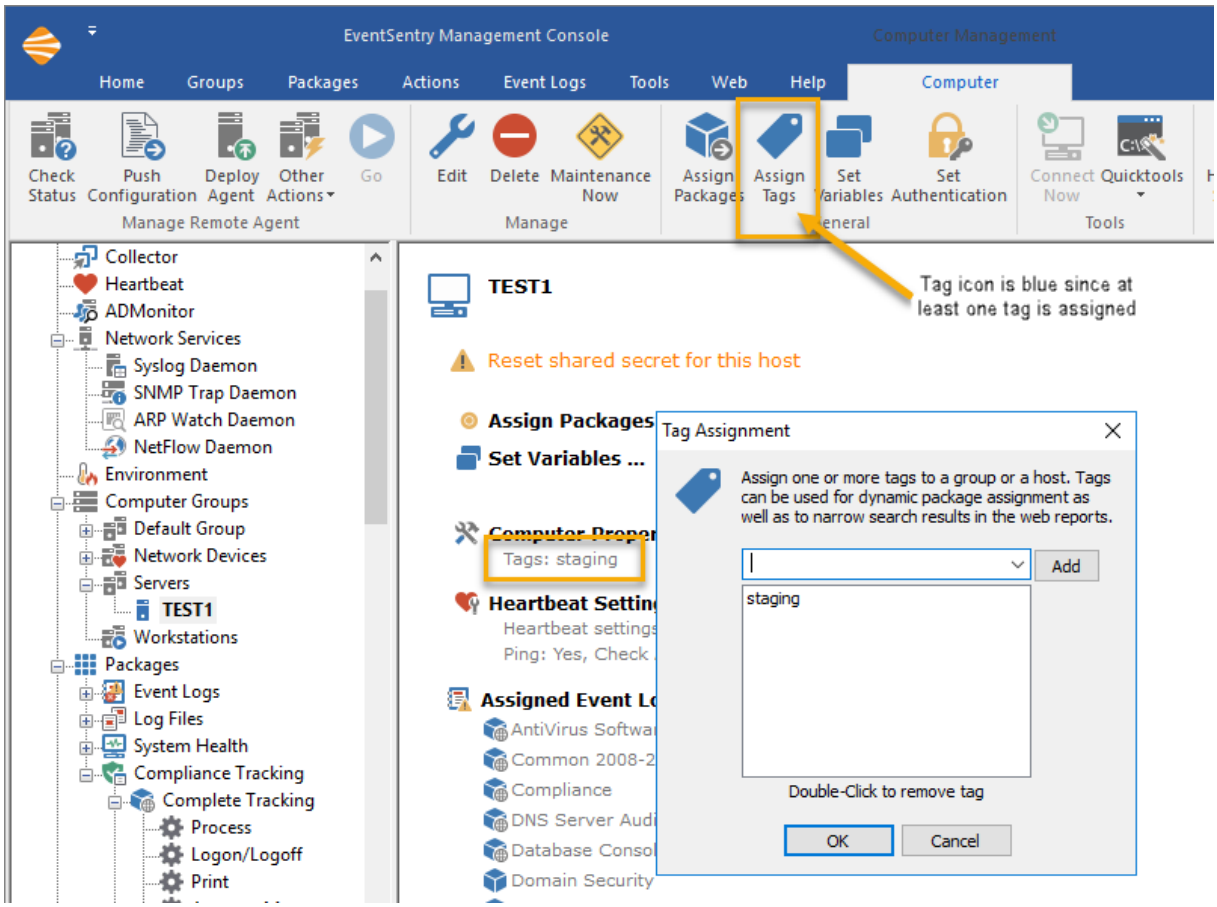
4.5.6 Tags

Tags können sowohl den Gruppen als auch den Hosts zugewiesen werden und können zur Vereinfachung der Paketzuweisung sowie für webbasierte Berichte verwendet werden. Tags sind besonders nützlich für größere Installationen, bei denen die Organisation von Hosts nur nach Gruppen unzureichend sein kann.

Betrachten Sie das folgende Szenario: Ihre Umgebung besteht sowohl aus Produktions- als auch aus Entwicklungs-Hosts, die alle Mitglieder verschiedener Gruppen sind (z.B. Webserver, Datenbankserver, ...).

Sie können keine Produktions- und Entwicklungsgruppe anlegen, da die Hosts bereits Mitglieder anderer Gruppen sind. Sie möchten den Produktionsrechnern verschiedene Pakete zuweisen und auch Berichte ausführen, die nur Ergebnisse für Produktions- oder Entwicklungsrechner liefern.

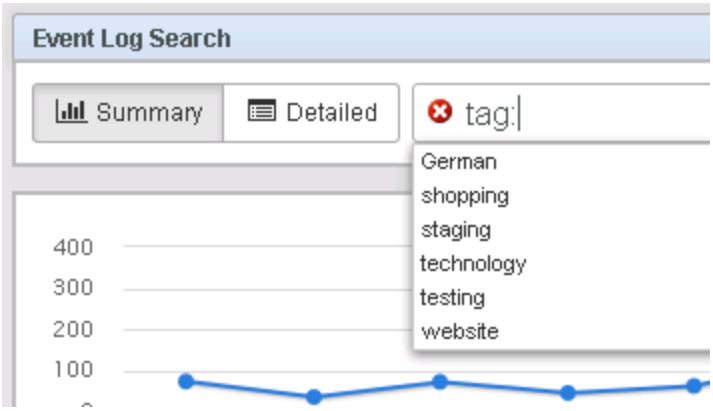
Durch die Markierung von Hosts mit ihren jeweiligen Tags kann die Funktion zur automatischen Zuweisung von Paketen für die dynamische Zuweisung von Paketen verwendet werden, während das Schlüsselwort "Tag" in den Web Reports nur Ergebnisse von Hosts liefern kann, die mit dem jeweiligen Tag markiert sind.



Hosts und Gruppen können durch Auswahl der Option "Tags zuweisen" aus dem Kontextmenü oder dem Ribbon mit einem Tag versehen werden. Das Tag-Symbol in der Multifunktionsleiste ist kontextsensitiv und wird blau angezeigt, wenn der aktuell ausgewählten Gruppe oder dem Host ein oder mehrere Tags zugewiesen sind, und wird ansonsten grau angezeigt.

Auf Gruppenebene gesetzte Tags werden automatisch an alle Hosts vererbt, die Mitglied dieser Gruppe sind; es ist nicht möglich, die Vererbung von Tags zu blockieren. Mehrere Tags können sowohl Gruppen als auch Hosts zugewiesen werden.

Sobald ein Gastgeber oder eine Gruppe mit einem Tag versehen ist, kann die Funktion zur automatischen Zuweisung eines Pakets oder zum Filtern jeder suchbasierten Web Reports-Seite mit dem **Tag:** Schlüsselwort verwendet werden.



Bearbeiten von Tags für mehrere Hosts
Tags können über das Kontextmenü der Funktion "Fernaktualisierung / Remote update" auf mehreren Hosts bearbeitet werden. Gehen Sie wie folgt vor, um ein Tag auf mehreren Hosts zu bearbeiten;

1. Wählen Sie "Computergruppen" oder eine bestimmte Gruppe
2. Wählen Sie "Status prüfen" aus dem Ribbon oder dem Kontextmenü
3. Aktivieren/deaktivieren Sie die Hosts, auf denen Sie Tags im rechten Fensterbereich bearbeiten möchten
4. Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle und wählen Sie "Tags bearbeiten".
5. Fügen Sie Tags hinzu oder entfernen Sie sie und klicken Sie auf "OK".

Hinweis: Wenn Sie Tags auf Hosts bearbeiten, denen bereits andere Tags zugewiesen sind, werden die angegebenen Tags zu den vorhandenen Tags der einzelnen markierten Hosts hinzugefügt. Vorhandene Tags sind davon nicht betroffen.

4.6 Agenten verwalten

Remote Update hilft Ihnen bei der Bereitstellung und Verwaltung des EventSentry-Agenten auf entfernten Hosts sowie bei der Überprüfung der Konnektivität mit Netzwerkgeräten. Die Agentenkonfiguration sowie die Agenten-Patches können ebenfalls durch den Collector verwaltet werden.

Remote Update hat die folgenden Fähigkeiten, die in drei Kategorien unterteilt sind:

Status prüfen
- Führt einen Verbindungstest basierend auf den Heartbeat-Einstellungen der Gruppe (oder des Hosts) durch, prüft auch den Agentenstatus bei der Verarbeitung von Windows-Hosts.

Agentenstatus prüfen
- Ruft den aktuellen Agentenstatus und die installierte Version von einer Reihe von Hosts ab, damit Sie sicherstellen können, dass der EventSentry-Agent ausgeführt wird und über die neueste Version verfügt. Fügt der Liste nur dann vollständige Hosts hinzu, wenn er aus dem Kontext "Computergruppen" ausgewählt wird.

Konfiguration aktualisieren

- Schickt die aktuelle Konfiguration an den/die entfernten Host(s)

Aktion ausführen

- Installieren Sie den Dienst (einschließlich der erforderlichen Dateien)
- Aktualisieren der auf entfernten Computern ausführbaren Dienstdatei
- Deinstallieren Sie den Dienst (einschließlich Dateien und Konfiguration)
- Starten Sie den Dienst auf entfernten Computern
- Beenden des Dienstes auf entfernten Computern

Anforderungen

Die Aufgaben der Fernaktualisierung haben unterschiedliche Anforderungen, je nachdem, welche Aktion durchgeführt wird. Die folgende Tabelle zeigt Ihnen, welche Tasks welche Anforderungen haben.

Anforderungen für Remote-Update

	- erforderlicher Zugriff/Funktionen auf Remote-Host -			
Remote Update Aufgabe	**Registrierung**	**ADMIN$**	**ES$**	**Service Control Manager**
Dienst installieren	optional, um die Option zum automatischen Neustart des Dienstes einzustellen	ja, um Servicedatei und Anfangskonfiguration zu kopieren	nein	ja, um den Dienst zu installieren
Dienst deinstallieren	ja, um die Konfiguration zu entfernen	ja, um Dienstakte zu entfernen	nein	ja, um den Dienst zu deinstallieren
Konfiguration aktualisieren	nein	ja, wenn ES$ nicht vorhanden	ja (erfordert **RemoteUpdate** Verzeichnis)	nein
Konfiguration aktualisieren (mit "Verkehr minimieren" aktiviert)	nein	optional, zur Abfrage der Version eines entfernten Agenten	ja (erfordert **RemoteUpdate** Verzeichnis	nein
Agentenstatus prüfen	nein	ja, zur Abfrage der Version eines entfernten Agenten	nein	ja, zur Abfrage der aktuellen Dienststatus
Update-Agent	nein	ja, um die Servicedatei zu aktualisieren	nein	ja, zu stoppen und Dienst starten
Dienst starten	nein	nein	nein	ja
Dienst anhalten	nein	nein	nein	ja

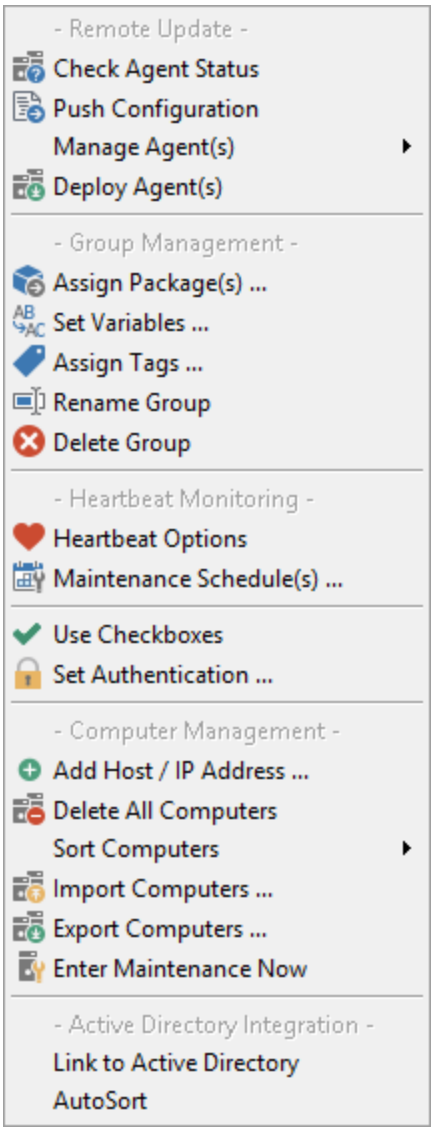
Um beispielsweise die Konfiguration auf einem Remote-Host zu aktualisieren, muss auf dem Remote-Host entweder die ADMIN$-Freigabe oder die ES$-Freigabe vorhanden sein. Für die Remote-Installation des Dienstes ist die ADMIN$-Freigabe obligatorisch, und der Zugriff auf den remote SCM (Service Control Manager) ist ebenfalls erforderlich.

So führen Sie ein Remote-Update durch:

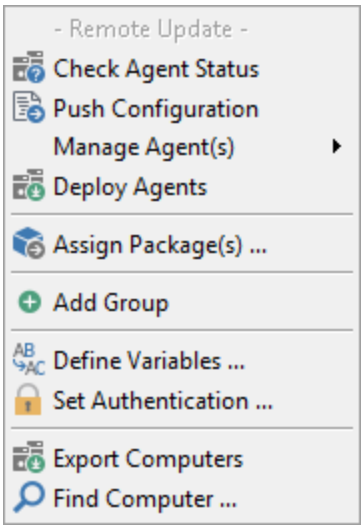
1. Fügen Sie alle Computer, die Sie aktualisieren möchten, zu einer Gruppe hinzu. Um Computer aus einer Textdatei, der Netzwerkumgebung, einem IP-Scan oder Active Directory hinzuzufügen, klicken Sie mit der rechten Maustaste auf eine **Gruppe** und wählen Sie **Importieren**. Auf der nächsten Seite finden Sie weitere Informationen zum Importieren von Computern. Sie können den lokalen Computernamen nicht in diese Liste aufnehmen, da davon ausgegangen wird, dass er bereits aktuell ist und als Vorlage dient.

2. Klicken Sie mit der rechten Maustaste auf eine Gruppe oder klicken Sie mit der rechten Maustaste auf **Gruppen**. Erstere aktualisiert nur Computer in der ausgewählten Gruppe, während letztere alle Computer aus allen Gruppen aktualisiert.

3. Wählen Sie die gewünschte Kategorie aus dem Kontextmenü



Kontextmenü für eine Gruppe



Kontextmenü für alle Gruppen

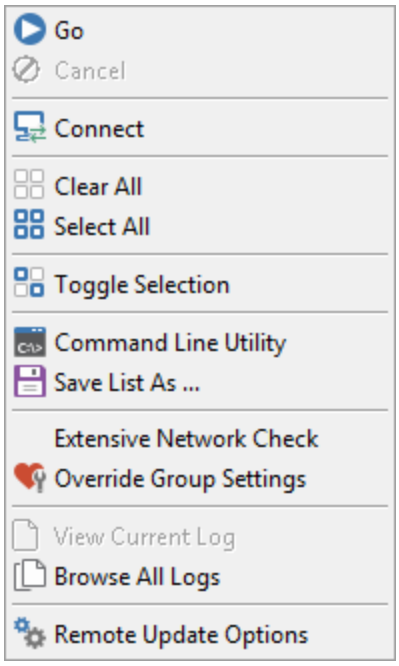
5. Klicken Sie auf eine Kategorie für weitere Details:

   - Abrufen des Dienststatus ("Status abrufen")
   - Durchführen von Updates ("Update Configuration")
   - Agenten verwalten ("Managing Agent(s)")

6. Wenn Sie **Kontrollkästchen verwenden** ausgewählt haben, müssen Sie nun die Computer überprüfen, auf die das Update angewendet werden soll. Klicken Sie dann mit der rechten Maustaste auf die Liste und wählen Sie **Go** aus dem Kontextmenü oder klicken Sie auf den grünen Pfeil in der Symbolleiste.

Speichern der Ergebnisse

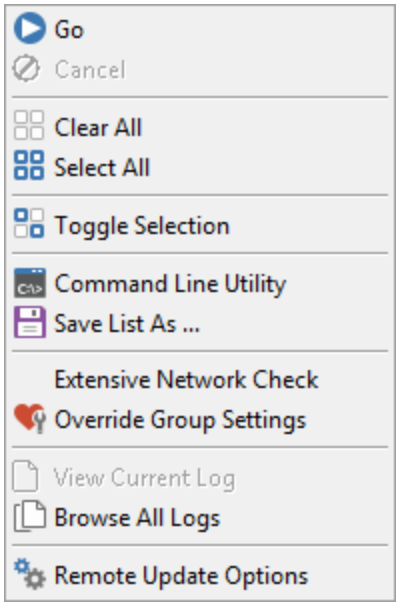
Sie können jederzeit die Ergebnisse eines Remote-Update-Status / Update / Aktion speichern, indem Sie mit der rechten Maustaste auf die Liste klicken und **Liste speichern unter** wählen.



Dadurch wird die aktuelle Ausgabe in einer Textdatei gespeichert.

Wiederholen einer Aktualisierung

Wenn Sie irgendeinen Status / Update / Aktion wiederholen möchten, dann klicken Sie mit der rechten Maustaste auf die Liste und wählen Sie **Repeat Update**. Die letzte von Ihnen durchgeführte Aktion wird wiederholt.



Hinweis: Wenn Sie die Funktion **Use Checkboxes** aktiviert haben, müssen Sie auf **Go** klicken anstatt auf **Repeat Update**.

4.6.1 Optionen

Sie können die Fernaktualisierungsfunktion anpassen und verschiedene Optionen konfigurieren, indem Sie zu **Extras -> Optionen -> Fernaktualisierung** navigieren. Beispielsweise können Sie den Remote-Update-Prozess für WAN-Netzwerke optimieren, Hosts pingen, bevor ein Remote-Update durchgeführt wird, und vieles mehr.

Weitere Informationen finden Sie unter Verwaltungskonsole -> Customizing -> Fernaktualisierung.

4.6.2 Authentifizierung

Standardmäßig verbindet sich EventSentry bei Verwendung des Remote-Updates mit Remote-Computern mit dem Benutzernamen, unter dem Sie gerade angemeldet sind. Dies kann sich als schwierig erweisen, wenn Sie verschiedene Domänen und/oder Server verwalten müssen, bei denen Sie sich als ein anderer Benutzer authentifizieren müssen.

Wenn Sie möchten, dass EventSentry bei der Verbindung mit Remote-Rechnern andere Anmeldeinformationen verwendet, können Sie eine der folgenden Möglichkeiten nutzen:

- Alternatives Benutzerkonto global angeben
- Benutzerkonto pro Gruppe angeben
- Benutzerkonto pro Rechner angeben

Anmeldeinformationen, die auf Rechnerebene festgelegt werden, haben Vorrang vor Anmeldeinformationen, die auf gruppenbezogener oder globaler Ebene festgelegt werden, Anmeldeinformationen, die auf Gruppenebene festgelegt werden, haben Vorrang vor globalen Anmeldeinformationen.

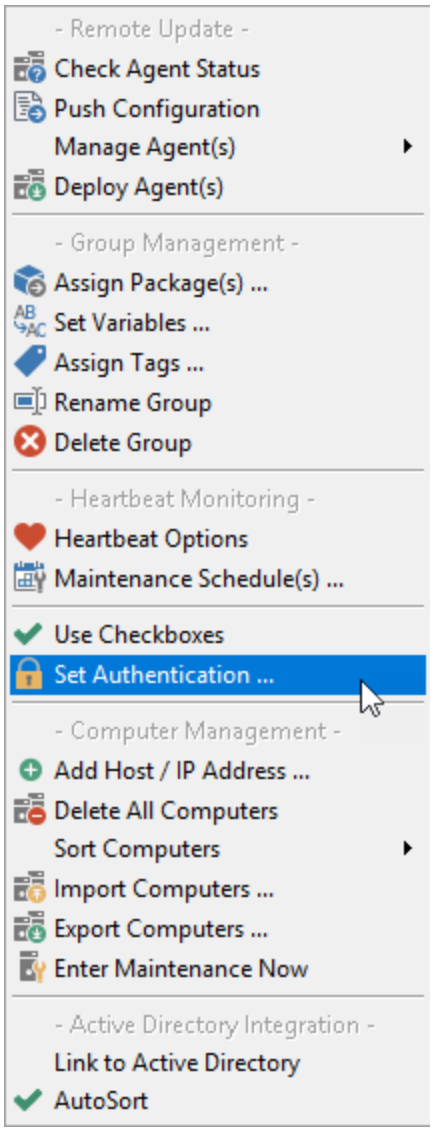
Wenn Sie beabsichtigen, den Status des EventSentry-Agenten auf Computern in einer Gruppe zu überwachen, in der Sie die Authentifizierung mit Hilfe des Heartbeat-Agenten einstellen, dann lesen Sie bitte diesen Hinweis.

Festlegen globaler Anmeldeinformationen

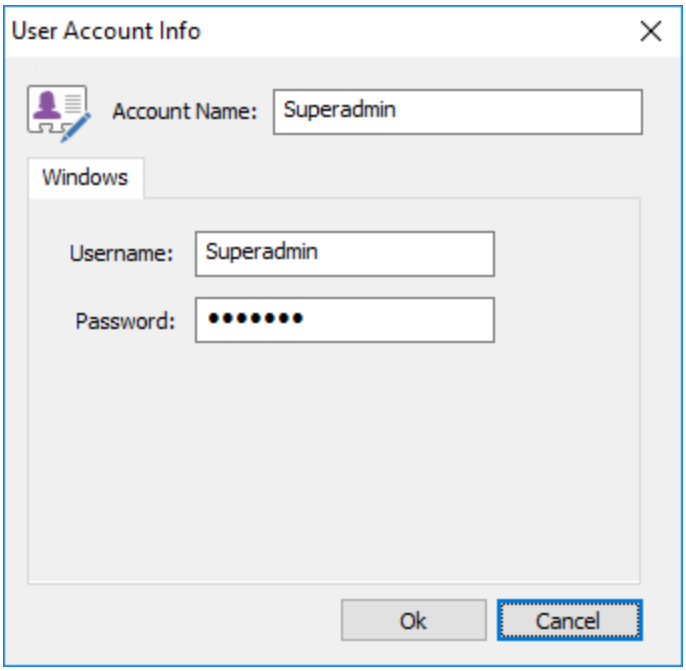
Unterschiedliche Berechtigungsnachweise können auf globaler Ebene festgelegt werden, um alle konfigurierten Computer zu beeinflussen. Um globale Anmeldeinformationen festzulegen, klicken Sie mit der rechten Maustaste auf den Container **Computer Groups** und wählen Sie **Set Authentication**. Globale Berechtigungsnachweise wirken sich auf alle Computer aus, es sei denn, andere Anmeldeinformationen werden auf einer gruppen- oder hostbezogenen Ebene festgelegt.

Angeben unterschiedlicher Anmeldeinformationen pro Gruppe

Sie können einen anderen Benutzernamen/ein anderes Kennwort festlegen, indem Sie mit der rechten Maustaste auf das Gruppensymbol klicken und **Set Authentication** wählen, wie unten dargestellt.



Daraufhin wird ein Dialog angezeigt, in dem Sie alternative Anmeldedaten eingeben können:

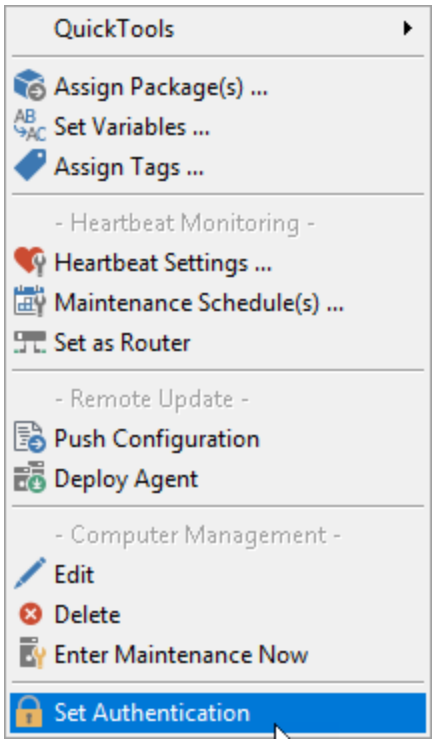


Sobald der Benutzername und das Passwort festgelegt sind, verwendet EventSentry diese Zugangsdaten, wenn eine Verbindung zu einem beliebigen Computer in dieser bestimmten Gruppe hergestellt wird. Dazu gehört auch die direkte Verbindung zu Computern mit der Verbindungsfunktion, wenn mit der rechten Maustaste auf Computerobjekte geklickt wird.

Der von Ihnen eingegebene Benutzername und das Passwort werden in der Registrierung verschlüsselt und können nur von dem Benutzer entschlüsselt werden, der sie verschlüsselt hat. Wenn sich z.B. **Admin1** an einem Computer anmeldet und einen Benutzernamen/ein Passwort für eine Gruppe oder einen Computer festlegt und **Admin2** sich am selben Computer anmeldet, dann kann **Admin2** den von **Admin1** eingegebenen Benutzernamen und das Passwort nicht sehen.

Angeben unterschiedlicher Berechtigungsnachweise pro Rechner

Wenn nur einige wenige Rechner unterschiedliche Zugangsdaten benötigen, können Sie einen Benutzernamen und ein Passwort für jeden Rechner festlegen. Klicken Sie diesmal mit der rechten Maustaste auf den Rechnernamen statt auf die Gruppe



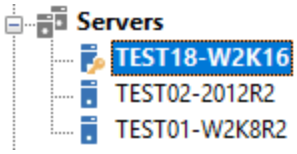
und wählen Sie erneut **Set Authentication**. Bitte beachten Sie, dass Anmeldeinformationen, die pro Computer festgelegt werden, immer Anmeldeinformationen auf Gruppenebene überschreiben.

Entfernen von Anmeldedaten

Um zuvor festgelegte Anmeldedaten wieder zu entfernen (ob für eine Gruppe oder für einen Computer), klicken Sie mit der rechten Maustaste auf das entsprechende Symbol und wählen Sie *Authentifizierung festlegen*. Klicken Sie im Dialogfeld auf *Authentifizierung entfernen*, um die Anmeldeinformationen zu löschen.

Icons

Wenn Sie unterschiedliche Anmeldeinformationen für Computerelemente oder -gruppen festlegen, werden Sie feststellen, dass dem im Strukturfenster angezeigten Symbol eine kleine grüne Karte hinzugefügt wird, wie in der Abbildung unten dargestellt:



Dies soll darauf hinweisen, dass unterschiedliche Anmeldeinformationen gespeichert sind, im obigen Beispiel auf **TEST18-W2K16**.

4.6.3 Status prüfen

Eine typische Statusprüfung sieht folgendermaßen aus:

Host	Action: Check Status	Agent	Config Revision	Tags	SNMP	Ping	TCP	Heartbeat	Customized
EVENTSENTRY	Running & connected to collector, last activity 29 seconds ago	5.1.1.98	328			0 ms	-	PA	X
SC-SRV1-2022	Running & connected to collector, last activity 104 seconds ago	5.1.1.98	320			0 ms	-	PA	
SC-SRV2-2019	Running & connected to collector, last activity 89 seconds ago	5.1.1.98	320			0 ms	-	PA	

Der Servicestatusbericht zeigt Ihnen die folgenden Informationen an:

- **Ob der EventSentry-Dienst installiert ist oder nicht**
  Diese Informationen sind in der Spalte *Status / Ergebnis* der Ausgabe sichtbar.

- **Der Status des Dienstes (läuft oder gestoppt)**
  Diese Informationen sind in der Spalte *Status / Ergebnis* der Ausgabe sichtbar.

- **Die Version des Dienstes**
  Diese Informationen sind in der Spalte *Version* sichtbar. Wenn der Dienst nicht installiert ist, ist die Versionsnummer **0.00**. Bitte beachten Sie, dass die Versionsinformation des Dienstes nur dann korrekt ist, wenn der Dienst läuft.

Um die netzwerkbezogenen Spalten (SNMP, Ping, TCP, ...) anzuzeigen, klicken Sie mit der rechten Maustaste auf das Ergebnisfenster und aktivieren Sie die Option "Extensive Network Check". Wenn Sie diese Option aktivieren, werden bei der Verarbeitung von Windows-Hosts zusätzliche Netzwerkverbindungschecks durchgeführt. Diese Option ist die Standardeinstellung bei der Verarbeitung von Netzwerkgeräten.

- **Der Computertyp des entfernten Rechners (Arbeitsstation oder Server)**
  Das Symbol neben dem Computernamen zeigt Ihnen an, ob auf dem entfernten Computer ein Workstation-Betriebssystem oder ein Server-Betriebssystem läuft.


Workstation-OS


Server-Betriebssystem

Zusätzlich zum Betriebssystemtyp zeigt Ihnen das Symbol zusätzliche Informationen über den Status des entfernten Computers an:

Symbol	Arbeitsstation oder Server	EventSentry-Agent-Status	Netzwerk-Status	Beschreibung
	Unbekannt	Unbekannt	Unbekannt	Anfangssymbol, bevor "Remote Update" versucht, die angeforderte Aktion auszuführen
	Unbekannt	Unbekannt	Abwärts	Wird angezeigt, wenn der entfernte Host nicht erreichbar ist (z. B. wenn er nicht auf Ping antwortet)
	Server	Laufende	Nach oben	Wird angezeigt, wenn auf dem entfernten Host ein Serverbetriebssystem läuft und der Agent ausgeführt wird
	Server	Angehalten oder nicht installiert	Nach oben	Wird angezeigt, wenn der Remote-Agent angehalten oder nicht installiert ist oder ein Remote-Aktualisierungsfehler aufgetreten ist.
	Arbeitsplatz	Laufende	Nach oben	Wird angezeigt, wenn auf dem entfernten Host ein Client-

			Betriebssystem läuft und der Agent ausgeführt wird
Arbeitsplatz	Angehalten oder nicht installiert	Nach oben	Wird angezeigt, wenn der Remote-Agent angehalten, nicht installiert oder ein Remote-Update-Fehler aufgetreten ist

4.6.4 Konfigurationsupdates

Mit "Push Configuration" können Sie die lokale Konfiguration an entfernte Hosts senden, um die manuelle Einrichtung mehrerer Hosts mit derselben Konfiguration zu vermeiden.

Die folgenden Einstellungen werden auf entfernten Hosts aktualisiert, wenn Sie eine **Push-Konfiguration** durchführen:

- Globale Optionen
- Alle Pakete, Scripts usw.
- Aktionen

Anforderungen

Um die Konfiguration auf den Remote-Host zu übertragen, muss entweder die **ADMIN$-** oder die ES$-Freigabe vorhanden sein. Weitere Informationen finden Sie weiter unten:

ADMIN$: Dies ist die standardmäßige administrative Freigabe, die auf allen Windows-Computern aktiviert ist und das Verzeichnis %SYSTEMROOT% (z.B. C:\Windows) für Benutzer der Gruppe Administratoren freigibt. Wenn diese Freigabe auf Ihren Hosts vorhanden ist, die von EventSentry, dann funktioniert die Fern-Aktualisierung einwandfrei.

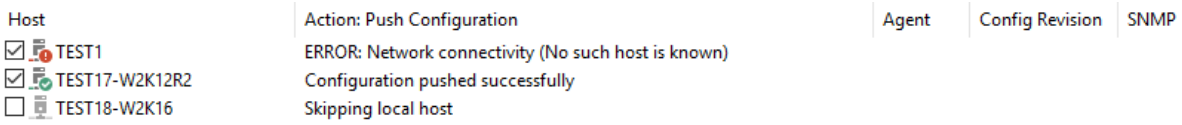
ES$: Wenn, aus welchem Grund auch immer, die ADMIN$-Freigaben auf Ihren überwachten Hosts nicht vorhanden sind, müssen Sie die ES$-Freigabe manuell erstellen.

Die Anweisungen lauten wie folgt:

1. Erstellen Sie das Verzeichnis `C:\Program Files\EventSentry\RemoteUpdate`
2. Geben Sie dieses Verzeichnis als **ES$** frei. Dadurch wird eine versteckte Freigabe erstellt, die für jemanden, der das Netzwerk durchsucht, nicht sichtbar ist.
3. 3. Erlauben Sie nur Mitgliedern der **Domänen-Admins** oder lokalen **Administratoren** Schreibzugriff auf diese Freigabe.
4. Starten Sie die EventSentry Agent(en).

Starten der Aktualisierung

Nachdem Sie auf die Schaltfläche **OK** geklickt haben, sehen Sie einen Bildschirm ähnlich dem untenstehenden, in dem die Konfiguration auf dem Host **TEST17-W2K8R2** aktualisiert wurde.



Das obige Bildschirmfoto zeigt, dass Remote Update keine Verbindung mit dem Computer TEST1 herstellen konnte (er war nicht eingeschaltet) und dass der Computer TEST17-W2K8R2 das Konfigurationsupdate erfolgreich empfangen hat. Der Computer TEST18-W2K16 wurde übersprungen, weil er der EventSentry-Verwaltungsserver (lokaler Host) ist und keine Push-Konfiguration erfordert -

jedes Mal, wenn Sie auf Speichern klicken, wird die Konfiguration auf dem EventSentry-Verwaltungsserver aktualisiert.

Wie bei jeder Fern-Aktualisierungsfunktion können Sie mit der rechten Maustaste auf die Liste klicken und die Ergebnisse in einer Textdatei speichern.

Ausschlüsse

Die folgenden Funktionen sind von der Fernaktualisierungsfunktion ausgeschlossen und müssen einzeln verwaltet werden:

- Umgebungseinstellungen (z.B. Temperatureinstellungen, Feuchtigkeitseinstellungen usw.)
- Alle Einstellungen unter "Network Services / Netzwerkdienste"

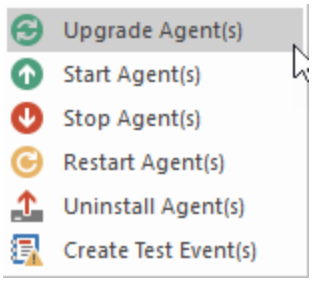
Um die oben genannten Einstellungen zu verwalten, kopieren Sie die Verwaltungskonsole (*eventsentry_gui_x64.exe* auf 64-Bit-Systemen *eventsentry_gui.exe* auf 32-Bit-Systemen) auf den Remote-Host und führen Sie die Verwaltungskonsole dort aus. Diese Einstellungen werden durch das nächste Konfigurationsupdate nicht überschrieben, unabhängig davon, ob es manuell oder über den Collector initiiert wird.

4.6.5 Agenten verwalten

Mit der Funktion "**Agenten verwalten**" können Sie den Status von EventSentry auf entfernten Computern kontrollieren und ändern. Die folgenden Aktionen können ausgeführt werden:

- **Installieren Sie** den Dienst (einschließlich des Kopierens notwendiger Dateien), indem Sie den Agenten einsetzen
- **Aktualisieren** der auf entfernten Computern ausführbaren Dienstdatei (startet den Dienst neu, falls erforderlich)
- **Deinstallieren Sie** den Dienst (einschließlich Dateien und Konfiguration)
- **Starten Sie** den Dienst auf entfernten Computern
- **Beenden** des Dienstes auf entfernten Computern

Um Aktionen mit Agenten durchzuführen, wählen Sie eine **Computergruppe** aus und klicken Sie in der Symbolleiste auf **Agent bereitstellen** oder klicken Sie in der Symbolleiste auf **Andere Aktionen** und wählen Sie eine Aktion wie z.B. **Upgrade/Update** aus dem Dropdown-Menü. Sie können auch mit der rechten Maustaste auf eine Computergruppe klicken und Aktionen aus dem Menü "**Manage Agent(s)**" auswählen:



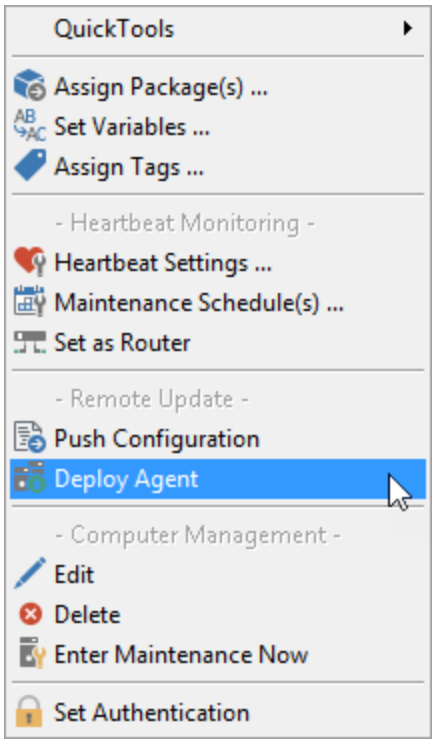
Nachdem Sie die gewünschte Aktion (z.B. **Upgrade**) gewählt haben, klicken Sie auf die Schaltfläche **GO** in der Symbolleiste, um die Aktion auszuführen. Sie sehen dann eine Bildschirmausgabe ähnlich der unten gezeigten:

Host	Action: Deploy Agent	Agent	Config Revision	SNMP	Ping	TCP
TEST17-W2K12R2	Agent updated successfully	4.0.1.2	10			

4.6.6 Agenten installieren

Wenn Sie EventSentry auf einem neu eingerichteten Computer einrichten möchten, d.h. auf einem Computer, auf dem EventSentry noch nicht installiert ist, dann können Sie die Funktion "**Agent verteilen**" verwenden.

Fügen Sie einfach den Host zu einer Computergruppe hinzu, klicken Sie mit der rechten Maustaste auf den Host und wählen Sie "**Agent bereitstellen**":



Remote Update wird automatisch die EventSentry-Dateien kopieren, den Dienst erstellen, alle Konfigurationsdaten (Ereignisprotokollfilter, Systemzustand, Aktionen, ...) kopieren und den Dienst starten. Sie können den Agent auf mehreren Hosts gleichzeitig verteilen, indem Sie eine Computergruppe auswählen und dann in der Symbolleiste auf die Schaltfläche "**Deploy Agent"** und dann auf die Schaltfläche "**Go"** klicken.

Diese Funktion ist der schnellste Weg, einen neuen Computer mit EventSentry zu überwachen.

ODBC-Treiber

Beginnend mit Version 2.93 installiert der EventSentry-Agent automatisch PostgreSQL-Treiber, wenn diese erforderlich sind (d.h. mindestens eine Aktion verwendet eine PostgreSQL-Datenbank). Die MSI-Treiberdateien werden von der Managementkonsole während einer Remote-Agent-Installation verteilt und dann später vom Agenten installiert.

ODBC-Treiber sind für Aktion welche den Collector verwenden nicht erforderlich.

4.6.7 Remote-Update automatisieren

Remote-Update und die automatischen Bereitstellungsfunktionen des Collectors erleichtern die Verwaltung von EventSentry-Agenten, da Sie die Software nicht manuell auf den Remote-Hosts installieren müssen. In einigen Fällen, z. B. wenn Sie den Collector nicht verwenden können und eine große Anzahl von Hosts verwalten müssen, kann es jedoch erforderlich sein, das Dienstprogramm für die Remote-Aktualisierung zu verwenden.

EventSentry enthält ein Utility mit dem Funktionen vom "Remote Update" (eventsentry_upd.exe) mit Hilfe des Windows-Schedulers in gewünschten Intervallen (z.B. einmal pro Tag) automatisch ausführen lassen können. Das Remote-Update-Dienstprogramm bietet die folgenden Funktionen:

- Übertragen der Konfiguration auf entfernte Hosts
- Nur ausführen, wenn sich die Konfiguration geändert hat
- Zusammenfassende Informationen zum Ereignisprotokoll protokollieren
- Automatische Aktualisierung entfernter Computer zur Verwendung des neuesten Agenten
- Automatisches Installieren des Agenten auf einem entfernten Host, falls er nicht bereits installiert ist
- Automatisches Starten des Agenten auf einem entfernten Host, wenn er angehalten wird

Wir empfehlen Ihnen, das Remote-Update-Dienstprogramm so einzuplanen, dass es ein oder mehrere Male am Tag ausgeführt wird (z.B. nachts und morgens), aber Sie können es auch manuell über die Befehlszeile ausführen. Das Remote-Update-Dienstprogramm besteht aus einer Datei (eventsentry_upd.exe) und wird in den Installationsordner von EventSentry installiert und unterstützt die folgenden Befehlszeilenoptionen:

Umfang (erforderlich)

`/allgroups`	Computer in allen Gruppen aktualisieren.
`/group:GRUPPENNAME`	Computer in der angegebenen Gruppe aktualisieren.

Optionen

`/log`	Protokollierung der Ergebnisse im Ereignisprotokoll (Details)
`/installupdate`	Gewährleistet das: • Der Remote-Agent wird auf die neueste Version aktualisiert, wenn er veraltet ist • Der EventSentry-Agent ist installiert, falls er nicht bereits • Der EventSentry-Agent wird gestartet, wenn er gestoppt wird
`/repeatfailed`	Wenn ein Host nicht erreichbar ist, speichert Remote Update den Hostnamen in einer temporären Datei und versucht, den Host erneut zu kontaktieren, wenn das Dienstprogramm das nächste Mal aufgerufen wird und sich die Konfiguration in der Zwischenzeit nicht geändert hat. Wenn sich die Konfiguration geändert hat, wird das Dienstprogramm unabhängig davon erneut mit allen Hosts sprechen.
`/usead`	Verwenden Sie Active Directory: Wenn Sie ActiveDirectory-Fähige Gruppen haben (mehr Info), dann sollten Sie diese Option aktivieren. Remote Update aktualisiert die Computerliste aus Active Directory und installiert den Agenten auf Computern, die einer OU oder Gruppe hinzugefügt wurden.
`/noping`	Pingen Sie entfernte Hosts nicht an, bevor Sie versuchen, ein Update durchzuführen

`/uninstall`	Deinstallieren des EventSentry-Agenten von entfernten Hosts
`/force`	Erzwingen einer Konfigurationsaktualisierung, auch wenn sich die lokale Konfiguration nicht geändert hat

Beispiele

Durch einfaches Ausführen von eventsentry_upd.exe mit einer Bereichs-Option (z. B. /allgroups) wird die neueste Konfiguration an alle Hosts ausgegeben, aber Sie können das Dienstprogramm durch Verwendung einiger Befehlszeilenoptionen besser nutzen.

Beispiel 1: Verschieben der Konfiguration auf alle Hosts

```
eventsentry_upd.exe /allgroups
```

Beispiel 2: Übertragen der Konfiguration auf alle Hosts in der Gruppe "Server", Protokollierung des Ergebnisses:

```
eventsentry_upd.exe /group:Server /log
```

Beispiel 3: Übertragen der Konfiguration auf alle Hosts, Protokollierung des Ergebnisses und Sicherstellung, dass die Agenten aktuell sind und laufen:

```
eventsentry_upd.exe /allgroups /log /installupdate
```

Beispiel 4: Übertragen der Konfiguration auf alle Hosts, Protokollieren des Ergebnisses, Aktualisieren der Computerliste aus ActiveDirectory und Installieren des Agenten auf neu hinzugefügten Computern:

```
eventsentry_upd.exe /allgroups /log /installupdate /usead
```

Der folgende Screenshot zeigt die Ausgabe der Ausführung des Remote-Update-Dienstprogramms:

4.6.7.1 Rückgabecodes & Ereignisprotokoll

Vom Fernaktualisierungsprogramm protokollierte Ereignisse:

Ereignis-ID	Beschreibung der Veranstaltung	Beispiel
1100	Das EventSentry Remote Update Utility wurde erfolgreich abgeschlossen.	Das EventSentry Remote Update Utility wurde abgeschlossen, 4 Host(s) wurden erfolgreich aktualisiert.
1101	Das EventSentry Remote-Update-Dienstprogramm wurde abgeschlossen, aber einige Hosts konnten nicht aktualisiert werden.	Das EventSentry Remote Update Utility wurde fertiggestellt. 4 Host(s) wurden erfolgreich aktualisiert, 1 Host(s) ist fehlgeschlagen. Die folgenden Hosts konnten nicht aktualisiert werden: DC2-W2K.

Die Ereignis-ID 1101 wird als **Warnung** protokolliert, wenn mindestens ein Computer für ein Update erreicht werden konnte, andernfalls wird sie als **Fehler** protokolliert.

Rückgabecodes (%ERRORLEVEL%):

Rückgabe-Code	Beschreibung
0	Keine Fehler, alle Hosts wurden erfolgreich aktualisiert
3	Fehler beim Lesen der Konfiguration
7	Ungültige Befehlszeilenoptionen bereitgestellt
9	Die Konfigurationsaktualisierungsdatei (.reg) konnte nicht erstellt werden
10	Ein oder mehrere Hosts konnten nicht erfolgreich verarbeitet werden
11	Ein oder mehrere Hosts konnten nicht erfolgreich verarbeitet werden, während zuvor fehlgeschlagene Hosts wiederholt wurden

4.6.8 Fernverwaltung

Es wird **nicht empfohlen**, eine Remote-Installation über eine Verbindung zu verwalten. Stattdessen empfehlen wir, alle Remote-Agenten mit **Remote Update** zu verwalten. Wenn möglich, verwenden Sie die Funktion "Verbinden mit" nur, um die aktive Konfiguration auf einem entfernten Host zu überprüfen, nicht um sie zu verwalten.

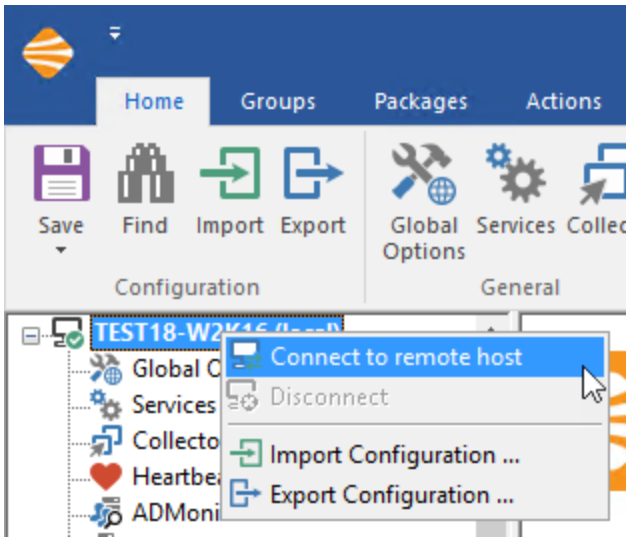
Sie können jede EventSentry-Installation genauso wie eine lokale Installation aus der Ferne verwalten. Die einzige Einstellung, die nicht fernadministriert werden kann, ist das Remote Update selbst.

Kriterien:

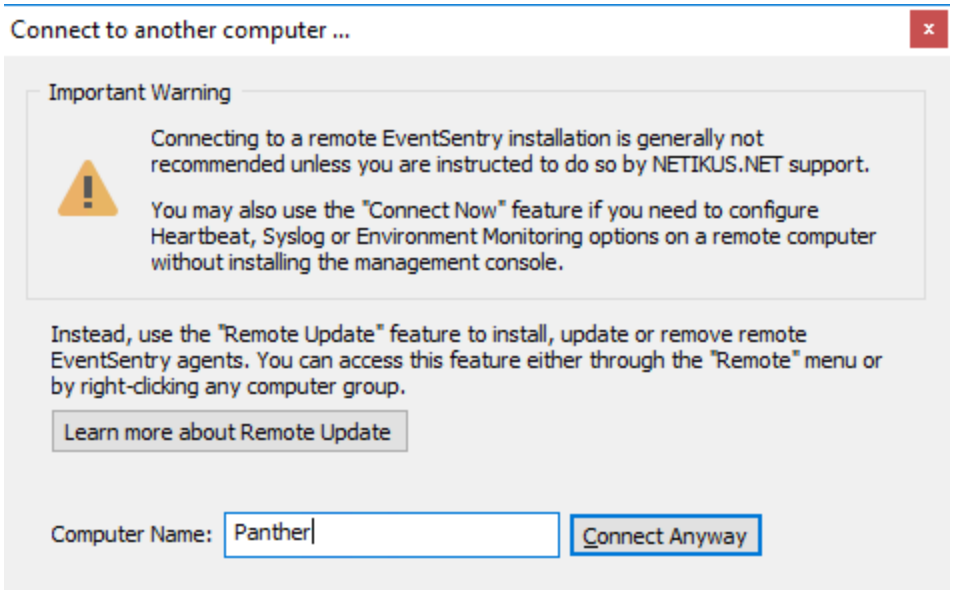
- Sie haben die Berechtigung, auf die Registrierung des entfernten Computers zuzugreifen (unter Win2k und höher stellen Sie bitte sicher, dass der **entfernte Registrierungsdienst** läuft)
- Sie haben Lese-/Schreibberechtigungen für den Registrierungsschlüssel **HKLM\Software\netikus.net\EventSentry**
- Die Standard-Administrationsfreigabe **ADMIN$** ist auf dem entfernten Computer vorhanden (nur für die Remote-Service-Installation erforderlich)

Anweisungen:

Option 1: Klicken Sie mit der rechten Maustaste auf das Objekt des lokalen Computers und wählen Sie "**Mit entferntem Host verbinden**". Sie können auch eine Verbindung zu einem Remote-Host herstellen, indem Sie einen Host innerhalb einer Computergruppe auswählen und dann auf die Schaltfläche "Jetzt verbinden" in der Symbolleiste klicken.



Wenn Sie "Mit entferntem Host verbinden" wählen, werden Sie aufgefordert, den Computernamen einzugeben und auf "**Auf jeden Fall verbinden**" zu klicken.



Remote Update-Funktionen sind nicht verfügbar, solange Sie mit einem entfernten Rechner verbunden sind. Sie müssen mit dem lokalen Rechner verbunden sein, um eine Fern-Aktualisierung durchführen zu können.

4.7 Skripte

Skripte erlauben die Einbettung von Skripten jeglicher Art (Befehlszeilenskripte, visuelle Basisskripte, Perl-Skripte usw.) in die EventSentry Konfiguration, so dass die Skripte selbst nicht auf den Zielcomputern gewartet werden müssen, was die Wartung von Umgebungen, die Skripte verwenden, erleichtert.

Aus diesen Komponenten können Skripte verwendet werden:

- Application Scheduler
- Process action
- Validation Scripts

Skripte können in jeder Sprache geschrieben werden, solange der Skript-Interpreter (z.B. Perl) auf dem Rechner, auf dem das Skript ausgeführt werden soll, richtig installiert ist. Beispielsweise muss ActivePerl auf einem Host installiert sein, auf dem Perl-Skripte zur Ausführung konfiguriert sind.

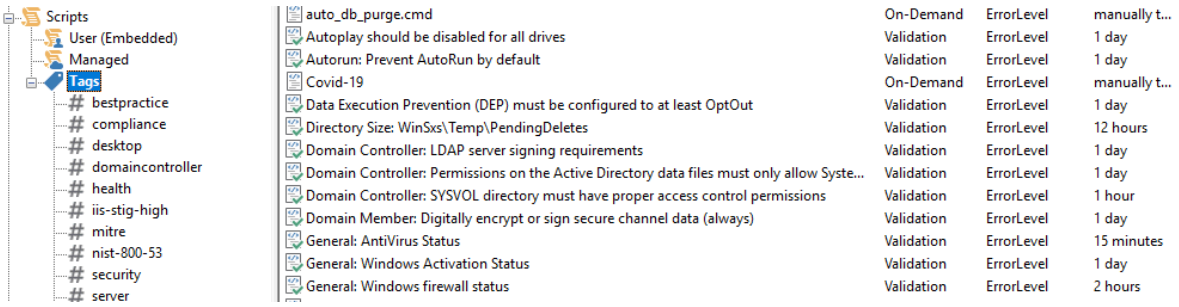
Skripte werden in der Registry gespeichert und können in den Unterknoten unter dem Hauptknoten **Skripte** konfiguriert werden, wo die allgemeinen Optionen konfiguriert werden.

User (embedded)
Von Benutzern gepflegte (eingebettete) Skripte können hier verwaltet werden, und wenn Sie auf diesen Knoten klicken, werden alle vorhandenen Benutzerskripte angezeigt.

Managed
Heruntergeladene Skripte, die von NETIKUS.NET verwaltet werden, werden hier angezeigt, und wenn Sie auf diesen Knoten klicken, werden alle verwalteten Skripte angezeigt. Verwaltete Skripte können zwar nicht bearbeitet oder gelöscht werden, aber sie können deaktiviert und die Ausführungshäufigkeit kann ebenfalls angepasst werden. Tags, die mit Skripten verknüpft sind, können nicht entfernt werden, aber es können zusätzliche Tags hinzugefügt werden.

Schlagwörter
Skripte können mit Tags versehen werden (und alle verwalteten Skripte haben mindestens ein Tag), die in Validierungsskript-Paketen verwendet werden können.

Skripte verwenden
Um ein Skript zu verwenden, stellen Sie dem Dateinamen in einem Anwendungszeitplan oder einer Prozessaktion das @-Symbol voran. Wenn Ihr Skript beispielsweise den Namen LaunchUpload.cmd hat, geben Sie **@LaunchUpload.cmd** an. Felder, die eingebettete Skripts unterstützen, verfügen über ein Pulldown-Menü, mit dem Sie aus jedem der konfigurierten Skripts auswählen können.



4.7.1 Allgemein

Allgemeine Optionen gelten für alle Skripte, unabhängig davon, ob es sich um Benutzer-, Verwaltungs-, On-Demand- oder Validierungsskripte handelt.

Verwaltete Skripte
Verwaltete Skripte werden regelmäßig gewartet und aktualisiert, Aktualisierungen stehen Evaluationsanwendern und Kunden mit aktiven Wartungsverträgen zur Verfügung. Benutzer können die verwalteten Skripte durch ihre eigenen ergänzen, aber die verwalteten Skripte können nicht geändert werden.

Start-Ordner
Dies ist das Verzeichnis, in dem sich die Skripte auf der Festplatte befinden und von dem aus sie ausgeführt werden. Die Standardeinstellung ist `%SYSTEMROOT%\system32\eventsentry.scripts` und kann durch Ändern des **Startordners** angepasst werden.

Eingebettete Skripte, die einem bestimmten Host zugeordnet sind, werden beim Start des Agenten im Startordner dieses Computers erstellt. Wenn ein Skript nicht zugeordnet ist, d.h. weder von einem Anwendungszeitplan, einer Prozessaktion oder einem Validierungsskript-Paket verwendet wird, wird es nicht im Dateisystem erstellt. Skripte im Startordner werden gelöscht, wenn der Agent gestoppt wird.

Berechtigungen einschränken
Der Startordner erbt seine Berechtigungen standardmäßig vom übergeordneten Ordner, die je nach Betriebssystem unterschiedlich sind. Um sicherzustellen, dass nur der Agent Zugriff auf die Skriptdateien im Startordner hat, können Sie das Kontrollkästchen **Berechtigungen einschränken** aktivieren. Dadurch wird sichergestellt, dass nur das Konto, unter dem der EventSentry-Dienst läuft (standardmäßig LocalSystem), die (NTFS-)Berechtigung für den Zugriff auf die Datei(en) hat.

4.7.2 User & Managed Scripts

Wenn Sie entweder auf "Benutzer (eingebettet)" oder "Verwaltet" klicken, wird eine Liste der verfügbaren Benutzer- oder verwalteten Skripte angezeigt.

Verwaltete Skripte sind schreibgeschützt, Skripte können nicht hinzugefügt, bearbeitet oder gelöscht werden. Nur **Benutzer-(eingebettete)** Scripts können hinzugefügt, gelöscht oder bearbeitet werden.

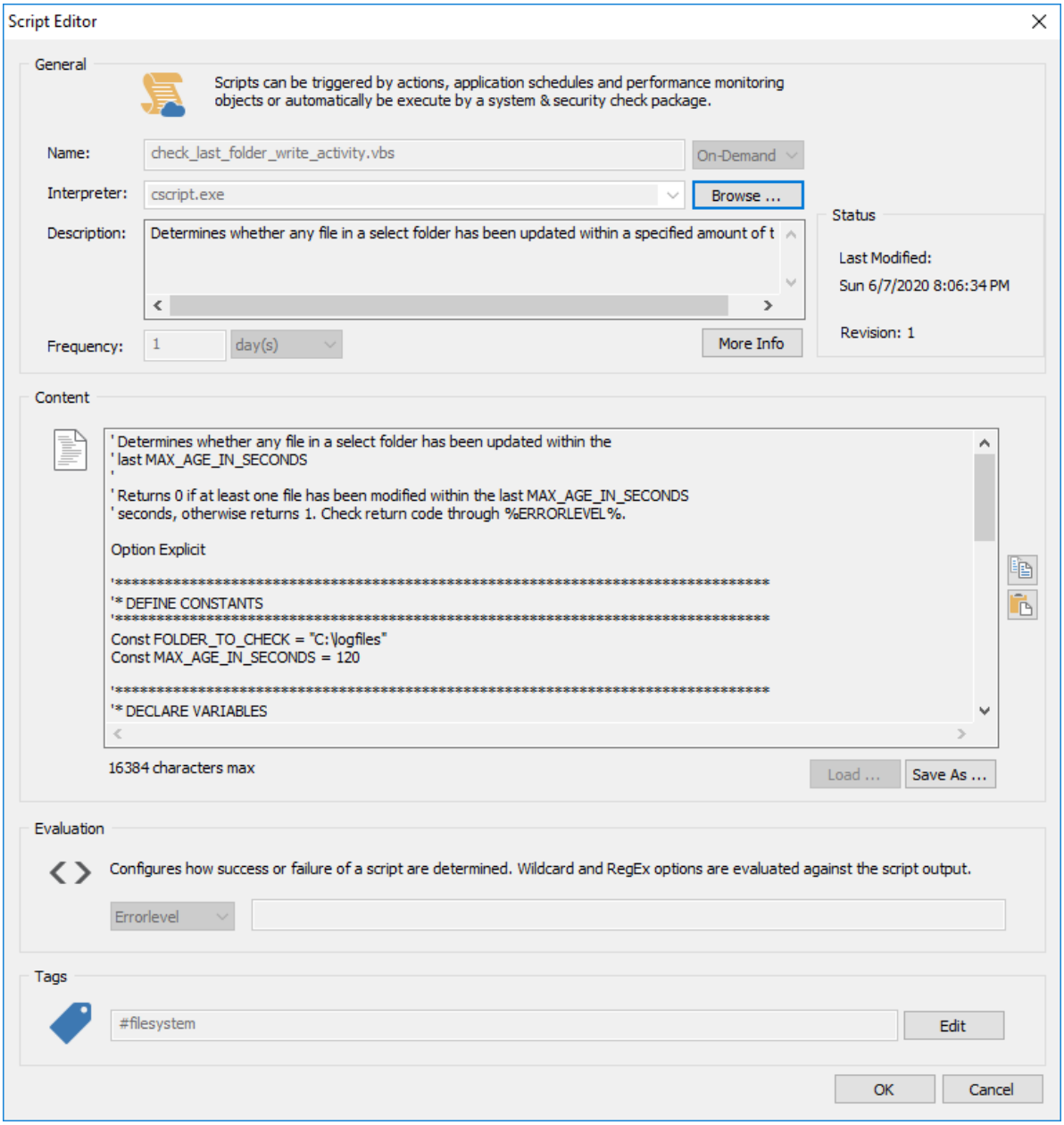
Hinzufügen
Um ein neues Skript zu erstellen, navigieren Sie zuerst zu **"Scripts -> User (Embedded)**" und klicken Sie dann auf die Schaltfläche "**Add"** im Ribbon. Der Name des Skripts ist wichtig, da dies der Name der Datei im Startordner sein wird. Es wird empfohlen, eine gültige Dateierweiterung anzugeben (erforderlich, wenn kein Interpreter angegeben ist).

Sie können den Skriptinhalt im Textbereich **Skriptinhalt** angeben, der Skripte mit bis zu 16384 Zeichen unterstützt. Skripte können entweder direkt im Textfeld Skriptinhalt bearbeitet, aus der Zwischenablage eingefügt (Schaltfläche "Einfügen") oder aus einer Datei geladen werden (Schaltfläche "**Laden"**).

Verwalten
Um ein vorhandenes Skript zu bearbeiten, navigieren Sie zu **Skripte -> Benutzer (eingebettet)**, suchen Sie das zu bearbeitende Skript und doppelklicken Sie darauf. Im daraufhin erscheinenden Dialog können Sie entweder das eigentliche Skript direkt im Textbereich **Skriptinhalt** bearbeiten, den Inhalt in die/aus der Zwischenablage kopieren und einfügen oder das Skript in eine Datei laden/speichern. Andere Eigenschaften, einschließlich des Interpreters und der Tags, können hier ebenfalls bearbeitet werden.

Löschen von

Um ein Skript zu löschen, navigieren Sie zu **Skripte -> Benutzer (eingebettet)**, wählen Sie das Skript aus und klicken Sie auf die Schaltfläche **Löschen** in der Multifunktionsleiste. Denken Sie daran, dass alle Anwendungszeitpläne und/oder Prozessaktionen, die auf das gelöschte Skript verweisen, nicht mehr funktionieren, wenn das Skript nicht mehr existiert.



Typ: On-Demand vs. Validierung

Alle Skripte, entweder User oder Managed, können entweder On-Demand- oder Validierungsskripte sein. Die überwiegende Mehrheit der verwalteten Skripte sind Validierungsskripte.

Auf Anfrage ("On Demand"): Werden entweder durch einen Anwendungszeitplan oder eine Prozessaktion referenziert.
Validierung ("Validation"): Werden von einem oder mehreren Validierungsskript-Paketen referenziert.

Aktiviert (nur Validierungsskripts)
Aktiviert oder deaktiviert ein Skript. Dies ist vor allem nützlich, um verwaltete Skripte zu deaktivieren, die aufgrund ihres Tags automatisch als Teil eines Validierungsskriptpakets enthalten sind, aber nicht ausgeführt werden sollen.

Interpreter
Ein Interpreter ist nur dann erforderlich, wenn die Dateierweiterung, die für die Datei verwendet wird, vom Betriebssystem nicht auf eine ausführbare Datei abgebildet werden kann. Wenn Sie z.B. ein PERL-Skript hinzufügen, können Sie **perl.exe** als Skript-Interpreter angeben.

Häufigkeit
Steuert, wie oft das Skript ausgeführt wird, nur für Validierungsskripts relevant. Die Frequenz von On-Demand-Skripts wird entweder vom Anwendungs-Scheduler oder von Ereignissen gesteuert, die die Aktion auslösen. Das Validierungsskript folgt diesem Zeitplan, auch wenn der Agent neu gestartet wird oder eine neue Konfiguration empfangen wird. Hinweis: Wenn ein zugewiesenes Validierungsskript aktualisiert und an den Agenten übertragen wird, wird es sofort ausgeführt, unabhängig von seinem Zeitplan.

Auswertung
Validation Script-Pakete bestimmen, ob ein Skript den Test besteht oder nicht, und zwar auf der Grundlage der Bewertungskriterien, die entweder sein ERRORLEVEL, eine Platzhalterprüfung oder eine RegEx-Prüfung sein können.

Fehlerstufe (%ERRORLEVEL%)
0: Skript hat Prüfung bestanden (OK)
998: Skript hat Prüfung mit Warnung bestanden (WARNING)
999: Das Skript ist auf dem System nicht anwendbar und sollte ignoriert werden.

Jede andere Fehlerstufe bedeutet einen Fehler.

Platzhalter:
Wendet das angegebene Platzhaltermuster auf die Ausgabe des Skripts an. Wenn das Muster übereinstimmt, besteht das Skript seine Prüfung.

RegEx:
Wendet das angegebene RegEx-Muster auf die Ausgabe des Skripts an. Wenn das Muster übereinstimmt, besteht das Skript die Prüfung.

Tags
Können sowohl für On-Demand- als auch für Validierungsskripte angegeben werden, sind aber im Allgemeinen für die Verwendung durch Validierungsskript-Pakete zu Zuweisungszwecken vorgesehen. Beispielsweise können Sie alle Validierungsskripte mit dem Tag **nist-800-53** Hosts zuweisen, die NIST-konform sein müssen. Tags, die mit verwalteten Skripten verknüpft sind, können nicht entfernt werden, aber es können zusätzliche benutzerdefinierte Tags hinzugefügt werden.

4.8 Internationalisierung

EventSentry kann in Umgebungen verwendet werden, in denen Englisch nicht als primäre Sprache und Zeichensatz verwendet wird, einschließlich, aber nicht beschränkt auf Japanisch, Koreanisch und andere. Während die Verwaltungskonsole selbst nur in Englisch verfügbar ist, unterstützen die meisten Benachrichtigungen (z.B. E-Mail, Datei, Datenbank) fremde Zeichensätze und Kodierungen.

Verwaltungskonsole

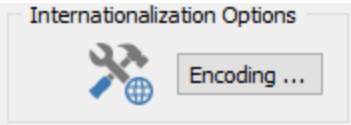
Die Verwaltungskonsole ist nur in Englisch verfügbar, zeigt aber fremdsprachige Zeichen in den Dialogen und im integrierten Ereignisprotokoll-Viewer korrekt an. Fremde Zeichen können auch zur Konfiguration von EventSentry verwendet werden, z. B. in Filterfeldern.

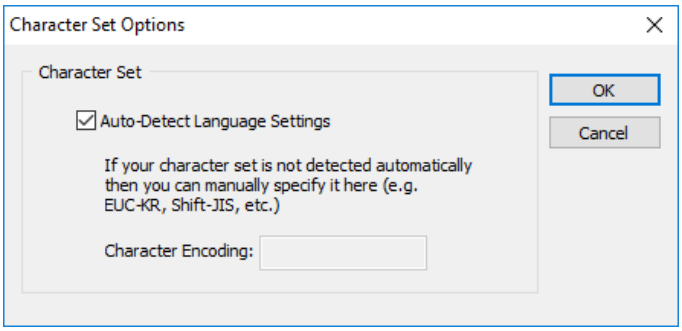
Web Reports

Für die Web Reports existieren mehrere Übersetzungen (z.B. Deutsch, Spanisch), und die Sprache kann mit dem Profileditor eingestellt werden. Wenn Sie eine der unterstützten Sprachen auswählen (weitere Informationen zu den verfügbaren Übersetzungen finden Sie unter Web Reports), wird die Zeichenkodierung der Web Reports automatisch eingestellt. Wenn eine Übersetzung für Ihre Sprache nicht vorhanden ist oder die automatische Kodierungsart falsch ist, können Sie die Kodierung mit dem Profileditor im Abschnitt Lokalisierung einstellen.

E-Mail- und Datei-Aktionen

Wenn Sie Ihre E-Mail- oder Dateibenachrichtigung für die Verwendung von HTML konfigurieren, versucht EventSentry, automatisch die richtige Kodierung zu erkennen. Wenn die Kodierung nicht richtig erkannt wird oder Sie sie manuell einstellen möchten, können Sie sie ändern, indem Sie im Abschnitt "Internationalisierungsoptionen" auf die Schaltfläche **Encoding** klicken. Deaktivieren Sie im daraufhin angezeigten Dialogfeld das Kontrollkästchen "Auto-Detect Language Settings", und geben Sie die korrekte Kodierung im Feld "**Character Encoding**" an.





Datenbank - ODBC-Aktionen

Bei der Verwendung einer Datenbankaktion sind keine zusätzlichen Konfigurationsschritte erforderlich, sie müssen jedoch sicherstellen dass Ihre Datenbank Ihr Gebietsschema unterstützt. Stellen Sie in Microsoft SQL Server® sicher, dass Sie bei der Erstellung einer neuen Datenbank die richtige Collation auswählen, d.h. Sie müssen **eine leere EventSentry-Datenbank erstellen, bevor Sie den EventSentry-Einrichtungs- oder Konfigurationsassistenten ausführen.** Für die integrierte PostgreSQL Datenbank sind keine besonderen Einstellungen erforderlich.

Bitte lesen Sie die folgenden zwei KB-Artikel, um bekannte Probleme bei der Verwendung von Sprachen zu vermeiden, die nicht auf Latein basieren:

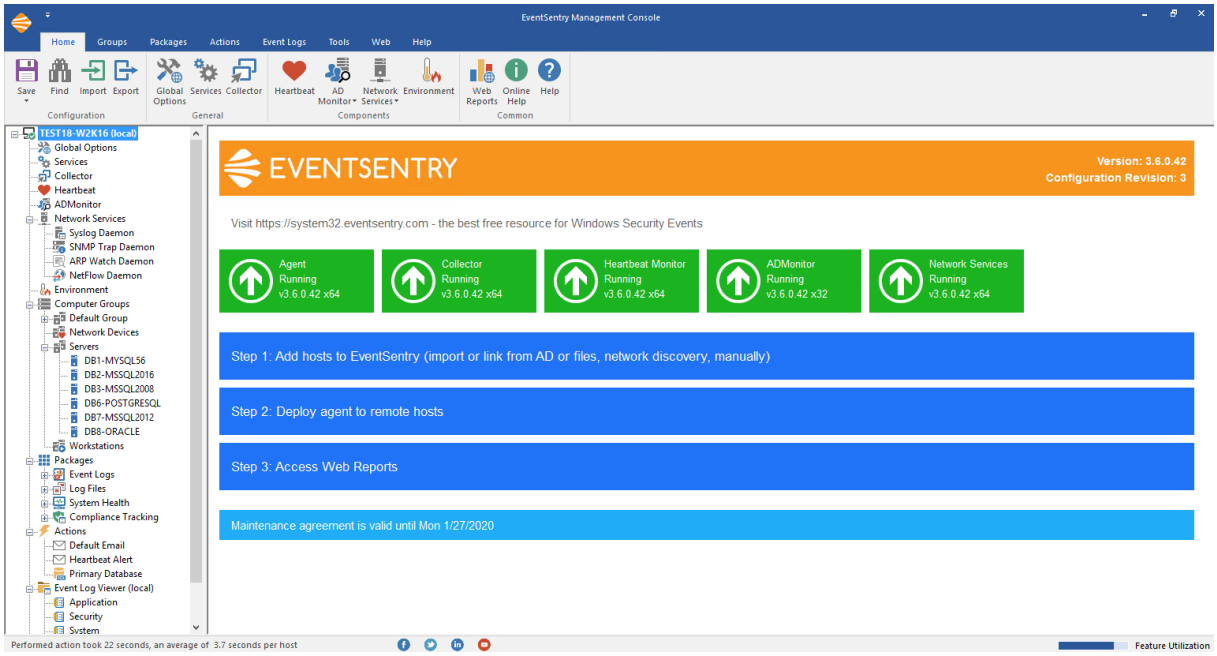
KB-111
KB-112
KB-333

5 Überwachung mit EventSentry

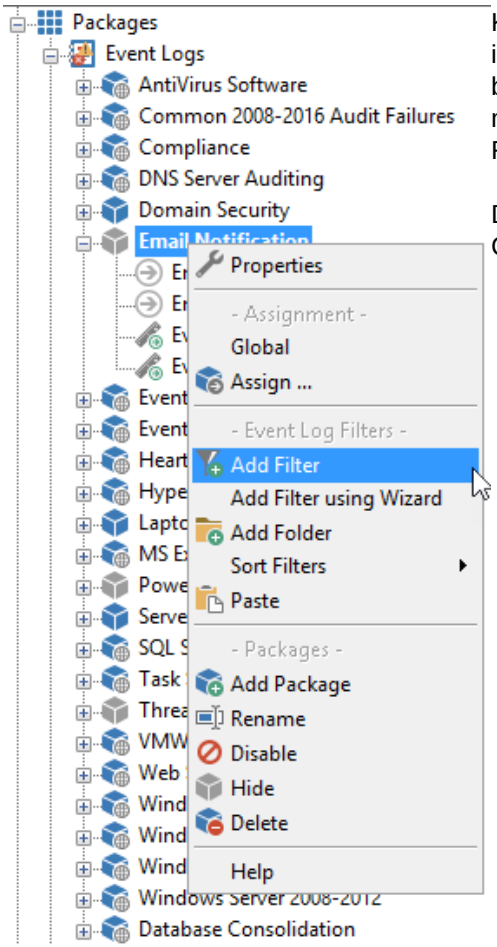
Übersicht

EventSentry wird mit der Anwendung **EventSentry Management Console** konfiguriert. Die Hauptoberfläche ist in zwei Teile unterteilt: das **Baumfenster** auf der linken Seite und das **Detailfenster** auf der rechten Seite.

Das Strukturfenster zeigt alle Objekte nach Typ geordnet, während das Detailfenster alle Details zu einem ausgewählten Objekt anzeigt:



Rechts-Klick

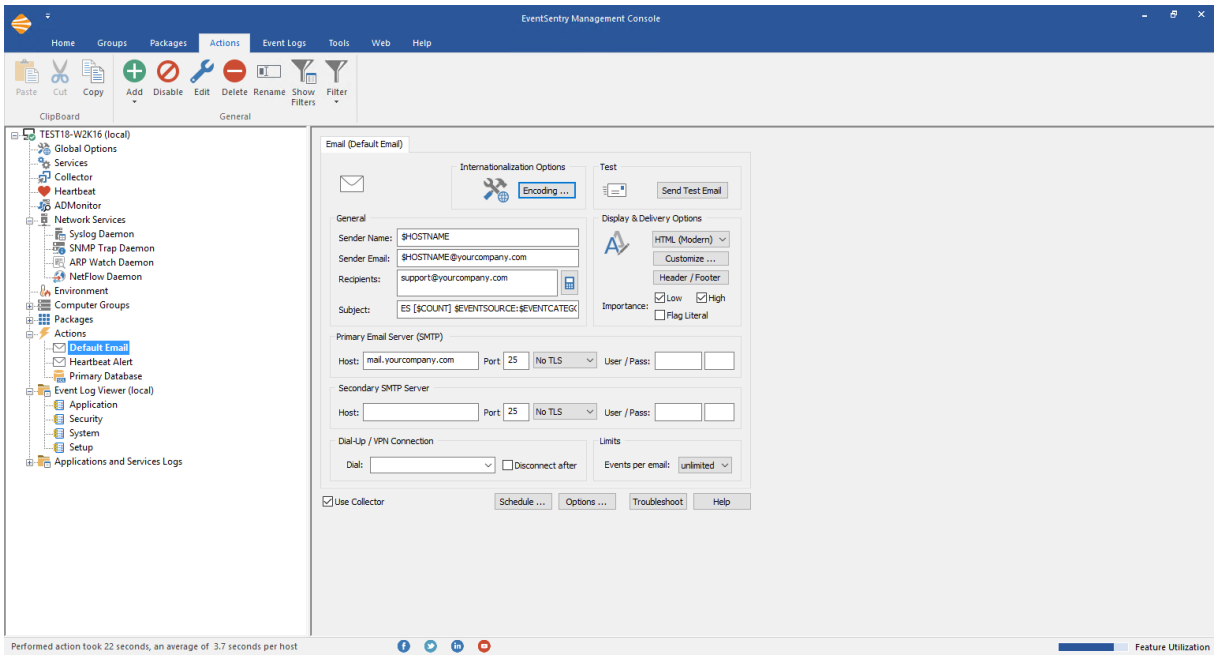


Klicken Sie mit der rechten Maustaste auf Elemente, die sich im linken Strukturfenster befinden, um sie zu ändern. Um beispielsweise einen neuen Filter hinzuzufügen, klicken Sie mit der rechten Maustaste auf die Gruppe, zu der Sie den Filter hinzufügen möchten.

Dies funktioniert für alle Objekte, einschließlich Aktionen und Computerobjekte, auf die gleiche Weise.

Links-Klick

Um die Details eines Objekts, das sich im linken Baumfenster befindet, anzuzeigen, klicken Sie mit der linken Maustaste oder doppelklicken Sie darauf (siehe Verwendbarkeit für diese Einstellung). Die Objektdetails (z.B. Aktionsdetails) werden dann in das Detailfenster geladen und das **aktive Objekt im linken Fenster wird fett** dargestellt, wie unten zu sehen ist:



Menü

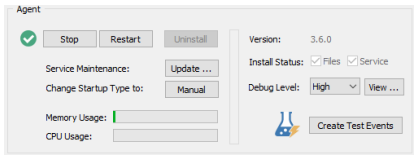
Zusätzlich kann das Verhalten der Verwaltungskonsole auch über den Ribbon angepasst werden:

- Bestätigungsmeldungen anpassen, um Bestätigungsdialoge zu aktivieren oder zu deaktivieren (z.B. bevor ein Filter endgültig gelöscht wird)
- **Remote Update-Einstellungen** anpassen
- Feedback, Vorschläge oder Bugs senden
- Ressourcen im Internet besuchen

> Dieser Agent muss nicht neu gestartet werden, wenn Konfigurationsänderungen vorgenommen werden, einschließlich Änderungen, die über ein Remote-Update durchgeführt werden.

5.1 Dienstkontrolle

Sie können das Menü "Dienste" verwenden, um den EventSentry-Agenten und andere EventSentry-Dienste zu verwalten. Der Agent-Abschnitt unterstützt die folgenden Steuerelemente:



- Start: Starten Sie den Dienst
- Stop: Den Dienst beenden
- Neustart: Neustart des Dienstes

- Installieren: Installieren Sie den Dienst manuell
- Deinstallieren: Deinstallieren Sie den Dienst manuell

- Startup-Typ: Schalten Sie den Dienst-Starttyp von Automatisch auf Manuell und umgekehrt
- Aktualisieren: Aktualisieren der ausführbaren Dienstdatei

- Debug-Level: Ändern Sie die Protokollierungsebene der Agentendiagnose. Empfohlener Wert: Hoch
- Ansicht: Zeigen Sie jetzt das Diagnoseprotokoll des Agenten an.

Die Kontrollkästchen Dateien/Dienst zeigen an, ob die erforderlichen Dateien und der Dienst richtig installiert sind.

Agent

Der "EventSentry"-Dienst ist der Hauptdienst, der das Ereignisprotokoll, die Dienste, den Plattenplatz usw. überwacht.

Es ist nicht möglich, den Agenten auf entfernten Computern über das Menü Dienste zu verwalten. **Verwenden Sie** stattdessen **die Registerkarte "Gruppen" in der Symbolleiste, um Agenten auf Remote-Computern zu verwalten**.

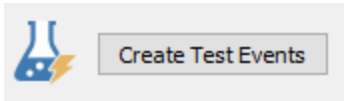
Weitere Informationen finden Sie im Kapitel Agenten verwalten.

Heartbeat-Monitor

Der "EventSentry Heartbeat Monitor"-Dienst wird zur Überwachung entfernter Hosts und entfernter Ereignisprotokoll-Agenten verwendet.

Fehlersuche & Testen

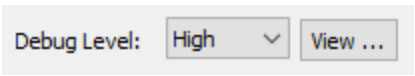
Um zu überprüfen, ob der Dienst korrekt funktioniert, können Sie auf die Schaltfläche *"Test-Ereignisse erstellen"* drücken. Dadurch werden drei Ereignisprotokollaufzeichnungen erstellt, die vom Dienst erkannt werden sollten, solange Sie das Anwendungsprotokoll und die Aufzeichnungen über *Informations-, Warn- oder* Fehlerereignisse überwachen.



Die *Aktuelle Version* zeigt die Version des Dienstes so an, wie sie vom Dienst beim letzten Start gemeldet wurde.

Debug-Logging

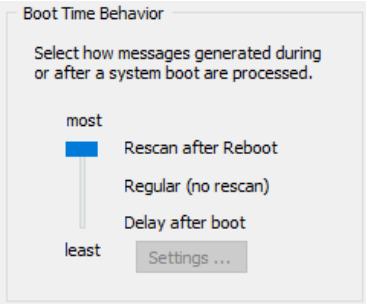
Der EventSentry-Agent schreibt auf Anfrage Statusmeldungen in das Ereignisprotokoll und/oder in eine Protokolldatei `%SYSTEMROOT%\eventsentry\logs\eventsentry_svc_X.log`. Es wird empfohlen, die Stufe "Hoch" zu verwenden, falls Sie Probleme mit dem Dienst haben. Die maximale Groesse der Protokolldateien ist standardmässig 64MB, kann aber über die Registrierung angepasst werden.



5.2 Globale Optionen

Die **Globalen Optionen** sind Einstellungen, die für alle Computer gelten, unabhängig von ihrer Gruppenzugehörigkeit. Die globalen Optionen sind in die Einstellungen "Allgemein" und "Heartbeat" unterteilt, klicken Sie auf die jeweilige Registerkarte, um sie aufzurufen.

Boot-Zeit-Verhalten



EventSentry überwacht das Ereignisprotokoll, wenn es ausgeführt wird. Wenn der Dienst nicht läuft (z. B. wenn das System neu gestartet wird), kann er die Ereignisprotokolle nicht überwachen. Ereignisprotokolleinträge, die erstellt werden, während der Dienst angehalten wird, werden nicht verarbeitet.

Um dieses Problem zu vermeiden, können Sie EventSentry so konfigurieren, dass es nach Ereignissen sucht, die nach dem letzten Beenden des Dienstes erstellt wurden, indem Sie diese Funktion auf "die meisten" setzen. Jedes Mal, wenn der Dienst gestartet wird, scannt er das Ereignisprotokoll vom letzten Kontrollpunkt aus. Diese Funktion ist auch nützlich, um festzustellen, ob ein Server neu gestartet wurde.

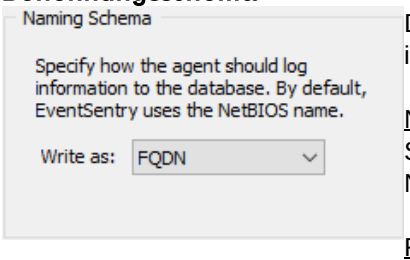
Hoch: EventSentry scannt das Ereignisprotokoll erneut und verarbeitet Ereignisse, die aufgetreten sind, während der Dienst angehalten wurde.

Standard: EventSentry überwacht das Ereignisprotokoll unmittelbar nach dem Start des Dienstes, verarbeitet jedoch keine Ereignisse, die während der Unterbrechung des Dienstes aufgetreten sind.

Minimum: EventSentry ignoriert Ereignisse, die in den ersten X Sekunden nach dem Hochfahren des Betriebssystems aufgetreten sind. Wenn EventSentry Ihnen z.B. viele Ereignisse per E-Mail schickt, wenn ein Server neu gestartet wird, dann können Sie diese Funktion so konfigurieren, dass Ereignisse für eine bestimmte Anzahl von Sekunden unterdrückt werden. Klicken Sie auf die Schaltfläche "Einstellungen", um das Dialogfeld "Boot-Verzögerungseinstellungen" aufzurufen, in dem Sie das Intervall und die Aktionstypen konfigurieren können, für die diese Funktion gilt.

Hinweis: Bei SMTP-E-Mails, die von einem Boot-Scan gesendet werden, wird "**[RESCAN]**" an den Betreff angehängt.

Benennungsschema



Diese Option steuert, wie Hosts sich in den Web Reports identifizieren.

NetBIOS
Standardmäßig erscheinen die Computernamen mit ihren NetBIOS-Namen (z.B. SERVER1) in Warnmeldungen und im Web-Reporting.

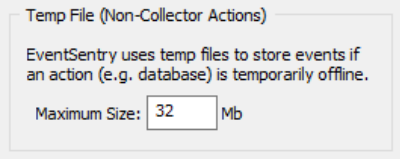
FQDN
Hosts erscheinen mit ihrem jeweiligen FQDN-Namen (z.B. server1.yourdomain.local) statt nur mit dem Hostnamen. Bitte beachten Sie, dass Sie den Agenten neu starten müssen, damit diese Änderung wirksam wird.

Alias

Erzwingt, dass Hosts mit dem in der Verwaltungskonsole definierten Namen anstelle ihres tatsächlichen Hostnamens angezeigt werden. Diese Einstellung erfordert, dass mindestens eine aktive IP-Adresse mit der IP-Adresse übereinstimmt, die für den Hostnamen in einer EventSentry-Gruppe konfiguriert ist. Diese Einstellung ist nützlich für Umgebungen, in denen Hosts mit identischen Namen, aber aus verschiedenen Subnetzen mit derselben EventSentry-Datenbank verbunden sind. Wenn sie konfiguriert ist, wird auch die Variable $HOSTNAMEALIAS unterstützt.

Es wird nicht empfohlen, die FQDN-Option bei der Verwaltung von Computern zu verwenden, die nicht Teil einer Active Directory-Domäne sind, wegen möglicher Probleme bei der Zuordnung von Paketen zu diesen Computern.

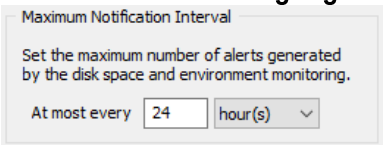
Temp-Datei



Bestimmte Aktionstypen, einschließlich E-Mail, Datenbank und Syslog, haben die Fähigkeit, Ereignisse zwischenzuspeichern, wenn der konfigurierte Server vorübergehend nicht verfügbar ist. Mit dieser Einstellung können Sie den maximalen Festplattenspeicherplatz konfigurieren, den EventSentry im temporären Systemverzeichnis (%TEMP%) für die Zwischenspeicherung von Ereignissen verwendet.

Diese Einstellung gilt auch für den Speicher, der für die summarischen Aktionen verwendet wird.

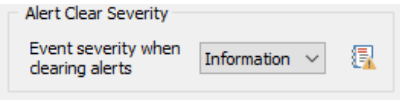
Maximale Benachrichtigungsintervalle



Viele Funktionen, einschließlich Umgebungsüberwachung, Festplattenspeicher- und Dienstüberwachung, schreiben Warnmeldungen in das Ereignisprotokoll, wenn ein bestimmtes Problem (z.B. zu wenig Festplattenspeicher, hohe Umgebungstemperatur usw.) erkannt wird. Um zu vermeiden, dass das Ereignisprotokoll mit demselben Ereignis, das sich auf dasselbe Problem bezieht, überflutet wird, können Sie hier ein maximales Benachrichtigungsintervall festlegen.

Wenn Sie z.B. ein maximales Benachrichtigungsintervall von 24 Stunden festlegen, wird eine Warnung wegen zu wenig Speicherplatz auf Laufwerk C nur einmal alle 24 Stunden protokolliert, bis das Problem mit zu wenig Speicherplatz behoben ist.

Alert Clear Severity



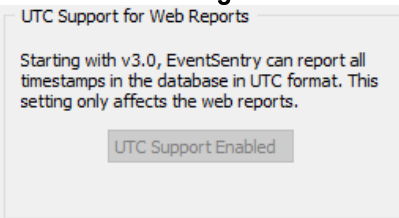
Standardmäßig werden bei der Überwachung von Leistung und Speicherplatz Ereignisse mit demselben Schweregrad protokolliert (wie im Objekt konfiguriert), unabhängig davon, ob ein Problem erkannt oder behoben wurde. Dies ist so, damit die Standard-Ereignisprotokollfilterregeln sowohl Warnungen als auch deren Resolution identisch verarbeiten.

Da beides verwirrend sein kann (ein Problem wird gelöst, aber als "Fehler" protokolliert), setzt diese Einstellung das Standardverhalten

außer Kraft und protokolliert Ereignisse welche die Resolution eines Fehlers protokollieren mit dem ausgewählten Schweregrad.

Diese Einstellung wirkt sich nur auf die Leistungsüberwachung und die Speicherplatzüberwachung aus.

UTC-Unterstützung



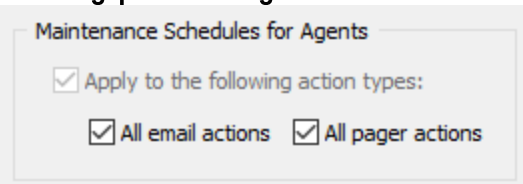
Beginnend mit Version 3.0 kann EventSentry alle Zeitstempel in der UTC-Zeitzone in die Datenbank schreiben. Dies ist hilfreich für Netzwerke, die sich über mehrere Zeitzonen erstrecken, da die Web Reports alle Daten in der lokalen Zeitzone des aktuell angemeldeten Benutzers anzeigen können.

Die UTC-Unterstützung ist für neue Installationen standardmäßig aktiviert und kann auch für Benutzer eingeschaltet werden, die von früheren Installationen upgraden. Einmal aktiviert, kann die UTC-Unterstützung nicht wieder ausgeschaltet werden.

UTC wirkt sich nur auf die Web-Reports aus, die von den Agenten generierten Alerts verwenden z.B. immer noch den Zeitstempel der lokalen Zeitzone, in der sich der Agent befindet.

Lesen Sie KB-Artikel #240, wenn die UTC-Unterstützung nach einem Upgrade von 2.93.1 oder früher aktiviert wird.

Wartungspläne für Agenten

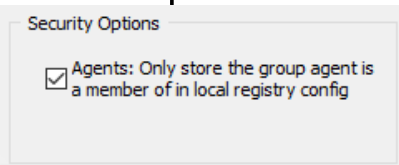


Wenn Wartungspläne für eine Gruppe oder einen Host erstellt werden, gelten sie nur für Heartbeat-Alarme, die vom Heartbeat-Agenten generiert werden; etwaige Alerts (z. B. Ereignisprotokoll-Alarm per E-Mail) werden weiterhin von einem Agenten verschickt.

Um **alle** E-Mail-Benachrichtigungen während eines Wartungsplans zu unterdrücken, aktivieren Sie das Kontrollkästchen "Alle E-Mail-Aktionen"; aktivieren Sie das Kontrollkästchen "Alle Pager-Aktionen", um **alle** Pager-Benachrichtigungen zu unterdrücken.

Beide Kontrollkästchen sind bei Neuinstallationen standardmäßig aktiviert.

Sicherheits-Optionen



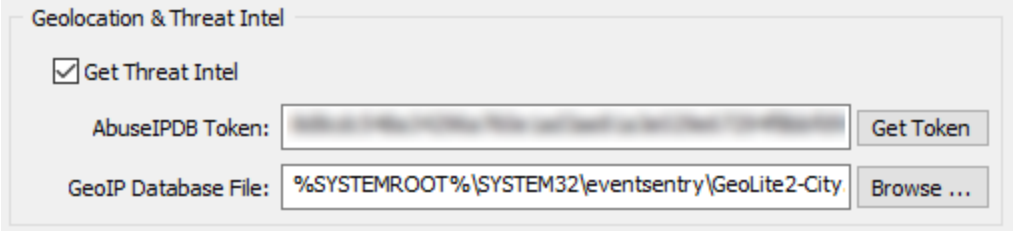
Agenten: speichern Sie in der lokalen Registrierungskonfiguration nur die Gruppe, in der der Agent Mitglied ist.
Standardmäßig erhalten alle Remote-Agenten die vollständige übertragene EventSentry-Konfiguration, einschließlich aller darin enthaltenen Gruppen und Hostnamen. Dies ist in Situationen, in denen dieselbe EventSentry-Konfiguration zur Überwachung disparater & isolierter Netzwerke verwendet wird, wie z.B. in MSP-Umgebungen, unter Umständen nicht wünschenswert. Die Aktivierung

dieser Option stellt sicher, dass ein Remote-Agent nur die Gruppendaten der Gruppe speichert, der er angehört.

Geolokalisierung

EventSentry wird mit einer kostenlosen Geolite-Stadtgeolokalisierungsdatenbank geliefert, die IP-Adressen mit ihrer entsprechenden Geolokalisierung ergänzt. EventSentry enthält diese Datenbank, die mit jedem EventSentry Update aktualisiert wird. Die neueste Version der Datenbank kann auch von http://dev.maxmind.com/geoip/geoip2/geolite2/ heruntergeladen werden. Folgen Sie den nachstehenden Schritten, um die Geodatenbank zu aktualisieren:

1. Klicken Sie in der Verwaltungskonsole auf "Dienste".
2. Beenden Sie den Dienst "Network Services".
3. Beenden Sie den Dienst "Collector", wenn er läuft
4. Ersetzen Sie die GeoIP-Datenbankdatei durch die neueste Version (nur im mmdb-Format!)
5. Starten Sie den "Collector"-Dienst erneut, wenn er lief
6. Starten Sie den Dienst "Network Services".



Bedrohungsintelligenz erhalten

Wenn ein API-Schlüssel konfiguriert ist, dann wird eine schwarze Liste von AbuseIPDB heruntergeladen (zusätzlich zu den drei kostenlosen schwarzen Listen) und ein Bedrohungsstatus jeder IP-Adresse wird ebenfalls in Echtzeit von der AbuseIPDB-Website abgerufen. Weitere Einzelheitenfinden Sie unter Preise von AbuseIPDB, ein kostenloser Dienst mit begrenzten Überprüfungen ist verfügbar (1000 Abfragen/Tag, Stand November 2020).

Benutzerdefinierte Schwarze Liste: Um Sperrlisten von Drittanbietern einzubinden, speichern Sie die gesperrten IPs im folgenden Format in der Datei **%SYSTEMROOT%\system32\eventsentry\temp\eventsentry_threatintel_custom.tmp**. Diese Datei wird, wenn sie vorhanden ist, bei jedem Download der anderen Blacklists importiert:

```
IP;Confidence Score;Titel
```

IP: IP-Adresse
Confidence-Score (optional): Zahl 0..100
Titel (optional): Titel oder Beschreibung der Bedrohung

Beispiel:

```
10.20.30.40;60;Port-Scan
10.20.80.22;90;Web-Angriff,Port-Scan,Spam
```

Optionale Felder können weggelassen werden: "Confidence Score" ist standardmäßig auf 50 gesetzt, wenn nicht vorhanden, "Titel" ist auf "n/a" gesetzt, wenn nicht vorhanden. Es muss mindestens eine IP-Adresse pro Zeile angegeben werden.

Der Bedrohungsintelligenzstatus kann in Ereignisprotokollfiltern und in den Webberichten verwendet werden, um Berichte auf der Grundlage des Bedrohungsstatus einer IP-Adresse zu filtern.

Heartbeat-Einstellungen

Weitere Informationen zu den allgemeinen Heartbeat-Einstellungen finden Sie unter "Allgemeine Optionen einstellen" im Kapitel Netzwerküberwachung.

5.3 Ereignisprotokoll

Ein Ereignisprotokollpaket wird verwendet, um einen oder mehrere Filter (in der Regel mehr als einen) zu einer logischen Einheit zu gruppieren, die dann einem oder mehreren Computern oder Gruppen zugeordnet werden kann. Filter sind Regeln, die festlegen, welche Ereignisse an welche Benachrichtigung weitergeleitet werden.

Optionen des Ereignisprotokoll-Pakets

Zusätzlich zu den allgemeinen Paketoptionen können Ereignisprotokollpakete

- als "Catch-All Notification"-Pakete konfiguriert werden
- so konfiguriert, dass Ausschlussfilter aus anderen Paketen ignoriert werden
- ausgelöst werden, um aktiviert zu werden, wenn ein bestimmter Dienst installiert wird

Siehe Paketoptionen für weitere Informationen.

Eingebaute Ereignisprotokoll-Pakete

NETIKUS.NET verwaltet eine Reihe von Ereignisprotokollpaketen, die gemeinsame Filterregeln enthalten. Diese Ereignisprotokollpakete werden automatisch mit EventSentry installiert und können automatisch über das Internet aktualisiert werden. Weitere Informationen finden Sie unter Herunterladen von Paketen.

Filter

Ereignisprotokollpakete enthalten einen oder mehrere Filter und Ordner. Sie können sich z.B. bestimmte Fehler aus dem Ereignisprotokoll der Anwendung per E-Mail zusenden lassen, bestimmte Ereignisse im Systemprotokoll auslagern und dennoch alle Ereignisse (unabhängig von ihren Eigenschaften) an eine Datenbank weiterleiten. Sie können auch Schwellenwerte auf Filter anwenden (z.B. um Ereignisprotokolleinträge zu erkennen, die mindestens X-mal während eines bestimmten Zeitraums auftreten) und wiederkehrende Filter erstellen, die Sie warnen, wenn ein bestimmtes Ereignis nicht aufgetreten ist. Siehe Filter für weitere Informationen.

Hinzufügen von vordefinierten Ereignisprotokollfiltern

Filter können schnell aus der EventSentry-KB oder den HowTo-Artikeln hinzugefügt werden, indem man ihre JSON-Syntax in die Zwischenablage kopiert und dann im Ribbon auf PASTE klickt.

Anwenden von Ereignisprotokollpaketen

Um ein Ereignisprotokollpaket anzuwenden, klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie "Zuweisen". Wählen Sie im daraufhin angezeigten Dialogfeld eine Gruppe oder einen Computer aus, auf den das Paket angewendet werden soll.

Erstellen und Löschen von Ereignisprotokollpaketen

Um ein neues Filterpaket zu erstellen, klicken Sie mit der rechten Maustaste auf den Container **Event Log Packages** und wählen Sie **Add Package** oder klicken Sie mit der rechten Maustaste auf ein Paket und wählen Sie **Add**.

Um ein Paket zu löschen, klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie Löschen. Alle im Ereignisprotokollpaket enthaltenen Filter werden ebenfalls gelöscht.

5.3.1 Optionen des Ereignisprotokoll-Pakets

Ereignisprotokollpakete bieten zusätzlich zu den allgemeinen Paketoptionen weitere Optionen.

Catch-All-Benachrichtigungspaket
Es wird empfohlen, diese Funktion bei Paketen zu aktivieren, die "Catch-all"-Filter enthalten.

Catch-All-Filter
Wir sprechen von "Catch-All"-Filtern, wenn Sie einen **Include-Filter** haben, der alle Ereignisse, zum Beispiel alle **Fehler** und **Warnungen**, an eine Aktion weiterleitet. Beispiele für Catch-All-Filter sind:

- Ein Filter, der alle Warnungen, Fehler und Audit-Fehler an einen E-Mail-Empfänger weiterleitet
- Ein Filter, der alle Audit-Erfolgs- und Audit-Fehler-Ereignisse an eine Datenbank weiterleitet

Da Ereignisprotokolle sehr viel Rauschen erzeugen, enthalten Konfigurationen mit Catch-All-Filtern in der Regel auch viele **Ausschluss-** und Schwellenwertfilter, damit keine unnötigen Warnungen an den E-Mail-Empfänger gesendet werden.

Wenn Sie ein Paket, das einen Catch-All-Filter enthält, nicht als "Catch-All-Benachrichtigungspaket" konfigurieren, funktionieren Filter mit Schwellenwerten aus anderen Paketen möglicherweise nicht wie erwartet.

Ereignisprotokollpakete, die auf **Catch-All** gesetzt sind, werden nach Ereignisprotokollpaketen verarbeitet, die nicht auf Catch-All-Pakete gesetzt sind. Dadurch wird sichergestellt, dass Include-Filter mit erweiterten Funktionen wie Schwellenwerten vor Filtern in einem Catch-All-Paket verarbeitet werden.

Filter-Verkettung
Die Filterverkettung wird auf Paketebene aktiviert und bietet eine einfache, einam Arbeitsablauf ähnliche Funktionalität. Wenn aktiviert, wird ein Ereignis (das mit einer Aktion verknüpft werden kann) erzeugt, wenn EventSentry **alle Filter im Paket** in einem konfigurierbaren Zeitraum übereinstimmen.

Ausschlussfilter aus anderen Paketen ignorieren
Ausschlussfilter aus allen Paketen werden standardmäßig immer verarbeitet, bevor eine Benachrichtigung versendet wird. Das heißt, es spielt keine Rolle, in welchem Paket ein Ausschlussfilter enthalten ist - er wird immer angewendet.

Wenn Sie Filter haben, für die Sie sicherstellen möchten, dass sie nicht durch Ausschlussfilter aus anderen Paketen ausgeschlossen werden, dann können Sie sie zu einem neuen Paket hinzufügen und das Paket so konfigurieren, dass Ausschlussfilter aus anderen Paketen ignoriert werden.

5.3.1.1 Filter-Verkettung

Die Filterverkettung ermöglicht es, eine Aktion auszulösen, wenn zwei oder mehr Ereignisse innerhalb eines konfigurierbaren Zeitraums auf demselben Host auftreten. Alle Include-Filter, die Teil des Pakets

sind, nehmen an der Filterverkettung teil. Wenn alle Filter übereinstimmen, protokolliert der EventSentry-Agent das Ereignis 10650 mit relevanten Details im Ereignisprotokoll.

Den Ereignisprotokollfiltern in einem Filterverkettungspaket sind keine Aktionen zugeordnet; folglich muss ein separater Ereignisprotokollfilter (in einem anderen Paket) erstellt werden, um eine Aktion auszulösen.

Erforderliche Sequenz

Standardmäßig können Filter Ereignisse in beliebiger Reihenfolge zuordnen, um die Filterkette zu vervollständigen. Die Aktivierung der Option "Require Sequence" erfordert, dass die Ereignisse mit den Filtern in derselben Reihenfolge übereinstimmen, wie sie im Ereignisprotokollpaket angezeigt wird.

Bei der Verwendung einer Sequenz empfiehlt es sich, entweder keine Ausschlussfilter im Paket zu haben oder Ausschlussfilter UNTER allen Einschlussfiltern zu positionieren. Andernfalls ist das Verhalten der Filterverkettungsfunktion undefiniert.

Auszeit

Der Zeitraum, in dem **alle Filter** des Ereignisprotokollpakets mit einem Ereignis übereinstimmen müssen.

Verknüpfung von Ereignissen durch Einfügungszeichenketten

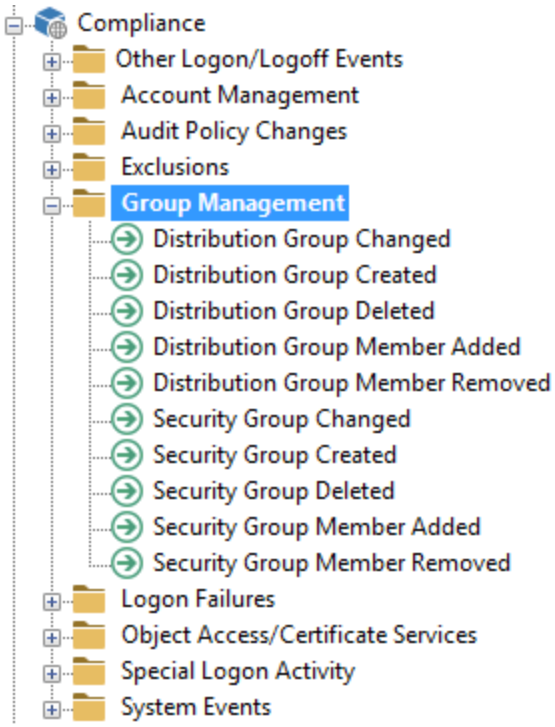
Um sicherzustellen, dass Ereignisse aus nicht zusammenhängenden Aktivitäten nicht dasselbe Filterverkettungsobjekt vervollständigen, können die Filter eines Filterverkettungspakets so eingestellt werden, dass eine oder mehrere Einfügungstexte übereinstimmen müssen. Eine ähnliche Funktionalität steht auch für Schwellenwertfilter zur Verfügung.

Einfügungstexte werden über die Schaltfläche "Ketteneinstellungen" konfiguriert, die im Filterdialog anstelle der Schaltfläche "Erweitert" angezeigt wird. Wenn **in zwei oder mehr** Filtern mindestens ein Einfügetext konfiguriert ist, extrahiert EventSentry den Laufzeitwert der Einfügetexte aus dem Ereignis und speichert sie für die Dauer der Filterverkettung.

Die Werte der extrahierten Einfügetexte müssen für alle Filter übereinstimmen, die mindestens einen Einfügetext konfiguriert haben. Nicht alle Filter im Paket müssen einen Einfügetext konfiguriert haben. Diese Filter werden immer als Übereinstimmung betrachtet, solange sie die Filterkriterien erfüllen.

5.3.2 Filter

Filter sind ein integraler Bestandteil von EventSentry und ermöglichen es Ihnen, Regeln dafür zu erstellen, welche Ereignisse an welche Benachrichtigungen weitergeleitet werden. Die einfachste EventSentry-Konfiguration würde zum Beispiel aus einem einzigen Filter bestehen, der alle Ereignisse von allen Protokollen in eine Datenbank schreibt.



Liste der Filter im Ereignisprotokoll-Paket "Compliance".

Filter-Verarbeitung

Da Exclude-Filter immer immer vor Include-Filtern verarbeitet werden spielt es keine Rolle, ob sich ein Ausschlussfilter vor oder nach einem Einschlussfilter - oder in einem anderen Paket befinden.

Include-Filter innerhalb eines Pakets werden weiterhin sequentiell verarbeitet - von oben nach unten. Die Reihenfolge der Include-Filter ist jedoch in den meisten Szenarien irrelevant, es sei denn, Sie verwenden erweiterte Funktionen wie Schwellenwerte und "Bestätigung erforderlich".

Die einzige Ausnahme sind "Catch-All"-Pakete und Pakete, die so konfiguriert sind, dass sie Ausschlussfilter aus anderen Paketen ignorieren, siehe Paketoptionen für weitere Informationen.

Filter-Typen

Ein Filter kann entweder ein Include-Filter sein (und Ereignisse an eine Benachrichtigung weiterleiten) oder ein Exclude-Filter (und verhindern, dass Ereignisse an eine Benachrichtigung weitergeleitet werden):

Exclude Filter ("Ausschlussfilter")
Ausschlussfilter verhindern, dass bestimmte Ereignisse verarbeitet werden, und können entweder auf alle Aktionen oder nur auf eine bestimmte Aktion angewendet werden. Dies gibt Ihnen die Möglichkeit, Ereignisse nur für einige Aktionen (z.B. E-Mail) auszuschließen, während alles für eine andere Aktion protokolliert wird (Ereignisprotokoll-Konsolidierung). Ausschlussfilter werden **immer** vor Einschlussfiltern verarbeitet.

Es spielt keine Rolle, in welches Ereignisprotokollpaket ein Ausschlussfilter platziert wird, Ausschlussfilter werden immer ausgewertet, bevor Einschlussfilter verarbeitet werden. Die einzige Ausnahme sind Ereignisprotokollpakete, die so konfiguriert sind, dass Ausschlussfilter aus anderen Paketen ignoriert werden.

Ausschlussfilter werden in der Filterliste mit einer roten Schaltfläche "Entfernen" angezeigt .

Include Filter ("Inklusionsfilter")
Verarbeitet Ereignisse die ihren Filterkriterien entsprechen, und leiten diese an die konfigurierte Aktion (oder alle Aktionen) weiter. Je mehr Felder Sie in einem Filter einschränken (z.B. Quelle, Kategorie, ID ...), desto weniger Ereignisse werden diesem Filter entsprechen.

Sie können auch Schwellenwerteinstellungen auf Include-Filter anwenden oder Include-Filter als Zusammenfassungsbenachrichtigungsfilter konfigurieren.

Einschlussfilter sind in der Filterliste mit einem blauen Pfeil gekennzeichnet  .

Filter für wiederkehrende Ereignisse
Filter für wiederkehrende Ereignisse erscheinen wie reguläre Include-Filter, leiten Ereignisse jedoch nicht wirklich an eine Benachrichtigung weiter. Stattdessen schreiben wiederkehrende Ereignisfilter einen **Fehler** in das Anwendungsereignisprotokoll, wenn ein Ereignis während einer bestimmten Zeitspanne nicht im Ereignisprotokoll **erscheint**. Beispielsweise kann ein Filter für wiederkehrende Ereignisse Sie benachrichtigen, wenn ein Sicherungsauftrag kein Erfolgsereignis in das Ereignisprotokoll geschrieben hat. Weitere Informationen finden Sie unter Filter für wiederkehrende Ereignisse.

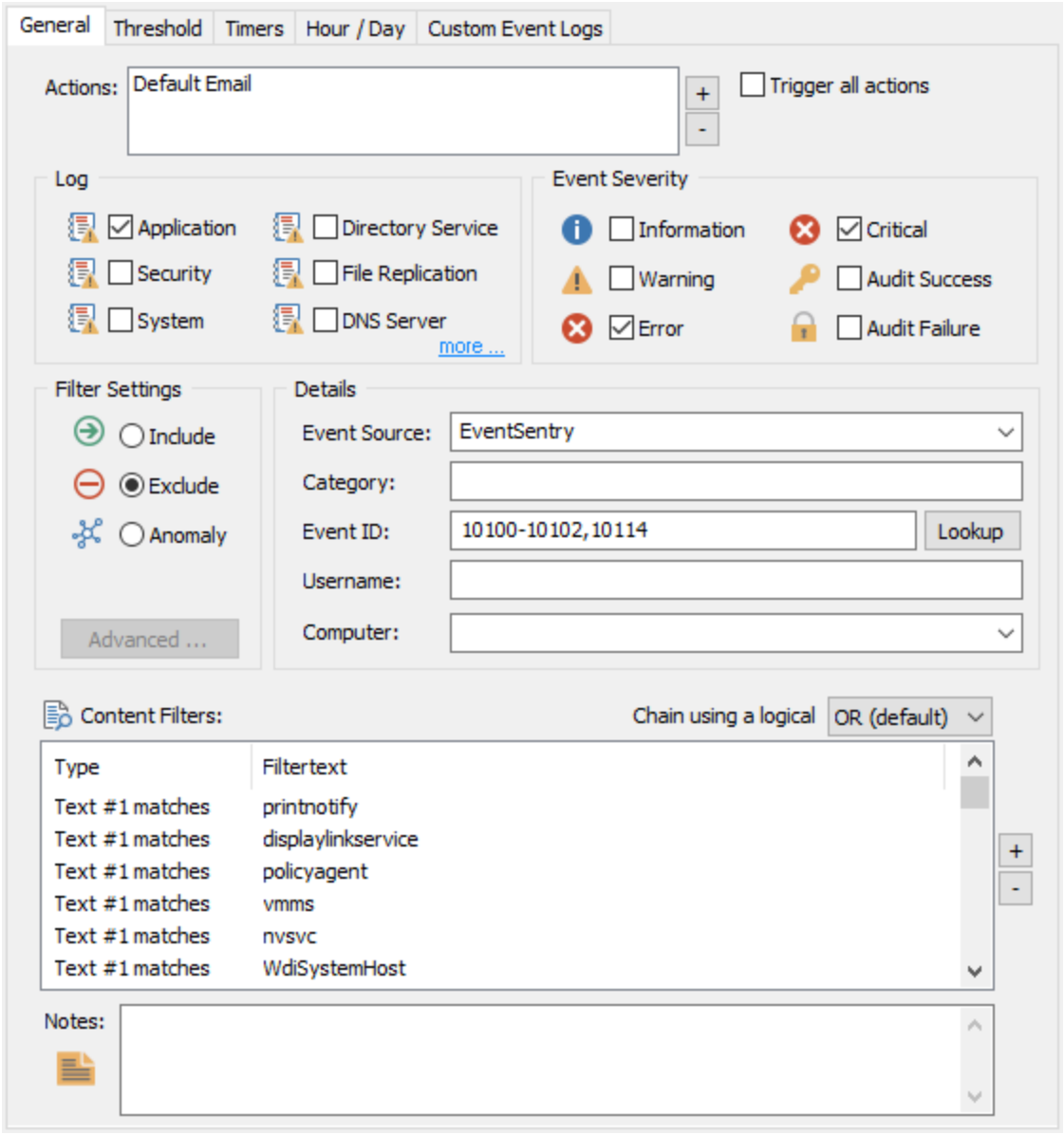
Filter-Eigenschaften

Sie können Ereignisse auf der Grundlage jeder Eigenschaft eines Ereignisprotokolls filtern, einschließlich

- Ereignisprotokoll (einschließlich benutzerdefinierter Ereignisprotokolle)
- Ereignis-Schweregrad
- Ereignis-Quelle
- Ereignis-Kategorie
- Ereignis-ID
- Ereignis Benutzer
- Ereignis-Computer
- Beschreibung der Veranstaltung
- Tag/Stunde

Weitere Informationen finden Sie unter Filtereigenschaften. Sie können auch Ereigniseigenschaften aus einer von EventSentry gesendeten E-Mail oder einem von der Windows-Ereignisanzeige kopierten Ereignis in den allgemeinen Filterdialog einfügen.

5.3.2.1 Filtereigenschaften



Alle Felder im Abschnitt **"Details" unterscheiden nicht zwischen Groß- und Kleinschreibung** und unterstützen Platzhalter, Negation und mehrere durch Kommata getrennte Werte. Weitere Informationen finden Sie unter Erweiterte Textverarbeitung.

Einfügen von Ereigniseigenschaften

Wenn Sie einen Filter auf der Grundlage eines Ereignisses erstellen, das Sie aus der Windows-Ereignisanzeige in die Zwischenablage kopiert oder **per E-Mail** erhalten haben, dann können Sie die wichtigsten Ereigniseigenschaften (Ereignisprotokoll, Ereignisschweregrad, Ereignisquelle, Kategorie, Ereignis-ID und Benutzername) automatisch in den Dialog einfügen, indem Sie auf ein beliebiges Feld klicken und STRG+V drücken.

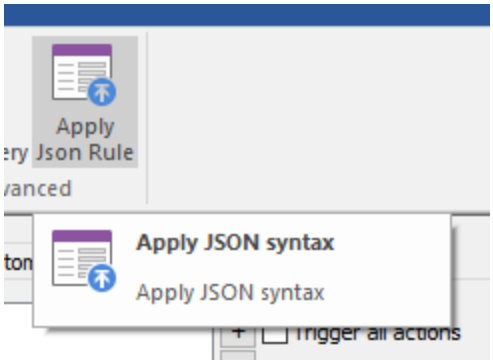
Per E-Mail: Öffnen Sie die E-Mail in Ihrem E-Mail-Client und wählen Sie das Ereignis aus. Wenn die E-Mail nur ein Ereignis enthält, sollten Sie einfach STRG+A drücken können, andernfalls wählen Sie das Ereignis aus. Wenn die E-Mail mehrere Ereignisse enthält und Sie alle auswählen, wird nur das erste Ereignis verwendet. Wenn das Ereignis ausgewählt wurde, kopieren Sie es durch Drücken von STRG+C in die Zwischenablage.

Über die Windows Ereignisanzeige: Öffnen Sie das betreffende Ereignis und klicken Sie im Dialog auf die Schaltfläche **Kopieren**.

Wechseln Sie dann zur Verwaltungskonsole und erstellen Sie entweder einen neuen Filter oder öffnen Sie einen vorhandenen Filter. Klicken Sie auf ein beliebiges Feld (z.B. Kategorie) und klicken Sie **CTRL+V**. Alle wichtigen Ereigniseigenschaften mit Ausnahme der Ereignismeldung sollten nun ausgefüllt sein. Nach dem Einfügen der Schlüsseleigenschaften des Ereignisses können Sie den Filter weiter anpassen, indem Sie zwischen einem Include oder Exclue Filter wählen.

Achtung: Bitte beachten Sie, dass das Klicken mit der rechten Maustaste und die Auswahl von "Einfügen" mit dieser Funktion nicht funktioniert, Sie müssen auf STRG+V klicken. Wenn Sie also nur Text in ein Feld in diesem Dialogfeld einfügen möchten, klicken Sie mit der rechten Maustaste auf das Feld und wählen Sie "Einfügen".

Über JSON-Syntax: Kopieren Sie die gesamte JSON-Syntax in die Zwischenablage und klicken Sie im Ribbon auf die Schaltfläche "Apply Json Jule". Sie können die JSON-Syntax auch einfügen, indem Sie ein beliebiges Event Log Package auswählen und auf die Schaltfläche PASTE im Menüband klicken.



Detaillierte Feldbeschreibungen:

Name

Der Filtername wird von Ihnen gewählt und kann ein beliebiger Text mit maximal 128 Zeichen sein. Filternamen müssen eindeutig sein. Der Filtername darf keinen Backslash (\) enthalten.

Aktionen

Alle Aktionen, die benachrichtigt werden sollen (Filter einschließen) oder nicht benachrichtigt werden sollen (Filter ausschließen), wenn dieser Filter zutrifft.

Alle Aktionen auslösen

Markieren Sie dieses Kontrollkästchen, um alle konfigurierten Aktionen anstelle der ausgewählten Aktionen zu benachrichtigen.

Ereignis-Schweregrad

Wählen Sie aus, welchen Ereignistypen dieser Filter entsprechen soll. "Überwachung erfolgreich" und "Überwachung gescheitert" sind nur relevant, wenn Sie auch das **Sicherheitsereignisprotokoll** überwachen.

Protokoll
Wählen Sie aus, welche(s) Ereignisprotokoll(e) dieser Filter überwachen soll. Die Ereignisprotokolle "Verzeichnisdienst" und "Dateireplikation (Dienst)" sind nur auf Domänencontrollern mit Windows 2000 (und höher) nützlich. Die Ereignisprotokolle "DNS-Server" sind nur auf Windows 2000-Servern (und höher) nützlich, wenn ein DNS-Server installiert ist.

Ereignis-Quelle
Geben Sie an, welcher Quelle dieser Filter entsprechen soll. Wenn Sie keine Ereignisquelle angeben, wird der Filter mit **jeder beliebigen** Quelle übereinstimmen.

Ereignis-Kategorie
Geben Sie an, welcher Kategorie dieser Filter entsprechen soll. Wenn Sie keine Ereigniskategorie angeben, passt der Filter auf **jede beliebige** Kategorie.

Ereignis-ID
Geben Sie an, welcher Ereignis-ID dieser Filter entsprechen soll. Sie können mehrere Ereignis-IDs durch ein Komma trennen, zum Beispiel "3,5,118". Ereignisbereiche (z.B. 4000-500) und Negation (z.B. !4624) werden ebenfalls unterstützt.

Ereignis-IDs sind **nur innerhalb einer Ereignisquelle eindeutig.** Geben Sie daher immer eine Ereignisquelle an, wenn Sie eine Ereignis-ID angeben. Andernfalls kann es vorkommen, dass ein Filter auf andere Ereignisse trifft, die er nie zuordnen sollte.

Benutzername
Geben Sie an, welchem Benutzernamen dieser Filter entsprechen soll. Dies ist derzeit nur für das Sicherheitsereignisprotokoll relevant. Benutzernamen werden vom Betriebssystem in der Form **DOMAIN\Benutzername** protokolliert.

Computer
Geben Sie an, welchem Computer dieser Filter entsprechen soll. Wenn Sie keinen Computernamen angeben, passt der Filter auf jeden Computer, auf den das Paket angewendet wird.

Wenn FQDN-Namen aktiviert sind, geben Sie den vollqualifizierten Hostnamen an (z. B. mailserver.mydomain.com), andernfalls geben Sie den NetBIOS-Namen an.

Filter-Typ
- Include / Einschließen — Das übereinstimmende Ereignis wird an die angegebene **(n) Aktion(en)** weitergeleitet
- Exclude / Ausschließen — Das übereinstimmende Ereignis wird für die Weiterleitung an die angegebene **(n) Aktion(en)** blockiert (oder keine Aktionen, wenn "Alle Aktionen auslösen" angekreuzt ist)

Fortgeschrittene
Wenn Sie auf Erweitert klicken, wird das Dialogfeld für erweiterte Optionen angezeigt.

Inhaltsfilter

Verwenden Sie den Inhaltsfilter um anstelle oder zusätzlich zu den oben aufgeführten Eigenschaften nach einem bestimmten Text zu filtern. Klicken Sie auf die Schaltfläche **+**, um eine neue Bedingung zur Liste der Inhaltsfilter hinzuzufügen, oder wählen Sie eine Zeichenfolge aus und klicken Sie auf die Schaltfläche **-**, um sie aus der Liste zu entfernen.

Wenn Sie mehrere Inhaltsfilter angeben, dann können Sie diese entweder mit einem logischen **ODER** oder einem logischen **UND** verknüpfen. Inhaltsfilter werden von oben nach unten abgearbeitet.

ODER: Der Inhaltsfilter passt, sobald die erste Bedingung zutrifft.
UND: Der Inhaltsfilter trifft nur zu, wenn **alle** aufgeführten Bedingungen übereinstimmen.

Die Verwendung mehrerer Negationsfilter in Kombination mit einer ODER-Bedingung wird nicht empfohlen, da dies zu unerwarteten Ergebnissen führen kann.

Anmerkungen

Sie können Filter mit persönlichen Beschreibungen versehen, die in Zukunft für Ihre Mitarbeiter oder für Sie selbst nützlich sein könnten.

Tages- und Zeitbeschränkungen

Einzelheiten finden Sie auf der Seite Tag & Stunde.

5.3.2.1.1 Inhaltsfilter

Das Inhaltsfilterfeld ermöglicht es Ihnen, Ereignisse auf der Grundlage Ereignisnachricht zu filtern und zu verarbeiten. Bei der Inhaltsfilterung wird zwischen folgenden Möglichkeiten unterschieden:

- Platzhalter-Übereinstimmung der gesamten Ereignisnachricht (Standard)
- Übereinstimmung der Einfügungstexte
- Regex-Übereinstimmung (Perl-Syntax)

Wildcard-Match

Mit dieser Option wird der angegebene Text mit dem gesamten Ereignisnachrichtentext (auch als Ereignisbeschreibung bezeichnet) abgeglichen. Sie können entweder Platzhalter in Ihrem Inhaltsfilter verwenden oder eine 1:1-Abgleichung angeben.

Übereinstimmung der Einfügungetexte

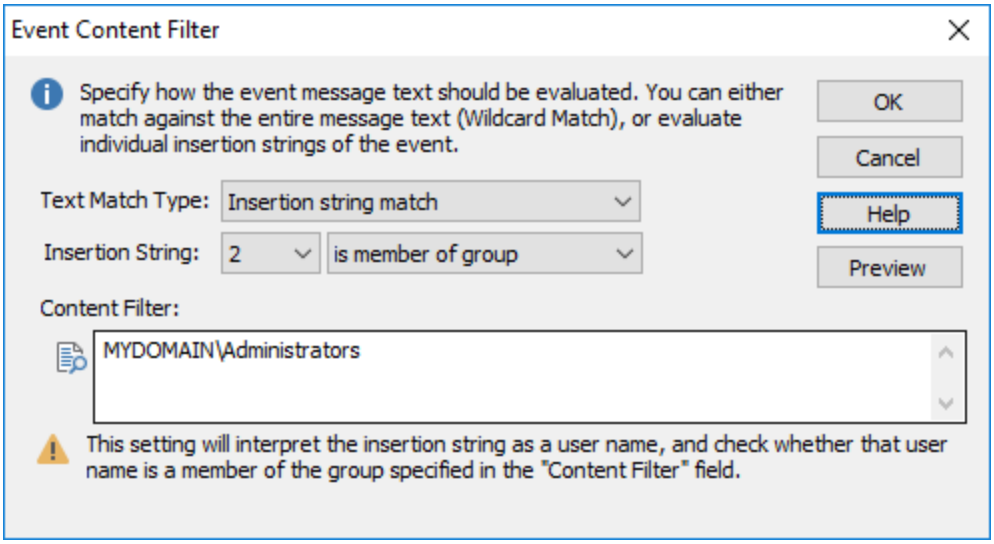
Die meisten Ereignisse, die im Ereignisprotokoll protokolliert werden und dynamische Informationen enthalten, enthalten eine oder mehrere Einfügungetexte (klicken Sie hier für eine detaillierte Diskussion über Ereignisnachrichtendateien und Einfügungetexte). Während ein einfacher Platzhalterabgleich in den meisten Fällen ausreicht, bietet Ihnen der Abgleich von Einfügungetexten die folgenden Vorteile:

1. Es müssen keine komplexen Abfragen erstellt werden, um mit einer Teilmenge der Ereignisnachricht übereinzustimmen
2. Zusätzliche Vergleichstypen (z.B. numerisch) sind für Einfügungszeichenketten verfügbar

Mit der Einfügungetext-Übereinstimmung können Sie nicht nur Textvergleiche von Einfügungetexten durchführen, sondern auch Folgendes:

1. Numerischer Vergleich (weniger als, gleich, nicht gleich, mehr als)
2. Datei-Prüfsummenvergleich
3. Überprüfung der Gruppenmitgliedschaft

Die Verwendung von Einfügungsstring-Variablen (z.B. $STR2) im Feld Inhaltsfilter wird unterstützt und ermöglicht es, Einfügungsstrings zur Laufzeit miteinander zu vergleichen.



1. Numerische Vergleiche
Wenn Sie einen der numerischen Vergleiche für einen Einfügetext auswählen, dann wird der textuelle Einfügetext in eine Zahl konvertiert und dann der ausgewählte numerische Vergleich für diese Zeichenfolge durchgeführt. Der numerische Vergleich unterstützt Fließkommazahlen.

Hinweis: Verwenden Sie diese Option nur, wenn der Einfügetext eine Zahl ist.

2. Datei-Prüfsummenvergleiche
Behandelt einen Einfügetext als Dateiname und erstellt eine SHA-256-Prüfsumme der Datei. Die von Ihnen angegebene Prüfsumme wird dann mit der Prüfsumme der Datei verglichen.

Verwenden Sie diese Optionen 2 und 3 nur, wenn der Einfügetext **auf einen Dateinamen zeigt**. Verwenden Sie diese Option nicht bei Ereignissen, die mit hoher Häufigkeit auftreten, oder bei Einfügetexten, die auf große Dateien verweisen, da die Prüfsummengenerierung einen erheblichen Teil der CPU-Zeit in Anspruch nehmen kann.

3. Datei-Entropie-Vergleiche
Ähnlich wie beim Prüfsummenvergleich wird ein Einfügetext als Dateiname behandelt und die Entropie (Zufälligkeit) einer Datei berechnet. Die Entropie wird als Gleitkommazahl mit einem Bereich von 0 bis 10 zurückgegeben. Je zufälliger eine Datei ist, desto höher ist ihre Entropie. Dies kann zur Erkennung eines Ransomware-Ausbruchs verwendet werden, der eine große Anzahl von Dateien mit einer hohen Entropie erzeugt. In der Praxis haben komprimierte und verschlüsselte Dateien eine hohe Entropie.

Sie können die Entropie einer Datei mit der Option /e des Dienstprogramms "checksum.exe" der EventSentry SysAdmin Tools überprüfen.

4. Überprüfung der Gruppenmitgliedschaft
Interpretiert den Einfügetext als Benutzername und überprüft, ob der Benutzername ein Mitglied der von Ihnen angegebenen Gruppe ist. Um Mehrdeutigkeiten zu vermeiden, wird empfohlen, Gruppennamen mit dem Domänen- oder Hostnamen anzugeben, z. B. **DOMAIN\GroupA** oder **SERVERB\GroupX**.

Verwenden Sie diese Option nur, wenn der Einfügetext auf **einen gültigen Benutzernamen** zeigt. Verwenden Sie diese Option nicht bei Ereignissen, die mit einer hohen Häufigkeit auftreten, da die Gruppenüberprüfung (relativ gesehen) zeitaufwändig sein kann und mehr CPU-Zeit in Anspruch nehmen kann.

5. Überprüfung bösartiger IP-Adressen
Prüft, ob eine IP-Adresse aus einem Ereignisprotokoll-Ereignis in einer der heruntergeladenen Blacklists aufgeführt ist (prüft auch AbuseIPDB, falls konfiguriert). Der Filter passt nur dann, wenn die IP-Adresse als bösartig eingestuft wird. Funktioniert nur bei Collector-aktivierten Aktionen, da die IP-Adressenprüfung auf dem Collector durchgeführt wird. Erfordert, dass Threat Intel aktiviert ist.

6. Wildcard-Vergleich ("Übereinstimmungen")
Ähnlich wie der Platzhalterabgleich, aber diese Option gleicht den ausgewählten Einfügetext mit dem angegebenen Text ab.

7. Befehlszeilenargumente
Zählt die Anzahl der in einer Zeichenkette enthaltenen Befehlszeilenargumente, wobei Anführungszeichen usw. berücksichtigt werden, so dass gefiltert werden kann, ob die Anzahl der Argumente kleiner, gleich oder größer als eine bestimmte Anzahl ist. Dies kann für die Erkennung bestimmter Malware oder anderer Anomalien nützlich sein.

8. Geo IP Länderabgleich
Ermittelt das Land der IP-Adresse um diese dann mit dem Ländercode zu vergleichen. Geben Sie den zweistelligen Ländercode (linke Spalte) an (z. B. AT, IT, US). Funktioniert nur für Collector-aktivierte Aktionen, da die IP-Adressprüfung auf dem Collector (und nicht auf dem Agenten) durchgeführt wird. Erfordert, dass eine GEO-Standort-IP-Datenbank vorhanden und konfiguriert ist (standardmäßig bereitgestellt und aktiviert). Ein Filter kann entweder passen, wenn eine IP mit einem Land übereinstimmt, oder wenn sie nicht mit einem bestimmten Ländercode übereinstimmt.

9. Digitale Signaturprüfung
Interpretiert die Einfügetext als Datei und ermittelt den Status der digitalen Signatur der Datei. Die Bedingung kann entweder zutreffen, wenn eine gültige digitale Signatur vorhanden ist, oder nicht vorhanden sein. Dies kann nützlich sein, um Malware oder potenziell unsichere Software zu erkennen.

10. Mindestens ein Token im Text gefunden (OR)
Ähnlich wie bei einer Wildcard-Übereinstimmung wird geprüft, ob mindestens eines der angegebenen Token (getrennt durch das Pipe **|** Zeichen) in der Einfügezeichenfolge gefunden wird. Bitte beachten Sie, dass Wildcards auch für nicht exakte Übereinstimmungen verwendet werden müssen. Dieser Übereinstimmungstyp kann nützlich sein, wenn er mit anderen Einfügetexten kombiniert wird.

11. Alle im Text gefundenen Token
Ähnlich wie bei einer Wildcard-Übereinstimmung wird geprüft, ob alle angegebenen Zeichen (getrennt durch das Pipezeichen **|**) in der Einfügezeichenfolge gefunden werden. Bitte beachten Sie, dass Wildcards auch für nicht exakte Übereinstimmungen verwendet werden müssen. Diese Art der Übereinstimmung kann nützlich sein, wenn sie mit anderen Einfügetexten kombiniert wird.

12. Dateigrößenvergleich
Behandelt eine Einfügezeichenfolge als Dateinamen und ermittelt die Dateigröße, die dann als Vergleich verwendet werden kann. Dies kann zur Erkennung bestimmter Malware verwendet werden, die die Größe bösartiger ausführbarer Dateien absichtlich aufbläht, um die A/V-Erkennung zu umgehen.

Wenn sowohl eine Ereignisquelle als auch eine Ereignis-ID in den Filtereigenschaften angegeben sind und die Nachrichtendatei korrekt registriert ist, kann die Schaltfläche Vorschau verwendet werden, um die Ereignisvorlage und ihre Einfügezeichenfolgen zu sehen. Der Ereignismeldungs-Browser kann auch die verfügbaren Einfügezeichenfolgen eines Ereignisses anzeigen.

Wenn sowohl eine Ereignisquelle als auch eine Ereignis-ID in den Filtereigenschaften angegeben sind und die Meldungsdatei korrekt registriert ist, kann die Schaltfläche Vorschau verwendet werden, um die Ereignisvorlage und ihren Einfügetext anzuzeigen. Der Ereignisnachrichten-Browser kann auch die verfügbaren Einfügetexte eines Ereignisses anzeigen.

Die folgende Tabelle zeigt die von den einzelnen Vergleichen erwarteten Zeichenfolgentypen:

Übereinstiummngskategorie	**Erwarteter Typ der Zeichenkette in "Content Filter".**
stimmt überein mit ("matches")	beliebiger Zeichenfolge
stimmt mit der Datei-Prüfsumme überein ("matches file checksum")	Dateiname mit vollständigem Pfad
ist Mitglied der Gruppe ("is member of group")	Benutzername
numerisch ("numerical")	beliebige Zahl

Regex-Übereinstimmung (Perl-Syntax)
Unterstützt groß- und kleingeschriebenen Textvergleich basierend auf regulären Ausdrücken. EventSentry verwendet die PCRE-Engine, siehe Reguläre Ausdrücke für die vollständige Syntax.

Die gebräuchlichsten Metazeichen für reguläre Ausdrücke sind

^	stimmt mit dem Anfang der Ereignisnachricht überein
$	stimmt mit dem Ende des Ereignisnachricht überein
.	passt auf beliebige Zeichen
\s	entspricht einem Leerzeichen
\d (\D)	entspricht einer Dezimalziffer (keine Ziffer)
\	das nächste Metazeichen zitieren
[]	Sequenz, z.B. [a-z] entspricht allen Kleinbuchstaben von a-z

Da eine Ereignisnachricht oft aus mehr als einer Zeile besteht, stimmt das Symbol ^ immer mit dem Anfang der Ereignisnachricht überein, auch wenn das Ereignis mehrere Zeilen enthält. Ebenso wird das $-Symbol immer mit dem Ende des gesamten Ereignisnachricht übereinstimmen, und nicht mit dem Ende der ersten Zeile.

Darüber hinaus unterstützen reguläre Ausdrücke die folgenden Quantifikatoren:

*	stimmt 0 oder mehre Male überein
+	stimmt ein oder mehrere Male überein
?	Stimme 1 oder 0 Mal überein
{n}	stimmt n-mal überein
{n,}	mindestens n Übereinstiummungen
{n,m}	mindestens n, aber nicht mehr als m Übereinstimmungen

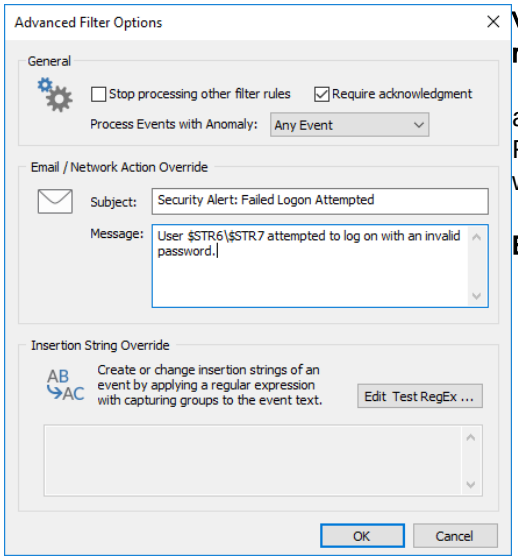
Die folgende Tabelle zeigt grundlegende Beispiele für reguläre Ausdrücke:

Text	Passender regulärer Ausdruck
Opera 11.61 (Opera Software ASA) wurde installiert.	^Opera\s\d\d\d\.\d+.*installiert.$
Computer TEST3-WIN2K8 wurde gebootet.	^.*TEST\d-WIN\dK\d.*$
Benutzer RENAULT\francois3 eingeloggt.	^Benutzer\s[A-Za-z]+\\[A-Za-z0-9]+ eingeloggt.$

Verneinung

Sie können das Negationszeichen (Ausrufezeichen, **!**) für jedes textbasierte Matching verwenden. Weitere Informationen finden Sie unter Erweiterte Textverarbeitung.

5.3.2.1.2 Erweiterte Funktionen



Verarbeitung stoppen / Stop processing other filter rules

Durch Aktivieren dieses Kästchens wird verhindert, dass alle Filter unterhalb dieses Filters im gleichen Paket oder Filter in Paketen unterhalb des aktuellen Pakets verarbeitet werden.

Bestätigung erforderlich / Require Acknowledgment

Bei der Konsolidierung von Ereignissen in einer Datenbank kann man für ausgewählte Ereignisse eine manuelle Bestätigung verlangen. Dies ist normalerweise bei kritischen Ereignissen nützlich, die überprüft und manuell "gelöscht" oder "bestätigt" werden müssen.

Beispielsweise können Sie einen Filter für Ereignisse erstellen, die sich auf ein fehlgeschlagenes Sicherungsereignis beziehen. Wenn ein Backup fehlschlägt, wird dieses Ereignis in den Web Reports als "ausstehende Bestätigung" angezeigt, so dass ein Administrator dokumentieren muss, welche Maßnahmen zur Lösung des Problems ergriffen wurden.

Ereignisse mit Anomalie verarbeiten

Filtert Ereignisse auf der Grundlage ihrer Anomalie-Eigenschaft. Voraussetzung ist, dass mindestens ein Anomalie-Filter eingerichtet ist. Filter können entweder alle Ereignisse unabhängig von ihrer Auffälligkeitseigenschaft verarbeiten oder Ereignisse, die entweder als Auffälligkeit gelten oder nicht.

In der Regel wird ein Filter so eingerichtet, dass er nur Ereignisse verarbeitet, die als Anomalien gelten (z. B. um die Eigenschaft "Bestätigung erforderlich / Require Acknowledgment" festzulegen).

Wenn bei einem Filter, der mit dem Ereignis übereinstimmt, "Bestätigung erforderlich" eingestellt ist, bleibt das Bestätigungsflag erhalten, auch wenn bei anderen übereinstimmenden Filtern diese Einstellung nicht aktiviert ist.

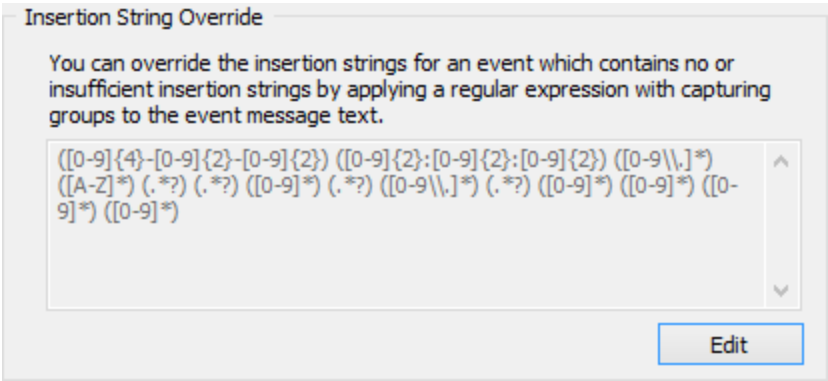
E-Mail / Netzwerk-Aktion überschreibt

Standardmäßig werden alle Ereignisse in der vorliegenden Form weitergeleitet, was für einige Benutzer überwältigend sein kann. Die Funktion "Überschreiben" ermöglicht es dem Benutzer, sowohl das Thema/Titel als auch den Inhalt einer E-Mail oder Netzwerknachricht zu definieren. Der Betreff/Titel oder die Nachricht kann entweder ein statischer Text sein oder beliebige Variablen aus dem Ereignis selbst enthalten (z.B. Einfügetexte oder Ereigniseigenschaften). Das obige Bildschirmfoto zeigt zwei Einfügetexten aus einem 4625-Sicherheitsereignis, das verwendet wird.

Wenn eine E-Mail mehr als ein Ereignis enthält, wird der E-Mail-Nachrichtentext nicht überschrieben und stattdessen auf den "Standard" zurückgesetzt, wo der Inhalt jedes Ereignisses aufgelistet ist.

Einfügungetexte überschreiben

Obwohl die meisten Ereignisse Nachrichten-DLLs ("event message files") verwenden, welche die Fähigkeit unterstützen, Filterregeln auf der Grundlage von Einfügetexten zu erstellen, verwenden einige Ereignisse entweder keine Nachrichtenvorlagen oder enthalten lange dynamische Inhalte, bei denen Einfügetexte nicht hilfreich sind.

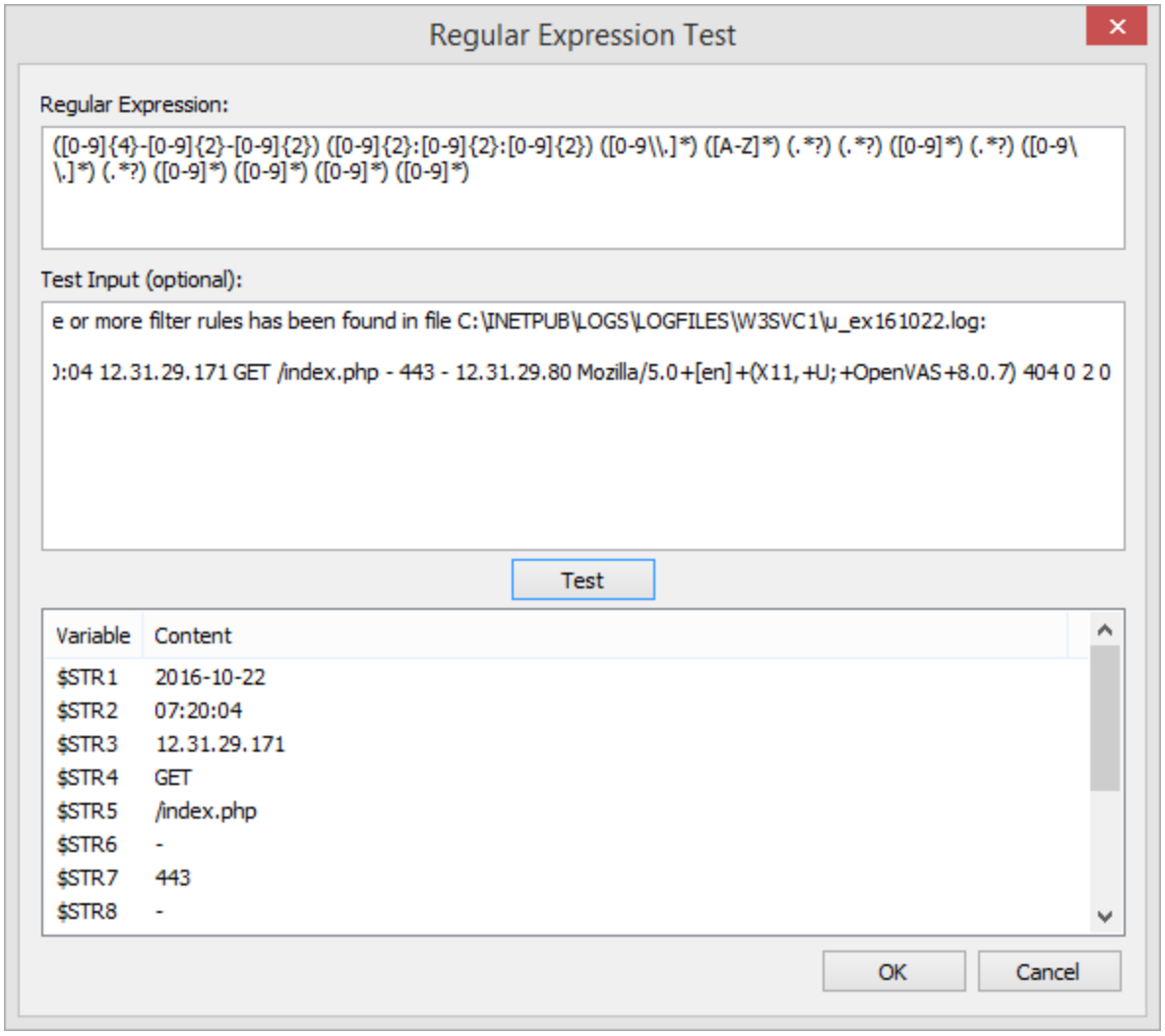


Wenn EventSentry beispielsweise den Inhalt einer Protokolldatei oder einer eingehenden Syslog-Nachricht protokolliert, wird dieser Inhalt einfach in das entsprechende EventSentry-Ereignis injiziert. Wenn der (Logdatei-)Inhalt einem bekannten Muster folgt, kann EventSentry die Einfügetexte des Ereignisses auf der Grundlage eines Musters regulärer Ausdrücke neu definieren. Die ursprünglichen Einfügetexte gehen verloren weil sie überschrieben werden.

	Template	Actual Event	Event after insertion string override
Event	Text matching one or more filter rules has been found in file %1:	Text matching one or more filter rules has been found in file C:\INETPUB\LOGS\LOGFILES\W3SVC1\u_ex161022.log:	Text matching one or more filter rules has been found in file C:\INETPUB\LOGS\LOGFILES\W3SVC1\u_ex161022.log:
Insertion Strings	%2	2016-10-22 07:20:04 12.31.29.171 GET /index.php - 443 - 12.31.29.80 Mozilla/5.0+[en]+(X11,+U; +OpenVAS+8.0.7) 404 0 2 0 $STR1 = C:\INETPUB\LOGS\LOGFILES\W3SVC1\u_ex161022.log	2016-10-22 07:20:04 12.31.29.171 GET /index.php - 443 - 12.31.29.80 Mozilla/5.0+[en]+(X11,+U; +OpenVAS+8.0.7) 404 0 2 0 $STR1 = 2016-10-22 $STR2 = 07:20:04 $STR3 = 12.31.29.171 $STR4 = GET

$STR2 = 2016-10-22 07:20:04 12.31.29.171 GET /index.php - 443 - 12.31.29.80 Mozilla/5.0+[en]+(X11, +U;+OpenVAS+8.0.7) 404 0 2 0

$STR5 = /index.php
$STR6 = -
$STR7 = 443
$STR8 = -
$STR9 = 12.31.29.80
$STR10 = Mozilla/5.0+[en]+(X11,+U; +OpenVAS+8.0.7)
$STR11 = 404
$STR12 = 0
$STR13 = 2
$STR14 = 0



5.3.2.2 Erweiterte Textverarbeitung

Kommagetrennte Werte (nur Ereignisprotokoll-Filter)

Sie können mehrere Werte durch ein Komma trennen, um die Erstellung mehrerer Filter zu vermeiden. Kombinieren Sie einfach alle Werte, mit denen das Feld übereinstimmen soll, mit Kommas und **stellen Sie sicher, dass Sie kein Leerzeichen nach oder vor dem Komma verwenden**. Zum Beispiel:

```
Print,MrxSmb
```

Unterstützt von allen Feldern im Abschnitt "Details".

Negationssymbol (nur Ereignisprotokoll-Filter)

Sie können einen Wert verneinen, indem Sie ihn mit einem Ausrufezeichen voranstellen. Um beispielsweise alle Ereignisse mit Ausnahme der Ereignisse mit der "Print" Source abzugleichen, könnten Sie Folgendes verwenden:

```
!Print
```

or

```
!*Print*
```

Kombinieren Sie keine regulären Werte (Werte ohne das Negationszeichen) und Werte mit einem Negationszeichen (z.B. "!Print,MrxSmb" wird nicht unterstützt).

Wildcards

Die Platzhalter ***** und **?** werden unterstützt.

***** entspricht **null oder mehr** Vorkommnissen **eines beliebigen** Zeichens
? entspricht **einem** Vorkommen **eines beliebigen** Zeichens

Hinweis: Filterzeichenketten, egal ob sie Platzhalter enthalten oder nicht, **sind niemals case-sensitiv**.

Beispiele

Filter mit wildcard	**Stimmt mit Text überein**
ipx*	**IPX**CP
	IPXRIP
	IPXRouterManager
	IPXSAP
*iptables*proto=? ?p*dpt=13*	syslog@netikus-router[kern.debug]: kernel: **IPTABLES** INPUT: IN=ppp0 OUT= MAC= SRC=65.35.223.155 DST=65.41.63.146 LEN=48 TOS=0x00 PREC=0x00 TTL=114 ID=54221 DF **PROTO=**TC**P** SPT=1429 **DPT=13**5 WINDOW=64240 RES=0x00 SYN URGP=0
VMnet*	**VMnet**Adapter
	VMnetBridge
	VMnetDHCP
	VMnetuserif
rip	IP**RIP**2
	IPX**RIP**

5.3.2.3 Filter-Verarbeitung

Die folgenden Regeln sind wichtig, wenn Filter in mehreren Paketen eingerichtet werden.

1. Es werden nur Filter aus globalen oder zugewiesenen Paketen verarbeitet.

2. Eine Meldung wird nie mehr als einmal bearbeitet. Wenn zwei für dieselbe Benachrichtigung konfigurierte Filter mit einem Ereignis übereinstimmen, wird dieses Ereignis trotzdem nur einmal an diese Benachrichtigung weitergeleitet.

3. Ausschlussfilter (Exclude) aus allen Paketen werden **immer** geprüft, bevor ein Ereignis an eine Benachrichtigung weitergeleitet wird. Ausnahme: Ein Ereignisprotokollpaket ist so konfiguriert, dass fremde Ausschlüsse ignoriert werden - in diesem Fall werden nur Ausschlussfilter aus dem gleichen Paket wie der Einschlussfilter geprüft.

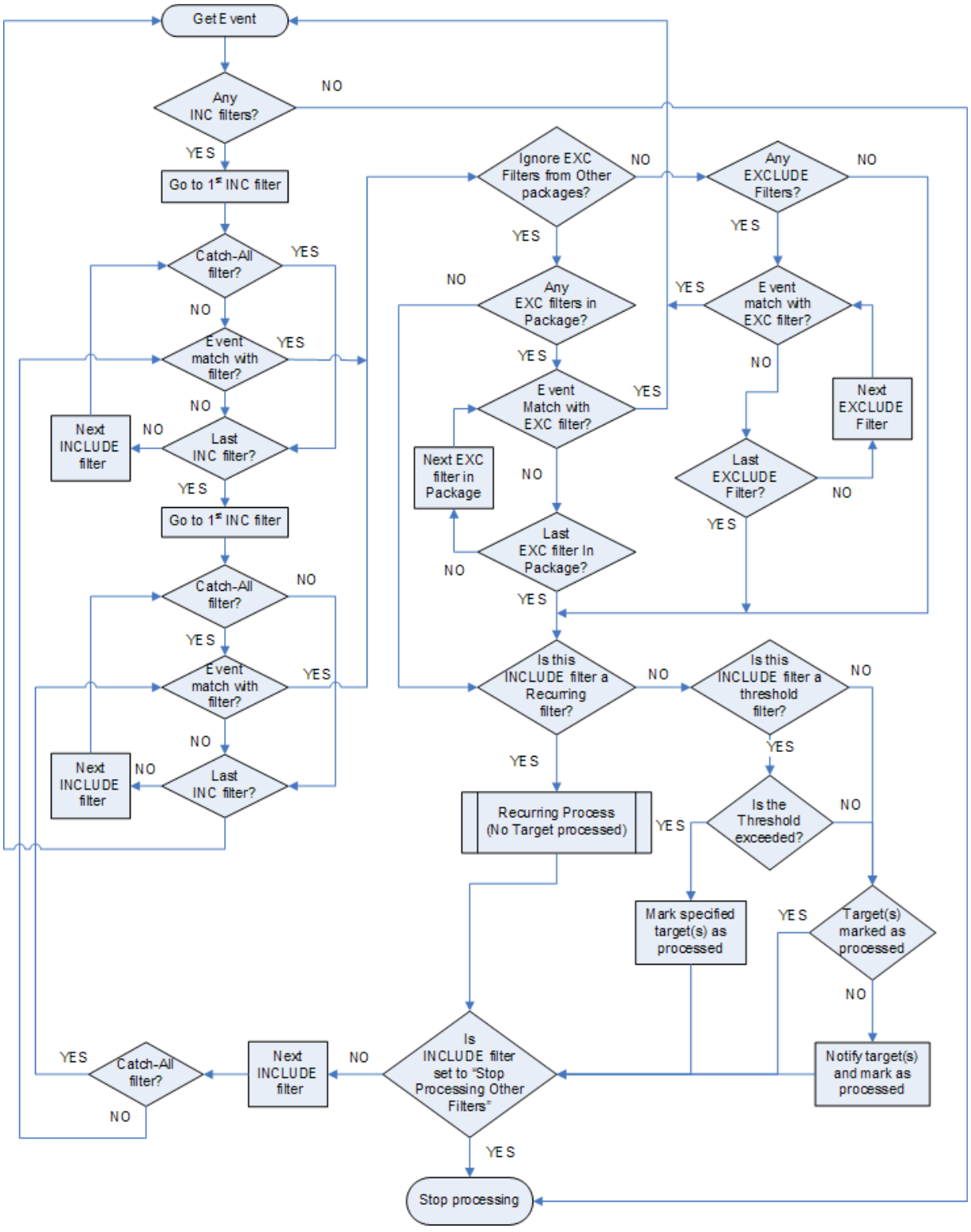
4. Filter aus Catch-All-Paketen werden **immer nach** Filtern aus Non-Catch-All-Paketen verarbeitet.

5. Wenn ein Include-Filter mit einer Schwellenwert-Einstellung auf ein Ereignis passt, dann wird ein nachfolgender passender Filter das Ereignis nicht verarbeiten.

6. Die Pakete werden in der Reihenfolge verarbeitet, wie sie in der Verwaltungsanwendung angezeigt werden, mit Ausnahme der Catch-All-Pakete, die immer nach den regulären Paketen verarbeitet werden.

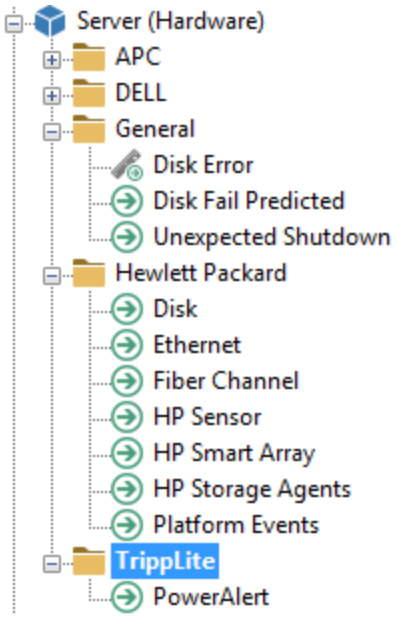
Flussdiagramm

Bitte sehen Sie sich das Flussdiagramm unten an, um zu sehen, wie Filter verarbeitet werden:



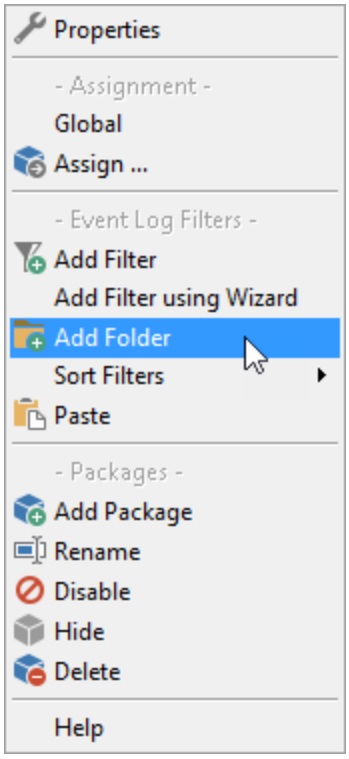
5.3.3 Ordner

Sie können Ordner verwenden, um verwandte Filter in Ordnern zu gruppieren, was nützlich ist um Filter zu organisieren. Derzeit wird eine Ebene von Ordnern unterstützt (es können keine Unterordner von Ordnern erstellt werden).



Ordner erstellen

Sie können einen Ordner erstellen, indem Sie mit der rechten Maustaste auf ein Filter- oder Ereignisprotokollpaket klicken und "Ordner hinzufügen" wählen:



Nachdem der Ordner erstellt wurde, können Sie entweder neue Filter in dem Ordner erstellen, indem Sie mit der rechten Maustaste auf den Ordner klicken und **Filter hinzufügen** wählen, oder indem Sie vorhandene Filter in den Ordner verschieben/kopieren. Ein übliches Szenario für Ordner ist es, Ausschlussfilter (Exclude) in einem Ordner zu gruppieren.

Löschen von Ordnern

Wenn Sie einen Ordner löschen, werden alle Filter innerhalb dieses Ordners ebenfalls gelöscht.

Filter in Ordner verschieben

Sie können vorhandene Filter auf zwei Arten in einen Ordner verschieben:

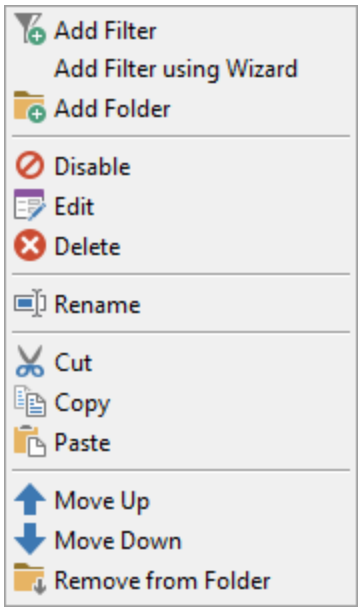
1. Verschieben Sie den Filter auf den Ordner. Der Filter wird unmittelbar nach dem Ordner positioniert, als erster Filter innerhalb des Ordners.
2. Verschieben Sie den Filter auf einen Filter im Ordner. Der Filter wird nach dem Filter positioniert, auf den er gezogen wurde

Filter in Ordnern erstellen

Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie **Filter hinzufügen**. Der Filter wird in dem Ordner erstellt.

Entfernen von Filtern aus Ordnern

Um einen Filter aus einem Ordner zu entfernen, können Sie den Filter entweder außerhalb des Ordners verschieben (z.B. indem Sie ihn auf einen anderen Filter verschieben) oder indem Sie mit der rechten Maustaste auf den Filter klicken und Aus **Ordner entfernen** wählen. Der Filter wird dann außerhalb des Ordners am Ende der Filterliste verschoben.



5.3.4 Bearbeiten von Filtern

Hinzufügen von Filtern

- Klicken Sie mit der rechten Maustaste auf das Ereignisprotokollpaket, zu dem Sie den neuen Filter hinzufügen möchten, und wählen Sie **Filter hinzufügen**
- Klicken Sie mit der rechten Maustaste auf einen vorhandenen Filter und wählen Sie **Hinzufügen**

Sie können dann einen Namen für den neuen Filter eingeben und **die Eingabetaste** drücken. Fahren Sie fort, indem Sie erweiterte Filteroptionen konfigurieren.

Bearbeiten von Filtern

- Klicken Sie mit der linken Maustaste (oder doppelklicken Sie, siehe Benutzerfreundlichkeit) auf das Filterelement im linken Fensterbereich
- Klicken Sie mit der rechten Maustaste auf das Filterobjekt und wählen Sie **Bearbeiten**

Die Filterdetails werden dann in den rechten Fensterbereich geladen und das aktive Filterobjekt im linken Fensterbereich wird fett dargestellt.

Löschen von Filtern

- Klicken Sie mit der rechten Maustaste auf den Filter und wählen Sie **Löschen** aus dem Menü
- Wählen Sie das Filterobjekt aus und drücken Sie die Taste **Entf** auf der Tastatur

Der Filter wird dann gelöscht.

Umbenennen von Filtern

- Klicken Sie mit der rechten Maustaste auf den Filter und wählen Sie **Umbenennen** aus dem Menü
- Wählen Sie den Filter aus und drücken Sie die Taste **F2** auf der Tastatur (funktioniert nur, wenn die Benutzerfreundlichkeit auf Doppelklicken eingestellt ist)
- Klicken Sie mit der linken Maustaste 1-2 Sekunden lang auf das Filterobjekt

Sie können dann einen neuen Namen für den Filter eingeben.

Ausschneiden, Kopieren und Einfügen

1. Klicken Sie auf das Filterobjekt im linken Fensterbereich und vergewissern Sie sich, dass es ausgewählt ist
2. Klicken Sie auf das **Ausschneiden-** oder Kopieren-Symbol in der Symbolleiste oder wählen Sie **Ausschneiden/Kopieren** aus dem Menü **Bearbeiten**
3. Wählen Sie die Position, an der Sie das Filterobjekt einfügen möchten. Dies kann sein

   - eine **Gruppe**, wenn Sie das Filterobjekt in eine neue Gruppe verschieben möchten
   - einen **Filter** in der gleichen **Gruppe**, wenn Sie das Filterobjekt neu ordnen möchten
   - einen **Filter** in einer **anderen Gruppe**, wenn Sie das Filterobjekt in eine andere Gruppe einfügen möchten

4. Klicken Sie auf das Einfügen-Symbol in der Symbolleiste oder wählen Sie **Einfügen** aus dem Menü **Bearbeiten**

Existiert bereits ein Filterobjekt mit dem gleichen Namen, werden automatisch **#1**, **#2** ... etc. an den Namen angehängt.

Filter nach oben/unten verschieben

Um die Reihenfolge eines Filters schnell zu ändern, können Sie einen Filter nach oben oder unten verschieben. Um einen Filter nach oben oder unten zu verschieben, klicken Sie einfach mit der rechten Maustaste auf den Filter und wählen Sie entweder **Move Up** oder **Move Down**.

Filter durch Ziehen und Ablegen

Sie können Filter per Drag & Drop kopieren oder verschieben.

- Um einen Filter zu verschieben, klicken Sie einfach mit der linken Maustaste auf das Filterobjekt und ziehen Sie es an eine andere Position oder in eine andere Gruppe
- Um einen Filter zu kopieren, klicken Sie einfach mit der rechten Maustaste auf das Filterobjekt und ziehen Sie es in eine andere Gruppe (zum Kopieren von Filterobjekten in der gleichen Gruppe verwenden Sie bitte die Funktion Kopieren/Einfügen).

5.3.5 Schwellenwerte

Mit Filterschwellen können Sie nicht nur *dann* Maßnahmen ergreifen, *wenn* ein bestimmtes Ereignis eintritt, sondern auch *in Abhängigkeit davon, wie oft* das Ereignis eintritt. Einige Schwellenwertszenarien:

- benachrichtigt werden, wenn ein Ereignis X-mal innerhalb einer bestimmten Zeitspanne auftritt
- Verhindern, dass Ereignisse eine Aktion überfluten
- Erkennen von lateralen Bewegungen im gesamten Netzwerk (erfordert Collector)
- Erkennen, ob sich Benutzer mehr als X Mal mit einem falschen Passwort anmelden

Die Schwellenwerte werden auf einer Pro-Filter-Basis eingerichtet, und Sie können auf die Schwellenwerteinstellungen zugreifen, indem Sie einen Filter bearbeiten und auf die Registerkarte "**Schwellenwert"** klicken. Setzen Sie einen Schwellenwert entweder auf "Agentenseite" oder "Collectorseite", um die Schwellenwerteinstellungen für einen Filter zu aktivieren. Filter mit Schwellenwerten werden mit einem kleinen Lineal  in der Liste angezeigt.

Schwellenwert-Typ

Agentenseitig
Diese Schwellenwerte werden auf dem Agenten ausgeführt, der einzige Typ von Schwellenwerten, der bis v3.3 unterstützt wurde. Agentenseitige Schwellenwerte sollten immer bevorzugt werden, es sei denn, eine Korrelation von Ereignissen, die auf mehreren Hosts auftreten, ist notwendig. Erforderlich für Filter, die Teil eines Filter-Verkettungspakets sind.

Collector-seitig
Diese Schwellenwerte werden auf dem Collector ausgeführt und erfordern dies:

- ein Collector installiert ist und läuft
- die referenzierte Aktion des Filters verwendet einen Collector
- vor dem Schwellenwert auf dem Collector werden keine agentenseitigen Schwellenwerte verarbeitet
- der Filter nicht Teil eines Filterverkettungspakets ist

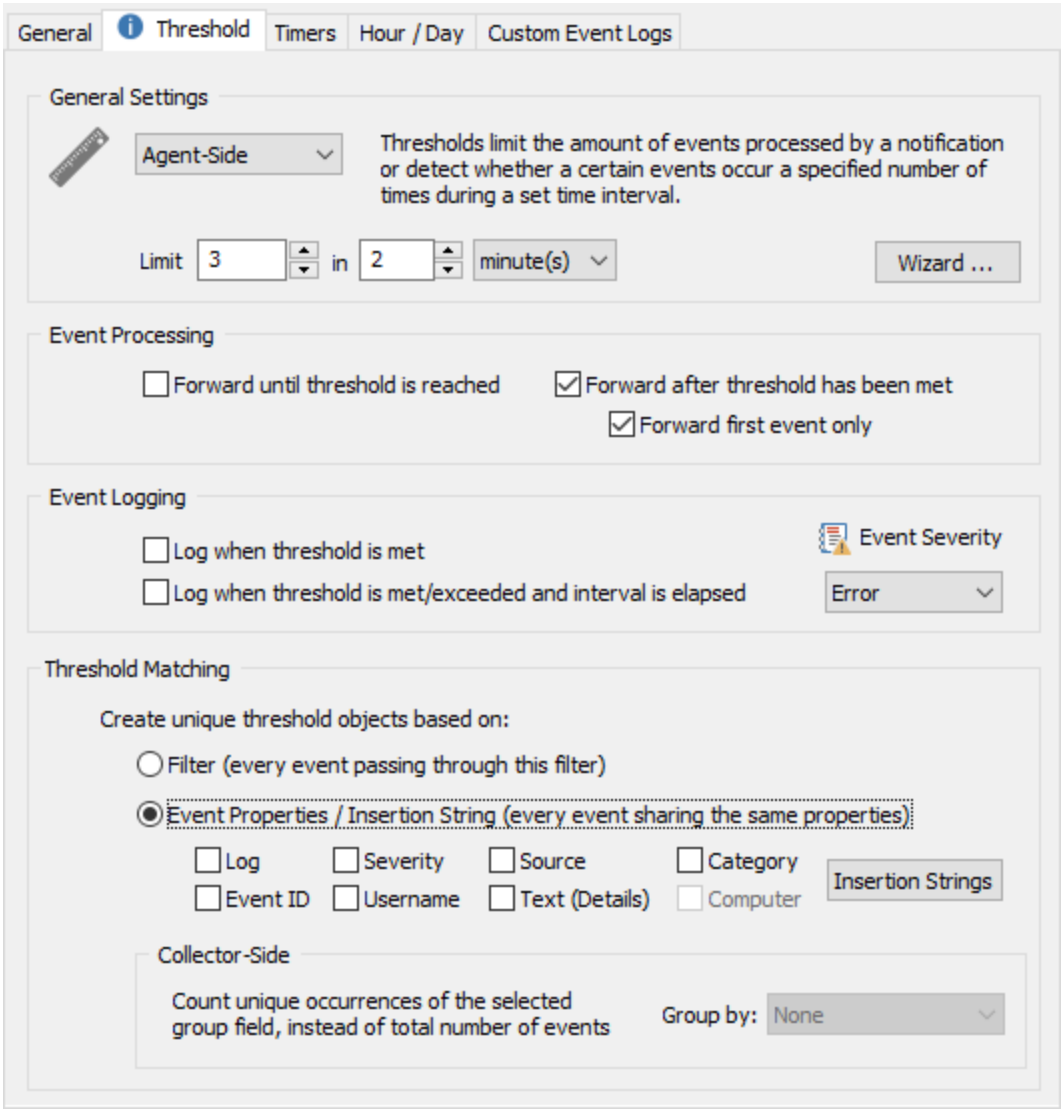
Collectorseitige Schwellenwerte ermöglichen es, Ereignisse von mehreren Hosts zu korrelieren und auszuwerten, um Bedrohungen und Muster zu erkennen, die mehr als einen Host betreffen. So können beispielsweise seitliche Bewegungen durch die Analyse bestimmter Anmeldeereignisse erkannt werden.

Das Ereignis "Computer" und die Optionen "Gruppieren nach" sind nur für collector-seitige Schwellenwerte verfügbar.

Wenn der primäre Zweck eines Collector-Schwellenwerts eher darin besteht, Aktivität zu erkennen als zu unterdrücken (z.B. wenn alle Kontrollkästchen unter "Ereignisverarbeitung" nicht markiert sind), dann wird empfohlen, wenn möglich eine Aktion zuzuordnen, die die

betreffenden Ereignisse bereits verarbeitet (z.B. eine Datenbankaktion), anstatt eine andere Aktion (z.B. E-Mail) zuzuordnen.

Bei häufig auftretenden Ereignissen kann dies das Datenvolumen reduzieren, indem sichergestellt wird, dass Ereignisse nicht zweimal - einmal für jede Aktion - übertragen werden.



Schwellenwert-Intervall

Geben Sie das Schwellenwertintervall an, z.B. 20 Ereignisse in einer Stunde.

Ereignisverarbeitung

Hiermit können Sie konfigurieren, ob Ereignisse vor und/oder nach Erreichen des Schwellenwerts an die konfigurierte Benachrichtigung weitergeleitet werden. Sie können in diesem Abschnitt entweder alle, eines oder keines der Ereignisse markieren.

Ereignisse weiterleiten, bis die Schwelle erreicht ist

Die Markierung dieses Kästchens bedeutet, dass Ereignisse, die Ihrem Filter entsprechen, verarbeitet (und an die Benachrichtigung weitergeleitet) werden, bis der Schwellenwert erreicht ist.

Ereignisse weiterleiten, nach Erreichen der Schwelle
Wenn Sie dieses Kästchen markieren, bedeutet dies, dass Ereignisse, die Ihrem Filter entsprechen, verarbeitet werden, nachdem der Schwellenwert erreicht wurde.

Nur erste Veranstaltung weiterleiten
Sie können einen Schwellenwertfilter so konfigurieren, dass er nur das erste Ereignis weiterleitet, nachdem ein Schwellenwert erreicht wurde, anstatt alle Ereignisse weiterzuleiten, nachdem der Schwellenwert erreicht wurde.
Dies ist besonders nützlich, wenn Sie mit Ereignissen aus dem Sicherheitsprotokoll arbeiten. Wenn Sie einen Schwellenwert für einen Filtertyp mit fehlgeschlagenen Anmeldeversuchen konfigurieren (z.B. Benachrichtigen Sie mich, wenn es mehr als 5 fehlgeschlagene Anmeldeversuche in 5 Minuten gibt), dann werden Sie normalerweise nicht die ersten fehlgeschlagenen Anmeldeversuche erhalten wollen, da Benutzer ständig falsche Passwörter eingeben. Wenn der Schwellenwert jedoch überschritten wird, möchten Sie wahrscheinlich wissen, welcher Benutzer versucht, sich anzumelden. Wenn Sie den Filter nur so konfigurieren, dass er alle Ereignisse nach dem Schwellenwert weiterleitet, dann erhalten Sie für jeden falschen Passwortversuch eine E-Mail, was normalerweise auch nicht erwünscht ist. Stattdessen konfigurieren Sie den Filter so, dass er nur das erste Ereignis nach Überschreiten des Schwellenwertes weiterleitet, und schreiben dann nach Ablauf des Zeitraums ein Ereignis in das Ereignisprotokoll, um anzugeben, wie viele fehlgeschlagene Anmeldeversuche es für dieses Benutzerkonto gegeben hat.

Es ist nicht erlaubt, keines der beiden Kontrollkästchen zu aktivieren, wenn Sie mindestens ein Kontrollkästchen im Abschnitt "Ereignisprotokollierung" aktivieren. In diesem Fall wird der Filter niemals Ereignisse weiterleiten, sondern ein Ereignis in das Ereignisprotokoll schreiben, wenn der Schwellenwert erreicht ist.

Ereignisprotokollierung

Dieser Abschnitt steuert, ob Ereignisse erzeugt und im Ereignisprotokoll der Anwendung protokolliert werden, wenn der Schwellenwert erreicht wird und/oder wenn die Schwellenwertperiode abgeschlossen ist.

Protokoll, wenn der Schwellenwert erreicht ist
Wenn Sie dieses Kästchen markieren, wird ein Ereignis sofort in das Ereignisprotokoll der Anwendung geschrieben, wenn der Filter seinen Schwellenwert erreicht.

Protokoll bei Erreichen/Überschreiten des Schwellenwerts und Ablauf des Intervalls
Diese Option ähnelt der ersten, außer dass diese Funktion ein Ereignis erst dann protokolliert, wenn der Schwellenwert erreicht **und** das Schwellenwertintervall verstrichen ist. Der Vorteil dieser Option besteht darin, dass das vom Schwellenwertfilter protokollierte Ereignis Sie wissen lässt, wie viele Ereignisse von diesem Filter verarbeitet und wie viele fallen gelassen wurden.

Protokollileren als
Geben Sie an, ob Sie Ereignisse als Fehler-, Warn- oder Informationsereignisse protokolliert haben möchten. Weitere Informationen darüber, welche Ereignisse durch diese Funktion im Ereignisprotokoll protokolliert werden, finden Sie unter Ereignisprotokolle.

Schwellenwert-Abgleich

Standardmäßig werden die internen Zähler (die zu den Schwellwertgrenzen zählen) jedes Mal erhöht, wenn ein Ereignis einem Filter entspricht (Filtereinstellung). Obwohl dies in den meisten Fällen wünschenswert ist, können Sie auch Schwellenwertzähler auf Ereignisaufzeichnungen anwenden lassen, was granularere Schwellenwerteinstellungen ermöglicht, aber etwas ressourcenintensiver ist.

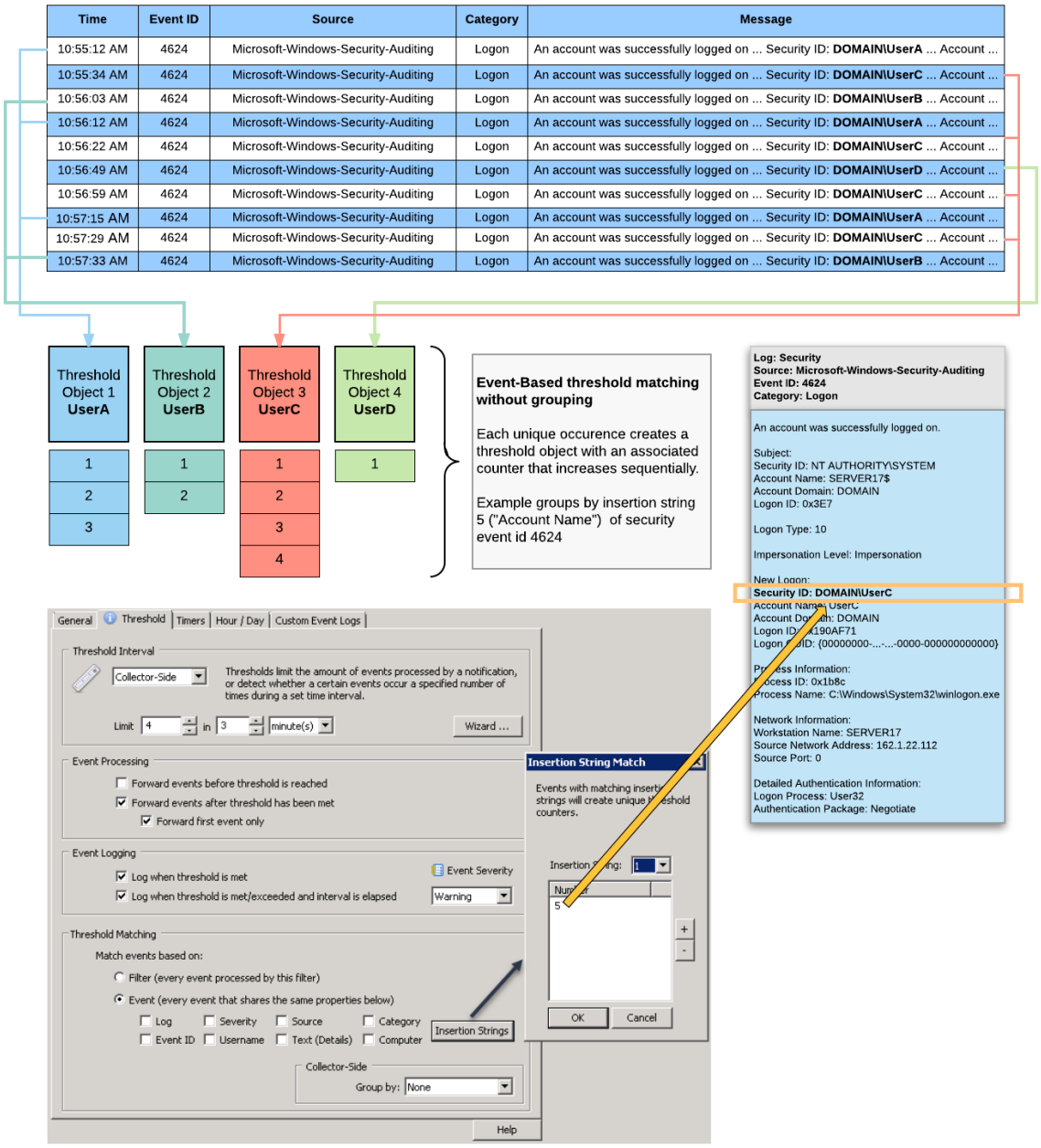
Filter (jedes Ereignis, das von diesem Filter verarbeitet wird)

Jedes Mal, wenn ein Ereignis dem Filter entspricht, werden die internen Schwellenwertzähler erhöht. Dies ist die empfohlene Option für Schwellenwertfilter, die auf Ereignisse angewendet werden, die nicht aus dem Sicherheitsereignisprotokoll stammen.

Ereignis-Eigenschaften / Einfügungs-Strings (jedes Ereignis hat gemeinsame Eigenschaften)
Jedes Ereignis, das die gleichen Werte für die ausgewählten Eigenschaften hat, erhöht die internen Schwellenwertzähler. Diese Funktion ist vor allem bei Ereignissen aus dem Sicherheitsereignisprotokoll nützlich, z.B. zur Analyse fehlgeschlagener Anmeldungen. Anstatt dass jedes Ereignis auf den Schwellenwert angerechnet wird, zählen nur Ereignisse, die bestimmte Ereigniseigenschaften gemeinsam haben, einschließlich Einfügetexten, falls ausgewählt, zum Gesamtzähler.

> ⚠ Das Feld "Computer" ist nur für Schwellenwerte auf der Collector-Seite verfügbar, da die Eigenschaft "Computer" für Schwellenwerte auf der Agent-Seite immer gleich ist.

Das folgende Diagramm veranschaulicht, wie die Anpassung auf der Grundlage von Ereigniseigenschaften und Einfügungetexten funktioniert. In diesem Beispiel verarbeitet ein Filter 4624 Ereignisse und verwendet Einfügungetext 5, welcher die "Sicherheits-ID" darstellt, als eindeutige Kennung. Folglich werden virtuelle Schwellenwertobjekte für jedes eindeutige Auftreten einer angetroffenen Sicherheits-ID erstellt. Wenn dieselbe Sicherheitskennung innerhalb von 3 Minuten 4 Mal auftritt, wird sofort ein Alarm erzeugt - in diesem Beispiel **UserC**. Ein weiterer Alarm wird erzeugt, wenn die Schwellenwertperiode von 3 Minuten verstrichen ist.

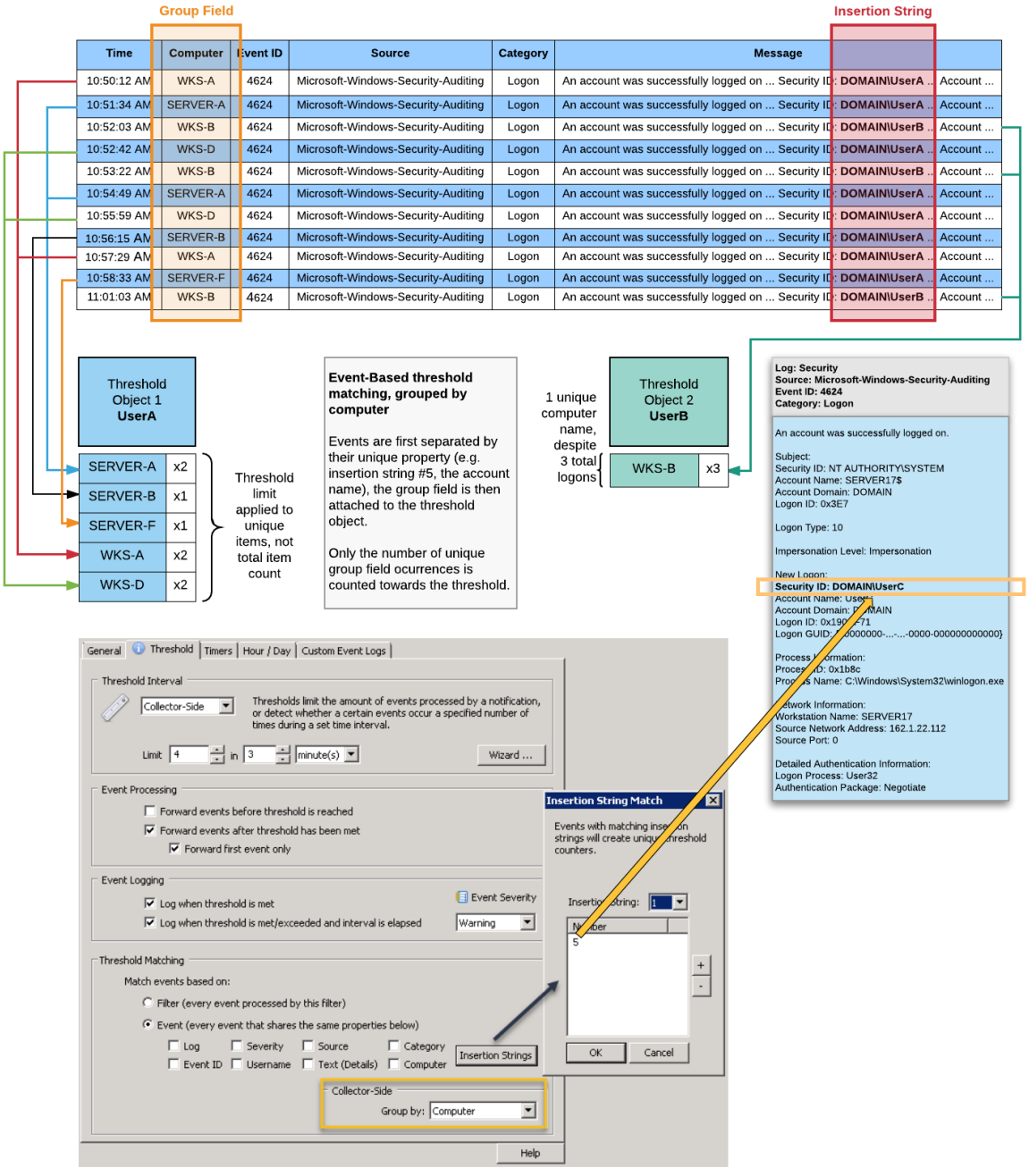


<u>Gruppieren nach (Collector-seitig)</u>
Standardmäßig werden die Schwellenwerte erhöht, wenn ein Ereignis einem Filter oder den ausgewählten Ereigniseigenschaften entspricht. Bei Verwendung der Funktion "Gruppieren nach" wird die Anzahl der erstellten Gruppen mit dem Schwellenwert anstelle der Anzahl der Ereignisse verglichen.

Das nachstehende Diagramm veranschaulicht, wie die Übereinstimmung auf der Grundlage von Ereigniseigenschaften und Einfügungetexten in Kombination mit der Gruppierung nach Computer funktioniert, um seitliche Netzwerkbewegungen zu erkennen. In diesem Beispiel verarbeitet ein Filter 4624 Ereignisse und verwendet Einfügungetext 5, welcher die "Sicherheits-ID" darstellt, als eindeutige Kennung. Anstatt jedoch nur die Vorkommen von Sicherheits-IDs zu zählen (wie im vorherigen Beispiel

gezeigt), verfolgt das Schwellenwertobjekt stattdessen alle verschiedenen Computernamen, auf die es stößt.

Im folgenden Beispiel hat sich BenutzerA bei 5 verschiedenen Hosts angemeldet, wodurch die Schwellengrenze von 4 überschritten wurde. Während die Gesamtzahl der Anmeldungen für diesen Benutzer aufgezeichnet wird (8), zählt diese Zahl nicht für den Schwellenwert. Nur die eindeutige Anzahl von Computerwerten (5) wird ausgewertet. BenutzerB hingegen hat sich nur an einem einzigen Computer angemeldet, insgesamt 3 Mal.



5.3.5.1 Ereignisprotokolle

Derzeit können die folgenden Ereignisprotokollaufzeichnungen mit dieser Funktion protokolliert werden:

Type	Event ID	Event Source	Event Description	Example
Agent-Side	10600	EventSentry	A threshold has been exceeded.	Event log filter **Logon Failures** exceeded the configured threshold (**20** entries / **3600** second(s)). **5** events (out of a total of **25**) were dropped by this filter. You can review the dropped events in the event log or the web reports. The matching events and their frequency were: **[ID=4771][LOG=Security]:10** **[ID=4624][LOG=Security]:10**
Agent-Side	10601	EventSentry	A threshold has been met.	Event log filter **Sample Threshold Filter** has reached the configured threshold (**20** entries / **600** second(s)). The matching events and their frequency were: **[ID=10100][LOG=Application]:20**
Agent-Side	10602	EventSentry	A threshold has been met and events will now be processed.	Event log filter **Sample Filter** has reached the configured threshold (**100** entries / **1200** second(s)). Events matching this filter will now be processed. The matching events and their frequency were: **[ID=4688][LOG=Security]:100**
Agent-Side	10603	EventSentry	A threshold with event-based matching has been met	Event log filter **Sample Filter** has reached or exceeded the configured threshold (**10** entries / **600** second(s)). **12** events were processed during the interval. The matching events and their frequency were: **[ID=4771][LOG=Security]:6** **[ID=4624][LOG=Security]:6**
Collector-Side	1200	EventSentry Collector	A threshold has been met	The limit of a threshold object has been reached, events will continue to be forwarded to the associated action: Name: %1 Identifier: %2 Limit: %3 event(s) Time remaining: %4 seconds Events forwarded: %5 Description: %6 Event Details: %7
Collector-Side	1201	EventSentry Collector	A threshold has been met (with group field)	The limit of a threshold object has been reached, events will continue to be forwarded to the associated action: Name: %1 Identifier: %2 Limit: %3 event(s) Time remaining: %4 seconds Events forwarded: %5 Description: %6 Events Summary: %8 Event Details: %9

Collector-Side	1202	EventSentry Collector	A threshold has been met	The limit of a threshold object has been reached, the next matching event will be forwarded to the associated action: Name: %1 Identifier: %2 Limit: %3 event(s) Time remaining: %4 seconds Events forwarded: %5 Description: %6 Event Details: %7
Collector-Side	1203	EventSentry Collector	A threshold has been met (with group field)	The limit of a threshold object has been reached, the next matching event will be forwarded to the associated action: Name: %1 Identifier: %2 Limit: %3 event(s) Time remaining: %4 seconds Events forwarded: %5 Description: %6 Events Summary: %8 Event Details: %9
Collector-Side	1204	EventSentry Collector	A threshold has been met	The limit of a threshold object has been reached, no more events will be forwarded until the threshold expires: Name: %1 Identifier: %2 Limit: %3 event(s) Time remaining: %4 seconds Events forwarded: %5 Description: %6 Event Details: %7
Collector-Side	1205	EventSentry Collector	A threshold has been met (with group field)	The limit of a threshold object has been reached, no more events will be forwarded until the threshold expires: Name: %1 Identifier: %2 Limit: %3 event(s) Time remaining: %4 seconds Events forwarded: %5 Description: %6 Events Summary: %8 Event Details: %9
Collector-Side	1206	EventSentry Collector	A threshold has been met	The limit of a threshold object has been reached, events will be forwarded to the associated action until the threshold expires and event ID 1220 is logged. Name: %1

				Identifier: %2 Limit: %3 event(s) Time remaining: %4 seconds Events forwarded: %5 Description: %6 Event Details: %7 The limit of a threshold object has been reached, events will be forwarded to the associated action until the threshold expires and event ID 1220 is logged.
Collector-Side	1207	EventSentry Collector	A threshold has been met (with group field)	Name: %1 Identifier: %2 Limit: %3 event(s) Time remaining: %4 seconds Events forwarded: %5 Description: %6 Events Summary: %8 Event Details: %9 The limit of a threshold object has been reached, the next matching event will be forwarded to the associated action until the threshold expires and event ID 1220 is logged.
Collector-Side	1208	EventSentry Collector	A threshold has been met	Name: %1 Identifier: %2 Limit: %3 event(s) Time remaining: %4 seconds Events forwarded: %5 Description: %6 Event Details: %7 The limit of a threshold object has been reached, the next matching event will be forwarded to the associated action until the threshold expires and event ID 1220 is logged.
Collector-Side	1209	EventSentry Collector	A threshold has been met (with group field)	Name: %1 Identifier: %2 Limit: %3 event(s) Time remaining: %4 seconds Events forwarded: %5 Description: %6 Events Summary: %8 Event Details: %9 The limit of a threshold object has been reached, no more events will be forwarded until the threshold expires and event ID 1220 is logged.
Collector-Side	1210	EventSentry Collector	A threshold has been met	Name: %1 Identifier: %2

				Limit: %3 event(s) Time remaining: %4 seconds Events forwarded: %5 Description: %6 Event Details: %7 The limit of a threshold object has been reached, no more events will be forwarded until the threshold expires and event ID 1220 is logged.
Collector-Side	1211	EventSentry Collector	A threshold has been met (with group field)	Name: %1 Identifier: %2 Limit: %3 event(s) Time remaining: %4 seconds Events forwarded: %5 Description: %6 Events Summary: %8
Collector-Side	1220	EventSentry Collector	A threshold has expired	Event Details: %9 A threshold object has expired: Name: %1 Identifier: %2 Events forwarded: %3 Time elapsed: %4 seconds Limit: %5 Actual Count: %6 Description: %7 Events Summary: %8

5.3.6 Zeitgeber

Filterzeitgeber geben Ihnen die Möglichkeit, ein Ereignis - selbst wenn es einem Ihrer Filter entspricht - zu ignorieren, wenn ein bestimmtes nachfolgendes Ereignis innerhalb einer konfigurierbaren Zeitspanne eintritt.

Betrachten Sie das folgende Szenario: *Ein kritischer Dienst stoppt, wird aber innerhalb von 1 Minute automatisch neu gestartet (z.B. nachdem sich eine AntiVirus-Engine aktualisiert hat), was zu zwei Ereignissen führt, die je einen Fehler im Ereignisprotokoll erzeugen. Erstens, wenn der Dienst stoppt und erneut, wenn der Dienst neu gestartet wird. Sie könnten natürlich die Überwachung des Dienstes ganz einstellen, aber das wäre nicht wünschenswert, da Sie vermutlich benachrichtigt werden möchten, wenn der Dienst ohne Neustart beendet wird. Filter-Timers bieten hier eine Lösung.*

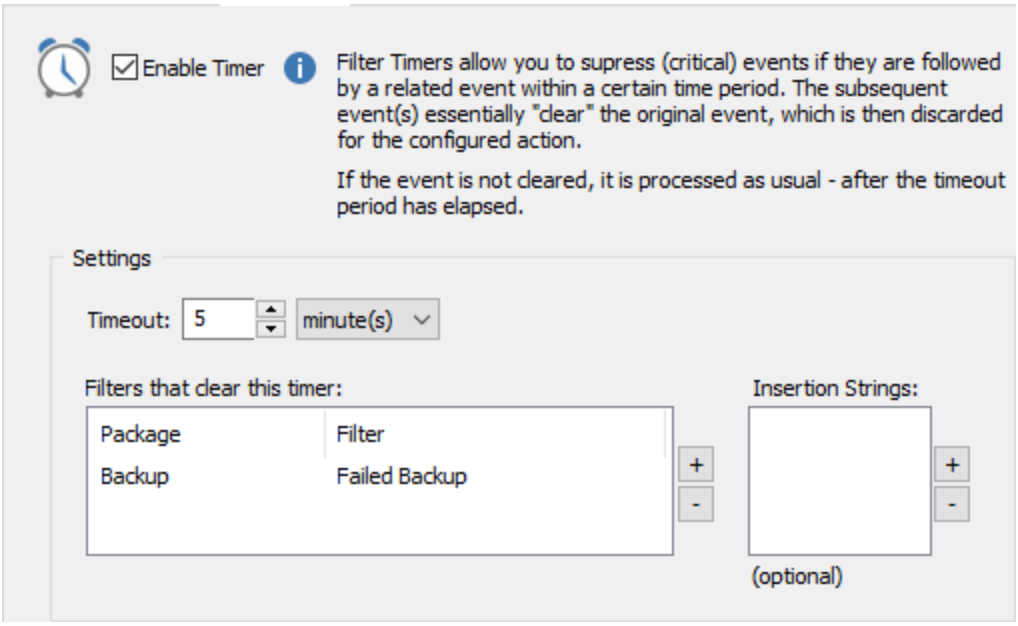
Filterzeitgeber lösen dieses Problem, indem sie es Ihnen ermöglichen, zwei Filter zu erstellen: Einen Filter, der mit dem ersten Ereignis übereinstimmt, und einen Filter, der mit dem nachfolgenden Ereignis übereinstimmt, das wiederum den ersten Alarm löscht. Als solches werden Sie nie über das ursprüngliche Ereignis benachrichtigt, wenn es innerhalb der Timeout-Periode "gelöscht" wurde.

Beachten Sie, dass Sie aufgrund der Art dieser Funktion erst nach Ablauf der Timer-Periode über ein Ereignis **benachrichtigt werden**, das auf einen Filter mit der Option

Enable Timer passt.

Aktivieren eines Timers

Um einen Timer im Filter zu aktivieren, bearbeiten Sie den Filter und klicken Sie auf die Registerkarte Timer. Wählen Sie auf der Registerkarte "Timer" die Option "Enable Timer", um den Timer zu aktivieren. Geben Sie dann eine Timeout-Periode an (z.B. 2 Minuten) und geben Sie einen Filter an, der den Timer durch Klicken auf die Schaltfläche "Plus **+"** löscht. Wenn Sie auf diese Schaltfläche klicken, erscheint ein Dialog, der alle geeigneten Filter (z.B. Include-Filter) anzeigt, die zum Löschen dieses Timers verwendet werden können.



Der "Clearing"-Filter

Dieser Filter wird von einem Timerfilter referenziert und hat die Fähigkeit, den Timer zu löschen. Wenn Sie diesen Filter einrichten, geben Sie dieselbe Aktion an wie die im Timer-Filter angegebene Aktion. Wenn dieser Filter übereinstimmt, während ein Timer-Filter von der eingestellten Zeitüberschreitung herunterzählt, löscht er den Timer, und die Aktion wird nicht benachrichtigt.

Wenn der Löschfilter mit einem Ereignis übereinstimmt, während kein Timer aktiv ist, verhält er sich wie ein normaler Filter. Als solcher können Sie mehrere Aktionen auf dem Löschfilter angeben.

Einfügungstexte

Diese Funktion ist besonders nützlich bei der Erstellung eines Filterzeitgebers, der mit einer Vielzahl von Ereignissen übereinstimmen sollte. Zum Beispiel eine "Service-Stop / Service-Start"-Kombination oder eine "Prozess-Ende / Prozess-Start"-Kombination. Ohne die Verwendung der Einfügetext wäre es notwendig, für jedes eindeutige Ereignis (z.B. Dienst), das Sie überwachen wollten, ein Filterpaar zu erstellen.

Nehmen wir an, Sie möchten benachrichtigt werden, wenn **ein überwachter Dienst** für mehr als 5 Minuten gestoppt wurde (oder wenn ein Host für mehr als 5 Minuten offline ist usw.). Nehmen wir an, der DNS-Server-Dienst würde angehalten, was einen Timer auslösen würde, der in **5** Minuten ablaufen würde. Nehmen wir auch an, dass der Lizenzprotokollierungsdienst auf demselben Host 3 Minuten nach dem Stoppen des DNS-Server-Dienstes gestartet wurde. Da beide mit dem generischen Filter

übereinstimmten, der Dienststartereignisse generell auffängt, würde der Zeitgeber gelöscht und Sie würden nicht über den gestoppten DNS-Server Dienst benachrichtigt werden.

Durch die Verwendung von Einfügetexten können Sie jedoch die ausgewählten Einfügetexte aus dem Ursprungsereignis, das den Filterzeitgeber festgelegt hat, und dem Zeitgeber, der den Filter löschen wird, zu vergleichen. Wenn sie übereinstimmen, wird der Filterzeitgeber gelöscht, andernfalls nicht. Wir empfehlen Ihnen, den Ereignis-Meldungs-Browser zu verwenden, um die Anzahl und Position der Einfügetexte innerhalb der Ereignisse zu bestimmen.

Beachten Sie folgende Ereignisse, die sowohl die Dienstüberwachung als auch die Prozessgestaltung/-beendigung betreffen:

Event Source	Event Category	Event ID	Event Description (insertion strings start with % character)
EventSentry	Service Monitoring	10100	The status for service **%1** (%2) changed from %3 to %4.
Security	Detailed Tracking	592	A new process has been created: New Process ID: %1 **Image File Name: %2** Creator Process ID: %3 User Name: %4 Domain: %5 Logon ID: %6
Security	Detailed Tracking	593	A process has exited: Process ID: %1 **Image File Name: %2** User Name: %3 Domain: %4 Logon ID: %5

Immer wenn EventSentry eine Dienststatusänderung aufzeichnet, protokolliert es Ereignis **10100** im Ereignisprotokoll und ersetzt **%1** durch den Namen des Dienstes, dessen Status sich geändert hat. Wenn also eine Übereinstimmung mit dem Einfügetext **#1** erforderlich ist, kann ein Ereignis, das sich auf den Dienst "Lizenzprotokollierung" bezieht, den eingestellten Timer nicht aus dem "DNS-Serverdienst" löschen.

Ein ähnlicher Aufbau könnte mit den Ereignissen erreicht werden, die von Windows protokolliert werden, wenn sich ein Benutzer anmeldet und dann wieder abmeldet. Wenn wir einen Filter-Timer auf der Grundlage des Ereignisses 4624 und den Filter-Clearing-Timer auf der Grundlage des Ereignisses 4647 einstellen, dann müssen wir die Einfügezeichenfolge #8 des Anmeldeereignisses mit der Einfügezeichenfolge #4 des Abmeldeereignisses verbinden.

Bei der Angabe von Einfügezeichenfolgen müssen sowohl die Einfügung aus dem Filtertimer-Ereignis als auch aus dem Löschungsereignis angegeben werden. Die gleiche Einfügezeichenfolge kann für beide Ereignisse angegeben werden, wenn sie gleich sind (in den obigen Beispielen sind die Einfügezeichenfolgen für das Dienstüberwachungsereignis gleich, aber nicht für die An-/Abmeldeereignisse).

Wie es funktioniert

Wenn ein Ereignis mit einem Timer-aktivierten Filter übereinstimmt, wartet EventSentry, bis die Timeout-Periode abgelaufen ist, bevor es das Ereignis an die konfigurierten Benachrichtigungen

weiterleitet. EventSentry hängt die Zeichenfolge **TIMER-DELAY** an den Betreff einer E-Mail an, wenn eine der konfigurierten Benachrichtigungen vom Typ SMTP ist.

Wenn der in der Liste "**Filter, der diesen Timer löschen kann**" angegebene Filter mit einem Ereignis innerhalb der Timeout-Periode übereinstimmt, dann wird weder der Original- noch der "Clearing"-Filter die Benachrichtigung, das Ziel dieser Funktion, verarbeiten.

Benachrichtigungen steurn

Der Sinn eines Filter-Timers besteht natürlich darin, Benachrichtigungen zu unterdrücken, wenn das Ereignis, das einen Filter-Timer auslöst, innerhalb des konfigurierten Zeitraums gelöscht wird. Folglich gibt es kein Szenario, in dem %PRODUCT% eine Benachrichtigung verschicken würde, wenn der Timer-Filter gelöscht wird.

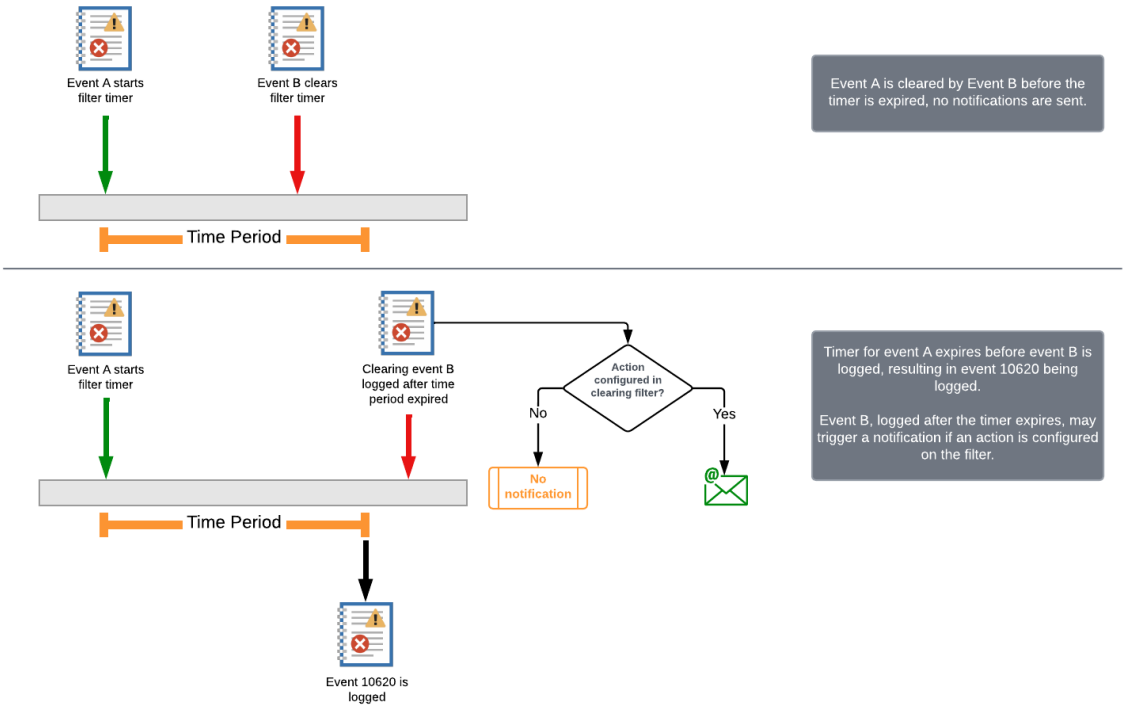
Es ist möglich zu steuern, ob Benachrichtigungen versendet werden, wenn das Ereignis, das einen Filtertimer löscht, außerhalb des konfigurierten Zeitfensters eintritt. Ein Beispiel: Ein Filter-Timer für einen Dienst ist für 3 Minuten konfiguriert, aber der Dienst wird erst nach 4 Minuten neu gestartet. Je nach den Umständen kann es wünschenswert sein oder nicht, eine Benachrichtigung zu erhalten, wenn der Filter, der den Timer löscht, das Ereignis verarbeitet.

Empfang einer Benachrichtigung

Um eine Benachrichtigung auszulösen, wenn das Ereignis außerhalb des konfigurierten Zeitfensters eintritt, konfigurieren Sie einfach die gleiche Aktion für den Löschfilter wie für den Zeitgeberfilter. Tritt das Ereignis, das den Timer löschen soll, verspätet ein, also außerhalb des Zeitfensters, dann wird eine Benachrichtigung ausgelöst. Im Fall des Beispiels der Dienstüberwachung würde dies den Benutzer darüber informieren, dass der Dienst schließlich neu gestartet wurde, wenn auch mit einer Verzögerung.

Unterdrückung von Benachrichtigungen

Um Benachrichtigungen zu unterdrücken und lediglich darüber informiert zu werden, dass der Timer des Filters abgelaufen ist, sollte für den Timer-Löschfilter keine Aktion angegeben werden. Dadurch wird der Timer-Filter immer noch gelöscht, wenn das Ereignis innerhalb des angegebenen Zeitfensters eintritt, es werden aber keine Benachrichtigungen gesendet, wenn das Ereignis außerhalb (nach) dem Zeitfenster eintritt.



5.3.7 Anomalie

Die Anomalie-Funktion von Ereignisprotokollfiltern hilft bei der Erkennung ungewöhnlicher Ereignisse, indem sie die Ereignisdaten (Einfügezeichenfolgen) nach einer Lernphase untersucht, in der eine Basislinie bekannter Daten festgelegt wurde.

Im Einzelnen bestimmt die Anomalieerkennung, ob eine Kombination von Einfügezeichenfolgen eines Ereignisses (die in einem Filter konfigurierbar sind) noch nie zuvor aufgetreten ist und daher als Anomalie gilt. Während die Anomalieerkennung mit jedem Ereignis verwendet werden kann, das Einfügezeichenfolgen verwendet (oder bei dem ein RegEx-Muster dynamische Einfügezeichenfolgen erstellen kann), lässt sie sich besonders gut mit Sicherheitsereignissen aus dem Windows-Sicherheitsereignisprotokoll integrieren.

Die Anomalieerkennung kann verwendet werden, um eine Vielzahl von ungewöhnlichen Aktivitäten zu erkennen:

- Ein Benutzer meldet sich über RDP von einer neuen Remote-IP-Adresse an
- Ein Benutzer startet einen neuen Prozess
- Eine Anmeldung durch einen Benutzer, der sich noch nie zuvor über denselben Anmeldetyp angemeldet hat (z. B. Konsole vs. RDP)

Die Erkennung von Anomalien erfolgt durch die Erstellung von **Schlüssel/Wert-Paaren** aus Einfügezeichenfolgen, wobei der **Schlüssel** in der Regel einen statischen Schlüsselwert darstellt (z. B. Benutzer, Computer), mit dem dann dynamische **Werte** verknüpft werden. Sowohl die Schlüssel als auch die Werte bestehen aus mindestens einer Einfügezeichenfolge, wobei auch eine Kombination von Einfügezeichenfolgen möglich ist.

Lernphase

Nachdem ein Anomalie-Filter zum ersten Mal ein übereinstimmendes Ereignis verarbeitet hat, beginnt eine Lernphase, in der eine Grundlinie bekannter Schlüssel/Wert-Paare erstellt wird (z. B. 2 Wochen). So kann ein Filter beispielsweise lernen, welche Prozesse Benutzer auf dem überwachten System starten, indem er die Ereignis-ID 4688 untersucht (die protokolliert wird, wenn ein neuer Prozess startet). Nach Abschluss der Lernphase werden alle Ereignisdaten, die noch nicht verarbeitet wurden, als Anomalie gekennzeichnet. Nachdem das Ereignis (und die zugehörigen Daten) verarbeitet wurden, wird es als Teil der Basislinie betrachtet und bei einer erneuten Verarbeitung in der Zukunft nicht als Anomalie eingestuft.

Separate Lernperiode für neue Schlüssel
Die Aktivierung dieser Option wird fast immer empfohlen, da sie sicherstellt, dass Werte, die mit einem Schlüssel verknüpft sind, eine eigene Lernperiode haben, die unabhängig von der anderer Schlüssel ist (siehe Beispiel 2 für Details).

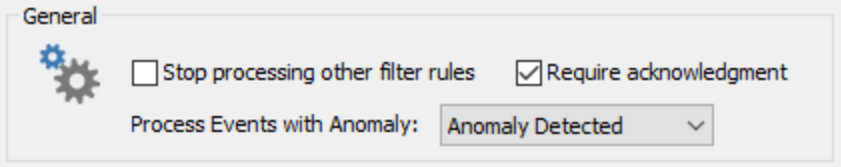
Anomalien werden von jedem einzelnen Agenten ermittelt, und jeder Agent/überwachte Host hat seine eigene Lernzeit und seinen eigenen Cache.

Auf Anomalien reagieren

Es ist wichtig zu verstehen, dass Anomaliefilter selbst keine Ereignisse an eine Aktion weiterleiten. Stattdessen werden passende Ereignisse intern als Anomalie gekennzeichnet. Ein anderer, nachfolgender Ereignisprotokollfilter kann dann diese Markierung auswerten und das Ereignis entsprechend verarbeiten, z. B.:

- Das Ereignis an eine andere Aktion weiterleiten
- Eine Überprüfung dieses Ereignisses in der DB anfordern ("Require Acknowledgment")

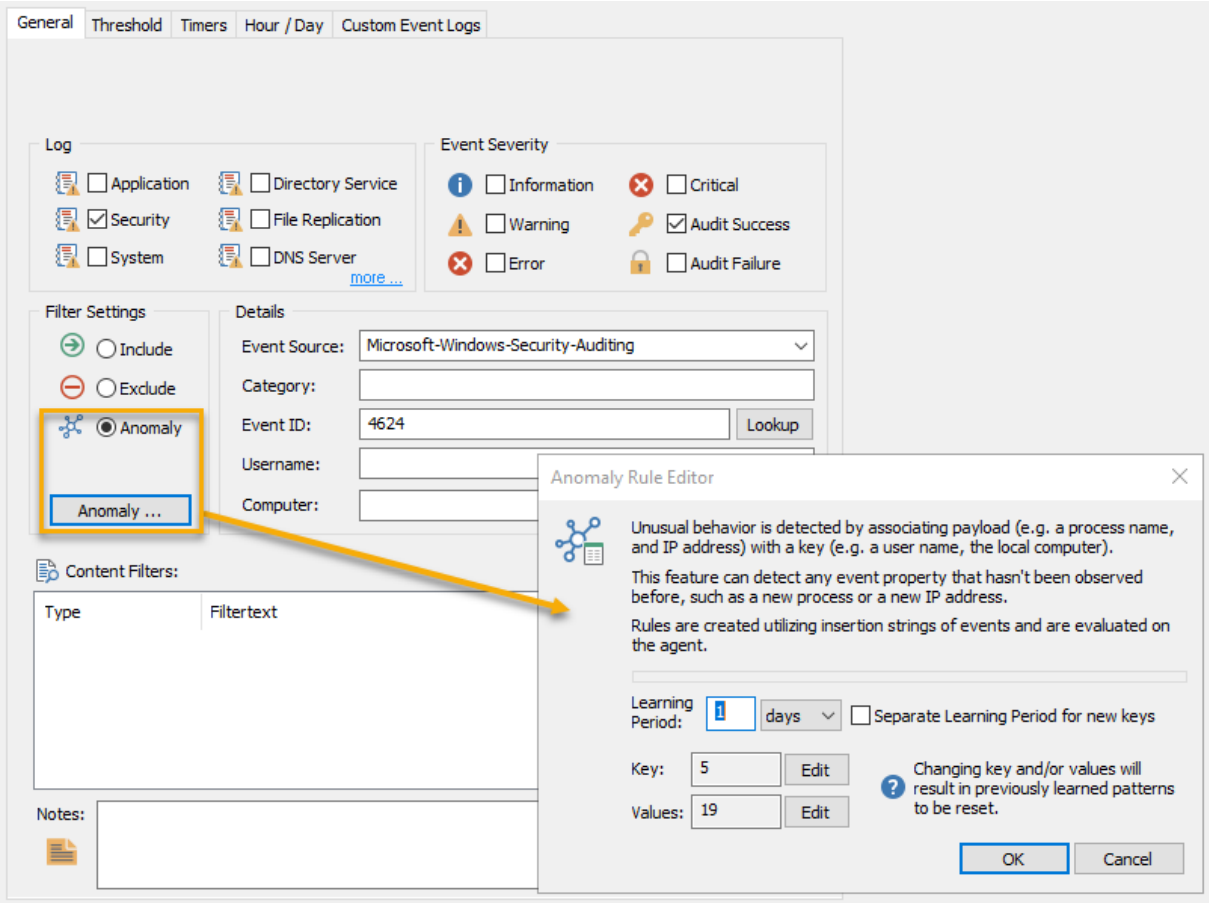
Ein Ereignisprotokollfilter kann so konfiguriert werden, dass er nur Ereignisse verarbeitet, die als Anomalie eingestuft werden, und zwar über die Option "Ereignisse mit Anomalie verarbeiten", die in den erweiterten Eigenschaften verfügbar ist.



Ereignisse, die als Anomalie gelten, werden jedoch in allen anwendbaren Funktionen zur Verfolgung der Einhaltung von Vorschriften als solche gekennzeichnet, wobei dieser Zustand über die Sucheigenschaft `isanomaly` ausgewertet werden kann. Dies erleichtert die Suche nach Prozessen oder Anmeldungen, die z. B. als Anomalie betrachtet werden.

Aktivieren von Anomalien

Um Anomalien zu analysieren, wählen Sie einfach die Option "Anomalie" in einem Ereignisprotokollfilter. Klicken Sie auf die Schaltfläche "Anomalie", um die Regeln für Anomalien zu konfigurieren.



Schlüssel und Werte
Jeder Anomalie-Filter benötigt mindestens einen Schlüssel und einen Wert, wobei dieser auf Einfügezeichenfolgen verweist, die dynamische Werte darstellen (z. B. Prozesse, Benutzer, IP-Adressen, ...).

Bei der Erkennung von Anomalien wird im Allgemeinen zwischen ein- und zweidimensionalen Konfigurationen unterschieden.

Eindimensional
Der "Schlüssel" verweist auf eine Einfügezeichenfolge, die sich nie ändert, z. B. den lokalen Hostnamen. Stattdessen werden die angetroffenen Werte (=Einfügezeichenfolgen) verwendet, um festzustellen, ob das Ereignis eine Anomalie ist oder nicht. Die Erkennung neuer Benutzer, die sich bei einem Computer anmelden, oder neuer IP-Adressen, die eine Verbindung zu einer RDP-Sitzung herstellen, wäre ein Beispiel für eine eindimensionale Einrichtung (siehe Beispiel 1).

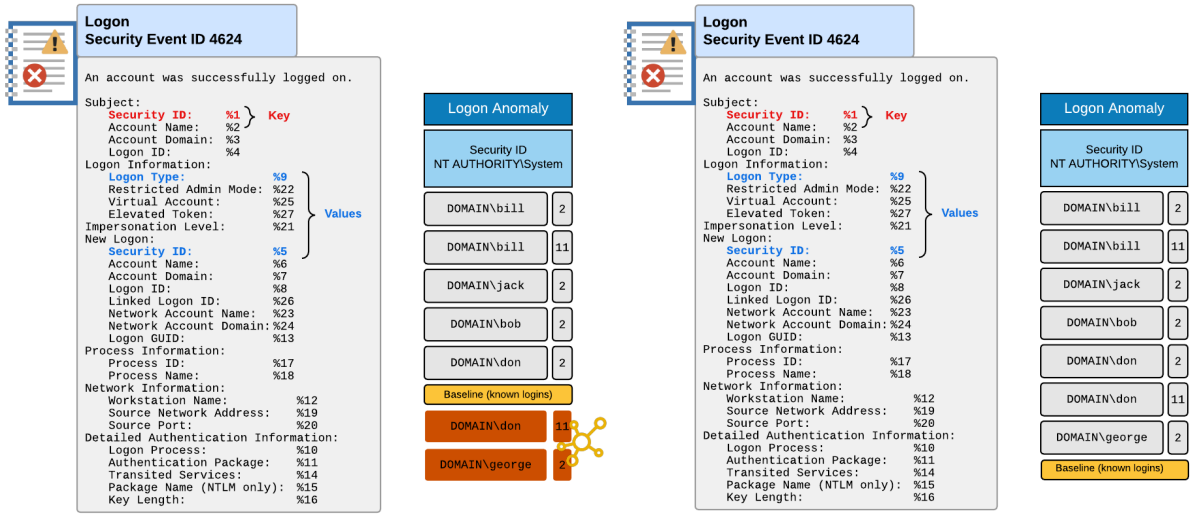
Zweidimensional
Hier ist eine als "Schlüssel" definierte Einfügezeichenfolge untrennbar mit einer oder mehreren als "Werte" definierten Einfügezeichenfolgen verbunden. So kann beispielsweise ein Benutzername mit einem Prozessnamen verbunden werden, so dass jeder Benutzer seine eigenen Anomalieeinstellungen hat. So würde beispielsweise "Benutzer A", der "ipconfig.exe" im März ausführt, "ipconfig.exe", das von "Benutzer B" im August ausgeführt wird, nicht automatisch als sicher betrachten - es würde als Anomalie gekennzeichnet werden (siehe Beispiel 2).

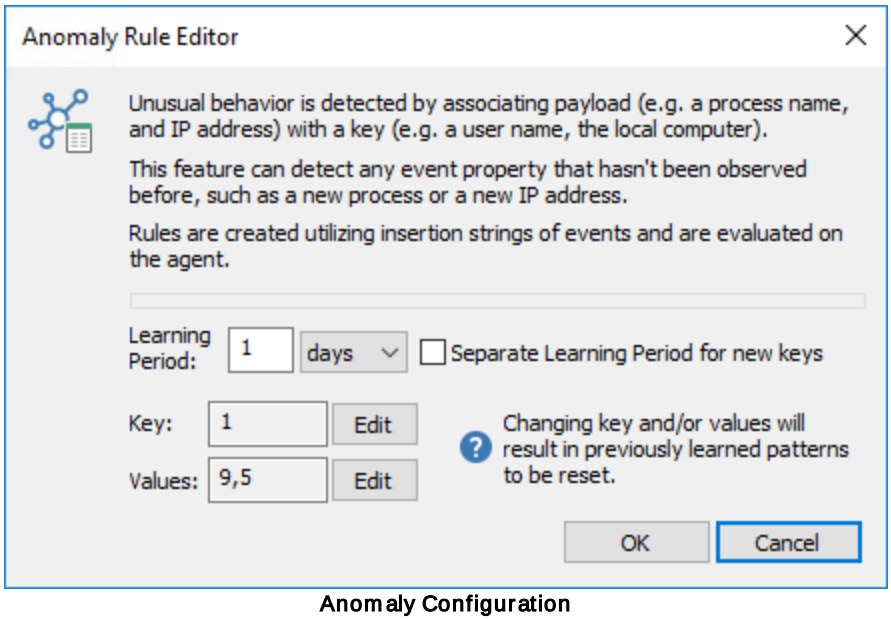
5.3.7.1 Beispiele

Beispiel 1: Anomalie bei der Anmeldung

Die folgenden Abbildungen zeigen eine mögliche Konfiguration für einen Anomalie-Filter für die Ereignis-ID 4624, die von Windows protokolliert wird, wenn sich ein Benutzer erfolgreich bei einem System anmeldet. In diesem Beispiel ist der Schlüsselwert von vornherein immer derselbe: **NT AUTHORITY\System.** Die Werte setzen sich zusammen aus dem Anmeldetyp (eine numerische Zahl, die die Art der Anmeldung angibt, z. B. Konsole oder RDP) sowie dem Benutzer, der sich anmeldet. Die linke Abbildung zeigt die Basislinie für 5 Anmeldungen mit unterschiedlichen Anmeldetypen, wobei 2 Anmeldungen als Anomalien betrachtet werden. Das rechte Bild zeigt die neue Basislinie, die die bisher unbekannten Anmeldungen einbezieht.

Da der angegebene Schlüsselwert immer derselbe ist (NT AUTHORITY\System), werden in diesem Beispiel im Wesentlichen nur Ereignisse in einer einzigen Dimension betrachtet - die Benutzernamen und die damit verbundenen Anmeldetypen. Beispiel 2 analysiert die Daten in zwei Dimensionen, da es Prozesse mit unterschiedlichen Benutzernamen verbindet.



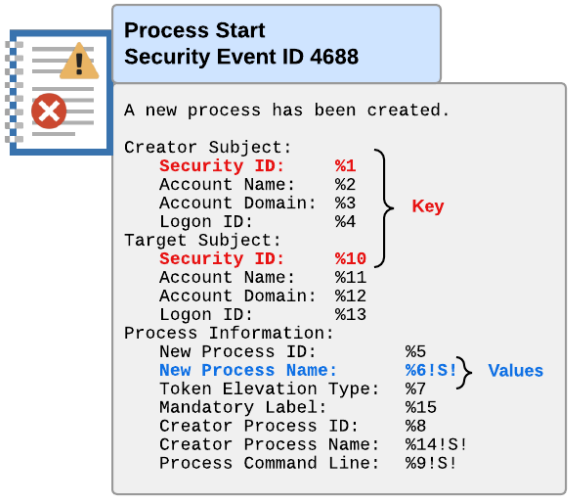


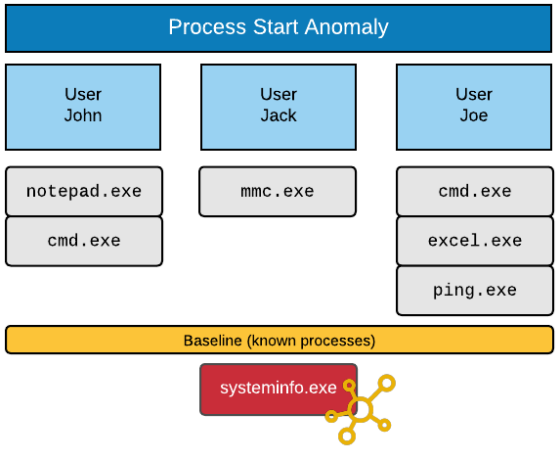
Anomaly Configuration

Beispiel 2: Prozessanomalie

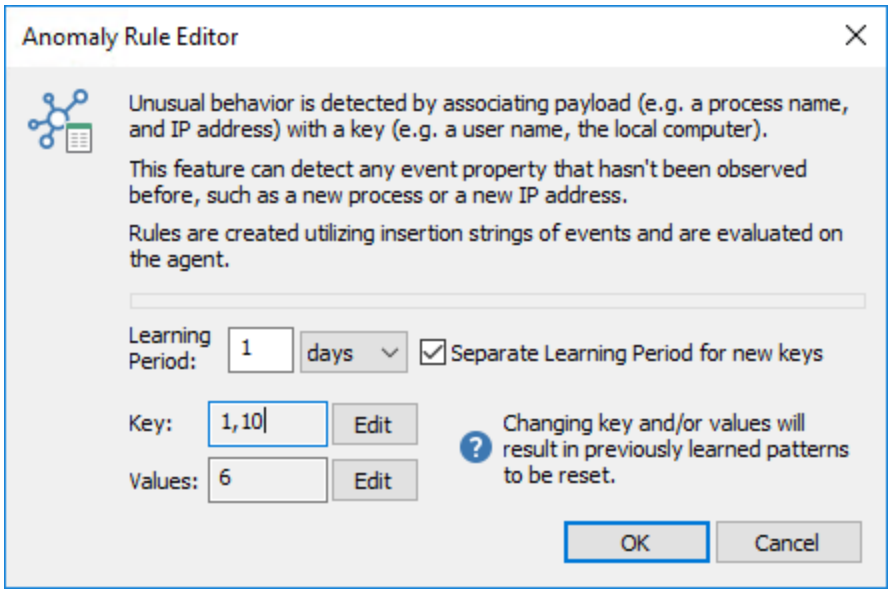
In diesem Beispiel wird versucht, Prozesse zu erkennen, die noch nicht von einem Benutzer ausgeführt wurden. Die Konfiguration ähnelt der des ersten Beispiels, mit der Ausnahme, dass die Ereignis-ID 4688 verarbeitet wird und dynamische Werte für den Anomalieschlüssel verwendet werden.

Der Anomalie-Filter verwendet die Einfügezeichenfolgen 1 und 10, um den Schlüssel zu erstellen. Dies ermöglicht es EventSentry, zwischen Prozessen zu unterscheiden, die als Administrator und Prozessen, die als nicht privilegierter Benutzer gestartet werden. Die Einfügezeichenfolge Nummer 6 ist einfach der Pfad zum Prozess selbst. Da Prozesse nun mit ihren jeweiligen Schlüsseln (Benutzern) verknüpft sind, wird beim Starten eines zuvor unbekannten Prozesses (z. B. **systeminfo.exe**) jedes Mal, wenn dieser Prozess unter einem anderen Benutzer gestartet wird, das Anomalie-Flag gesetzt.





Beachten Sie, dass die Anomaliekonfiguration für "Separate Lernperiode für neue Schlüssel" konfiguriert ist. Dadurch wird sichergestellt, dass ein neuer Benutzer, wenn er seinen ersten Prozess startet, automatisch einen neuen Lernzeitraum erhält. Wäre diese Einstellung nicht aktiviert, würde jeder Prozess, der von einem Benutzer nach dem Beginn des ersten Lernzeitraums gestartet wird, als Anomalie gekennzeichnet werden, was zu vielen Fehlalarmen führen würde.



Anomalie Konfiguration

5.3.8 Erweiterte Stunden-/Tage-Einstellungen

Die Einstellungen **Stunde / Tag** erlauben es Ihnen, Ihre Filter weiter einzuschränken oder zusätzliche Aufgaben durchzuführen.

Filter Tag & Stunde Konfiguration
Die Konfiguration Filter Tag & Stunde ermöglicht es Ihnen, einen Filter für bestimmte Stunden der Woche aktiv/inaktiv zu setzen (weitere Informationen).

Ablauf filtern
Filter können so konfiguriert werden, dass sie zu einem bestimmten Datum/Zeitpunkt in der Zukunft automatisch ablaufen (weitere Informationen).

Boot-Verhalten
Filter können so konfiguriert werden, dass sie nur während oder nach dem Booten des Systems aktiv sind (weitere Informationen).

Benachrichtigungszusammenfassung
Zusammenfassende Benachrichtigungen ermöglichen es Ihnen, zu bestimmten Zeiten während der Woche/des Tages eine zusammenfassende E-Mail zu erhalten, anstatt sofort E-Mails zu erhalten. Diese Funktion kann auch in Verbindung mit einer ODBC-Benachrichtigung verwendet werden (weitere Informationen).

Wiederkehrende Ereignisse
Sie können sich benachrichtigen lassen, wenn ein bestimmtes Ereignis während einer bestimmten Zeitspanne **nicht** im Ereignisprotokoll erscheint, z.B. ein Ereignis, das bestätigt, dass ein Sicherungsauftrag erfolgreich war (weitere Informationen).

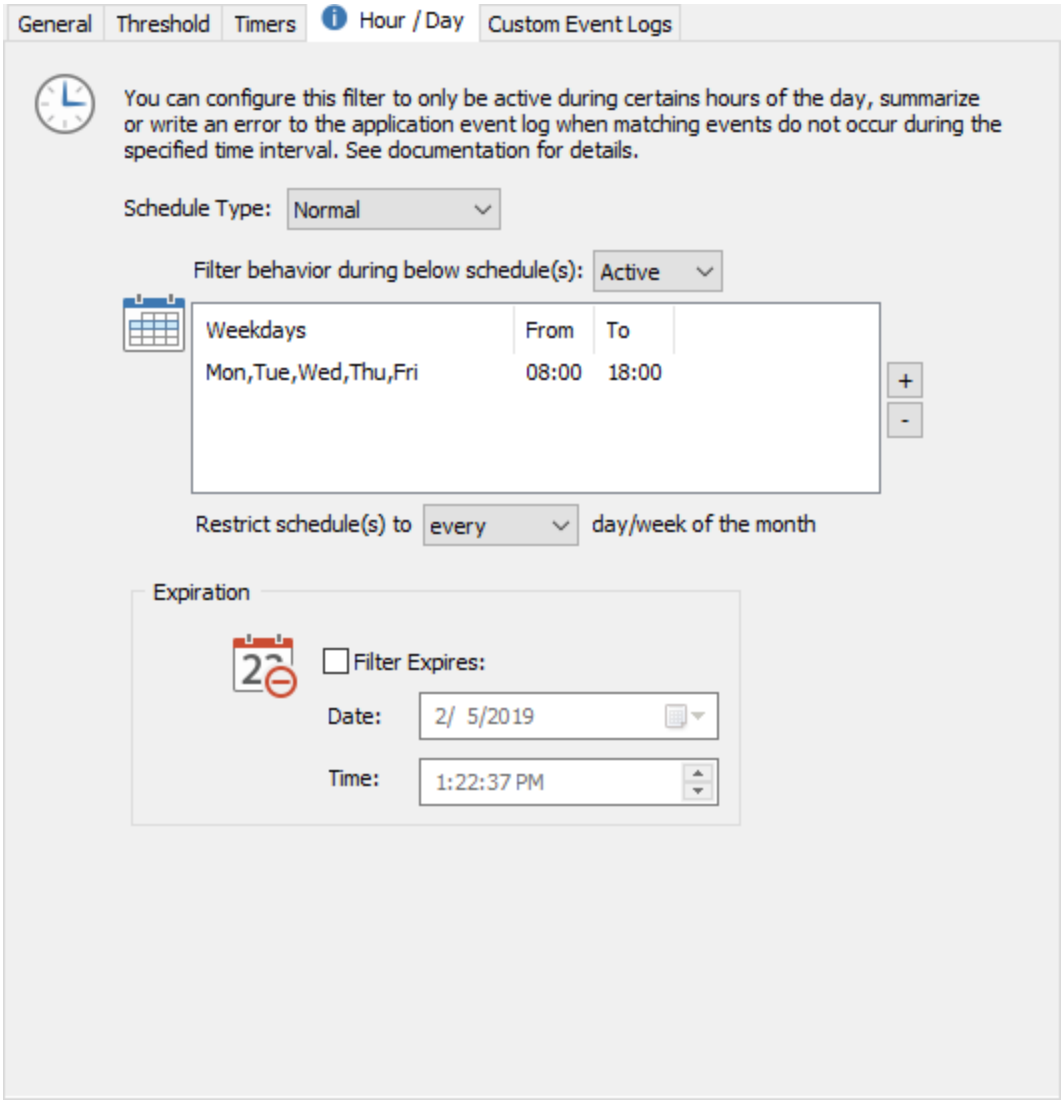
5.3.8.1 Tag & Stunde Konfiguration

Zusätzlich zu den allgemeinen Filteroptionen können Sie auch den Tag oder die Uhrzeit festlegen, zu der ein Filter aktiv ist. Wenn Sie beispielsweise nicht daran interessiert sind, während des Tages

Ereignisaufzeichnungen aus dem Sicherheitsereignisprotokoll zu erhalten, dann können Sie den Filter während bestimmter Stunden des Tages deaktivieren.

Um zu ändern, wann ein Filter aktiv ist, stellen Sie den "Zeitplantyp" auf "Normal", fügen Sie einen oder mehrere Zeitpläne hinzu und geben Sie an, ob der Filter während der unten aufgeführten Zeitpläne **aktiv** oder **inaktiv** sein wird. Andere verfügbare Zeitplantypen sind "Zusammenfassung" und "Wiederkehrend".

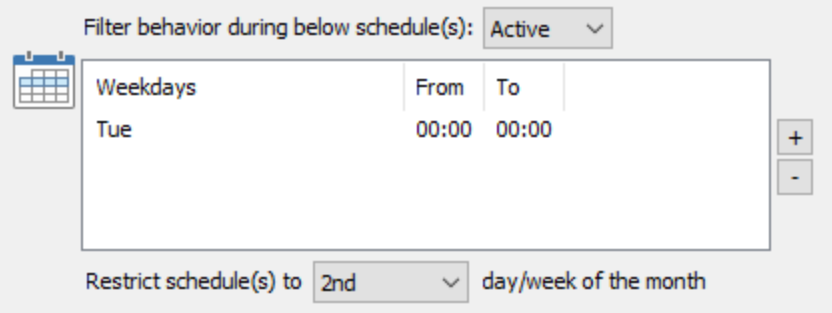
Filter mit einem Zeitplan werden mit einer kleinen Uhr in der Baumstruktur angezeigt.



Der oben angezeigte Filter ist nur unter der Woche von 8:00 bis 18:00 Uhr inaktiv.

Anwenden eines Filters auf den "n-ten" Tag des Monats

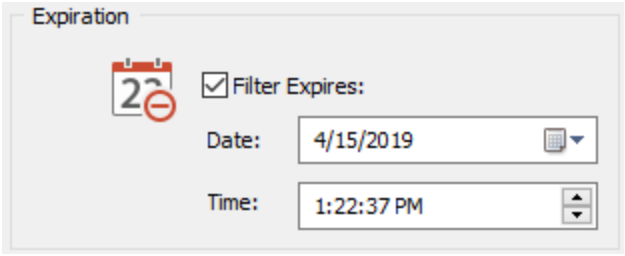
Standardmäßig ist der obige Stunden-/Tagesplan jede Woche des Monats aktiv. Der Zeitplan kann so eingeschränkt werden, dass er nur für jede n-te Woche des Monats gilt, indem die Einstellung "Anwenden auf" geändert wird. Zum Beispiel würde der untenstehende Zeitplan einen Filter so einschränken, dass er nur an jedem 2. Dienstag des Monats aktiv ist. Dies könnte z.B. für einen Ausschlussfilter nützlich sein, der bestimmte Ereignisse während eines monatlichen Patch-Zeitplans ausschließt.



Ein ganztägiger Zeitplan wird mit 00:00 bis 00:00 Uhr angegeben.

5.3.8.2 Ablauf

Sie können konfigurieren, dass ein Filter abläuft, indem Sie das Kontrollkästchen "Filter Expires" auf der Registerkarte Stunde/Tag aktivieren. Auf diese Weise können Sie Regeln erstellen, die ab einem bestimmten Zeitpunkt nicht mehr aktiv sind.



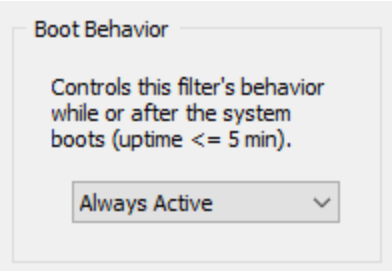
So könnten Sie beispielsweise wiederkehrende E-Mail-Benachrichtigungen für ein bestimmtes Problem erhalten, das Ihnen nicht bekannt ist. Dieses Problem wird gerade behandelt, aber es wird drei Tage dauern, bis es gelöst ist. Da Sie sich also des Problems bewusst sind, würden Sie es wahrscheinlich vorziehen, in der Zwischenzeit keine Benachrichtigungen zu erhalten.

Wenn Sie einfach einen Ausschlussfilter für den Alarm erstellen, könnten Sie das Problem möglicherweise vergessen. Stattdessen können Sie immer noch einen Ausschlussfilter erstellen, aber diesmal den Ausschlussfilter so einstellen, dass er an einem bestimmten Tag abläuft. Im obigen Beispiel würden Sie den Filter so einstellen, dass er genau dann abläuft, wenn das Proble*gelöst werden* soll. Auf diese Weise erhalten Sie nur dann weiter E-Mail-Benachrichtigungen, wenn das Problem nicht rechtzeitig gelöst werden konnte.

Der EventSentry-Agent protokolliert die Ereignis-ID 250 mit dem Schweregrad Warnung (nur auf dem Host, auf dem EventSentry mit dem Setup installiert wurde), wenn ein Filter abläuft. Diese Warnung wird nur einmal protokolliert, es sei denn, das Ablaufdatum ändert sich und es wird eine neue Konfiguration angewendet.

5.3.8.3 Boot-Verhalten

Filterregeln können so konfiguriert werden, dass sie erst aktiv werden, nachdem ein System gebootet hat (wenn die Betriebszeit > 5 Minuten ist), was unnötige Alarme, die nur während des Bootvorgangs erzeugt werden, reduzieren kann. Die Option Boot-Verhalten unterstützt drei verschiedene Einstellungen:



1. Immer aktiv
Der Filter ist immer aktiv, unabhängig davon, ob das System gerade bootet oder nicht. Dies ist die Voreinstellung.

2. Nur beim Booten
Der Filter ist nur während des Systemstarts aktiv.

3. Nur nach dem Booten
Der Filter ist nur aktiv, nachdem das System gebootet hat.

Ein Filter, der nur während des Bootvorgangs aktiv ist, kann nützlich sein, um bestimmte Alarme auszuschließen, die nur während des Bootvorgangs erzeugt werden.

Ein Filter, der erst nach Abschluss des Boot-Vorgangs aktiv ist, alarmiert nicht bei potenziellen Störungen, die nur während des Boot-Vorgangs erzeugt werden.

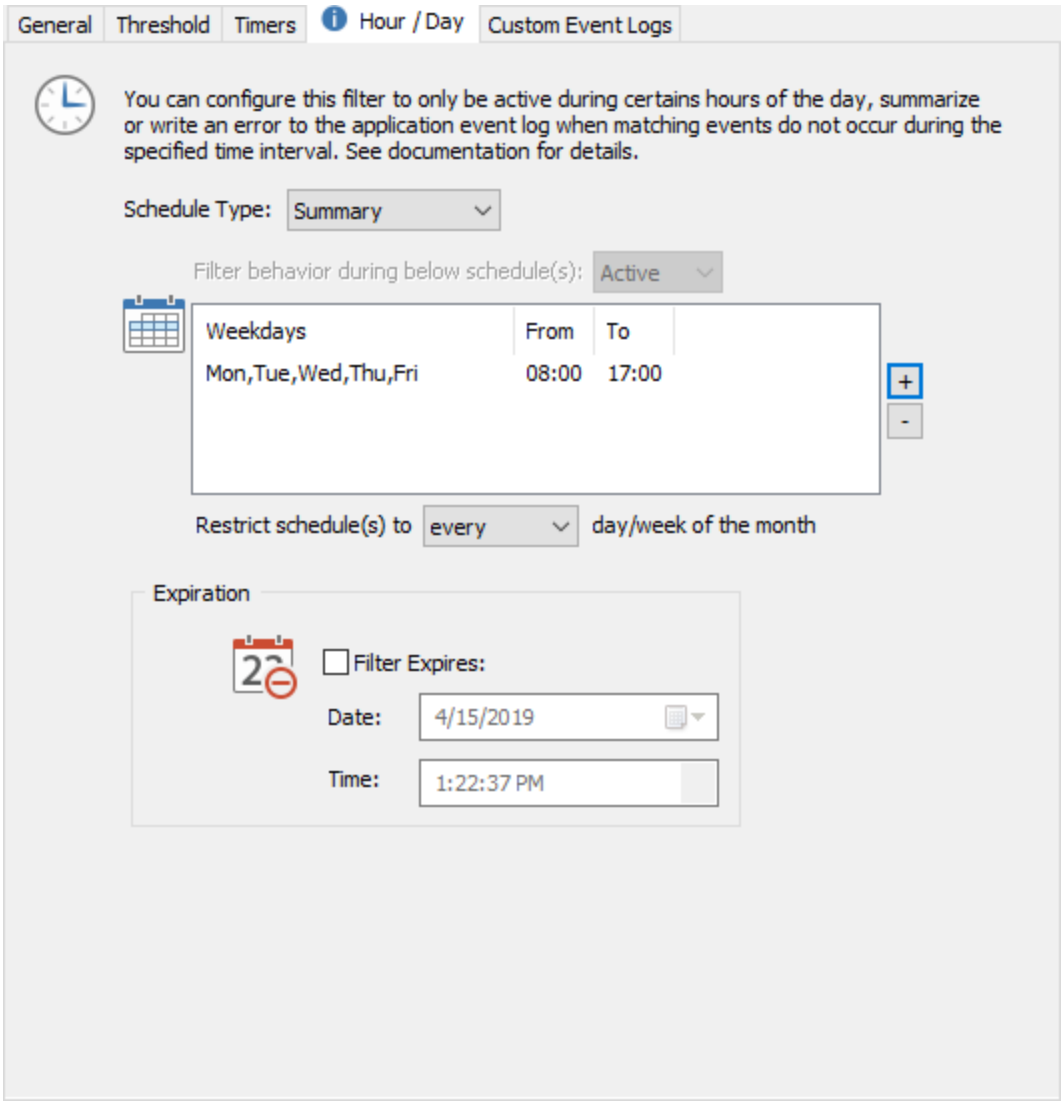
5.3.8.4 Benachrichtigungszusammenfassung

Benachrichtigungszusammenfassungen sammeln und zwischenspeichern Ereignisse, anstatt sie sofort an eine Aktion weiterzuleiten. Wenn der Zeitplan endet, werden alle zwischengespeicherten Ereignisse in einem Stapel an die beabsichtigte Aktion weitergeleitet. Filter mit einem zusammenfassenden Zeitplan werden mit einer kleinen Uhr in der Liste angezeigt. Jobs in den Web Reports werden im Allgemeinen über Zusammenfassungsbenachrichtigungen empfohlen, da sie Ereignisse von mehreren Hosts zusammenfassen können und mehrere Ausgabeformate unterstützen.

Zusammenfassungsfilter können mit jeder Aktion arbeiten, mit Ausnahme der speziellen Einstellung "Alle Aktionen auslösen (Trigger all actions)". Benachrichtigungszusammenfassungen sind an eine bestimmte Aktion gebunden. Es wird nicht empfohlen, mehrere Benachrichtigungszusammenfassungen zu erstellen welche die gleiche Aktion verwenden; stattdessen sollte für jede Benachrichtigungszusammenfassung eine neue Aktion erstellt werden.

Beim Konfigurieren eines zusammenfassenden Zeitplans gibt der aufgelistete Zeitplan den Zeitraum an, in dem Ereignisse gesammelt und zwischengespeichert werden. Die Ereignisse werden an die auf der Registerkarte "Allgemein" aufgelistete Benachrichtigung weitergeleitet, wenn der Zeitplan endet (z.B. 5PM im unten aufgeführten Screenshot).

Der Filter wird kein Ereignis außerhalb der aufgelisteten Liste(n) finden.



Sammelt Ereignisse von Mo-Fr, die zwischen 8 Uhr morgens und 17 Uhr abends stattfinden, und verschickt eine Zusammenfassung per E-Mail Mo-Fr um 17 Uhr

Wie es funktioniert

Wenn ein Ereignis während eines Listenplans eintritt, wird das Ereignis gesammelt. Die gesammelten Ereignisse werden erst dann gesendet wenn der Zeitplan endet.

Beispiel oben: Ereignisse, die zwischen 8.00 und 17.00 Uhr von Mo bis Fr auftreten, werden gesammelt und zwischengespeichert. Jeden Wochentag um 17 Uhr werden die gesammelten Ereignisse an die konfigurierte Aktion weitergeleitet. Ereignisse, die an Wochenenden oder außerhalb des Zeitplans von 8.00-17.00 Uhr auftreten, passen nicht zu diesem Filter und werden daher nicht verarbeitet.

Szenarien der realen Welt

Man kann die Funktion der zusammenfassenden Benachrichtigung in einer Reihe von Szenarien verwenden:

- Erhalten Sie jeden Montagmorgen eine Zusammenfassung per E-Mail

- Senden Sie eine wöchentliche Zusammenfassung per E-Mail an einen Vorgesetzten, die alle Fehlerereignisse der Woche enthält
- Ereignisse nur zweimal täglich in einer Datenbank protokollieren, um Bandbreite von einem Server zu sparen, der über eine langsame Verbindung angeschlossen ist

Dienst-Neustarts

Zusammenfassende Ereignisse werden beibehalten, wenn der EventSentry-Dienst neu gestartet wird. Gesammelte Ereignisse werden in eine temporäre Datei im **temporären** Unterverzeichnis von EventSentry geschrieben und beginnen mit "**eventsentry_summary_**" und werden beim Start des Dienstes verarbeitet.

Beispiele finden Sie im Abschnitt Beispiele für zusammenfassende Benachrichtigungen.

5.3.8.5 Wiederkehrende Ereignisse

Wenn zu erwarten ist, dass Ereignisse regelmäßig auftreten (z.B. ein Backup-Ereignis), dann kann ein Filter für wiederkehrende Ereignisse den Benutzer benachrichtigen, wenn das Ereignis **nicht** eingetreten ist. Um diese Funktion zu aktivieren, setzen Sie den **Zeitplantyp** auf **Wiederkehrendes Ereignis ("Recurring Event")**. Wiederkehrende Filter sind in der Liste mit einem Kreispfeil gekennzeichnet.

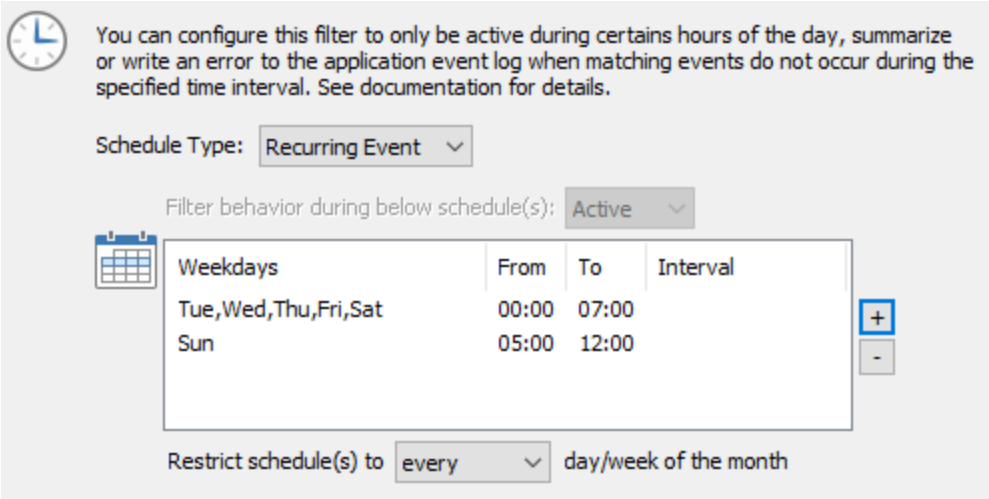
Durch die Aktivierung dieser Funktion wird der Bereich "Aktionen" auf der Registerkarte "Allgemein" deaktiviert. Im Gegensatz zu regulären Filtern **benachrichtigt** ein Filter für wiederkehrende Ereignisse **nicht über eine Aktion**, sondern schreibt ein **Fehlerereignis** in das Anwendungsprotokoll (siehe "Ereignisprotokoll" weiter unten), wenn das/die erforderliche(n) Ereignis(e) im angegebenen Zeitraum nicht erschienen ist/sind. Daher ist es unbedingt erforderlich, dass ein anderer Filter vorhanden ist, der den Benutzer über dieses Fehlerereignis benachrichtigt, z.B. per E-Mail.

Einstellung der Zeiträume

Nachdem Sie die allgemeinen Filtereigenschaften auf der Registerkarte "Allgemein" festgelegt haben, fügen Sie einen oder mehrere Zeitpläne zu der Liste hinzu, wenn das Ereignis eintreten soll. Ein Zeitplan kann entweder ein Zeitrahmen (z.B. Mo, Di von 2 bis 5 Uhr morgens) oder ein Intervall (z.B. alle 10 Minuten) sein.

Wenn das Ereignis während des Zeitrahmens oder Intervalls nicht auftritt, schreibt EventSentry ein Ereignis in das Ereignisprotokoll welches anzeigt, dass der Filter keine Ereignisse gefunden hat.

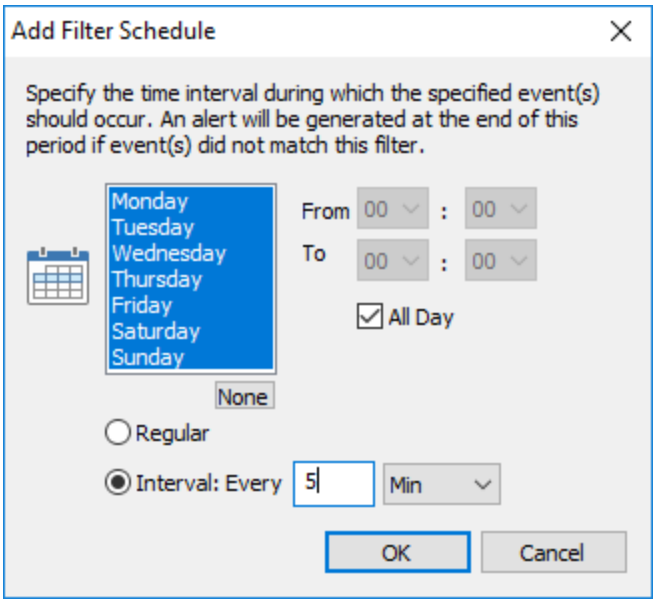
Im Beispiel unten muss ein Ereignis jeden Tag zwischen 12:00 und 7:00 Uhr erscheinen, Dienstags bis Samstags. Am Sonntag muss das Ereignis zwischen 5:00 Uhr morgens und 12:00 Uhr abends erscheinen.



Recurring schedule, e.g. for a backup job that runs daily with different schedules

Intervalle

Statt eines festen Zeitrahmens kann ein wiederkehrender Filter so konfiguriert werden, dass der Filter alle X Minuten oder Stunden übereinstimmen muss. Bei der Einstellung eines Intervalls gelten weiterhin die Einstellungen für Wochentag und "von/bis". Dies ermöglicht eine flexible Konfiguration, bei der Sie ein Intervall nur während bestimmter Stunden des Tages verlangen können.



Filter needs to match every 5 minutes, every day

Ereignisprotokoll

Die folgenden Ereignisprotokollaufzeichnungen werden durch diese Funktion protokolliert:

Ereignis-ID	Beschreibung der Veranstaltung	Beispiel
10620	Kein Ereignis entsprach dem Filter für wiederkehrende Ereignisse.	Im Ereignisprotokoll ist in der konfigurierten Zeitspanne kein Ereignisabgleichsfilter *Backup* aufgetreten. Laut Zeitplan sollte mindestens ein Ereignisabgleichsfilter

		ckup während der letzten 420 Minuten protokolliert worden sein.
10621	Kein Ereignis entsprach dem Filter für wiederkehrende Intervallereignisse.	Im Ereignisprotokoll ist in den letzten 5 Minuten(n) kein Ereignis, das mit dem Filter übereinstimmt, Watchdog aufgetreten. Nach dem Zeitplan sollte alle 5 Minuten(n) mindestens ein Ereignis, das mit dem Ereignisfilter übereinstimmt, als Watchdog protokolliert werden.

5.3.9 Überwachung benutzerdefinierter Ereignisprotokolle

Mit benutzerdefinierten Ereignisprotokollen können Sie Ereignisaufzeichnungen nach ihrer Ereignisquelle kategorisieren und in einem separaten Ereignisprotokoll speichern. Dies kann nützlich sein, wenn Sie Ereignisse nach ihrer Quelle organisieren möchten. Dadurch leiten Sie die Protokolleinträge in ein von Ihnen angegebenes Ereignisprotokoll um.

Unter Vista und später kann die benutzerdefinierte Ereignisprotokoll-Registerkarte auch zur Überwachung von "Anwendungs- und Dienstprotokollen" verwendet werden, z.B. das Ereignisprotokoll "Microsoft-Windows-TaskScheduler/Operational".

Sie können z. B. ein benutzerdefiniertes Ereignisprotokoll namens **Web Server** erstellen**,** das Ereignisse aus den Quellen **IISADMIN**, **SMTPSVC** und **VBRuntime** speichert.

Ereignisse aus diesen angegebenen Quellen werden in eine andere Ereignisdatei geschrieben (und nicht in die Standard-Ereignisprotokolldatei). Benutzerdefinierte Ereignisprotokolldateien werden standardmäßig im Verzeichnis **`%SYSTEMROOT%\SYSTEM32\CONFIG`** gespeichert; am selben Ort, an dem auch die Standardprotokolldateien (Anwendung, Sicherheit, System usw.) gespeichert sind.

EventSentry macht es Ihnen leicht, benutzerdefinierte Ereignisprotokolle zu verwalten, ohne dass Sie die Registrierung manuell manipulieren müssen. EventSentry kümmert sich um die Erstellung aller Registrierungsschlüssel und Registrierungswerte. Es kümmert sich sogar um das Verschieben von Nachrichtendateiinformationen in das benutzerdefinierte Ereignisprotokoll, so dass die Anzeige von Ereignisdetails erwartungsgemäß funktioniert.

Sie können diese benutzerdefinierten Ereignisprotokolle auch mit EventSentry überwachen, das ein Maximum von 30 benutzerdefinierte Ereignisprotokolle (zusätzlich zu den 3-6 Standard-Ereignisprotokollen).

EventSentry unterstützt nicht die Überwachung der Ereignisprotokolle "Forwarded Events" oder "EventCollector". Alle anderen Ereignisprotokolle können in Echtzeit überwacht werden.

5.3.9.1 Verwaltung benutzerdefinierter Ereignisprotokolle

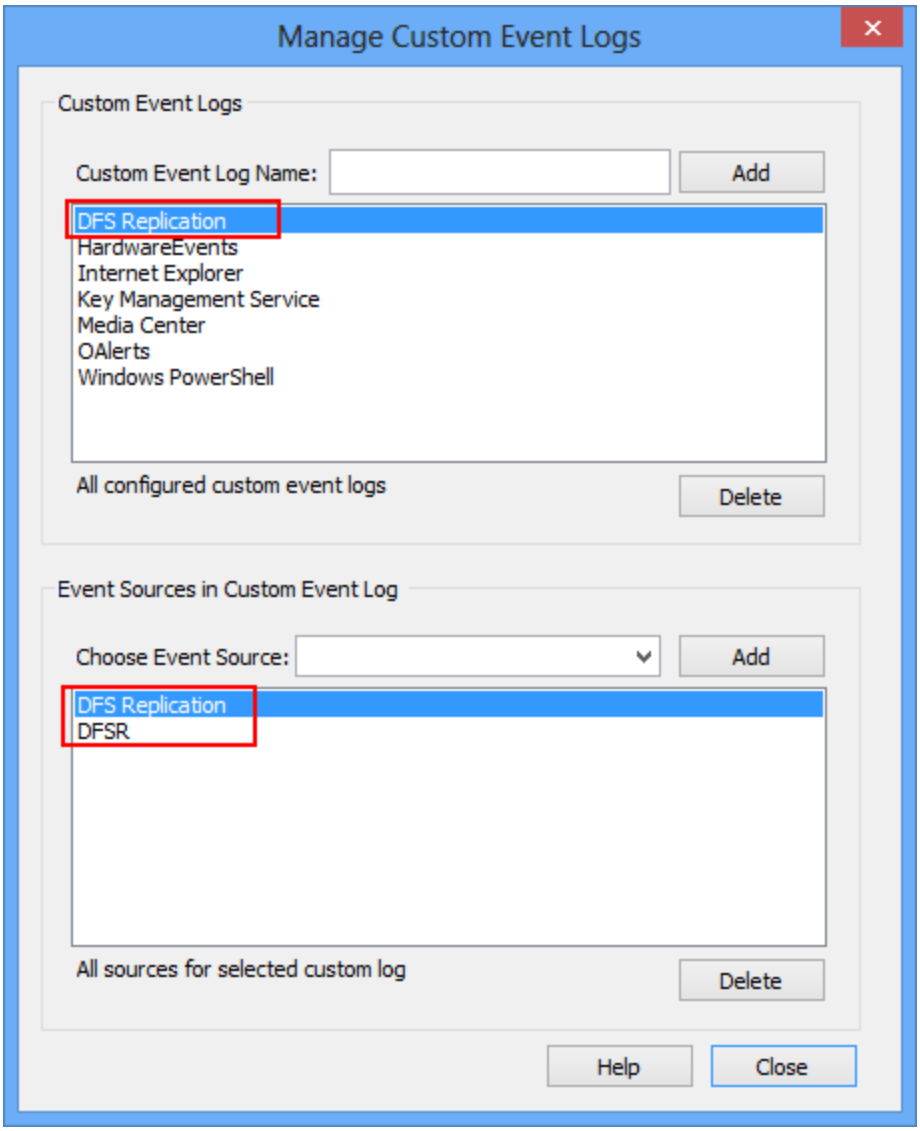
Benutzerdefinierte Ereignisprotokolle können mit dem Dialogfeld **Benutzerdefinierte Ereignisprotokolle verwalten** verwaltet werden. Um dieses Dialogfeld zu öffnen, klicken Sie auf

- **Verwalten Sie benutzerdefinierte Ereignisprotokolle** im Menü **Extras**

oder klicken Sie auf

- **Verwalten Sie die benutzerdefinierten Protokolldateien** auf der Registerkarte Benutzerdefinierte Ereignisprotokolle der Details aller Filter.

Der Dialog zeigt alle benutzerdefinierten Ereignisprotokolle und, nach dem Klicken auf ein benutzerdefiniertes Ereignisprotokoll, die zugehörigen Ereignisquellen an:



Das benutzerdefinierte Ereignisprotokoll 3rd Party Applications hat zwei zugeordnete Ereignisquellen

Erstellen eines benutzerdefinierten Ereignisprotokolls

Geben Sie den Namen des benutzerdefinierten Ereignisprotokolls in das Feld **Name des benutzerdefinierten Ereignisprotokolls** ein und klicken Sie auf die Schaltfläche **Hinzufügen**. Eine benutzerdefinierte Protokolldatei wird vom Betriebssystem automatisch in **%SYSTEMROOT% \ SYSTEM32\ CONFI G** erstellt. Nachdem das benutzerdefinierte Ereignisprotokoll erstellt wurde, können Sie diesem Protokoll Ereignisquellen zuweisen.

Löschen eines benutzerdefinierten Ereignisprotokolls

Um ein benutzerdefiniertes Ereignisprotokoll zu löschen, wählen Sie das Protokoll aus der Liste **Alle konfigurierten benutzerdefinierten Ereignisprotokolle** aus und klicken Sie auf die Schaltfläche

Löschen. Die Protokolldatei selbst kann nach einem Neustart manuell aus dem Verzeichnis %SYSTEMROOT%\SYSTEM32\CONFIG verschoben oder gelöscht werden.

Beim Löschen eines benutzerdefinierten Ereignisprotokolls werden alle zugehörigen Ereignisquellen entfernt. Um den Verlust von Meldungsdateiinformationen zu vermeiden, entfernen Sie alle zugehörigen Ereignisquellen manuell aus dem betroffenen Protokoll (siehe unten), bevor Sie das benutzerdefinierte Protokoll selbst entfernen.

Verknüpfen einer Ereignisquelle mit einem benutzerdefinierten Ereignisprotokoll

Benutzerdefinierte Ereignisprotokolle funktionieren nur, wenn Sie Ereignisquellen mit ihnen verknüpfen. Die verknüpften Ereignisquellen werden dann in die benutzerdefinierte Protokolldatei und nicht in eine der Standardprotokolldateien geschrieben.

Sie können entweder

1. **neue Ereignisquellen** mit dem benutzerdefinierten Protokoll (z.B. wenn Sie eine (Web-) Anwendung entwickeln, die sich in das Ereignisprotokoll einloggen wird)
2. **vorhandene Ereignisquellen** aus einem anderen Ereignisprotokoll (z.B. Anwendung) zuordnen

1. Neue Ereignisquellen

Wenn Sie beabsichtigen, neue Ereignisquellen zu erstellen, dann ist nur der Registrierungsschlüssel

HKLM\System\CurrentControlSet\Dienste\Eventlog\Ihr Kundenlog\Ihre Neue Quelle

erstellt werden. Sie müssen eine Nachrichtendatei-DLL manuell registrieren, wenn Sie beabsichtigen, eine solche zu verwenden.

2. Vorhandene Ereignisquellen

Sie können eine der bereits registrierten Ereignisquellen auswählen und sie zum benutzerdefinierten Ereignisprotokoll hinzufügen. EventSentry kopiert die erforderlichen Registrierungsinformationen 1:1 in das benutzerdefinierte Ereignisprotokoll. Dies hat den Vorteil, dass die Verknüpfungen der Nachrichtendateien erhalten bleiben und Probleme mit der Ereignisanzeige vermieden werden.

Um eine Ereignisquelle mit einem benutzerdefinierten Ereignisprotokoll einfach zu erstellen/zuzuweisen:

- Wählen Sie das benutzerdefinierte Ereignisprotokoll (falls nicht bereits ausgewählt)
- Geben Sie den Namen der Ereignisquelle neben **Ereignisquelle auswählen** ein oder wählen Sie ihn aus der Liste
- Klicken Sie auf Hinzufügen

Löschen einer Ereignisquelle

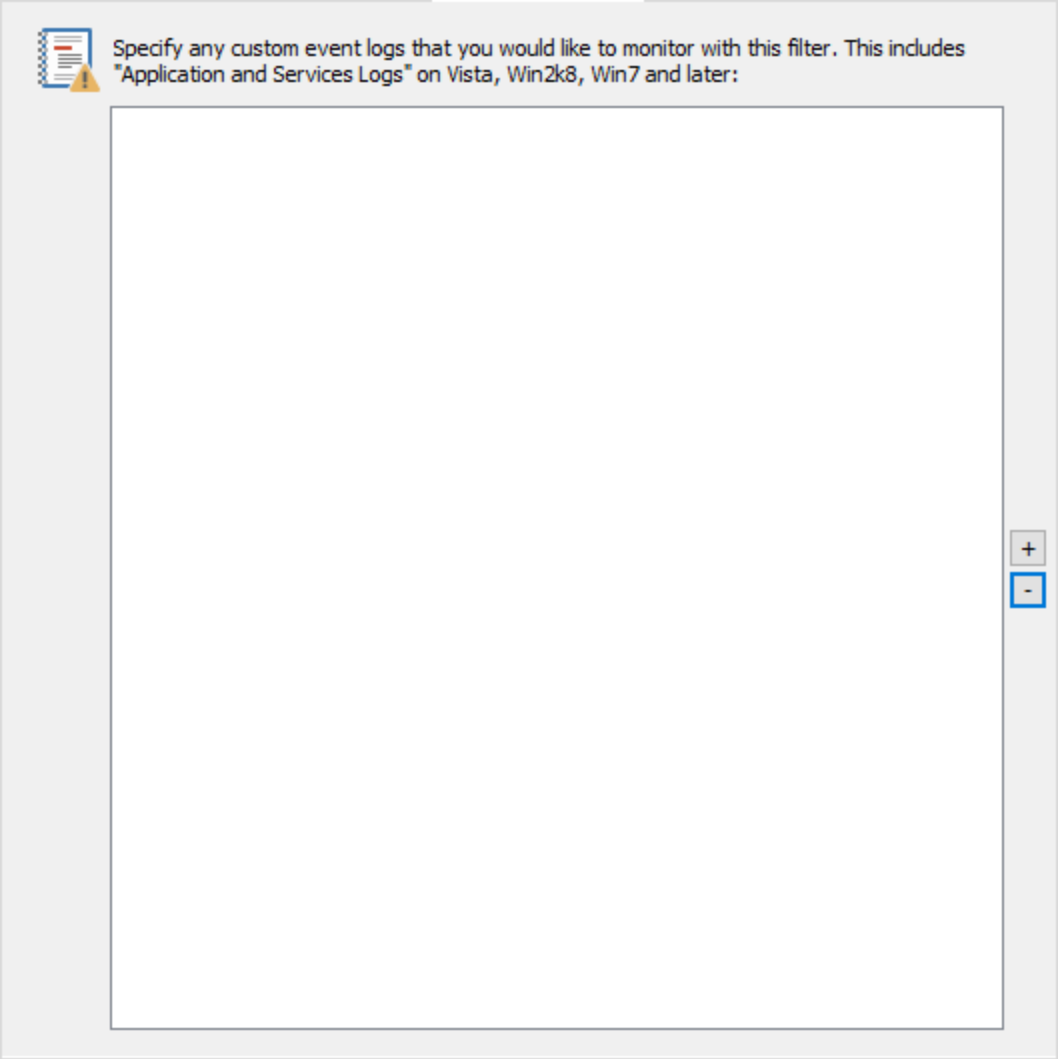
So löschen Sie einfach eine Ereignisquelle oder verknüpfen sie erneut mit einem Standard-Ereignisprotokoll:

- Wählen Sie das benutzerdefinierte Ereignisprotokoll (falls nicht bereits ausgewählt)
- Wählen Sie die zu entfernende Ereignisquelle
- Klicken Sie auf Löschen

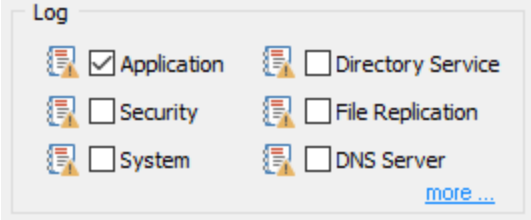
Sie haben dann die Möglichkeit, die Ereignisquelle mit einem der Standard-Ereignisprotokolle (Anwendung, Sicherheit, ...) neu zuzuweisen.

5.3.9.2 Überwachung benutzerdefinierter Ereignisprotokolle

EventSentry can monitor up to 30 custom event logs. From the **Custom Event Logs** dialog in filter details, select your custom event logs to monitor:



Monitoring custom event logs is no different than monitoring the default event logs



except that you have to choose the names of the custom event logs. After you have selected the appropriate custom event logs (on a global basis) you can then configure EventSentry to monitor one or more of these custom logs on a per filter basis.

5.4 Logdateien

EventSentry kann jede beliebige Protokolldatei überwachen und Inhalte auf der Grundlage der von Ihnen aufgestellten Regeln verarbeiten. Sie können z.B. alle Zeilen aus einer Protokolldatei in Ihrer Datenbank speichern und/oder ausgewählte Inhalte in das Anwendungsereignisprotokoll protokollieren.

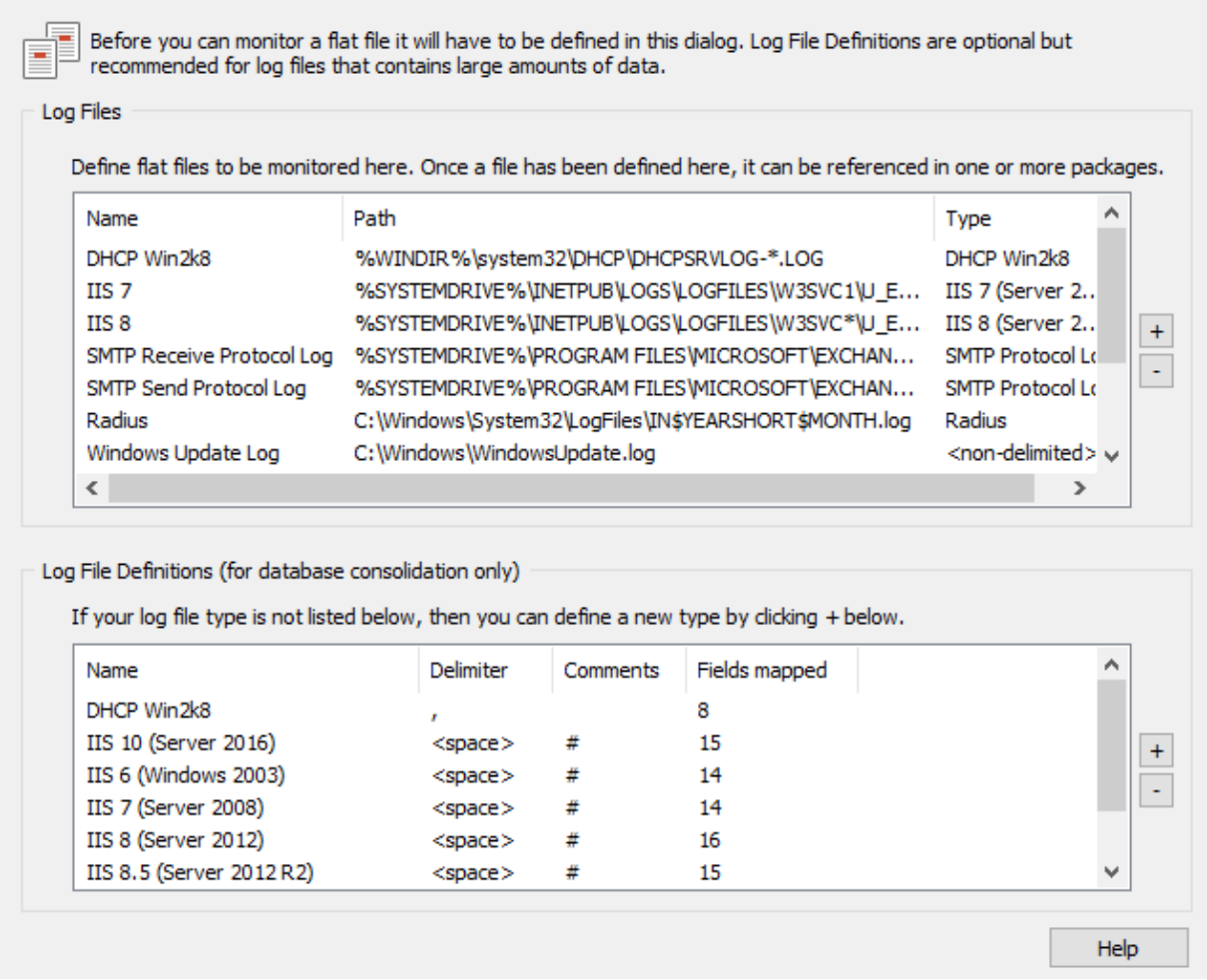
Voraussetzungen

Ähnlich wie bei der Überwachung von Ereignisprotokollen werden beim Start des EventSentry-Agenten vorhandene Dateien **nicht** erneut gescannt. Daher werden nur neue Zeilen geparst, die der/den Monitor-Protokolldatei(en) hinzugefügt werden.

Log-Datei-Typen

Bei der Überwachung von Logdateien unterscheiden wir zwischen

- Einfachen Protokolldateien (ohne Formatierung)
- Formatierte Protokolldateien (z.Bsp. CSV)



Protokolldateien werden in Echtzeit überwacht, und jedes Mal, wenn der Protokolldatei eine oder mehrere neue Zeilen (abgeschlossen mit einem konfigurierbaren Neuzeilenzeichen) hinzugefügt werden, werden diese von EventSentry verarbeitet.

Einfache Protokolldateien

Einfache Protokolldateien sind Dateien, die keinem bestimmten Muster folgen und keine Trennzeichen enthalten. Bei der Konsolidierung dieser Dateien speichert EventSentry einfach jede Zeile (gemäß Ihren Regeln) in der Datenbank für spätere Analyse und Archivierungszwecke. Beispiele für nicht einfache Protokolldateien sind etliche Protokolldateien von Windows (windowsupdate.log, setupapi dev log) und von Entwicklungswerkzeugen erzeugte Debug-Dateien.

Einfache Protokolldateien sind am einfachsten zu konfigurieren, erlauben aber keine Sortierung oder Gruppierung in den Web-Reports.

Formatierte Protokolldateien

Hier handelt es sich um Dateien, die einem voreingestellten Format folgen, bei dem jede Zeile aus einer Reihe von Feldern besteht, die mit einem gemeinsamen Trennzeichen, z.B. einem Semikolon, abgegrenzt sind. Bei der Konsolidierung dieser Protokolldateien speichert EventSentry jedes Feld separat in der Datenbank und ermöglicht es Ihnen, Informationen auf verschiedene Weise zu suchen und anzuzeigen, z.B. durch Gruppierung der Ausgabe nach einem bestimmten Feld.

Formatierte Protokolldateien erfordern eine Dateidefinition, damit EventSentry weiß, wie jede Zeile analysiert werden muss. Das Einrichten von Dateidefinitionen ist einfach, wenn eine der vordefinierten Vorlagen (z.B. IIS, DHCP) verwendet wird, kann aber zeitaufwendiger sein, wenn Sie einen Dateityp überwachen müssen, für den keine Definitionen vorhanden sind.

Das Einrichten von Dateidefinitionen für formatierte Protokolldateien ist nur bei der Konsolidierung von Inhalten in einer Datenbank erforderlich. Wenn Sie nur ausgewählte Zeilen in das Ereignisprotokoll protokollieren wollen, dann können auch formatierte Protokolldateien wie einfache Protokolldateien behandelt werden.

Schritte zur Überwachung einer Protokolldatei

1. Nur formatierte Dateien: Erstellen einer Dateidefinition wenn keine existiert
2. Definieren der überwachte(n) Datei(en)
3. Erstellen & Zuweisen eines Protokolldateipakets
4. Spezifizieren der Konsolidierungs- und Überwachungsoptionen

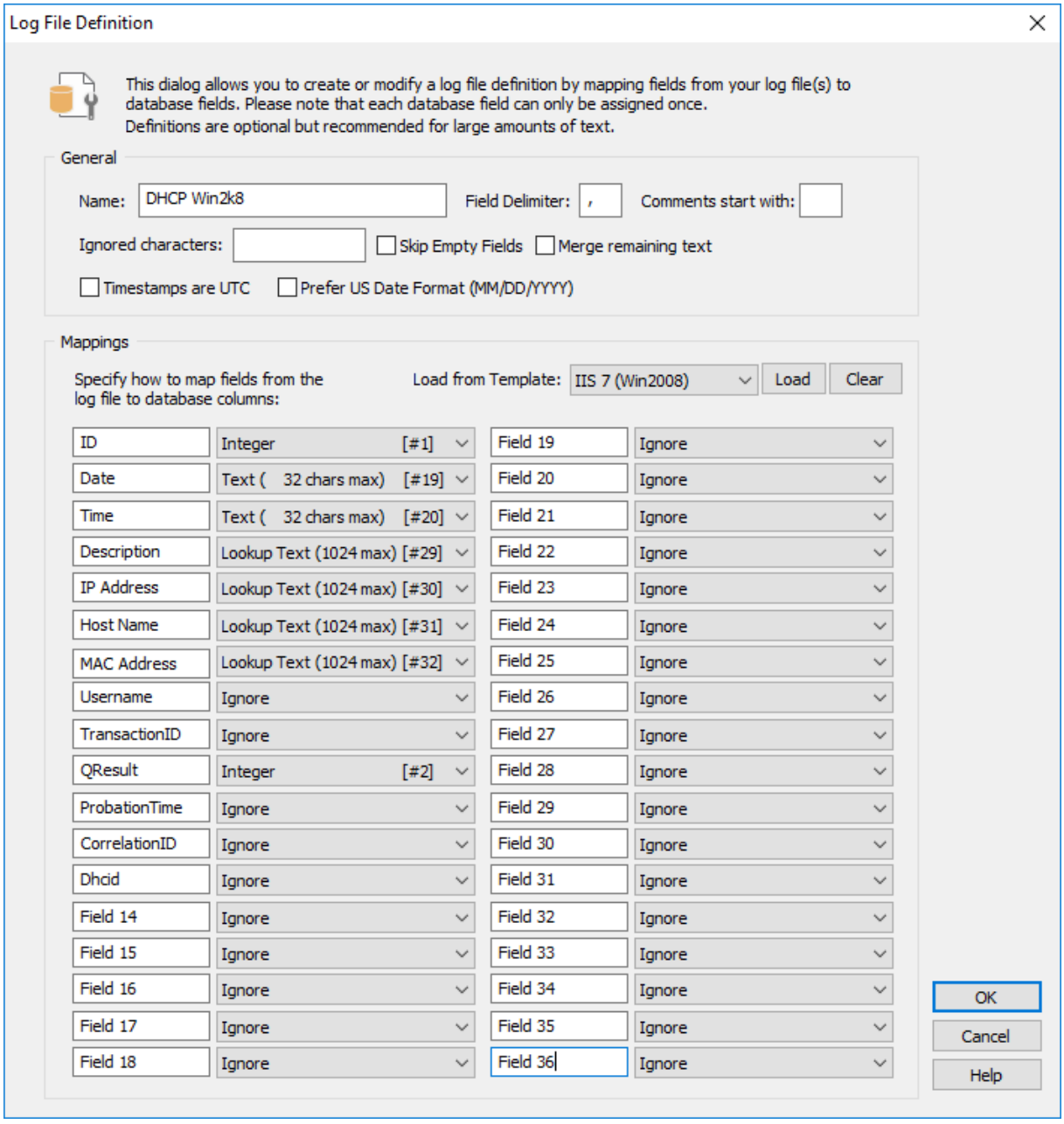
5.4.1 Datei-Definitionen erstellen

Dieses Kapitel trifft nur auf formatierte Protokolldateien zu.

Da formatierte Protokolldateien einem vordefinierten Muster folgen, müssen Sie das Layout der abgegrenzten Protokolldatei in EventSentry spiegeln, so dass EventSentry weiß, wie die Protokolldatei analysiert und aufgeteilt werden muss, wenn es Informationen in der Datenbank konsolidiert. Sobald eine Protokolldatei-Definition erstellt wurde, kann sie auf eine oder mehrere Protokolldateien angewendet werden (siehe nächster Abschnitt).

Die Überwachung formatierter Protokolldateien hat den Vorteil, dass Sie Suchvorgänge durchführen und Berichte auf der Grundlage der verfügbaren Felder in der Protokolldatei erstellen können. Wenn Sie z.B. eine IIS-Protokolldatei überwachen, können Sie die am häufigsten protokollierten IP-Adressen in einem Bericht anzeigen.

Um eine neue Dateidefinition zu erstellen oder eine vorhandene zu bearbeiten, klicken Sie mit der rechten Maustaste auf den Container **Log File Packages** und wählen Sie **Files and Files Types**. Der Bereich **Protokolldatei-Definitionen** zeigt Ihnen alle derzeit konfigurierten Dateidefinitionen an und ermöglicht es Ihnen, neue Definitionen hinzuzufügen.



Um eine neue Definition hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**, wodurch das Dialogfeld **Protokolldateidefinition** angezeigt wird. Sie können auch eine vorhandene Definition bearbeiten, indem Sie auf eine Definition aus der Liste doppelklicken. Das Dialogfeld ist in zwei Hauptabschnitte unterteilt - "Allgemein" und "Zuordnungen" - die beide erforderlich sind.

Allgemein

Option	Beschreibung / Erläuterung	Beispiel

Name	Name der Definition	Firewall-Protokoll
Zeilentrennzeichen	Konfiguriert das Zeilenende (\r\n) von den Protokolldateien, in den meisten Fällen sollte hier **Windows** ausgewählt werden. Wenn Protokolldateien von einem Linux/Server importiert werden, oder das Zeilenende Unix (\n) enspricht, dann sollte hier Unix ausgewählt werden.	Windows
Trennzeichen	Das Zeichen, durch das Felder in der Protokolldatei getrennt werden	;
Kommentare beginnen mit	Zeilen, die mit dem angegebenen Zeichen beginnen, werden ignoriert	#
Folgende Zeichen ignorieren	Alle hier angegebenen Zeichen werden aus der aktuellen Zeile entfernt, bevor sie analysiert wird.	()[]
Leere Felder überspringen	Leere Felder ignorieren, hat den gleichen Effekt wie das Setzen einzelner Felder auf "Ignorieren". Die Verwendung dieser Option kann bei Protokolldateien, die viele leere Felder enthalten, einfacher zu konfigurieren sein als die Verwendung von "Ignorieren".	
Restlichen Text zusammenführen	Standardmäßig ordnet EventSentry nur Felder zu, die zugeordnet sind. Wenn die Protokolldatei mehr Felder enthält, werden diese ignoriert. Wenn Sie diese Option aktivieren, werden alle verbleibenden Felder am Ende der Zeile zusammengeführt und an das letzte zugeordnete Feld angehängt. Dies ist normalerweise nur für Protokolldateien sinnvoll, die eine variable Anzahl von Feldern enthalten, die selten benutzt werden, aber dennoch konsolidiert werden sollten.	
Zeitstempel sind UTC	Zeigt an, dass der Zeitstempel in UTC protokolliert wird (im Gegensatz zur lokalen Zeit)	2019-02-25 18:00:01
US-Datumsformat bevorzugen	Aufgrund der unterschiedlichen Datumsformate, die weltweit verwendet werden (MM/DD vs. DD/MM), ist es dem Agenten nicht immer möglich, das Datumsformat automatisch zu erkennen. Wenn das Datumsformat in einer Protokolldatei im US-Datumsformat (Monat vor dem Tag) vorliegt, wird empfohlen, dieses Kästchen anzukreuzen	

Zuordnungen

Der Abschnitt Zuordnungen ermöglicht es EventSentry mitzuteilen, wie die Struktur der Protokolldatei aussieht, so dass EventSentry die Datei korrekt analzsieren und die einzelnen Felder ihren jeweiligen Datentypen zuordnen kann. Lassen Sie sich nicht von der Anzahl der Felder im Dialogfeld einschüchtern, dieses Kapitel erklärt, wie man eine neue Zuordnung von Grund auf erstellt.

Verwendung von Vorlagen

Wenn eine Dateidefinition bereits im Abschnitt "Laden aus Vorlage" aufgeführt ist, wird dringend empfohlen, die Definition aus der Pulldown-Liste auszuwählen und auf **Laden** zu klicken, um die Zuordnungen vorzufüllen. Sobald die Zuordnungen angezeigt werden, vergleichen Sie sie mit der Protokolldatei, die Sie überwachen wollen und stellen Sie sicher, dass die Zuordnungen aus der Temporärdatei mit dem Inhalt der Datei übereinstimmen. Einige Anwendungen enthalten ein Standardprotokollformat, das angepasst werden kann. Es ist daher wichtig, dass Sie die Zuordnungen anpassen, wenn das Standardformat geändert wurde.

Der beste Weg eine Protokolldatei abzubilden, ist das Öffnen der Protokolldatei in einem Tabellenkalkulationsprogramm wie Microsoft Excel oder OpenOffice Calc. Auf diese Weise können Sie

die Datei in Felder konvertieren und jede Zeile, die in die einzelnen Felder aufgeteilt ist, leicht erkennen. Wenn Sie kein Tabellenkalkulationsprogramm zur Verfügung haben, können Sie die Protokolldatei einfach in einem Texteditor wie Notepad öffnen.

Wenn Sie ein klares Bild von den verfügbaren Feldern in der Protokolldatei haben, können Sie von links beginnend entscheiden, wie Sie die einzelnen Felder abbilden wollen. Für jedes der in der Protokolldatei verfügbaren Felder müssen die folgenden Schritte durchgeführt werden:

1. Geben Sie eine Beschreibung des Feldes an
2. Zuordnung des Feldtyps zu einem der verfügbaren Datenbank-Datentypen

1. Feld Beschreibung

Die Angabe einer Feldbeschreibung hilft bei der Analyse der Protokolldatei über die EventSentry-WebReports. Anstatt die Standardbeschreibung "Feld XX" beizubehalten, geben Sie einen passenden Feldnamen ein, z.B. "Quell-IP" oder "Übertragene Bytes". Diese Informationen werden dann in der Suchausgabe und in den Berichten angezeigt. Sie finden diese Informationen entweder im Header der Protokolldatei oder in der Anwendung welche die Protokolldatei erzeugt.

2. Mapping auf einen Datenbank-Datentyp

Nachdem Sie die Feldbeschreibung eingegeben haben, können Sie den Feldinhalt auf einen Datentyp abbilden. Welche Datenbanktypen für die Verwendung zur Verfügung stehen, entnehmen Sie bitte der folgenden Tabelle. Beachten Sie, dass für jeden Typ nur eine begrenzte Anzahl von Feldern zur Verfügung steht. Wenn Sie z. B. einmal den Datentyp "**Integer** [**#1**]" für ein Feld verwendet haben, können Sie ihn nicht mehr verwenden und müssen "**Integer** [**#2**]" verwenden, wenn Sie das nächste Mal ein Feld dem Typ Integer zuordnen wollen.

Please see the table below to see which types are available for use:

	Maximum Length	Maximum Usage Count	Best Use
Ignore	n/a	unlimited	Feld ignorieren
Integer	0 - 2147483647	18	Zahlen
Text (32 chars max)	32 characters	4	Für kurzen Text, der in den meisten Zeilen der Protokolldatei eindeutig ist (keine oder wenig Wiederholungen)
Text (512 chars max)	512 characters	4	Für längeren Text, der in den meisten Zeilen der Protokolldatei eindeutig ist (keine oder wenig Wiederholungen)
Text (1024 chars max)	1024 characters	2	Für langen Text, der in den meisten Zeilen der Protokolldatei eindeutig ist (keine oder wenig Wiederholungen)
Lookup Text	1024 characters	8	Für langen Text welcher oft wiederholt wird
Date / Time	n/a	2	Für Text der entweder ein Datum oder eine Uhrzeit darstellt (siehe unten für weitere Informationen)

Text oder Lookup Text?

Während der Unterschied zwischen den Feldtypen "Ignorieren" und "Ganzzahl" relativ einfach zu verstehen, ist es weniger offensichtlich, ob Sie den Datentyp "Text ..." oder "Lookuptext" für ein Textfeld verwenden sollten.

Verwenden Sie diese Regel: Wenn der Text des Feldes weiterhin durch die Protokolldatei(en) hindurch angezeigt wird, z.B. eine IP-Adresse in einer Firewall-Protokolldatei, dann sollten Sie den Datentyp "Lookup-Text" verwenden. Text dieses Typs wird **nur einmal** in einer zentralen Nachschlagetabelle gespeichert, wodurch Speicherplatz in der Datenbank gespart wird und Sie die Ausgabe in den Berichten nach dem Feld gruppieren können. Wenn es sich bei dem Feld beispielsweise um die IP-Adresse interner Hosts aus einer Firewall-Protokolldatei handelt, können Sie einen Bericht anzeigen lassen, der zeigt, wie viele Zeilen vom Computer durch die Firewall protokolliert wurden!

Wenn dagegen der Text des Feldes für fast jede Zeile eindeutig ist (z.B. eine Checksumme, Anmelde-ID), dann ordnen Sie den Text am besten einer regulären Textart zu. Es würde keinen Sinn machen, eine Lookuptabelle mit Werten zu füllen, die sich millionenfach ändern.

Datum/Uhrzeit

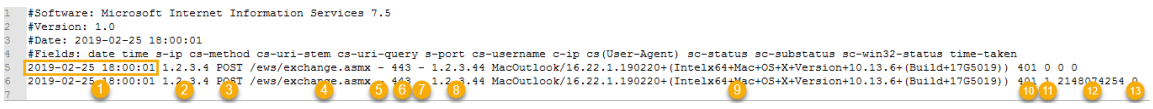
Anstatt Zeitstempel als String-Werte zu speichern, können gängige Datums-/Zeitformate geparst und in einen Zeitstempelwert konvertiert werden, wenn einer der folgenden Punkte für das ausgewählte Feld (Spalte) in der Protokolldatei zutrifft:

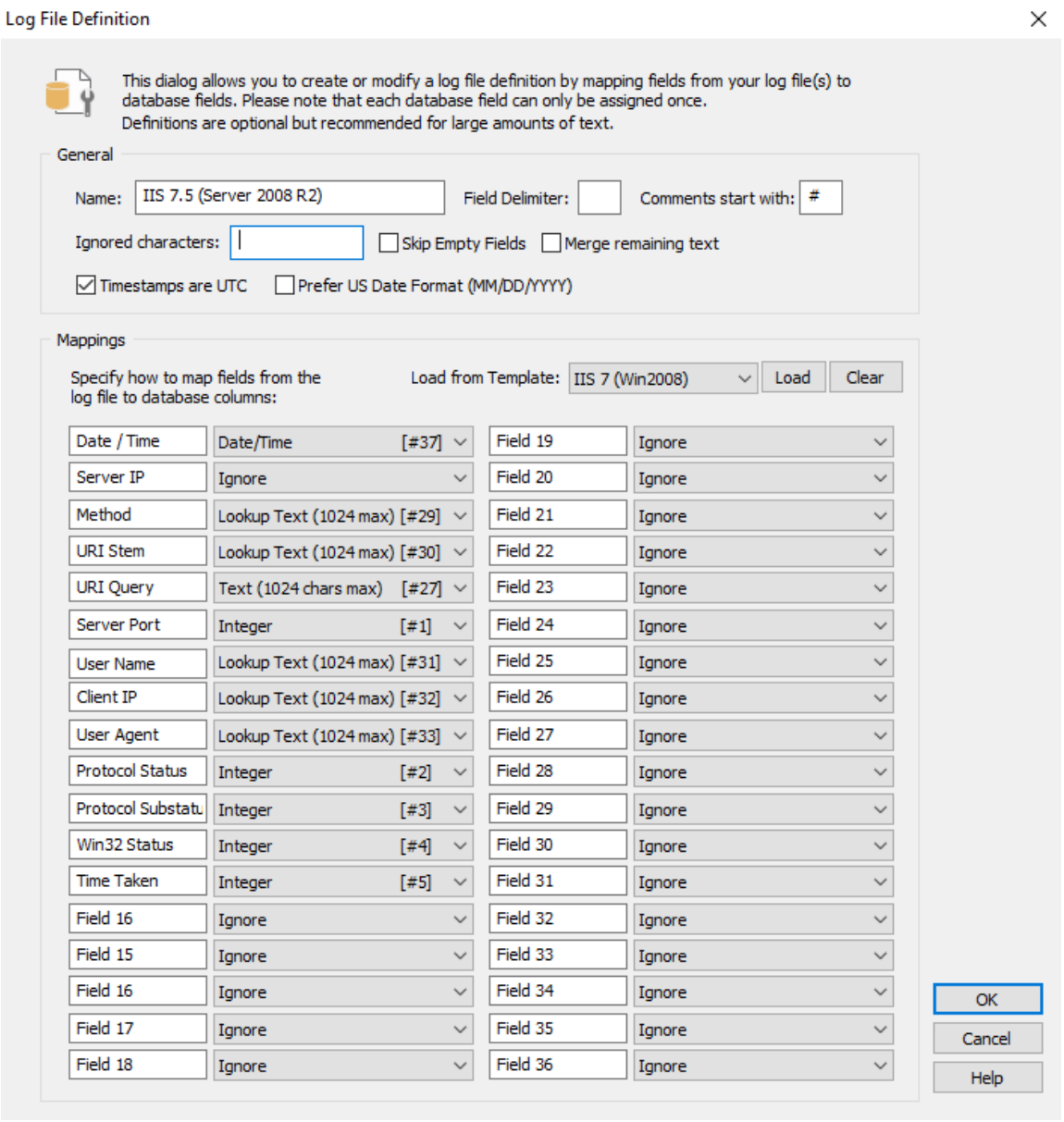
- Der Zeitstempel enthält das Datum **und die** Uhrzeit
- Der Zeitstempel enthält nur das Datum, aber das Feld unmittelbar nach dem Datum enthält die Uhrzeit (siehe Bildschirmfoto unten)

Wenn die Spalte einer Protokolldatei, die als **Datum/Uhrzeit** markiert ist, nur ein Datum (ohne die Uhrzeit) enthält, holt EventSentry die Uhrzeit aus der nächsten Spalte, indem es die beiden Spalten zusammenführt. Wenn also eine Protokolldatei Datum und Uhrzeit in getrennten Spalten protokolliert, ist nur eine einzige Datum/Uhrzeit-Definition erforderlich.

Das Parsen nur eines Datums (z.B. 12/1/2019) oder nur einer Uhrzeit (z.B. 15:03:44) wird nicht unterstützt; unvollständige Datumsangaben erfordern einen Feldtyp im Textstil (Text oder Nachschlagetext).

Die Bildschirmkopie unten zeigt eine Protokolldatei, in der Datum und Zeit in zwei Spalten aufgeteilt sind, die entsprechende Definition der Protokolldatei ist unten dargestellt:





5.4.2 Überwachte Dateien definieren

Sobald Sie eine Dateidefinition erstellt haben oder falls nur einfache Dateien überwacht werden, müssen die eigentlichen Dateien, die überwacht werden sollen, konfiguriert werden. EventSentry unterstützt Variablen und Platzhalter für Protokolldateien, die dynamische Zeichenfolgen wie Datum, Uhrzeit und Sequenznummern enthalten.

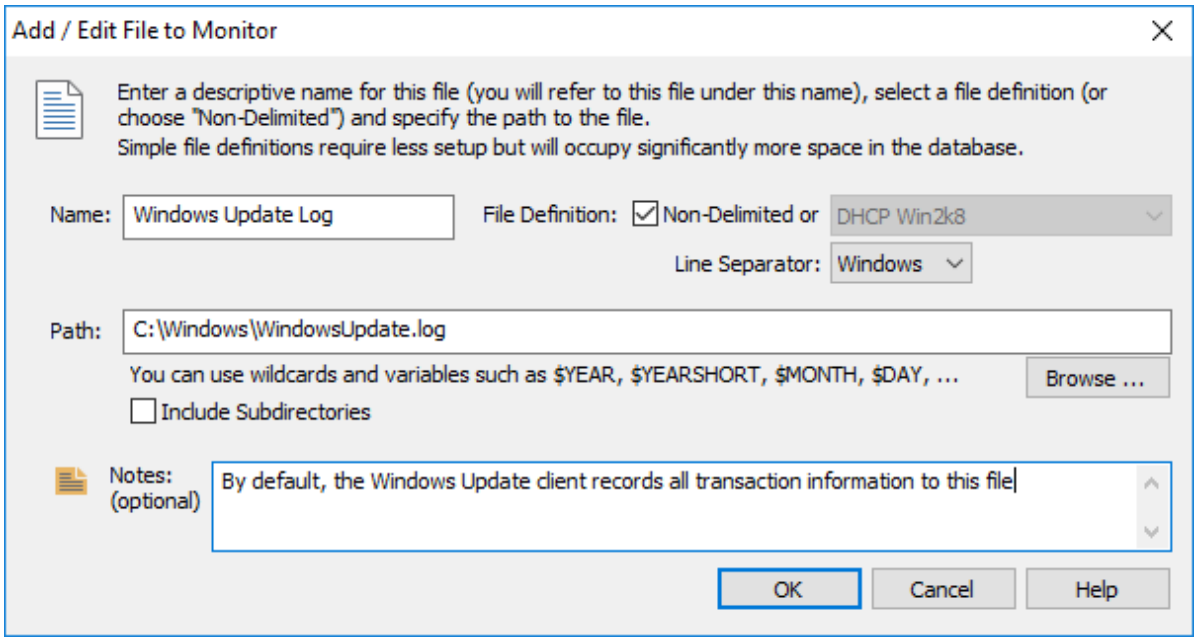
Wenn Sie eine neue Datei hinzufügen, müssen Sie auf den Pfad der Protokolldatei verweisen (Variablen und Platzhalter werden unterstützt), einen eindeutigen Namen für die Protokolldatei wählen und angeben ob es sich um eine formatierte Protokolldatei (einschließlich des Dateityps) oder um eine einfache Protokolldatei handelt.

Um eine neue Dateidefinition zu erstellen oder eine vorhandene zu bearbeiten, klicken Sie mit der rechten Maustaste auf den Container **Log File Packages** und wählen Sie **Files and Files Types**. Der

Dateibereich zeigt Ihnen alle derzeit konfigurierten Dateien an und ermöglicht Ihnen die Angabe neuer Dateien.

Überwachung einer neuen Protokolldatei

Klicken Sie auf die Schaltfläche **Hinzufügen**, um das Dialogfeld **Add / Edit File to Monitor** aufzurufen.



Name

Geben Sie einen beschreibenden Namen für die Protokolldatei an. Geben Sie z.B. *Firewall Log File* ein, wenn Sie die Log-Datei Ihrer Firewall überwachen.

Datei-Definition

Wenn Sie eine nicht abgegrenzte Datei überwachen, markieren Sie das Kontrollkästchen "Non-Delimited". Andernfalls wählen Sie die Dateidefinition aus dem Pulldown-Menü. Wenn eine geeignete Definition nicht in der Liste enthalten ist, müssen Sie eine neue Dateidefinition erstellen.

Pfad

Geben Sie den vollständigen Pfad zur Protokolldatei an. Da Protokolldateien normalerweise dynamische Zeichenfolgen wie das aktuelle Datum, die Datei usw. enthalten, können Sie Variablen und/oder Platzhalter in den Pfadnamen aufnehmen. Die folgenden Variablen und Wildcards werden unterstützt:

Character/Name	Typ	Beschreibung
*	Wildcard	entspricht keinem oder mehr Zeichen
?	Wildcard	entspricht einem einzelnen Zeichen
$YEAR	Variable	4-stellige Jahreszahl
$YEARSHORT	Variable	2-stellige Jahreszahl
$MONTH	Variable	2-stelliger Monat
$DAY	Variable	2-stelliger Tag
$HOUR	Variable	2-stellige Stunde (24-Stunden-Format)
$MINUTE	Variable	2-stellige Minute

Da Sie sowohl Platzhalter als auch Variablen verwenden können, können Sie den Dateinamen Ihrer Protokolldateien oft auf zwei verschiedene Arten angeben - entweder durch Verwendung von Platzhaltern oder durch Verwendung von Variablen. In der Tabelle unten finden Sie Beispiele für die Zuordnung von Dateinamen:

Filename	Filename	Filename	Filename
ntbackup01.log	ex070501.log	ex070501.log	20070110232333 Mar 15, 2007 12.33 PM.txt
ntbackup02.log	ex070502.log	ex070502.log	20070340242343 Mar 16, 2007 12.35 PM.txt
ntbackup03.log	ex070503.log	ex070503.log	20070139619433 Mar 15, 2007 12.37 PM.txt
ntbackup*.log	**ex$YEARSHORT$MONTH$DAY.log**	**ex*.log**	**$YEAR*$DAY, $YEAR*.txt**

Wie aus der 2. und 3. Spalte ersichtlich ist, kann der Name der Protokolldatei manchmal auf unterschiedliche Weise angegeben werden.

Unterverzeichnisse einbeziehen
Dateien in Unterverzeichnissen können durch Markieren dieses Kästchens überwacht werden. Bei der Überwachung von Dateien in Unterverzeichnissen kann der Pfad auf verschiedene Arten angegeben werden:

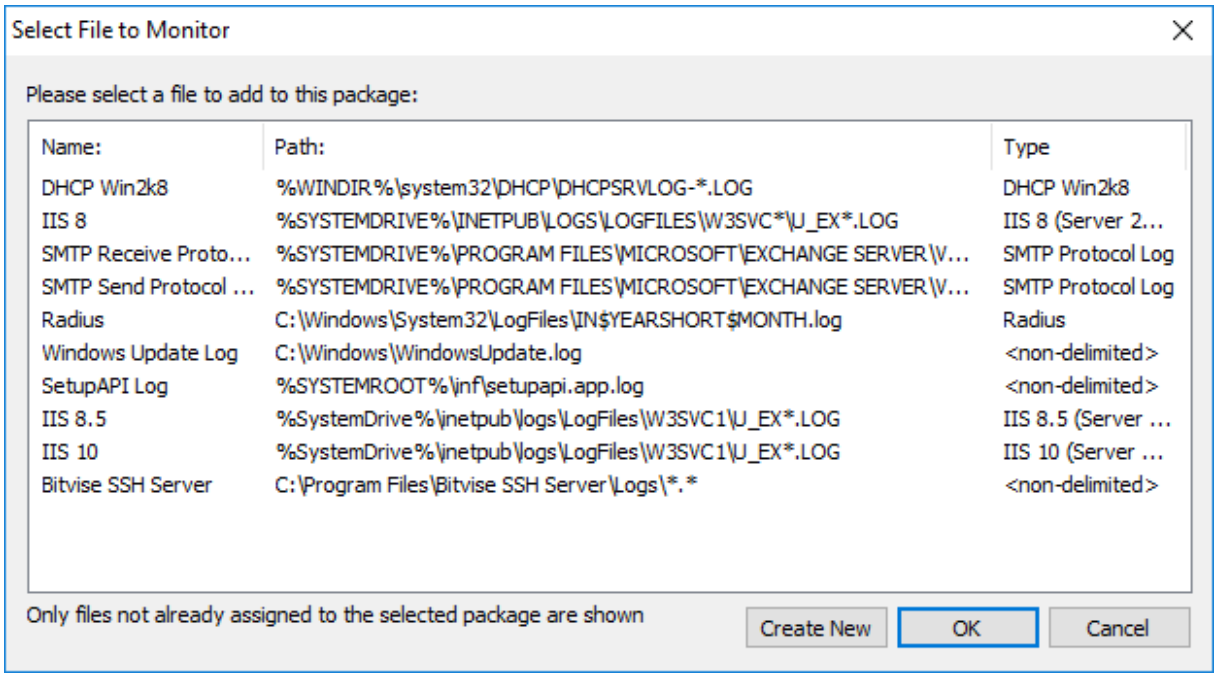
Pfad	Überwachte Dateien
C:\LogFiles*.log	Überwacht alle Dateien mit der Erweiterung .log im Ordner C:\LogFiles sowie Unterverzeichnisse
C:\LogFiles**.log	Überwacht alle Dateien mit der Erweiterung .log in einem beliebigen Unterverzeichnis des Ordners C:\LogFiles (und **nicht** im Hauptordner C:\LogFiles)
C:\inetpub\logs\LogFiles\W3SVC*\u_*.log	Überwacht alle Dateien, die mit dem **u_*.**log-Muster übereinstimmen, in jedem Unterverzeichnis von **C:\inetpub\logs\LogFiles**, das mit dem W3SVC*-Muster übereinstimmt.

Hinweise
Sie können Notizen verwenden, um anzugeben, welche Anwendung die Protokolldatei oder andere Beschreibungen erzeugt.

5.4.3 Hinzufügen von Dateien zu einem Protokolldatei-Paket

Ein Logdatei-Paket enthält eine oder mehrere überwachte Dateien und kann global oder einzelnen Computern oder Gruppen zugeordnet werden. Um ein neues Logdatei-Paket zu erstellen, klicken Sie mit der rechten Maustaste auf den Container **Logdatei-Pakete**, wählen Sie **Paket hinzufügen** und geben Sie einen Namen für das neue Paket ein.

Um eine Datei zu diesem Paket hinzuzufügen, klicken Sie mit der rechten Maustaste auf das Protokolldatei-Paket und wählen Sie **Datei hinzufügen**. Daraufhin erscheint das Dialogfeld "Select File to Monitor", das alle Dateien anzeigt, die zu diesem Protokolldatei-Paket hinzugefügt werden können. Dateien, die bereits im Protokolldatei-Paket enthalten sind, werden im Dialogfeld nicht angezeigt. Um eine Datei hinzuzufügen, wählen Sie sie aus und klicken Sie auf die Schaltfläche OK.



Die ausgewählte Datei erscheint unter dem Protokolldateipaket, dem sie hinzugefügt wurde, und kann durch Klicken auf den Dateinamen bearbeitet werden.

Entfernen oder Deaktivieren von Protokolldateien

Um eine Datei aus der Überwachung zu entfernen, klicken Sie mit der rechten Maustaste auf die Datei unter dem Protokolldatei-Paket und wählen Sie "Löschen". Dadurch wird die Datei aus dem ausgewählten Paket entfernt. Sie können auch mit der rechten Maustaste auf das Paket klicken und "Deaktivieren" wählen, um zu verhindern, dass die Datei überwacht wird.

5.4.4 Konsolidierungs- und Überwachungsoptionen

Sobald eine Datei zu einem Paket hinzugefügt wurde, müssen Sie EventSentry anweisen, was mit ihrem Inhalt zu tun ist. Sie können entweder Zeilen aus der Protokolldatei in einer Datenbank konsolidieren, den Text im Ereignisprotokoll der Anwendung protokollieren oder beides. Außerdem können Sie mit EventSentry Zeilen auf der Grundlage der Schlüsselwörter ein- oder ausschließen.

> Sie können auf das Minus-Symbol **-**doppelklicken , um alle Einträge aus der Filterliste zu entfernen.

Speichern von Protokolldateien in einer Datenbank

Um Inhalte aus Protokolldateien in einer Datenbank zu konsolidieren, klicken Sie auf die Registerkarte "Datenbankkonsolidierung" und wählen Sie im Abschnitt "Destination" ein Datenbankziel aus, indem Sie auf die Schaltfläche "Hinzufügen" klicken. Sie können bis zu vier verschiedene Datenbanken angeben.

Standardmäßig werden alle aus der Protokolldatei geparsten Zeilen an die angegebene(n) Datenbank(en) gesendet. Um dieses Verhalten zu ändern, können Sie entweder bestimmte Zeilen ignorieren ("Include") oder nur bestimmte Zeilen an die Datenbank senden. Klicken Sie auf das Symbol **+**, um Zeichenfolgen hinzuzufügen, die die Datenbank auslösen werden.

Include: Log all lines to the database, except for exclusions below
Dies ist die Standardeinstellung, und es werden alle geparsten Zeilen aus der Protokolldatei an die Datenbank gesendet. Zeilen in der Protokolldatei, die unten aufgeführte Zeichenfolgen enthalten, werden **nicht** an die Datenbank gesendet. Auf diese Weise können Sie Platz in der Datenbank sparen, wenn Ihre Protokolldatei nicht benötigten Inhalt enthält.

Exclude: Only log lines to the database that are included below
Diese Einstellung ist restriktiver und sendet nur Zeilen aus der Protokolldatei an diese Datenbank, die unten aufgeführt sind. Dadurch können Sie nur Inhalte an die Datenbank senden, die Ihren Filtern entsprechen. Beispielsweise können Sie nur Zeilen, die "Fehler" oder "Warnung" enthalten, an die Datenbank senden, um die Fehlerbehebung zu erleichtern.

Load / Laden
Lädt Filterregeln aus einer Textdatei (ein Eintrag pro Zeile) und hängt sie an die aktuelle Liste der Filter an.

Zeilen von der Protokolldatei in das Ereignisprotokoll schreiben
Um Zeilen aus den Protokolldateien in das Anwendungsereignisprotokoll zu protokollieren, klicken Sie auf die Registerkarte "Ereignisprotokoll-Warnungen" und aktivieren Sie das Kontrollkästchen "In das Anwendungsereignisprotokoll protokollieren". Sie können auch den Schweregrad wählen, unter dem Einträge im Ereignisprotokoll geschrieben werden.

Kontext
Wenn eine übereinstimmende Zeile in einer Protokolldatei gefunden wird, kann die Warnung bis zu 5 Zeilen vor und nach der übereinstimmenden Zeile enthalten, um den Kontext zu liefern. Setzen Sie diese Option auf "Keine", um die Protokollkontextfunktion zu deaktivieren.

Standardmäßig werden keine aus der Protokolldatei geparsten Zeilen in das Ereignisprotokoll aufgenommen. Klicken Sie auf das Symbol **+**, um Zeichenfolgen hinzuzufügen, die Alarme für das Ereignisprotokoll auslösen.

Include: Log all lines to the event log, except for exclusions below
Diese Einstellung **protokolliert alle** geparsten Zeilen aus der Protokolldatei in das Ereignisprotokoll. Zeilen in der Protokolldatei, die unten aufgeführte Zeichenfolgen enthalten, werden **nicht** im Ereignisprotokoll protokolliert. Diese Einstellung wird nicht empfohlen, da sie das Anwendungsprotokoll schnell füllen kann.

Exclude: Only log lines to the database that are included below
Dies ist die Standardeinstellung und protokolliert Zeilen aus der Protokolldatei in das Ereignisprotokoll, die mit den unten aufgeführten Zeichenfolgen übereinstimmen. Auf diese Weise können Sie nur Inhalte an das Ereignisprotokoll senden, die Ihren Filtern entsprechen. Beispielsweise können Sie nur Zeilen, die "Fehler" oder "Warnung" enthalten, in das Ereignisprotokoll protokollieren, um die Fehlerbehebung zu erleichtern.

Load / Laden
Lädt Filterregeln aus einer Textdatei (ein Eintrag pro Zeile) und hängt sie an die aktuelle Liste der Filter an.

Text-Übereinstimmungstyp
Gibt an, ob beim Textabgleich ein einfacher wildcard Vergleich oder ein RegEx-Musterabgleich verwendet wird.

5.4.4.1 Ereignisprotokolle

Die folgenden Ereignisprotokolleinträge werden durch diese Funktion mit der Kategorie **Logdatei-Überwachung** protokolliert:

Ereignis-ID	Beschreibung des Ereignisses	Beispiel
8000	Es wurde Text gefunden, der einer oder mehreren Filterregeln entspricht.	Text, der einer oder mehreren Filterregeln entspricht, wurde in der Datei C:\Logs\ntbackup01.log gefunden: Zeile in der überwachten Datei
8001	EventSentry stellt mehr als 1024 Dateien im überwachten Verzeichnis C:\Logs zwischengespeichert.	EventSentry speichert mehr als 1024 Dateien im überwachten Verzeichnis C:\Logs im Cache. Um den Ressourcenverbrauch des EventSentry-Agenten gering zu halten, wird empfohlen, alte Dateien in ein Unterverzeichnis oder ein anderes Verzeichnis zu verschieben.
8002	Eine Zeile enthielt keine CRLF.	Eine Zeile in der zuvor überwachten Datei C:\Logs\ntbackup01.log enthielt kein CRLF und wurde als solche nicht gemäß der Filterregel verarbeitet. Die Zeile aus der Textdatei ist unten dargestellt: Zeile in der überwachten Datei
8050	Eine Zeile in einer überwachten Datei enthielt nicht genügend Trennzeichen.	Die Protokolldatei "ex00001.log", die der Dateidefinition "IIS" zugeordnet ist, enthält nicht genügend Feldnamen (Trennzeichen) und wurde nicht verarbeitet. Bitte stellen Sie sicher, dass die in EventSentry eingestellte Dateidefinition mit dem Layout der überwachten Protokolldatei übereinstimmt. Die ersten 128 Zeichen der angetroffenen Zeile sind unten dargestellt: Feld1,Feld2,Feld3,Feld4

5.5 Systemüberwachung

EventSentry kann verschiedene Metriken des Betriebssystems überwachen, um potenzielle Fehler und Probleme zu erkennen. Mit System Health Monitoring kann EventSentry Alerts im Anwendungs-Ereignisprotokoll generieren und/oder Informationen (z.B. CPU-Nutzungshistorie, installierte Anwendungen) in einer zentralen Datenbank konsolidieren.

Übersicht

Die folgenden Systemobjekte können überwacht werden:

- Dienste
- Leistungsobjekte (Performance Monitoring)
- Speichernutzung von Prozessen, um fehlerhafte Anwendungen mit Speicherlecks zu erkennen
- Überwachen, ob bestimmte Prozesse aktiv sind
- Überwachung und Aufzeichnung von Festplattenplatz
- Ausgewählte Verzeichnisse
- Überwachung bestimmter Registrierungsschlüssel und Dateispeicherorte um festzustellen, ob Anwendungen installiert/deinstalliert werden oder ob sich eine Anwendung so registriert, dass sie automatisch gestartet wird, wenn sich ein Benutzer anmeldet.
- Überwachen von Verzeichnissen auf Änderungen der Dateigröße, Hinzufügen/Löschen von Dateien und Änderungen der Dateiprüfsumme
- Sicherstellen, dass die Zeit mit einem NTP-Server synchronisiert ist

- Geplante Aufgaben

Zusätzlich können

- Anwendungen zu definierten Zeitplänen gestartet werden und deren Ausgabe im Ereignisprotokoll protokollieren
- Sicherung und Löschen von Ereignisprotokollen zu definierten Zeitpunkten
- Dienste kontrolliert werden
- Verwenden einer System-Tray-Anwendung

Alle Alarme, die durch eine Systemzustandsfunktion erzeugt werden (z.B. Änderung des Dienststatus, Alarm bei zu wenig Speicherplatz, Leistungsalarm), werden **im Ereignisprotokoll der Anwendung protokolliert**.

Daher muss das Anwendungsereignisprotokoll mit mindestens einem Ereignisprotokollfilter überwacht werden (dieser ist standardmäßig aktiviert). Darüber hinaus enthält jeder Systemzustandsdialog einen "**Alerts ...** ", die einen Assistenten startet, der den erforderlichen Ereignisprotokollfilter erstellt.

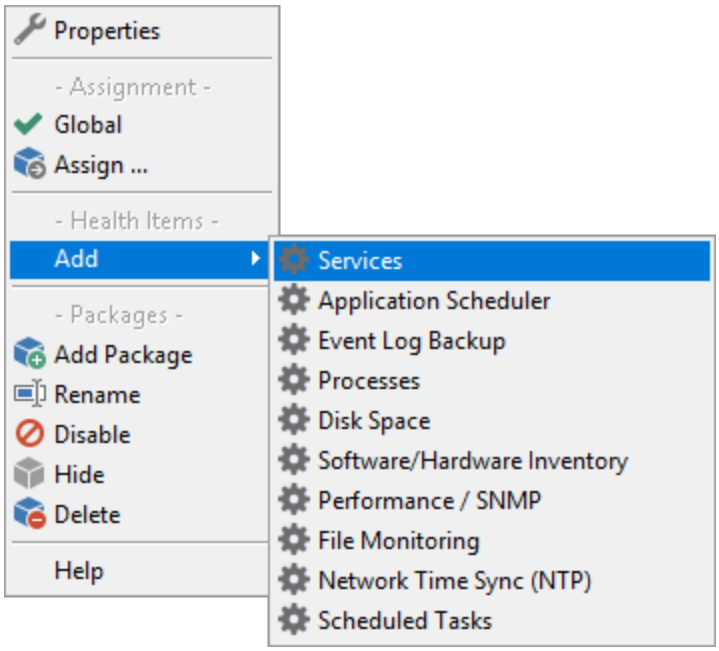
Integrierte System-Health-Pakete

NETIKUS.NET unterhält eine Reihe von Paketen, die allgemeine Gesundheitseinstellungen für die Dienst-, Festplattenspeicher- und Leistungsüberwachung enthalten. Diese Ereignisprotokollpakete werden automatisch mit EventSentry installiert und können automatisch über das Internet aktualisiert werden. Weitere Informationen finden Sie unter Herunterladen von Paketen.

Hinzufügen/Entfernen von Gesundheitsobjekten zu einem Gesundheitspaket

Ein System-Healthpaket besteht aus einem oder mehreren Objekten, wobei jedes Überwachungsmerkmal (Dienstüberwachung, Leistungsüberwachung usw.) ein Objekt ist, das zu einem Paket hinzugefügt werden kann.

Um ein Objekt zu einem Paket hinzuzufügen, klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie das gewünschte Objekt aus dem Untermenü **Hinzufügen**:



Das neue Objekt erscheint dann unter dem Paket mit einem Radsymbol, das ihm zugeordnet ist. Es ist zu beachten dass nicht mehr als ein Objekt desselben Typs zum selben Paket hinzugefügt werden kann. Sie können z. B. nicht zwei Service-Monitoring-Objekte zu demselben Health-Objekt hinzufügen.

Objekt können von einem System-Healthpaket entfernt werden indem mit der rechten Maustaste auf das Objekt geklickt und **Remove this object** ausgewählt wird.

5.5.1 Alerts

Fast alle System Health Objekte speichern Daten in der EventSentry Datenbank, können aber auch Warnmeldungen erzeugen (z. B. wenig Speicherplatz), die in das Ereignisprotokoll geschrieben werden. In der nachstehenden Tabelle finden Sie weitere Informationen darüber, welche Funktionen an die Datenbank senden und/oder Warnmeldungen erzeugen. Jede Funktion kann individuell konfiguriert werden, und Warnmeldungen können entweder aktiviert oder deaktiviert werden.

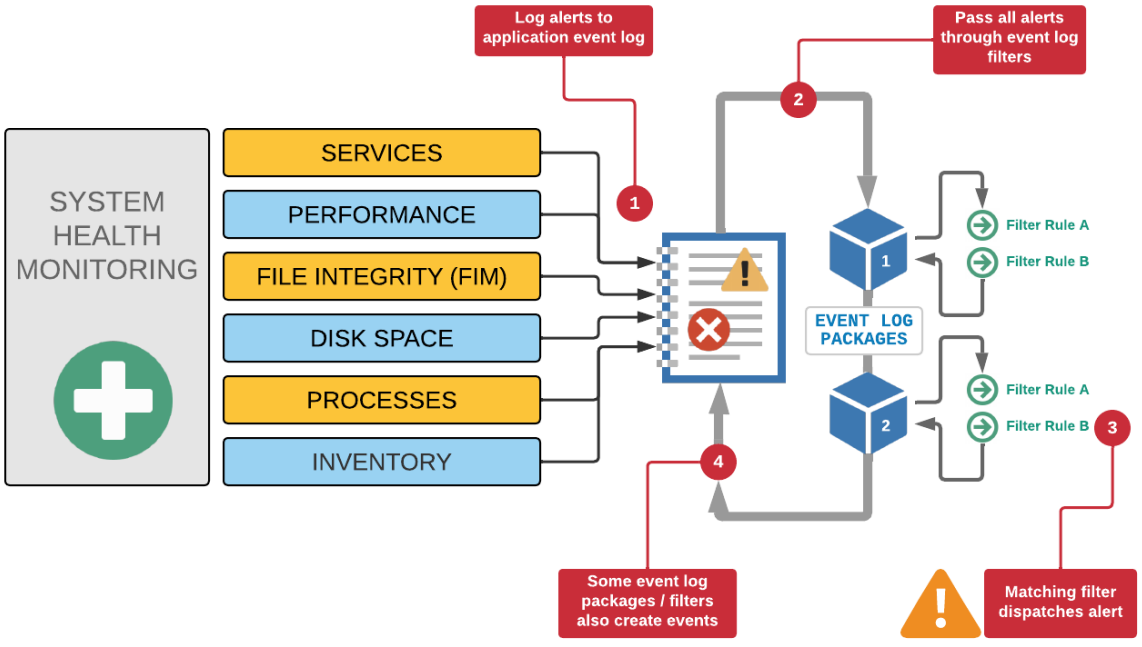
Funktion	Datenbank	Warnmeldungen	Alerts Beschreibung
Dienstüberwachung	Ja	Ja	Wenn Dienste oder Treiber hinzugefügt oder entfernt werden oder ihren Status ändern.
Anwendungs-Scheduler	Nein	Ja	Prozessausgabe (wenn konfiguriert) oder wenn Fehler aufgetreten sind.
Sicherung von Ereignisprotokollen	Nein	Ja	Wenn Backups von Ereignisprotokollen usw. abgeschlossen sind oder wenn Fehler aufgetreten sind
Prozessüberwachung	Ja	Ja	Wenn kritische Prozesse inaktiv sind oder neue Prozesse Netzwerkverbindungen annehmen.
Festplattenkapazitätsüberwachung	Ja	Ja	Wenn der Speicherplatz auf der Festplatte knapp wird.
Verzeichnisüberwachung	Ja	Ja	Wenn die Größe des Verzeichnisses oder die Anzahl der Dateien Grenzen überschreitet.
Software/Hardware-Inventar	Ja	Ja	Wenn Software-/Browser-Erweiterungen hinzugefügt/entfernt werden, wenn sich BIOS oder installierter Speicher ändern

Leistungsüberwachung	Ja	Ja	Wenn Leistungszähler Grenzwerte überschreiten
Überwachung von Dateiänderungen und -integrität	Ja	Ja	Wenn überwachte Dateien hinzugefügt, entfernt oder geändert werden
NTP-Überwachung	Nein	Ja	Regelmäßige Statusaktualisierungen und wenn die Systemzeit nicht synchronisiert ist
Aufgabenplanung (Scheduled Tasks)	Ja	Ja	Wenn geplante Aufgaben hinzugefügt, geändert oder entfernt werden
System Status Tray Applikation	Nein	Nein	

Um die Konsistenz zu wahren und ein Protokoll aller von einer Systemzustandsfunktion erzeugten Warnmeldungen zu erhalten, werden alle Warnmeldungen in das Ereignisprotokoll geschrieben. Bitte lesen Sie dazu das entsprechende Unterkapitel "Event Log" der jeweiligen Funktion.

Um Benachrichtigungen (z. B. per E-Mail) über Systemzustandswarnungen zu erhalten, müssen die Ereignisprotokollfilter diese Warnmeldungen an die entsprechende Aktion weiterleiten. Viele Warnungen, die von Systemzustandsfunktionen erzeugt werden, werden mit einem Fehlerschweregrad protokolliert ("Error"), der sicherstellt, dass sie automatisch von den Standard-E-Mail-Filterregeln aufgefangen werden. Die Schweregrade können jedoch geändert werden, weshalb es wichtig ist die Architektur und den Ablauf von Ereignissen zu verstehen.

Das folgende Diagramm veranschaulicht, wie jede Funktion Warnungen im Ereignisprotokoll protokolliert, die dann analysiert und bei Übereinstimmung an eine oder mehrere Aktionen weitergeleitet werden.



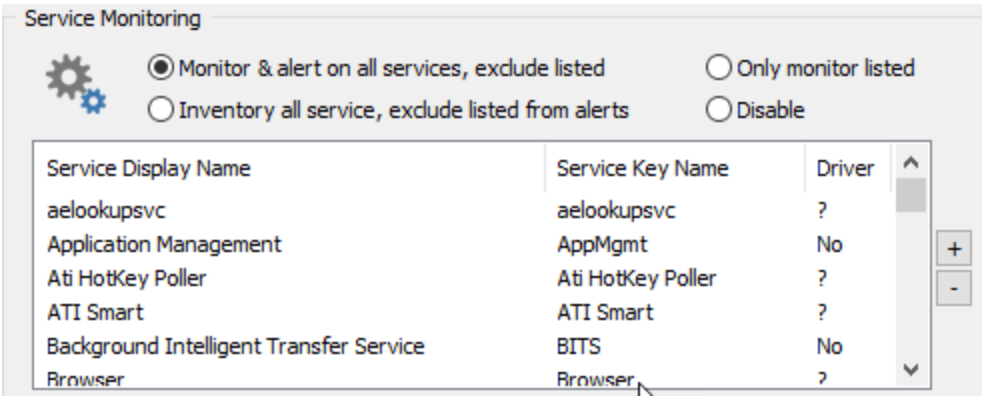
5.5.2 Dienstüberwachung

Die Dienstüberwachung bietet die folgenden Funktionen:

- Erkennung von Änderungen des Dienststatus (gestoppt -> läuft, pausiert -> gestoppt usw.)
- Erkennen, ob Services hinzugefügt oder entfernt werden
- Erkennen von Änderungen der Dienstkonfiguration (Änderung des Dienstkontos, Änderung der ausführbaren Datei)
- Erkennen, ob ein auf *Autostart* eingestellter Dienst nicht gestartet wurde
- Sicherstellen, dass ein Dienst immer in einem gewünschten Zustand ist (gestoppt oder läuft)
- Verfolgen von Dienststatus, Änderungen und Aktivität in einer Datenbank

Service Monitoring is supported on Unix/Linux hosts when SSH credentials are configured. Service monitoring alerts are identical between Windows and Non-Windows hosts but generally contain more details on Windows.

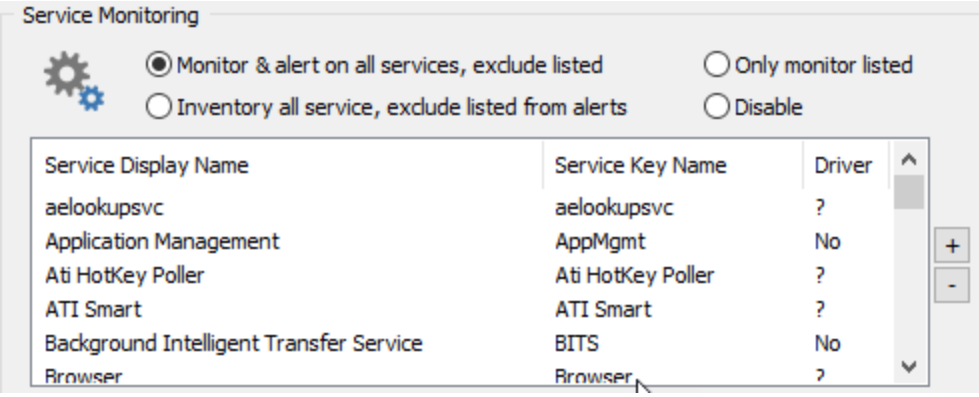
Service data on Non-Windows hosts is collected by the Heartbeat Agent.



Dienst- & Treiberüberwachung

Diese Komponente kann so konfiguriert werden, dass entweder alle Dienste, nur bestimmte Dienste oder keine Dienste überwacht werden.

Alle Dienste überwachen:	Alle Dienste, mit Ausnahme der in der Listbox enthaltenen, werden überwacht.
Nur ausgewählte Dienste überwachen:	Nur die in der Listbox angezeigten Dienste werden überwacht. Wenn das Listenfeld leer ist, ist die Dienstüberwachung nicht aktiv.
Dienste nicht überwachen	Es werden keine Dienste überwacht, und alle Dienste aus dem Listenfeld werden entfernt.



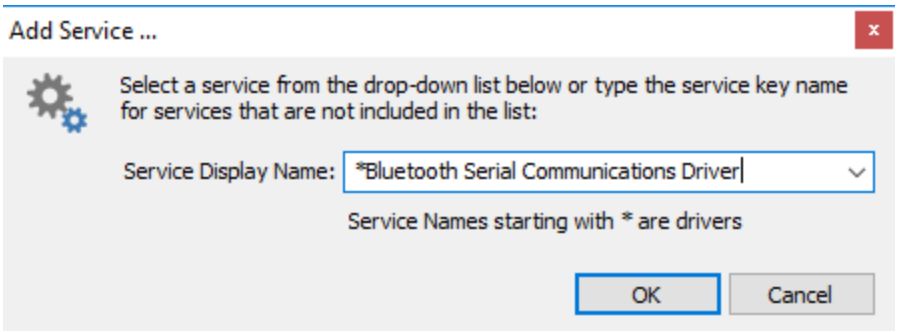
Wenn das Boot-Zeitverhalten auf "Neuscan nach Neustart" eingestellt ist, werden Änderungen des Dienststatus auch bei Neustarts und/oder Neustarts des EventSentry-Dienstes überwacht. Wenn z.B. der Serverdienst-Status lief, als Sie den EventSentry-Dienst stoppten, aber angehalten wurde, als Sie den EventSentry-Dienst starteten, dann wird diese Statusänderung protokolliert.

Dienste werden sowohl mit dem Anzeigenamen als auch mit dem Namen des Dienstschlüssels in der Liste angezeigt. Wenn es sich bei einem Dienst um einen Treiber handelt, wird in der Spalte Treiber Ja angezeigt, andernfalls Nein.

Hinzufügen und Entfernen von Diensten aus der Liste

Durch Klicken auf das Plus (+) rechts in der Liste wird ein Dienst zur Liste der überwachten (oder ausgeschlossenen) Dienste hinzugefügt. Das Dialogfeld, das beim Klicken auf die Plus-Schaltfläche angezeigt wird, ermöglicht es Ihnen, einen Dienst (oder Treiber) aus einer Dropdown-Liste auszuwählen, der der Liste hinzugefügt werden soll. Bitte beachten Sie, dass Dienste, die mit einem Sternchen (*) beginnen andeuten, dass es sich bei diesem Dienst um einen Treiber handelt. Treiber werden nur dann in dieser Liste angezeigt, wenn Sie das Kontrollkästchen *Treiber überwachen* aktivieren. Teilweise Dienstnamen mit Platzhaltern (z.B. sql*) werden unterstützt.

Wenn ein in dieser Liste angegebener Dienst auf einem entfernten Host nicht existiert, wird er einfach ignoriert - es wird keine Warnung ausgegeben.



Ein Dienst kann entfernt werden, indem man ihn in der Liste auswählt und auf die Schaltfläche Minus (-) klickt.

Sie können auch Dienste hinzufügen, die nicht in der Liste "Service Display Name" aufgeführt sind, indem Sie den Dienstnamen (Service Key Name) eingeben. Dies kann der Fall sein, wenn ein Dienst auf einem überwachten Server, aber nicht auf dem Management-Server installiert ist. Teilweise Dienstnamen mit Platzhaltern werden unterstützt.

Überwachungsintervall

Dienste werden alle 10 Sekunden überwacht. Wenn eine Dienständerung erkannt wird, wird das Dienstüberwachungsintervall vorübergehend für eine Minute auf 5 Sekunden reduziert.

Was zu überwachen ist

Service Monitoring kann Änderungen des Servicestatus, Änderungen in der SCM (=Service Control Manager)-Datenbank oder beides überwachen. Die Überwachung von Treibern ist konfigurierbar.

Statusänderungen überwachen: Wenn sich der Status eines Dienstes ändert, wird ein Ereignis im Ereignisprotokoll der Anwendung erzeugt. Wenn beispielsweise der Messenger-Dienst angehalten wird, zeigt EventSentry an, dass der Messenger von "Läuft" in "Angehalten" geändert wurde.

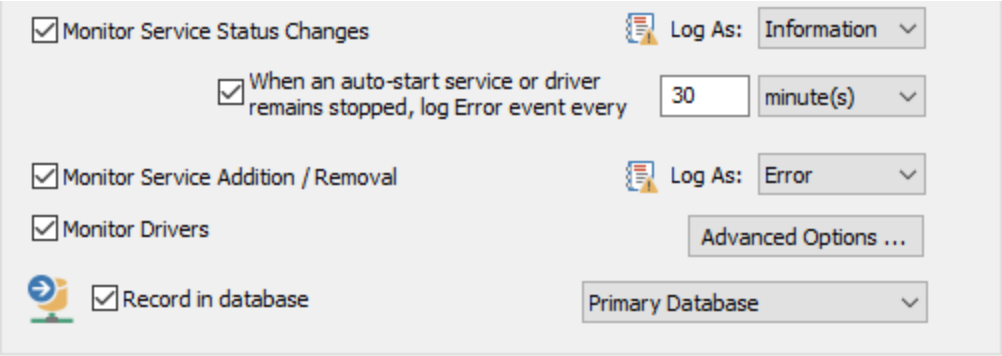
Wenn der Dienst gestoppt wird, benachrichtigen Sie alle: Wenn dieses Kontrollkästchen aktiviert ist, werden zusätzlich kontinuierliche Benachrichtigungen generiert, wenn ein Dienst für den angegebenen Zeitraum im Zustand "Angehalten" verbleibt.

Überwachen Sie SCM-Änderungen: Wenn ein Service hinzugefügt oder entfernt wird, protokolliert EventSentry ein Ereignis im Ereignisprotokoll der Anwendung.

Treiber überwachen: Wählen Sie diese Option, um Treiber zu überwachen.

Log Changes As: konfiguriert den Schweregrad, mit dem Ereignisse in das Anwendungsereignisprotokoll geschrieben werden.

Aufzeichnung in der Datenbank
Konfiguriert, ob diese Komponente die Aktivität in einer Datenbank aufzeichnet (Aktion).



Erweiterte Optionen

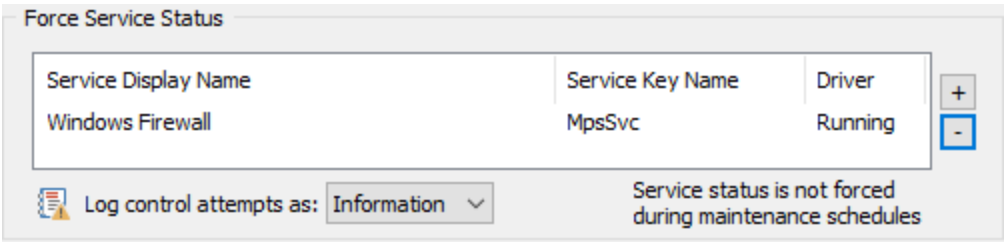
Siehe "Erweiterte Optionen" für weitere Einzelheiten.

Status des Zwangsdienstes

Stellt sicher, dass sich bestimmte Dienste immer im Zustand *"Läuft"* oder *"Gestoppt"* befinden (individuell pro Dienst konfigurierbar).

Um einen Dienst zu steuern, klicken Sie auf die Schaltfläche **"+"** und wählen Sie einen Dienst aus der Liste aus. Wenn sich der angeforderte Dienst nicht in der Liste befindet, können Sie einfach den Namen des Dienstschlüssels in das Feld "Service Display Name" eingeben. Geben Sie dann den gewünschten Dienststatus an (z.B. "Laufend") und klicken Sie auf die Schaltfläche OK. EventSentry stellt nun sicher, dass sich der Dienst immer im gewünschten Zustand befindet.

Im folgenden Beispiel wird sichergestellt dass der "Windows Firewall" Dienst (Service Key Name: MpsSvc) immer läuft, und sofort gestartet wird wenn der Dienst nicht läuft.



Immer wenn der Agent feststellt, dass sich ein Dienst nicht im angeforderten Zustand befindet, versucht er, den Status entsprechend zu ändern und schreibt eine Meldung in das Ereignisprotokoll, es sei denn, der Host befindet sich in einem Wartungsplan. Die Einstellung **Log control attempts as** bestimmt den Schweregrad, mit dem diese Meldungen in das Ereignisprotokoll geschrieben werden.

Einem Host kann ein Wartungsplan zugewiesen werden, um den Status eines Dienstes vorübergehend zu ändern. Die Dienststatus-Kontrollfunktion ist inaktiv, während sich ein Gastgeber im Wartungsplan befindet.

Limitations

If a service status is changed twice during a monitoring interval, then the status change cannot be detected by EventSentry, this is extremely unlikely to happen however.

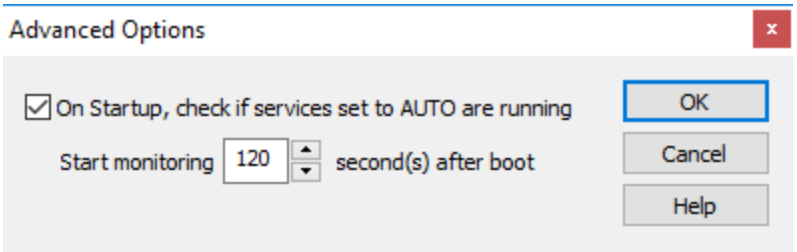
Implications on System Load

Service monitoring does not have a high impact on the system load.

5.5.2.1 Erweiterte Optionen

Prüfen Sie beim Start, ob die auf AUTO eingestellten Dienste laufen

Sie können automatisch überprüfen, ob alle Dienste, die so eingestellt sind, dass sie automatisch mit Windows gestartet werden, auch tatsächlich ausgeführt werden. Es wird empfohlen, auch eine Startverzögerung (Startüberwachung ...) einzustellen, wenn Sie diese Funktion aktivieren. Viele Dienste und Treiber (die nach oder mit EventSentry gestartet werden) sind beim Start von EventSentry noch nicht in Betrieb, werden aber einige Minuten danach ausgeführt. Die Einstellung der Verzögerung hängt von der Hardware, dem von Ihnen verwendeten Betriebssystem und der Anzahl der zu überwachenden Dienste ab. Die empfohlene Standardeinstellung beträgt 120 Sekunden.



5.5.2.2 Linux / Unix Konfiguration

Um die Funktion "Force Service Status" auf Unix/Linux-Betriebssystemen nutzen zu können, können aus Sicherheitsgründen zusätzliche Konfigurationsschritte erforderlich sein. Die folgenden Schritte sind nicht erforderlich, wenn das Zielsystem, das Sie überwachen, Root-Anmeldungen über SSH zulässt und das in %PRODUCT% konfigurierte Konto der Root-Benutzer oder ein gleichwertiges Konto ist.

Die folgenden Anweisungen sollten auf den meisten gängigen Linux-Distributionen funktionieren, können aber abweichen und sind ohne Gewähr. Führen Sie auf den Zielsystemen die folgenden Schritte durch.

1. Erstellen Sie einen neuen Benutzer, indem Sie diesen Befehl ausführen:

```
sudo useradd -m [username]
```

2. Erstellen Sie ein Passwort für den neuen Benutzer (notieren Sie sich den Benutzernamen und das Passwort, da diese später in %PRODUCT% konfiguriert werden müssen:

```
sudo passwd [username]
```

3. Gewähren Sie dem neuen Benutzer Zugriff auf den Befehl zum Starten/Stoppen von Diensten. Dazu muss eine Datei in `/etc/sudoers.d` mit dem Namen `[username]` erstellt werden. Sie können Ihren bevorzugten Texteditor verwenden, für dieses Beispiel benutzen wir nano.

Die Datei **sudoers** ist eine kritische und sensible Datei; ein Tippfehler oder ein Fehler in dieser Datei kann zu Problemen bei der Ausführung erweiterter Befehle führen und das System unbrauchbar machen. Überprüfen Sie diese Datei vor dem Speichern sicherheitshalber nochmals.

```
sudo nano /etc/sudoers.d/[username]
```

Die folgenden 3 Zeilen müssen zu dieser neuen Datei hinzugefügt werden:

```
[username] ALL=NOPASSWD: /bin/systemctl start *
[username] ALL=NOPASSWD: /bin/systemctl stop *
[username] ALL=NOPASSWD: /bin/systemctl status *
```

Ersetzen Sie [username] durch den Benutzernamen, den Sie in Schritt 1 eingegeben haben. Speichern Sie die Änderungen mit CTRL+S und verlassen Sie den Editor mit CTRL+X.

Alternativ dazu können Sie auch unser Erstellungsskript herunterladen und es ausführen:

```
wget
https://raw.githubusercontent.com/eventsentry/configuration/main/es_servicemonitor.sh
sudo sh es_servicemonitor.sh
```

Das Skript fragt nach dem Benutzernamen und dem Passwort und erstellt die entsprechenden Dateien, die den Benutzer zum Starten und Stoppen der Dienste berechtigen.

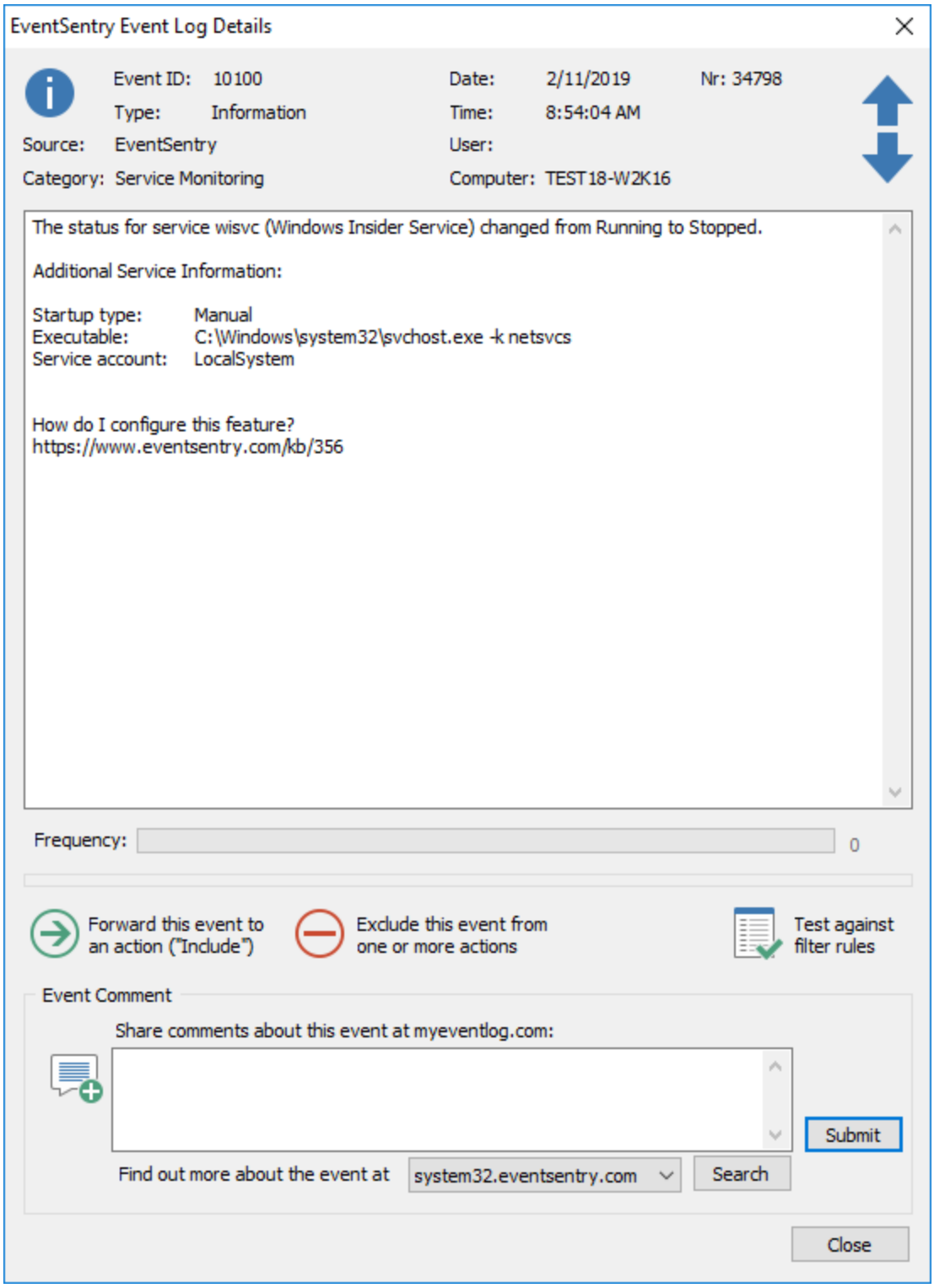
5.5.2.3 Event Log

Die folgenden Ereignisse werden von dieser Funktion mit der Ereigniskategorie **Service Monitoring** protokolliert. Die obere Ereignis-ID wird protokolliert, wenn eine Aktivität mit einem Service erkannt wird, die untere Ereignis-ID wird protokolliert, wenn eine Aktivität mit einem Treiber erkannt wird.

Event ID	Event Description	Example
10100 10150	A service status changed	The status for service BITS (Background Intelligent Transfer Service) changed from Start Pending to Running. Additional Service Information: Startup type: Automatic Executable: C:\WINDOWS\system32\svchost.exe -k netsvcs Service account: LocalSystem
10101 10151	A service was added	A service was added: Additional Service Information: Name: GatewayIPMonitor (Gateway IP Monitor) Status: Running Startup type: Automatic Executable: C:\Program Files (x86)\Gateway IP Monitor\gwipmon_svc.exe Service Account: LocalSystem
10102 10152	A service was removed	A service was removed: GatewayIPMonitor (Gateway IP Monitor). Additional Service Information: Status: Running Startup type: Automatic Executable: C:\Program Files (x86)\Gateway IP Monitor\gwipmon_svc.exe Service Account: LocalSystem
10103 10153	A service is being monitored	The service EventSentry (EventSentry) is now being monitored. Additional Service Information: Status: Running Startup type: Automatic Executable: C:\Program Files (x86)\Gateway IP Monitor\gwipmon_svc.exe Service Account: LocalSystem
10104 10154	A service is not being monitored anymore	The service Cdaudio (Cdaudio) will not be monitored anymore. Last service status was Stopped.
10105	Services configured for autostart are not running	The following 3 service(s) are configured to AUTOSTART but are currently not running: Cdaudio Digital CD Audio Playback Filter Driver

		Sfloppy
10106	Unable to connect to SCM	Unable to connect to the Service Control Manager (SCM), services cannot be monitored.
10107	Unable to enumerate services	Unable to enumerate services, services cannot be monitored.
10108 10158	Successfully changed service state	The state of service USB Mass Storage Driver was Running, requested state is Stopped. EventSentry successfully changed the service status to Stopped.
10109 10159	Unable to change service state	The state of service iPodService is Start Pending, requested state is Stopped. EventSentry was not able to change the service status due to the following error: The service is pending stop.
10110 10160	A service startup type changed	The Startup Type for service dcevt64 (DSM SA Event Manager) changed from Automatic to Manual. Additional Service Information: Status: Running Startup type: Automatic Executable: "C:\Program Files\Dell\SysMgt\dataeng\bin\dsm_sa_eventmgr64.exe" Service Account: LocalSystem
10111	The user account for a service changed	The user account for service dcevt64 (DSM SA Event Manager) changed from LocalSystem to DellServiceAccount. Additional Service Information: Status: Running Startup type: Automatic Executable: "C:\Program Files\Dell\SysMgt\dataeng\bin\dsm_sa_eventmgr64.exe"
10112 10162	The executable for a service changed	The executable for service dcevt64 (DSM SA Event Manager) changed from "C:\Program Files (x86)\Dell\SysMgt\dataeng\bin\dsm_sa_eventmgr.exe" to "C:\Program Files\Dell\SysMgt\dataeng\bin\dsm_sa_eventmgr64.exe" Additional Service Information: Status: Running Startup type: Automatic Service Account: LocalSystem
10114	A service remains stopped	The status for service dcevt64 (DSM SA Event Manager) remains stopped.

10164		Additional Service Information: Startup type: Automatic Executable: "C:\Program Files\Dell\SysMgt\dataeng\bin\dsm_sa_eventmgr64.exe" Service Account: LocalSystem



A Service Status changed and is logged to the Event Log

5.5.3 Anwendungs-Scheduler

Planen Sie beliebige (Befehlszeilen-)Anwendungen aus EventSentry heraus für die benutzerdefinierte Systemüberwachung und Aufgabenautomatisierung. Unterstützung von Batch-Dateien, ausführbaren

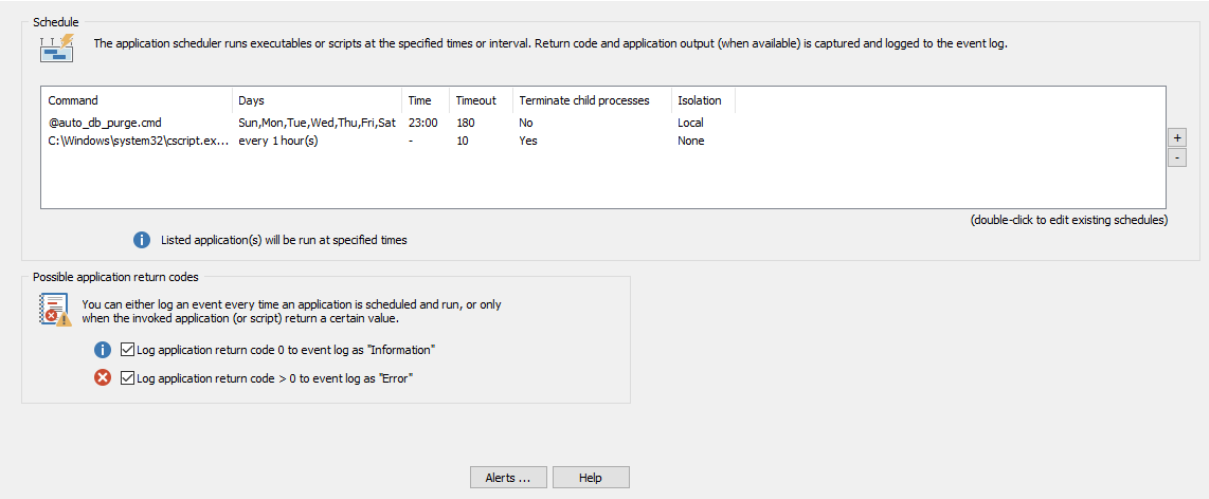
Dateien und jeder Skriptsprache (z.B. PowerShell, Perl, Visual Basic Script, ...), für die ein Interpreter installiert ist.

Zusätzlich zur Planung von Anwendungen und Skripten zu festgelegten Daten und Zeiten werden auch kontinuierliche Zeitpläne alle X Minuten unterstützt. Der Agent protokolliert die Ausgabe der Anwendung im Ereignisprotokoll mit einem dynamischen Schweregrad (Information oder Fehler), der die Fehlerbehandlung und automatische Behebung unter Verwendung von Ereignisprotokollfilen unterstützt. Siehe Ereignisprotokolle für alle möglichen Ereignisprotokollaufzeichnungen, die von dieser Funktion protokolliert werden.

Ausführbare Dateien, die mit dieser Funktion gestartet werden, laufen unter demselben Sicherheitskonto, unter dem auch der EventSentry-Agent läuft, standardmäßig unter dem LocalSystem-Konto. Berücksichtigen Sie dies, wenn Sie beabsichtigen, Anwendungen auszuführen, die Zugriff auf Ressourcen benötigen, die sich im Netzwerk befinden.

Eingebettete Skripte

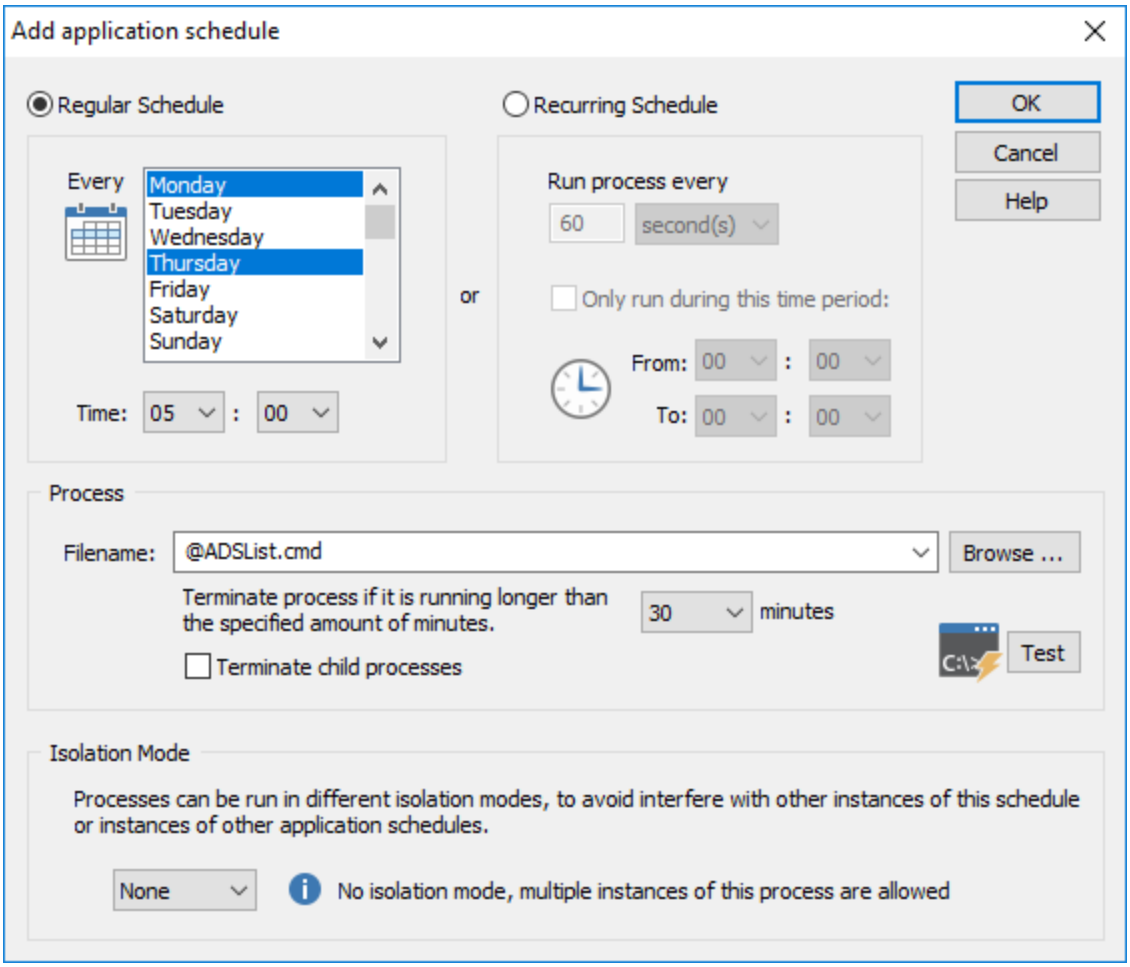
Der Anwendungs-Scheduler kann entweder vorhandene Skripte starten, die auf dem Host vorhanden sind, oder ein eingebettetes Skript starten.



Vom Anwendungsplaner gestartete Prozesse und/oder Skripte, die Nachrichtenboxen, Lizenzdialoge und Ähnliches anzeigen, funktionieren nicht, da sie auf unbestimmte Zeit blockiert werden. Dies betrifft z.B. einige der Sysinternals-Dienstprogramme, die dazu neigen, einen Lizenzdialog anzuzeigen, wenn sie zum ersten Mal ausgeführt werden.

Planen einer Anwendung zur Ausführung an einem bestimmten Datum/zu einer bestimmten Zeit

Um eine Anwendung zu einem voreingestellten Datum und einer voreingestellten Zeit zu planen, z.B. jeden Tag um 15 Uhr, klicken Sie auf die Plus-Schaltfläche neben der Terminliste. Der folgende Dialog wird Ihnen angezeigt:



Setzen Sie den Zeitplantyp auf "Regulärer Zeitplan" und planen Sie im Bereich Datum & Zeit die Anwendung so, dass sie entweder an bestimmten Wochentagen, an bestimmten Tagen des Monats oder an beiden Tagen ausgeführt wird.

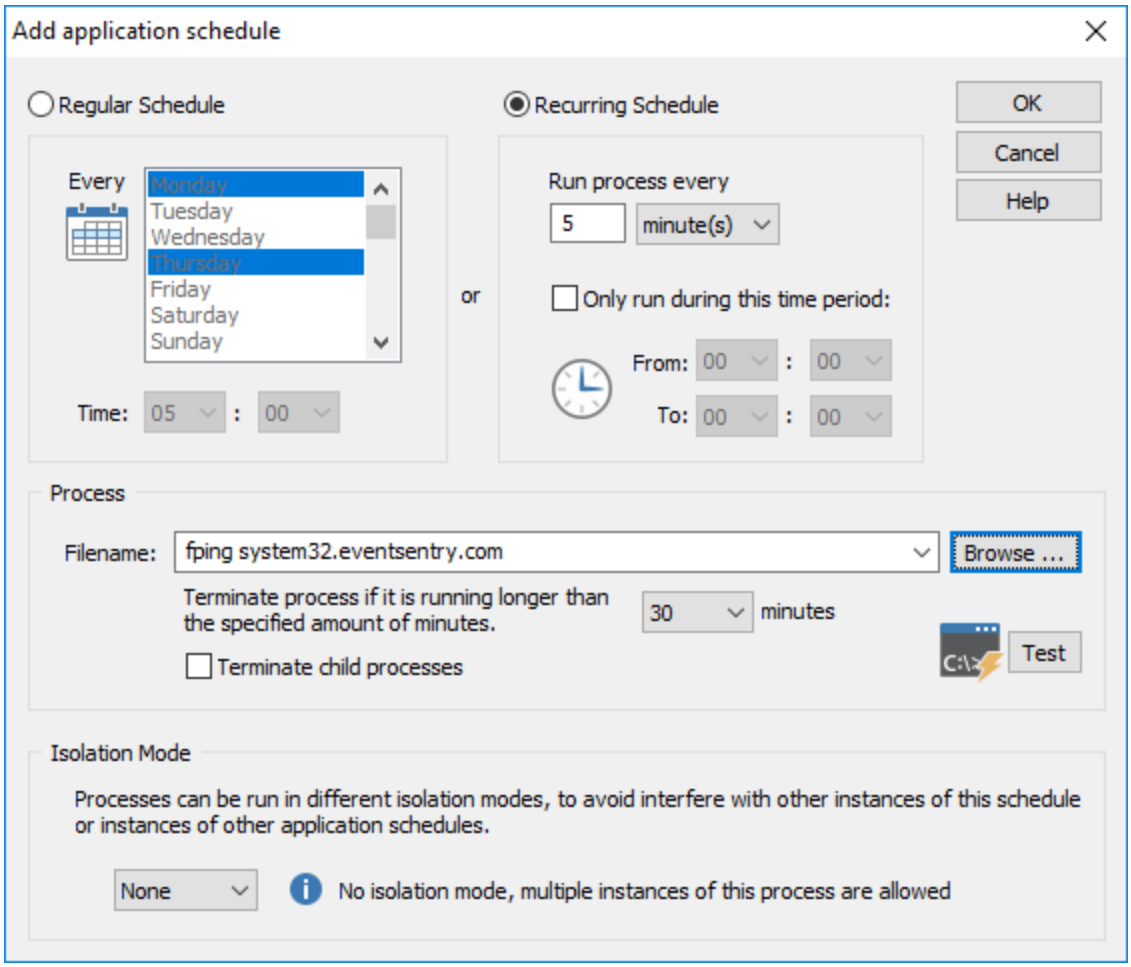
Die Funktion Prozess-Timeout ermöglicht es Ihnen, einen Prozess zu beenden, wenn er länger als eine bestimmte Anzahl von Minuten läuft. Setzen Sie diese Option auf 0 (Minuten), um Prozesse so lange laufen zu lassen, bis sie sich von selbst beenden.

Geben Sie die auszuführende Datei im Feld Dateiname an. Sie können entweder ein vorhandenes Skript angeben oder mit der Schaltfläche "Durchsuchen" auswählen oder mit dem Dropdown-Menü ein eingebettetes Skript auswählen. Eingebettete Skripte werden mit dem @-Symbol vor der Datei angegeben, wie im obigen Screenshot gezeigt.

Wenn Terminate child processes markiert ist, werden alle vererbten Prozesse, die durch *Dateiname* gestartet wurden, rekursiv beendet.

Planen einer periodisch auszuführenden Anwendung

Um eine Anwendung so zu planen, dass sie kontinuierlich läuft, z.B. alle 5 Minuten, klicken Sie auf die Plus-Schaltfläche neben der Zeitplanliste. Das folgende Dialogfeld wird angezeigt:



Stellen Sie den Zeitplantyp auf "Wiederkehrender Zeitplan" und konfigurieren Sie ihn entsprechend. Der Zeitplan kann weiter eingeschränkt werden, indem die Anwendung nur während bestimmter Zeiträume ausgeführt wird, zum Beispiel zwischen 8AM und 5PM.

Ändern eines bestehenden Zeitplans

Sie können bestehende Zeitpläne ändern, indem Sie auf die Einträge in der Zeitplanliste doppelklicken.

Wenn ein Skript (z.B. VBScript) gestartet wird, dann wird empfohlen, das Feld Dateiname auf die Skript-Engine (z.B. cscript.exe) mit der Skriptdatei als Argument zu zeigen. Zum Beispiel

```
c:\windows\system32\cscript.exe c:\batch\files_count.vbs
```

um die Datei **c:\batch\files_count.vbs** auszuführen.

Rückgabecodes der Anwendung

Um die Vorteile der Rückgabecode-Analyse zu nutzen, empfiehlt es sich, entweder direkt ausführbare Anwendungen aufzurufen (z.B. ping.exe) oder Skripte mit einer Skripting-Engine aufzurufen, mit der Sie den Rückgabecode angeben können (z.B. VBScript mit cscript.exe). Es wird nicht empfohlen, Batch-Dateien zu verwenden, wenn der Rückgabecode der Anwendung von Bedeutung ist.

- Wenn Sie den "Log application return code 0 to event log" überprüfen, wird ein Informationsereignis im Ereignisprotokoll der Anwendung protokolliert, das die Textausgabe des Skripts anzeigt.

- Wenn Sie "Log application return code > 0 to event log" prüfen, wird ein Fehler im Ereignisprotokoll der Anwendung protokolliert, der die Textausgabe des Skripts anzeigt.

Das nächste Kapitel, "Beispielskripte", listet Visual Basic-Skripte auf, die gut mit der Funktion Anwendungsplaner zusammenarbeiten.

5.5.3.1 Beispielskripte

Die folgenden Skripte können vom Anwendungsplaner verwendet werden und geben einen Fehlercode zurück, je nachdem, ob sie erfolgreich ausgeführt wurden oder nicht. Variablen, die angepasst werden müssen, sind unten grün markiert. Alle nachstehenden Beispiele verwenden Visual Basic-Skript. Weitere Beispielskripte sind im Unterordner **Scripts** des EventSentry Installationsverzeichnises.

Dieses Skript zählt die Anzahl der Dateien in einem Ordner und kann 1 zurückgeben, wenn die Anzahl der Dateien einen Schwellenwert überschreitet.

```
' ----------------------
' --- file_count.vbs ---
' ----------------------
' Counts the number of files in a folder (without traversing subfolders)
'
' Returns 1 if the number of files is larger than MyLimit or 0 if the number
' of files is equal or less than MyLimit

Dim FS, FO, FC
Dim MyFolder, MyLimit

' Set your values here
MyFolder      = "C:\Batch"
MyLimit       = 200

Set FS = CreateObject("Scripting.FileSystemObject")
Set FO = FS.GetFolder(MyFolder)
Set FC = FO.Files

WScript.Echo "Folder " & MyFolder & " contains " & FC.Count & " files."

If FC.Count > MyLimit Then
       WScript.Quit(1)
Else
       WScript.Quit(0)
End If
```

Dieses Skript listet alle Fans im System auf, die über WMI überwacht werden können (falls unterstützt). Wenn einer oder mehrere der überwachten Ventilatoren einen anderen Status als "Andere", "Unbekannt" oder "Läuft" melden, gibt das Skript 1 zurück.

```
' -------------------------
' --- system_faninfo.vbs ---
' -------------------------
On Error Resume Next
```

```
Dim GlobalError

GlobalError = 0

Function ExplainAvailability(Availability)
       Select Case Availability
              Case 1:  ExplainAvailability = "Other"
              Case 2:  ExplainAvailability = "Unknown"
              Case 3:  ExplainAvailability = "Running / Full Power"
              Case 4:  ExplainAvailability = "Warning"
              Case 5:  ExplainAvailability = "In Test"
              Case 6:  ExplainAvailability = "Not Applicable"
              Case 7:  ExplainAvailability = "Power Off"
              Case 8:  ExplainAvailability = "Off Line"
              Case 9:  ExplainAvailability = "Off Duty"
              Case 10: ExplainAvailability = "Degraded"
              Case 11: ExplainAvailability = "Not Installed"
              Case 12: ExplainAvailability = "Install Error"
              Case 13: ExplainAvailability = "Power Save - Unknown"
              Case 14: ExplainAvailability = "Power Save - Low Power Mode"
              Case 15: ExplainAvailability = "Power Save - Standby"
              Case 16: ExplainAvailability = "Power Cycle"
              Case 17: ExplainAvailability = "Power Save - Warning"
       End Select
End Function

Function ExplainStatus(Status)
       Select Case Status
              Case 1: ExplainStatus = "Other"
              Case 2: ExplainStatus = "Unknown"
              Case 3: ExplainStatus = "Enabled"
              Case 4: ExplainStatus = "Disabled"
              Case 5: ExplainStatus = "Not Applicable"
       End Select
End Function

strComputer = "."
Set objWMIService = GetObject("winmgmts:" & "{impersonationLevel=impersonate}!\\" &
strComputer & "\root\cimv2")

Set colItems = objWMIService.ExecQuery("Select * from Win32_Fan")

For Each objItem in colItems
    Wscript.Echo "Name:           " & objItem.Name
    Wscript.Echo "Active Cooling: " & objItem.ActiveCooling
    Wscript.Echo "Availability:   " & ExplainAvailability(objItem.Availability) & " ("
& objItem.Availability & ")"
    Wscript.Echo "Device ID:      " & objItem.DeviceID
    Wscript.Echo "Status Info:    " & ExplainStatus(objItem.StatusInfo) & " (" &
objItem.StatusInfo & ")"
    Wscript.Echo

    ' Analyze
    If objItem.Availability > 3 Then
```

```
        GlobalError = 1
    End If
Next

Wscript.Quit(GlobalError)
```

5.5.3.2 Event Log

Die folgenden Ereignisse werden von dieser Funktion mit der Ereigniskategorie **Application Scheduler** protokolliert.

Event ID	Event Description	Example
10200	An application was executed successfully.	`superdel.exe was run for 15 seconds with the result shown below. Return Code was 0.`
10201	A process could not be created.	`The process superdel.exe could not be created due to the following error: The file could not be found.`
10202	A process exceeded the maximum configured time interval, but the process could not be terminated.	`The process superdel.exe exceeded the maximum allowed time interval of 15 minute(s). EventSentry was unable to terminate the process due to the following error: Acess Denied.`
10203	A process exceeded the maximum configured time interval and was terminated.	`The process superdel.exe exceeded the maximum allowed time interval of 15 minute(s). The process was terminated. Please increase the timeout interval for this drive in the management application (System Health -> 3rd Party Applications).`
10204	A process was executed successfully.	`dosomething.exe was executed successfully.`

10205	A process exceeded the maximum configured time interval but could not be terminated. 0 or more child processes were terminated.	`The process dosomething.exe exceeded the maximum allowed time interval of 2 minute(s). EventSentry was unable to terminate the process due to the following error:`
		
		`Access Denied`
		
		`1 child process(es) were successfully terminated.`

10206	A process exceeded the maximum configured time interval and was terminated.	`The process adlist.exe exceeded the maximum allowed time interval of 5 minute(s). The process and 0 child process(es) was terminated. Please`

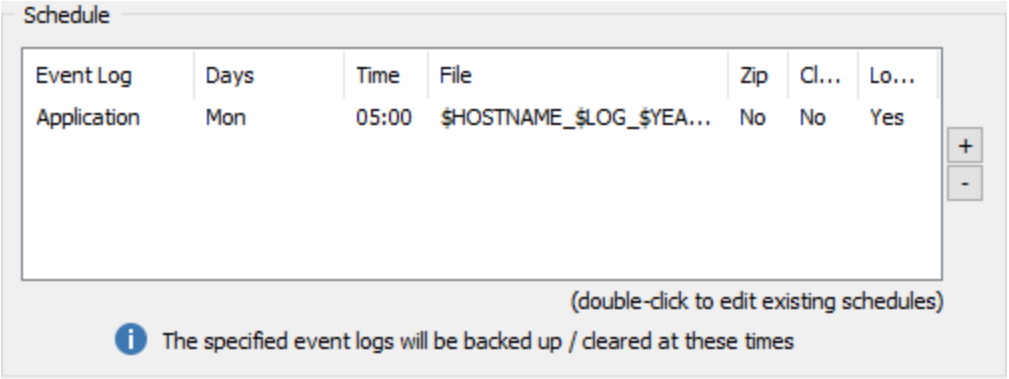
		increase the timeout interval for this process in the management console (System Health -> Application Scheduler).
10210	A process was not started because the isolation level of the schedule is set to local and another instance of the same process is already running.	The process adlist.exe was not started because the script is configured for local isolation and another instance of the same script is already running.
10211	A process wasn't started because it is configured for global isolation, and another process also configured for global isolation is already running.	The process adslist was not started because a script which is configured for global isolation (avscan.exe) is already running.

5.5.4 Ereignisprotokolle sichern

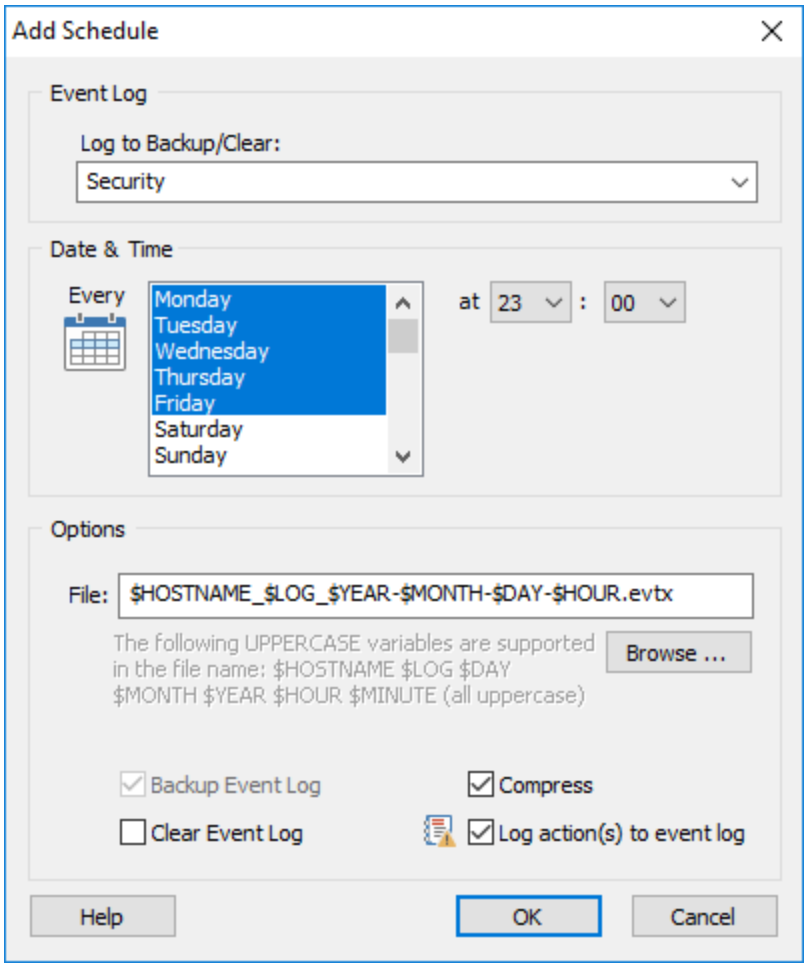
Das Sichern und/oder Löschen von Ereignisprotokollen kann so geplant werden, dass sie in bestimmten Intervallen ausgeführt werden; die Ergebnisse werden immer im Ereignisprotokoll protokolliert. Es können auch Warnungen ausgelöst werden, wenn ein Ereignisprotokoll voll ist.

Wenn Sie beim Sichern und Löschen der Ereignisprotokolle auf Probleme stoßen, finden Sie in KB-Artikel 21 eine Lösung für häufige Probleme.

Der Screenshot unten zeigt einen bestehenden Zeitplan, der das Ereignisprotokoll *Anwendung* jeden Montag um 5 Uhr morgens sichert. Das Ereignisprotokoll wird nicht gelöscht, und die Ergebnisse werden im Ereignisprotokoll protokolliert.



Um einen neuen Zeitplan hinzuzufügen, klicken Sie auf die Schaltfläche **+** neben der Zeitplanliste, um einen bestehenden Eintrag zu bearbeiten, **doppelklicken Sie** einfach **auf** den Eintrag:



Ereignisprotokoll

Wählen Sie entweder das zu sichernde/löschende Ereignisprotokoll aus dem Pulldown-Menü oder geben Sie den Protokollnamen manuell an. Um alle Ereignisprotokolle auf dem Computer zu sichern, geben Sie die Option "Alle Ereignisprotokolle" an.

Datum und Uhrzeit

Plant das Backup/Clearing so, dass es entweder an bestimmten Wochentagen, an bestimmten Tagen des Monats oder an beiden Tagen ausgeführt wird.

Sicherung

Die Angabe eines Dateinamens im Abschnitt "Datei" bewirkt, dass das Kontrollkästchen "Backup-Ereignisprotokoll" automatisch aktiviert wird; das Ereignisprotokoll wird in die angegebene Datei gesichert. Wir empfehlen Ihnen, die Erweiterung .evtx für den Dateinamen zu verwenden, um Verwechslungen zu vermeiden. Die folgenden Variablen **mit Berücksichtigung der Groß-/Kleinschreibung** werden in den Dateinamen unterstützt: **$HOSTNAME, $LOG, $DAY, $MONTH, $YEAR, $HOUR** und **$MINUTE**.

Ereignisprotokoll löschen

Durch Aktivieren des Kontrollkästchens "**Ereignisprotokoll löschen**" wird ein Ereignisprotokoll gelöscht. Das Ereignisprotokoll kann gelöscht werden, nachdem es gesichert wurde (wenn Sie einen Dateinamen angegeben haben), oder es kann gelöscht werden, ohne dass es gesichert wird.

komprimieren
Da die Ereignisprotokoll-Sicherungsdateien ziemlich groß sein können (abhängig von der Größe Ihres Ereignisprotokolls) und sich gut komprimieren lassen, können Sie die gesicherten Ereignisprotokoll-Sicherungsdateien automatisch komprimieren mit EventSentry. Komprimierte Dateien haben den gleichen Namen wie die Sicherungsdatei mit der Erweiterung .zip angehängt. Wenn beispielsweise der Name der Sicherungsdatei des Ereignisprotokolls **SRV01_Security_20070808.evt** lautet, dann lautet der Name des Archivs SRV01_Security_20070808.evt. **zip**.

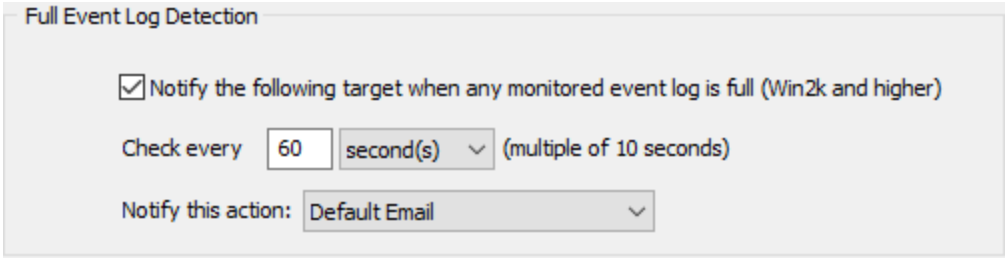
Wenn Sie dieses Kästchen ankreuzen, wird die Sicherungsdatei des Ereignisprotokolls nach der Sicherung automatisch komprimiert, und die unkomprimierte Version wird gelöscht. Die Größe der komprimierten Ereignisprotokoll-Sicherungsdateien beträgt normalerweise nur etwa 20% (oder weniger) ihrer ursprünglichen Dateigröße.

Da Ereignisprotokoll-Sicherungsdateien mit dem ZIP-Algorithmus komprimiert werden, können sie mit allen gängigen Komprimierungsprogrammen, wie z. B. 7-Zip, extrahiert bzw. dekomprimiert werden.

Protokoll Aktion(en) zum Ereignisprotokoll
Um eine Historie aller Sicherungs- und Löschaktionen im Ereignisprotokoll zu protokollieren, aktivieren Sie das Kontrollkästchen "**Aktion(en) im Ereignisprotokoll protokollieren**". Siehe Ereignisprotokolle für alle möglichen Ereignisprotokollaufzeichnungen, die durch diese Funktion protokolliert werden.

5.5.4.1 Erkennen voller Ereignisprotokolle

Wenn Sie mit Windows 2000 oder höher arbeiten, können Sie sich benachrichtigen lassen, wenn ein Ereignisprotokoll voll ist.



Alle von Ihren Filtern überwachten Ereignisprotokolle werden in dem von Ihnen angegebenen Intervall (muss ein Vielfaches von 10 Sekunden sein) überprüft. Wenn ein bestimmtes Ereignisprotokoll voll ist, wird die angegebene Smtp-Aktion benachrichtigt. Es werden keine Meldungen in die Ereignisprotokolle geschrieben. Es wird eine E-Mail mit folgendem Text versandt:

Das Ereignisprotokoll Sicherheit ist voll. Bitte erhöhen Sie die Größe des Ereignisprotokolls oder löschen Sie das Ereignisprotokoll. Bitte beachten Sie, dass dies eine reine E-Mail-Nachricht ist, die weder im Ereignisprotokoll der Anwendung noch in anderen Zielen erscheint.

5.5.4.2 Event Log

Die folgenden Ereignisse werden von dieser Funktion mit der Ereigniskategorie **Ereignisprotokollsicherung/Löschen** protokolliert.

Event ID	Event Description	Example

10300	An event log was cleared.	The Application event log was successfully cleared.
10301	An event log was successfully backed up.	Event log was successfully backed up: Event log: Application File: d:\eventlogs\srv01_app_20120329.evtx File size: 512000 kBytes Checksum: 9036E4F5137D957BF0E99176F9C062CE863540D243F7C594E1F54213C4BB259C
10302	An event log was successfully cleared and backed up.	Event log was successfully backed up and cleared: Event log: Application File: d:\eventlogs\srv01_app_20120329.evtx File size: 512000 kBytes Checksum: 9036E4F5137D957BF0E99176F9C062CE863540D243F7C594E1F54213C4BB259C
10303	An event log could not be cleared due to an error.	The Security event log could not be cleared due to the following error: Access is Denied.
10304	An event log could not be backed up due to an error.	The Security event log could not be backed up due to the following error: Access is Denied.
10305	An event log could not be cleared and backed up due to an error.	The System event log could not be cleared and backed up due to the following error: Access is Denied.
10306	The event log backup file "%1" could not be compressed due to the following error:	The event log backup file "C:\Logs\SRV01_Application_20070823.evt" could not be compressed due to the following error: Insufficient Memory.
10307	The event log backup file "%1" appears to have been compressed successfully, but the compressed event log backup file "%2" could not be verified. The original event log backup file will not be deleted.	The event log backup file "C:\Logs\SRV01_Application_20070823.evt" appears to have been compressed successfully, but the compressed event log backup file "C:\Logs\SRV01_Application_20070823.evt.zip" could not be verified. The original event log backup file will not be deleted.
10320	Full event logs cannot be detected.	Full event logs cannot be detected on this machine, this feature is not supported on this platform (only Windows 2000 or higher).

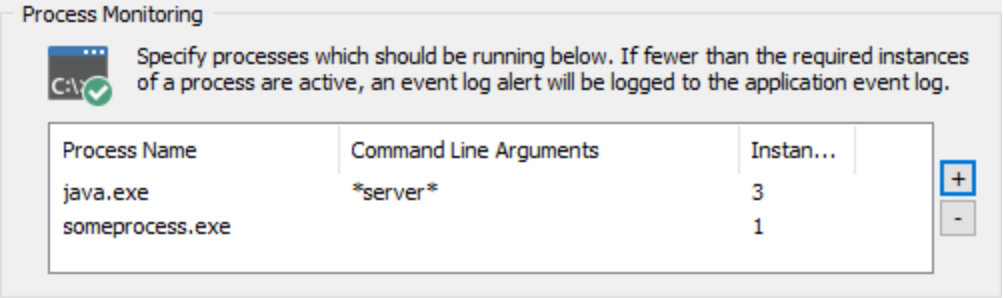
5.5.5 Prozessüberwachung

Die Prozessüberwachung erkennt, wenn ein erforderlicher Prozess inaktiv ist und kann die Befehlszeilenparameter eines Prozesses auswerten. Die Mindestanzahl der erforderlichen Instanzen eines Prozesses kann ebenfalls festgelegt werden.

Process Monitoring can also alert on inactive processes from a remote SNMP agent by polling SNMP counter values. Process monitoring alerts are identical between Windows and Non-Windows hosts.

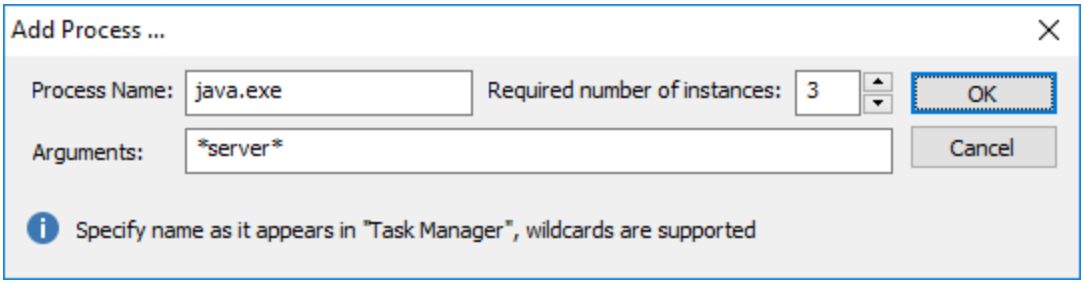
SNMP data is collected by the Heartbeat Agent.

Prozessüberwachung



Überwachung eines Prozesses
Um einen Prozess zu überwachen, klicken Sie auf die Schaltfläche **+** und geben Sie den Prozessnamen sowie die Anzahl der erforderlichen Instanzen an (Standard ist "1"). Für den Prozessnamen können Platzhalter angegeben werden, z.B. würde "java*" auf alle Prozesse passen, die mit "java" beginnen.

Kommandozeilen-Parameter
Sollen nur Prozesse mit bestimmten Kommandozeilenparametern ausgewertet werden, so kann auch die gewünschte Kommandozeile angegeben werden. Wird keine Kommandozeile angegeben, so wird diese ignoriert. Dieser Parameter unterstützt auch Wildcards.



Prozess-Netzwerkstatus (alias Netstat)
Zählt alle Prozesse auf, die über eine aktive TCP-Netzwerkverbindung verfügen, und stellt diese Informationen in den Web Reports zur Verfügung; es liefert die gleichen Daten wie der eingebaute Befehl netstat. Wenn "Änderungen erkennen" ausgewählt ist, erzeugt er optional auch einen Alarm, wenn ein Prozess beginnt, eine zuvor inaktive TCP-Verbindung zu überwachen und umgekehrt.

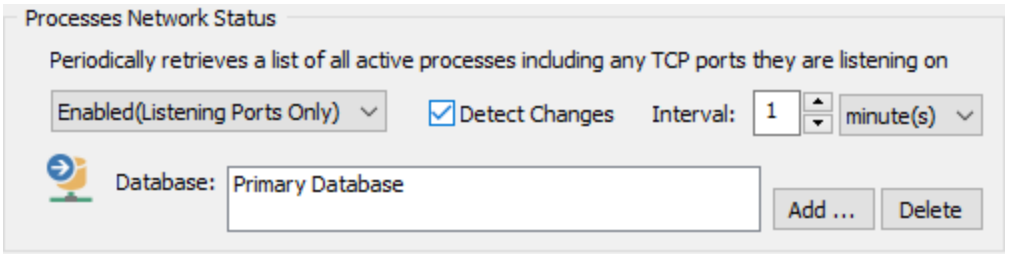
Die folgenden Optionen sind verfügbar:

- Aktiviert (alle Verbindungen): Zählt alle Prozesse auf, die über eine aktive TCP-Netzwerkverbindung verfügen, einschließlich sowohl client- als auch serverseitiger Prozesse.
- Aktiviert (Nur lauschende Ports): Zählt alle Prozesse auf, die auf eingehende TCP-Anforderungen lauschen, in der Regel serverseitige Prozesse wie Webserver, Datenbankserver und dergleichen.
- Deaktiviert

Änderungen erkennen
Erkennt, wenn sich ein zuvor geschlossener TCP-Port im aktiven Abhörzustand befindet oder wenn ein TCP-Port, der zuvor abgehört hat, jetzt geschlossen ist. Ereignisse werden mit der in den Optionen unten gewählten Ereignisschwere protokolliert.

Intervall
Bestimmt, wie oft der Prozesszustand aufgefrischt wird.

Datenbank
Legt die Datenbank fest, in der die Prozessdaten gespeichert werden.

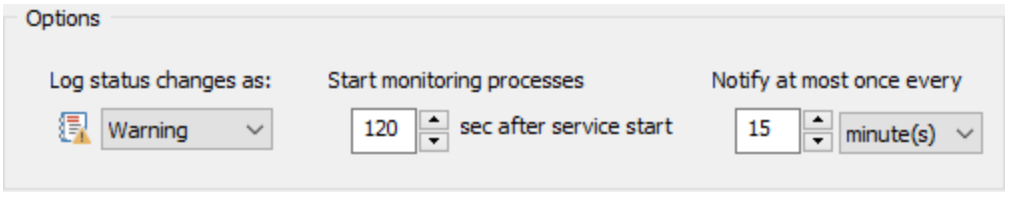


Die Funktion Prozessnetzwerkstatus ist nur auf Windows-basierten Hosts verfügbar.

Optionen
Der Schweregrad, mit dem ein Ereignis in das Ereignisprotokoll geschrieben wird, kann durch Ändern der Option "**Fehler protokollieren als**" unterhalb der Liste eingestellt werden. Wenn ein angegebener Prozess nicht aktiv ist, wird das Ereignis **10401** einmal in das Ereignisprotokoll geschrieben. Wenn der Prozess wieder aktiv wird, wird Ereignis **10402** im Ereignisprotokoll der Anwendung protokolliert (siehe auch Ereignisprotokoll).

Um Fehlalarme während des Systemstarts zu vermeiden, passen Sie die Startverzögerung entsprechend an. Stellen Sie einfach die Option "Überwachungsprozesse starten" auf die Anzahl von Sekunden ein, die es dauert, bis alle Prozesse aktiv sind.

"Benachrichtigung höchstens einmal alle" legt fest, wie oft eine Warnung erzeugt wird, wenn der/die erforderliche(n) Prozess(e) nicht aktiv ist/sind.



5.5.5.1 Event Log

Die folgenden Ereignisse werden von dieser Funktion mit der Ereigniskategorie **Prozessüberwachung** protokolliert.

Event ID	Event Description	Example
10401	%2 instance(s) of process "%1" on host %4 are active, but %3 instance(s) is/are required.	`0 instance(s) of process "eventsentry_gui.exe" on host server14 are active, but 1 instance(s) is/are required.`
10402	%2 instances of process "%1" is/are currently active on host %3.	`1 instances of process "eventsentry_gui.exe" is/are currently active on host server14.`

10410	A new process is listening for incoming TCP connections:
	
	Process Name: %1 (PID=%2)
	Local TCP Port: %3
	Local Address: %4
	
	Note: Connection requests may be blocked if a firewall is active.
		`A new process is listening for incoming TCP connections:`
		
		`Process Name: evilagent.exe (PID=20218)`
		`Local TCP Port: 2500`
		`Local Address: 192.168.15.56 [myserver.mydomain.local]`
		
		`Note: Connection requests may be blocked if a firewall is active.`

10411	A process previously listening for incoming TCP connections is no longer actively listening on this port:
	
	Process Name: %1 (PID=%2)
	Local TCP Port: %3
	Local Address: %4
		`A process previously listening for incoming TCP connections is no longer actively listening on this port:`
		
		`Process Name: evilagent.exe (PID=20218)`
		`Local TCP Port: 2500`
		`Local Address: 192.168.15.56 [myserver.mydomain.local]`

5.5.6 Festplattenkapazitätsüberwachung

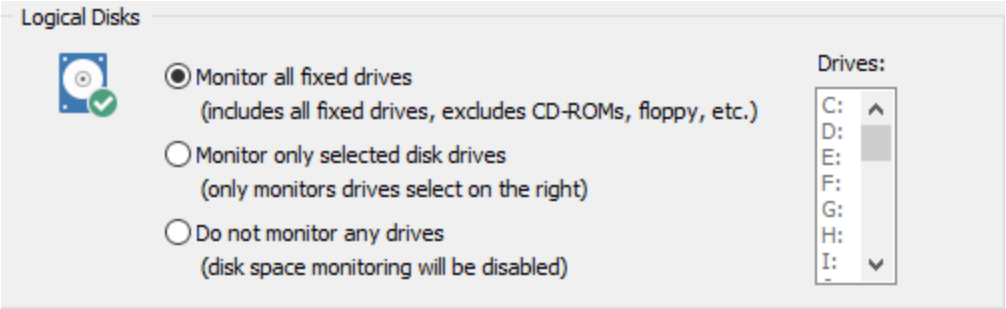
Überwacht die Speicherplatznutzung von festen Laufwerken und gibt Warnmeldungen aus, wenn Grenzwerte überschritten wurden oder sich Trendmuster geändert haben.

Die Festplattenplatzüberwachung kann Daten auch über SNMP von einem entfernten SNMP-Agenten erhalten, indem SNMP-Zählerwerte abgefragt werden. Die gesammelten Daten werden auf die gleiche Art und Weise wie die Windows-Daten zum Plattenplatz alarmiert und präsentiert.

SNMP-Daten werden vom Heartbeat-Agent gesammelt.

Logische Datenträger

Überwacht entweder alle festen Laufwerke oder nur ausgewählte Laufwerke. "Keine Laufwerke überwachen" kann verwendet werden, wenn in einem Paket nur die Verzeichnisüberwachung erforderlich ist. Bei der Überwachung logischer Laufwerke werden bei der Generierung von Alerts die Volumepunkte, auf die die Knotenpunkte zeigen, zur Berechnung der Gesamt-/Frei-Größe hinzugefügt.



Maximaler Benachrichtigungsintervall

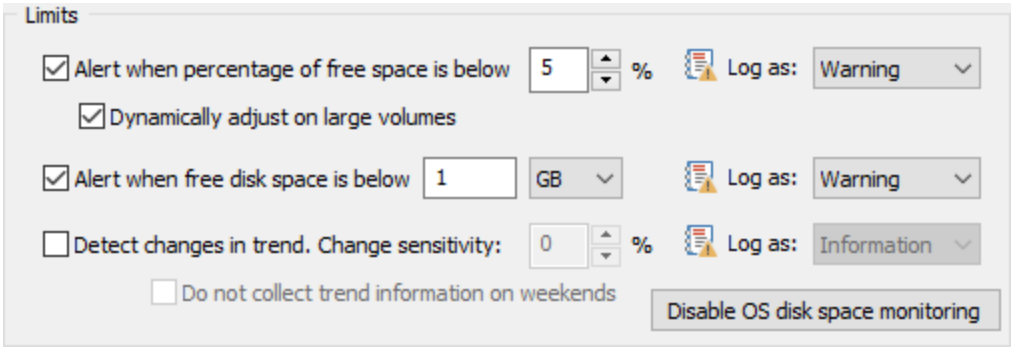
Protokolliert nur maximal ein Ereignis (pro Laufwerk) im angegebenen Intervall, während ein Laufwerk in einem Alarmzustand bleibt (z.B. Festplattenplatz unter einer absoluten oder prozentualen Grenze). Das maximale Benachrichtigungsintervall kann in den globalen Optionen konfiguriert werden.

Nur Windows: Wenn der Alarmstatus eines Laufwerks während des maximalen Benachrichtigungsintervalls zwischen "alarmiert" und "gelöscht" wechselt, z. B. wenn der Festplattenspeicher um den konfigurierten Schwellenwert herum ständig zu- und abnimmt, werden die unten angegebenen Benachrichtigungsgrenzen angewendet. Nicht mehr als

- 1 Alarm pro 30 Minuten
- 2 Alarme pro Stunde
- 3 Warnungen alle 3 Stunden
- 4 Warnungen alle 6 Stunden
- 5 Warnungen alle 12 Stunden
- 6 Warnungen alle 24 Stunden

Begrenzungen

Sie können die Grenzen entweder prozentual und/oder nach einer bestimmten Größe festlegen.



Prozentuale Begrenzungen

Um Grenzwerte auf der Grundlage des Prozentsatzes an freiem Speicherplatz festzulegen, wählen Sie die Option "**Alert when percentage of free space is below**" und geben Sie einen Prozentsatz an. Wenn diese Grenze überschritten wird, protokolliert EventSentry einen Eintrag im Anwendungsereignisprotokoll mit dem unter "**Log As**" angegebenen Schweregrad.

Dynamische Anpassungen: Bei größeren Laufwerken (z.B. > 1Tb) lösen prozentuale Grenzen oft zu früh Warnungen aus, da 5% von 1Tb immer noch 50Gb betragen. Diese Option verwendet einen proprietären Algorithmus, um die prozentuale Grenze dynamisch an einen nützlicheren Schwellenwert anzupassen. Der EventSentry-Agent protokolliert die Ereignis-ID 10509 (Information), welcher die

berechnete Grenze beschreibt. Diese Funktion unterstützt Laufwerke mit einer Gesamtkapazität von ~80 Gb oder mehr.

> ⚠ Dynamische Limits sind nur auf Windows-basierten Hosts verfügbar.

Absolute Limits

Um Grenzwerte auf der Grundlage der auf einem Laufwerk verfügbaren freien Bytes festzulegen, wählen Sie die Option "**Alert when free disk space is below**" und geben Sie die Anzahl der Megabytes oder Gigabytes an. Wenn diese Grenze überschritten wird, protokolliert EventSentry einen Eintrag mit dem unter "**Log As**" angegebenen Schweregrad im Application Event Log.

> ℹ Harte Begrenzungen, die auf eine höhere Zahl als die Gesamtmenge des auf einem Laufwerk verfügbaren Speicherplatzes gesetzt werden, werden ignoriert. Wenn das Limit z.B. so eingestellt ist, dass ein Alarm unterhalb von 200 Gb ausgelöst wird, die Gesamtgröße des Laufwerks aber nur 80 Gb beträgt, wird kein Alarm ausgegeben.

Überschreiben

Die Speicherplatzbeschränkungen können für jeden Host einzeln überschrieben/angepasst werden, wodurch vermieden wird, dass mehrere Speicherplatzpakete erstellt werden müssen, um unterschiedliche Beschränkungen für einige Hosts zu unterstützen. Siehe Override für weitere Details.

Trend-Erkennung

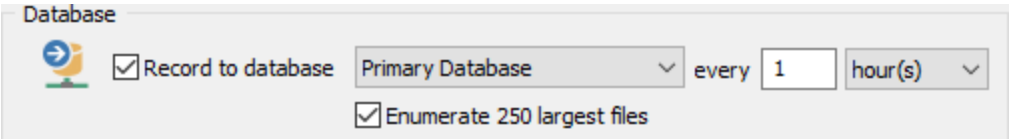
Die Speicherplatznutzung wird über längere Zeiträume erfasst, standardmäßig zwei Tage. EventSentry kann feststellen, ob die Plattenaktivität ungewöhnlich hoch ist, auch wenn ein prozentualer oder absoluter Grenzwert nicht überschritten wurde. Sie können die Empfindlichkeit der Trenderkennung anpassen, indem Sie den Prozentsatz anpassen.

Wenn eine Trendänderung festgestellt wird, protokolliert EventSentry einen Eintrag im Anwendungsereignisprotokoll mit dem unter "Log As" angegebenen Schweregrad. Wenn Sie an Wochenenden keine Speicherplatzinformationen sammeln möchten, aktivieren Sie das Kontrollkästchen "An Wochenenden keine Trendinformationen sammeln".

Beispiel: Wenn der freie Speicherplatz täglich um etwa 100 Mb abnimmt, dann würde eine Abnahme von 200 Mb als 100%ige Änderung betrachtet werden.

Plattenplatz-Datenerfassung

Wenn Sie "In Datenbank aufnehmen" wählen, werden historische Speicherplatzdaten in der Datenbank gespeichert und diese Daten in den Web-Reports zur Verfügung gestellt.



Bitte beachten Sie, dass Volumes, auf die durch Knotenpunkte verwiesen wird, bei der Aufzeichnung von Festplattenplatzinformationen in der EventSentry-Datenbank nicht berücksichtigt werden.

Die 250 größten Dateien aufzählen

Wenn diese Option ausgewählt wird, stellt EventSentry die 250 größten Dateien auf jedem überwachten Volume in den Web Reports zur Verfügung.

Deaktivieren der Überwachung des OS-Plattenplatzes

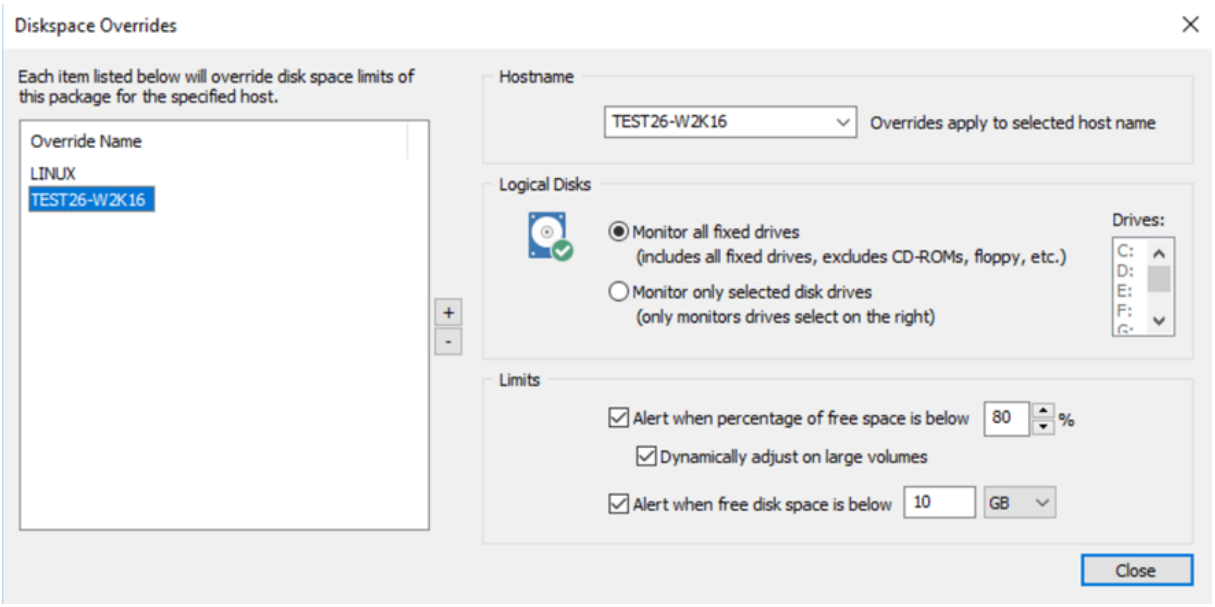
Windows schreibt automatisch einen Eintrag in das Ereignisprotokoll, wenn der freie Plattenplatz unter 10% liegt. Um doppelte Speicherplatzbenachrichtigungen zu vermeiden, können die eingebauten Warnungen des Betriebssystems durch Klicken auf die Schaltfläche "**Deaktivieren der Speicherplatzüberwachung des Betriebssystems**" deaktiviert werden.

Wenn Sie zu einem späteren Zeitpunkt Ihre Meinung ändern, können Sie die Überwachung des Betriebssystems wieder aktivieren, indem Sie auf die gleiche Schaltfläche klicken (auf der dann "**Überwachung des Betriebssystems aktivieren**" steht).

5.5.6.1 Anpassung

Das Dialogfeld "Speicherplatz überschreiben" kann verwendet werden, um die Speicherplatzeinstellungen pro Host anzupassen, ohne mehrere Speicherplatzpakete erstellen und zuweisen zu müssen. Wenn Sie auf die Schaltfläche "Überschreiben" klicken, wird das Dialogfeld "Festplattenplatzüberschreibungen" angezeigt, in dem mehrere Hosts hinzugefügt werden können.

Um einen Host hinzuzufügen, klicken Sie einfach auf das **+-Symbol** und wählen Sie einen vorhandenen Host aus dem Dropdown-Dialogfeld " **Hostname"** aus und geben Sie die angepassten Einstellungen an. Um benutzerdefinierte Einstellungen zu entfernen und zu den Standardeinstellungen aus dem Paket zurückzukehren, wählen Sie den Host aus und klicken Sie auf die Schaltfläche **-**. Wenn Sie auf **Schließen** klicken, werden alle Einstellungen gespeichert.



5.5.6.2 Event Log

Die folgenden Ereignisse werden von dieser Funktion mit der Ereigniskategorie **Plattenplatzüberwachung** protokolliert.

Event ID	Event Description	Example

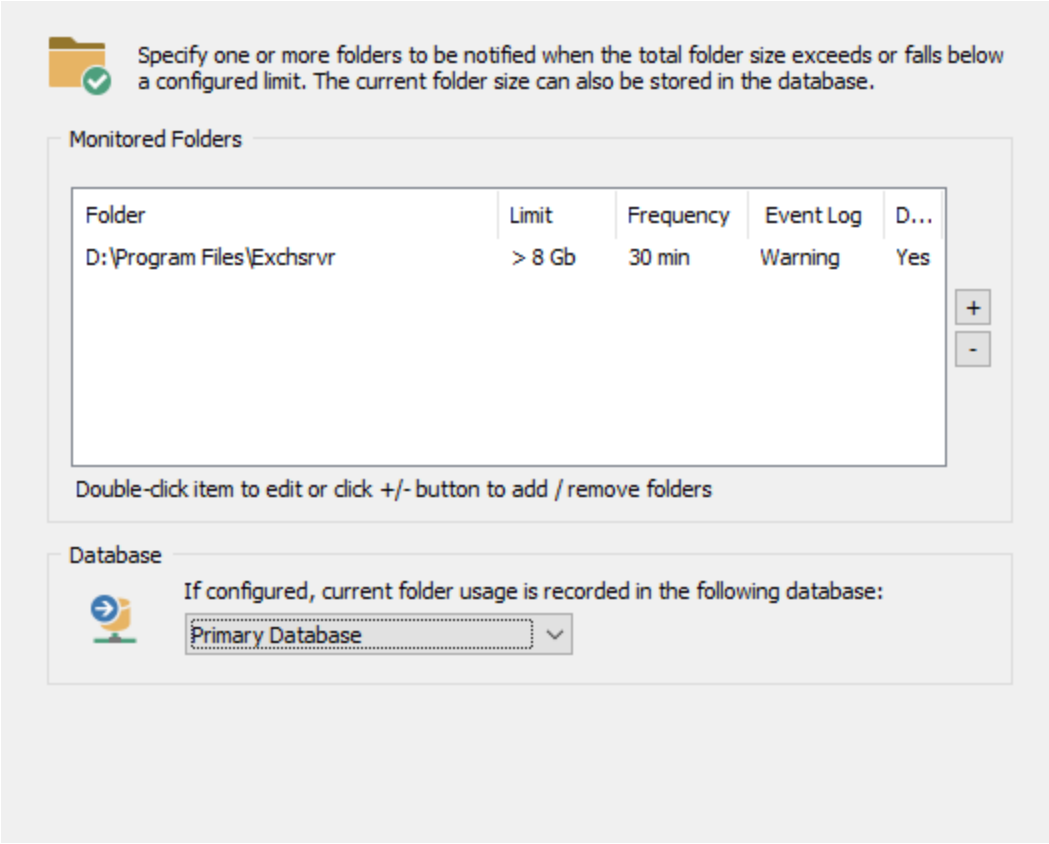
10500	Disk space is below a configured percentage limit.	Free disk space for drive C: (BOOT) is below the configured limit of 15 percent. 12 percent of disk space (756 Mb) are currently available on drive C:\. Top 5 Directories: 001: [16.84 GB] C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL (18084796490 bytes) 002: [4.01 GB] C:\System Volume Information (4307181526 bytes) 003: [2.71 GB] C:\Windows\winsxs (2909796747 bytes) 004: [1.89 GB] C:\Users\bax (2030310546 bytes) 005: [1.89 GB] C:\Users\bax\AppData\Local\Microsoft\Windows (2030179456 bytes) Top 5 Files: 001: [15.87 GB] C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA\tempdb.mdf (17043095552 bytes) 002: [3.97 GB] C:\System Volume Information\{a9bac31b-02fc-11e7-89ee-00101915f0e6}{1843876b-c276-3e48-b7ae-04046e6cc752} (4261412864 bytes) 003: [920 MB] C:\Windows\SoftwareDistribution\DataStore\DataStore.edb (964755456 bytes) 004: [800 MB] C:\pagefile.sys (838860800 bytes) 005: [496 MB] C:\Windows\winsxs\ManifestCache\a786a517e28d5687_blobs.bin (520795521 bytes)
10501	Disk space is below a configured absolute limit.	Free disk space for drive C: is below the configured limit of 1024 Mb. 877 Mb of disk space are currently available on drive C:. Top Directories: *e 10500 event above* Top Files: *e 10500 event above*
10502	Trend analysis has detected an usually high disk space consumption.	Trend analysis has determined unusual high disk usage on drive D:. The average recorded trend on drive D: was 8976 kb, the current trend was 25432 kb, an increase of 283%. If this trend change is expected (for example, caused by a daily backup routine) then you will see this message two more times before the pattern is recognized. With the recorded trend, disk space will be exhausted in 62 days, with the current trend in 15 days.
10504	Delayed directory file analysis is complete	Directory and file analysis of drive E: has been initiated by an earlier 10500 or 10501 event and is now complete. Top 5 Directories:

		001: [16.84 GB] C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL (18084796490 bytes) 002: [4.01 GB] C:\System Volume Information (4307181526 bytes) 003: [2.71 GB] C:\Windows\winsxs (2909796747 bytes) 004: [1.89 GB] C:\Users\bax (2030310546 bytes) 005: [1.89 GB] C:\Users\bax\AppData\Local\Microsoft\Windows (2030179456 bytes) Top 5 Files: 001: [15.87 GB] C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA\tempdb.mdf (17043095552 bytes) 002: [3.97 GB] C:\System Volume Information\{a9bac31b-02fc-11e7-89ee-00101915f0e6}{1843876b-c276-3e48-b7ae-04046e6cc752} (4261412864 bytes) 003: [920 MB] C:\Windows\SoftwareDistribution\DataStore\DataStore.edb (964755456 bytes) 004: [800 MB] C:\pagefile.sys (838860800 bytes) 005: [496 MB] C:\Windows\winsxs\ManifestCache\a786a517e28d5687_blobs.bin (520795521 bytes)
10509	Percent limit has been dynamically adjusted	The percentage-based threshold on drive C: has been dynamically adjusted from 5% percent to 1.58% percent based on the total drive size of 129 GB. A low disk space alert will be triggered when the available space on this volume falls below 841 MB.
10550	Disk space is back above the percentage limit.	Free disk space for drive C: (BOOT) is back above the configured limit of 15 percent. 20 percent of disk space (1120 Mb) are currently available on drive C:
10551	Disk space is back above the absolute limit.	Free disk space for drive C: (BOOT) is back above the configured limit of 1024 Mb. 1325 Mb of disk space are currently available on drive C:.

5.5.7 Verzeichnisüberwachung

Die Verzeichnisüberwachung überwacht die Größe oder die Anzahl der Dateien eines Verzeichnisses und löst Warnmeldungen aus, wenn die Gesamtgröße (oder die Anzahl der Dateien) eines Verzeichnisses entweder über oder unter einer festgelegten Grenze liegt. Zusätzliche Konfigurationsoptionen, z.B. ob die physische oder die logische Größe eines Verzeichnisses überwacht werden soll und ob Unterverzeichnisse einbezogen werden sollen, sind verfügbar.

Die Verzeichnisüberwachung ist Teil der Festplattenkapazitätsüberwachung und kann entweder zu einem bestehenden Paket welches bereits ein Festplattenkapazitätsüberwachungsobjekt enthält, oder zu einem neuen Paket hinzugefügt werden.



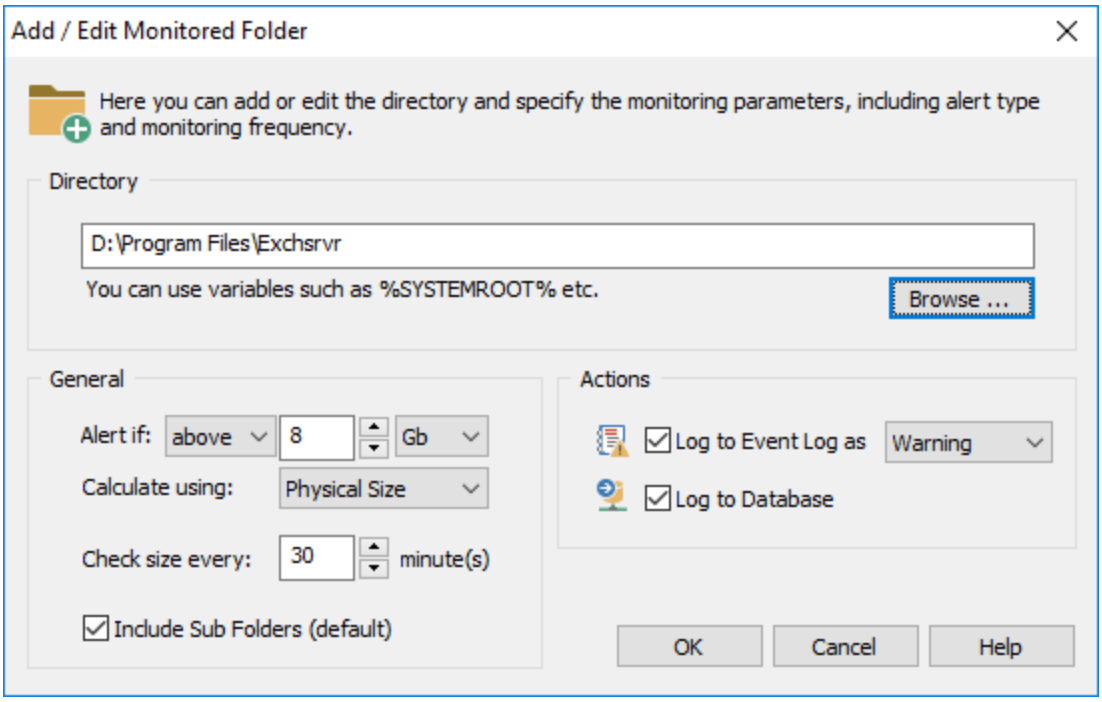
Hinzufügen zu einem vorhandenen Objekt

Um diese Funktion zu einem vorhandenen Paket hinzuzufügen, wählen Sie einfach das Objekt "Disk Space" im Paket und klicken Sie auf die Registerkarte "**Directory Monitoring"**.

Erstellen eines neuen Pakets

Erstellen Sie ein neues Paket, indem Sie mit der rechten Maustaste auf den Container "System Health Packages" klicken, und fügen Sie dem Paket ein neues "Disk Space"-Objekt hinzu, indem Sie mit der rechten Maustaste auf das Paket klicken und "Hinzufügen" wählen. Sie können auch ein vorhandenes System Health Package auswählen, das bereits ein "Disk Space"-Objekt enthält, und im linken Fensterbereich darauf klicken.

Da das Paket nur zur Überwachung von Verzeichnissen verwendet wird, sollte "Logical Disks" auf "Do not monitor any drives" konfiguriert werden. Die eigentlich Konfiguration kann dann in der Registerkarte "Directory Monitoring" vorgenommen werden.



Datenbank

Geben Sie die Datenbank an, die verwendet werden soll, wenn ein Verzeichnis so konfiguriert wird, dass die aktuelle Größe in der zentralen Datenbank aufgezeichnet wird.

Überwachung eines Verzeichnisses

Um ein neues Verzeichnis zu überwachen, klicken Sie auf die Schaltfläche **+** oder doppelklicken Sie auf ein vorhandenes Verzeichnis.

Verzeichnis

Wählen Sie das Verzeichnis aus, das Sie überwachen möchten, z. B. D:\Payroll; Sie können auch Umgebungsvariablen wie %SYSTEMROOT% verwenden. Die Überwachung eines UNC-Pfads (wie z.B. \ \SERVER1\Payroll) wird **nicht unterstützt;** Sie müssen das reale Verzeichnis der Netzwerkfreigabe verwenden, wie z.B. D:\Payroll.

Allgemein

Geben Sie die Größen- oder Dateianzahlbegrenzung des Ordners an. Grenzwerte können entweder in Mb, Gb, Tb angegeben werden. Um die Anzahl der Dateien zu überwachen, setzen Sie diese Option auf "Dateien".

Geben Sie auch an, ob die Größe des Ordners anhand der physischen Größe oder der logischen Größe der Dateien berechnet werden soll (dies wird bei der Überwachung der Dateianzahl ignoriert). Da die Festplatten in Sektoren angeordnet sind, ist die physische Größe normalerweise etwas größer als die logische Größe, mit Ausnahme von Ordnern, bei denen die Komprimierung aktiviert ist. Diese Verzeichnisse haben in der Regel eine geringere physische Größe, weshalb die Berechnung der physischen Größe die **Standardeinstellung und empfohlene Einstellung** ist.

Geben Sie an, wie oft der Agent das Verzeichnis überprüfen soll. Da die Berechnung einer Verzeichnisgröße bei größeren Verzeichnissen ressourcenintensiv sein kann, stellen Sie dieses Intervall entsprechend ein.

Aktivieren Sie das Kontrollkästchen "Unterordner einbeziehen", um Unterverzeichnisse in die Berechnung der Gesamtgröße einzubeziehen.

Aktionen

Zum Ereignisprotokoll anmelden als: Protokolliert einen Alert mit dem angegebenen Schweregrad im Ereignisprotokoll der Anwendung, wenn der konfigurierte Schwellenwert überschritten wird. Weitere Einzelheiten zu Ereignissen, die mit dieser Funktion protokolliert werden können, finden Sie unter Ereignisprotokoll.

Zur Datenbank anmelden: Zeichnet die aktuelle Verzeichnisgröße in der im übergeordneten Dialog ausgewählten Datenbank auf.

5.5.7.1 Event Log

Die folgenden Ereignisse werden von dieser Funktion mit der Ereigniskategorie **Festplattenkapazitätsüberwachung** protokolliert.

Event ID	Event Description	Example

10510	The directory size is above the configured limit.	`The physical size of folder "C:\TempStorage" is above the configured limit of 1,048,576 bytes.`
		
		`Folder Information:`
		`Logical Size: 41,864,341`
		`Physical Size: 42,192,896`
		`Files: 115`

10511	The directory size is below the configured limit.	`The physical size of folder "C:\TempStorage" is below the configured limit of 100,048,576 bytes.`
		
		`Folder Information:`
		`Logical Size: 41,864,341`
		`Physical Size: 42,192,896`
		`Files: 129`

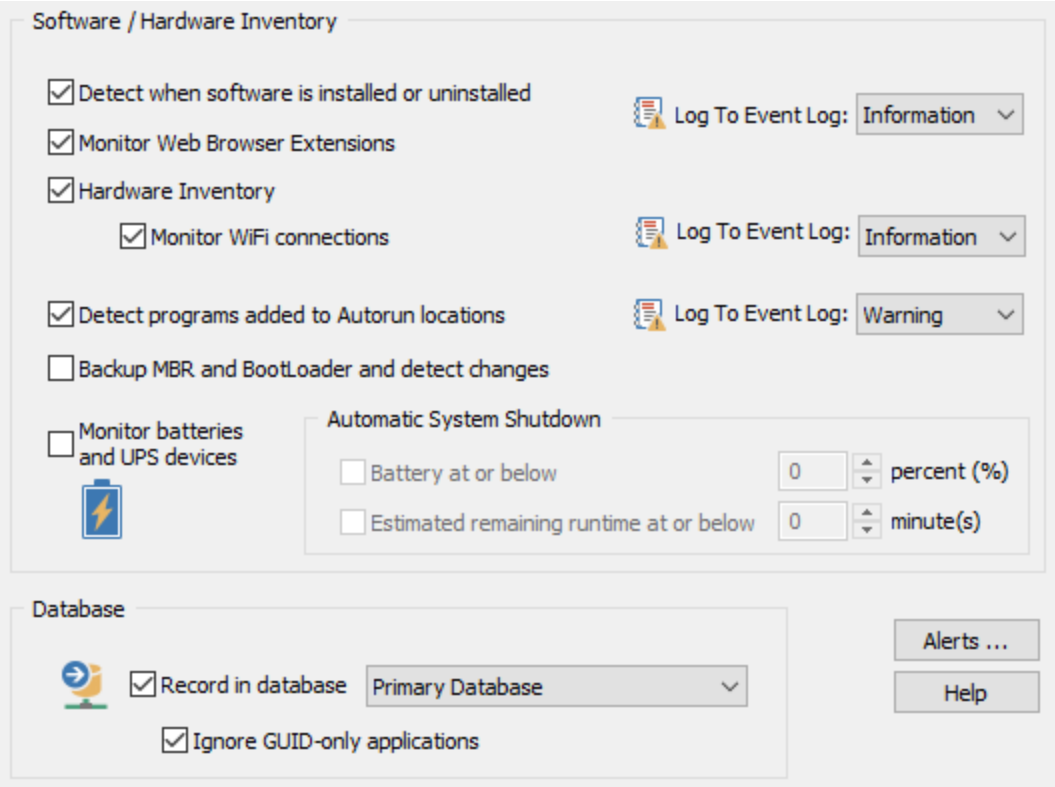
10512	The number of files in the folder exceeded the maximum threshold.	`The maximum file count of 500 files in folder "C:\MySoftware\Temp" was exceeded, 506 files were found.`
		
		`Folder Information:`
		`Logical Size: 41,864,341`
		`Physical Size: 42,192,896`
		`Files: 506`

10513	The number of files in the folder is below the minimum.	`Folder "C:\MySoftware\Temp" contains 488 files, which is below the minimum of 500 files.`
		
		`Folder Information:`
		`Logical Size: 41,864,341`
		`Physical Size: 42,192,896`
		`Files: 488`

10560	The directory size is back below the configured limit.	The physical size of folder "C:\TempStorage" is back below the configured limit of 1,048,576 bytes. Folder Information: Logical Size: 964,341 Physical Size: 964,512 Files: 45.
10561	The directory size is back above the configured limit.	The physical size of folder "C:\TempStorage" is back above the configured limit of 1,048,576 bytes. Folder Information: Logical Size: 41,864,341 Physical Size: 42,192,896 Files: 129.
10562	Number of files in folder is back below the limit.	The number of files (231) in folder "C:\MySoftware\Temp" is back below the configured limit of 500 files. Folder Information: Logical Size: 11,864,341 Physical Size: 12,192,896 Files: 231
10563	The number of files in the folder is back above the minimum.	The number of files (893) in folder "C:\MySoftware\Temp" is back above the configured limit of 500 files. Folder Information: Logical Size: 92,864,341 Physical Size: 93,192,896 Files: 893

5.5.8 Software/Hardware-Inventar

Die Software-/Hardware-Bestandsaufnahme bietet ein vollständiges, durchsuchbares Inventar von Hardware, Software, Patches und virtuellen Maschinen sowie die Möglichkeit, Warnmeldungen auszugeben, wenn Software (un)installiert wird oder wenn sich Anwendungen in bestimmten Registrierungsschlüsseln registrieren. In Kombination mit der Service-Überwachung und der Datei-Überwachung erkennt EventSentry den Großteil der am System vorgenommenen Änderungen.



Inventar virtueller Maschinen (Hyper-V, Proxmox & VMWare)

Inventarisiert alle virtuellen Maschinen von Hyper-V, Proxmox- oder VMWare-Hosts sowie die Versionsnummer des Hosts der virtuellen Maschine. Die Hyper-V-Inventarisierung wird automatisch durchgeführt, wenn Hyper-V auf dem Host erkannt wird, auf dem der EventSentry-Agent ausgeführt wird. Proxmox-Inventarinformationen werden ueber SSH abgerufen, VMWare-Inventarinformationen werden über SNMP abgerufen, wenn die erforderlichen SNMP-OIDs vorhanden sind. Die folgenden Informationen sind verfügbar:

Host der virtuellen Maschine
- Name des Gastgebers
- Produkt-Name
- Produkt-Version

Virtuelle Maschinen
- Name des Gastgebers
- Stand
- CPU-Zählung
- Erinnerung
- Betriebssystem (falls verfügbar)

> Für die Proxmox-Inventarisierung müssen SSH-Anmeldedaten konfiguriert werden, für die Inventarisierung von VMWare ist es erforderlich, dass SNMP auf den VMWare ESXi-Hosts aktiviert ist.

WiFi-Verbindungen überwachen

Verfolgt alle WiFi-Aktivitäten und zeigt an, mit welchem drahtlosen Netzwerk ein Adapter verbunden ist, sowie einen Verlauf aller Verbindungen und Trennungen. Der %PRODUCT%-Agent protokolliert außerdem jedes Mal, wenn ein Adapter eine Verbindung zu einem WiFi-Netzwerk herstellt oder trennt, Ereignisse im Ereignisprotokoll, was die Automatisierung durch Filter ermöglicht.

Die folgenden Details sind verfügbar:

- Name und GUID des Adapters
- Status
- Signalstärke
- SSID
- Verschlüsselung (z.B. RSNA mit PSK)
- Authentifizierung (z. B. CCMP)

Überwachung von Batterien und USV-Geräten

Überwacht eingebaute Batterien in Laptops sowie angeschlossene USV-Geräte (falls von Windows erkannt). Der aktuelle Akkustatus, der Ladezustand sowie die gesamte Akkukapazität sind auf der Seite "Host / Inventar" in der webbasierten Berichterstattung verfügbar. EventSentry kann auch einen Host herunterfahren, wenn der Akkustatus unter einen konfigurierbaren prozentualen Schwellenwert fällt oder wenn die geschätzte Laufzeit unter einem voreingestellten Grenzwert liegt, unabhängig vom Hersteller und/oder Modell der USV.

MBR und BootLoader sichern und Änderungen erkennen

Lädt sowohl die Sektoren 0-77 als auch die Sektoren 2048-2057 aller Festplatten des überwachten Systems herunter. Wenn Änderungen in den überwachten Sektoren festgestellt werden, wird ein Ereignis protokolliert, das angibt, wie viele Bytes geändert wurden und ob der MBR oder der BootLoader geändert wurde. Alle überwachten Sektoren werden auch beim Start des Agenten in der Datenbank gespeichert (falls aktiviert) und können auf der Seite "Host / Inventar" in der webbasierten Berichterstattung heruntergeladen werden.

Diese Funktion soll einen gewissen Schutz gegen bestimmte Ransomware-Infektionen bieten. Die Ereignisse, die protokolliert werden, wenn überwachte Sektoren geändert werden, können verwendet werden, um Aktionen wie Ruhezustand, Abmeldung oder Herunterfahren auszulösen. Die Sektor-Backups können auf eine USB-Stick heruntergeladen und manuell wiederhergestellt werden, falls die ursprünglichen Sektoren überschrieben wurden.

Software-Bestandsaufnahme

Wenn eine Anwendung installiert ist und sich in der Systemsteuerung unter Programme hinzufügen/entfernen registriert, benachrichtigt EventSentry Sie und protokolliert, welche Anwendung installiert oder entfernt wurde.

Wenn sich eine Anwendung nicht selbst unter Software registriert, z. B. wenn sie auf einer Pro-Benutzer-Basis installiert wird, wird sie von EventSentry nicht erkannt. Sie werden möglicherweise trotzdem benachrichtigt, wenn sich die Anwendung in einem der vielen Autorun-Registrierungsschlüssel registriert.

Die folgenden Informationen werden in der Datenbank gespeichert und können über die Web Reports abgefragt werden, wenn das Kontrollkästchen "In Datenbank aufnehmen" aktiviert ist:

- Name der Software
- Installationsverzeichnis*
- Software-Herausgeber*

- Software-Version*
- Plattform-Informationen (32-Bit vs. 64-Bit)

Mit dieser Funktion wird auch die Anwendungshistorie in die Datenbank geschrieben, so dass Sie herausfinden können, wann Software installiert/deinstalliert wurde (beachten Sie, dass diese Informationen möglicherweise auch über die Ereignisprotokolle verfügbar sind).

Überwachung von Web-Browser-Erweiterungen

Überwachen Sie alle installierten Erweiterungen für die folgenden Webbrowser

- Mozilla Firefox
- Google Chrom
- Microsoft Edge (auf Chrombasis)

und bietet eine vollständige Bestandsaufnahme/Historie sowie Warnmeldungen, wenn Erweiterungen installiert oder deinstalliert werden. Browserprofile werden ebenfalls unterstützt. Die folgenden Erweiterungsinformationen werden erfasst:

- Name
- Herausgeber
- Version
- Aktiviert/Deaktiviert
- Herausgeber (wenn verfügbar)
- Benutzername

Bitte beachten Sie unten die Einschränkungen dieser Funktion, da es keinen offiziellen Standard gibt, wie Browser-Erweiterungen gespeichert werden.

- Unter bestimmten Umständen wird der Erweiterungsname nicht angezeigt; in diesem Fall wird stattdessen der Herausgeber angezeigt.
- Eine Erweiterung wird als **aktiviert** angezeigt, wenn sie in mehreren Profilen installiert und in mindestens einem Profil aktiviert ist.

Patch-Bestand

Alle installierten Microsoft-Patches werden gesammelt und können über die Web Reports abgefragt werden. EventSentry kann auch Warnmeldungen ausgeben, wenn ein Patch (un)installiert wird. Die folgenden Informationen sind verfügbar:

- Patch-Name
- Plattform-Informationen (32-Bit vs. 64-Bit)
- Installationsdatum
- Installationsverzeichnis (falls zutreffend)
- Herausgeber

Hardware-Inventar

Die folgenden Hardware-Informationen werden erfasst; Hardware-Informationen werden durch Dateiinformationen, Registrierungsdaten und WMI erhalten.

- Betriebssystem, einschließlich Edition und Service Pack
- Der Lokation des SYSTEMROOT-Verzeichnisses
- Datum an dem das Betriebssystem installiert wurde

- Ob auf dem Rechner die x64-Bit-Edition des Betriebssystems läuft
- Konfigurierte UAC-Ebene (Vista und höher)
- Ob es sich bei dem Rechner um einen Terminalserver handelt, auf dem Hyper-V oder Server-Core läuft
- Wenn es sich bei der Maschine um eine virtuelle Maschine handelt, und in einigen Fällen den Typ der VM-Plattform (z. B. VMWare ESX)
- Installierte CPU's (einschließlich Typ, Geschwindigkeit und Anzahl der installierten CPU's)**
- Die Anzahl der installierten CPUs, einschließlich Hyper-Threading und Multi-Core-Erkennung
- Eingetragener Eigentümer und eingetragenes Unternehmen** (falls verfügbar)
- Computerhersteller und -modell** (falls verfügbar)
- Chassis-Typ (z.B. Rack-Montage, Mini-Tower, Laptop, usw.)
- Garantieinformationen (nur für DELL-, HP-, IBM- und Lenovo-Hardware)
- BIOS-Version***
- Seriennummer, Service-Tag (je nach Hersteller)***
- Installierter Speicher, einschließlich des maximalen Speichers, der Anzahl der installierten Speicherchips und der verfügbaren freien Steckplätze
- Installierte Netzwerkadapter, einschließlich Adaptername, Verbindungsgeschwindigkeit, IP-Adresse (regelmäßig aktualisiert und aufgefrischt) und MAC-Adresse
- Installierte Festplattencontroller, einschließlich Adaptername, Adaptertyp (IDE/SCSI) und Hersteller
- Fabrikat der installierten Grafikkarte
- Die Anzahl der CD-ROM-, DVD-, Disketten- und Wechsellaufwerke
- Die aktuelle Laufzeit
- Die maximale Laufzeit des Hosts seit der Installation von EventSentry
- Höchste unterstützte USB-Version

Grundlegende System- und Hardware-Informationen können auch über SNMP von einem entfernten SNMP-Agenten bezogen werden indem SNMP-Werte abgefragt werden. Dazu gehören (sofern verfügbar):

- Informationen zum System
- Netzwerk-Schnittstellen
- Informationen zu Prozessor, Speicher und Festplattenplatz
- Informationen zur Betriebszeit

SNMP-Daten werden vom Heartbeat-Agent gesammelt.

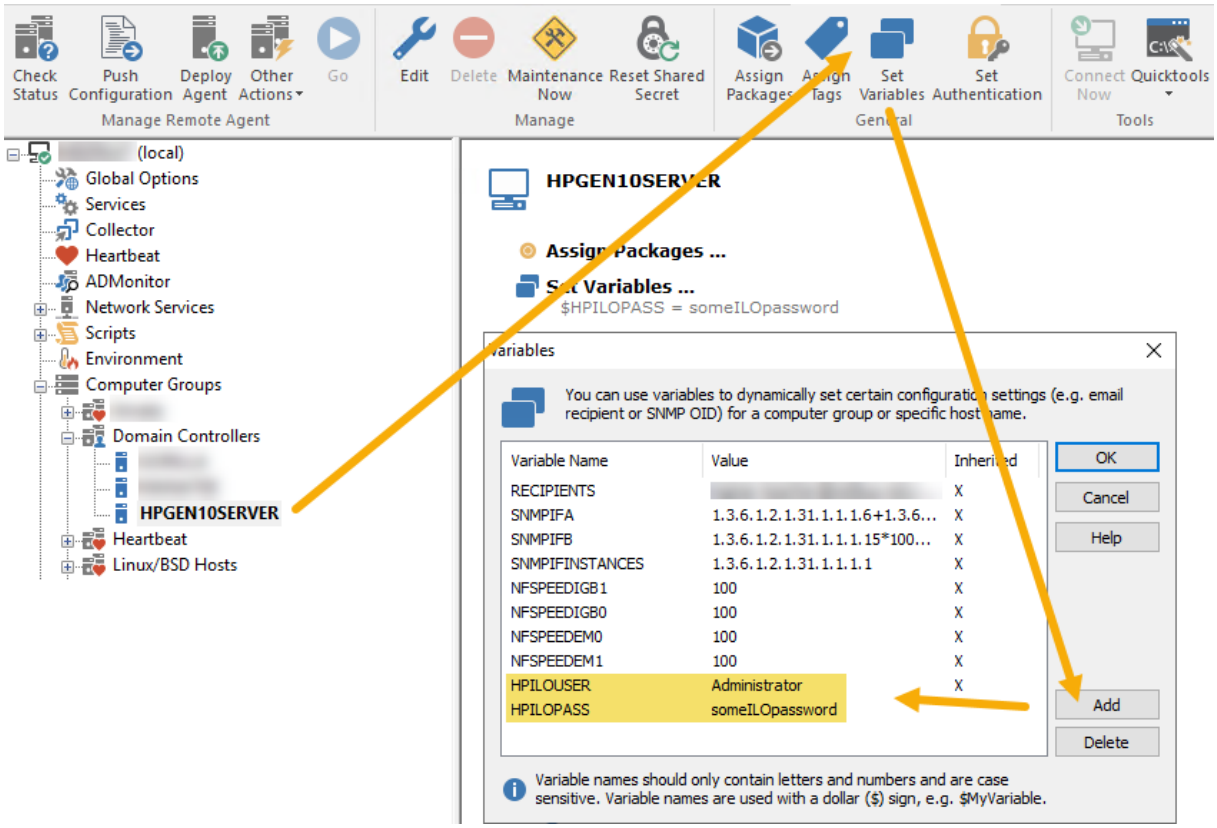
Auf DELL©- und HP©-Servern, auf denen die entsprechenden Systemverwaltungstools der Hersteller installiert sind, erfasst EventSentry nach der Installation auch die folgenden Informationen:

- Status von redundanten Stromversorgungen (PSUs)
- Aktuelle Temperatur der installierten Temperatursensoren
- Aktueller Status und Drehzahl der installierten Ventilatoren
- Verfügbarkeit und IP-Adresse aller installierten Fernverwaltungskarten
- Status und Details jedes installierten Hardware-RAID-Controllers (z.B. Modellnummer, Cache-Größe, Firmware-Version)
- Status aller konfigurierten RAIDs (einschließlich Stripe-Größe (falls verfügbar), Status, Raid-Level)
- Status aller installierten physischen Festplatten, einschließlich Laufwerksdetails wie Modellnummer, Seriennummer

HP GEN 10+ SERVERS: Ab der Generation 10 ist für das Erfassen von erweiterten Hardware-Informationen von HP-Servern - mit Ausnahme von Informationen über physische Festplatten (Raids) - eine iLO-Karte erforderlich, die nicht dieselbe Netzwerkschnittstelle wie das Windows-Betriebssystem nutzen darf.

Da iLO-Karten eine Authentifizierung erfordern, müssen auf dem/den Host(s) oder der/den Gruppe(n) von Servern mit iLO-Karten der Generation 10 zwei Variablen gesetzt werden:

HPILOUSER*iLO User*
HPILOPASS*Passwort*



Setzen einer Variable für den Zugriff auf eine HP Gen10 iLO

Beim Start des Agenten kann die Hardware-Bestandsaufnahme-Funktion auch ein Ereignis im Ereignisprotokoll protokollieren, wenn sich die Anzahl der folgenden installierten Hardware-Geräte seit der letzten Ausführung des EventSentry-Agenten geändert hat:

- Installierter Speicher
- Anzahl der installierten Prozessoren
- Anzahl der installierten Diskettenlaufwerke
- Anzahl der installierten CDROM-Laufwerke
- Anzahl der installierten DVD-Laufwerke
- Anzahl der Wechsellaufwerke
- Verbindungsgeschwindigkeit eines Netzwerkadapters
- Hinzufügen/Entfernen eines USB-Laufwerks
- S.M.A.R.T.-Statusfehler eines physikalischen Laufwerks

Ignorieren Sie reine GUID-Anwendungen: Einige Software schreibt bei der Installation nur die GUID (eine hexadezimale Zahl) in die Registrierung. Aktivieren Sie dieses Kontrollkästchen, um Software ohne einen sinnvollen Anzeigenamen zu ignorieren.

Die System-Hardware-Informationen werden bei jedem Start des EventSentry-Dienstes aktualisiert.

Überwachung der Betriebszeit

Die aktuelle Betriebszeit eines Hosts wird alle 5 Minuten aktualisiert und bietet die folgenden Funktionen:

- Verfolgt die maximale Betriebszeit über mehrere Neustarts hinweg. Dies kann helfen problematische Server, die häufig neu gestartet werden, zu isolieren.
- Speichert die Uptime-Historie in der Datenbank, auf die über Heartbeat - Availability - Uptime History zugegriffen werden kann. Die Uptime-Historie wird bei jedem Booten des Betriebssystems aktualisiert und zeichnet auf, wie lange das Betriebssystem vor dem aktuellen Boot-Prozess lief.

Der Betriebszeitverlauf verfolgt, wie lange das Betriebssystem zwischen den Neustarts lief, und wird nur aktualisiert, wenn Sie einen Host neu starten.

Autorun-Registrierungsschlüssel

Einige Anwendungen registrieren Dateien, die automatisch ausgeführt werden, wenn der Computer gestartet wird oder wenn sich ein Benutzer am System anmeldet. Während diese Dateien normalerweise erforderlich und harmlos sind, werden sie leider von Spyware, Trojanern und Viren missbraucht.

EventSentry überwacht bestimmte Registrierungsorte und benachrichtigt Sie, wenn eine Anwendung an einem der überwachten Orte hinzugefügt oder entfernt wird. Bitte beachten Sie, dass zu diesem Zeitpunkt nur die Registrierungsschlüssel HKEY_LOCAL_MACHINE überwacht werden, die alle Benutzer des Systems betreffen. HKEY_CURRENT_USER-Schlüssel werden nicht überwacht.

EventSentry überwacht die folgenden Registrierungswerte:

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Taskman
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Shell
```

EventSentry monitors the following registry keys:

```
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Startup
HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Logon
```

Autorun-Verzeichnisse

Zusätzlich zu den oben aufgeführten Registrierungsschlüsseln überwacht diese Funktion auch die folgenden Verzeichnisse und benachrichtigt Sie, wenn eine Datei hinzugefügt wird:

```
<Documents and Settings>\All Users\Start Menu\Programs\Startup
```

Zusätzliche Informationen

Der Registrierungsunterschlüssel "**Active Setup\Installated Components**" ist dafür vorgesehen, von Installationen verwendet zu werden, um sicherzustellen, dass alle Benutzer eines Systems aktuelle Informationen in ihrem Profil haben, und wird als solcher jedes Mal überprüft, wenn sich ein Benutzer anmeldet. Dieser Schlüssel wurde leider von Software missbraucht, um bösartige Anwendungen zu installieren und auszuführen. Wir bitten Sie dringend, alle Änderungen an diesem Registrierungsschlüssel zu untersuchen um sicherzustellen, dass sich nur autorisierte Anwendungen dort registrieren.

Im nächsten Kapitel finden Sie alle Ereignisaufzeichnungen, die mit dieser Funktion in das Ereignisprotokoll der Anwendung aufgenommen wurden.

* Der Umfang der von EventSentry aufgezeichneten Informationen hängt von den Informationen ab, die von der Installationsroutine der jeweiligen Software bereitgestellt werden. Es obliegt dem Softwarehersteller zu bestimmen, wie viele Installationen er in der Registry aufzeichnet. Die meiste moderne Software wird den Namen, den Herausgeber und die Version der installierten Anwendung protokollieren.

** Einige Informationen sind möglicherweise nicht verfügbar. Modell und Hersteller sind auf den meisten vorinstallierten Computern verfügbar; die registrierte Firma ist nur verfügbar, wenn dies bei der Installation angegeben wurde; in einigen Fällen zeigen die CPU-Informationen (insbesondere bei älteren Modellen) nicht den CPU-Typ an.

5.5.8.1 Event Log

The following events are be logged by this feature.

Event ID	Event Category	Event Description	Example

12000	Software Monitoring	An application was installed.	`Application {51A3EF81-FAAF-4E70-815C-74D34D4EC313} (Backdoor Manager) was installed.`
			`Additional Information:`
			`Publisher: Global Intruder Corp`
			`Installation Directory: C:\Program Files\BDM`

12001	Software Monitoring	An application was uninstalled.	`Application {51A3EF81-FAAF-4E70-815C-74D34D4EC313} (Backdoor Manager)`
12002	Software Monitoring	An application or file registered itself in a autorun registry key and will be run automatically when a user logs on.	`Application badtrojan.exe registered itself in the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Run and will be automatically run when a user logs into the system.`
12003	Software Monitoring	An application or file registered itself in the registry by changing a value.	`The registry value Shell in key HKLM\Software\Microsoft\Windows NT\Current Version\Winlogon changed from "explorer.exe" to "badandevilshell.exe". All files specified in this value will be automatically run when a user logs into the system.`

12004	Software Monitoring	An application was removed from an autorun registry key.	Application desktophog.exe was removed from the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Run and will no longer be run when a user logs into the system.
12005	Software Monitoring	A file was registered in an autorun directory.	The application eraseallfiles.exe registered itself in the directory c:\Documents and Settings\All Users\Start Menu\Programs\Startup and will be automatically run when a user logs into the system.
12006	Software Monitoring	A shortcut was registered in an autorun directory.	The shortcut PerformanceEnhancer.lnk (using file c:\windows\evilvirus.exe) registered itself in the directory C:\Documents and Settings\All Users\Start Menu\Programs\Startup and will be automatically run when a user logs into the system.
12007	Software Monitoring	A shortcut was removed from an autorun directory.	The shortcut PerformanceEnhancer.lnk (using file c:\windows\evilvirus.exe) was removed from directory C:\Documents and Settings\All Users\Start Menu\Programs\Startup and will no longer run when a user logs into the system.
12008	Software Monitoring	An application registered itself in an autorun registry key and will be run automatically when the computer starts.	Application YourPersonalAdware.exe was added to the registry key HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Startup and will be automatically run when the system boots.
12009	Software Monitoring	An application was removed from an autorun key and will no longer be run when the system boots.	Application YourPersonalAdware.exe was removed from the registry key HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Startup and will no longer be run the system boots.
12010	Software Monitoring	An application registered itself in a registry key and might be automatically run when a user logs into the system.	The application SmartTrojan registered file c:\windows\eraseanddestroy.exe in registry key HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components and might be automatically run when a user logs into the system. Please see the help file (search for ACTIVE SETUP) for more information.
12011	Software Monitoring	An application removed itself from a registry key and will no longer be run when a user logs into the system.	Application SmartTrojan (using file c:\windows\eraseanddestroy.exe) was removed from the registry key HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components and will no longer be run when a user logs into the system.

12012	Software Monitoring	A registry key could not be monitored and the feature disabled itself.	There was an error (999) monitoring registry key HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components. Please restart the EventSentry agent or notify NETIKUS.NET support if this problem persists. Autorun monitoring will NOT continue.
12020	Software Monitoring	A browser extension was installed	The %1 browser extension "%2" was added by user %4: Web Browser: %1 Name: %2 Version: %3 User: %4 Enabled: %5
12021	Software Monitoring	A browser extension was changed / updated	The %1 browser extension "%2" was modified by user %4: Web Browser: %1 Name: %2 Version: %3 User: %4 Enabled: %5 Field Changed: %6 ("%7" -> "%8")
12022	Software Monitoring	A browser extension was removed	The %1 browser extension "%2" was removed by user %4: Web Browser: %1 Name: %2 Version: %3 User: %4 Enabled: %5
12030	Hardware Monitoring	The installed memory changed.	The amount of physically installed memory changed from 512 Mb to 256 Mb.
12031	Hardware Monitoring	The number of installed processors changed.	The number of installed processors changed from 1 to 2.
12032	Hardware Monitoring	The number of installed floppy drives changed.	The number of installed floppy drives changed from 0 to 1.
12033	Hardware Monitoring	The number of installed CDROM drives changed.	The number of installed CDROM drives changed from 1 to 0.
12034	Hardware Monitoring	The number of installed DVD drives changed.	The number of installed DVD drives changed from 1 to 2.
12035	Hardware Monitoring	The number of removable drives changed.	The number of removable drives changed from 0 to 2.
12036	Hardware Monitoring	The link speed of a network adapter changed.	The link speed of adapter Gigabit Network Card changed from 1Gb to 100Mb.
12040	Hardware Monitoring	A removable drive has been added.	

12041	Hardware Monitoring	A removable drive has been removed.	
12042	Hardware Monitoring	A drive reported a S.M.A.R.T. status error.	
12050	Hardware Inventory	A network adapter connected to a WiFi network	A network adapter connected to a WiFi network. Connection details: Adapter Name: %1 Adapter ID: %2 SSID: %3 Signal Strength: %4 Cipher Algorithm: %5 Authentication Algorithm: %6
12051	Hardware Inventory	A network adapter disconnected from a WiFi network	A network adapter disconnected from a WiFi network. Last connection details: Adapter Name: %1 Adapter ID: %2 SSID: %3 Signal Strength: %4 Cipher Algorithm: %5 Authentication Algorithm: %6
12500	UPS Monitoring	At least one battery has been detect and will be monitored.	EventSentry will monitor the attached UPS devices and/or built-in batteries. 2 detected device(s): Battery #1: Current Charge: 98%, Voltage=12V, Status=Online, BatterySize=17930mAh Battery #2: Current Charge: 86%, Voltage=11V, Status=Discharging, BatterySize=65430mAh
12501	UPS Monitoring	The system is running on battery power.	At least one connected UPS/battery is now running on battery power. EventSentry will periodically log event 12502 with estimated run times until the UPS is back online. EventSentry will perform a system shutdown when the remaining battery or runtime gets below a configured threshold. Battery #1: Current Charge: 97%, Voltage=12V, Status=Online, BatterySize=17930mAh Battery #2: Current Charge: 98%, Voltage=12V, Status=Discharging, BatterySize=65410mAh

12502	UPS Monitoring	The system continues to run on battery power.	At least one connected UPS/battery continues to operate on battery power. Charge Remaining: 85% Estimated remaining runtime: 23411 seconds
12503	UPS Monitoring	The system is no longer running on battery power.	All connected UPS/battery devices are back online. Battery #1: Current Charge: 98%, Voltage=12V, Status=Online, BatterySize=17930mAh Battery #2: Current Charge: 100%, Voltage=12V, Status=Online, BatterySize=65410mAh
12504	UPS Monitoring	All attached batteries are fully or almost fully charged.	All connected UPS/battery devices are fully or almost fully charged. Battery #1: Current Charge: 98%, Voltage=12V, Status=Online, BatterySize=17930mAh Battery #2: Current Charge: 100%, Voltage=12V, Status=Online, BatterySize=65410mAh
12510	UPS Monitoring	A system shutdown will be initiated based on a low battery charge level.	The charge level of all attached UPS devices is at or below the threshold of 50% and a shutdown will now be initiated. Battery #1: Current Charge: 47%, Voltage=12V, Status=Online, BatterySize=17930mAh
12511	UPS Monitoring	A system shutdown will be initiated based on a low remaining runtime.	The estimated runtime of this system is at or below the threshold of 5 minutes and a shutdown will now be initiated. Battery #1: Current Charge: 47%, Voltage=12V, Status=Online, BatterySize=17930mAh
12512	UPS Monitoring	System Shutdown Result.	System Shutdown Result: Success.
12600	Boot Sector Monitoring	A change to the MBR and/or following sectors was detected.	EventSentry detected changes in a protected area of a hard drive, the new contents are embedded as binary data. If this change is unexpected, then the original data (MBR) can be downloaded from the EventSentry Web Reports (Inventory -> Host) and subsequently restored with boot media. Drive: \\.\PhysicalDrive0 Sectors Monitored: 0 - 78 (MBR)

			Bytes Changed: 67
12601	Boot Sector Monitoring	A change to the BootLoader and/or following sectors was detected.	EventSentry detected changes in a protected area of a hard drive, the new contents are embedded as binary data. If this change is unexpected then you can restore the boot loader by retrieving the original BootLoader from the EventSentry Web Reports (Inventory -> Host) and copying the data over with boot media. Drive: \\.\PhysicalDrive0 Sectors Monitored: 2048-2057 Bytes Changed: 34

5.5.9 Leistungsüberwachung

Mit der Leistungsüberwachung kann folgendes überwacht werden:

- **Alle Leistungsindikatoren, die durch das Betriebssystem und Anwendungen von Drittanbietern verfügbar sind**
- **SNMP-Objekte, die durch SNMP-Agenten verfügbar sind**
- **Ausgabe von Befehlszeilen-Dienstprogrammen**

Die Leistungsüberwachung kann auch Daten über SNMP von einem SNMP-Agenten erhalten, indem SNMP-Zählerwerte abgefragt werden. Die gesammelten Daten werden mit Alarmen versehen und auf die gleiche Weise wie Windows-Leistungsdaten dargestellt.

SNMP-Daten werden vom Heartbeat-Agent gesammelt.

Warnungen

Gibt Ereignisprotokoll-Alarme aus (die an eine Aktion, z.B. E-Mail, weitergeleitet werden können), wenn ein bestimmter Leistungszähler ein konfiguriertes Limit überschreitet. Beispielsweise kann ein Alarm ausgelöst werden, wenn ein Prozess mehr als 70% CPU-Zeit für mehr als 10 Minuten verbraucht.

Alerts sind in hohem Maße konfigurierbar und ermöglichen es Ihnen, einzustellen, wie oft ein Leistungszähler überprüft wird (z.B. alle 10 Sekunden) und wie lange der Zähler über Ihrem Schwellenwert bleiben muss, bevor ein Fehler im Anwendungsereignisprotokoll protokolliert wird. Siehe Alerts für weitere Informationen.

Leck-Erkennung

Manchmal können Anwendungen oder Treiber im Laufe der Zeit Ressourcen (z.B. Speicher, Handles) verlieren, was dazu führt, dass wertvolle Systemressourcen übermäßig beansprucht werden. In schweren Fällen kann ein Ressourcenleck sogar zu einer Systeminstabilität oder einem Absturz führen. EventSentry kann einige Ressourcenlecks mit Hilfe von bestimmten Leistungszählern erkennen. Beispielsweise können die folgenden Leistungsindikatoren überwacht werden, um Lecks zu erkennen:

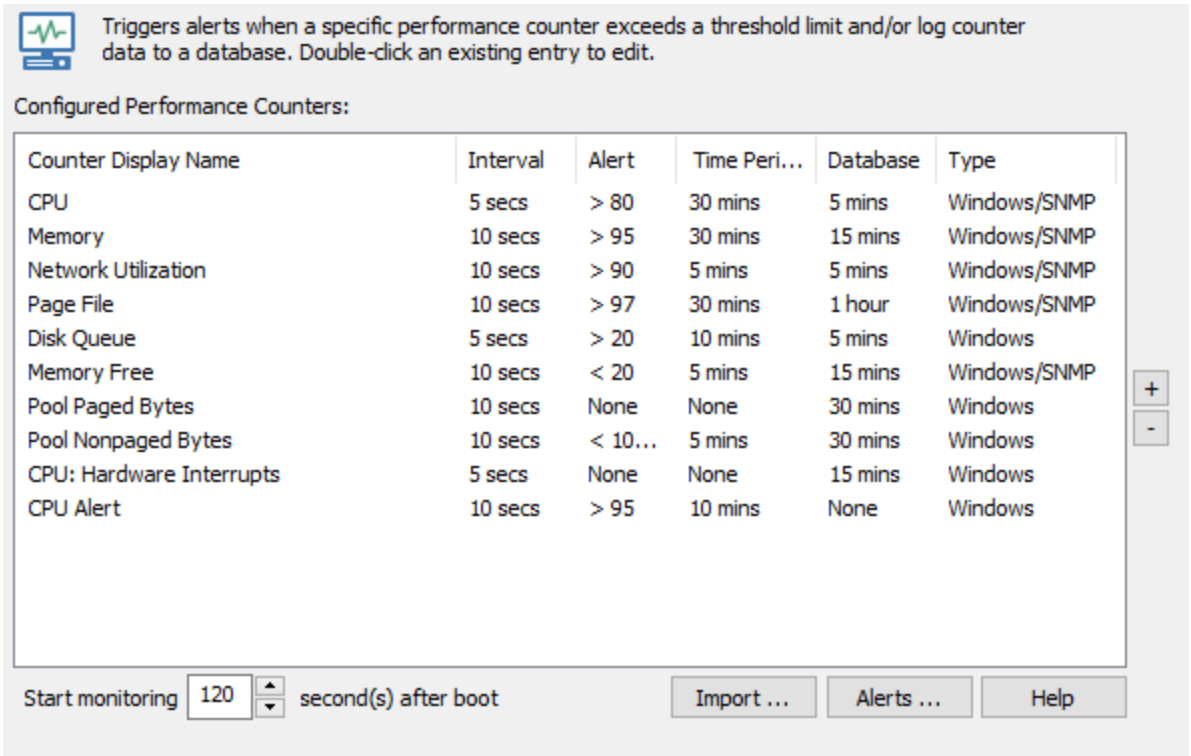
- Prozess(*)\Working Set
- Prozess(*)\Handles
- Speicher\Pool Paged Bytes

Sammlung von Leistungsdaten

Mit Hilfe einer Datenbank kann EventSentry Leistungsdaten in eine Datenbank schreiben, die dann über die EventSentry-Web Reports abgefragt werden können. Auf diese Weise können Sie eine Historie von Leistungsdaten (z.B. Speichernutzung, CPU-Auslastung usw.) über einen bestimmten Zeitraum anhand von Diagrammen und/oder Rohdaten anzeigen.

Die Leistungsverfolgung ermöglicht es Ihnen auch, den aktuellen Status aller überwachten Leistungszähler auf einen Blick zu sehen, so dass Sie sich schnell einen Überblick über den Status eines Servers verschaffen können. Weitere Informationen finden Sie unter Historie & Trending.

EventSentry wird mit einer Vielzahl von integrierten Leistungspaketen geliefert, die bereits eingerichtet sind, einschließlich des Pakets **Performance System**. Dieses Paket enthält sprachunabhängige Objekte, die Systemmetriken wie CPU-Nutzung und Speicherauslastung überwachen. Die Zähler in diesem Paket können nicht gelöscht oder geändert werden, da dies die Funktionalität in den Web-Reports beeinträchtigen kann. Die Überwachungsintervalle dieser Zähler können allerdings angepasst werden, und dem Paket können zusätzliche Zähler hinzugefügt werden.



5.5.9.1 Konfiguration von Leistungsobjekten

Die Leistungsüberwachung unterstützt die Erfassung von numerischen Daten aus drei verschiedenen Arten von Quellen:

- Windows-Leistungsindikatoren (Performance Monitoring)
- SNMP-Daten
- Ausführbare Dateien

Windows-Leistungsobjekte und die Ausgabe von ausführbaren Dateien werden durch den EventSentry-Agenten überwacht, der auf dem überwachten Rechner läuft, während SNMP-Objekte durch den Heartbeat-Agenten überwacht werden.

Trend- und Leckerkennung sind nur bei der Überwachung von Windows-Leistungsobjekten verfügbar.

Häufigkeitsintervall (Daten alle ... sammeln)
Das Frequenzintervall bestimmt, wie oft die Leistungsobjekte vom Betriebssystem abgerufen/aufgefrischt werden. Verwenden Sie niedrige Frequenzen (< 5 Sekunden) für Leistungsobjekte welche sich of ändern, wie z.Bsp. "Processor(*)\% Processor Time" oder "PhysicalDisk(*)\Avg. Disk Queue Length", oder wenn akkurate Werte erforderlich sind. Verwenden Sie größere Intervalle für Leistungsobjekte, die sich langsam ändern (z.B. "Memory\Available MBytes"). Die Erfassung von Leistungsdaten ist sehr effizient, und eine Änderung des Intervalls hat nur geringe Auswirkungen auf die CPU-Auslastung des EventSentry-Agenten. Dennoch wird es als gute Praxis angesehen, Intervalle auf der Grundlage des Leistungsobjektes auszuwählen.

Bei SNMP-Objekten kann dieser Wert nicht kleiner als das Heartbeat-Abfrageintervall sein.

Name
Ein Name welcher das Objekt gut beschreibt, dieser Name wird in Alerts und den Web Reports sichtbar sein.

Daten als Fließkommazahlen behandeln
Standardmäßig werden Werte als ganzzahlig interpretiert, was normalerweise die beste Wahl ist. Aktivieren Sie diese Option, um zu erzwingen, dass die Werte als Gleitkommazahlen interpretiert werden (z.B. für Leistungsobjekte die Werte kleiner als 1 zurückgeben).

Wenn sowohl ein Windows-Leistungszähler als auch ein SNMP-Zähler verfügbar sind, empfiehlt es sich, beide **im gleichen** Dialog zu konfigurieren.

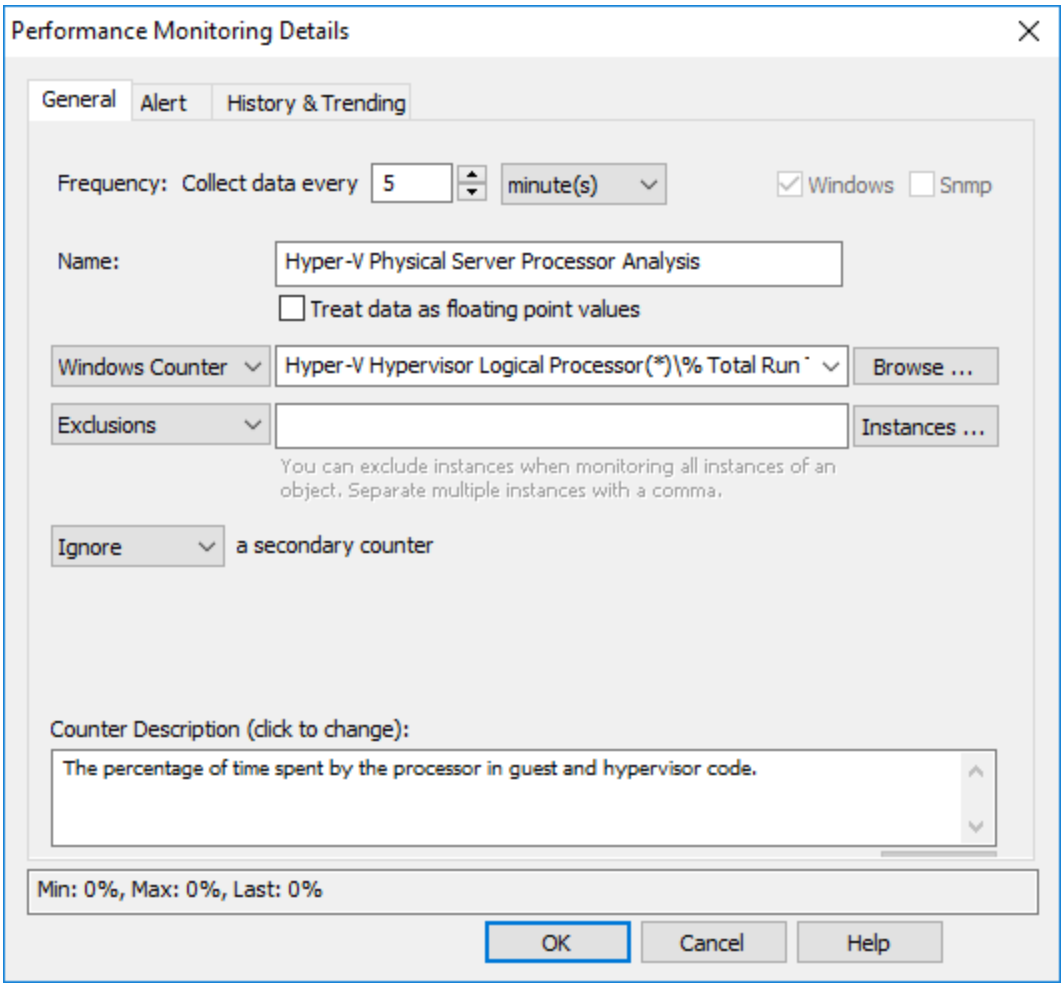
5.5.9.1.1 Windows Leistungsobjekte

Dies ist der Name des tatsächlichen Leistungsobjektes, wie es vom Betriebssystem offengelegt wird. Leistungsobjekte können auf mehrerer Weisen konfiguriert werden:

- wählen eines häufig verwendeten Objektes aus der Dropdown-Liste
- klicken Sie auf die Schaltfläche BROWSE, um eine Liste aller verfügbaren Zähler zu durchsuchen
- manuelle Eingabe vom Namen des Leistungsobjektes (z.B. `Process(*)\% Processor Time`)
- Eingabe der Leistungszähler-IDs (z.B. 238(*)\6), um dieses Objekt auch auf einem nicht-englischen Windows-Betriebssystem zu unterstützen

Mit Ausnahme einiger Kernleistungsindikatoren wie CPU und Speicher sind die IDs vieler Leistungsindikatoren spezifisch für eine Maschine. Die IDs von Leistungszählern können in der Registry unter **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib** nachgeschlagen werden.

Instanzen: Wenn ein Leistungszähler die Zeichenfolge **(*)** enthält, dann hat dieses Objekt Instanzen. EventSentry überwacht immer alle Instanzen eines Objekte, es sei denn, sie sind ausgeschlossen (siehe unten).



Inkludieren/Exkludieren

Wenn ein Windows-Leistungsobjekt Instanzen unterstützt (z.B. Prozess(*)\% Prozessorzeit), dann können bestimmte Instanzen (z.B. _Total) je nach Einstellung der Dropdown-Liste inkludiert oder exkludiert werden. Mehrere Instanzen können mit einem Komma getrennt werden, Wildcards werden unterstützt.

Beispielsweise umfasst das Leistungsobjekt **Process(*)\% Processor Time** auch die Idle-Instanz, die immer nahe bei 100% liegt (da sie die ungenutzte CPU-Zeit anzeigt), und die _Total-Instanz, die die Gesamtmenge der CPU-Zeit aller Anwendungen misst. Daten aus diesen Instanzen sind normalerweise nicht relevant, so dass sie beide ausgeschlossen werden können, indem Sie die Dropdown-Liste auf "Exclude" und das Feld auf **Idle,_Total** setzen.

Wenn Sie auf die Schaltfläche "Instanzen" klicken, werden alle aktuellen Instanzen des ausgewählten Leistungsobjekte angezeigt, und alle angegebenen Ausschlüsse werden ausgewählt. Wenn ein angegebener Ausschluss in der Liste der Instanzen nicht vorhanden ist, werden die Ausschlüsse durch Klicken auf die Schaltfläche "OK" im Dialogfeld "Leistungsobjekt-Instanzen" zurückgesetzt.

Rechnen mit einem Sekundärobjekt

Einige Leistungsindikatoren bieten zusätzliche Einblicke, wenn ihre Werte in Kombination mit einem anderen Leistungsindikator verwendet werden. Sie können die erhaltenen Werte eines Leistungsobjekts

addieren, subtrahieren, dividieren oder multiplizieren mit/durch die Werte eines "sekundären" Leistungsobjektes.

EventSentry bietet auch integrierte Leistungsobjekte:

[PhysicalMemory]	gibt die Menge des installierten physischen Speichers zurück
[CpuCountLogisch]	gibt die Anzahl aller verfügbaren logischen Prozessoren (z.B. Cores) zurück
[CpuZahlPhysisch]	gibt die Anzahl aller verfügbaren physischen Prozessoren zurück

Multiplikator verwenden

Das berechnete Ergebnis kann mit der angegebenen Zahl multipliziert werden.

Standardmäßig enthält EventSentry das Leistungsobjekt "Speicherauslastung", welches die Vorteile sekundärer Objekte ausnutzt. Das primäre Leistungsobjekt (Verfügbare MBytes) wird durch den physischen Speicher ([PhysicalMemory]) geteilt und dann mit 100 multipliziert (Beispiel: 1522/4096 * 100 = **37,16%**).

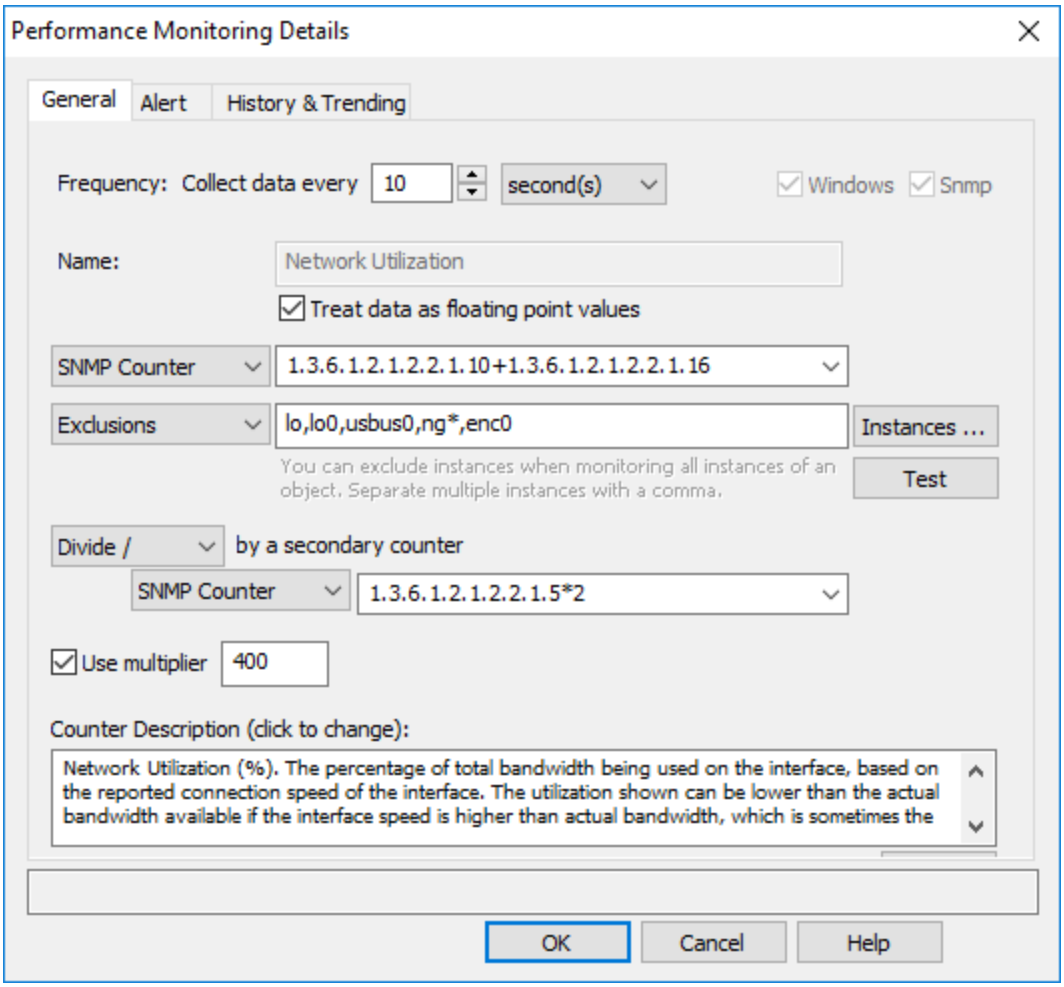
Beschreibung des Leistungsobjektes

Zeigt die Beschreibung des Leistungsobjektes, die in der Regel von dem Betriebssystem oder dem Softwarehersteller, der den Leistungszähler bereitstellt, bereitgestellt wird.

5.5.9.1.2 SNMP Objekte

Geben Sie die OID eines SNMP-Objektes in numerischer Form an, z. B. **1.3.6.1.4.1.2021.11.9.0**. Grundrechenarten wie Addition, Subtraktion, Multiplikation und Division werden unterstützt. SNMP-Werte werden durch den Heartbeat-Agent abgefragt.

Im SNMP Feld werden Variablen unterstützt. Wenn Sie beispielsweise einige Geräte haben, die nur SNMP v1 unterstützen, und einige Geräte, die SNMP v2c und höher unterstützen, dann können Sie immer noch ein einzelnes Objekt verwenden und einfach die Standard-OID auf einer Ebene pro Host oder pro Gruppe außer Kraft setzen. Dies ist nützlich für Netzwerke mit mehreren Versionen von SNMP und OIDs, die sich zwischen verschiedenen SNMP-Versionen unterscheiden.



Berechnen der Netzwerkbandbreite und Ausschließen bestimmter Instanzen

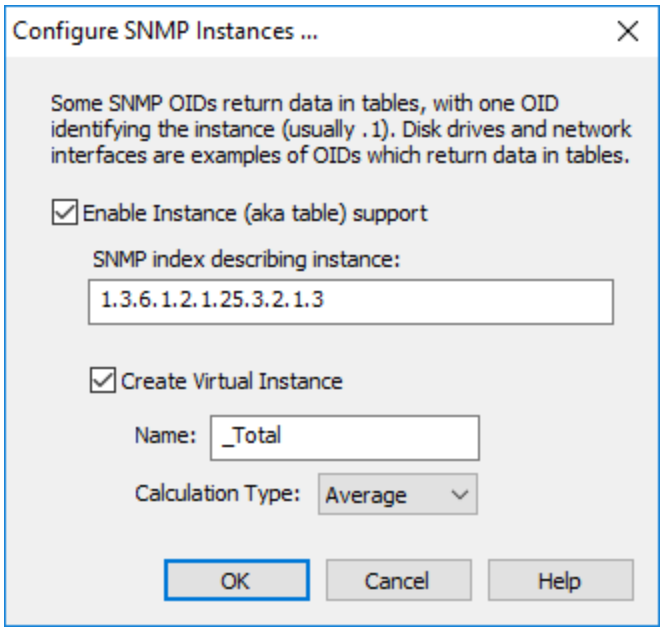
Inkludieren/Exkludieren

Wenn ein SNMP-Zähler als Tabelle (aka SEQUENCE) organisiert ist, dann können bestimmte "Instanzen" inkludiert oder exkludiert werden, wenn die OID, welche den Instanznamen beschreibt, über die Schaltfläche **Instanzen** konfiguriert wird. Wenn eine Instanz aktiviert wird, ist der Index, welcher die tatsächlichen Instanzen beschreibt, erforderlich, damit die von den Instanzen gesammelten Daten unterschieden werden können.

Wenn der Instanztyp auf **Include (Einschließen)** eingestellt ist und nur eine Instanz angegeben ist, wird ein SNMP-basierter Zähler wie ein regulärer SNMP-Zähler behandelt und der Instanzname wird nicht in der Datenbank gespeichert.

Im folgenden Beispiel sind alle Instanzen unter 1.3.6.1.2.1.31.1.1.1.1.1 aufgeführt, wobei jede Zeile der Tabelle eine Netzschnittstelle beschreibt.

Wenn eine Instanz definiert wird, können eine oder mehrere Instanzen exkludiert oder bestimmte Instanzen inkludiert werden.



Rechnen mit einem sekundären Objekt

Einige SNMP-Objekte bieten zusätzliche Einblicke, wenn ihre Werte in Kombination mit einem anderen Objekten verwendet werden. Sie können die erhaltenen Werte eines SNMP-Objekts mit/durch die Werte eines "sekundären" SNMP-Objekts addieren, subtrahieren, dividieren oder multiplizieren.

Da SNMP-Objekte die Grundrechenarten unterstützen, könnte das obige Beispiel auch unter Verwendung eines sekundären Objektes berechnet werden, indem im Feld für des primären SNMP-Objektes folgendes angegeben wird:

```
(1.3.6.1.2.1.31.1.1.1.6+1.3.6.1.2.1.31.1.1.1.10)/
(1.3.6.1.2.1.31.1.1.1.15*1600000000)
```

Testen

Ein SNMP-Objekt kann getestet werden, indem man auf die Schaltfläche "Test" klickt und einen SNMP-fähigen Remote-Host angibt. Wenn der Remote-Host auf SNMP-GET-Anforderungen antwortet, werden die aktuellen Daten unten im Dialogfeld angezeigt und in regelmäßigen Abständen aktualisiert. Wenn der angegebene Computer bereits in einer EventSentry-Gruppe vorhanden ist, werden alle auf diesen Host angewandten Authentifizierungseinstellungen automatisch beim Senden der SNMP-GET-Anforderung verwendet.

Beschreibung

Löst die angegebene(n) OID(s) unter Verwendung der im Dialogfeld SNMP-Trap-Daemon konfigurierten MIBs auf.

SNMP Instanzen

Aktivieren Sie diese Option wenn ein SNMP OID Daten in einer Tabelle zurückgibt, d.h. mehrere Instanzen für denselben Zähler bereitgestellt werden. Dies gilt in der Regel für Leistungsmetriken von Hardware-Komponenten wie Netzwerkkarten oder CPUs bei denen mehrere Instanzen desselben Typs von Leistungsquelle vorhanden sind. Die Abbildung unten zeigt ein Beispiel für SNMP-Daten (aktuelle CPU-Auslastung durch jeden Kern von einem VMWare(c)-Host), die in einer Tabelle zurückgegeben werden:

```
iso.3.6.1.2.1.25.3.3.1.2.1 = INTEGER: 1
iso.3.6.1.2.1.25.3.3.1.2.2 = INTEGER: 0
iso.3.6.1.2.1.25.3.3.1.2.3 = INTEGER: 1
iso.3.6.1.2.1.25.3.3.1.2.4 = INTEGER: 1
iso.3.6.1.2.1.25.3.3.1.2.5 = INTEGER: 2
iso.3.6.1.2.1.25.3.3.1.2.6 = INTEGER: 1
iso.3.6.1.2.1.25.3.3.1.2.7 = INTEGER: 0
iso.3.6.1.2.1.25.3.3.1.2.8 = INTEGER: 1
```

SNMP-Index: Da in einer Tabelle zurückgegebene Datenwerte möglicherweise keinen Kontext haben, können sie mit einer anderen Tabelle verknüpft werden welche diese Werte beschreibt, wie in der Abbildung unten gezeigt. Die Tabelle, die die Instanzen beschreibt, kann sich an beliebiger Stelle im SNMP-Baum befinden, solange die Indizes (gelb markiert) übereinstimmen.

```
iso.3.6.1.2.1.25.3.2.1.3.1 = STRING: "CPU Pkg/ID/Node: 0/0/0 Intel(R) Xeon(R) CPU L5520 @ 2.27GHz"
iso.3.6.1.2.1.25.3.2.1.3.2 = STRING: "CPU Pkg/ID/Node: 0/1/0 Intel(R) Xeon(R) CPU L5520 @ 2.27GHz"
iso.3.6.1.2.1.25.3.2.1.3.3 = STRING: "CPU Pkg/ID/Node: 0/2/0 Intel(R) Xeon(R) CPU L5520 @ 2.27GHz"
iso.3.6.1.2.1.25.3.2.1.3.4 = STRING: "CPU Pkg/ID/Node: 0/3/0 Intel(R) Xeon(R) CPU L5520 @ 2.27GHz"
iso.3.6.1.2.1.25.3.2.1.3.5 = STRING: "CPU Pkg/ID/Node: 0/4/0 Intel(R) Xeon(R) CPU L5520 @ 2.27GHz"
iso.3.6.1.2.1.25.3.2.1.3.6 = STRING: "CPU Pkg/ID/Node: 0/5/0 Intel(R) Xeon(R) CPU L5520 @ 2.27GHz"
iso.3.6.1.2.1.25.3.2.1.3.7 = STRING: "CPU Pkg/ID/Node: 0/6/0 Intel(R) Xeon(R) CPU L5520 @ 2.27GHz"
iso.3.6.1.2.1.25.3.2.1.3.8 = STRING: "CPU Pkg/ID/Node: 0/7/0 Intel(R) Xeon(R) CPU L5520 @ 2.27GHz"
```

Virtuelle Instanzen
Eine virtuelle Instanz ist eine zusätzliche Instanz (Tabellenzeile), die während der Laufzeit erstellt wird, wobei ihr Wert aus den vorhandenen SNMP-Werten berechnet wird. Der Wert der virtuellen Instanz kann entweder der Durchschnitt oder die Summe aller vorhandenen Werte sein. Beispielsweise kann die **_Total** Instanz, die normalerweise nur auf Windows-basierten Hosts verfügbar ist, auf VMWare(c)-Hosts erstellt werden, indem die aktuelle CPU-Auslastung aller Cores berechnet wird.

Name: Der Name der virtuellen Instanz
Berechnungsart: Durchschnitt oder Summe aller Werte

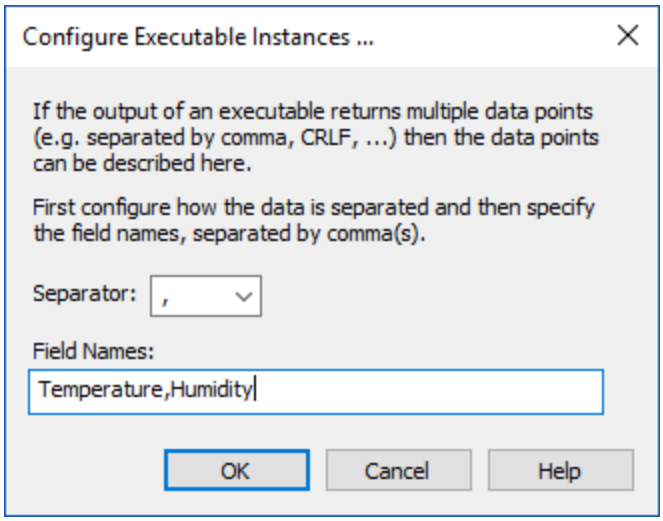
5.5.9.1.3 Executables

Die Ausgabe von ausführbaren Dateien (oder Skripten) kann als Input für die Leistungsüberwachung verwendet werden, um numerische Daten zu überwachen, die nicht über einen Windows-Leistungszähler oder SNMP verfügbar sind.

Ausführbare Datei
Geben Sie den Pfad zu der Datei an, aus der die Ausgabe interpretiert werden soll. In ihrer einfachsten Form gibt die ausführbare Datei oder das Skript eine einzige Zahl zurück, mehrere Werte werden auch als Instanzen unterstützt. Fließkommazahlen werden unterstützt, wenn das Kontrollkästchen "Daten als Fließkommawerte behandeln" aktiviert ist.

Eingebettete Skripte können mit dem @-Symbol referenziert werden.

Die Ausgabe von ausführbaren Dateien und Skripten wird nur ausgewertet, wenn das vom Prozess zurückgegebene %ERRORLEVEL% 0 (Null) ist. Die Ausgabe wird verworfen, wenn die ausführbare Datei auf einen Fehler gestoßen ist und das resultierende %ERRORLEVEL% 1 oder höher ist.



Instanzen

Wenn die Ausgabe mehrere Werte enthält, die durch ein gemeinsames Trennzeichen getrennt sind, können die verschiedenen Datenwerte als Instanzen verarbeitet werden, ähnlich wie Instanzen mit Windows Leistungsobjekten. Wenn Sie auf die Schaltfläche **Instanzen** klicken, wird das Dialogfeld Instanzen aufgerufen, das die Konfiguration des Trennzeichens zusammen mit den Feldnamen ermöglicht. Feldnamen sind erforderlich, um die verschiedenen Datenwerte zu unterscheiden.

Dynamische Instanzen

Dynamische Instanzen werden auch unterstützt wenn die Anzahl und/oder die Namen der Instanzen nicht im Voraus bekannt sind, zum Beispiel bei der Aufzählung von Docker-Containern. Um dynamische Instanzen zu verwenden:

1. Geben Sie ein Sternchen ***** für den Instanznamen an
2. Vergewissern Sie sich, dass die ausführbare Datei die Instanznamen im CSV-Format (unabhängig von der Einstellung von "Separator") als erste Zeile zurückgibt
3. Die restlichen Daten werden so interpretiert, als ob statische Instanzen verwendet würden

Wichtige Hinweise

Prozesse, die vom Agenten EventSentry im Rahmen der Leistungsüberwachung gestartet werden, können nicht länger als 120 Sekunden laufen.

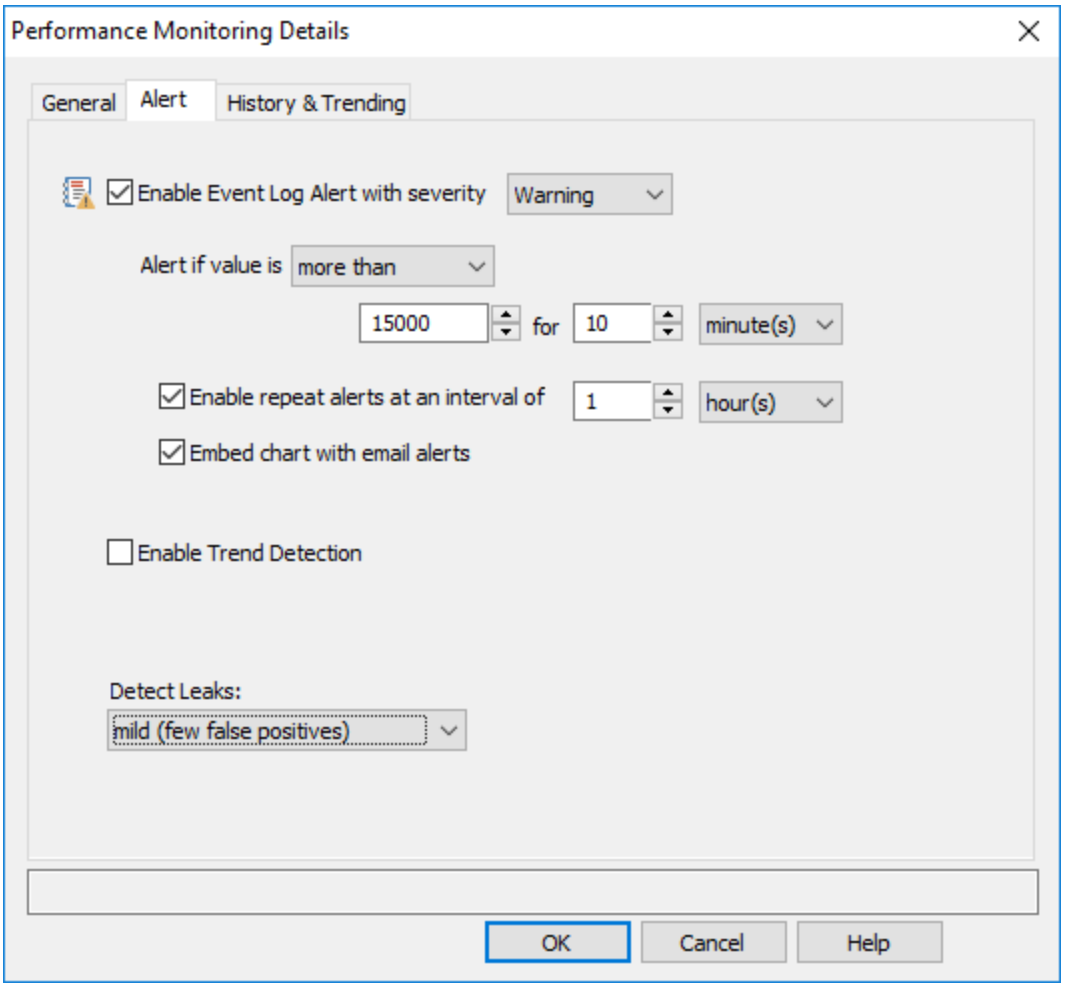
Ausführungsbasierte Leistungszähler, die Nicht-Windows-Hosts zugewiesen sind, werden vom EventSentry Heartbeat Monitor-Dienst (für jeden Host, dem sie zugewiesen sind) ausgeführt, wobei entweder die Variable $HOSTNAME oder $IPADDRESS an die ausführbare Datei übergeben werden kann. Es wird in diesem Fall **nicht empfohlen**, eingebettete Skripte zu verwenden, da der Heartbeat-Dienst möglicherweise keinen Zugriff auf sie hat.

Da der EventSentry Agent normalerweise unter einem privilegierten Konto wie dem LocalSystem-Konto ausgeführt wird, ist es wichtig sicherzustellen, dass alle Skripte, die von dieser Funktion verwendet werden, ordnungsgemäß durch NTFS-Berechtigungen gesichert sind, um zu verhindern, dass nicht privilegierte Benutzer Code einführen.

5.5.9.2 Warnungen

Leistungswarnungen benachrichtigen Sie, wenn ein bestimmtes Leistungsobjekt den konfigurierten Schwellenwert überschreitet, indem ein Ereignis im Ereignisprotokoll protokolliert wird. Anstatt sofort einen Alarm auszulösen, wenn ein Leistungswert den Schwellenwert überschreitet, werden alle Warnungen mit einem Zeitraum verknüpft, über den der aktuelle Leistungswert ausgewertet wird. Eine Warnung wird nur dann protokolliert, wenn der durchschnittliche Leistungswert während des konfigurierten Zeitraums den Grenzwert überschreitet - dadurch werden unnötige Warnungen reduziert.

Beispielsweise können Sie benachrichtigt werden, wenn der Prozentsatz der CPU-Auslastung über einen Zeitraum von 10 Minuten 80% übersteigt. Das bedeutet, dass Sie nicht benachrichtigt werden, wenn die CPU-Zeit nur 30 Sekunden lang auf 100% ansteigt.



Aktivieren des Ereignisprotokoll-Alarms mit Schweregrad
Alerts werden immer in das Ereignisprotokoll geschrieben, und Ereignisprotokollfilter sind erforderlich, um diese Ereignisse (Alerts) an eine tatsächliche Benachrichtigung, z.B. per E-Mail, weiterzuleiten. Wählen Sie einen Schweregrad, mit dem Alerts für diesen Zähler im Ereignisprotokoll protokolliert werden sollen.

Schwellenwert-Einstellung (Alarm, wenn Wert ...)
Konfiguriert die Schwellenwerteinstellungen, wenn der Zählerwert unter, über, unter, zwischen oder nicht zwischen einem Schwellenwert liegt.

Zeitintervall

Das konfigurierte Zeitintervall bestimmt, wie lange der Zählerwert Ihren Schwellenwert überschreiten muss, bevor ein Alert in das Ereignisprotokoll geschrieben wird.

Aktivieren Sie wiederholte Alarme

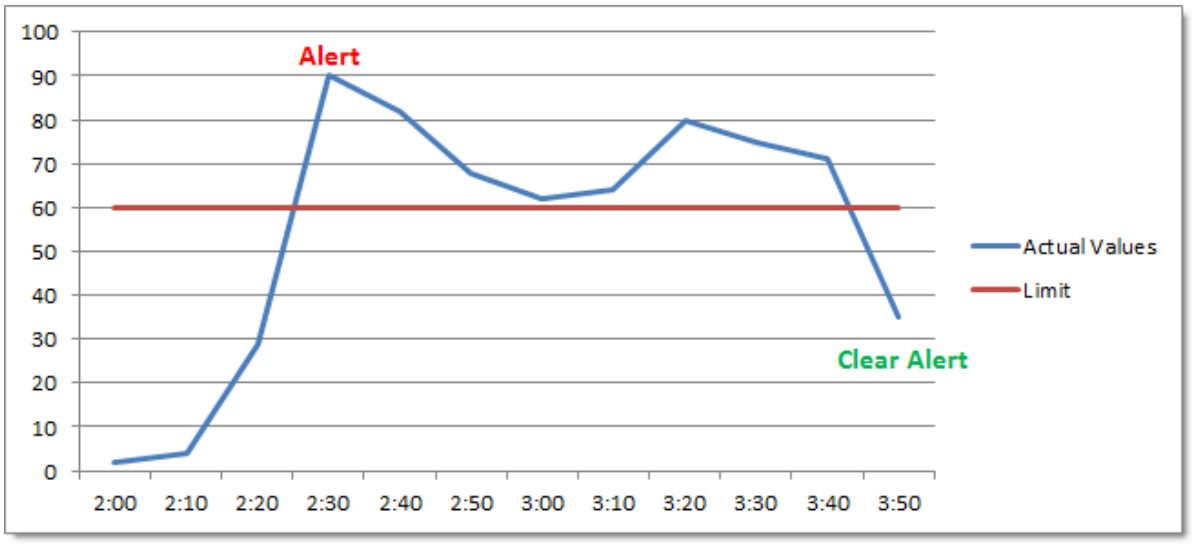
Wenn "Wiederholungsalarme in einem Intervall von" nicht angekreuzt ist, wird ein Ereignisprotokoll-Alarm erzeugt, sobald der aktuelle (oder durchschnittliche) Wert des überwachten Zählers von einem nicht alarmierten Zustand in einen alarmierten Zustand **und** umgekehrt wechselt. Diese Einstellung wird für instablile Leistungszähler (z.B. CPU-Auslastung) nicht empfohlen, da sie zu einer großen Anzahl von Alerts führen kann; sie eignet sich besser für stabile Leistungszähler, wie z.B. Speichernutzung, Handle-Count und dergleichen.

Es wird allgemein empfohlen, diese Option zu aktivieren, damit Alarme nicht öfter als das angegebene Intervall generiert werden.

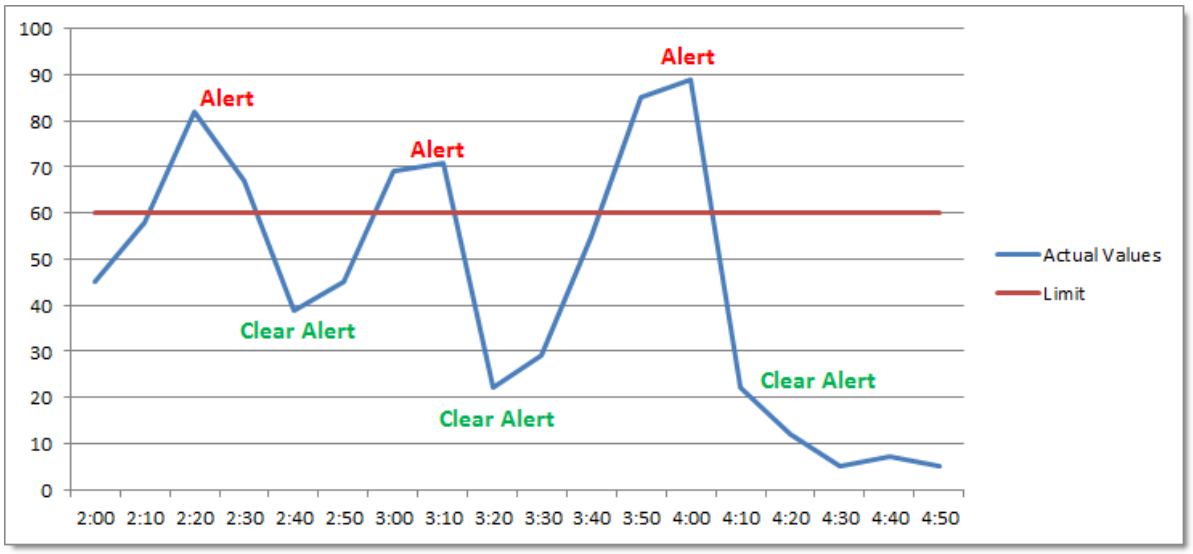
Enable Repeat Alerts OFF

Wenn das Zeitintervall auf 10 Minuten eingestellt ist und der Leistungszähler den Schwellenwert 40 Minuten lang überschreitet, wird nur einmal (nach Ablauf der anfänglichen 10 Minuten) ein Alert generiert. Fällt der Zähler jedoch wieder unter den Schwellenwert zurück und springt dann nach einiger Zeit wieder hoch, dann wird ein weiterer Alert generiert.

Die nachstehende Grafik zeigt dies: EventSentry protokolliert nur einen Alarm um 2:30 Uhr, alle nachfolgenden Alerts werden als Teil des ersten Alerts betrachtet und werden daher nicht generiert. Der Alarm wird um **3:50 Uhr** gelöscht.



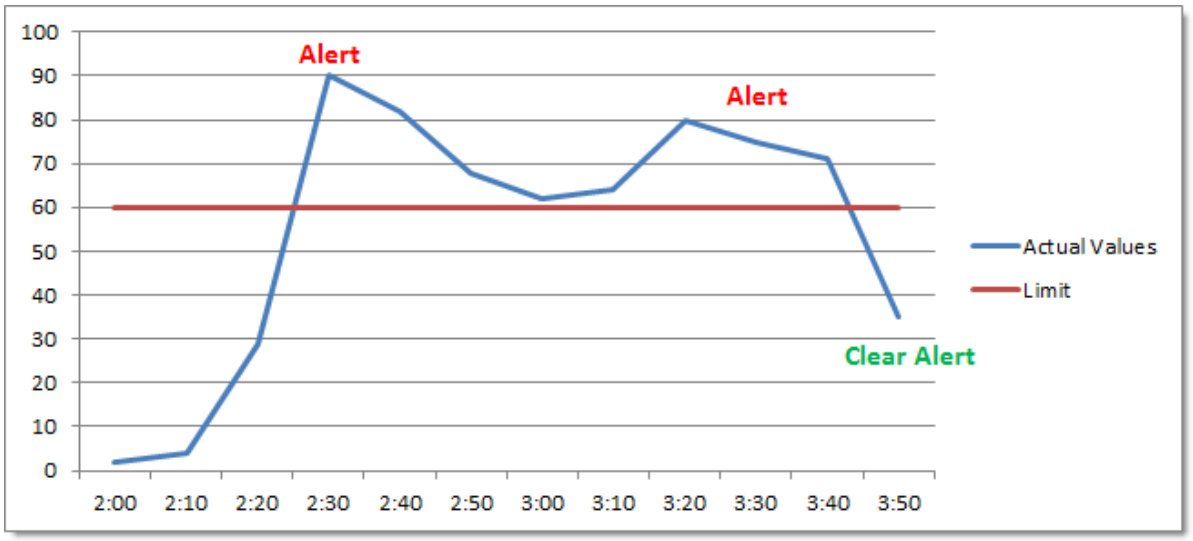
Beachten Sie jedoch, dass ein Leistungswert, der wiederholt von einem alarmierten in einen nicht alarmierten Zustand übergeht, mehr Alarme (und "Clear Alert"-Ereignisse) erzeugen kann als gewünscht:



Enable Repeat Alerts ON

Wenn Sie jedoch das Kontrollkästchen **Notify at most every** markieren und ein Zeitintervall einstellen, dann werden Sie jedes Mal, wenn dieses Intervall verstrichen ist, benachrichtigt, wenn sich der Leistungszähler weiterhin in einem alarmierten Zustand befindet. Der Alarm wird erst dann beendet, wenn der Leistungszähler wieder unter dem Schwellenwert liegt.

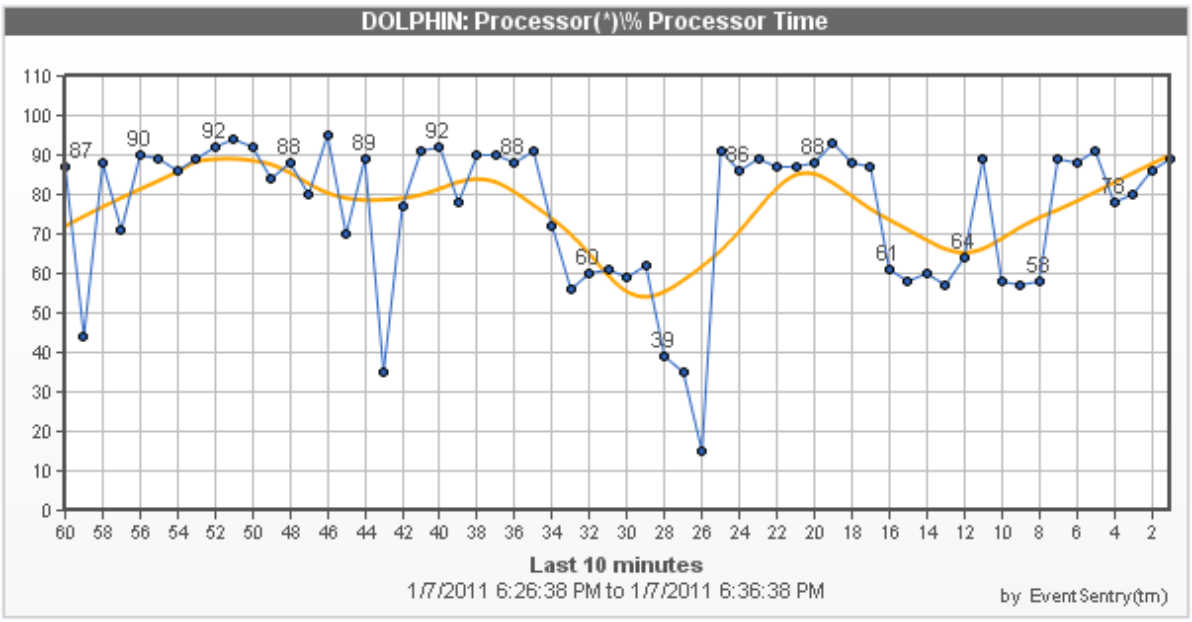
Das untenstehende Diagramm zeigt das gleiche Beispiel wie oben, wobei **Notify höchstens alle 1 Stunde** eingestellt ist. Da sich der überwachte Wert immer noch in einem Alarmzustand befindet, wird EventSentry um **3:30 Uhr** einen weiteren Fehler protokollieren und den Alarm um **3:50 Uhr** löschen.



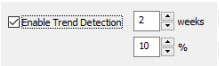
Einbetten von Diagrammen (für E-Mail-Benachrichtigungen)

Wenn dieses Kontrollkästchen aktiviert ist, erstellt EventSentry aus den während des konfigurierten Zeitintervalls (siehe oben, z.B. 30 Minuten) gesammelten Daten ein PNG-Diagramm und bettet es als Binärdaten in das Ereignis ein. Der EventSentry-Agent wird dann die eingebetteten Binärdaten als Bild an alle E-Mails anhängen, die den Performance-Alarm enthalten. Diese Funktion ist daher nur dann

nützlich, wenn den Leistungsalarmen mindestens ein Filter zugeordnet ist, der Ereignisse per E-Mail versendet. Das Diagramm enthält eine automatisch berechnete Trendlinie in Orange.



Aktivieren der Trenderkennung (nur Windows-Leistungszähler)



Die Trenderkennung unterdrückt Warnmeldungen über wiederkehrende und erwartete Leistung und funktioniert am besten mit prozentbasierten Leistungszählern wie der CPU-Auslastung. Die Trenderkennung verfolgt die Durchschnittswerte der Leistungszähler und kann Warnmeldungen unterdrücken, wenn der gemessene Wert die konfigurierte harte Grenze überschreitet - wenn der aktuelle Durchschnitt mit dem historischen Durchschnitt übereinstimmt.

Um ein durchschnittliches Leistungsobjekt als gültig zu betrachten, muss er Daten für mindestens die festgelegte Anzahl von "Wochen", standardmäßig 2, gesammelt haben. Sobald der Durchschnitt als gültig erachtet wird, vergleicht er den aktuellen Zählerdurchschnitt mit dem historischen Zählerdurchschnitt und unterdrückt den Alarm, wenn der aktuelle Wert nicht mehr als die konfigurierte Anzahl von Prozentpunkten abweicht.

Um dies zu erreichen, verfolgt EventSentry den durchschnittlichen Zählerwert in 12-Minuten-Intervallen für jeden Wochentag. Zähler-Durchschnittswerte werden in temporären Dateien (%SYSTEMROOT%\EventSentry\temp) mit Dateinamen, die mit "eventsentry_performance_trend" beginnen, gespeichert und bleiben auch bei Neustarts des Agenten gültig.

Lecks aufspüren (nur Windows-Leistungszähler)

Einige Leistungsindikatoren zeigen den Ressourcenverbrauch eines Dienstes, Prozesses oder einer Dienstleistung an. Bei der Leckerkennung wird versucht, Objekte zu finden, die Ressourcen lecken, ohne dass harte Grenzen festgelegt werden müssen. Die Leck-Erkennung funktioniert am besten bei Leistungszählern, die Ressourcen zählen (z.B. Handle-Count, Working-Set-Bytes usw.), und nicht bei prozentbasierten Leistungszählern.

Die Lecksuche kann auf drei Arten konfiguriert werden:

Einstellung	Für die Analyse verwendeter Zeitraum	Beschreibung
Mild	48 Stunden	wird weniger potenzielle Lecks entdecken, aber weniger falsch-positive Ergebnisse erzeugen
Moderieren	36 Stunden	ausgewogene Einstellung zwischen mild und aggressiv
Aggressiv	24 Stunden	findet die meisten potentiellen Lecks, erzeugt aber die meisten falsch-positiven Ergebnisse

Die Lecksuche kann mit dem numerischen Vergleich des Inhaltsfilters kombiniert werden, um Leckwarnungen unterhalb oder oberhalb eines bestimmten Wertes auszuschließen/einzubeziehen. Beispielsweise können Sie die Leckerkennung für die Handle-Zahl von Prozessen aktivieren, aber alle Warnungen für Handle-Zahlen unter 5000 ausschließen.

Bei einigen Prozessen kann es den Anschein haben, dass Ressourcen ein "Leak" haben, obwohl dieses Verhalten in Wirklichkeit nur vorübergehend ist (z.B. Datenbankserver), um Anfragen zu befriedigen. Es wird empfohlen, auch historische Zählerinformationen in einer Datenbank zu konsolidieren, so dass langfristige Muster der überwachten Prozesse beobachtet werden können.

5.5.9.3 History & Trending

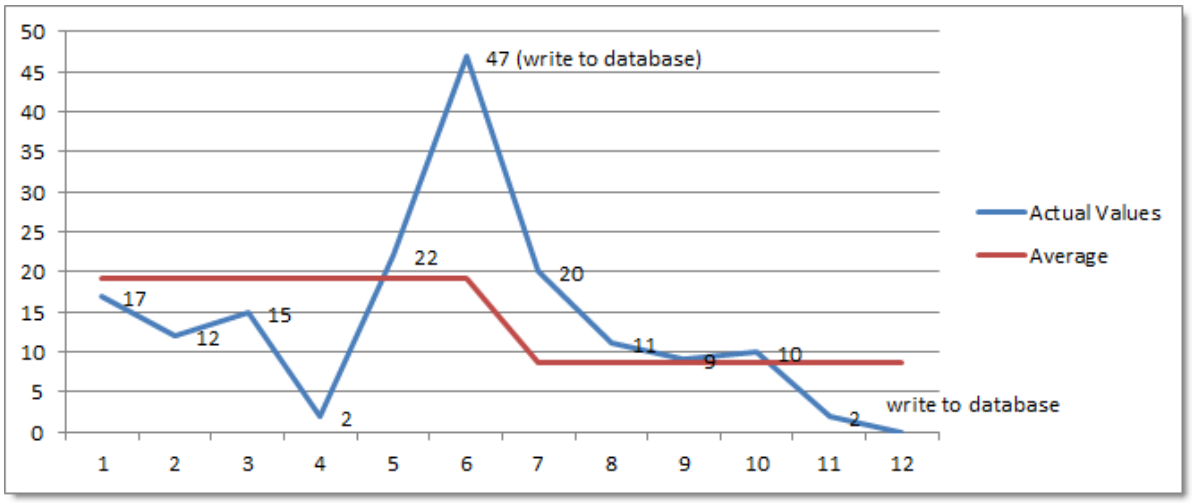
Das Sammeln von Leistungsdaten in einer Datenbank ermöglicht es, den aktuellen Leistungsstatus und den Verlauf der Leistungsdaten über die Web Reports zu betrachten, entweder unter Verwendung grafischer Diagramme oder durch Ausgabe im HTML / CSV-Format.

EventSentry bietet Ihnen Flexibilität, da Sie für jeden Zähler benutzerdefinierte Datenbankintervalle konfigurieren können.

Aufzeichnung in der Datenbank alle ...
Durch Aktivieren dieses Kästchens werden Leistungsobjekte im angegebenen Intervall aufgezeichnet. Das Aufzeichnungsintervall muss gleich oder höher als das Abfrageintervall sein, da der Abfrageintervall definiert, wie oft die Daten tatsächlich vom Betriebssystem abgerufen werden.

Historie aufbewahren
Wenn dieses Kontrollkästchen aktiviert ist (Standard), werden alle historischen Daten für diesen Leistungswert aufbewahrt, um die Anzeige von Trends in den Web Reports zu unterstützen. Wenn nicht angekreuzt, werden nur die aktuellen Daten des Leistungswerts aufbewahrt. Dies ist nützlich für Leistungsdaten, bei denen nur der aktuelle Wert relevant ist und die Aufbewahrung historischer Daten nicht sinnvoll ist (z.B. Tonerstand eines Druckers, Batterietemperatur einer USV).

EventSentry schreibt den **Durchschnitt der über das Protokollierungsintervall gesammelten Daten in die Datenbank**. Ein kürzeres Protokollierungsintervall führt zu einer genaueren Darstellung der Leistungsdaten in der Datenbank, nimmt aber mehr Platz in der Datenbank in Anspruch. Wenn z.B. Zählerdaten alle 5 Sekunden gesammelt werden und das Datenbank-Protokollierungsintervall auf 10 Minuten eingestellt ist, berechnet EventSentry den Durchschnitt von 120 gesammelten Leistungswerten.



Leistungsdaten können gleichzeitig in eine oder mehrere Datenbanken geschrieben werden.

5.5.9.4 Event Log

Die folgenden Ereignisse werden von dieser Funktion mit der Ereigniskategorie **Performance Monitoring** protokolliert.

Event ID	Event Description	Event Type	Example

12100	Performance counter fell below threshold	Alert	`The performance counter "%5" (%1) fell below the threshold of %2, the current values are:`
			
			`Average: %3`
			`Minimum: %6`
			`Maximum: %7`
			
			`Counter Description:`
			`%8`

12101	Performance counter (with instance) fell below threshold	Alert	`The performance counter "%6" ("%1", instance "%2") fell below the threshold of %3, the current values are:`
			
			`Average: %4`
			`Minimum: %7`
			`Maximum: %8`
			
			`Bottom %9 instances:`
			`%10`
			
			`Counter Description:`
			`%11`

12102	Performance counter equals value	Alert	`The performance counter "%4" (%1) equals the value of %2.`
			
			`Counter Description:`

			%5
12103	Instance of a performance equals value	Alert	The performance counter "%5" ("%1", instance "%2") equals the value of %3. Counter Description: %6
12104	Performance counter exceeds threshold	Alert	The performance counter "%5" (%1) exceeded the threshold of %2, the current values are: Average: %3 Minimum: %6 Maximum: %7 Counter Description: %8
12105	Instance of performance counter exceeds threshold	Alert	The performance counter "%6" ("%1", instance "%2") exceeded the threshold of %3, the current values are: Average: %4 Minimum: %7 Maximum: %8 Top %9 instances: %10 Counter Description: %11
12107	Counter value is not equal to desired value	Alert	The performance counter "%1" (%2) on host %3 does not equal the value of %4, the current value is %5. Counter Description: %6
12108	Counter value (instance) is not equal to desired value	Alert	The performance counter "%1" ("%2", instance "%3") on host %4 does not equal the value of %5, the current value is %6. Counter Description: %7
12110	Required entry points could not be found in PDH.DLL	Error	One or more required function entry points could not be found in the dynamic link library PDH.DLL. Please make sure that the latest version of PDH.DLL is installed on this machine, for example you may copy the DLL from another machine running a later Operating System. Performance monitoring cannot continue.
12111	PDH.DLL could not be found	Error	The dynamic link library PDH.DLL could not be found and is required for performance monitoring. Please make sure that the latest

			version of PDH.DLL is installed on this machine, for example you may copy the DLL from another machine running a later Operating System. Performance monitoring cannot continue.
12114	High handle count due to missing hotfix	Warning	The EventSentry agent is experiencing an unusually high handle count (%1 handles) and/or high memory usage (%2 bytes), which is most likely due to a known issue in Windows Server 2003 SP2 (http://support.microsoft.com/kb/938135). It is highly recommended that you navigate to http://support.microsoft.com/kb/938135 to download and install the hotfix to resolve this issue. It is not recommended that you continue to run the agent for an extended time period without installing the Microsoft hotfix.%n%nFailure to install the hotfix may eventually result in system instability or a system crash. Installation of the hotfix will require a reboot.
12120	Counter value is between range	Alert	The performance counter "%6" (%1) is between the range of %2 and %3, the current values are: \ Average: %4 Minimum: %7 Maximum: %8 Counter Description: %8
12121	Counter value (instance) is between range	Alert	The performance counter "%7" ("%1", instance "%2") is between the range of %3 and %4, the current values are: Average: %5 Minimum: %8 Maximum: %9 Counter Description: %10
12122	Counter value not between range	Alert	The performance counter "%6" (%1) is not between the range of %2 and %3, the current values are: Average: %4 Minimum: %7 Maximum: %8 Counter Description: %9

12123	Counter value (instance) not between range	Alert	The performance counter "%7" ("%1", instance "%2") is not between the range of %3 and %4, the current values are: Average: %5 Minimum: %8 Maximum: %9 View recent performance data from web reports:%6 Counter Description: %10
12150	Performance counter is back above threshold	Alert cleared	The performance counter "%4" (%1) is back above the threshold of %2, the current values are: Average: %3 Minimum: %6 Maximum: %7 Counter Description: %8
12151	Instance of a performance counter is back above threshold	Alert cleared	The performance counter "%5" ("%1", instance "%2") is back above the threshold of %3, the current values are: Average: %4 Minimum: %7 Maximum: %8 Counter Description: %9
12154	Performance counter is back below threshold	Alert cleared	The performance counter "%4" (%1) is back below the threshold of %2, the current values are: Average: %3 Minimum: %6 Maximum: %7 Counter Description: %8
12155	Instance of a performance counter is back below threshold	Alert cleared	The performance counter "%5" ("%1", instance "%2") is back below or at the threshold of %3, the current values are: Average: %4 Minimum: %7 Maximum: %8 Counter Description: %9

12156	A previously alerted performance counter is not available anymore	Alert cleared	The performance counter "Process(*)\% Processor Time" (instance "setup") which previously exceeded the configured threshold, is not available anymore and will not be monitored.
12157	Performance counter equals value again		The performance counter "%1" (%2) on host %3 equals the value of %4 again. Counter Description: %5
12158	Performance counter (instance) equals value again		The performance counter "%1" ("%2", instance "%3") on host %4 equals the value of %5 again. Counter Description: %6
12170	Counter value not between range	Alert cleared	The performance counter "%5" (%1) is not between the range of %2 and %3 anymore, the current values are: Average: %4 Minimum: %6 Maximum: %7 Counter Description: %9
12171	Counter value (instance) not between range anymore	Alert cleared	The performance counter "%6" ("%1", instance "%2") is not between the range of %3 and %4 anymore, the current values are: Average: %5 Minimum: %7 Maximum: %8 Counter Description: %10
12172	Counter value back between range	Alert cleared	The performance counter "%5" (%1) is back between the range of %2 and %3, the current values are: Average: %4 Minimum: %6 Maximum: %7% View recent performance data from web reports: %8 Counter Description: %9
12173	Counter value (instance) back between range	Alert cleared	The performance counter "%6" ("%1", instance "%2") is back between the range of %3 and %4, the current values are:

			Average: %5 Minimum: %7 Maximum: %8 Counter Description: %10
12174	Counter leak detected	Alert	EventSentry detected a potential leak for performance counter "%1" ("%2") over the last %3 hours. During this time, the counter value increased from %4 to %5, with an average increase of %6%% per hour. Out of a total of %3 hours, the hourly average increased %7 times (%8%%). Average: %9 Minimum: %10 Maximum: %11 If available, then you should review the performance data history in the web-based reporting to determine whether you need to take action. If this counter value is not leaking memory, then you may be able to adjust the leak detection settings in the management console. View recent performance data from web reports: %12 Counter Description: %13
12175	Counter leak (instance) detected	Alert	EventSentry detected a potential leak for performance counter "%1" ("%2", instance "%13") over the last %3 hours. During this time, the counter value increased from %4 to %5, with an average increase of %6%% per hour. Out of a total of %3 hours, the hourly average increased %7 times (%8%%). Average: %9 Minimum: %10 Maximum: %11 If available, then you should review the performance data history in the web-based reporting to determine whether you need to take action. If this counter value is not leaking memory, then you may be able to adjust the leak detection settings in the management console. Counter Description: %14

12176	Counter leak is resolved	Alert cleared	The potential leak for performance counter "%1" ("%2") has been resolved, during the last %3 hours the hourly average increased %4 times. The current values are: Average: %5 Minimum: %6 Maximum: %7 Counter Description:%9
12177	Counter leak (instance) is resolved	Alert cleared	The potential leak for performance counter "%1" ("%2", instance "%10") has been resolved, during the last %3 hours the hourly average increased %4 times. The current values are: Average: %5 Minimum: %6 Maximum: %7 Counter Description: %9

Binary data of performance alerts (events) which are dispatched to an email action is converted to images which are subsequently attached to the email alerts. It is not shown as binary data. This is because the EventSentry agent, if configured, generates chart images which are then attached to the event as binary data.

5.5.10 Überwachung von Dateiänderungen und -integrität

Siehe File Monitoring vs. File Access Tracking für einen Vergleich zwischen Datei-Änderungsüberwachung und Dateizugriffsverfolgung.

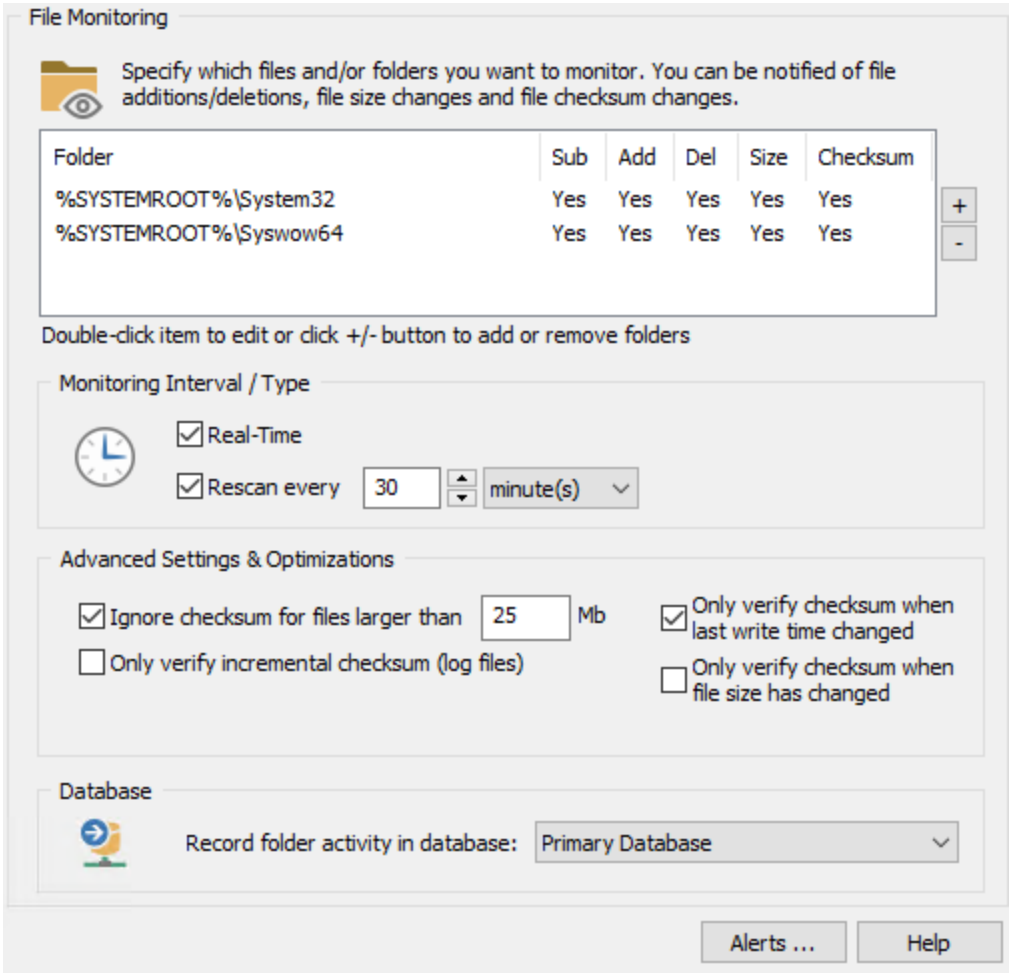
Die Dateiänderungsüberwachung überwacht ein oder mehrere Verzeichnisse und erzeugt Warnmeldungen, wenn Änderungen an bestimmten Dateien in einem Verzeichnis auftreten:

- eine Datei wurde zu einem Verzeichnis hinzugefügt
- eine Datei wurde aus einem Verzeichnis entfernt
- eine Datei vergrößert
- eine Datei verringerte sich in der Größe
- eine Datei hat ihre Prüfsumme geändert (SHA256)

Darüber hinaus kann EventSentry alle Änderungen an der Datenbank protokollieren und ermöglicht die Anzeige des aktuellen Status und der Historie der in den überwachten Verzeichnissen vorgenommenen Änderungen. Die folgenden Dateieigenschaften sind in den Webberichten verfügbar:

- Version
- Hash (SHA256)
- Größe
- Entropie
- Digitale Signatur (falls verfügbar)

- Stream-Informationen



Überwachungsintervall / Typ

Ordner in Echtzeit überwachen

Standardmäßig werden die aufgeführten Verzeichnisse in Echtzeit überwacht. Das bedeutet, dass das Betriebssystem EventSentry benachrichtigt, wenn Änderungen in den betroffenen Verzeichnissen auftreten. Dies ist die effizienteste Überwachungsoption, könnte aber unnötigen Overhead hinzufügen, wenn das überwachte Verzeichnis eine große Anzahl von Dateien enthält, die sich häufig ändern.

Bei der Überwachung von Verzeichnissen in Echtzeit wird empfohlen, die Option "Prüfsumme nur bei der letzten Änderung der Schreibzeit überprüfen" zu aktivieren.

Die Einstellung einer wiederkehrenden Überwachungsoption zusätzlich zur Überwachung von Verzeichnissen in Echtzeit wird auch dann empfohlen, wenn das Betriebssystem aufgrund von Fehlern oder Überlastung keine Echtzeit-Benachrichtigungen an EventSentry sendet.

Überwachung alle X Sekunden

Anstatt Ordner in Echtzeit zu überwachen, können Dateien auch mit einem wiederkehrenden Zeitplan überwacht werden, zum Beispiel alle 10 Minuten. Dies ist nützlich für Verzeichnisse, die eine große Anzahl von Dateien enthalten, die sich sehr häufig ändern, oder für Verzeichnisse, bei denen keine Benachrichtigungen in Echtzeit erforderlich sind.

Die Dateiüberwachungsfunktion kann potenziell eine **erhebliche Menge an CPU-Zeit** verbrauchen, insbesondere bei Verwendung der Prüfsummenfunktion und bei der Überwachung von Ordnern mit vielen Dateien.

Wenn Ordner **mit Tausenden von Dateien** überwacht werden müssen und die CPU-Zeit des EventSentry-Agenten höher als erwartet ist, sollten Sie die folgenden Einstellungen sorgfältig prüfen und anpassen:

- "Alle x Minute(n) überwachen" sollte von der Vorgabe von einer Stunde erhöht werden.
- "Prüfsummen für Dateien ignorieren, die größer sind als" muss möglicherweise verringert werden, um die Anzahl der Erstellungen einer Prüfsumme zu reduzieren.
- "Erkennen von Datei-Prüfsummenänderungen" sollte deaktiviert werden, wenn es nicht benötigt wird

Erweiterte Einstellungen & Optimierungen

Es wird empfohlen, die Optimierungsoptionen in diesem Abschnitt einzustellen, um die Last zu verringern, die der EventSentry-Agent bei der Überwachung von Datei-Prüfsummen auf dem/den überwachten System(en) hat.

Ignore checksums for files larger than

Wenn die überwachten Verzeichnisse große Dateien enthalten (z.B. Dateien, die größer als 50Mb sind), kann die Berechnung der Prüfsumme viele Minuten dauern und die meiste verfügbare CPU-Zeit auf einem Server verbrauchen. Indem Sie eine maximale Dateigröße für die Prüfsummenfunktion festlegen, können Sie verhindern, dass der Dienst die Prüfsumme großer Dateien berechnet.

Only verify incremental checksum (log files)

Berechnet und vergleicht die Prüfsumme nur bis zur vorher bekannten Größe, wenn eine überwachte Datei an Größe zunimmt. Dies ist nützlich für Dateien, die Transaktionen speichern, bei denen bestehende Daten nicht geändert werden, aber neue Daten hinzugefügt werden.

Disable folder redirection on 64-bit systems (Wow64)

Wenn der EventSentry-Agent auf einem 64-Bit-Rechner ausgeführt wird und Ordner überwacht werden, für die das Betriebssystem die Dateiumleitung für 32-Bit-Prozesse aktiviert hat (z.B. %SYSTEMROOT%\SYSTEM32), dann leitet das Betriebssystem diese automatisch zu ihrem "Windows on Windows"-Gegenstück um. Zum Beispiel würde C:\Windows\System32 zu C:\Windows\SysWOW64 umgeleitet werden. Wenn Sie diese Option aktivieren, wird die Ordnerumleitung auf 64-Bit-Systemen deaktiviert.

Only verify checksum when last write time changed

Standardmäßig berechnet EventSentry die Prüfsumme jeder eingebundenen Datei in einem überwachten Verzeichnis, wenn eine Dateiänderung vom Betriebssystem gemeldet wird. Dies kann wiederum eine große Menge an CPU-Zeit verbrauchen, wenn das überwachte Verzeichnis eine große Anzahl von Dateien enthält. Wenn diese Option aktiviert ist, berechnet und vergleicht der Agent die Prüfsumme einer Datei nur dann, wenn sich die letzte Schreibzeit geändert hat.

Only verify checksum when file size has changed

Standardmäßig berechnet EventSentry die Prüfsumme jeder eingebundenen Datei in einem überwachten Verzeichnis, wenn eine Dateiänderung vom Betriebssystem gemeldet wird. Dies kann wiederum eine große Menge an CPU-Zeit verbrauchen, wenn das überwachte Verzeichnis eine große Anzahl von Dateien enthält. Wenn diese Option aktiviert ist, berechnet und vergleicht der Agent die Prüfsumme einer Datei nur dann, wenn sich die Dateigröße geändert hat.

Bekannte Einschränkungen

- Es wird **nicht empfohlen**, auch Verzeichnisse anzugeben, die Unterverzeichnisse von bereits konfigurierten Verzeichnissen sind, wenn die Option "Unterverzeichnisse einbeziehen" gewählt ist. Es wird zum Beispiel nicht empfohlen, sowohl **C:\Dokumente** als auch **C:\Dokumente\Finanzen** zu überwachen.
- Die Überwachung von UNC-Pfaden (z.B. \\SERVER1\Payroll) **wird nicht unterstützt**.

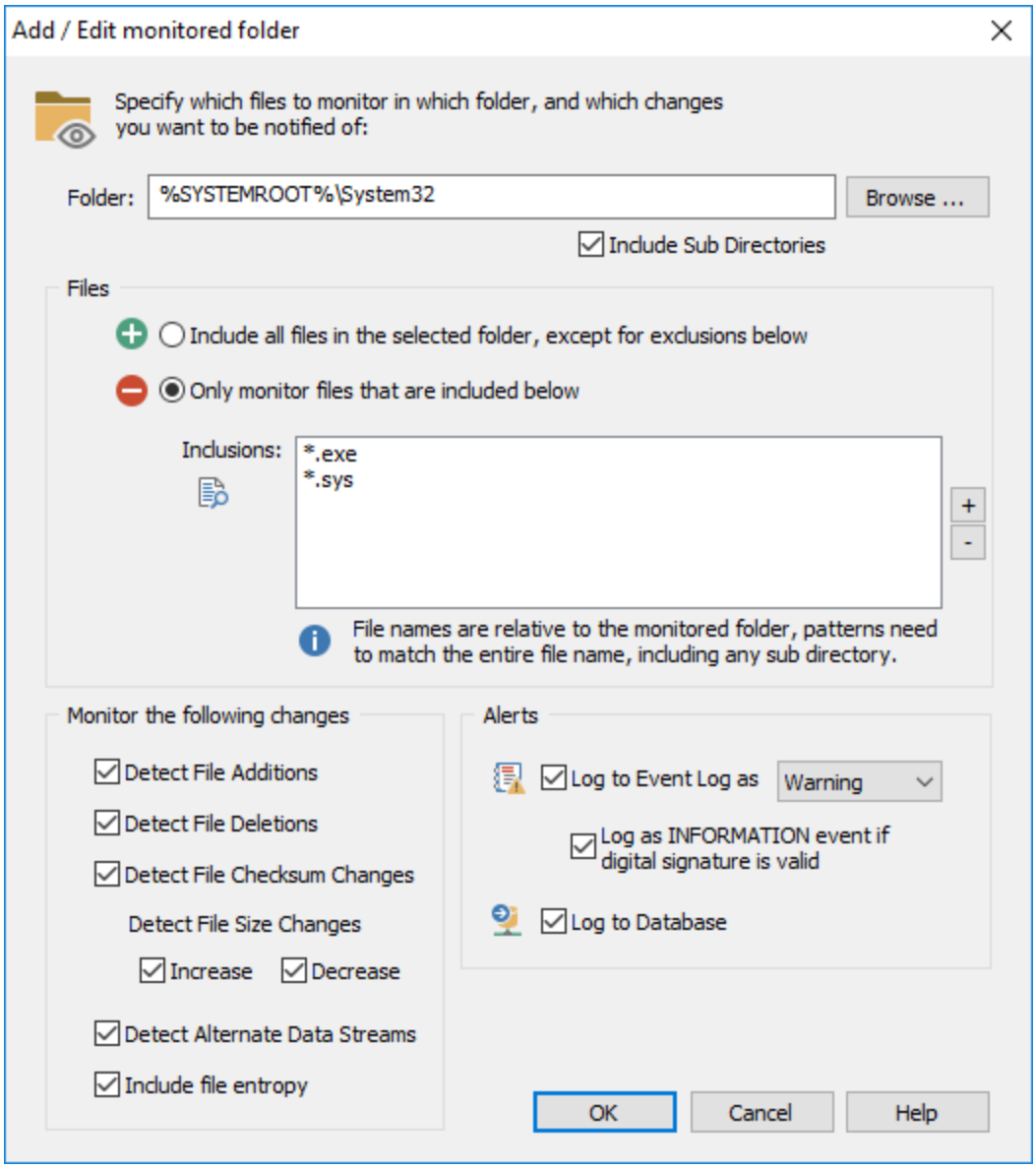
Datenbank

Geben Sie die Datenbank an, die verwendet werden soll, wenn ein Verzeichnis zur Aufzeichnung von Änderungen in der zentralen Datenbank konfiguriert wird.

5.5.10.1 Verzeichnisse

Um ein Verzeichnis hinzuzufügen, klicken Sie auf das Symbol **+** im Abschnitt "Dateiüberwachung", wodurch das Dialogfeld "Überwachten Ordner hinzufügen/bearbeiten" angezeigt wird. In diesem Dialogfeld können Sie Folgendes angeben

- Welches Verzeichnis überwacht werden soll
- Welche Dateien innerhalb des Verzeichnisses überwacht werden sollen
- welche Attribute/Eigenschaften überwacht werden sollen
- Ob Sie Ereignisprotokoll-Warnungen bei Änderungen erzeugen möchten
- ob Änderungen in der Datenbank aufgezeichnet werden sollen

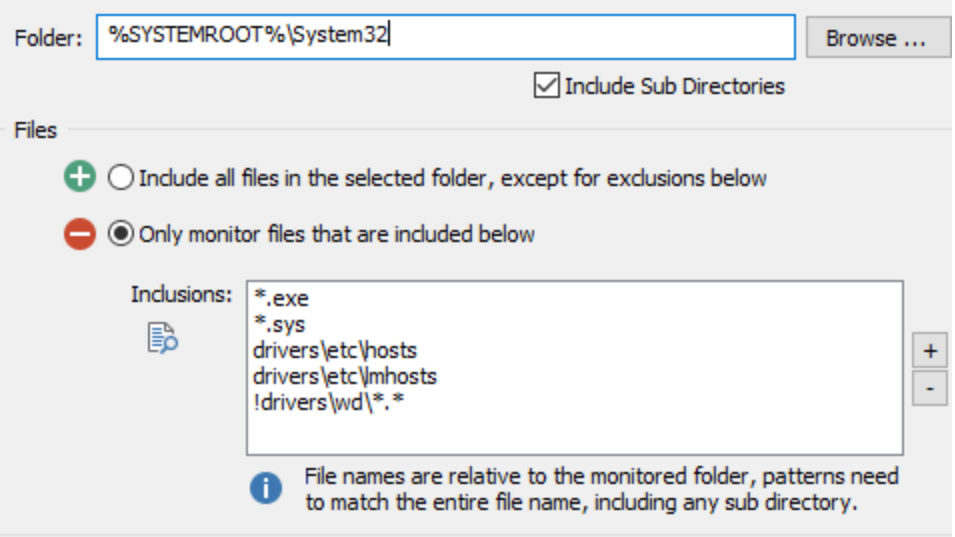


Das im Feld **Ordner** angegebene Verzeichnis wird überwacht, Umgebungsvariablen wie **%SYSTEMROOT%** werden unterstützt. **Die Angabe eines UNC-Pfads wie z.B. \\Server1\Ordner1 wird NICHT UNTERSTÜTZT,** stattdessen muss das Ursprungsverzeichnis der Netzwerkfreigabe verwendet werden, z.B. C:\Payroll. Die Option "Unterverzeichnisse einbeziehen" ermöglicht die Überwachung von Dateien und Ordnern in Unterverzeichnissen des angegebenen Verzeichnisses.

Dateien

Standardmäßig überwacht der Agent alle Dateien im angegebenen Verzeichnis, aber Sie können festlegen, wie die Dateien im angegebenen Verzeichnis überwacht werden. Sie können entweder alle Dateien überwachen und eine Teilmenge von Dateien ausschließen oder nur eine bestimmte Gruppe von Dateien auf der Grundlage von Erweiterung, Dateiname oder Unterordner überwachen.

Einträge in der Dateiliste können auch ausgeschlossen werden, indem ihnen das Ausrufezeichen **!** vorangestellt wird. Die folgende Konfiguration überwacht beispielsweise alle **.exe-** und **.sys-Dateien** sowie die **hosts-** und **lmhosts-Datei** im Verzeichnis **%SYSTEMROOT%\system32**, schließt aber alle Dateien im Verzeichnis **%SYSTEMROOT%\system32\drivers\wd** aus.



Include all files in the selected folder, except for exclusion below

Mit dieser Einstellung werden alle Dateien im ausgewählten Ordner überwacht, mit Ausnahme der Dateien und/oder Platzhalterzeichen, die in der "Ausschlussliste" aufgeführt sind. Klicken Sie daher auf die Symbole + und -, um Dateien oder Muster hinzuzufügen oder zu entfernen, die von der Überwachung ausgeschlossen werden sollen.

Only monitor files that are included below

Überwacht nur einen bestimmten Satz von Dateien im angegebenen Verzeichnis. Klicken Sie auf die Symbole + und -, um Dateien oder Muster hinzuzufügen oder zu entfernen, die überwacht werden sollen. Um zum Beispiel alle ausführbaren Dateien in einem Verzeichnis zu überwachen, klicken Sie auf das Symbol + und geben Sie *.exe ein.

Dateinamen und Pfade müssen relativ zu dem überwachten Ordner angegeben werden. Wenn Sie zum Beispiel den Ordner **C:\Logfiles** überwachen, aber jede Datei im Unterverzeichnis **Temp** (C:\Logfiles\Temp) ausschließen möchten, dann müssten Sie den Filter als **Temp*.*** angeben.

Überwachen Sie die folgenden Änderungen

Dateizusätze erkennen: Erkennt, wenn dem Verzeichnis neue Dateien hinzugefügt werden

Erkennen von Dateilöschungen: Erkennt, wenn Dateien aus dem Verzeichnis gelöscht werden

Erkennen von Datei-Prüfsummenänderungen: Erkennt anhand einer 256-Bit-SHA-Prüfsumme, wenn sich die Prüfsumme einer Datei ändert.

Erhöhte Dateigröße erkennen: Erkennt, wenn die Größe einer Datei zunimmt

Dateigrößenverringerungen erkennen: Erkennt, wenn die Größe einer Datei abnimmt

Warnungen

Sie können den Agenten veranlassen, ein Ereignis im Anwendungsereignisprotokoll zu protokollieren, wenn eine Änderung festgestellt wurde, und Sie können alle Änderungen in einer ausgewählten Datenbank verfolgen.

Log to Event Log as: Protokolliert Änderungen im Anwendungsereignisprotokoll mit dem angegebenen Schweregrad, siehe Ereignisprotokoll für weitere Einzelheiten zu Ereignissen, die mit dieser Funktion protokolliert werden können.
Log as INFORMATION event if digital signature is valid: EventSentry kann die digitale Signatur von Dateien überprüfen und die Ereignisschwere automatisch anpassen, wenn eine Datei eine gültige Signatur hat. Dies kann das Rauschen von Dateiüberwachungsereignissen reduzieren, indem Ereignisse von Dateien, die als legitim erachtet werden, automatisch unterdrückt werden.

Log to Database: Zeichnet Änderungen an der im übergeordneten Dialogfeld ausgewählten Datenbank auf.
Include file entropy: Wenn Sie diese Option aktivieren, wird die Entropie jeder Datei berechnet und in der Datenbank gespeichert.

5.5.10.2 Event Log

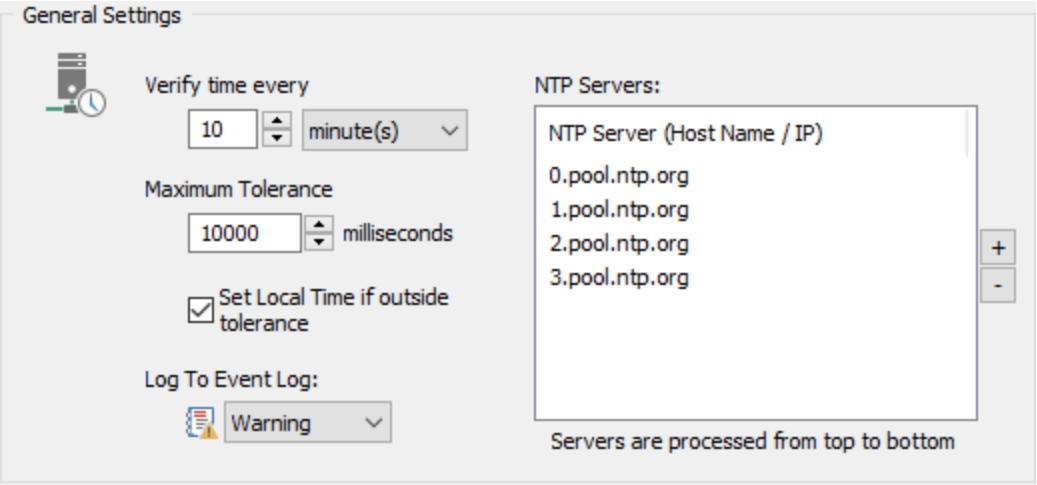

The following events are logged by this feature with the **File Monitoring** event category.

Event ID	Event Description	Example
12200	A SHA-256 checksum change has been detected.	A SHA-256 checksum change has been detected: Package: File Integrity System32 x64 File: C:\WINDOWS\system32\ntoskrnl.exe Old Checksum: B2728620F63488A32597DD97EA40F54460C55D97942748716051F60199C682F8 New Checksum: FE12E1FAEAE5DDF34A93128C7009B69EE88249E6B28BC3D279F2E37ADD3EDC52 Signed: Yes: SHA1 by NETIKUS.NET ltd on 6/15/2018 3:35:51 AM (COMODO RSA Code Signing CA) Entropy: 6.53 The content of the above file has been modified.
12201	A file size change has been detected.	A file size change has been detected: File: C:\WINDOWS\system32\MRT.exe Old Size: 12,619,736 byte(s) New Size: 13,511,640 byte(s) Change: +891,904 byte(s)
12202	A file has been added.	A file has been added to a monitored directory: Directory: C:\WINDOWS\system32 File: C:\WINDOWS\system32_000007_.tmp.dll Size: 14,640 byte(s) Checksum: 93BB82EB2786708ADD9F1538283658EE949AA79E658196F0386AD88FB61320B1

		Signed: no Entropy: 7.23 Version: 3.12.00
12203	A file has been deleted.	A file has been removed from a monitored directory: Directory: C:\WINDOWS\system32 File: _003244_.tmp.dll Last size: 822,272 byte(s) Last checksum: FE2FE85EC553E8DFE0B04900EFE5BDA53F0F087730BDEBB95F681A0DF9900938 Last version: 3.12.00
12210	A directory could not be monitored due to an error.	EventSentry was unable to monitor the directory C:\Files for changes due to the following error: Access Denied. The directory will not be monitored.
12211	A directory could not be monitored in real-time due to an error.	EventSentry was unable to associate the directory C:\Files with an existing I/O completion port due to error: Access Denied. The directory will not be monitored.
12212	A directory could not be opened / accessed due to an error.	EventSentry was unable to open the directory C:\Files due to error: Access Denied. The directory will not be monitored.
12214	A temporary file was upgraded from an earlier, deprecated version of EventSentry.	
12215	Indexing of all monitored directories started.	File monitoring will now index all monitored directories. This process can take several minutes, depending on the number of files and the performance of the computer. When complete, event 12216 will be logged.
12216	Indexing of all monitored directories is complete.	File monitoring has finished indexing all monitored directories.

5.5.11 NTP-Überwachung

Die NTP-Überwachung verifiziert und korrigiert optional die lokale Systemzeit mit einem RFC 1769- und RFC 1305-NTP-Server (bis Version 3) im lokalen Netzwerk und/oder im Internet. Bei der Berechnung des Zeitunterschiedes wird die Netzwerklatenz mit einer Genauigkeit bis auf Millisekunden genau berücksichtigt.

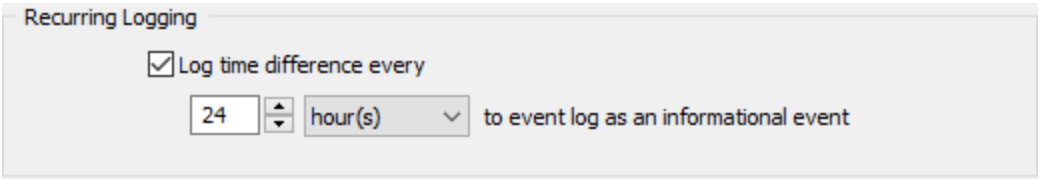


Intervall (Zeit überprüfen)
Gibt an, wie oft die lokale Zeit mit der Zeit des/der konfigurierten NTP-Server(s) verglichen wird.

Maximale Toleranz
Die maximalen Zeitunterschiede (in ms), die zwischen dem lokalen Host und dem NTP-Server akzeptabel sind. Wenn der Zeitunterschied zwischen dem lokalen Host und dem NTP-Server die maximale Toleranz überschreitet, wird ein Ereignis im Ereignisprotokoll protokolliert (mit dem im **Ereignisprotokoll** angegebenen Schweregrad), und die lokale Zeit wird, falls konfiguriert, angepasst.

Ortszeit einstellen, wenn außerhalb der Toleranz
Wenn der Zeitunterschied zwischen dem lokalen Host und dem NTP-Server die maximale Toleranz überschreitet, wird die lokale Zeit an die des NTP-Servers angepasst.

NTP-Server
Die Liste der NTP-Server, die im angegebenen Intervall abgefragt werden. Sie können mehrere NTP-Server angeben, und die Server werden von oben nach unten abgefragt. Wenn ein Server nicht erreichbar ist, wird der nächste NTP-Server kontaktiert.



Wiederkehrende Protokollierung
Aktivieren Sie das Kontrollkästchen **Zeitdifferenz bei jedem protokollieren**, um im angegebenen Intervall ein Informationsereignis im Ereignisprotokoll zu protokollieren. Das Ereignis enthält die aktuelle Zeitdifferenz zwischen dem lokalen Host und dem NTP-Server.

5.5.11.1 Event Log

Die folgenden Ereignisse werden von dieser Funktion mit der Ereigniskategorie **NTP Synchronisation** protokolliert.

Event ID	Event Description	Example

12300	A time difference has been detected.	The time difference between this computer and the NTP server "%1" has exceeded the maximum tolerance of %2 milliseconds. The time difference is: %3.
12301	A time difference has been detected and the local time has been adjusted.	A The local time has been successfully adjusted to %1 after a time difference (%2) has been detected between this computer and NTP server "%3".
12302	The local time could not be adjusted due to an error.	The local time could not be adjusted, even though a time difference (%1) has been detected. The error was: %2.
12303	The current time could not be retrieved from a NTP server.	EventSentry was unable to retrieve the current time from host %1 due to the following error: %2.
12304	The connection to a NTP host timed out.	EventSentry was unable to retrieve the current time from host %1, the connection timed out.
12305	EventSentry has been unable to connect to a NTP server for an extended time period.	EventSentry was unable to retrieve the current time from host %1 for %2 seconds. EventSentry will not attempt to connect to this host again for %2 seconds and will try to use the other NTP servers in the list (if available).
12306	None of the configured NTP servers could be reached.	EventSentry was unable to connect to any of the configured NTP servers (%1). Please make sure that at least one of the listed hosts is a valid NTP server.
12307	This events logs the current time difference between the local host and the NTP server.	Time difference between local host and %1: %2.

5.5.12 Aufgabenplanung (Scheduled Tasks)

Die Überwachung von Scheduled Tasks bietet eine Inventarisierung und Änderungserkennung von Aufgaben (Scheduled Tasks).

Bestandsaufnahme

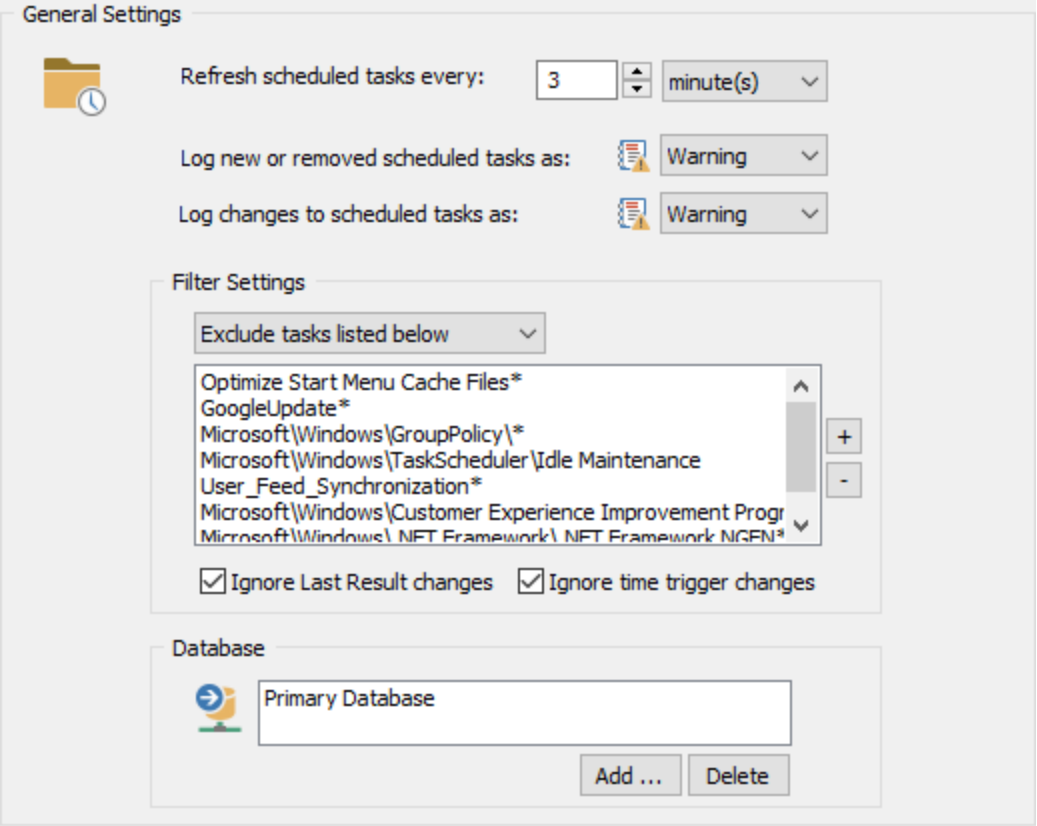
Das Inventar der geplanten Aufgaben ist über das Menü "Status" in den Web Reports zugänglich und umfasst die folgenden Aufgabeneigenschaften:

- Status
- Name der Aufgabe
- Ergebnis des letzten Laufs
- Letzte Laufzeit
- Anzahl der Aktionen
- Details zur Aktion
- Anzahl der Auslöser
- Auslöser-Details

Geschichte & Erkennung von Änderungen

Erkannte Änderungen werden entweder über das Menü "Verlauf" in den Web Reports oder im jeweiligen Ereignisprotokoll angezeigt. Generierte Ereignisse aus geplanten Aufgabenänderungen können Aktionen wie z.B. E-Mail-Benachrichtigungen auslösen. Die folgenden Änderungen werden erkannt:

- Eine geplante Aufgabe wird hinzugefügt
- Eine geplante Aufgabe wird entfernt
- Die mit einer geplanten Aufgabe verbundenen Aktionen werden geändert
- Die mit einer geplanten Aufgabe verbundenen Auslöser werden geändert
- Änderungen zum Status "Aktiviert".
- Der Benutzer, unter dem die Aufgabe läuft, wird geändert



Aktualisierungsintervall

Konfiguriert, wie oft die geplanten Aufgaben auf dem System aktualisiert werden.

Ereignis-Schweregrade

Konfiguriert die Ereignisschwere, mit der neue oder entfernte Aufgaben oder geänderte Aufgaben im Ereignisprotokoll protokolliert werden.

Filter-Einstellungen

Bestimmte Aufgaben können von der Überwachung ausgeschlossen werden ("unten aufgeführte Aufgaben ausschließen"), oder es können nur bestimmte Aufgaben überwacht werden ("Nur unten aufgeführte Aufgaben überwachen"), indem sie mit den Schaltflächen + und - in die Liste aufgenommen werden. Die Option "Alle Aufgaben überwachen" löscht alle Filter und überwacht alle Aufgaben.

Letzte Ergebnisänderungen ignorieren: Kein Ereignis wenn sich das letzte Ergebnis einer Aufgabe ändert.

Ignoriere Zeit-Trigger-Änderungen: Kein Ereignis wenn sich die Zeit eines Triggers ändert.

5.5.12.1 Event Log

Die folgenden Ereignisse werden von dieser Funktion mit der Ereigniskategorie "**Geplante Aufgaben**" protokolliert.

Event ID	Event Description	Example
12400	The Scheduled Tasks monitoring engine has been initialized. %1 cached tasks have been found, %2 tasks are currently configured on this system.	`The Scheduled Tasks monitoring engine has been initialized. 152 cached tasks have been found, 153 tasks are currently configured on this system.`

12410	A new scheduled task has been added:
	
	Name: %1
	Enabled: %2
	User: %3
	State: %4
	
	Triggers:
	%5
	
	Actions:
	%6
		`A new scheduled task has been added:`
		
		`Name: Test`
		`Enabled: 1`
		`User: DOMAIN\UserA`
		`State: Ready`
		
		`Triggers: Type: Schedule (Daily)`
		`Enabled: Yes`
		`Time: 2014-11-25T16:20:57`
		`Day Interval: 1`
		
		`Actions: Type: Start a program`
		`Path: C:\doit.exe`

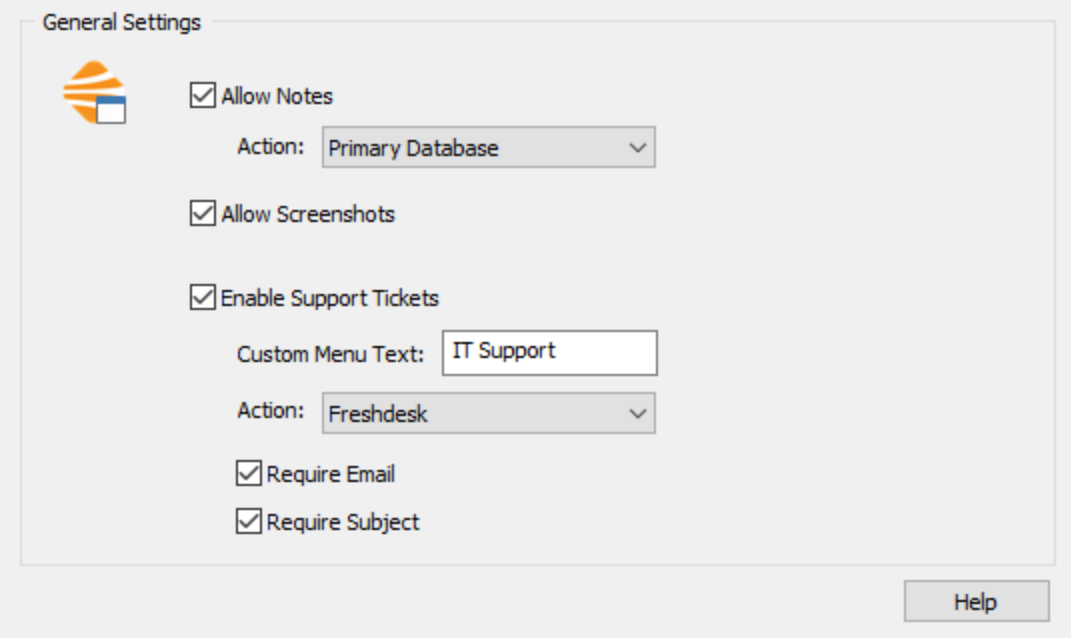
12411	A scheduled task has been removed:
	
	Name: %1
	Enabled: %2
	User: %3
	State: %4
	
	Triggers:
	%5
	
	Actions:
	%6
		`A scheduled task has been removed:`
		
		`Name: Test`
		`Enabled: 1`
		`User: DOMAIN\UserA`
		`State: Ready`
		
		`Triggers: Type: Schedule (Daily)`
		`Enabled: Yes`
		`Time: 2014-11-25T16:20:57`
		`Day Interval: 1`
		
		`Actions: Type: Start a program`
		`Path: C:\doit.exe`

12412	A scheduled task has been changed:
	
	Name: %1
	Field Changed: %2
	
	New Value:
	%3
		`A scheduled task has been changed:`
		
		`Name: Microsoft\Windows\WindowsUpdate\AUScheduledInstall`
		`Field Changed: Triggers`
		
		`New Value:`

	Old Value: %4	Old Value: Type: Schedule (One time) Enabled: Yes Time: 2014-11-25T13:00:00Z

5.5.13 System Status Tray Applikation

Der Systemstatus ist eine Anwendung, die, wenn sie aktiviert ist, im System-Tray sichtbar ist. Über die Tray-Anwendung kann sich der Endbenutzer einen schnellen Überblick über den aktuellen Systemstatus verschaffen, Notizen zu den Web Reports (einschließlich eines Screenshots) senden und eine HTTP-basierte Web-API nutzen, um ein Support-Ticket mit kompatiblen Websites zu erstellen. Die Anwendung für den Systemstatus wird auch als "EventSentray" bezeichnet und ist eine erweiterte Version von "EventSentray", die Teil der kostenlosen EventSentry Sysadmin Tools ist.



Tablett-Symbol
Das Tray-Symbol ist dynamisch und zeigt standardmäßig ein EventSentry-Logo (mit einem Status-Overlay). Wenn Sie mit der Maus über das Symbol fahren, wird der aktuelle Hostname zusammen mit der aktuellen Betriebszeit angezeigt. Die Anwendung überwacht die CPU- und Plattenwarteschlangenlänge im Hintergrund und ändert das Tray-Symbol dynamisch in ein CPU- oder DISK-Symbol, wenn eine hohe Auslastung festgestellt wird:

Der EventSentry-Dienst wird ausgeführt. Wenn der Agent einen Remote-Collector verwendet, wird auch bestätigt, dass der Agent derzeit mit dem Collector verbunden ist.
Der EventSentry-Dienst wird angehalten.
Der EventSentry-Dienst wird ausgeführt, ist aber nicht mit einem Collector verbunden (wird nur angezeigt, wenn der Agent für die Verwendung eines Collectors konfiguriert ist).
CPU-Alarm: CPU-Auslastung 85% oder höher


CPU-Warnung: CPU-Auslastung 70% oder höher

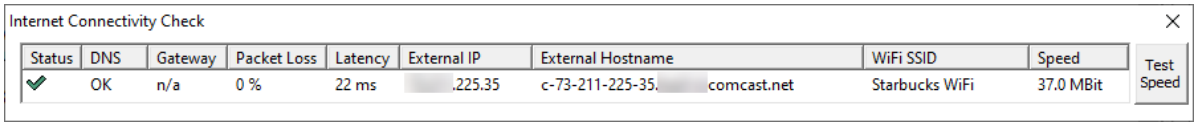

Festplatten-Warnung: Plattenwarteschlangenlänge 3 oder höher

Internet Connectivity Test

Überprüft die Internetverbindung mit einer Reihe von Tests:

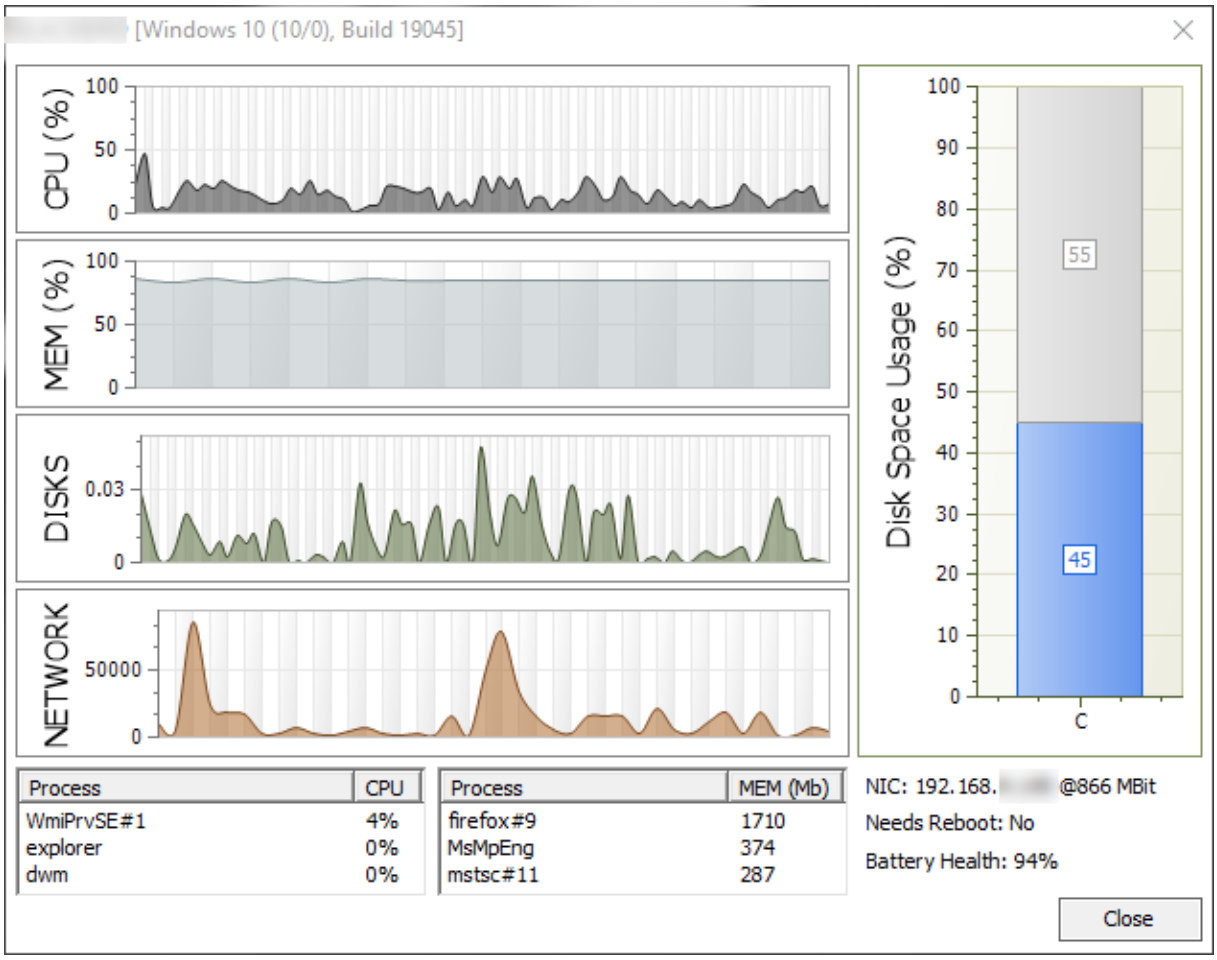
- Überprüfung der DNS-Auflösung
- Versucht die Gateway-IP zu pingen
- Messung von Paketverlusten und Latenzzeiten
- Ermittlung der externen IP-Adresse und des Hostnamens (falls Reverse Lookup möglich ist)
- Zeigt die aktuelle WiFi SSID an, wenn eine Verbindung zu einem WiFi-Netzwerk besteht

Mit der Schaltfläche "Test Speed" wird ein grundlegender Test der **Download-Geschwindigkeit** durchgeführt, indem bis zu 4 Dateien (mit einer Gesamtgröße von weniger als 100 MB) heruntergeladen und die Übertragungsgeschwindigkeit gemessen wird.



System-Informationen

Der Systeminformationsdialog zeigt zusätzliche Leistungsstatistiken und Systeminformationen an und kann entweder durch Doppelklicken auf das Tray-Symbol oder durch Klicken mit der rechten Maustaste auf das Symbol und Auswahl von "Systeminformationen" angezeigt werden.



Der Systeminformationsdialog und das Taskleistensymbol zeigen die folgenden Informationen an:

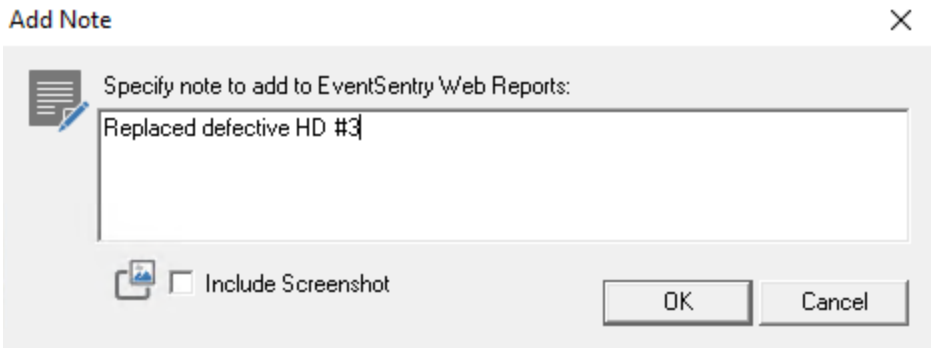
- Hostname
- Verfügbarkeit
- EventSentry-Status
- CPU-Auslastung
- Speicherauslastung
- Festplattennutzung
- Speicherplatznutzung aller physischen Festplatten
- Top 3 Prozesse (CPU-Auslastung)
- Top 3 Prozesse (Speichernutzung)
- Aktuelle IP-Adresse und Verbindungsgeschwindigkeit
- Angabe, ob der Host einen Neustart benötigt
- Batteriezustand (falls zutreffend)
- Andere angemeldete Benutzer (falls vorhanden)

Da die EventSentray-Anwendung nicht mit erhöhten Privilegien ausgeführt wird, enthalten die oben angezeigten Prozesse möglicherweise keine Systemprozesse oder Prozesse von anderen Benutzern, auf die nicht zugegriffen werden kann.

Anmerkungen

Die Web Reports unterstützen das Hinzufügen von Notizen zu Dokumentationszwecken über die Web Reports; Notizen können mit Hostnamen versehen werden, um Notizen mit bestimmten Hosts zu verknüpfen. Die Tray-Anwendung unterstützt das Hinzufügen von Notizen ohne Aufrufen der Web Reports und unterstützt auch das automatische Anhängen von Screen Shots. Dies macht es extrem einfach, Änderungen und Aktivitäten zu dokumentieren, die für andere Teammitglieder nützlich sein können.

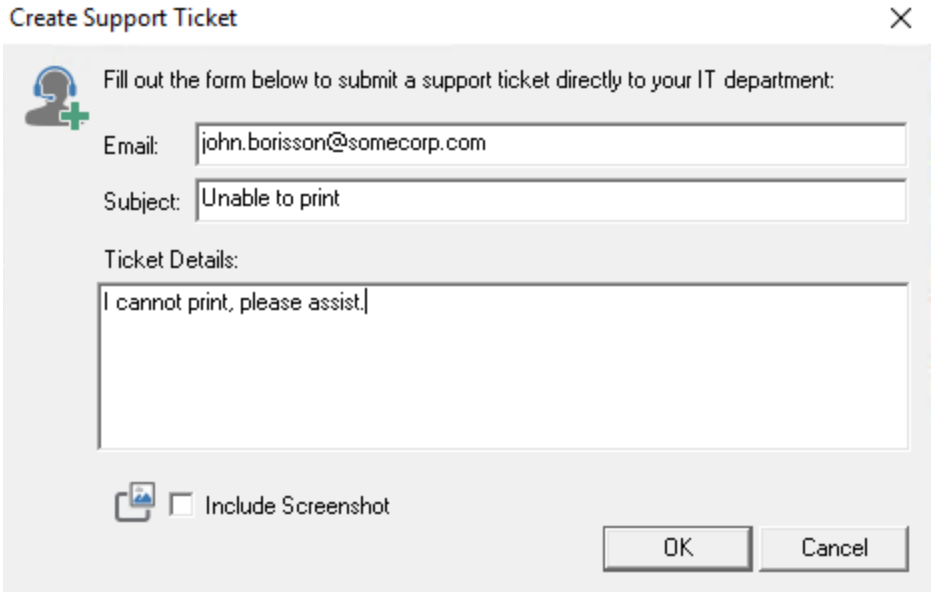
Das Einbeziehen von Screenshots erfordert, dass die ausgewählte Datenbank den Collector verwendet und dass der Collector-Dienst auf demselben Host wie die Web Reports läuft.



Support-Tickets

Wenn ein Ticketing-System eingehende E-Mails akzeptiert und/oder eine Web-API bereitstellt, kann die Tray-Anwendung so konfiguriert werden, dass jeder angemeldete Benutzer Support-Anfragen öffnen kann.

- Name des Hosts
- Angemeldeter Benutzer
- Systemstatistiken einschließlich Betriebssystem, Betriebszeit, IP-Adresse und Version des EventSentry-Agenten (identisch mit E-Mail-Fußzeilen)



Hilfe-Menü
Das Hilfemenü bietet einen Link zur webbasierten Dokumentation von EventSentry, und die Option "Support Package" erstellt ein Archiv, das Informationen enthält, die für die Fehlerbehebung bei technischen Problemen mit dem EventSentry-Agenten relevant sein können und beinhaltet:

- Debug-Protokolle
- Konfiguration
- Crash-Dumps (falls vorhanden)

Die resultierende Zip-Datei kann auf das Support-Portal hochgeladen werden.

5.5.13.1 Konfiguration

Die Konfiguration der Tray-Anwendung ist Teil eines System-Health-Pakets.

Die Einstellungen steuern die folgenden Funktionen der Tray-Anwendung:

- Fähigkeit, Notizen zu speichern
- Unterstützung für Screenshots für Notizen oder Support-Tickets
- Fähigkeit zum Öffnen von Support-Tickets

Wenn alle Optionen deaktiviert sind, unterstützt die Anwendung nur den Systeminformationsdialog und das Hilfemenü.

Notizen
Wenn aktiviert, wird der Menüeintrag "Notiz hinzufügen" zur Tray-Anwendung hinzugefügt, mit dem Benutzer Notizen hinzufügen können.

Screenshots zulassen
Wenn aktiviert, können Benutzer Screenshots sowohl an Notizen als auch an Support-Tickets anhängen.

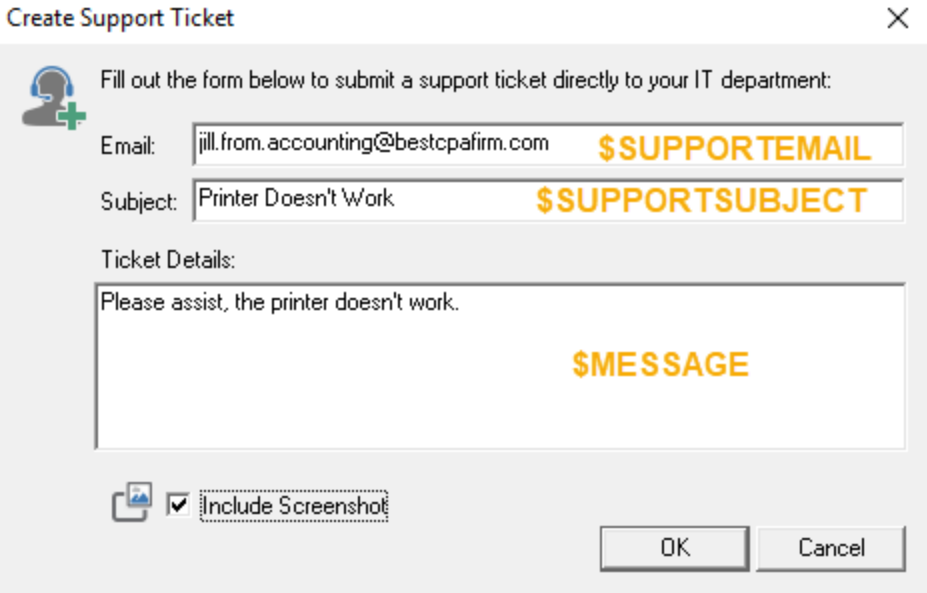
> ⚠ Das Einbeziehen von Screenshots erfordert, dass die ausgewählte Datenbank den Collector verwendet und dass der Collector-Dienst auf demselben Host wie die Web Reports läuft.

Support-Tickets (erfordert den Collector)
Diese Funktion nutzt die HTTP-Aktion zum Einreichen von Support-Tickets im Namen des Benutzers, und als solches kann jedes Ticketing-System integriert werden, das eine HTTP-API bereitstellt.

Custom Menu Entry: Ändert den Standardmenüeintrag "Supportanfrage" in einen vom Benutzer bereitgestellten Eintrag.
Require Email: Erfordert vom Benutzer die Angabe einer E-Mail-Adresse
Require Subject: Erfordert vom Benutzer die Angabe eines Betreffs für die Support-Anfrage

Aktion: Die HTTP-Aktion, die ausgelöst werden soll, muss für den Collector konfiguriert werden. Vom Benutzer eingegebene Daten sind über die folgenden Variablen verfügbar:

Email: $SUPPORTEMAIL
Subject: $SUPPORTSUBJECT
Ticket Details: $MESSAGE



Screenshots werden für HTTP-Aktionen unterstützt, die für "Form Submission" konfiguriert sind, und können im Feld "Form field name for attachments" konfiguriert werden.

5.6 Sicherheit und Compliance

Die Sicherheits- und Compliance-Funktionen analysieren sicherheitsrelevante Informationen aus dem Sicherheitsereignisprotokoll, normalisieren die Daten und speichern sie in der EventSentry-Datenbank. Diese Funktionen sind nicht nur nützlich wenn Sie Regeltreue einhalten müssen, sondern auch für die allgemeine Fehlerbehebung, Statistiken und einen einfacheren Zugriff auf eine Fülle von sicherheitsbezogenen Daten.

> ⚠ Weitere Informationen zur Einhaltung von Vorschriften durch die Regierung finden Sie unter Ressourcen - Compliance - Regulations.

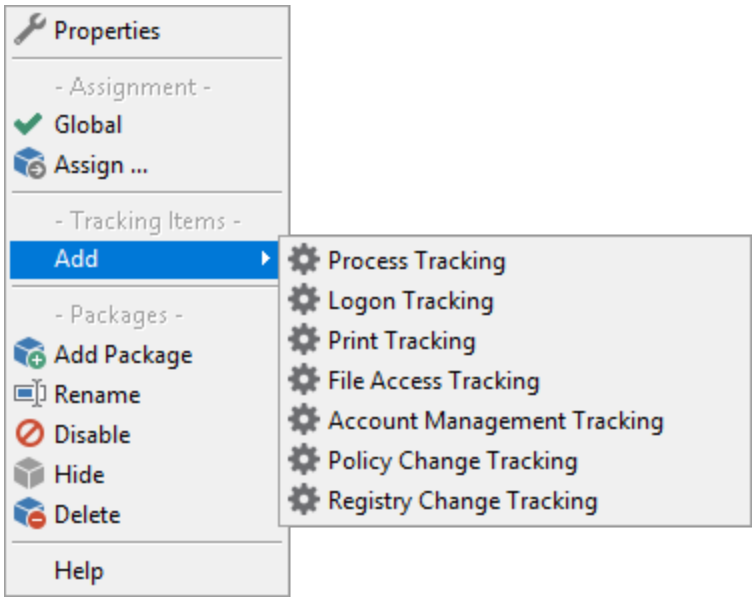
Übersicht

Die folgenden Sicherheits- und Konformitätsfunktionen werden unterstützt und können zu einem Paket hinzugefügt werden:

- Process Tracking
- Logon Tracking
- Print Tracking
- File Access Tracking
- Account Management Tracking
- Policy Change Tracking
- Registry Tracking

Hinzufügen/Entfernen von Objekten zu/von einem Sicherheits- & Compliance-Paket

Um ein neues Objekt zu einem Paket hinzuzufügen, klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie im Untermenü **Hinzufügen** das gewünschte Sicherheits- und Complianceobjekt aus:



Das neue Objekt erscheint unter dem Paket mit einem blauen Radsymbol, das ihm zugeordnet ist. Bitte beachten Sie, dass Sie nicht mehr als ein Objekt desselben Typs zum selben Paket hinzufügen können. Beispielsweise können Sie nicht zwei Objekte **der Registerverfolgung zum** selben Paket hinzufügen.

Um ein Sicherheits- und Complianceobjekt zu entfernen, klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie **Dieses Objekt entfernen**.

5.6.1 Paket-Optionen

Die Paketoptionen unterstützen die Aktivierung oder Deaktivierung eines Pakets, die Eingabe einer Beschreibung, die Zuweisung des Pakets oder die Angabe einer Datenbankaktion auf Paketebene (anstatt sie in jedem Objekt zu konfigurieren).

Siehe "Package Options" für weitere Einzelheiten.

5.6.2 Anforderungen

Alle Sicherheits- und Compliance-Funktionen funktionieren durch das Abfangen von Audit-Fehlschlägen und Audit-Erfolgsereignissen aus den Sicherheitsereignissen. Als solche müssen die jeweiligen Audit-Funktionen in der Sicherheitsrichtlinie der überwachten Computer aktiviert werden. Um zum Beispiel die Erstellung neuer Benutzerkonten zu entdecken, muss die Kontoverwaltungsrichtlinie aktiviert werden.

Alle Funktionen können so konfiguriert werden, dass die Richtlinie automatisch für Sie aktiviert wird, wenn sie nicht bereits aktiv ist. Wir empfehlen jedoch trotzdem, die Überprüfung auf Domänenebene mit Hilfe von Gruppenrichtlinien zu aktivieren, wenn dies möglich ist.

Bitte entnehmen Sie der folgenden Liste, welche Überwachungsrichtlinien für die jeweiligen Funktion erforderlich sind:

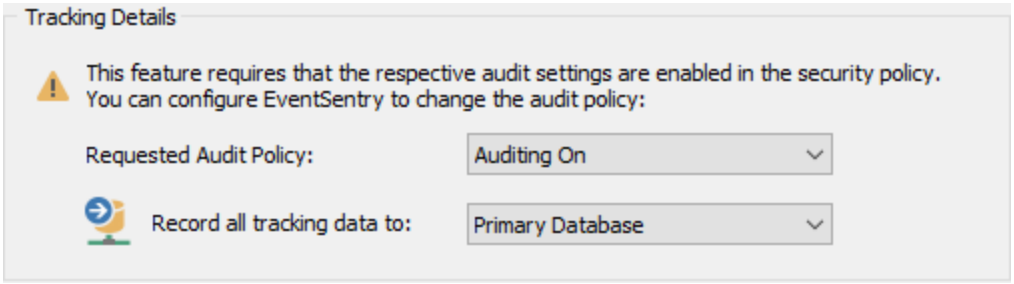
Erforderliche Audit-Konfiguration für Sicherheit & Compliance

Security & Compliance Feature	Windows Auditing Category Windows 2003 und früher	Windows Auditing Category Windows Vista und höher
Process Tracking	Audit process tracking (Success) Prozessnachverfolgung (Erfolg)	Detailed Tracking: - Audit Process Creation - Audit Process Termination Detaillierte Überwachung: - Prozesserstellung überwachen - Prozessbeendung überwachen
Logon Tracking (Console Sessions)	Audit logon events Anmeldeereignisse überwachen	Logon and Logoff: - Logon - Logoff Anmelden / Abmelden - Anmelden überwachen - Abmelden überwachen
Logon Tracking (Network Logons)		Account Logon: - Credential Validation - Kerberos Authentication Service - Kerberos Service Ticket Operations - Other Account Logon Events Kontoanmeldung: - Überprüfung der Anmeldeinformationen - Kerberos-Authentifizierungsdienst - Ticketvorgänge des Kerberos-Diensts - Andere Kontoanmeldungen
File Access Tracking	Audit object access Objektzugriffsversuche überwachen	Object Access: - File System Objektzugriff: - Dateisystem
Account Management Tracking	Audit account management Kontenverwaltung überwachen	Account Management: all subcategories Kontoverwaltung: alle Subkategorien
Policy Change Tracking	Audit policy change Richtlinienänderungen überwachen	Policy Change: - Audit Policy Change - Authentication Policy Change - Authorization Policy Change Richtlinienänderungen:

		- Überwachungsrichtlinienänderungen - Authentifizierungsrichtlinienänderungen - Autorisierungsrichtlinienänderungen
Print Tracking	Log spooler information events	Ereignisprotokoll "Microsoft-Windows-PrintService/Operational" aktivieren
Registry Change Tracking	n/a	Object Access: - Registry Objektzugriff: - Registrierung
Permission Inventory	n/a	n/a

Sobald die erforderlichen Auditing-Optionen festgelegt sind, kann eine der folgenden drei Optionen verwendet werden, um das Auditing zu ermöglichen. Die erforderliche Auditing-Einstellung aus der Spalte **Erforderliches Auditing** wird als **[Auditingoption]** bezeichnet.

1. Sie können den EventSentry-Agenten veranlassen, die erforderliche Revisionseinstellung automatisch zu aktivieren, wenn der Dienst startet, indem Sie **"Auditing ein"** aus der **angeforderten Revisionsrichtlinie** wählen. Stellen Sie in diesem Fall sicher, dass **keine Gruppenrichtlinien** die vom EventSentry-Agenten **festgelegten Richtlinieneinstellungen überschreiben.**



Verwendung des EventSentry-Agenten zur automatischen Aktivierung der "Prozessverfolgung".

2. Es gibt mehrere Möglichkeiten, die "Audit-Prozessverfolgung" außerhalb von EventSentry zu aktivieren:

   Windows 2003 ohne Active Directory
   Öffnen Sie "Lokale Sicherheitsrichtlinien" und navigieren Sie zu "Sicherheitseinstellungen" -> "Lokale Richtlinien" -> "Überwachungsrichtlinie". Doppelklicken Sie auf **[Überprüfungsoption]** und markieren Sie das Kontrollkästchen "Erfolg". Diese Änderung kann einige Minuten dauern, bis sie wirksam wird.

   Windows 2003 mit Active Directory
   Öffnen Sie die entsprechende Gruppenrichtlinie oder öffnen Sie die "Domain-Sicherheitsrichtlinie". Navigieren Sie dort zu "Überwachungsrichtlinie" und setzen Sie **[Audit-**

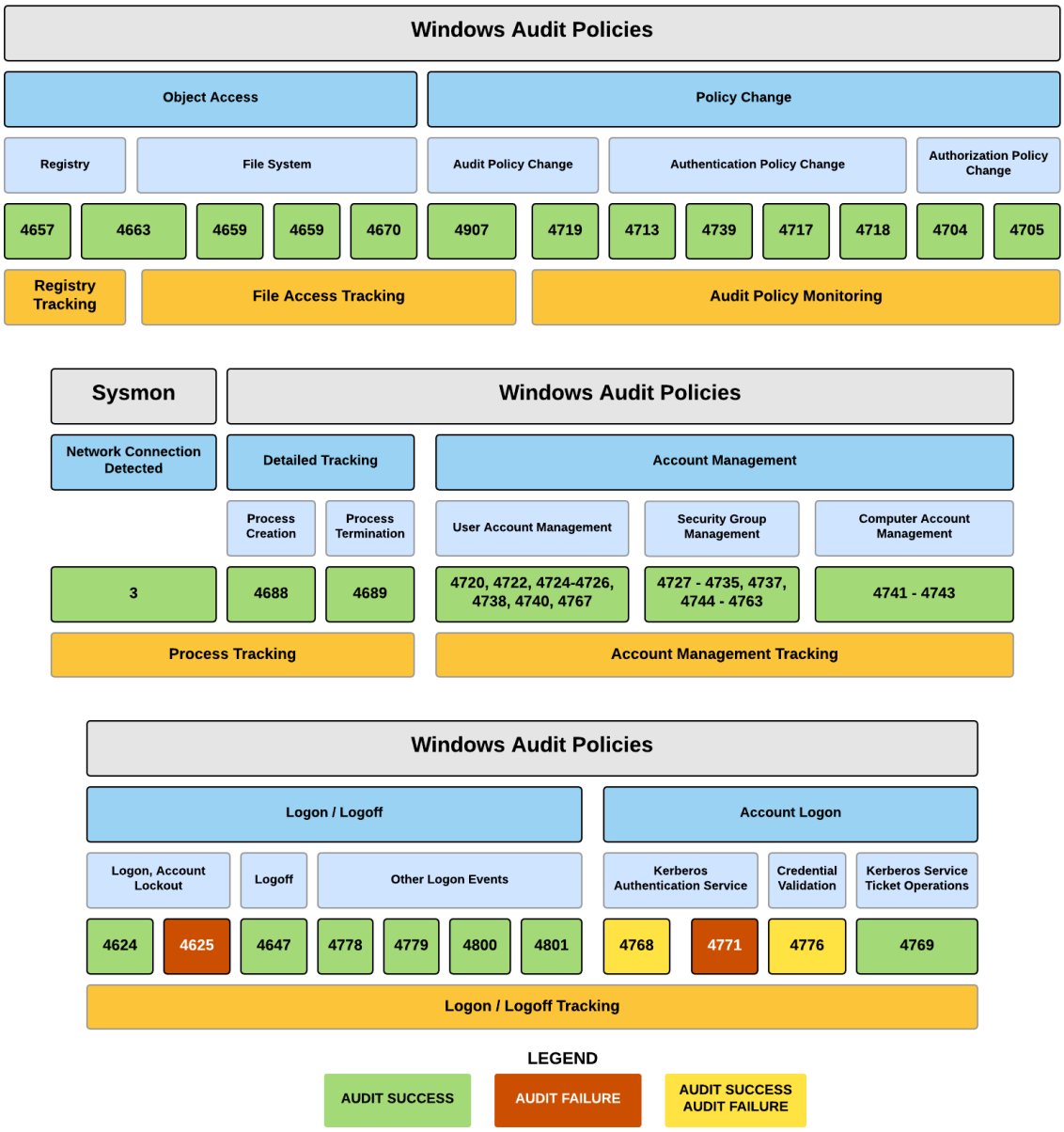
Option] auf "Erfolg". Abhängig von Ihrer Active Directory-Einrichtung müssen Sie möglicherweise eine andere Gruppenrichtlinie als die "Domänen-Sicherheitsrichtlinie" bearbeiten.

Windows 2008 (and höher) mit "Unterkategorieeinstellungen der Überwachungsrichtlinie erzwingen" aktiviert
Öffnen Sie die entsprechende Gruppenrichtlinie oder öffnen Sie die "Domain-Sicherheitsrichtlinie". Navigieren Sie dort zu "Erweiterte Überwachungsrichtlinienkonfiguration" und erweitern Sie die entsprechende Kategorie (siehe Tabelle "Erforderliche Audit-Konfiguration für Sicherheit & Compliance" oben). Konfigurieren Sie dort die erforderlichen Einstellungen auf "Audit-Erfolg".

3. Das Sicherheitsereignisprotokoll "Protokollgröße" muss so konfiguriert werden, dass es "Ereignisse nach Bedarf überschreibt". Es wird außerdem empfohlen, eine Größe von mindestens 2048kb anzugeben. Der EventSentry-Agent schreibt beim Start eine Fehlermeldung in das Anwendungsereignisprotokoll, wenn das Ereignisprotokoll nicht korrekt konfiguriert ist.

   Sie können die Einstellungen für die "Protokollgröße" ändern, indem Sie die "Ereignisanzeige" öffnen (aus den Verwaltungstools) und mit der rechten Maustaste auf "Sicherheitsprotokoll" klicken. Wählen Sie "Eigenschaften" aus dem Menü und überprüfen Sie, ob die "Protokollgröße" korrekt auf "Ereignisse nach Bedarf überschreiben" eingestellt ist. Vergewissern Sie sich auch, dass die "Maximale Protokollgröße" ausreichend groß ist.

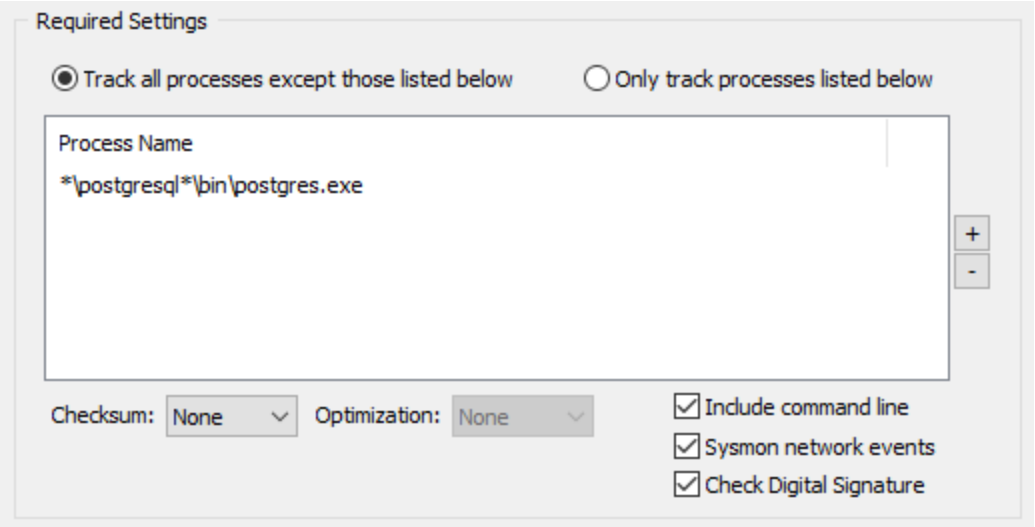
Um die **zuvor aktivierte Prozessverfolgung** des Betriebssystems **zu deaktivieren**, setzen Sie die **angeforderte Audit-Politik auf Auditing aus**. Stellen Sie sicher, dass keine Domänenrichtlinien die vom EventSentry-Agenten durchgeführten Richtlinienänderungen rückgängig machen.



5.6.3 Prozesse

Die Prozessverfolgung zeichnet alle Prozessaktivitäten (Prozesserstellung, Prozessausgang) in einer zentralen Datenbank auf und dient der Überwachung der Anwendungsnutzung. Die gesammelten Informationen können über die Webschnittstelle abgefragt werden, um Tracking-Daten, Historie, Statistiken usw. zu erhalten.

In Kombination mit Sysmon und NetFlow kann die Prozessverfolgungsfunktion **viele Einblicke** in die Prozessaktivität, einschließlich der damit verbundenen Netzwerkaktivität, auf überwachten Systemen liefern.



Anforderungen

Diese Funktion funktioniert durch Abfangen von Audit-Erfolgsereignissen, die in das Sicherheitsereignisprotokoll geschrieben werden, wenn die Audit-Prozessverfolgung in der lokalen Sicherheitsrichtlinie des überwachten Hosts aktiviert ist. Daher müssen einige Voraussetzungen erfüllt sein, bevor die Prozessverfolgung ordnungsgemäß funktionieren kann. Einzelheiten finden Sie unter Anforderungen.

Konfiguration

Nachverfolgung aller Prozesse (mit Ausnahmen)

Wählen Sie "Alle Prozesse außer den unten aufgeführten verfolgen", um alle Prozesse zu überwachen. Um Prozesse auszuschließen, klicken Sie auf die Schaltfläche "+" und geben Sie die auszuschließende Prozessdatei an (siehe Infobox unten).

Nur ausgewählte Prozesse verfolgen

Wählen Sie "Nur unten aufgeführte Prozesse verfolgen" und klicken Sie auf die Schaltfläche +, um Prozesse, die überwacht werden sollen, zur Liste hinzuzufügen.

Prozesse müssen entweder mit einem Platzhalter (z.B. ***\postgres.exe**) oder unter Verwendung des vollständigen Pfades (z.B. C:\Program Files (x86) \EventSentry\postgresql\bin\postgres.exe) hinzugefügt werden.

Befehlszeile einbeziehen

Erfasst die Befehlszeile von Prozessen, wenn aktiviert. Die Prozessbefehlszeile wird entweder von Ereignis 4688 aus geparst, wenn es im Betriebssystem konfiguriert und vorhanden ist (suchen Sie hier nach "Process Command Line" für weitere Einzelheiten) oder vom laufenden Prozess aus abgefragt. Letzteres funktioniert nur, wenn der Prozess noch läuft, wenn der Agent versucht, diese Information zu erhalten, und funktioniert möglicherweise nicht für Prozesse, die nur für eine sehr kurze Zeit aktiv sind (z.B. weniger als 1 Sekunde).

Leistungswarnung: Wenn die Prozessbefehlszeile im Ereignis 4688 nicht verfügbar ist, kann EventSentry WMI verwenden, um die Prozessbefehlszeile zu erhalten. Dies kann zu einer erheblichen Leistungseinbuße führen, insbesondere auf Systemen mit einer hohen Prozessaktivität.

Sicherheitswarnung: Verwenden Sie diese Option mit Vorsicht, Befehlszeilenargumente können sensible Informationen wie Benutzernamen und Passwörter enthalten.

Ereignisse im Sysmon-Netzwerk
EventSentry kann mit dem Dienstprogramm Sysmon von Windows Sysinternals integriert werden.

Digitale Signatur prüfen
Prüft und zeigt an, ob die ausführbare Datei digital signiert ist.

Prüfsumme
Wenn diese Option aktiviert ist, wird die angegebene Art der Prüfsumme (SHA 256, 384 oder 512) jedes ausgeführten Prozesses berechnet und im Bericht zur Verfügung gestellt. Prüfsummen können mit Sites wie virustotal.com korreliert werden.

Es wird empfohlen, die Optimierung zu aktivieren, um die potenzielle CPU-Last zu reduzieren, die der EventSentry-Agent auf dem überwachten System hat, und die Optimierung in Hochsicherheitsumgebungen zu deaktivieren. Wenn die Optimierung aktiviert ist, wird der Agent die Prüfsumme häufig ausgeführter Prozesse vorübergehend zwischenspeichern. Die Standard-Optimierung greift auf zwischengespeicherte Prüfsummen zu, wenn sich die Schreibzeit der Datei seit der letzten Generierung einer Prüfsumme nicht geändert hat; die Hoch-Optimierung greift auf zwischengespeicherte Prüfsummen zu, wenn die gleiche Datei innerhalb der letzten 5 Sekunden ausgeführt wurde **und** sich die Schreibzeit nicht geändert hat.

Aktivieren der Prozessverfolgung im Betriebssystem
Da die Prozessverfolgung im Betriebssystem aktiviert sein muss, können Sie den Agenten so konfigurieren, dass er automatisch aktiviert wird, wenn er nicht bereits aktiviert ist. Weitere Informationen finden Sie unter Anforderungen.

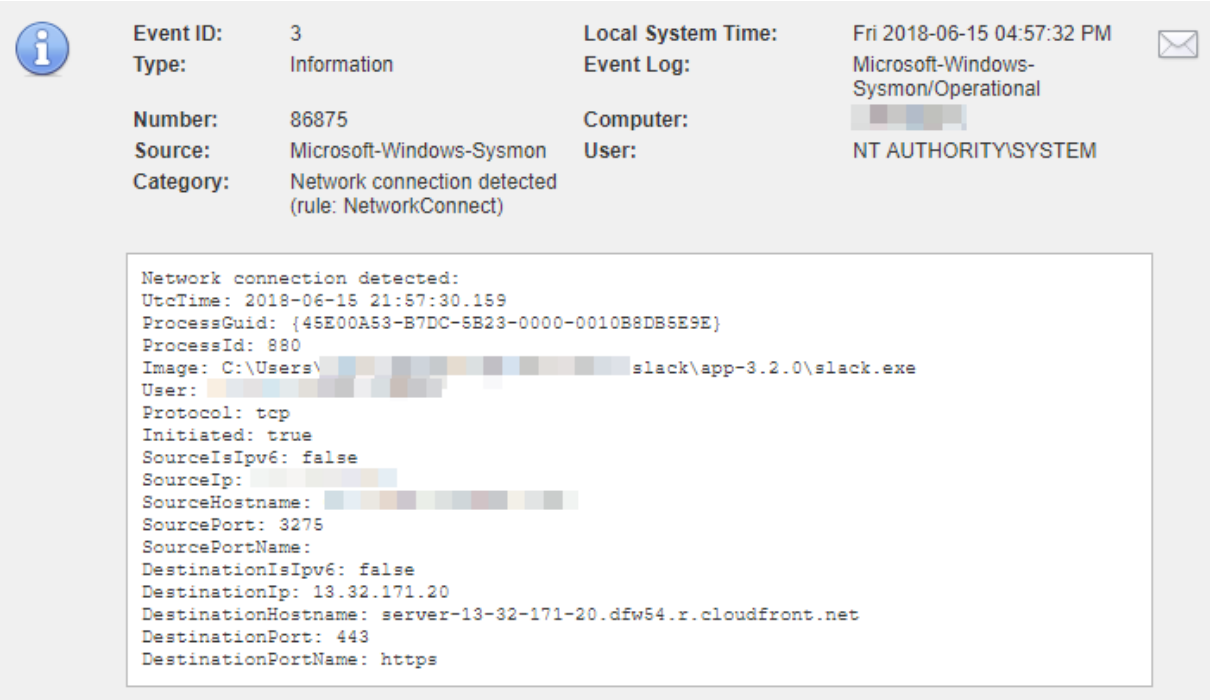
Datenbank
Wählen Sie die Datenbankaktion, die auf die richtige Datenbank verweist.

Zusätzliche Merkmale
Wenn die angegebene Datenbank vorübergehend nicht verfügbar ist, dann speichert EventSentry die ausstehenden Prozessverfolgungsdaten im Cache und führt die Transaktionen aus, wenn der Datenbankserver wieder verfügbar ist.

5.6.3.1 Sysmon Integration

Der System Monitor Service & Driver (kurz Sysmon) protokolliert eine Vielzahl von Ereignissen - meist als Reaktion auf Prozessaktivitäten, die auf einem System auftreten - im Microsoft-Windows-Sysmon/Operational-Ereignisprotokoll. Sysmon-Ereignisse ähneln den 4688- und 4689-Ereignissen, die von Windows beim Starten und Beenden eines Prozesses im Sicherheitsereignisprotokoll protokolliert werden. Die von Sysmon erzeugten Ereignisse sind jedoch wesentlich detaillierter und decken andere Bereiche ab, wie z.B. Netzwerkaktivität, Dateischreibaktivität und mehr.

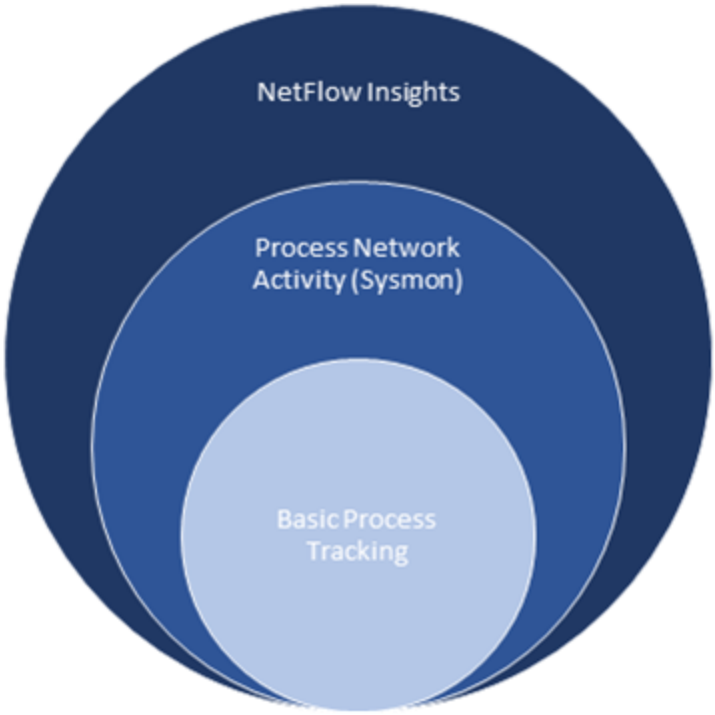
Wenn Sysmon für die Protokollierung der Netzwerkaktivität konfiguriert ist, protokolliert es ein Ereignis immer dann, wenn ein Windows-Prozess eine Netzwerkverbindung herstellt:



Sysmon logs network activity by slack.exe

Wenn aktiviert, fängt EventSentry die Ereignis-ID 3 aus dem Microsoft-Windows-Sysmon/Operational-Ereignisprotokoll ab, die angibt, dass ein lokaler Prozess eine Netzwerkverbindung erstellt hat. Diese Daten werden mit den Prozessverfolgungsdaten korreliert, die aus dem Windows-Sicherheitsereignisprotokoll gesammelt wurden und in den Web Reports verfügbar sind. Wenn Sysmon-Daten für einen Prozessverfolgungseintrag verfügbar sind, dann wird in den Web Reports neben der PID ein schwarzes Plus-Symbol angezeigt.

Wenn EventSentry so konfiguriert ist, dass es auch NetFlow-Daten erfasst, können die von Sysmon bereitgestellten Daten zur Untersuchung des vom Prozess erzeugten zugehörigen Netzwerkverkehrs verwendet werden. Jede Zeile im Sysmon-Bericht enthält einen Link zum NetFlow History-Bericht.



Sysmon Installation

Sysmon kann von https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon#configuration-files heruntergeladen und von einer erweiterten Eingabeaufforderung aus mit einem der beiden folgenden Befehle installiert werden:

Standardinstallation mit Netzwerkverbindungen	Installation mit benutzerdefinierter Sysmon-Konfigurationsdatei (zusätzliche Protokollierung)
`Sysmon64.exe -accepteula -i -n`	`Sysmon64.exe -accepteula -i "C:\Program Files\EventSentry\resources\sysmon.conf"`

Der -n-Switch ist wichtig, da er Sysmon anweist, die Netzwerkaktivität von Prozessen zu protokollieren. Ersetzen Sie "Sysmon64.exe" durch "Sysmon.exe" auf 32-Bit-Systemen. Ungeachtet dessen, was in der offiziellen Dokumentation angegeben ist, ist oft ein Neustart erforderlich, um die Protokollierung der Ereignis-ID 3 zu aktivieren.

Um zu überprüfen, ob Sysmon korrekt installiert und konfiguriert wurde, führen Sie `sysmon64 -c` aus, das eine ähnliche Ausgabe wie die unten gezeigte liefern sollte (wenn mit -n installiert):

```
System Monitor v7.03 - System activity monitor
Copyright (C) 2014-2018 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Current configuration:
- Service name: Sysmon64
- Driver name: SysmonDrv
- HashingAlgorithms: SHA1
- Network connection: enabled
- Image loading: disabled
- CRL checking: disabled
- Process Access: disabled
```

Es ist wichtig das **Network connection** "**enabled**" anzeigt.

> NETIKUS.NET ltd und EventSentry sind in keiner Weise mit Sysinternals verbunden und sind nicht in der Lage, Support für das Dienstprogramm Sysmon zu leisten.

5.6.4 Anmeldungen

Logon Tracking verfolgt sowohl erfolgreiche Konsolenanmeldungen als auch eine Vielzahl von Netzwerkanmeldungen - fehlgeschlagene als auch erfolgreiche.

Konsolen-Anmeldungen

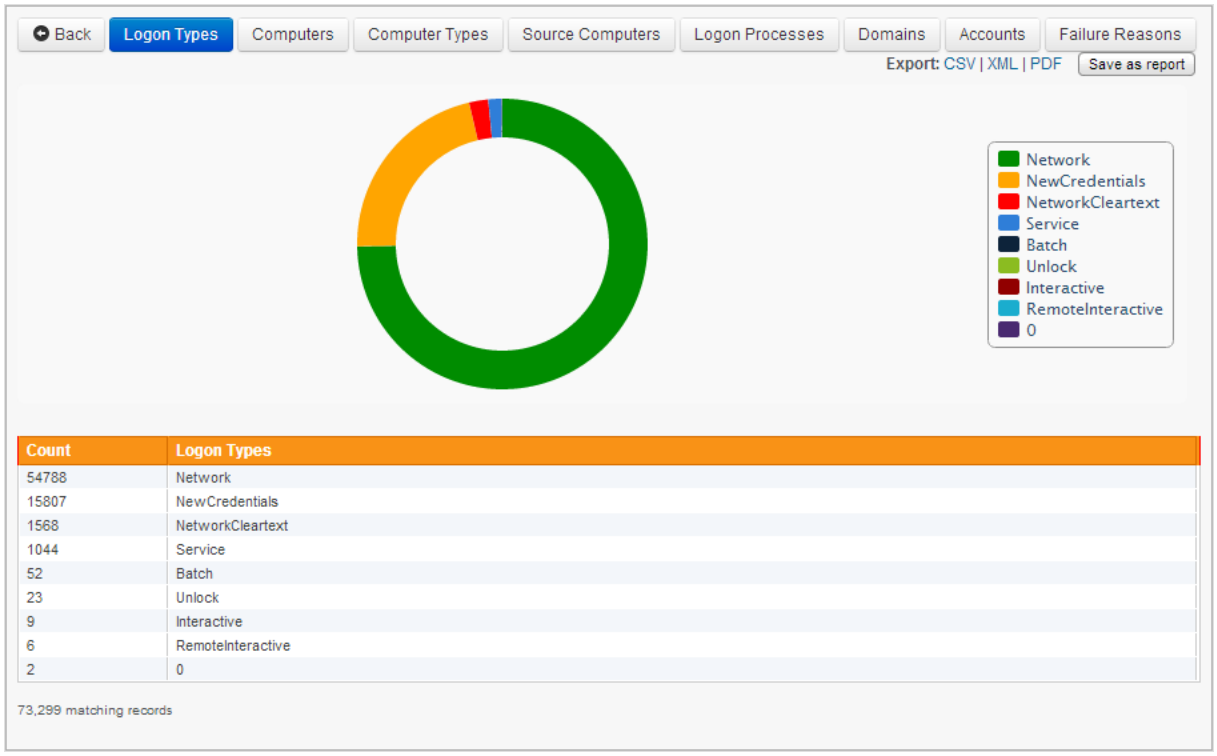
Verfolgt interaktive Anmeldungen, die entweder physisch oder über Remote-Desktop (Terminaldienste) durchgeführt wurden. Diese Funktion sammelt eine Vielzahl von Informationen über eine Anmeldesitzung, wie z.B. den Quellcomputer, Anmeldedauer und mehr. Weitere Informationen finden Sie unter Konsolensitzung.

Netzwerk-Anmeldungen

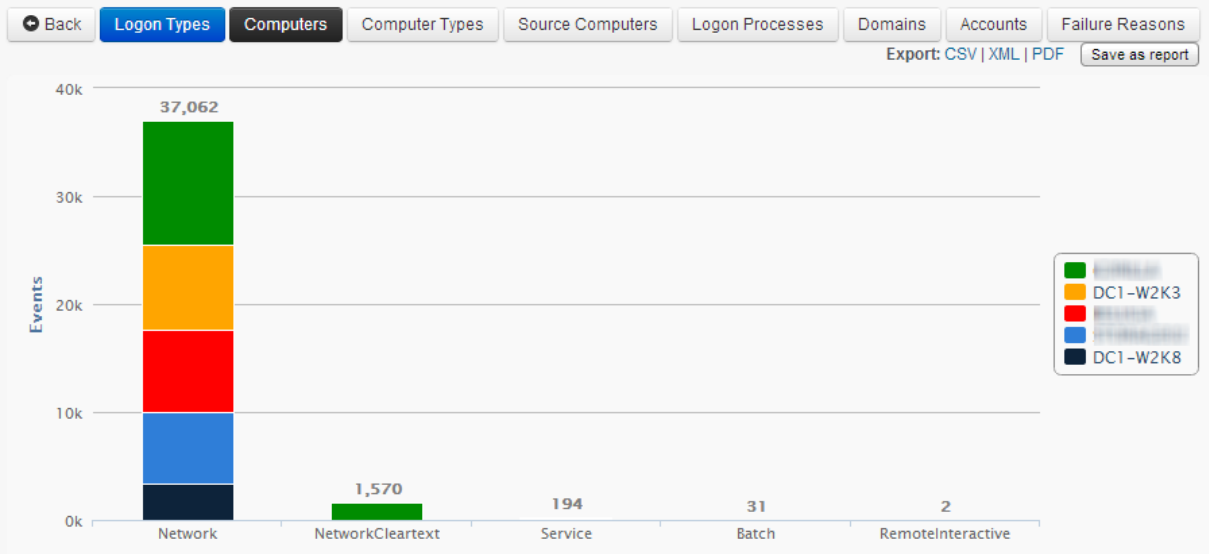
Die Verfolgung der Netzwerkanmeldung umfasst Folgendes:

- Analyse von Anmeldefehlern: Verfolgt alle Authentifizierungsfehler
- Domänenkonto-Authentifizierung: Verfolgt alle erfolgreichen Domänenkonto-Authentifizierungen
- Benutzeranmeldung nach Servertyp: Verfolgt alle Anmeldungen

Siehe Netzwerkanmeldungen für weitere Informationen.



Logon By Type: Verteilung von Anmeldetyp



Logon By Type: Anmeldetypen sind per Domain Controller gruppiert

5.6.4.1 Konsolen-Anmeldungen

Die Konsolen-Anmeldeverfolgung zeichnet alle Anmeldeaktivitäten (interaktive Anmeldungen und Terminaldienste-Anmeldungen) in einer zentralen Datenbank auf und dient der Überwachung der Anmeldungsnutzung auf Workstations und Servern. Die gesammelten Informationen können über die Web-Reports abgefragt werden, um Informationen zu erhalten wie

- Welcher Benutzer hat sich auf welchem Computer angemeldet
- Wie lange der Benutzer angemeldet war
- Kumulative Informationen wie z.B. wie lange ein Benutzer im Laufe eines Zeitraums angemeldet war

Anforderungen

Diese Funktion funktioniert durch Abfangen von Audit-Erfolgsereignissen, die in das Sicherheitsereignisprotokoll geschrieben werden, wenn Audit-Anmeldeereignisse in der lokalen Sicherheitsrichtlinie des überwachten Hosts aktiviert ist. Daher müssen einige Voraussetzungen erfüllt sein, bevor die Anmeldeverfolgung ordnungsgemäß funktionieren kann. Einzelheiten finden Sie unter Anforderungen.

> ⚠ Windows zeichnet An- und Abmeldeaktivitäten nur auf dem Host auf, auf dem sich der Benutzer tatsächlich anmeldet. Wenn Sie das An- und Abmelden aller Benutzer in einer Domänenumgebung überwachen wollen, müssen Sie die EventSentry Agent auf allen Computern, auf denen sich Benutzer anmelden können, einschließlich aller Arbeitsstationen. Sie werden nicht in der Lage sein, alle An- und vor allem Abmeldeaktivitäten zu verfolgen, indem Agenten nur auf dem/den Domänencontroller(n) installiert werden. Dies ist keine Einschränkung von EventSentry, sondern von Windows selbst.

Gesammelte Daten

EventSentry sammelt die folgenden Anmeldeinformationen auf allen unterstützten Windows-Plattformen:

Bereich	Beschreibung

Anmeldungs-Typ	"Konsole" oder "Terminaldienste"
Anmelde-ID	Eine eindeutige hexadezimale Zahl, die die Anmeldung an der Maschine identifiziert
Computer	Der Computer, auf dem sich der Benutzer angemeldet hat
Gruppe	Die Gruppe, in der der Computer Mitglied ist
Benutzername	Benutzername des Benutzers, der sich an-/abgemeldet hat
Bereich	Domäne (oder Computername) des Benutzers, der sich an-/abgemeldet hat
Logon-Privilegien	ob der Benutzer ein lokaler Administrator ist
Login Datum / Uhrzeit	Datum und Uhrzeit, zu der sich der Benutzer angemeldet hat
Abmeldedatum/-zeit	Datum und Uhrzeit der Abmeldung des Benutzers
Dauer	Die Zeitspanne, in der der Benutzer angemeldet war

Datenschutz

Da das Sammeln von Anmeldedaten die Aktivitäten eines Benutzers bis zu einem gewissen Grad nachverfolgt, müssen Sie dennoch sicherstellen, dass das Sammeln dieser Daten nicht die geltenden Unternehmensrichtlinien oder Gesetze beeinträchtigt oder gegen diese verstößt.

Konfiguration

Alle Benutzer verfolgen (mit Ausnahmen)

Wählen Sie "Alle Benutzer außer den unten aufgeführten verfolgen", um alle Anmeldungen zu überwachen. Um Benutzer auszuschließen, klicken Sie auf die Schaltfläche "+" und geben Sie den Benutzernamen oder einen Teil des auszuschließenden Benutzernamens an.

Nur ausgewählte Benutzer verfolgen

Wählen Sie "Nur unten aufgeführte Benutzer verfolgen" und klicken Sie auf die Schaltfläche +, um Benutzer, die verfolgt werden sollen, zur Liste hinzuzufügen.

Nur administrative Benutzeranmeldungen verfolgen

Wenn dieses Kontrollkästchen aktiviert ist, wird eine Konsolenanmeldung nur dann verfolgt, wenn der sich anmeldende Benutzer Teil der lokalen Gruppe "Administratoren" ist - entweder direkt oder durch verschachtelte Gruppenmitgliedschaft.

Aktivieren der Anmeldeverfolgung im Betriebssystem

Da die Anmeldeverfolgung im Betriebssystem aktiviert sein muss, können Sie den Agent so konfigurieren, dass er automatisch aktiviert wird, wenn er nicht bereits aktiviert ist. Bitte beachten Sie die Anforderungen für weitere Informationen.

 Datenbank

Wählen Sie eine Datenbankaktion, in der die Anmeldedaten gespeichert werden sollen.

RDP Gateway Servers

Bei der Verwendung von RDP-Gateway-Servern kann %PRODUCT% die tatsächliche Remote-IP-Adresse des Clients melden, der sich über den Gateway-Server verbindet. Dies erfordert die folgenden Anforderungen:

1. Das Ereignisprotokoll "Microsoft-Windows-TerminalServices-Gateway" wird auf dem RDP-Gateway-Server überwacht und die Ereignisse werden in dieselbe Collector-aktivierte Datenbank geschrieben, die auch für die Konsolenverfolgung verwendet wird.
2. Der Collector ist aktiviert.

Wenn die oben genannten Voraussetzungen erfüllt sind, sollte die Spalte "Remote-IP" im Konsolenbericht die tatsächliche IP-Adresse des Remote-Clients anzeigen, der die RDP-Verbindung initiiert, und nicht die IP-Adresse des RDP-Gatewayservers.

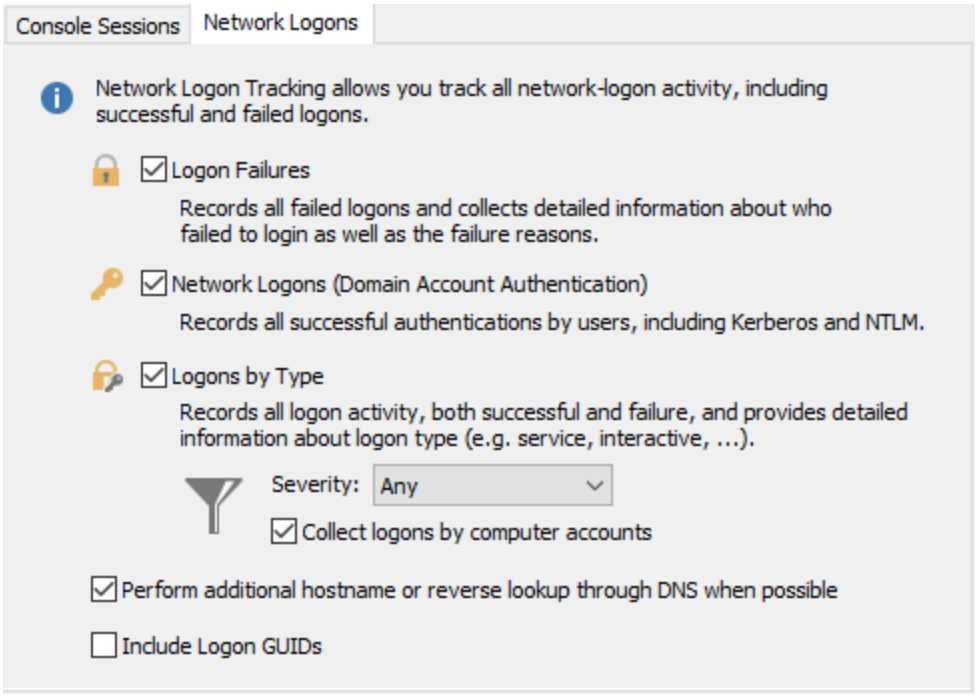
5.6.4.2 Anmelde-Aktivität

Die Netzwerkanmeldeverfolgung sammelt eine Vielzahl von Informationen über erfolgreiche und fehlgeschlagene Anmeldungen in einem Netzwerk. Die Netzwerkanmeldeverfolgung ist in einer Vielzahl von Szenarien nützlich:

- Einhaltung gesetzlicher Vorschriften
- Überprüfung der Netzwerksicherheit
- Fehlerbehebung
- Netzwerk-Anmeldestatistik

Mit den gesammelten Daten können z.B. die folgenden Statistiken / Berichte erstellt werden:

- Häufigste Gründe für fehlgeschlagene Anmeldungen
- Server/Workstations mit den meisten fehlgeschlagenen Anmeldungen
- Häufigste Anmeldungsarten (z.B. Dienst, interaktiv, etc.)
- Protokollverteilung (z.B. NTLM vs. Kerberos)
- und vieles mehr



Fehlgeschlagene Anmeldungen

Dokumentiert alle Authentifizierungen von Benutzern an Domänencontrollern. Beachten Sie, dass jedes Mal, wenn sich ein solcher Benutzer bei seiner eigenen Arbeitsstation oder seinem eigenen Mitgliedsserver anmeldet, eine Netzwerkanmeldung bei einem DC erzeugt wird, da die Arbeitsstation des Benutzers auf den Domänencontroller unter den Anmeldedaten des Benutzers zugreifen muss, um Gruppenrichtlinien/Benutzerkonfiguration anzuwenden.

Fehlgeschlagene Anmeldungen

Windows 2003 und älter

Ereignis-IDs	672, 675, 676, 680, 681 Windows Vista, Windows 2008 und später 4768, 4771, 4776

Netzwerk-Anmeldungen

Dokumentiert alle Authentifizierungen von Benutzern an Domänencontrollern. Beachten Sie, dass jedes Mal, wenn sich ein solcher Benutzer bei seiner eigenen Arbeitsstation oder seinem eigenen Mitgliedsserver anmeldet, eine Netzwerkanmeldung bei einem DC erzeugt wird, da die Arbeitsstation des Benutzers auf den Domänencontroller unter den Anmeldedaten des Benutzers zugreifen muss, um Gruppenrichtlinien/Benutzerkonfiguration anzuwenden.

	Netzwerk-Anmeldungen
 Ereignis-IDs	Windows 2003 und älter 672, 673, 680 Windows Vista, Windows 2008 und später 4768, 4769, 4776

Anmeldungen nach Typ

Dokumentiert alle Anmeldungen an überwachten Servern. Es bietet Folgendes:

- Vollständige Aufzeichnung aller Zugriffsversuche auf den Computer, unabhängig von der Art des verwendeten Kontos
- Art der Anmeldung und Anmeldevorgang
- IP-Adresse und Name des Client-Rechners

	Logons By Type
 Event IDs	Windows 2003 und älter 528-537, 539, 540 Windows Vista, Windows 2008 und später 4624, 4625

Ereignisse nach Schweregrad filtern

Aufgrund der hohen Anzahl von Ereignissen, die von Windows generiert werden, kann diese Funktion eine große Anzahl von Ereignissen aufzeichnen. Sie können die Option "Schweregrad" auf "Nur Prüfungsfehler" einstellen, um die Anzahl der von dieser Funktion erfassten Ereignisse zu reduzieren. Wenn Sie gesetzlich zur Erfassung dieser Daten verpflichtet sind, sollten Sie sich bei Ihrem Compliance Officer (und/oder Audit-Anforderungen) erkundigen, um sicherzustellen, dass Sie diese Einstellung ändern können und trotzdem konform bleiben.

Anmeldungen nach Computerkonten sammeln

Netzwerkanmeldungen durch Computerkonten können eine große Anzahl von Datensätzen in der Datenbank ausmachen und die Berichterstattung verwässern. Deaktivieren Sie das Kontrollkästchen, um alle Audit-Ereignisse zu ignorieren, die von Computer-Accounts stammen.

Zusätzlichen Hostnamen oder Reverse-Lookup über DNS durchführen

Wenn die im Anmeldeereignis enthaltene Anmelde-ID (gilt nur für Audit-Erfolgsereignisse) mit einer früheren Anmeldesitzung verknüpft (korreliert) werden kann, dann werden IP-Adresse und/oder Hostnamen inkludiert. Für den Fall, dass nur der Hostname oder die IP-Adresse verfügbar sind, wird ein DNS (Reverse) Lookup durchgeführt, um die fehlenden Informationen zu sammeln.

Da DNS-Daten, vor allem wenn DHCP IP-Adressen involviert sind, nicht immer 100% genau sind, sollte man sich nicht nur auf diese Daten verlassen.

Logon GUIDs

Erfasst die Anmelde-GUID, die bei einigen Anmeldeereignissen verfügbar ist, und nimmt sie in die Suchergebnisse auf. Die Erfassung von Anmelde-GUIDs ist im Allgemeinen nicht erforderlich, da sie für die forensische Analyse wenig Nutzen bringt, aber die Leistung des Collectors in Netzwerken, die in kurzer Zeit viele Anmelde-GUIDs erzeugen, erheblich beeinträchtigen kann.

5.6.5 Druckaufträge

Drucküberwachung zeichnet Druckaufträge in einer zentralen Datenbank auf und überwacht die Drucknutzung auf Workstations und Druckservern. Die gesammelten Informationen können über die Web-Reports abgefragt werden, um Informationen zu erhalten wie

- Wie viele Dokumente und/oder Seiten wurden auf einem bestimmten Drucker gedruckt
- Welche Dokumente wurden auf einem Drucker gedruckt?
- Kumulative Informationen wie z.B. wie viele Dokumente von jedem Benutzer gedruckt wurden

Anforderungen

Diese Funktion fängt Informationsereignisse ab, die in das Anwendungsereignisprotokoll geschrieben werden, wenn "Spooler-Informationsereignisse protokollieren" in den Druckserver-Eigenschaften des überwachten Hosts aktiviert ist. Daher müssen einige Voraussetzungen erfüllt sein, bevor die Druckverfolgung ordnungsgemäß funktionieren kann. Einzelheiten finden Sie unter Anforderungen.

Windows zeichnet Druckaktivitäten auf dem Host auf, auf dem sich die Druckerwarteschlange befindet. Daher funktioniert die Druckverfolgung am besten in Netzwerken, in denen Drucker auf Servern oder dedizierten Druckservern gemeinsam genutzt werden.

EventSentry kann auch Druckaktivitäten von Druckern verfolgen, die direkt an Arbeitsstationen angeschlossen sind. In diesem Szenario muss der EventSentry-Agent auf allen Computern installiert werden, an denen Drucker angeschlossen sind.

Gesammelte Daten

EventSentry wird die folgenden Druckinformationen auf allen unterstützten Windows-Plattformen sammeln:

Bereich	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit, wann der Druckauftrag eingereicht wurde
Druck-Server	Der Computer, auf dem sich die Druckerwarteschlange befindet, normalerweise der Druckserver
Druck-Warteschlange	Der Name des Druckers (Warteschlange)
Dokument	Der Name des gedruckten Dokuments
Dokument-ID	Die ID des gedruckten Dokuments, eine Nummer, die bei jedem neuen Druck um eins erhöht wird.

Benutzername	Der Name des Benutzers, der den Druckauftrag eingereicht hat
Seiten	Die Anzahl der gedruckten Seiten
Größe	die Gesamtgröße des Druckauftrags

Datenschutz

Da das Sammeln von Druckinformationen die Aktivitäten eines Benutzers bis zu einem gewissen Grad nachverfolgt, müssen Sie dennoch sicherstellen, dass das Sammeln dieser Informationen nicht die geltenden Unternehmensrichtlinien oder Gesetze beeinträchtigt oder verletzt.

Konfiguration

Tracking All print jobs (with exceptions)

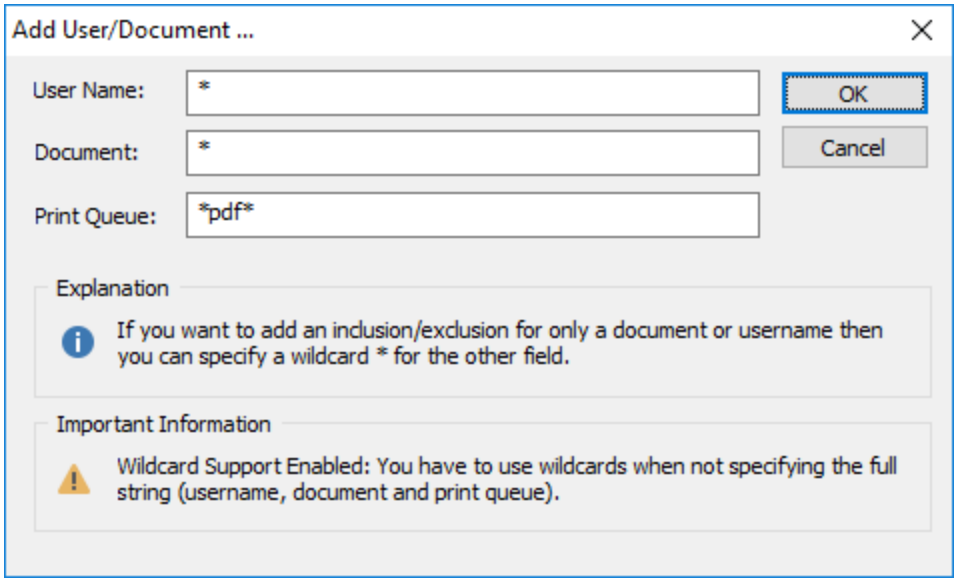
Wählen Sie "Alle außer den unten aufgeführten verfolgen", um alle Druckaufträge zu überwachen. Um bestimmte Benutzer und/oder Dokumente auszuschließen, klicken Sie auf die Schaltfläche "+" und geben Sie den auszuschließenden Benutzernamen oder das auszuschließende Dokument an.

Um ein Dokument von der Überwachung auszuschließen, geben Sie im Feld Dokument entweder den vollständigen Dokumentnamen oder einen Teil des Dokumentnamens ein (achten Sie darauf, * einzuschließen, wenn die Wildcard-Unterstützung aktiviert ist, z.B. *manual.doc). Geben Sie ein * für den Benutzernamen ein, wenn Sie dieses Dokument für alle Benutzer ausschließen möchten.

Um einen Benutzer von der Überwachung auszuschliessen, geben Sie entweder den vollständigen Benutzernamen (DOMAIN\Benutzer) oder einen Teil des Benutzernamens (z.B. *Benutzer1) ein. Geben Sie ein * für das Dokument ein, wenn Sie alle Dokumente dieses Benutzers ausschliessen möchten.

Tracking only selected print jobs

Wählen Sie "Only track listed below" und klicken Sie auf die Schaltfläche +, um Benutzer/Dokumente (siehe voriger Absatz) hinzuzufügen, die in die Liste aufgenommen werden sollen.



Aktivieren der Druckverfolgung im Betriebssystem

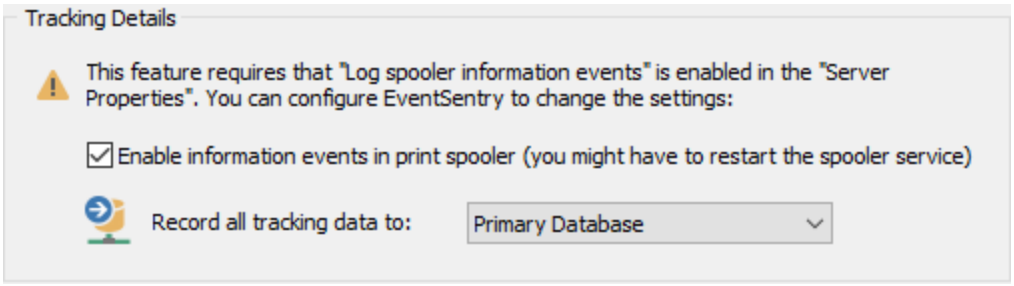
Da die Druckverfolgung im Betriebssystem aktiviert sein muss, können Sie den Agenten so konfigurieren, dass er automatisch aktiviert wird, wenn er nicht bereits aktiviert ist. Weitere Informationen finden Sie unter Anforderungen.

Database
Wählen Sie eine Datenbankaktion, in der die Anmeldedaten gespeichert werden sollen.

5.6.5.1 Anforderungen

Die Druckverfolgungsfunktion funktioniert durch das Abfangen von Informationsereignissen, die in das Anwendungsereignisprotokoll geschrieben werden, wenn in der *Druckserver-Eigenschaften* des überwachten Hosts die Option *Informationsereignisse des Protokollspoolers* aktiviert ist. Als solche bestehen die folgenden Anforderungen:

1. "Protokollspooler-Informationsereignisse" muss aktiviert sein. Sie können den EventSentry-Agenten automatisch die Druckverfolgung beim Start des Dienstes aktivieren lassen, indem Sie **"Enable information events in print spooler"** in den **Druckservereigenschaften** wählen.



2. So aktivieren Sie "Print Tracking / Auditing" ohne EventSentry:

   Windows 2003 und früher
   Navigieren Sie zu Start -> Einstellungen und klicken oder doppelklicken Sie auf das Symbol Drucker (und Faxgeräte). Wählen Sie "Servereigenschaften" aus dem Menü "Datei". Klicken Sie dort auf die Registerkarte "Erweitert" und kreuzen Sie das Kästchen neben "Log information spooler events" an. Möglicherweise müssen Sie den "Print Spooler"-Dienst neu starten.

   Windows Vista und höher (einschließlich Windows 2008)
   Öffnen Sie die "Ereignisanzeige" und navigieren Sie zu "Anwendungs- und Dienstprotokolle -> Microsoft -> Windows -> PrintService -> Betriebsbereit". Klicken Sie mit der rechten Maustaste auf "Protokoll Aktivieren", um die Protokollierung der Druckereignisse zu starten. Um die Protokollierung wieder zu deaktivieren, klicken Sie mit der rechten Maustaste auf "Betriebsbereit" und wählen Sie "Protokoll deaktivieren".

3. Das Anwendungs-Ereignisprotokoll "Protokollgröße" muss so konfiguriert werden, dass es "Ereignisse nach Bedarf überschreibt". Es wird außerdem empfohlen, eine Größe von mindestens 2048kb anzugeben. Der EventSentry-Agent schreibt beim Start eine Fehlermeldung in das Anwendungsereignisprotokoll, wenn das Ereignisprotokoll nicht korrekt konfiguriert ist.

   Sie können die Einstellungen für die "Log-Grösse" ändern, indem Sie die "Ereignisanzeige" öffnen (aus den Verwaltungstools) und mit der rechten Maustaste auf "Anwendungsprotokoll" klicken. Wählen Sie "Eigenschaften" aus dem Menü und vergewissern Sie sich, dass die "Protokollgröße" korrekt auf "Ereignisse nach Bedarf überschreiben" eingestellt ist. Vergewissern Sie sich auch, dass die "Maximale Protokollgröße" ausreichend groß ist.

5.6.6 Dateizugriffe

Dateizugriffsverfolgung sammelt alle **erfolgreichen** Dateizugriffsaktivitäten, die vom Betriebssystem protokolliert werden, wenn das Auditing für ein Verzeichnis und/oder eine Datei aktiviert ist. File Access Tracking umfasst:

- Dateien, die zu einem Verzeichnis hinzugefügt werden
- Dateien, die aus einem Verzeichnis gelöscht werden
- modifizierte Dateien
- andere Dateiänderungen wie z.B. Erlaubnis- oder Eigentumsänderungen

Darüber hinaus kann die Dateizugriffsverfolgung die folgenden Informationen über eine Dateiänderung enthalten:

- Der Benutzername des Benutzers, der die Aktion ausgeführt hat
- Der Computer und/oder die IP-Adresse, von dem/der die Aktion ausgeführt wurde (optional)
- Der Prozess, der die Aktion ausgeführt hat (es sei denn, sie wurde über eine Dateifreigabe ausgeführt)

Unter Datei-Überwachung vs. Dateizugriffsverfolgung finden Sie einen Vergleich zwischen Dateizugriffsverfolgung und Dateiüberwachung.

Die Dateizugriffsverfolgung funktioniert, indem Ereignis 560 (auf Computern mit Windows 2003 und früher) oder Ereignis 4663 (auf Computern mit Vista und später) überwacht und normalisiert wird und zusätzliche Aktionen durchgeführt werden, um erweiterte Informationen über die Ereignisse zu erhalten (z. B. den Quellcomputer) und die Dateizugriffsaktion zu kategorisieren.

Verwendung der Dateizugriffsverfolgung unter Windows 2003 und früher

Ein Problem mit den 560 Sicherheitsereignissen unter Windows 2003 und früher ist, dass sie nicht nur protokolliert werden, wenn Änderungen an Dateien vorgenommen werden, sondern auch, wenn Änderungen an Dateien angefordert werden. Microsoft® hat mit Windows 2003 so genannte Betriebsereignisse (Ereignis-ID 567) eingeführt, die versuchen, dieses Problem zu lösen, indem sie nur tatsächliche Dateiänderungen im Sicherheitsereignisprotokoll protokollieren. Wir haben jedoch festgestellt, dass die Betriebsereignisse unter Windows 2003 etwas unzuverlässig sind, insbesondere wenn auf Dateien über eine Dateifreigabe über ein Netzwerk zugegriffen wird. Wir haben dieses Problem in unserem Ereignisprotokoll-Blog ausführlich diskutiert. Daher wird die Funktion zur Verfolgung des Dateizugriffs die 567 Ereignisse unter Windows 2003 und früher nicht nutzen, sie werden jedoch unter Vista, Windows Server 2008 und später genutzt.

Um diese Einschränkung auszugleichen, kann EventSentry bestimmte Dateiaktionen manuell verifizieren, indem es eine zusätzliche Verifizierung der Dateien durchführt, wie z.B. die Erstellung von Prüfsummen bei der Änderung von Dateien, oder die Überprüfung ob Dateien tatsächlich gelöscht wurden. Diese Funktion heißt **Verify**, ist optional und kann aktiviert werden, wenn Sie den Dateizugriff auf Hosts mit Windows Server 2003 (und früher) überwachen.

Verwendung der Dateizugriffsverfolgung unter Vista, Windows Server 2008 und höher

Wenn Sie den Dateizugriff auf Windows Server 2008 und höher überwachen (dies schließt Dateien ein, auf die von Computern über Dateifreigaben zugegriffen wird), dann fängt EventSentry"Operation Events" ab und normalisiert sie, wodurch die zusätzliche Verarbeitung durch die Verifizierungsfunktion (wie oben beschrieben) in den meisten Szenarien unnötig wird.

5.6.6.1 Voraussetzungen

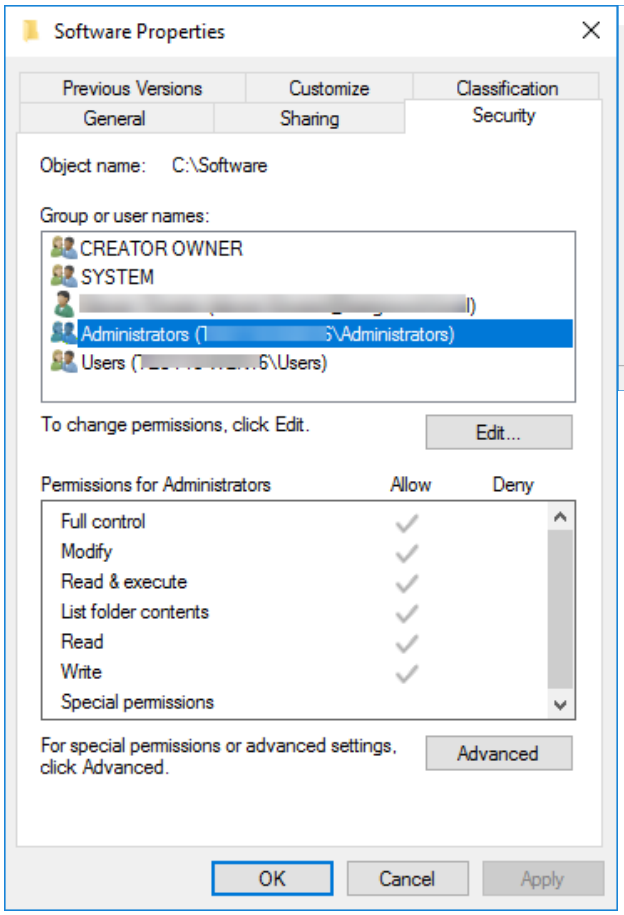
Um die Dateizugriffsverfolgung verwenden zu können, muss das Auditing für die Dateien und/oder Ordner konfiguriert werden, die Sie mit EventSentry verfolgen würden. Zusätzlich muss die Objektverfolgung entweder durch die Gruppenrichtlinie oder durch die lokale Sicherheitsrichtlinie aktiviert werden.

1. Objektverfolgung aktivieren

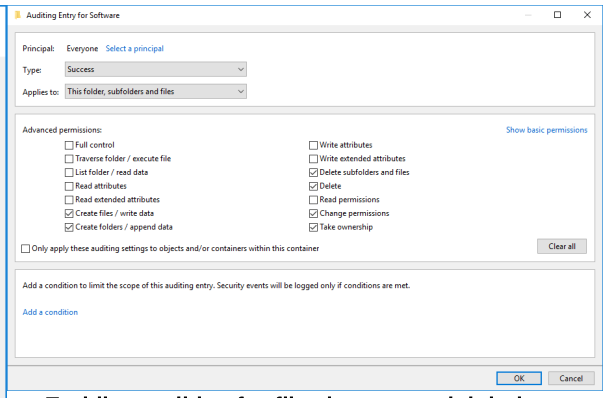
Weitere Informationen darüber, wie Sie die Audit-Kategorie für die Objektverfolgung aktivieren können, finden Sie unter Verfolgungsanforderungen. Wenn die Objektverfolgung nicht aktiviert ist, werden die erforderlichen 560 oder 4663 Ereignisse nicht vom Betriebssystem erzeugt, selbst wenn die Überwachung eines Verzeichnisses aktiviert ist.

2. Auditing für eine Datei und/oder einen Ordner aktivieren

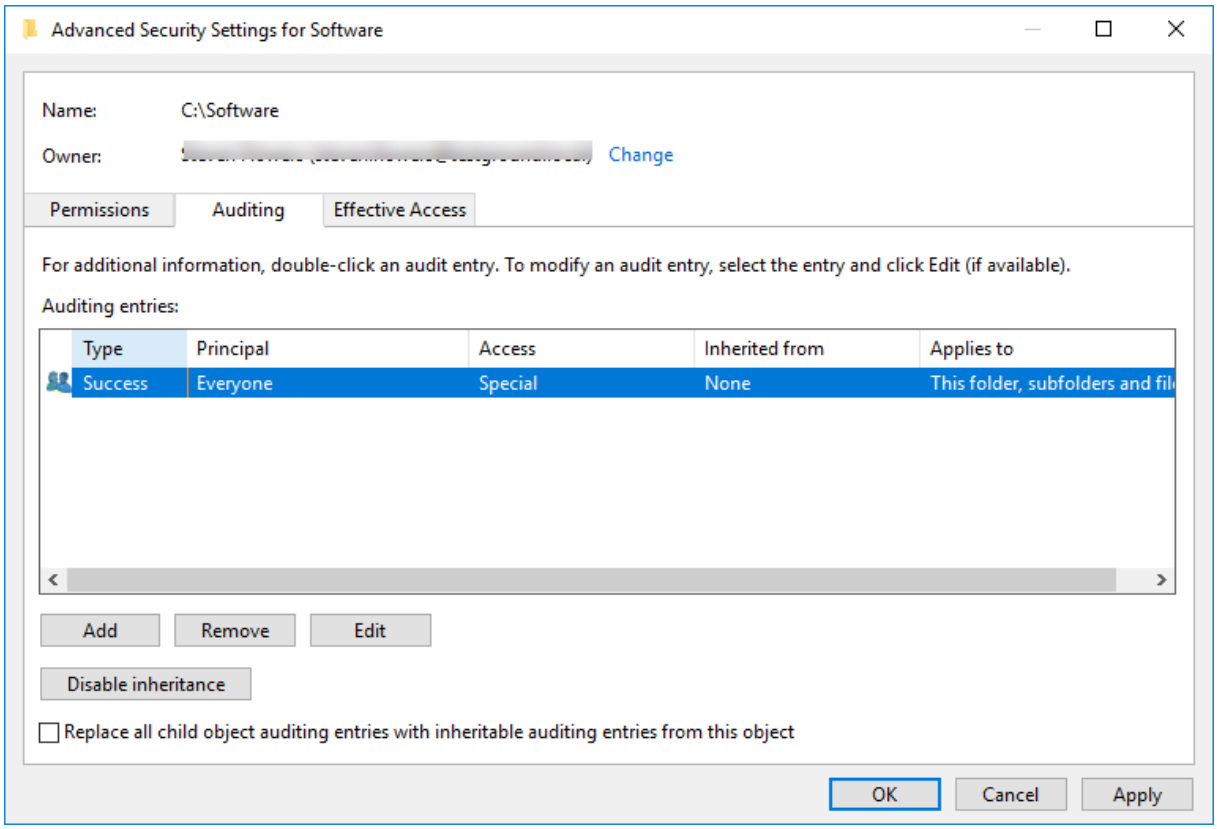
Sobald die Objektzugriffsverfolgung aktiviert wurde, müssen Sie das Auditing für die Verzeichnisse konfigurieren, die Sie mit EventSentry überwachen möchten. Sie konfigurieren die Überwachung, indem Sie auf die Ordnereigenschaften im Windows-Explorer zugreifen und auf die erweiterten Sicherheitseigenschaften zugreifen, wie in den folgenden Screenshots gezeigt:



Viewing current file/folder permissions



Enabling auditing for file changes and deletions



List of auditing entries after EVERYONE was added

Die detaillierten Schritte zur Ermöglichung von Audits sind wie folgt:

1. Klicken Sie mit der rechten Maustaste auf den Ordner, in dem Sie die Prüfung aktivieren möchten, und wählen Sie "Eigenschaften".
2. Klicken Sie auf die Registerkarte "Sicherheit".
3. Wählen Sie die Schaltfläche "Erweitert".
4. Wählen Sie die Registerkarte "Überwachung".
5. Klicken Sie auf "Bearbeiten".
6. Klicken Sie auf "Hinzufügen".
7. Geben Sie im Auswahldialog den/die Benutzer und/oder die Gruppe(n) an, die Sie auditieren möchten. Um alle zu auditieren, wählen Sie **Everyone**
8. Geben Sie im Dialog "Eintrag prüfen" die Art des Zugriffs an, den Sie prüfen möchten, z.B. "Ändern".
9. Klicken Sie mehrmals auf OK, um Ihre Auswahl zu bestätigen.

Auditing-Einträge sind sofort wirksam.

5.6.6.2 Einrichten der Dateizugriffsverfolgung

Sobald das Auditing auf einem oder mehreren Verzeichnissen konfiguriert wurde, können Sie sich entweder dafür entscheiden, ein oder mehrere bestimmte Verzeichnisse mit EventSentry zu überwachen oder einfach alle Dateizugriffsverfolgungsereignisse abzufangen und zu normalisieren.

Ereignis-Analyse

Wenn Sie eine Dateizugriffsverfolgung einrichten, müssen Sie festlegen, wie Sie Ereignisse analysieren möchten. Sie können entweder Ereignisse **normalisieren**, **normalisieren & verifizieren** oder Ereignisse **normalisieren, verifizieren & filtern**.

Normalisieren ("Normalize Only")
Dies ist die am wenigsten ressourcenintensive Option, bei der Objektverfolgungsereignisse abgefangen, normalisiert und in die EventSentry-Datenbank geschrieben werden. Bei der Einstellung dieser Option wird keine zusätzliche Überprüfung der Dateien durchgeführt, auf die zugegriffen wird. Dies ist die einzige Option, die bei Verwendung der **Aktivität Alle Dateizugriffe verfolgen** verfügbar ist.

Nur normalisieren ist die empfohlene Einstellung für Computer mit Vista und höher, da diese Computer bereits "Operational Events" erzeugen.

Normalisieren & Verifizieren ("Normalize & Verify")
Diese Option führt neben der einfachen Normalisierung von Ereignissen, wie oben beschrieben, auch zusätzliche Überprüfungen der Dateien durch, auf die zugegriffen wird. Diese Option erfordert mehr Ressourcen, da sie für jede Datei in den überwachten Verzeichnissen sowie für jede Datei, welche geschrieben wird, eine Prüfsumme erstellt.

Verifizieren versucht die meisten Dateiänderungen zu ermitteln:

1. Der Schreibzugriff auf Dateien wird anhand der SHA-Prüfsummen der Dateien überprüft
2. Datei-Löschungen werden überprüft, indem die Nicht-Existenz der Dateien überprüft wird.
3. Hinzugefügte Dateien werden überprüft

Wenn eine Aktion verifiziert werden kann, dann wird das Ereignis als "verifiziert" gekennzeichnet.

Die Option **Verifizieren** ist nur verfügbar wenn Sie ein oder mehrere Verzeichnisse angeben, da der Agent jedes überwachte Verzeichnis initialisieren muss.

Normalisieren, Verifizieren & Filtern ("Normalize, Verify & Filter")
Diese Auswahl ist identisch mit der Einstellung **Normalisieren & Verifizieren**, außer dass nur Dateiänderungen, die (z.B. durch eine Prüfsumme) verifiziert wurden, in der Datenbank protokolliert werden. Wenn eine Aktion nicht verifiziert werden kann, dann wird das Ereignis verworfen.

Diese Option wird für sicherheitsempfindliche Umgebungen nicht empfohlen, da wichtige Ereignisse ignoriert werden könnten, wenn eine Aktion nicht richtig bestimmt werden kann.

Tracking-Verzeichnisse

Sie können entweder alle Dateizugriffsaktivitäten verfolgen oder ein oder mehrere Verzeichnisse angeben, die überwacht werden sollen.

Tracking all file access activity
Wählen Sie diese Option, um alle Objektverfolgungsereignisse zu verfolgen, die auf einem System erzeugt werden. Wenn Sie diese Option wählen, wird die **Ereignisanalyse** automatisch auf **Nur normalisieren** gesetzt.

Monitoring one or more directories
Fügen Sie ein oder mehrere Verzeichnisse zu der Liste hinzu, um nur Dateizugriffsereignisse aus ausgewählten Verzeichnissen zu verfolgen. Sie müssen diese Option auch auswählen, um die Option "Normalisieren & Verifizieren" oder "Normalisieren, Verifizieren & Filtern" zu verwenden. Klicken Sie auf das Plus-Symbol, um ein Verzeichnis zur Liste der überwachten Verzeichnisse hinzuzufügen. Die

Überwachung eines UNC-Pfades oder einer Netzwerkfreigabe (wie \\SERVER1\Payroll) wird **nicht unterstützt**.

Zusätzlich können Sie konfigurieren, welche Zugriffsmasken aufgezeichnet werden sollen (z.B. nur *WriteData* oder *Delete*) und auch einen Dateifilter angeben, der nur bestimmte Dateien einschließt oder Dateien ausschließt, die nicht nachverfolgt werden sollen. Siehe Zugriffsmasken & Filter für weitere Informationen.

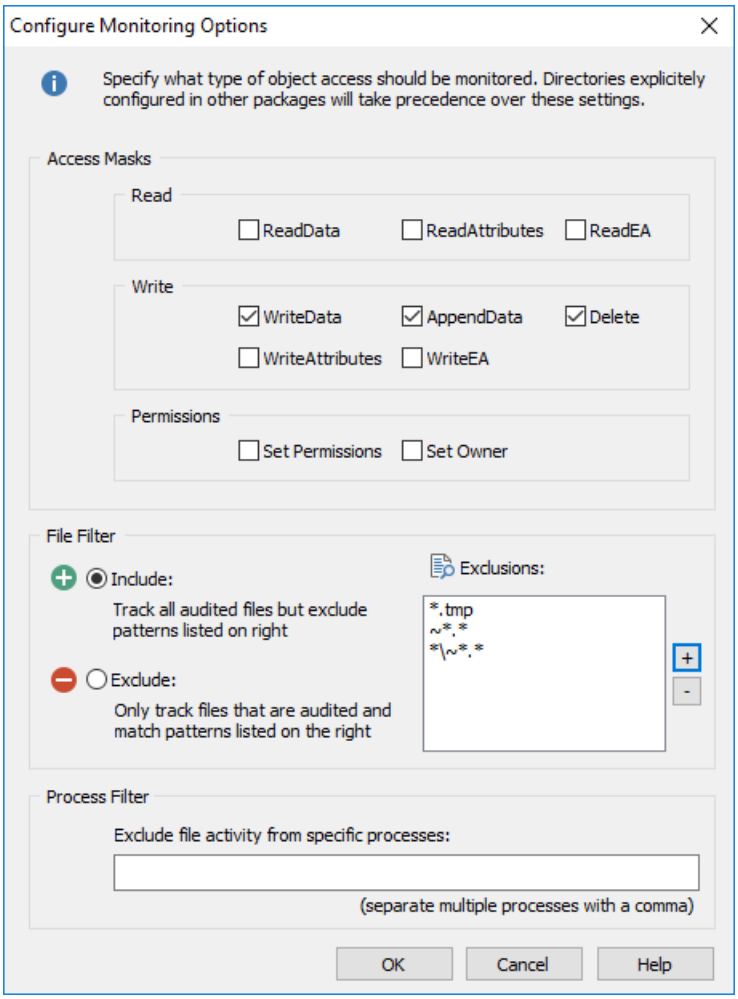
Retrieve Source IP address and Computer Name

Wenn die im Ereignis zur Verfolgung des Dateizugriffs enthaltene Anmelde-ID mit einer früheren Anmeldesitzung verknüpft (korreliert) werden kann, dann enthält EventSentry die IP-Adresse und/oder den Hostnamen. Für den Fall, dass nur der Hostname oder die IP-Adresse verfügbar sind, wird ein DNS (Reverse) Lookup versucht um die fehlenden Informationen zu sammeln.

Da DNS-Daten, vor allem wenn DHCP IP-Adressen involviert sind, nicht immer 100% genau sind, sollte man sich nicht nur auf diese Daten verlassen.

5.6.6.3 Berechtigungen & Filter

Sie können angeben, welche Arten des Dateizugriffs verfolgt werden um sicherzustellen, dass nur relevante Ereignisse in der Datenbank aufgezeichnet werden. Zusätzlich können Sie Dateifilter einrichten, um Dateien, die einem Muster entsprechen, ein- oder auszuschließen.



Zugangsmasken

Windows unterscheidet bei der Aufzeichnung von Dateizugriffsaktivitäten - entweder durch normale oder "Operational Events" - zwischen den folgenden Zugriffsmasken:

- ReadData
- ReadAttributes
- ReadEA
- SetPermissions
- SetOwner
- WriteData
- WriteAttributes
- WriteEA
- AppendData
- Delete

Um beispielsweise zu verfolgen, wenn Benutzer Dateien ändern, stellen Sie sicher, dass **WriteData** und **AppendData** beide ausgewählt sind. Um zu verfolgen, wann Dateien gelöscht werden, stellen Sie sicher, dass **Delete** markiert ist.

File Filter

Der Standardfilter ("Include") schließt alle Dateien ein, aber Sie können Exklusionen von Fall zu Fall festlegen. Sie könnten z.B. alle Dateien mit der Erweiterung **tmp** exkludieren indem Sie den folgenden Filter angeben:

***.tmp**

Dateinamen und Pfade müssen relativ zum überwachten Ordner angegeben werden. Wenn Sie z.B. den Ordner **C:\Logfiles** überwachen, aber jede Datei im Unterverzeichnis **Temp** (C:\Logfiles\Temp) filtern möchten, dann müssten Sie den Filter als **Temp*.*** angeben.

Prozessfilter

Dateiaktivitäten, die durch bestimmte Prozesse ausgelöst werden, können von der Verfolgung mit dem Prozessfilter ausgeschlossen werden. Geben Sie entweder den vollständigen Pfad zum Prozess an oder verwenden Sie z.B. ein Platzhalterzeichen:

```
*filescanner.exe

C:\Program Files\FileScannerSoftware\filescanner.exe
```

Mehrere Prozesse können mit Kommas getrennt werden.

Das Ausschließen eines Prozesses funktioniert nur, wenn der betreffende Prozess direkt auf die Dateien zugreift (und nicht über eine Netzwerkfreigabe) und auf den 4663 Ereignissen aufgeführt ist. Prozesse, die auf Clients laufen, welche wiederum auf entfernte Dateien zugreifen, können nicht exkludiert werden.

5.6.7 Benutzerkonten

Die Benutzerkontenüberwachung fängt Ereignisse im Zusammenhang mit der Erstellung, Änderung und Löschung von Benutzerkonten, Gruppen und Computerkonten ab. Je nach Art des Computers, auf dem diese Funktion verwendet wird, werden entweder lokale oder Domänenkonten überwatcht.

Benutzerkontenverwaltung

Anlegen und Löschen von Benutzern
Verfolgt, wann Benutzerkonten erstellt oder gelöscht werden.

Änderungen an Benutzerkonten
Verfolgt, wenn Benutzerkonten geändert werden, z.B. wenn ein Passwort gesetzt wird.

Änderungen des Benutzerstatus
Verfolgt Änderungen des Benutzerstatus, z.B. wenn ein Benutzerkonto deaktiviert oder aktiviert wird.


Event IDs

User Account Management

Windows 2003 und älter
624, 626, 628, 629, 630, 642, 644, 671

Windows Vista, Windows 2008 und später
4720, 4722, 4724, 4725, 4726, 4738, 4740, 4767

Gruppenkontenverwaltung

Hinzufügen und Löschen von Gruppen
Überwacht die Erstellung und das Löschen von Gruppen.

Änderungen von Gruppen
Überwacht wenn Gruppen geändert werden, z.B. wenn eine globale Gruppe in eine universelle Gruppe geändert wird.

Änderungen der Gruppenmitgliedschaft
Überwacht die Änderungen in der Gruppenzugehörigkeit, z.B. wenn Mitglieder zu einer Gruppe hinzugefügt oder aus einer Gruppe entfernt werden.

Sicherheitsfähige Gruppen, Verteilergruppen
Konfiguriert welche Arten von Gruppen überwacht werden sollen.

Computerkontenverwaltung

Erstellung und Löschung von Computerkonten
Verfolgt, wann Computerkonten hinzugefügt oder gelöscht werden.

Änderungen an Computerkonten
Verfolgt Änderungen an Computerkonten, z. B. wenn das Kennwort eines Computerkontos geändert wird.

Hinweis: Änderungen von Computerkonten treten nur auf Domänencontrollern auf.

Quell-IP-Adresse und Computername abrufen

Wenn die im Kontoverwaltungsereignis enthaltene Anmelde-ID mit einer früheren Anmeldesitzung verknüpft (korreliert) werden kann, dann enthält EventSentry die IP-Adresse und/oder den Hostnamen. Für den Fall, dass nur der Hostname oder die IP-Adresse verfügbar ist, wird ein DNS (Reverse) Lookup durchgeführt, um die fehlenden Informationen zu ermitteln.

Da DNS-Daten, vor allem wenn DHCP IP-Adressen involviert sind, nicht immer 100% genau sind, sollte man sich nicht nur auf diese Daten verlassen.

5.6.8 Richtlinienänderungen

Fragt kontinuierlich die aktuelle Audit-Politik ab, so dass der aktuelle Audit-Status jedes überwachten Systems in den Web Reports verfügbar ist. Policy Change Tracking fängt auch verschiedene Ereignisse im Zusammenhang mit Policy-Änderungen ab, wie z.B. die Änderung einer Domain-Passwort-Policy oder die Zuweisung eines Benutzerrechts.

Richtlinienänderungen
Verfolgt alle Richtlinienänderungen, einschließlich

- Änderungen der Domänenrichtlinien (z. B. Änderungen der Passwortrichtlinien)
- Änderungen der Überwachungsrichtlinien
- Änderungen der Kerberosrichtlinien


Event IDs

Policy Changes

Windows 2003 und älter
612, 617, 643

Windows Vista, Windows 2008 und später
4719, 4713, 4739

Benutzerrechte
Überwacht wenn Benutzerrechte an Benutzerkonten zugewiesen oder von Benutzerkonten entfernt werden, z.B. das Recht "Auslagerungsdatei erstellen".


Event IDs

User Rights Changes

Windows 2003 und älter
608, 609

Windows Vista, Windows 2008 und später
4704, 4705

Anmelderechte
Überwacht wenn Anmelderechte gewährt oder aus Benutzerkonten entfernt werden, z.Bsp. "Logon as a service".

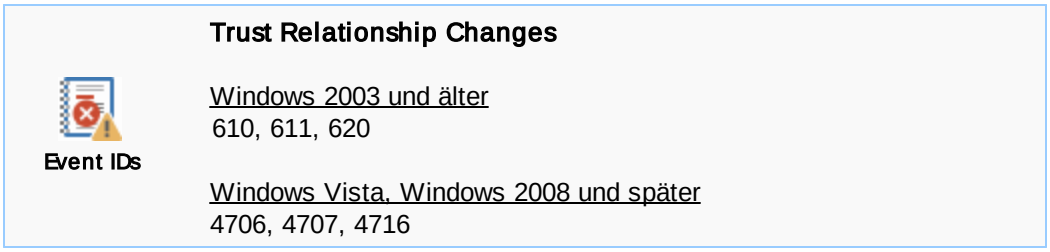

Event IDs

Logon Rights Changes

Windows 2003 und älter
621, 622

Windows Vista, Windows 2008 und später
4717, 4718

Vertrauensbeziehungen
Überwatcht alle Änderungen an Vertrauensbeziehungen, einschließlich der Erstellung, Änderung und Entfernung von Vertrauensbeziehungen.



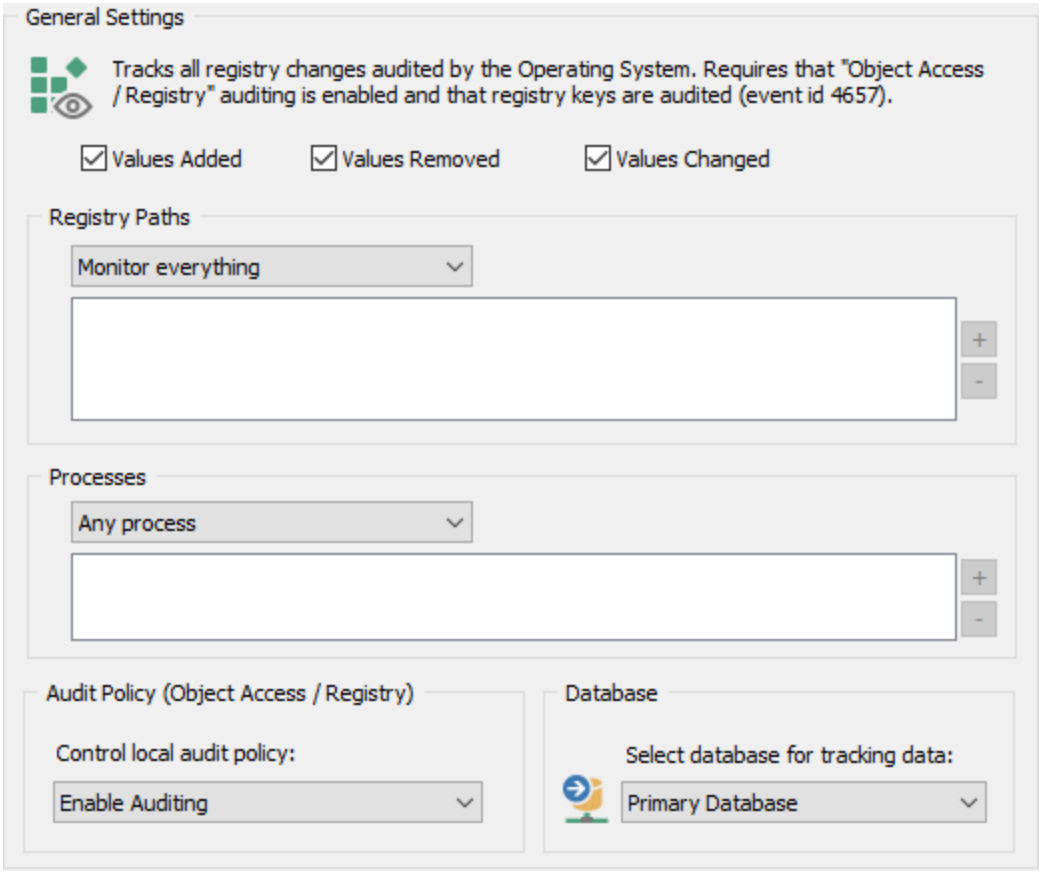
Quell-IP-Adresse und Computername abrufen

Wenn die im Kontoverwaltungsereignis enthaltene Anmelde-ID mit einer früheren Anmeldesitzung verknüpft (korreliert) werden kann, dann enthält EventSentry die IP-Adresse und/oder den Hostnamen. Für den Fall, dass nur der Hostname oder die IP-Adresse verfügbar ist, wird ein DNS (Reverse) Lookup durchgeführt, um die fehlenden Informationen zu ermitteln.

Da DNS-Daten, vor allem wenn DHCP IP-Adressen involviert sind, nicht immer 100% genau sind, sollte man sich nicht nur auf diese Daten verlassen.

5.6.9 Registrierung / Registry

Fängt von Windows generierte Audit-Ereignisse ab und stellt sie in Web Reports zur Verfügung.



Anforderungen: Diese Funktion funktioniert durch Abfangen von Audit-Erfolgsereignissen mit der Ereignis-ID 4657, die in das Sicherheitsereignisprotokoll geschrieben werden, wenn die Überprüfung der Registrierung aktiviert ist (entweder in der lokalen Sicherheitsrichtlinie oder über AD) und mindestens ein Registrierungsschlüssel für die Überprüfung konfiguriert ist. Siehe Anforderungen für Einzelheiten.

Gesammelte Daten

Die folgenden Registrierungsdaten werden auf allen unterstützten Windows-Plattformen gesammelt:

Bereich	Beschreibung
Aktion	Hinzugefügt, entfernt oder modifiziert
Register-Pfad	Pfad des Werts, der hinzugefügt, entfernt oder geändert wurde, starten immer mit \REGISTRY\
Registrierungswert Name	Name des Registrierungswerts, der hinzugefügt, entfernt oder geändert wurde
Wert vorher	Wert vor der Änderung
Wert nach	Wert nach der Änderung
Typ Vorher	Typ des Wertes vor der Änderung
Eingeben nach	Typ des Wertes nach der Änderung
Anruferpfad/Datei	Prozesse, die die Änderung eingeleitet haben, für Änderungen, die entfernt eingeleitet wurden, ignorieren
Benutzername	Benutzer, der die Änderung initiiert hat
Anmelde-ID	Anmelde-ID der Sitzung, die die Änderung vorgenommen hat
Ereignis #	Ereignisnummer des Ereignisses, das die Änderung beschreibt

Konfiguration

Allgemeiner Filter

Bestimmt, welche Registrierungsaktivität verarbeitet wird.

Register-Pfade

Konfigurieren Sie, ob alle Registrierungsänderungen, die vom Betriebssystem geprüft werden, verarbeitet werden (alles überwachen), ob bestimmte Pfade exkludiert werden sollen ("unten aufgeführte Pfade ausschließen") oder ob nur ausgewählte Pfade überwacht werden sollen ("nur unten aufgeführte Pfade überwachen").

Registry-Pfadfilter müssen mit dem Format übereinstimmen, das im Ereignis 4657 verwendet wird, und in der Regel z.B. mit \REGISTRY\ beginnen:

```
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
\REGISTRY\USER\S-1-5-21-2574282233-618468577-1958264051-
1122\Software\Microsoft\Windows\CurrentVersion\Run
```

Im Zweifelsfall ist dem Registrierungspfad ein Sternchen voranzustellen, z.B.
`*\Software\Microsoft\Windows\CurrentVersion\Run`

Unterordner werden automatisch mitüberwacht.

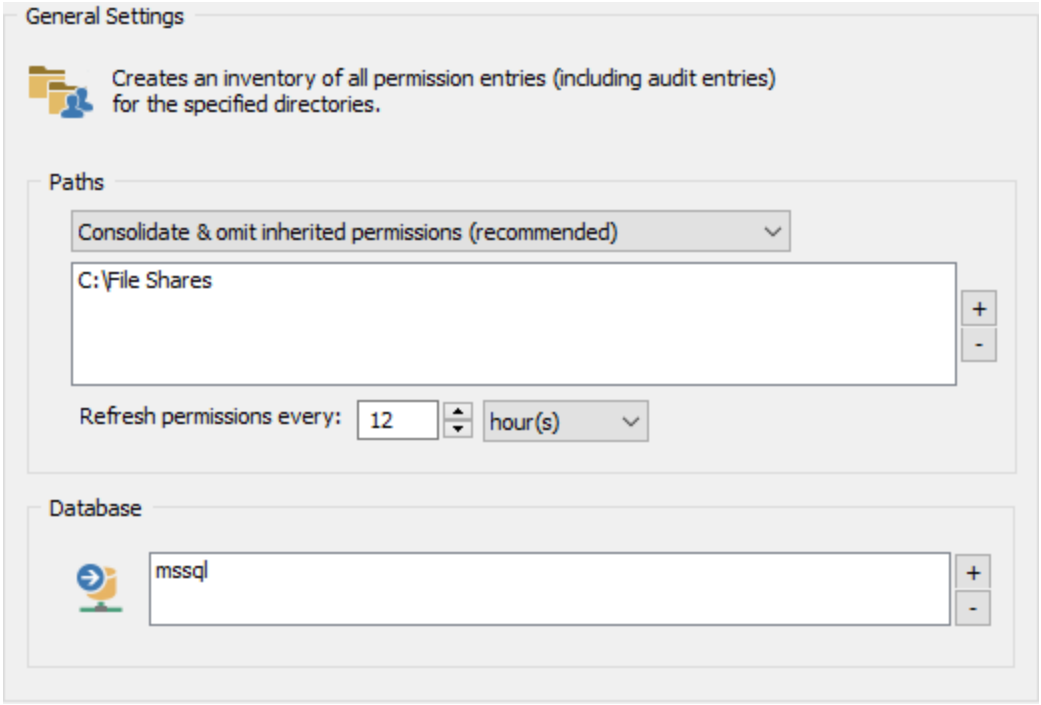
Prozesse

Konfigurieren Sie, ob die Registrierungsaktivität aller Prozesse verarbeitet werden soll ("Jeder Prozess"), ob bestimmte Prozesse ausgeschlossen werden sollen ("Ausschließen der unten aufgeführten Prozesse") oder ob nur bestimmte Prozesse überwacht werden sollen ("Nur die unten aufgeführten Prozesse überwachen").

5.6.10 Zugriffsinventar

Die Berechtigungsinventur listet die Berechtigungen ausgewählter Ordner auf und stellt die Berechtigungsdaten (ACL, ACE) in den Webberichten zur Verfügung. Wie bei allen anderen Funktionen, die auf Ordner verweisen, müssen die Ordner relativ zum überwachten Host mit lokalen Pfaden referenziert werden. UNC-Pfade werden nicht empfohlen, da das Konto, unter dem der Agent läuft, im Allgemeinen keinen ausreichenden Zugriff auf Remote-Hosts hat.

Um die Berechtigungen für mehrere Ordner auf mehreren Rechnern zu inventarisieren, müssen einzelne Pakete erstellt werden, die entsprechend zugewiesen werden müssen. Die Berechtigungsinventarisierungsfunktion kann mit den folgenden Konfigurationsoptionen angepasst werden.



Anforderungen: Das **LocalSystem**-Konto benötigt mindestens **LESE/READ**-Zugriff auf die angegebenen Dateien und Ordner, um auf die Dateien zugreifen und die Berechtigungen auflisten zu können.

Inventar-Typ

Vererbte Berechtigungen konsolidieren und weglassen

Obwohl für jede Datei in NTFS individuelle Berechtigungen festgelegt sind, werden die Berechtigungen im Allgemeinen für die große Mehrheit der Dateien vererbt. Wenn Sie den Inventartyp auf diese Option einstellen, werden nur Berechtigungseinträge aufgezeichnet, die von den Berechtigungen des übergeordneten Ordners abweichen, wodurch die Anzahl der in der Datenbank gespeicherten Daten erheblich reduziert wird. Dies ist die empfohlene Option, insbesondere für Verzeichnisse mit einer großen Anzahl von Dateien.

Inventarisierung aller Dateien und Verzeichnisse

Zeichnet die Berechtigungseinträge von jeder Datei auf, auch wenn der Berechtigungseintrag mit dem des übergeordneten Ordners identisch ist. Diese Option wird nur für Verzeichnisse empfohlen, die eine geringe Anzahl von Dateien enthalten, oder wenn die Standardoption (siehe oben) nicht die gewünschten Ergebnisse liefert.

Intervall aktualisieren
Legt fest, wie oft die Berechtigungen aller Dateien in den ausgewählten Ordnern aktualisiert werden, standardmäßig 12 Stunden. Da bei einem erneuten Scan jede einzelne Datei überprüft werden muss, wird für Verzeichnisse mit einer großen Anzahl von Dateien ein höheres Intervall empfohlen.

Datenbank
Legt Sie fest, in welcher(n) Datenbank(en) die Daten des Berechtigungsinventars gespeichert werden sollen.

5.7 Validierungs-Skripte

Pakete mit Validierungsskripten verwenden Skripte (vom Typ Validierung) um zu überprüfen, ob die Betriebssystemkonfiguration in Bezug auf Sicherheit und Verfügbarkeit den Best Practices entspricht und/oder Sicherheits- und Compliance-Anforderungen enspricht.

EventSentry enthält 100+ Skripte (Checks), die von NETIKUS.NET ltd (alias "Managed Scripts") gewartet und aktualisiert werden und die zur Durchführung einer Vielzahl von Prüfungen verwendet werden können:

- STIG
- CMMC
- CIS
- NIAP
- MITRE
- NIST 800-53
- CCE
- General System Health
- Bewährte Praktiken

Verwaltete Skripte werden regelmäßig gewartet und aktualisiert, Aktualisierungen stehen Evaluationsanwendern und Kunden mit aktiven Wartungsverträgen zur Verfügung. Benutzer können die verwalteten Skripte durch ihre eigenen ergänzen, beachten Sie aber, dass verwaltete Skripte nicht modifiziert werden können.

Die Skripte werden mit Hilfe von Tags organisiert, und Benutzer können die eingebauten Tags mit ihren eigenen ergänzen, um die Zuweisung von Skripten zu erleichtern.

Konfiguration

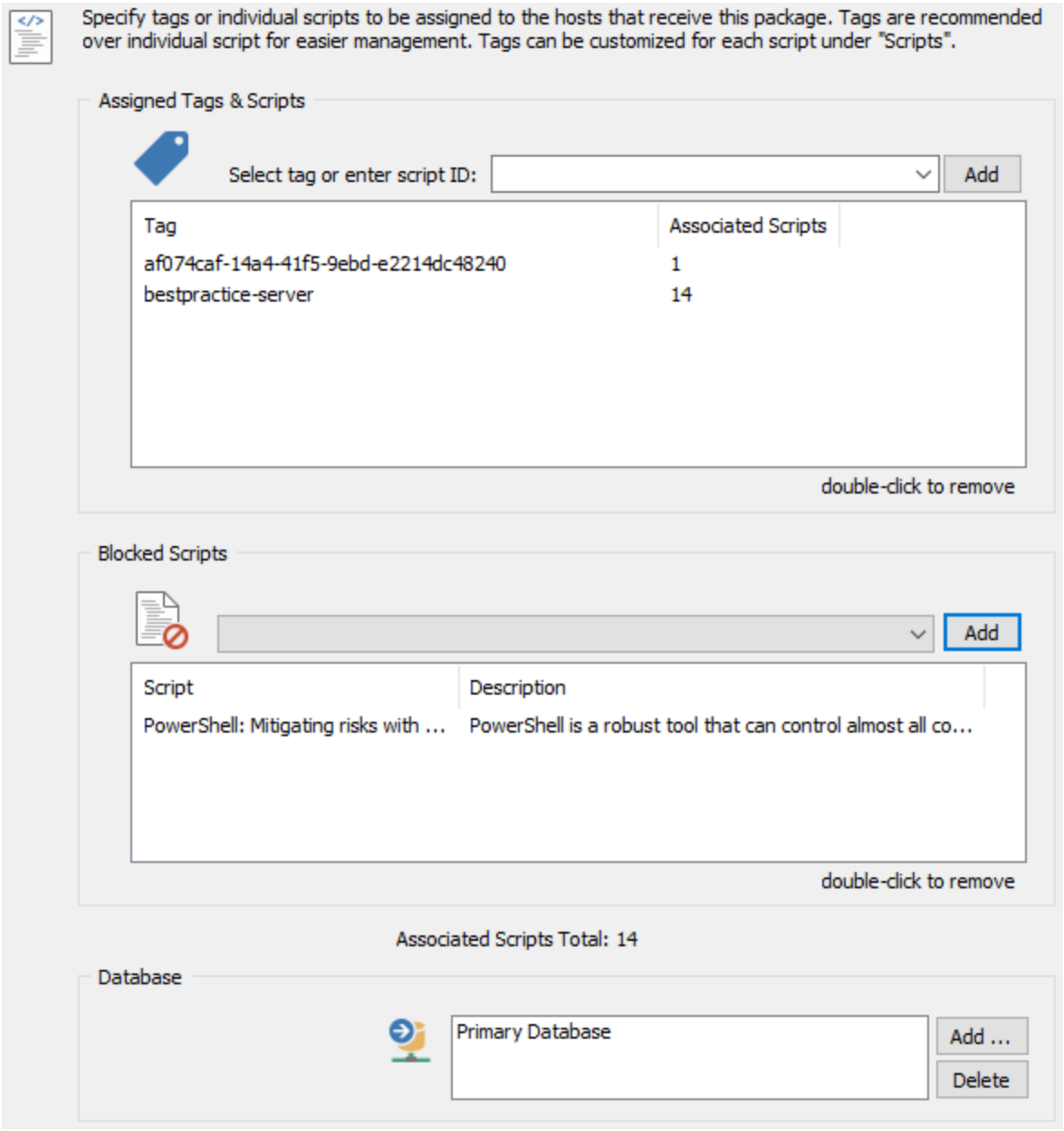
Assigned Tags & Scripts
Ein Validierungsskript-Paket ermöglicht es Benutzern, vorhandene Validierungsskripte entweder durch ein passendes Tag oder eine Skript-GUID zu verknüpfen, die auf allen Hosts ausgeführt werden, denen das Paket zugeordnet ist. Ergebnisse können in einer oder mehreren Datenbankaktionen gespeichert werden.

Blocked Scripts
Wenn ein oder mehrere Skripte trotz Übereinstimmung mit den angegebenen Tags nicht im Paket enthalten sein sollten, kann es im Abschnitt "Blockierte Skripte" blockiert werden. Dies kann bei

Prüfungen hilfreich sein die nicht behoben werden können oder die nicht auf die betroffenen Hosts anwendbar sind.

Ergebnisse von Validierungsskripten sind in den Web Reports verfügbar, Ereignisse im Ereignisprotokoll werden nicht erzeugt. Die Web Reports bieten zusammenfassende Statistiken, einzelne Skriptergebnisse und Korrekturschritte für fehlgeschlagene Checks.

Skripte können im Abschnitt Skripte deaktiviert werden, um zu verhindern, dass sie unabhängig von Tag-Zuweisungen überall ausgeführt werden. Die Häufigkeit, mit der Skripte ausgeführt werden, wird ebenfalls im Abschnitt Skripte konfiguriert.



5.8 Überwachung mit Sensoren

EventSentry kann Temperatur, Feuchtigkeit, Bewegung, Rauch und Wasser über externe Sensoren überwachen, die an den seriellen Anschluss angeschlossen sind. Die Hardwaresensoren sind separat erhältlich und können entweder über https://store.netikus.net (wenn Sie sich in den USA befinden) oder direkt von PCMeasure in Deutschland bezogen werden, wenn Sie sich außerhalb der USA befinden.

Die folgenden Funktionen sind verfügbar und werden über **Environment** der Management Konsole konfiguriert. Alle von der Umgebungsüberwachungsfunktion erzeugten Alerts werden in das Ereignisprotokoll der Anwendung geschrieben.

EventSentry unterstützt derzeit nur Sensoren von PCMeasure, und einige der unterstützten Sensoren erfordern zusätzliche Hardware. Die nachstehende Tabelle gibt einen Überblick über die Anforderungen:

Sensor-Beschreibung	Hersteller Modell-Nummer	Anschlüsse an Sensor	Erfordert USB-Anschluss	Erfordert serielle Schnittstelle	Benötigt Adapter (RJ-45 bis seriell)	Erfordert Treibersoftware (im Lieferumfang enthalten)
Temperatur / Luftfeuchtigkeit (serieller Anschluss)	30106	9-polig seriell, USB	ja, für Strom	ja	nein	nein
Temperatur / Luftfeuchtigkeit (USB)	30602	USB	ja	nein	nein	ja
Temperatur	30101	RJ-45	ja, für Strom	ja	ja	nein
Luftfeuchtigkeit	30103	RJ-45	ja, für Strom	ja	ja	nein
Wasser	30115	RJ-45	ja, für Strom	ja	ja	nein
Rauch	30111	RJ-45	ja, für Strom	ja	ja	nein
Bewegung	30114	RJ-45	ja, für Strom	ja	ja	nein

Bei allen Sensoren/Adaptern **mit Ausnahme des Sensors 30602** werden die USB-Anschlüsse **nur zur Stromaufnahme verwendet**. Daten von den Sensoren werden über den seriellen Anschluss übertragen. Um die Sensoren verwenden zu können, müssen Sie sowohl den USB- als auch den seriellen Anschluss anschließen.

Für Sensoren, die Adapter benötigen (siehe rechte Spalte "Erfordert Adapter"), gibt es die folgenden seriellen Adapter. Jeder Adapter als **ein 9-poliger serieller und ein USB-Port**, sowie **ein oder mehrere RJ-45-Stecker** zum Anschluss der eigentlichen Sensoren.

Beschreibung des Adapters	Hersteller Modell-Nummer	Anzahl von RJ-45 Verbinder
Serieller 1-Port-Adapter	30201	1
Serieller Adapter mit 2 Anschlüssen	30203	2
Serieller Adapter mit 4 Anschlüssen	30205	4

An den seriellen Adaptern angeschlossene Sensoren müssen eindeutig sein; Sie können derzeit einen Sensortyp nicht mehrmals an denselben Computer anschließen. Sie können immer nur einen seriellen Adapter mit 4 Anschlüssen gleichzeitig anschließen.

Temperatur-Überwachung

- Alarm, wenn die Temperatur außerhalb eines konfigurierten Bereichs liegt
- Aufzeichnung der Temperatur in der Datenbank zur historischen Analyse in den Web-Reports
- Fahrenheit / Celsius Unterstützung

Überwachung von Temperatur + Luftfeuchtigkeit

- Alarm, wenn die Luftfeuchtigkeit außerhalb eines konfigurierten Bereichs liegt
- Feuchtigkeit in der Datenbank für die historische Analyse in den Web-Reports aufzeichnen

Bewegungssensoren

- Alarm, wenn Bewegung erkannt wird
- Zeichnet Bewegungsaktivität in der Datenbank auf
- Erfordert seriellen Adapter

Rauch-Sensor

Der Rauchsensor wird an den seriellen Anschluss angeschlossen und kann alarmieren wenn Rauch entdeckt wird.

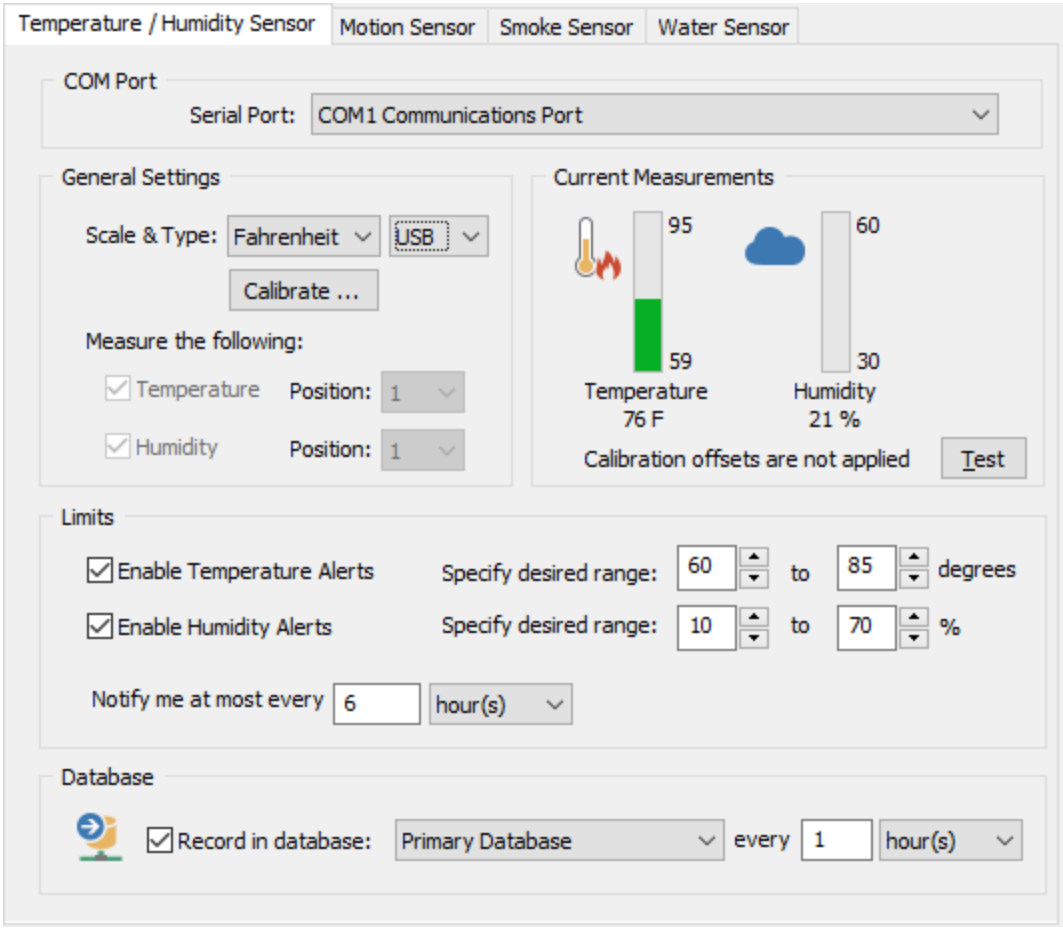
Wasser-Sensor

Der Wassersensor wird an den seriellen Anschluss angeschlossen und kann alarmieren wenn Wasser entdeckt wird.

Weitere Informationen über die Konfiguration der verschiedenen Sensoren finden Sie im nächsten Kapitel.

5.8.1 Temperatur / Luftfeuchtigkeit

Die Temperatur- und Luftfeuchtigkeitsüberwachung wird durch Klicken auf den Container **Environment** konfiguriert.



Allgemeine Einstellungen

Konfiguriert die serielle Schnittstelle, an der der Sensor angebracht ist, und stellt die gewünschte Temperaturskala ein. Abhängig von der Art des Sensors kann man entweder die Temperatur, die Luftfeuchtigkeit oder beides überwachen.

Wählen Sie den Typ des angeschlossenen Sensors, standardmäßig "Seriell". Der USB-Sensor 30602 ist der einzige Sensor, der die "USB"-Auswahl für den Typ unterstützt (siehe unten für Einzelheiten).

Beim Anbringen eines Temperatur- oder Feuchtigkeitssensors muss die jeweilige Position auf dem seriellen Adapter, an der der Sensor angebracht wird, ausgewählt werden. Die Position ist auf dem eigentlichen Adapter angegeben und beträgt immer **1**, wenn der Adapter nur einen Sensor unterstützt.

Wenn ein kombinierter Temperatur- und Luftfeuchtigkeitssensor angeschlossen wird, sind beide Positionsfelder deaktiviert, da dieser Sensor intern immer die Positionen 1 und 2 verwendet.

> Der reine USB-Temperatur-/Feuchtigkeitssensor (30602) und der serielle Temperatur-/Feuchtigkeitssensor (30106) können nicht gleichzeitig an denselben Host angeschlossen werden.

Wichtige Informationen für den USB-Sensor 30602

Wenn der Typ von "Seriell" auf "USB" umgeschaltet wird, versucht die Management-Konsole automatisch die erforderlichen virtuellen COM-Port-Treiber von FTDI zu installieren. Diese Treiber

emulieren eine serielle Schnittstelle und sind für die korrekte Funktion des Sensors erforderlich. Die Treiber sind WHQL-zertifiziert, und die Installation erfordert keinen Neustart. Das Treiber-Installationsprogramm ist **ftdichip_environment_usb_com_driver.exe** und befindet sich im Unterverzeichnis resources des Installationsverzeichnisses. Wenn die automatische Installation nicht funktioniert, kann der Treiber manuell von der Eingabeaufforderung aus installiert werden, indem Sie **ftdichip_environment_usb_com_driver**.exe ausführen.

Weitere Informationen zu den USB-Sensoren, einschließlich Deinstallationsanweisungen, finden Sie unter http://www.ftdichip.com/Support/Documents/InstallGuides.htm.

Kalibrierung
In einigen Fällen kann es notwendig sein die Temperatur und/oder die Luftfeuchtigkeit des Sensors zu korrigieren, z.B. wenn der Sensor an einer Stelle positioniert wird, an der die gemessene Temperatur nicht genau die Temperatur des restlichen Raumes widerspiegelt. Durch Klicken auf die Schaltfläche "Kalibrieren" kann der Benutzer entweder zu jedem vom Sensor gemeldeten Messwert addieren oder davon subtrahieren.

Aktuelle Messungen

Wenn ein Sensor an den lokalen Rechner angeschlossen ist, zeigen diese beiden Balken den letzten Temperatur- und/oder Feuchtigkeitsmesswert an, wie er vom Agenten gemeldet wurde.

Grenzwerte

Temperatur- und Luftfeuchtigkeitsalarme schreiben ein **Fehlerereignis in das Ereignisprotokoll**, wenn der gemessene Wert außerhalb des von Ihnen konfigurierten Bereichs liegt, und protokollieren ein Informationsereignis im Ereignisprotokoll, wenn der gemessene Wert wieder im konfigurierten Bereich liegt, wodurch der Alarm gelöscht wird.

Temperaturwarnungen (Enable Temperature Alerts): Warnmeldungen, wenn die Temperatur außerhalb eines konfigurierbaren Bereichs liegt, werden Alarme generiert, sobald die gemessene Temperatur außerhalb des gewünschten Bereichs liegt.

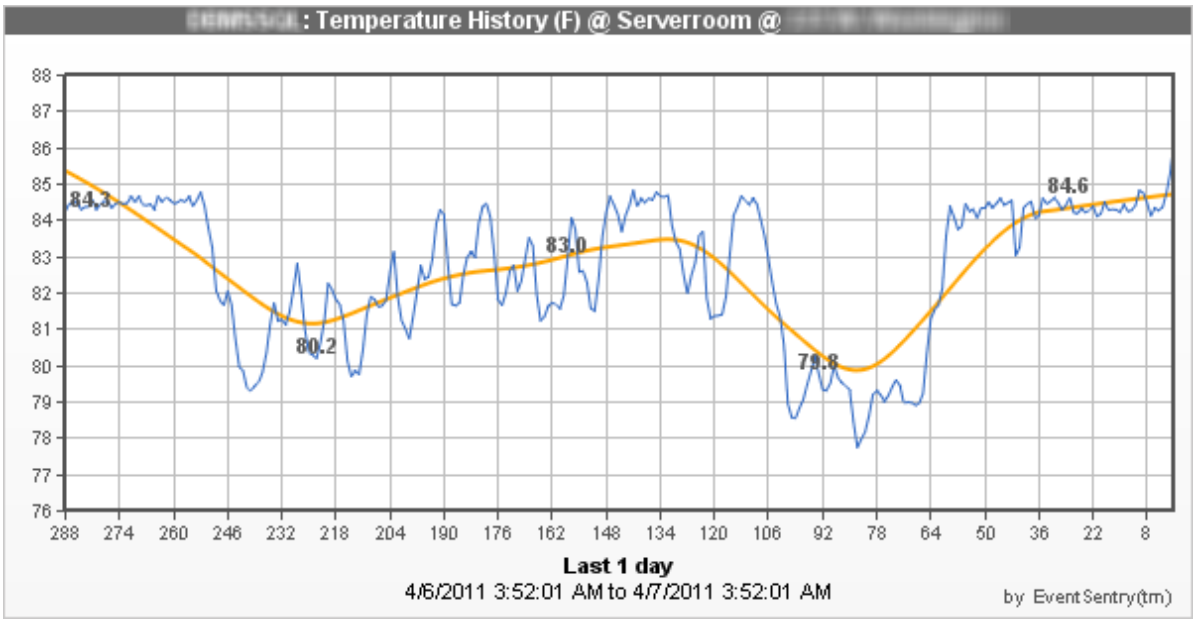
Geben Sie 0 für das untere Ende des Bereichs an, wenn kein Mindestwert eingestellt werden soll.

Luftfeuchtigkeitswarnungen (Enable Humidity Alerts): Warnmeldungen, wenn die Luftfeuchtigkeit außerhalb eines konfigurierbaren Bereichs liegt, werden Alarme generiert, sobald die gemessene Luftfeuchtigkeit außerhalb des gewünschten Bereichs liegt.

Geben Sie 0 für das untere Ende des Bereichs an, wenn kein Mindestwert festgelegt werden soll.

Notify me at most every XX: Legen Sie fest, wie oft ein Fehler in das Ereignisprotokoll geschrieben werden soll, wenn die Temperatur und/oder Luftfeuchtigkeit außerhalb des konfigurierten Bereichs liegt.

Eingebettete Diagramme: Wenn Temperaturalarm-Ereignisse von EventSentry per E-Mail verschickt werden, enthalten sie automatisch ein PNG-Diagramm aus den in den letzten 24 Stunden gesammelten Umgebungsdaten. Das Bild enthält den Hostnamen, die Art der Umgebungsdaten, die grafisch dargestellt werden (z.B. Temperatur in Grad Fahrenheit), sowie die Beschreibung (wenn konfiguriert). Das Diagramm enthält eine automatisch berechnete Trendlinie in Orange.



Datenbank

Zusätzlich zur Benachrichtigung bei Überschreitung der Schwellenwerte können Sie auch die aktuelle Temperatur und/oder Luftfeuchtigkeit in einer Datenbank protokollieren, um Trends und den Verlauf anzuzeigen.

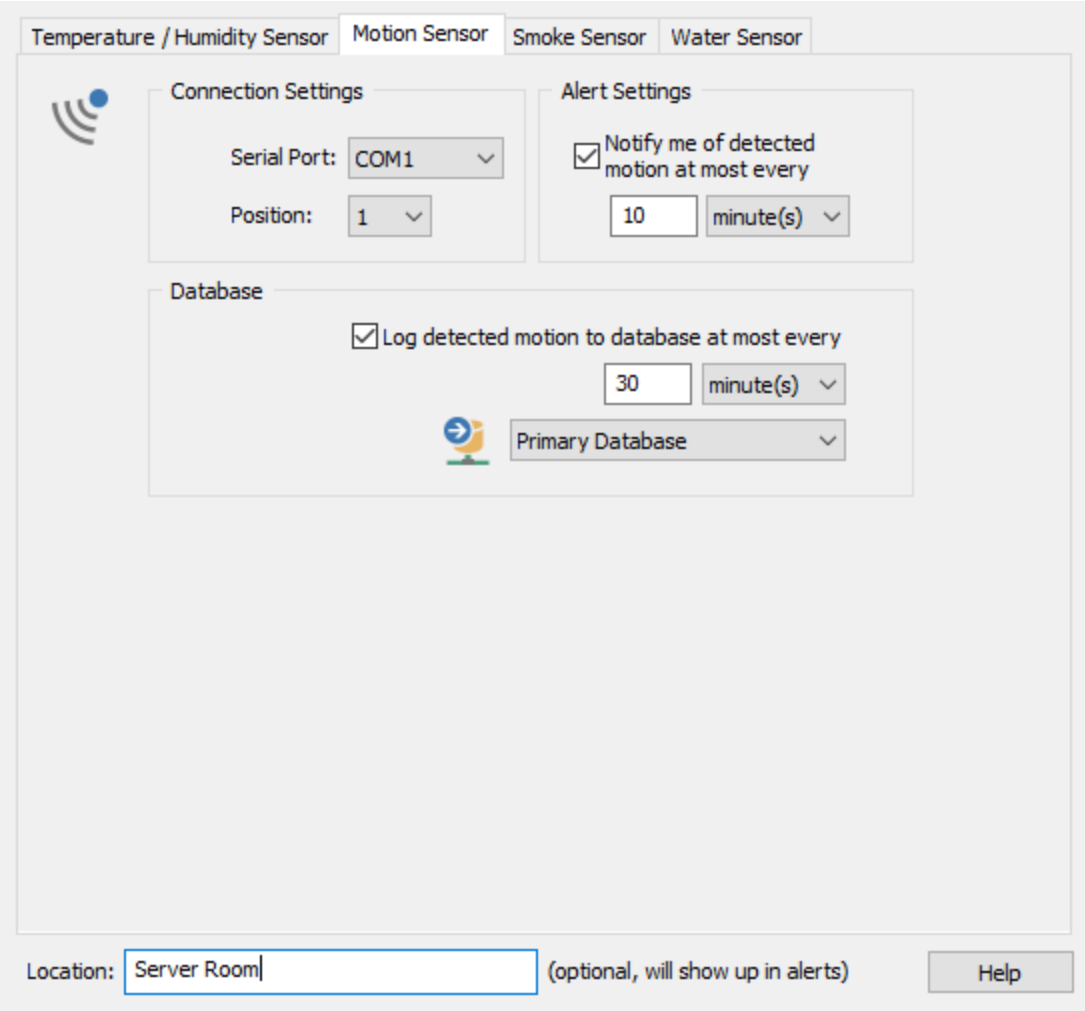
Wählen Sie die Datenbankaktion, in die die Historie geschrieben werden soll und wie oft die aktuellen Daten in die Datenbank geschrieben werden sollen. Das minimale Zeitintervall beträgt 5 Minuten.

Standort

Wenn Sie Temperatur-/Luftfeuchtesensoren an mehreren Standorten in Ihrer Organisation verwenden, können Sie den Standort hier angeben. Der Standort ist in den Alarmen enthalten, die im Ereignisprotokoll protokolliert werden, er wird in den Web Reports nicht angezeigt.

5.8.2 Bewegungsüberwachung

Die Bewegungsüberwachung wird auf der Registerkarte "Motion Sensor" unter Environment konfiguriert.



Verbindungseinstellungen

Wählen Sie den seriellen Anschluss, an den der serielle Adapter angeschlossen ist, und geben Sie an, an welcher Position (1-4) der Sensor angeschlossen ist. Die Position wird auf dem eigentlichen Adapter angegeben und ist immer **1**, wenn der Adapter nur einen Sensor unterstützt.

Alert-Einstellungen

Konfiguriert wie oft Alarme generiert werden sollen wenn kontinuierliche Bewegung erkannt wird.

Datenbank

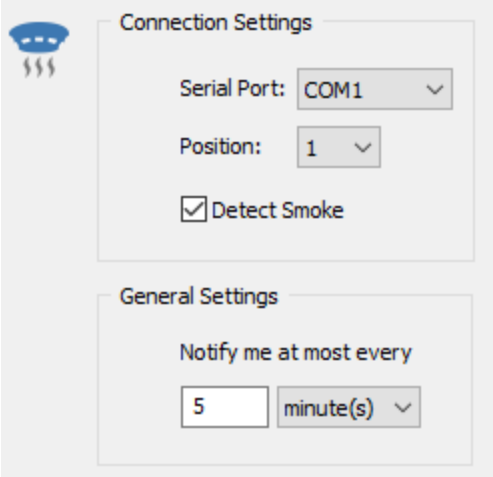
Wählen Sie die Datenbankaktion, in die Bewegungsinformationen geschrieben werden sollen, und geben Sie an, wie oft Daten zur Datenbank hinzugefügt werden sollen, wenn kontinuierliche Bewegung erkannt wird.

Standort

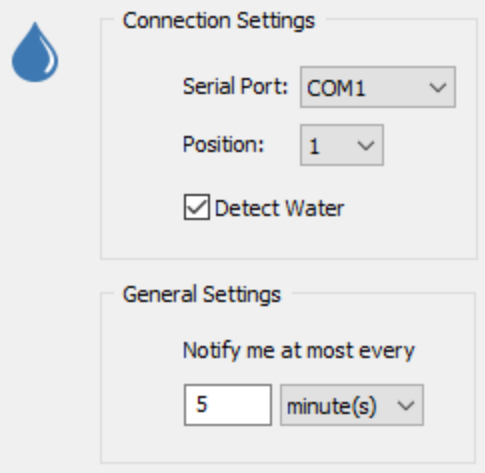
Wenn Sie in Ihrer Organisation mehrere Bewegungssensoren verwenden, können Sie den Standort hier angeben. Der Standort ist in den Alerts enthalten, die im Ereignisprotokoll protokolliert werden, er wird in den Web Reports nicht angezeigt.

5.8.3 Rauch / Wasser

Rauch- und Wasserüberwachung werden auf der Registerkarte "Smoke" und/oder "Water" unter Environment konfiguriert.



Konfiguration des Rauchsensors



Konfiguration des Wassersensors

Verbindungseinstellungen

Wählen Sie den seriellen Anschluss, an dem der serielle Adapter angeschlossen ist, und geben Sie an, an welcher Position (1-4) der Sensor angeschlossen ist. Die Position wird auf dem eigentlichen Adapter angegeben und ist immer **1**, wenn der Adapter nur einen Sensor unterstützt.

Allgemeine Einstellungen

Wählen Sie aus, wie oft Alarme erzeugt werden sollen, wenn kontinuierlich Rauch oder Wasser erkannt wird.

Standort

Wenn Sie in Ihrer Organisation mehrere Rauch- oder Wassersensoren verwenden, können Sie hier den Standort angeben. Der Standort ist in den Alarmen enthalten, die im Ereignisprotokoll protokolliert werden, er wird in den Web Reports nicht angezeigt.

5.8.4 Ereignisprotokolle

Die folgenden Ereignisse werden mit der Ereigniskategorie **Environment Sensors** protokolliert.

Event ID	Severity	Event Description	Example
10903	Error	No environment monitor found	EventSentry was unable to find a temperature and/or humidity sensor on serial port COM1. Please make sure the device is connected properly.
10904	Error	Database interval too small	The database write interval for environment monitoring is set too small. The interval was automatically adjusted to 900 seconds.
10908	Error	The temperature has fallen outside the	The current temperature has fallen outside the configured range (60F to 76F). The current temperature is 83.58 degrees

		configured range.	(F).
10909	Error	The humidity has fallen outside the configured range.	The current humidity has fallen outside the configured range (10% to 60%). The current humidity is 9%.
10910	Information	The temperature is back inside the configured range.	The current temperature is back in the configured range (60F to 76F). The current temperature is 74.57 degrees (F).
10911	Information	The humidity is back inside the configured range.	The current humidity is back in the configured range (10% to 60%). The current humidity is 12%.
10912	Error	Motion detected	Motion sensor (Server Room ABC) detected motion.
10913	Error	Smoke detected	Smoke sensor (Server Room ABC) detected smoke.
10914	Error	Water detected	Water sensor (Server Room ABC) detected water.
10915	Error	Smoke sensor failed self test	EventSentry failed to detect the required self-test of the smoke sensor which is run every 24 hours. Please press the TEST button on the smoke sensor for at least 30 seconds to make sure that the sensor works correctly and an alert is generated by EventSentry.
10916	Error	Sensor error	The attached Water sensor reported an error, or no sensor is attached. This feature has been turned off.

5.9 Heartbeat Überwachung

Die Heartbeat-Überwachung überwacht jedes Netzwerkgerät, das über TCP/IP erreichbar ist. Die Herzschlagüberwachung selbst wird durch den **EventSentry Heartbeat** Monitor-Dienst durchgeführt und normalerweise auf einem Computer in Ihrem Netzwerk installiert.

Die Heartbeat-Überwachung pingt entfernte Hosts an und überprüft TCP-Ports, kann aber auch Informationen von entfernten SNMP-Agenten abfragen, um Informationen wie Festplattenplatz, Systeminfo, Betriebszeit und Leistungsinformationen zu erhalten.

1. Auswählen der zu überwachenden Computer und Festlegen eines Gruppentyps
Damit ein Computer überwacht werden kann, muss er hinzugefügt oder in eine Gruppe importiert werden, die Heartbeat-fähig ist (weitere Informationen).

2. Globale Heartbeat-Konfigurationsoptionen einstellen
Einige Konfigurationsoptionen (wie z.B. das Abfrageintervall) werden global festgelegt und gelten für alle Computer. Andere Optionen können pro Gruppe und pro Host festgelegt werden (weitere Informationen).

3. Einstellung von Gruppenoptionen
Dieses Kapitel zeigt, wie die anfängliche Überwachungskonfiguration für eine Gruppe eingerichtet wird (weitere Informationen).

4. Anpassen der Heartbeat-Optionen auf einer Pro-Host-Basis
In diesem Kapitel wird erklärt, wie Gruppeneinstellungen auf der Ebene der einzelnen Hosts überschrieben werden können (weitere Informationen).

5. Einstellung von Wartungsplänen für planmäßige Ausfälle

Wenn eine oder mehrere Maschinen an einem bestimmten Tag oder zu einer bestimmten Stunde ausfallen sollen, können Sie Wartungspläne für diese Zeiträume festlegen, um den Erhalt von Benachrichtigungen zu vermeiden (weitere Informationen).

6. Anzeigen des Herzschlagstatus und -verlaufs über die Web Reports
Der aktuelle Heartbeat-Status ist unter "Status - Heartbeat" in den Web Reports verfügbar.

5.9.1 SNMP / SSH Überwachung

Der Heartbeat Agent nutzt **SNMP (v1, v2c & V3) und SSH (**sofern verfügbar) auf dem Remote-Host, um weitere Informationen vom überwachten Gerät zu erhalten.

Über **SNMP** können die folgenden Informationen abgerufen werden:

- Informationen zum Festplattenplatz
- Leistungsüberwachung
- Hardware-Zusammenfassung
- Laufende Prozesse(nur Alerting)

Mit **SSH** können die folgenden Informationen abgerufen werden:

- Erweiterte Systeminformationen (Zeitzone, USB-Version, BIOS, OS-Installationsdatum, erweiterte CPU-Informationen)
- Laufende Daemons/Dienste

Automatische Erkennung
Der Heartbeat-Agent versucht, bestimmte Merkmale auf einem entfernten Host automatisch zu erkennen und die zugehörigen Informationen über SNMP abzurufen. Die unterstützten Funktionen sind unten aufgeführt.

VMWare ESXi
Wenn VMWare auf einem Remote-Host erkannt wird, wird ein VM-Bestand vom Remote-Host abgerufen und steht auf der Seite **Bestand - Virtuelle Maschine** zur Verfügung. Die folgenden Details sind verfügbar:

- Produkt-Name
- Produkt-Version
- Produkt-Build
- VM-Name
- Aktueller VM-Status
- VM-Betriebssystem (falls Tools installiert sind)
- Zugewiesene CPUs
- Zugewiesener Speicher
- Pfad zur .vmx-Datei

MAC zu Switch-Port-Zuordnung
Wenn es sich bei dem überwachten Gerät um einen Switch handelt, werden die MAC-Adressen der Switch-Teilzuordnungen automatisch abgerufen und sind auf der Seite **Inventar - Switch** verfügbar. Die MAC-Adressen werden mit den von den Agenten und dem ARP-Dämon erhaltenen Hardware-Informationen korreliert, so dass die Hostnamen, wann immer möglich, angezeigt werden können.

Protokollierung

Die SNMP-Fähigkeiten eines entfernten Geräts werden automatisch bestimmt, wenn der Heartbeat-Agent nach dem Start initialisiert wird, und das Ereignis 11020 wird für jedes Gerät protokolliert, das mindestens SNMP v1 unterstützt.

> Für alle Funktionen ist es erforderlich, dass das jeweilige Systemintegritätsobjekt (z.B. Festplattenplatz, Leistungsüberwachung) den überwachten Hosts zugewiesen ist.
>
> Wenn einem Host kein Objekt für Festplattenplatz, Leistung oder Software/Hardware-Inventar zugewiesen ist, wird er nicht per SNMP überwacht.

Fehlerbehandlung

EventSentry setzt die SNMP-Überwachung eines Hosts unter den folgenden Bedingungen aus:

1. Der Heartbeat Service ist nicht in der Lage, während des ersten Überwachungsintervalls nach dem Start des Dienstes einen Remote-Host über SNMP abzufragen.
2. Der Heartbeat Service kann einen Remote-Host mehr als 24 Stunden lang nicht per SNMP abfragen, die Ereignis-ID 11023 wird protokolliert und die SNMP-Überwachung für den Host deaktiviert.
3. Der Heartbeat Service kann während eines Zeitraums von 48 Stunden in mindestens 50% der Zeit keinen Remote-Host über SNMP abfragen, die Ereignis-ID 11015 wird protokolliert und die SNMP-Überwachung wird für den Host deaktiviert.

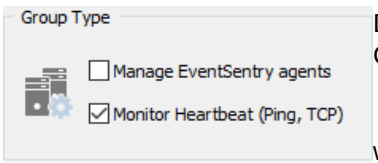
> Um die SNMP-Überwachung wieder zu aktivieren, befolgen Sie die Anweisungen im protokollierten Ereignis oder öffnen Sie die Verwaltungskonsole, suchen Sie den Host innerhalb seiner jeweiligen Computergruppe und klicken Sie auf ihn und klicken Sie schließlich auf die SNMP-bezogene Warnung, um die SNMP-Überwachung wieder zu aktivieren.

5.9.2 Computer hinzufügen

Auswählen von Gruppenfunktionen

Bevor Computer zu einer bestehenden oder neuen Gruppe hinzugefügt werden, müssen die entsprechenden Gruppenoptionen ausgewählt werden. Die Gruppenoptionen bestimmen, ob Computer in einer Gruppe durch den Heartbeat-Dienst überwacht werden oder nicht. Gruppenfunktionen werden durch Kontrollkästchen im Abschnitt "Gruppenfunktionen" konfiguriert.

Die folgenden Gruppentypen sind verfügbar:



Verwalten von EventSentry-Agenten

Ermöglicht die Verwaltung von Computern in dieser Gruppe über die Funktion "Remote Update". Dies unterstützt die Installation, Deinstallation und Aktualisierung von EventSentry-Agenten auf allen Computern in dieser Gruppe.

Wenn auf keinem der Hosts in dieser Gruppe Windows ausgeführt wird, sollte dieses Kontrollkästchen **nicht aktiviert werden**, damit kostengünstigere Lizenzen für Netzwerkgeräte verwendet werden können.

Netzwerk überwachen (Ping, TCP-Status)
Überwacht alle Computer/Geräte in dieser Gruppe mit dem Heartbeat-Dienst. Beachten Sie, dass die Option "EventSentry-Agenten überwachen" nur verfügbar ist, wenn das erste Kontrollkästchen ebenfalls aktiviert ist.

Hinweis: Mindestens ein Häkchen in einem der beiden Kontrollkästchen muss gesetzt werden.

Hinzufügen oder Importieren von Computern

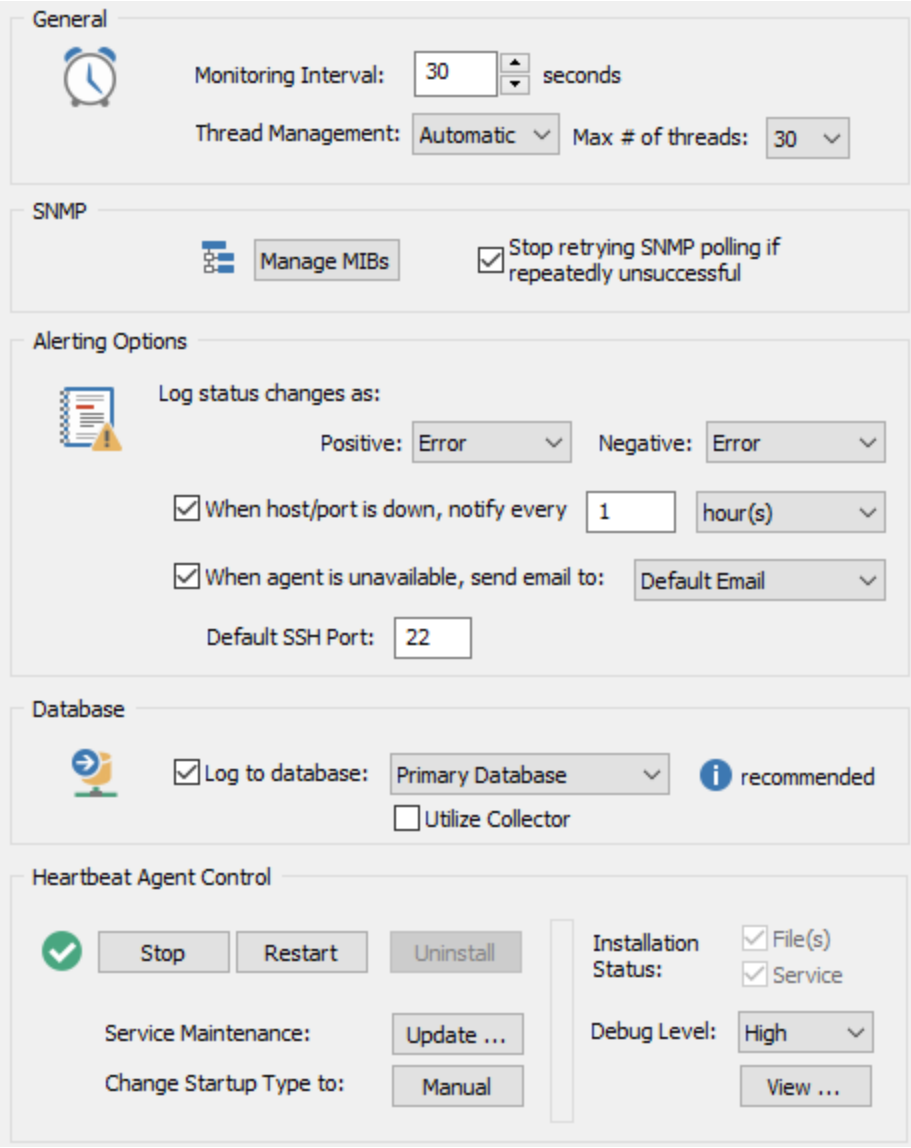
Computer können entweder manuell hinzugefügt werden, indem Sie mit der rechten Maustaste auf den Container "Computers" einer bestimmten Gruppe klicken, oder sie können auf verschiedene Weise importiert werden, siehe Remote Update -> Importieren für weitere Informationen zum Importieren von Computern.

Wenn Sie eine Gruppe mit Active Directory verknüpfen, stellen Sie sicher, dass Sie einmal auf "Get Service Status" klicken (Rechtsklick auf den Computer-Container), damit die Computer aus Active Directory zwischengespeichert werden.

Sie müssen auch "Get Service Status" wählen oder die Verwaltungskonsole jedes Mal neu starten, wenn sich die Liste der Computer in Active Directory ändert.

5.9.3 Globale Optionen

Globale Heartbeat-Optionen werden im Heartbeat-Container konfiguriert, wo eine Vielzahl von Heartbeat-Überwachungsoptionen konfiguriert werden, die alle Hosts unabhängig von der Gruppenzugehörigkeit betreffen.



Allgemein

Überwachungsintervall: Dieses Intervall bestimmt, wie oft die überwachten Computer abgefragt werden, in Sekunden.

Thread-Verwaltung: Der Heartbeat-Agent verwendet Threads, um Hosts parallel zu scannen. Bei der Einstellung **automatisch** berechnet der Agent automatisch die Anzahl der zu verwendenden Threads auf der Grundlage der Anzahl der zu überwachenden Hosts sowie der Zeit, die für die Überwachung der Hosts benötigt wird. Abhängig von der tatsächlichen Scan-Geschwindigkeit passt der Agent die Thread-Anzahl dynamisch an und erhöht oder verringert die Thread-Anzahl je nach Bedarf. Wenn auf **manuell** eingestellt, verwendet der Agent unabhängig von der Anzahl der Hosts und der Scan-Geschwindigkeit immer die unter "Max. Anzahl der Threads" angegebene Anzahl von Threads.

Maximale Anzahl von Threads: Wenn die Thread-Verwaltung auf **automatisch** gesetzt ist, gibt die maximale Anzahl der Threads (Obergrenze) an, die der Agent verwendet. Wenn die Thread-Verwaltung auf **manuell** eingestellt ist, bestimmt diese Zahl die Anzahl der Threads die verwendet werden.

Unabhängig von dieser Einstellung wird der Agent nie mehr Threads verwenden, als Hosts zu überwachen sind.

Ereignisprotokoll-Protokollierung

Statusänderungen protokollieren: Sie können optional Statusänderungen in das Ereignisprotokoll schreiben, so dass Sie benachrichtigt werden können, wenn ein bestimmter Computer oder Dienst nicht mehr verfügbar ist. Eine positive Statusänderung liegt vor, wenn ein Computer oder Dienst zuvor nicht erreichbar war, jetzt aber wieder erreichbar ist. Eine negative Statusänderung liegt vor, wenn ein Computer oder Dienst vorher nicht erreichbar war, jetzt aber nicht mehr erreichbar ist. Es wird daher empfohlen, negative Statusänderungen zumindest als Warnungen zu protokollieren. Siehe Ereignisprotokoll für alle durch diese Funktion protokollierten Ereignisse.

Wenn der Gastgeber ausgefallen ist, benachrichtigen Sie alle: Standardmäßig benachrichtigt der Heartbeat-Dienst nur über Änderungen des Host-Status. Das heißt, er erzeugt immer dann ein Ereignis, wenn ein Host oder TCP-Port von online auf offline und umgekehrt wechselt. Wenn diese Option aktiviert ist, wird der Heartbeat-Dienst so konfiguriert, dass er kontinuierlich einen Alarm erzeugt, wenn ein Host, Dienst oder Remote-Agent ausgefallen ist. Das gewählte Zeitintervall legt fest, wie oft diese kontinuierlichen Alarme generiert werden.

Benachrichtigen, wenn der EventSentry-Dienst nicht verfügbar ist: Der Heartbeat-Dienst ist auf den EventSentry-Dienst angewiesen, um Sofortbenachrichtigungen wie E-Mail- oder Seitenbenachrichtigungen durchzuführen. Dies liegt daran, dass der Heartbeat-Dienst alle Statusbenachrichtigungen (z.B. wenn ein Host nicht erreichbar ist) im Ereignisprotokoll protokolliert. Wenn also Heartbeat-Benachrichtigungen verwendet werden, sollte diese Option aktiviert werden, damit der Heartbeat-Dienst eine E-Mail-Benachrichtigung sendet, wenn der EventSentry-Dienst nicht läuft. Diese Option kann ignoriert werden, wenn Heartbeat-Informationen nur in den Web Reports verwendet werden.

Standard-SSH-Port: Der SSH-Port, der verwendet wird, wenn SSH-Anmeldeinformationen für einen Host oder eine Gruppe konfiguriert werden. SSH wird nur für Nicht-Windows-Hosts verwendet.

Datenbank

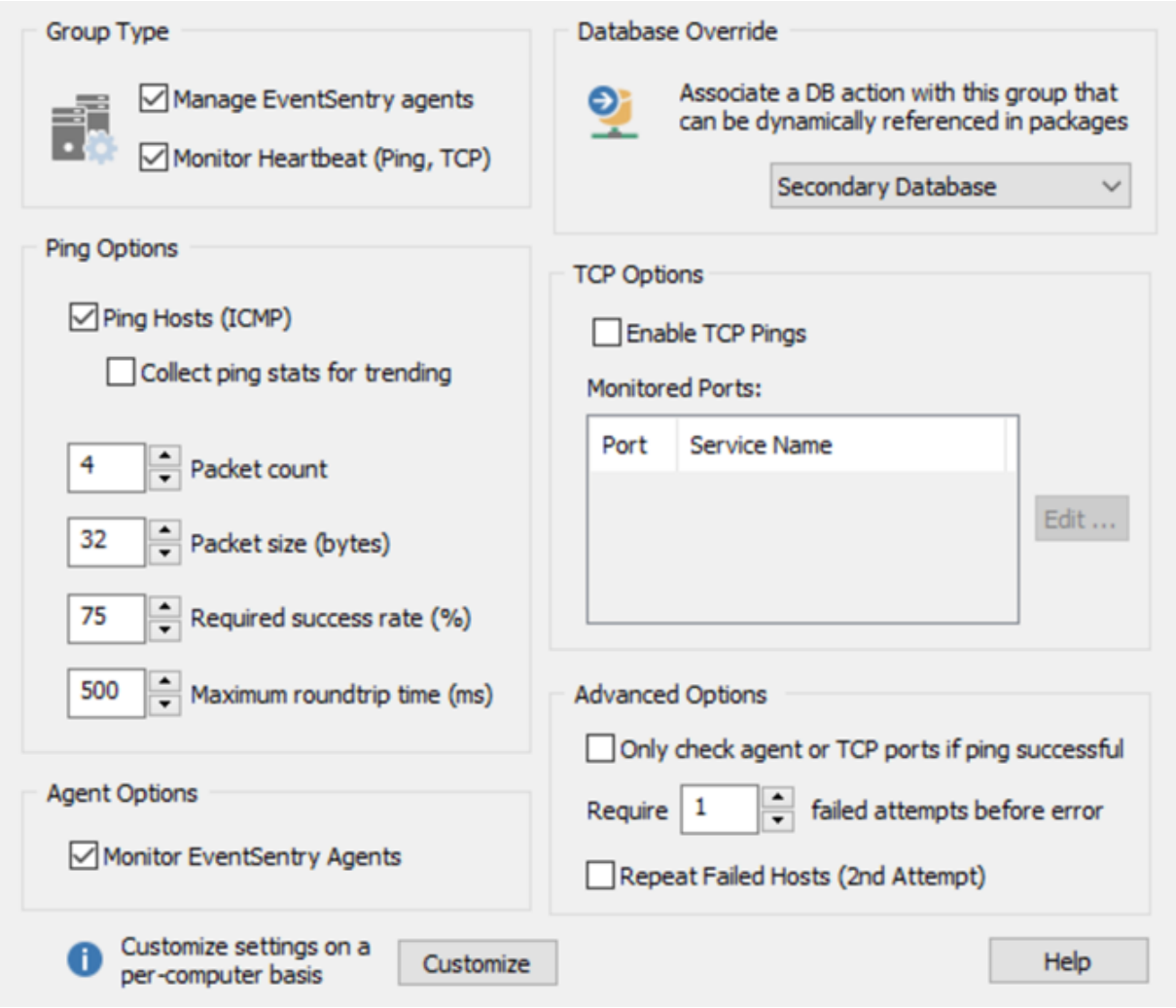
Speichert alle Daten vom Heartbeat-Dienst in der ausgewählten Datenbank um sowohl den aktuellen Status als auch historische Daten bereitzustellen. Zu den vom Herzschlag-Agenten gesammelten Daten gehören

- Aktueller Status aller überwachten Host-Indikatoren (Ping, Agent und/oder TCP)
- Alle SNMP-Metriken, einschließlich Leistung und Festplattenkapazität
- Systeminformationen von Netzwerkgeräten
- VM-Inventar von VMWare-Hosts
- MAC zum Umschalten der Portzuordnungen

Collector verwenden: Wenn ein Collector verfügbar ist und der Heartbeat-Dienst in einem Netzwerk installiert ist, dass keine direkte Verbindung zur ausgewählten Datenbank hat, wird der Heartbeat-Agent bei Aktivierung dieser Option so konfiguriert, dass er alle Daten über den Collector sendet. Diese Option ist standardmäßig deaktiviert und sollte nur in Szenarien im MSP-Stil aktiviert werden.

5.9.4 Optionen für Gruppen

Definiert die Standardüberwachungsparameter von Computern in einer Gruppe, wie z. B. die erforderliche Ping-Erfolgsrate. Um die Herzschlagoptionen für eine Gruppe festzulegen, markieren Sie einfach die Gruppe und wählen Sie "Herzschlagoptionen" im Kontextmenü oder im Ribbon.



Alle Einstellungen, die in diesem Dialogfeld definiert werden, dienen als anfänglicher Standard für alle Computer in der Gruppe. Sobald Sie die Optionen für einen bestimmten Computer einzeln konfigurieren (=überschreiben), gelten diese Einstellungen nicht mehr für diesen Computer.

Standarddatenbank für Gruppen

Einer Gruppe kann eine Standarddatenbankaktion zugewiesen werden , auf die dann in einem Paket dynamisch verwiesen werden kann. Auf diese Weise kann für jede Gruppe eine eigene Datenbank konfiguriert werden, die von Agenten dynamisch genutzt werden kann, ohne dass eine Duplizierung von Paketen erforderlich ist.

Erweiterte Optionen

Only check agent status or TCP ports if ping successful: Wenn diese Funktion aktiviert ist und ein überwachter Host nicht über PINGs erreichbar ist, versucht der Heartbeat-Agent nicht, den Agentenstatus und/oder den TCP-Status zu überprüfen, vorausgesetzt, der Host ist ausgefallen. Der Agenten- oder TCP-Status des Hosts wechselt dann in den Status *UNBEKANNT* .

Require X attempts before error: Die Aktivierung erfordert, dass eine überwachte Funktion (Ping, Agent oder TCP-Port) X-mal ausgefallen ist, bevor ein Fehler in das Ereignisprotokoll geschrieben wird. Bitte

beachten Sie, dass Informationen, die in den Web-Reports reflektiert werden, von dieser Einstellung nicht betroffen sind, Statusänderungen werden immer sofort in den Web-Reports reflektiert.

Repeat Failed Hosts (2nd Attempt): Nachdem alle Hosts überprüft worden sind und festgestellt wurde, dass ein oder mehrere Checks fehlgeschlagen sind, werden diese fehlgeschlagenen Checks wiederholt. Wenn der 2. Versuch erfolgreich ist, wird kein Fehler protokolliert (auch nicht in den Web Reports).

Ping Optionen

Um die Überwachung durch PING zu aktivieren, markieren Sie das Kontrollkästchen **Ping-Hosts**. Sie können dann anpassen, wie ICMP-Pakete gesendet werden:

Packet Count: Wie viele Pakete zu senden sind, standardmäßig 4.
Packet Size: Die Packetgröße der ausgehenden Pakete beträgt standardmäßig 32 Byte.
Required Success Rate: Der Prozentsatz der Pakete muss bestätigt werden, damit ein PING als erfolgreich angesehen werden kann.
Maximum Roundtrip time: Die minimal erforderliche **durchschnittliche** Hin- und Rückflugzeit, bevor der Status auf Fehler wechselt.

Collect ping stats for trending: Protokolliert die Hin- und Rücklaufzeit und den prozentualen Paketverlust von ICMP-Paketen in der Datenbank. Die Daten sind unter "Netzwerk - Antwortzeiten" in den Web Reports eingesehen werden" verfügbar.

Agenten-Optionen

Aktivieren Sie dieses Kontrollkästchen, um den **EventSentry-Agenten** auf den Remote-Computern zu überwachen. Wenn der aktuelle Dienststatus etwas anderes als **"Wird Ausgeführt"** ist, ändert sich der Status des Agenten in "Fehler".

Beginnend mit v3.3 verwendet EventSentry zwei Methoden um den Agentenstatus von einem entfernten Host zu erhalten wenn der Collector deaktiviert ist, drei, wenn der Collector aktiviert ist. Nur wenn eine vorherige Methode fehlschlägt oder nicht verfügbar ist, versucht der Heartbeat-Dienst die nächste Methode.

1. Collector aktiviert: Der Heartbeat-Monitor kommuniziert direkt mit dem (lokalen) Collector, um den Agentenstatus eines entfernten Hosts zu ermitteln. **Hinweis:** Der Collector muss auf demselben Host wie der Heartbeat-Monitor installiert sein.
2. Datenbank: Fragt die Datenbank ab, um den Status eines Remote-Hosts zu ermitteln. Hinweis: Erfordert, dass ein Software/Hardware-Paket zugewiesen und die Option "Refresh Uptime" auf das niedrigste Intervall eingestellt ist.
3. Direkt: Der Heartbeat-Dienst verbindet sich direkt mit dem SCM (Service Control Manager) des Remote-Hosts und fragt den "EventSentry"-Dienst ab.

Wichtige Informationen zur Authentifizierung

Wenn die Abfrage des Agenten über Collector und Datenbank fehlschlägt, ist die direkte Verbindung mit dem Remote-Host die einzige Möglichkeit, den EventSentry-Agentenstatus zu erhalten. Dieser Ansatz setzt jedoch voraus, dass der Heartbeat-Monitor über ausreichende Privilegien verfügt, um den Remote-Host abzufragen.

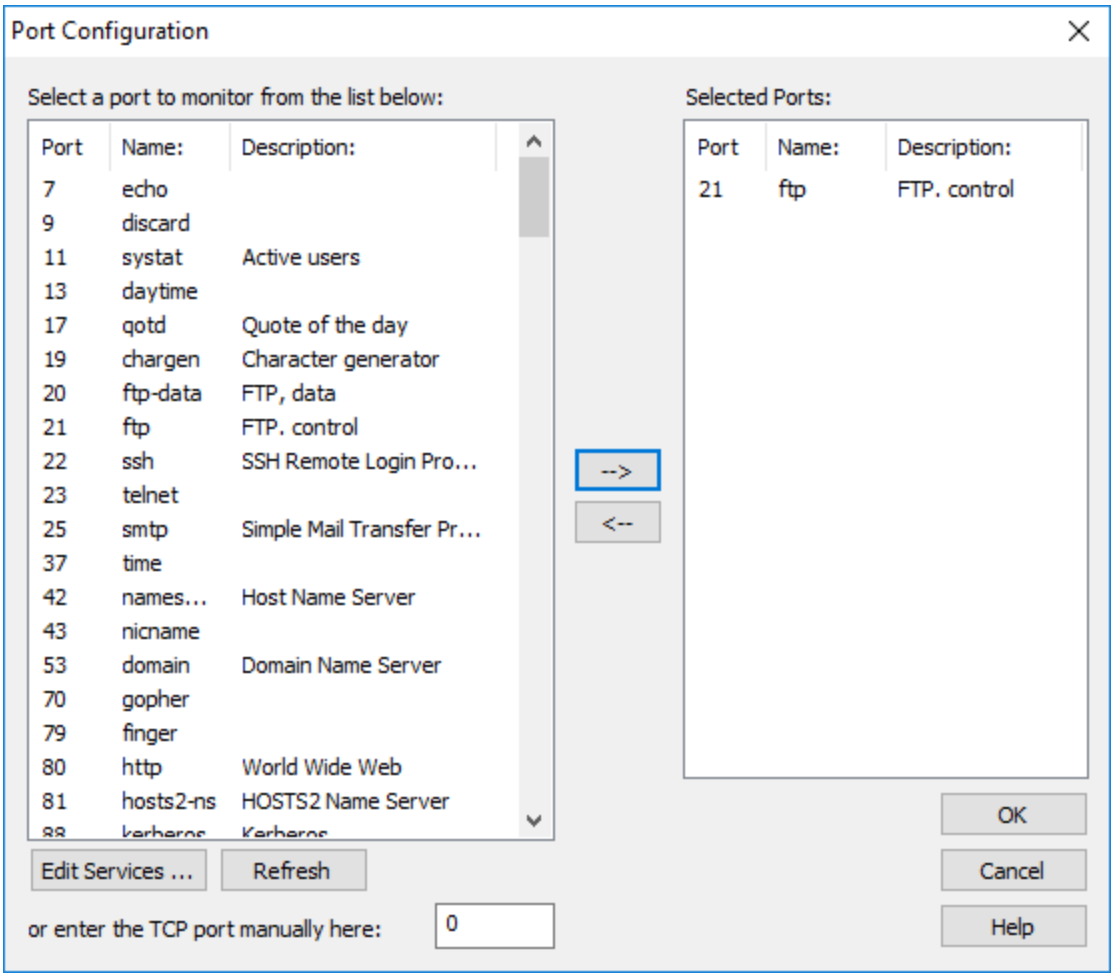
Standardmäßig wird der EventSentry Heartbeat-Dienst unter dem LocalSystem-Konto ausgeführt, das nur begrenzten Zugriff auf entfernte Computer hat. Wenn Sie also beabsichtigen, den Status des EventSentry-Agenten mit dem Heartbeat-Dienst zu überwachen und die Authentifizierung für einen Ordner oder Computer festgelegt haben, sollten Sie

sicherstellen, dass der EventSentry Heartbeat-Dienst unter demselben Konto läuft, unter dem die Authentifizierungsdaten festgelegt wurden.

Kurz gesagt, wenn Sie bei dem Server, auf dem EventSentry installiert wurde, als Benutzer **JoeAdmin** angemeldet sind und die Authentifizierung in der Verwaltungskonsole für eine oder mehrere Gruppen eingestellt haben, dann sollten Sie sicherstellen, dass der EventSentry Heartbeat-Dienst auch unter dem JoeAdmin-Benutzerkonto läuft. Nur dann kann der Heartbeat-Dienst diese Authentifizierungsinformationen verwenden.

TCP Optionen

Überprüfen Sie, ob ein oder mehrere TCP-Ports zuhören oder nicht. Sie können die Liste verwalten, indem Sie auf **Edit Services ...** klicken.



Um einen oder mehrere Ports zu überwachen, wählen Sie einfach den Port aus der Liste auf der linken Seite aus (Sie können mehrere Ports auswählen, indem Sie die STRG-Taste auf Ihrer Tastatur gedrückt halten) und klicken Sie auf den Rechtspfeil. Um einen oder mehrere Ports zu entfernen, klicken Sie auf <--. Wenn ein Port nicht in der Liste links aufgeführt ist, geben Sie ihn manuell in das Bearbeitungsfeld unten links ein.

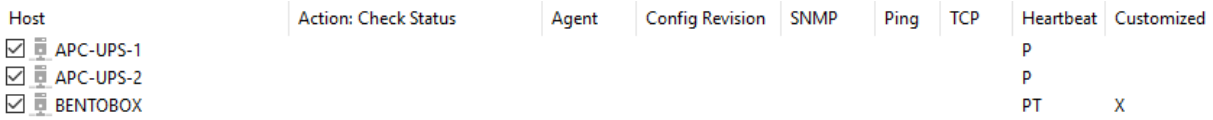
5.9.5 Heartbeat-Optionen anpassen

Sobald die globalen Heartbeatoptionen konfiguriert sind, können bei Bedarf individuelle Computereinstellungen angepasst werden.

Die Heartbeat-Einstellungen können auf verschiedene Weise angepasst werden:

1. Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie "Heartbeat-Optionen".
2. Wählen Sie den Host aus und wählen Sie "Heartbeat Options" im Ribbon
3. Führen Sie einen "Check-Status" für die Gruppe oder alle Gruppen durch (siehe unten)

Um die aktuellen Heartbeat-Einstellungen aller Hosts in einer Gruppe (oder aller konfigurierten Hosts) anzuzeigen, wählen Sie **Status prüfen** im Ribbon oder durch Klicken mit der rechten Maustaste auf den Container Computer.

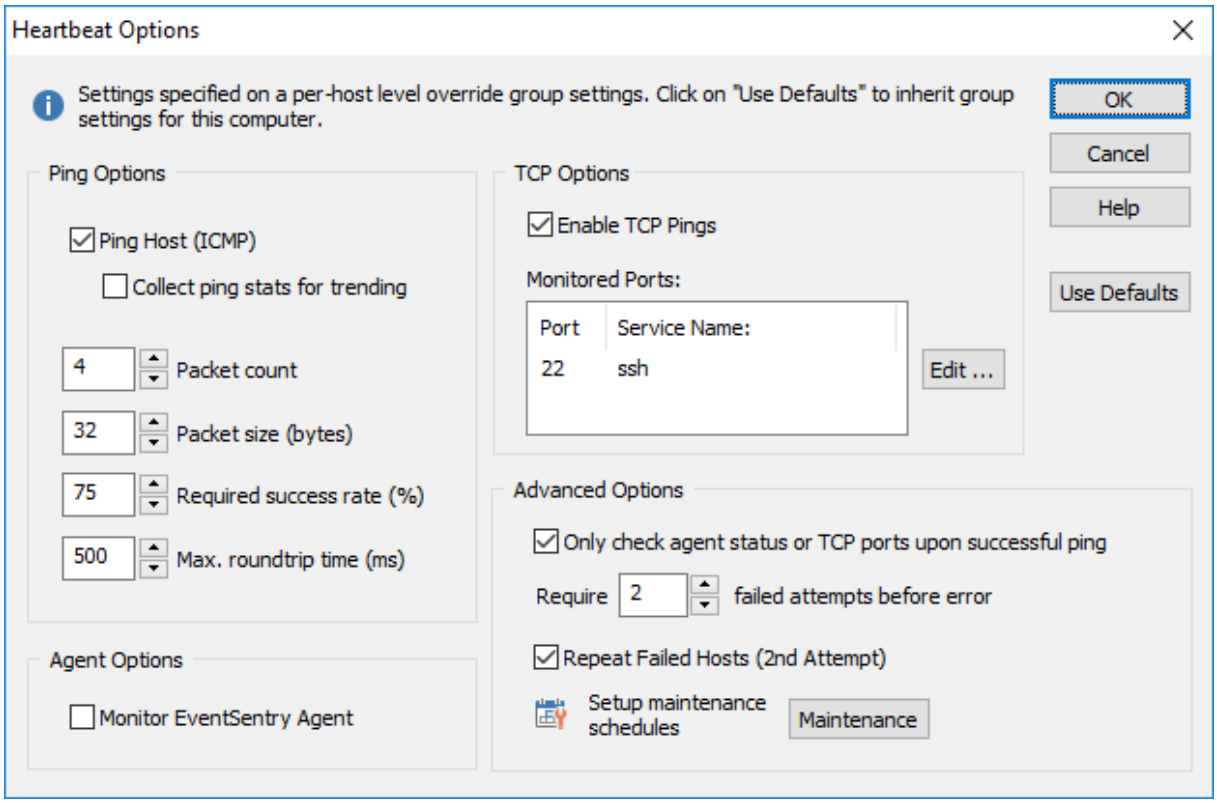


Host	Action: Check Status	Agent	Config Revision	SNMP	Ping	TCP	Heartbeat	Customized
APC-UPS-1							P	
APC-UPS-2							P	
BENTOBOX							PT	X

Der Screenshot zeigt drei Hosts, wobei ein Host über angepasste Heartbeat-Einstellungen verfügt.

Die in der Spalte **Optionen** angezeigten Buchstaben sind Abkürzungen für Ping [P], Agent [A] und TCP [T]. Wenn der Buchstabe für das jeweilige Merkmal in der Spalte Optionen angezeigt wird, dann wird der entsprechende Dienst überwacht.

Um die Einstellungen für einen Computer anzupassen, klicken Sie mit der rechten Maustaste auf den Host und wählen Sie "Gruppeneinstellungen überschreiben". Daraufhin wird ein Dialog ähnlich dem unten gezeigten angezeigt:



Wenn Sie den OK-Knopf drücken, wird der Computer mit den im Dialog festgelegten Einstellungen überwacht. Es ist derzeit nicht möglich, nur eine bestimmte Option außer Kraft zu setzen, z.B. nur die TCP-Option außer Kraft zu setzen.

> Nachdem Sie die Konfiguration gespeichert haben, müssen Sie das nächste Heartbeat-Überwachungsintervall abwarten, bevor Ihre Änderungen auf der Seite mit dem Heartbeat-Status angezeigt werden.

Damit ein Computer wieder die Standardgruppeneinstellungen vererbt, klicken Sie auf die Schaltfläche **Standardeinstellungen verwenden**. Dadurch wird das Dialogfeld beendet und der Computer erbt wieder die Gruppeneinstellungen.

5.9.6 Host als Router definieren

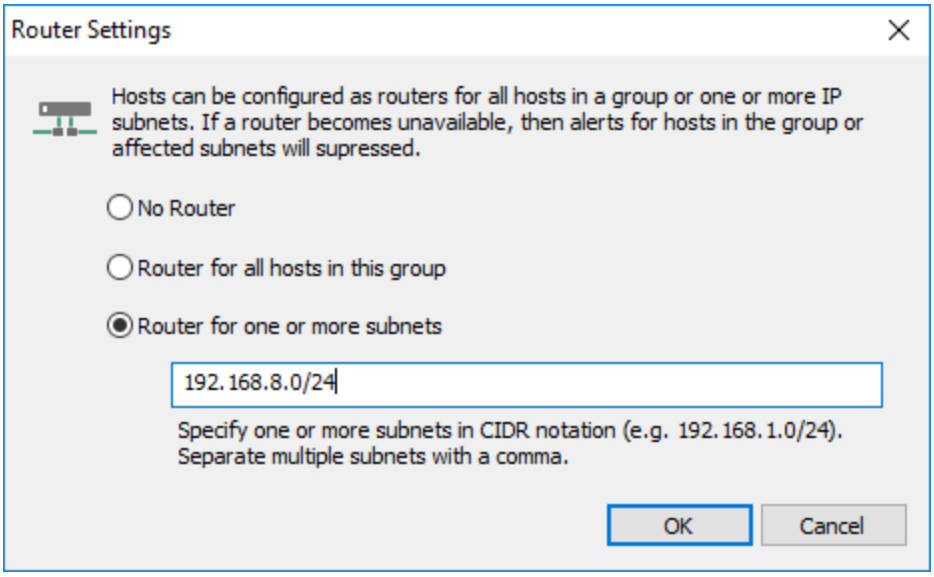
Bei der Überwachung von Routern zusätzlich zu anderen Netzwerkgeräten, wie z.Bsp. Server die sich hinter diesem Router befinden, können unnötige Heartbeat-Alarme vermieden werden indem das "Router"-Flag einem überwachten Computer zugewiesen wird.

Router können auf zwei Arten definiert werden:

- Router für alle Hosts in einer Gruppe
- Router für ein oder mehrere spezifische Subnetze

Ein Host kann als Router konfiguriert werden, indem Sie mit der rechten Maustaste auf den Host im linken Baumfenster klicken oder indem Sie den Host auswählen und "Als Router festlegen" im Ribbon wählen.

Wenn ein Host in einer Gruppe als Router festgelegt ist, werden in das Ereignisprotokoll geschriebene Alarme für alle Hosts, für die der Router zuständig ist, unterdrückt, mit Ausnahme des Hosts, der als Router festgelegt ist. Informationen, die in die Datenbank geschrieben werden, sind von dieser Einstellung nicht betroffen und Heartbeat-Status usw. zeigen weiterhin den aktuellen Netzwerkstatus an.



Router für alle Hosts in einer Gruppe
Wenn diese Option ausgewählt ist, wird der Host zum dedizierten Router für alle Hosts in der gleichen EventSentry Gruppe.

Router für ein oder mehrere Subnetze
Wenn dieses Kontrollkästchen aktiviert ist, wird der Host zum dedizierten Router für alle Hosts im angegebenen Subnetz bzw. in den angegebenen Subnetzen. Wenn das angegebene Subnetz beispielsweise 192.168.8.0/24 ist und der dedizierte Router offline wird, werden Ereignisprotokoll-Alarme für alle Hosts im IP-Bereich von 192.168.8.1 bis 192.168.8.254 unterdrückt (solange der Router offline ist). Geben Sie die Netzwerkmaske in CIDR-Notation an.

Die folgende Tabelle zeigt, welche Art von Warnungen erzeugt werden, wenn ein Router nicht mehr verfügbar ist:

Computer	Router	Netzwerk-Status	Ereignisprotokoll	Heartbeat-Status	Heartbeat-History
ROUTER	Ja	Host Down	Ja	Ja	Ja
GASTGEBER 1	Nein	Unbekannt	Nein	Ja	Ja
GEISEL2	Nein	Unbekannt	Nein	Ja	Ja

5.9.7 Setting Maintenance Schedules

Wartungspläne sind nützlich, wenn Server oder Geräte, die durch den Heartbeat-Agenten überwacht werden, geplante Ausfallzeiten haben, während derer keine Warnungen z.B. per E-Mail oder Pager gesendet werden sollten. EventSentry unterstützt zwei Arten von Wartungsplänen:

- Unverzüglich: Setzt einen Host sofort in einen Wartungsplan ein, entweder für X Minuten/Stunden/Tage oder bis zu einer bestimmten Zeit. Diese Aktion kann nur auf einen einzelnen Host angewendet werden.
- Feste Zeitpläne: Sie geben ein Startdatum/eine Startzeit und ein Enddatum/eine Endzeit an, zu denen ein Gerät planmäßig offline sein soll.
- Wiederkehrende Zeitpläne: Sie können einen Wochentag (z. B. Samstag) oder einen Tag des Monats (z. B. den 4.) angeben, an dem ein Gerät offline sein soll.

Wartungspläne können angewendet werden auf

- Einzelne Computer
- Heartbeat Gruppen

Wartungspläne betreffen nur Heartbeat-Alerts, die in das Ereignisprotokoll der Anwendung geschrieben werden. Statusänderungen werden weiterhin der Heartbeat-Historie hinzugefügt, auch wenn sie während eines Wartungsplans auftreten.

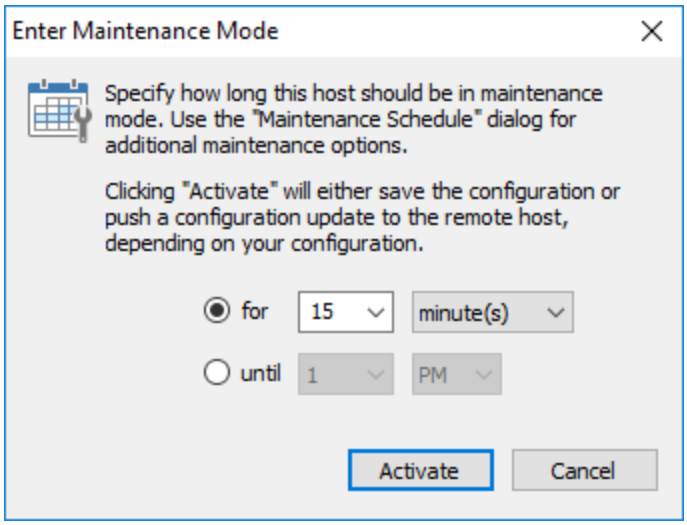
Zum Unterdrücken von E-Mail- und/oder Pager-Benachrichtigungen, die von einem Agenten während eines Wartungsplans gesendet werden, siehe Wartungspläne für Agenten festlegen.

Maintenance Now

Ein einzelner Host kann mit der Funktion "Maintenance Now", die über den Ribbon oder das Kontextmenü aufgerufen werden kann, sofort in den Wartungsmodus wechseln. Mit dieser Aktion stehen zwei Wartungsoptionen zur Verfügung:

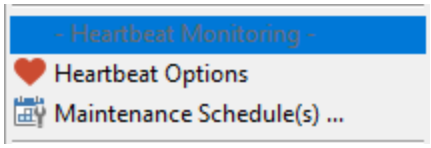
- Wechseln Sie in den Wartungsmodus für eine Anzahl von Minuten, Stunden oder Tagen.
- Eintritt in den Wartungsmodus bis zu einer festgelegten Stunde - bis zu 23 Stunden in die Zukunft. Die gewählte Stunde gilt für den nächsten Tag wenn sie vor der aktuellen Stunde liegt.

Es ist nicht notwendig, die Konfiguration zu speichern oder zu verschieben, wenn "Wartung jetzt" angegeben ist. Die Konfiguration wird automatisch gespeichert und bei Bedarf an den Remote-Host verschoben.

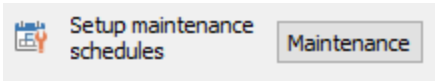


Wartungspläne anzeigen

Klicken Sie mit der rechten Maustaste auf die Gruppe oder den Computer-Container und wählen Sie "Maintenance Schedule(s) ...".

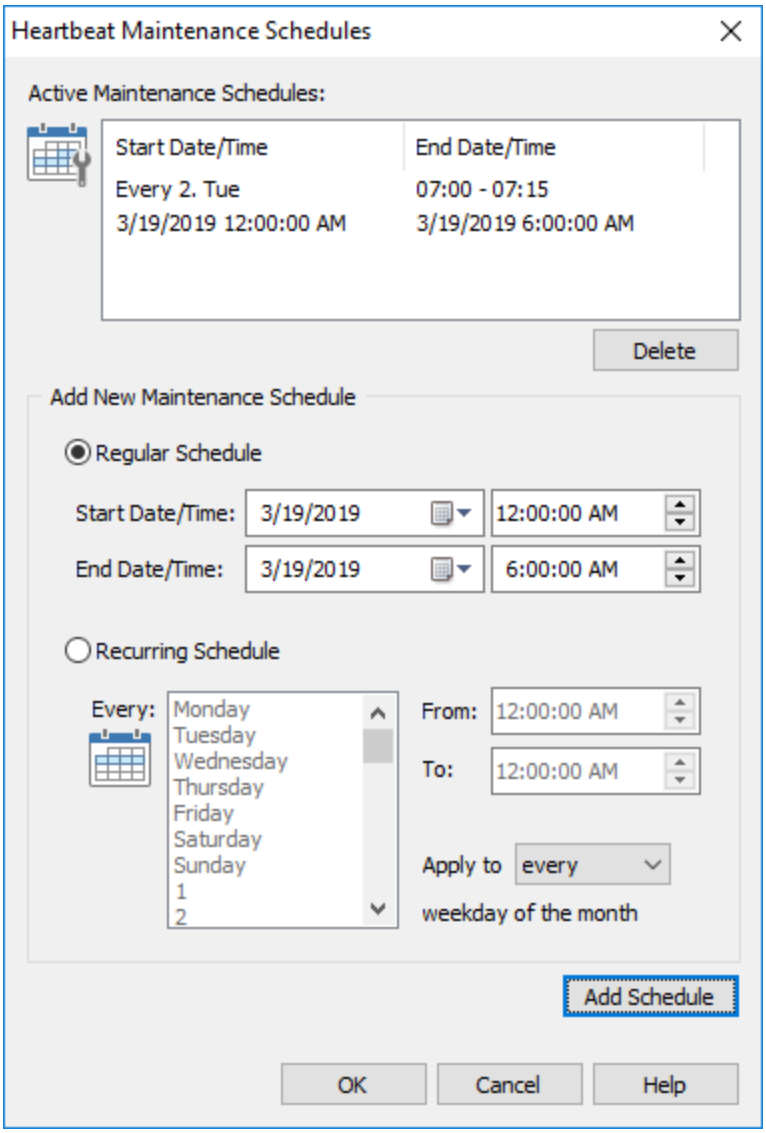


oder klicken Sie auf die Schaltfläche "Wartung" im Dialogfeld "Heartbeat Optionen" einer Gruppe oder eines Computers:



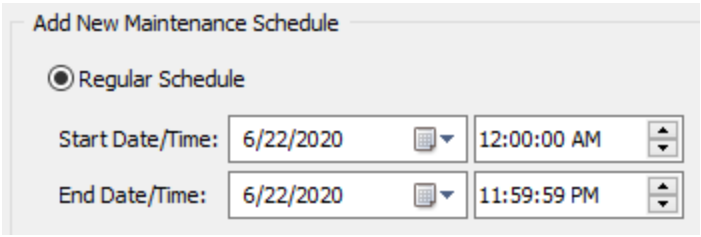
Hinzufügen von Wartungsplänen

Im Dialogfeld "Heartbeat Maintenance Schedules" können Sie Wartungspläne anzeigen, hinzufügen und entfernen:



Um einen regelmäßigen Zeitplan hinzuzufügen, geben Sie das Start- und Enddatum und die Uhrzeit an und klicken Sie auf die Schaltfläche Hinzufügen. Um einen wiederkehrenden Zeitplan hinzuzufügen, geben Sie entweder einen oder mehrere Wochentage oder einen oder mehrere Tage des Monats an.

Um einen ganzen Tag abzudecken, muss die Startzeit auf **12:00:00 Uhr morgens** und die Endzeit auf **11:59:59 Uhr abends** eingestellt werden, wie unten dargestellt:



Auf den n-ten Wochentag des Monats anwenden

Wartungspläne können nur auf den n-ten Tag eines Monats angewendet werden (im Gegensatz zu jedem Wochentag), indem Sie den 1., 2., 3., 4. oder 5. aus der Dropdown-Liste auswählen. Wählen Sie "jeder", wenn der Wartungsplan auf jeden Wochentag angewendet werden soll (Standardeinstellung).

Entfernen von Wartungsplänen

Bestehende Wartungspläne können gelöscht werden, indem man sie aus der Liste der aktiven Wartungspläne auswählt und auf "Löschen" klickt.

5.9.8 Event Log

Die folgenden Ereignisse werden vom Heartbeat Agent mit der Ereigniskategorie **Netzwerküberwachung** protokolliert.

Event ID	Event Description	Example / Description
11000	Host %1 (%2) changed its PING status from %3 to %4. The reason for the status change was: "%5".	Host www.competition.com (BigBrother) changed its PING status from OK to ERROR. The reason for the status change was: "100% packets missing".
11001	Host %1 (%2) changed its AGENT status from %3 to %4. The reason for the status change was: "%5".	Host DC1 (DomainControllers) changed its AGENT status from OK to ERROR. The reason for the status change was: "Agent Stopped".
11002	Host %1 (%2) changed its TCP status from % 3 to %4. The reason for the status change was: "%5".	Host mail.yourdomain.com (DMZ) changed its TCP status from OK to ERROR. The reason for the status change was: "Unable to establish a TCP connection (10060) (TCP Port: 25)".
11005	The EventSentry Heartbeat monitor is ready and will now start monitoring the configured hosts.	The EventSentry Heartbeat monitor is ready and will now start monitoring the configured hosts.
11006	The EventSentry Heartbeat agent was unable to find the required HTML template files in % 1\Heartbeat. Please make sure that the following files exist in %1\Heartbeat: template_status_start.html template_history_start.html template_end.html image subdirectory These files are optional if you are already logging heartbeat information to a database.	The EventSentry Heartbeat agent was unable to find the required HTML template files in C: \Program Files\Heartbeat. Please make sure that the following files exist in C:\Program Files\Heartbeat: template_status_start.html template_history_start.html template_end.html image subdirectory These files are optional if you are already logging heartbeat information to a database.
11007	The EventSentry Heartbeat agent was unable to find the required HTML template files and is not configured to log heartbeat status information to a database. The heartbeat agent will only notify you of host status changes through the event log.	The EventSentry Heartbeat agent was unable to find the required HTML template files and is not configured to log heartbeat status information to a database. The heartbeat agent will only notify you of host status changes through the event log.

11008	The database action specified for the heartbeat monitoring service is invalid and database logging has been disabled. Please review the configuration and restart the heartbeat monitoring service.	The database action specified for the heartbeat monitoring service is invalid and database logging has been disabled. Please review the configuration and restart the heartbeat monitoring service.
11009	The Heartbeat Monitor detected that the EventSentry service is currently not running. If the EventSentry service is not running, then event log alerts generated by the Heartbeat Agent cannot be forwarded to a notification. You can disable this check under "Global Options -> Heartbeat".	*is event indicates that the EventSentry agent not currently running, and thus not able to spatch any heartbeat alerts.*
11010	The EventSentry Heartbeat service encountered an unrecoverable error and will now automatically restart. If you see this message on a regular basis, then set the "Debug Level" under "Heartbeat" to "High" and contact support@netikus.net the next time this message is generated.	*is acceptable to observe this event on casion, but a frequent occurrence (e.g. once day) should be reported to our support team r investigation.*
11011	Scanning of host %1 was forcefully aborted because the scan duration (%3) exceeded the maximum allowed time (%2 seconds). Review the monitoring settings of this host, and optionally disable Agent and/or TCP checks on this host.	*order to monitor all configured hosts in a nely fashion and thus dispatch alerts as soon they occur, the heartbeat monitor limits the ne it takes to monitor a single remote host. If is time is exceeded, scanning of the remote st is aborted and this error is logged.* *eview this error and optionally exclude certain atures from being monitored (e.g. SNMP, ent status or TCP).*
11012	Scanning of host %1 was interrupted %4 consecutive times because the scan duration (%2) exceeded the maximum allowed time (% 3 seconds). TCP Port and/or SNMP scanning may be incomplete on this host.	*dicates that a host scan had to be aborted ultiple, consecutive times and that its hosts atus may be incomplete.*
11014	SNMP monitoring of host %1 has failed %2 consecutive times and is now disabled. To re-enable SNMP monitoring of host %1, restore SNMP connectivity and restart the EventSentry Heartbeat Monitor service.	*dicates that SNMP monitoring for a host has en disabled because the heartbeat monitor s unable to obtain any SNMP data from the mote host.*
11015	SNMP or agent monitoring of host %1 has failed %2% of the time over the last %3 seconds and is now disabled. To re-enable SNMP and/or agent monitoring of host %1, restore full connectivity to the remote host, locate the host in the management console and click the "Retry" button in the summary view.	*dicates that SNMP monitoring has been rmanently disabled and needs to be anually re-activated through the management nsole.*

11016	The following error occurred while communicating, or attempting to communicate with database action "%1": "%2". Please verify that the database is accessible and the database is on the latest schema.	*dicates an error while trying to store data in e EventSentry database. Run the nfiguration assistant to ensure that all tabase are on the latest schema.*
11017	The connection with database action "%1" has been reestablished, the database is no longer offline.	*dicates that a previously unavailable tabase is now available.*
11018	Starting with EventSentry build 3.2.1.28, the heartbeat agent can query the EventSentry database to determine a remote agent status, instead of querying the remote agent status using the Windows API. This can drastically improve the monitoring speed and is recommended for networks consisting of 50 or more Windows hosts.	Click here for more information.
11019	Monitoring of the remote EventSentry agent on host %1 has been unsuccessful %2 times in a row. Remote agent monitoring will now be disabled on host %1.	*nitoring of a remote agent failed too many nes and is now disabled.*
11020	The heartbeat agent will monitor the following host using SNMP: Host: %1 SNMP Version: %2 System Description: %3	The heartbeat agent will monitor the following host using SNMP: Host: 192.168.73.43 SNMP Version: 2c System Description:ProCurve J9021A Switch 2810-24G, revision N.15.09, ROM N.12.03 (/sw/code/build/bass(bh7))
11050	The PING status of host %1 (%2) remains at %4 due to error "%5".	The PING status of host mail.somedomain.com (Heartbeat Hosts) remains at ERROR due to error "100% packets missing".
11051	The AGENT status of host %1 (%2) remains at %4 due to error "%5".	The AGENT status of host DC1 (DomainControllers) remains at ERROR due to error "Agent Stopped".
11052	The TCP status of host %1 (%2) remains at % 4 due to error "%5".	The TCP status of host mail.yourdomain.com (DMZ) remains at ERROR due to error "Unable to establish a TCP connection (10060) (TCP Port: 25)".

5.10 Netzwerk-Dienste

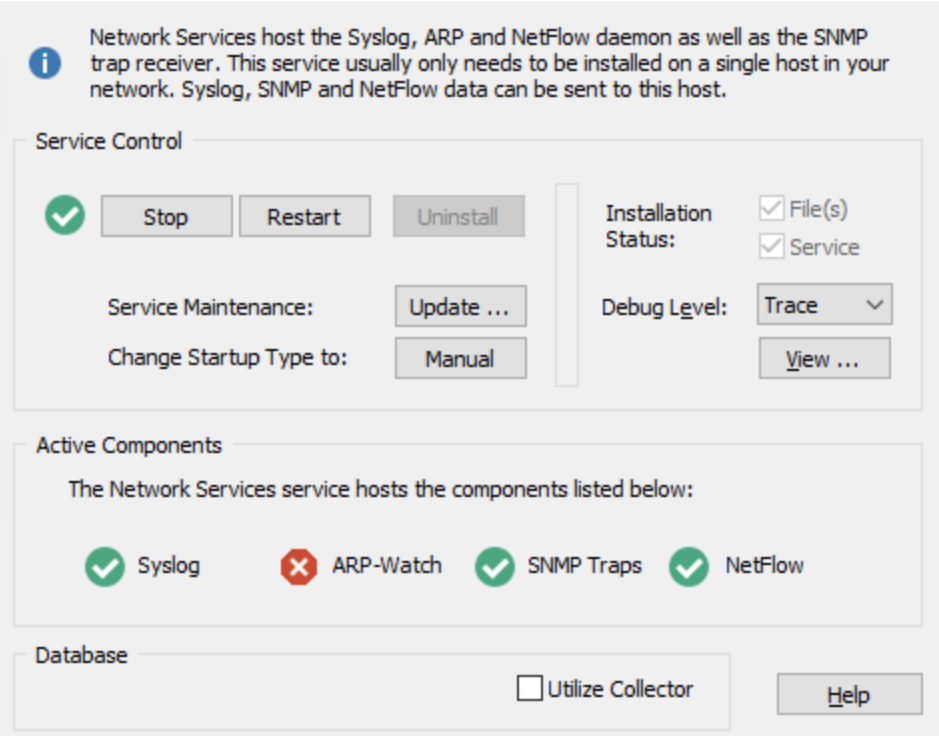
Die Netzwerkdienste-Funktion, die als separater Windows-Dienst läuft ("EventSentry Network Services"), enthält die folgenden Komponenten:

- Syslog daemon
- SNMP Trap daemon
- ARP daemon
- NetFlow collector

Daher muss der Dienst "EventSentry Network Services" installiert und ausgeführt werden, wenn eine der oben genannten Komponenten verwendet wird.

1. Installieren des Dienstes "Netzwerkdienste"

Der Dienst wird normalerweise während des Setups installiert, wenn Syslog- oder SNMP-Funktionalität angefordert wird. Der Dienst kann auch manuell in der Verwaltungskonsole installiert werden, indem Sie zu "Netzwerkdienste" navigieren und auf die Schaltfläche "Installieren" klicken.



2. Anforderungen

Betriebssystem: Das korrekte Microsoft® Visual C++ Redistributable muss installiert sein, damit der Dienst gestartet werden kann (ist standardmäßig installiert). Siehe Anforderungen für weitere Informationen.

Lizenzierung: Es müssen mindestens 5 Host-Heartbeat-/Netzwerkgeräte-Lizenzen installiert sein, damit der Dienst starten und Netzwerkpakete akzeptieren kann. Für Evaluationslizenzen gilt diese Anforderung nicht.

3. Debug-Ebene

Sie können einen Debug-Level zur Fehlerbehebung festlegen, z.B. auf Anweisung des EventSentry-Supports. Die folgenden Debug-Level sind verfügbar:

- Keine
- Fehler
- Warnung
- Infos
- Fehlersuche
- Trace (die meisten)

Es wird nicht empfohlen, die Debug- oder Trace-Protokollierungsebenen zu aktivieren, es sei denn, dies wird vom NETIKUS.NET-Support angewiesen.

4. Aktive Komponenten

Dieser Bereich zeigt, welche Komponenten innerhalb der Netzwerkdienste aktiv laufen. Ein grünes Häkchen zeigt an, dass die Komponente aktiv ist, während ein "X" anzeigt, dass die Komponente inaktiv ist.

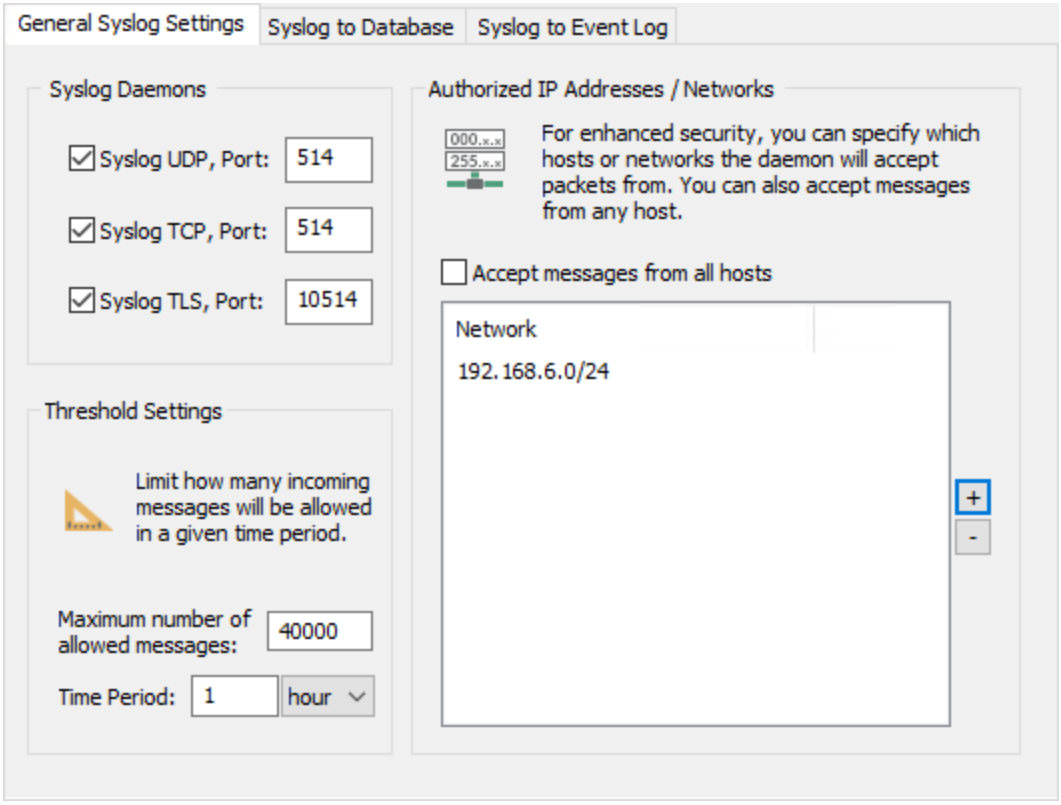
5. Datenbank

Verwenden Sie den Collector: Wenn ein Collector verfügbar ist und die Netzwerkdienste in einem Netzwerk installiert sind, das keine direkte Verbindung zur ausgewählten Datenbank hat, konfiguriert die Aktivierung dieser Option die Netzwerkdienste so, dass sie alle Daten über den Collector senden. Diese Option ist standardmäßig deaktiviert und sollte nur in Szenarien im MSP-Stil aktiviert werden.

5.10.1 Syslog Daemon

EventSentry kann einen Unix-/Linux-Syslog-Server emulieren, der es ihm ermöglicht, Syslog-Nachrichten von Syslog-fähigen Hosts und Geräten zu empfangen. Der Syslog-Dämon unterstützt UDP-, TCP- und TCP+TLS-Verbindungen, und Sie können eingehende Syslog-Nachrichten entweder im Ereignisprotokoll der Anwendung protokollieren oder in einer Datenbank speichern.

Um den Syslog-Dämon zu aktivieren, aktivieren Sie eines der Kontrollkästchen im Abschnitt **Syslog-Dämonen** auf der Registerkarte "General Syslog Settings" und konfigurieren Sie entweder die Datenbank- oder die Ereignisprotokollfunktion.



Syslog-Daemon

Der Syslog-Dämon kann UDP- und TCP-Verbindungen von entfernten Syslog-fähigen Geräten annehmen. Um eines der beiden Protokolle zu aktivieren, markieren Sie das entsprechende

Kontrollkästchen. Der Standardport für das Syslog-Protokoll ist 514, kann aber zur Verwendung eines benutzerdefinierten Ports angepasst werden.

TCP + TLS
Erstellt automatisch eine selbstsignierte Zertifikatsdatei, wenn die Funktion zum ersten Mal aktiviert wird, um die TLS-Kommunikation zu ermöglichen. Erstellt die folgenden Dateien:

- **%SYSTEMROOT%\system32\eventsentry\secure\es_network_svc.pfx**
- **%SYSTEMROOT%\system32\eventsentry\secure\es_network_svc.pem** (öffentliches Zertifikat zur Verteilung)

Die öffentliche PEM-Datei kann auf entfernte Syslog-Clients kopiert werden, die diese Datei benötigen, um der selbstsignierten Zertifikatsdatei zu vertrauen.

Schwellenwert-Einstellungen
Um die Anzahl der Syslog-Meldungen, die vom Syslog-Daemon verarbeitet werden, zu begrenzen, ändern Sie die maximale Anzahl von Meldungen und den anwendbaren Zeitraum. Der Syslog-Dämon verwirft eingehende Pakete, wenn die Anzahl die unter Maximale Anzahl zulässiger Nachrichten für den Konfigurationszeitraum angegebene Anzahl überschreitet.

Autorisierte IP-Adressen / Netzwerke
Für erhöhte Sicherheit kann der Syslog-Dämon so konfiguriert werden, dass er nur Pakete von bestimmten IP-Adressen und/oder Netzwerken akzeptiert. Hostnamen sind in der Liste nicht erlaubt, es können nur IP-Adressen angegeben werden.

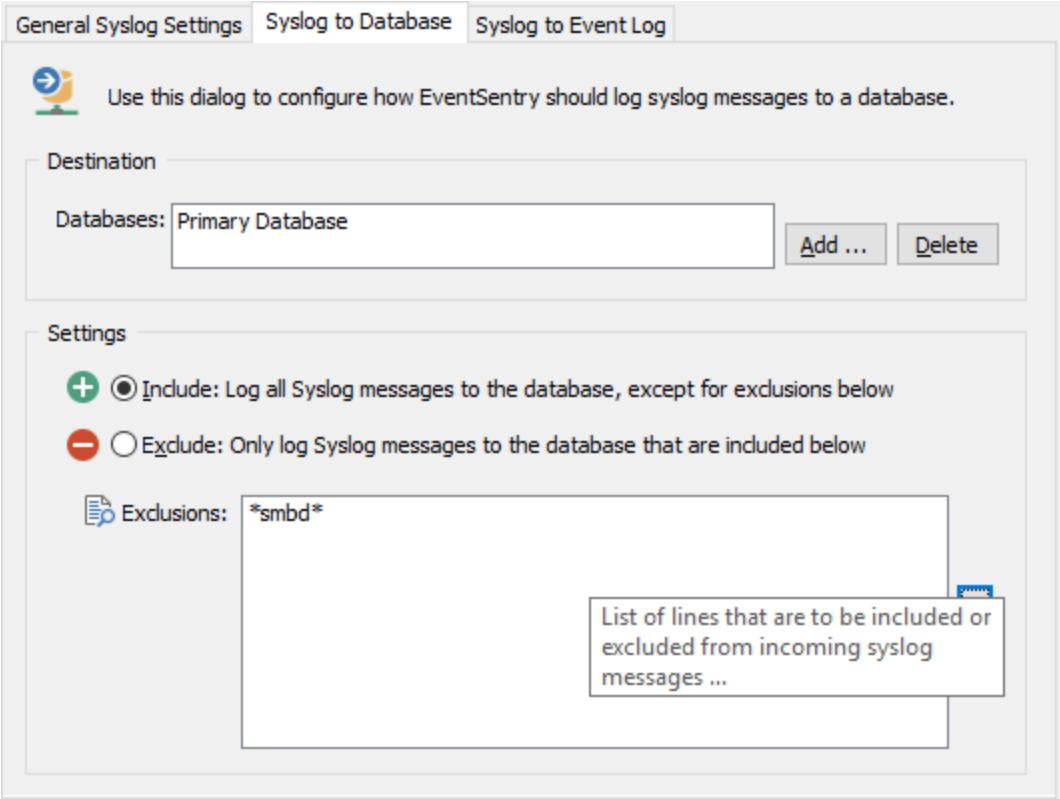
IP-Adressen können mit oder ohne Angabe der Subnetzbits eingegeben werden. Wenn Sie z.B. nur zwei Server mit den IP-Adressen 184.23.22.11 und 184.23.22.43 hinzufügen möchten, fügen Sie einfach diese beiden IP-Adressen der Liste hinzu.

Um ein ganzes Subnetz zu autorisieren, zum Beispiel die IP-Adressen 184.23.22.1 - 184.23.22.254, fügen Sie 184.23.22.0/24 hinzu. Um nur den Bereich von 184.23.22.128 - 184.23.22.22.254 zuzulassen, geben Sie dann 184.23.22.128/25 an.

Kompatibilität
Der EventSentry Syslog-Dämon funktioniert mit jedem Unix-Syslog-Dämon (jeder Linux-, Solaris-, OSX-, ...) und Netzwerkgeräten, die das Syslog RFC 3164-Protokoll unterstützen.

5.10.1.1 Datenbank-Konsolidierung

Der Syslog-Dämon kann so konfiguriert werden, dass er eingehende Pakete in eine Datenbank auf der Registerkarte "Syslog zur Datenbank" schreibt, wo eine oder mehrere Datenbanken durch Klicken auf die Schaltfläche "Hinzufügen" zur Liste hinzugefügt werden können.



Einstellungen

Standardmäßig werden alle empfangenen Syslog-Nachrichten an die angegebene(n) Datenbank(en) gesendet. Um dieses Verhalten zu ändern, können bestimmte Nachrichten vom Hinzufügen zur Datenbank ausgeschlossen werden (alle einschließen, einige ausschließen), oder es können nur bestimmte Syslog-Nachrichten an die Datenbank gesendet werden.

Einschließen: Protokollierung aller Syslog-Meldungen in der Datenbank, mit Ausnahme der folgenden Ausschlüsse

Dies ist die Standardeinstellung und sendet alle Syslog-Meldungen an die Datenbank. Syslog-Meldungen, die Zeichenketten enthalten, die unten aufgelistet sind, werden gefiltert, um unnötige Nachrichten zu reduzieren, Wildcards werden unterstützt.

Ausschließen: Nur Syslog-Meldungen in die Datenbank protokollieren, die unten aufgeführt sind

Diese Einstellung ist restriktiver und sendet nur Syslog-Meldungen an die Datenbank, die den aufgeführten Filtern entsprechen; Platzhalter werden unterstützt.

> Weitere Einzelheiten über die Filtersyntax werden im Kapitel "Syslog zum Ereignisprotokoll" erläutert.

5.10.1.2 Syslog zum Ereignisprotokoll

Eingehende Syslog-Pakete können im Ereignisprotokoll protokolliert werden, um Echtzeitwarnungen, z.B. per E-Mail, zu erleichtern. Die Funktion wird auf der Registerkarte "Syslog to Event Log" mit dem Kontrollkästchen "Log to the APPLICATION event log" aktiviert. Da das Syslog-Protokoll 8 verschiedene Schweregrade unterstützt (im Vergleich zu nur 3 für das Windows-Ereignisprotokoll), muss eine Zuordnung der Schweregrade konfiguriert werden.

EventSentry protokolliert alle Meldungen im Anwendungsereignisprotokoll mit der Ereignis-ID 500 und der Ereignisquelle **EventSentry Network Services**.

Schweregrad-Abbildung

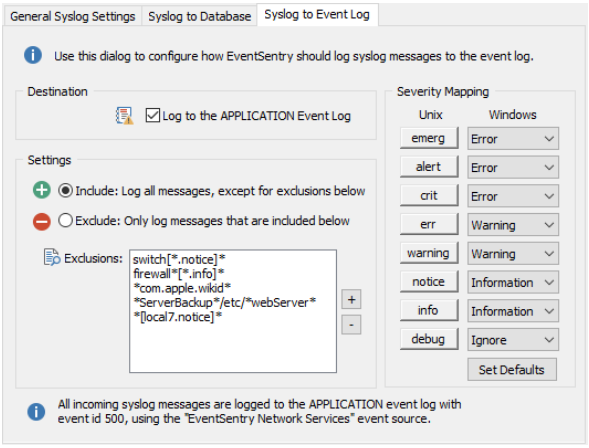
Konfiguriert die Zuordnung zwischen Syslog-Schweregraden und Windows-Ereignisprotokoll-Schweregraden.

Unix Syslog defines eight severity levels:

- EMERG *Emergency*
- ALERT *Alert*
- CRIT *Critical*
- ERR *Error*
- WARNING *Warning*
- NOTICE *Notice*
- INFO *Info*
- DEBUG *Debug*

The Windows event log defines only three severities (*SUCCESS* is not mentioned since it is basically equivalent to *INFORMATION*):

- ERROR
- WARNING
- INFORMATION
- Ignore (does not log message to the event log)



Um zu verhindern, dass eine bestimmte Fehlerstufe (z.B. Debug) in das Windows-Ereignisprotokoll geschrieben wird, geben Sie **Ignorieren** in der entsprechenden Windows-Spalte an. Dadurch werden alle Pakete in der angegebenen Fehlerstufe verworfen, ohne sie im Ereignisprotokoll zu protokollieren.

Einstellungen

Standardmäßig werden keine eingehenden Syslog-Meldungen in das Ereignisprotokoll aufgenommen. Durch Klicken auf das Symbol + werden der Liste zusätzliche Filter hinzugefügt (siehe unten für Filtersyntax und Beispiele). Wildcards * und ? werden unterstützt.

Include: Log all messages to the event log, except for exclusions below

Diese Einstellung protokolliert alle Syslog-Meldungen im Ereignisprotokoll. Syslog-Meldungen, die Zeichenfolgen enthalten, die unten aufgelistet sind, werden ausgeschlossen.

Exclude: Only log messages to the database that are included below

Dies ist die Standardeinstellung und protokolliert im Ereignisprotokoll nur Syslog-Meldungen, die den aufgeführten Filtern entsprechen.

Syntax

Syslog-Nachrichtenfilter werden mit dem folgenden Syslog-Format verglichen:

hostname[facility.severity]: content
ipaddress[facility.severity]: content

hostname: The host name of the remote host, if the remote IP address as was able to be resolved to a host name
ipaddress: The IP address of the remote host, if the host name could not be resolved with a reverse lookup
facility: The Syslog facility, e.g. auth, cron, kern, etc.
severity: The Syslog severity, e.g. emerg, alert, crit, etc.
content: The actual content of the Syslog message

Beispiele:

```
firewall01.prod.local[kern.crit]: Invalid login from 11.32.23.111
192.1.3.4[cron.notice]: /USR/SBIN/CRON[26051]: (root) CMD ( cd / && run-parts --report /etc/cron
ubuntu-box[authpriv.notice]: sudo: root : TTY=unknown ; PWD=/ ; USER=administrator ; COMMAND=/us
```

Beispiel-Filter

- Vergleichen Sie alle "Info"-Schweregrade von Hosts, die mit "Firewall" beginnen: **firewall*[*.info]***
- Überprüfen Sie alle Nachrichten, die "com.apple.wikid" enthalten: ***com.apple.wikid*: *com.apple.wikid***
- Vergleichen Sie alle Nachrichten aus der Einrichtung "local7" mit dem Schweregrad "Hinweis": ***[local7.notice]***
- Alle Nachrichten von Hosts aus dem Subnetz 192.1.1.0/24 kommen: **192.1.1.***

5.10.1.3 Unix/Linux Konfiguration

Bevor Unix-/Linux-Hosts Syslog-Meldungen an EventSentry senden können, müssen sie dafür konfiguriert werden. Die Hauptkonfigurationsdatei für die meisten Unix-Varianten ist **syslog.conf**, die sich normalerweise im Verzeichnis **/etc** befindet. Für Ubuntu-basierte Systeme muss die Datei **/etc/rsyslog.d/50-default.conf** bearbeitet werden.

Da sich die Syntax für diese Datei von Unix-Version zu Unix-Version leicht unterscheidet, wird EventSentry nur die RedHat© Linux-Konfiguration abdecken. Alle unten aufgeführten Aktionen werden unter Linux durchgeführt.

1. Stellen Sie sicher, dass Sie den Host, auf dem EventSentry läuft, von Ihrem Unix-/Linux-Rechner aus anpingen können. Falls nicht, aktualisieren Sie die Datei **/etc/hosts** oder bitten Sie Ihren Namensdienstleister, die Änderung für Sie vorzunehmen.

2. Bearbeiten Sie die Datei **/etc/syslog.conf** und fügen Sie die folgende Zeile hinzu

```
*.debug                @your host name
```

Sie müssen diese Zeile mit der richtigen Anzahl von Tabs formatieren.

***.debug** ist ein extremes Beispiel und wird Ihnen jede einzelne Nachricht aus der Linux-Box schicken. Sie können dies reduzieren, indem Sie eine höhere Ebene wie ***.notice** wählen. Der Syslog-Daemon wird Ihnen alle Nachrichten ab der angegebenen Ebene und höher senden, aber nicht von den niedrigeren. Natürlich können Sie auch die Einrichtung (wie **Kern** oder **Mail**) angeben. Bitte lesen Sie die Syslog-Manpage für weitere Details zur Konfiguration von **syslog.conf**.

3. Starten Sie den Syslog-Dämon mit dem folgenden Kommando neu: **/etc/init.d/syslog restart**

4. Einige Unix-Betriebssysteme werden mit einem Kommandozeilen-Dienstprogramm namens **Logger** geliefert, mit dem Sie Ihre eigenen Log-Einträge erstellen können, was für das Testen nützlich sein kann. Unter Linux können Sie Folgendes eingeben

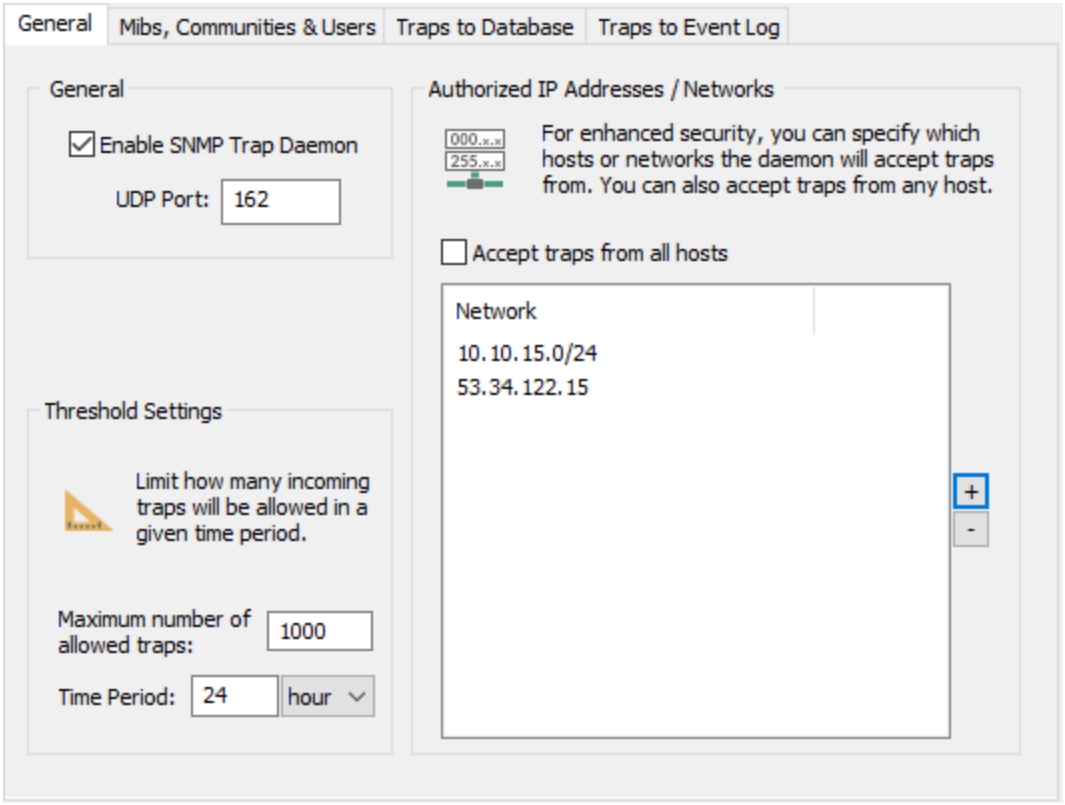
```
logger -p auth.notice TESTMESSAGE
```

um eine Nachricht mit dem Inhalt "TESTMESSAGE" für die **Berechtigungs-** und **Schweregradnachricht** der Einrichtung zu erstellen. Bitte prüfen Sie in der Dokumentation Ihres Betriebssystems, ob das gleiche oder ein ähnliches Dienstprogramm enthalten ist. Bitte beachten Sie auch, dass die Syntax für diesen Befehl auf verschiedenen Plattformen unterschiedlich sein kann.

5.10.2 Snmp Trap Daemon

EventSentry kann SNMP v1-, v2c- und v3-Traps von entfernten Netzwerkgeräten empfangen. Der SNMP-Trap-Daemon kann eingehende Traps entweder im Ereignisprotokoll der Anwendung protokollieren oder in einer Datenbank speichern.

Um den SNMP-Trap-Daemon zu aktivieren, aktivieren Sie das Kontrollkästchen **SNMP-Trap-Daemon aktivieren** auf der Registerkarte "Allgemein" und konfigurieren Sie entweder die **Datenbank-** oder die Ereignisprotokollfunktion. Der Standard-SNMP-Port ist 162, kann aber auf einen anderen Port geändert werden.



Schwellenwert-Einstellungen

Um die Anzahl der eingehenden Traps, die vom Dämon verarbeitet werden, zu begrenzen, ändern Sie die maximale Anzahl von Nachrichten und den anwendbaren Zeitraum. Der Dämon verwirft eingehende Pakete, wenn die Anzahl die unter Maximale Anzahl zulässiger Nachrichten für den Konfigurationszeitraum angegebene Anzahl überschreitet.

Autorisierte IP-Adressen / Netzwerke

Um die Sicherheit zu erhöhen, müssen Sie angeben, von welchen Hosts der Dämon Pakete annehmen wird. Bitte beachten Sie, dass Hostnamen in der Liste nicht erlaubt sind, Sie können nur IP-Adressen angeben.

IP-Adressen können mit oder ohne Angabe der Subnetzbits eingegeben werden. Wenn Sie beispielsweise nur zwei Server mit den IP-Adressen 184.23.22.11 und 184.23.22.43 hinzufügen möchten, fügen Sie diese beiden IP-Adressen einfach der Liste hinzu.

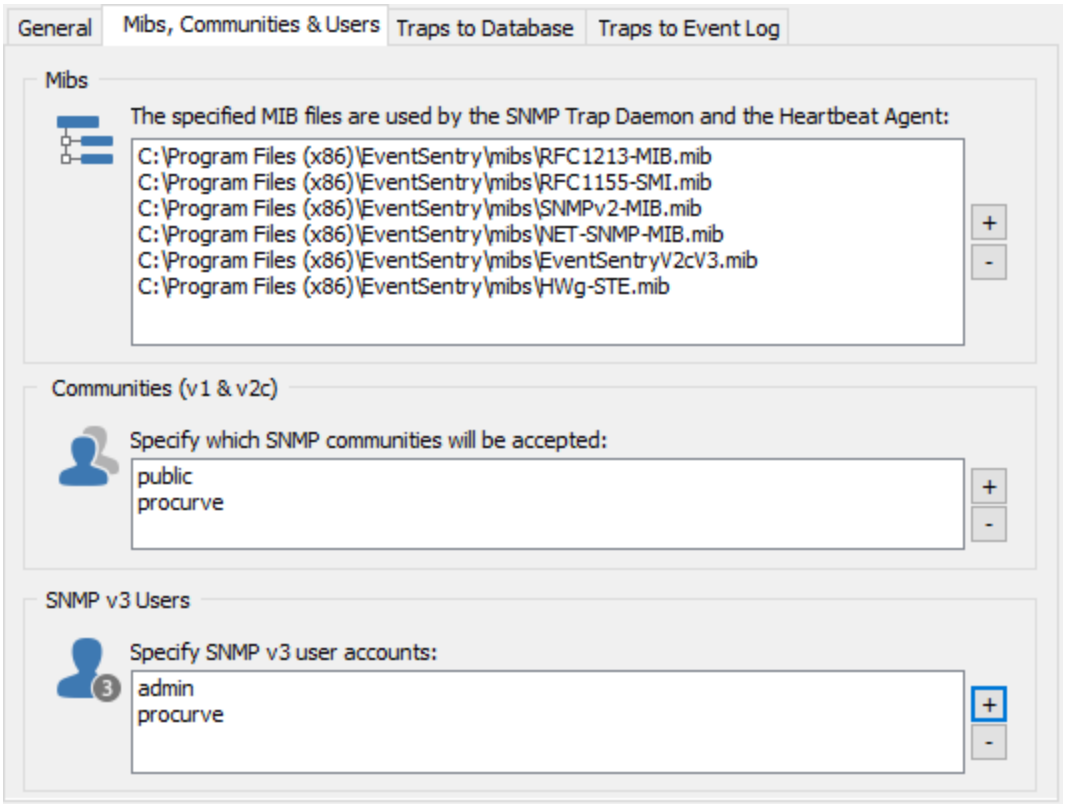
Um ein ganzes Subnetz zu autorisieren, zum Beispiel die IP-Adressen 184.23.22.1 - 184.23.22.254, fügen Sie 184.23.22.0/24 hinzu. Um nur den Bereich von 184.23.22.128 - 184.23.22.22.254 zuzulassen, geben Sie dann 184.23.22.128/25 an.

Kompatibilität

Der Dämon sollte mit jedem SNMP-kompatiblen Host arbeiten der v1, v2c oder v3 unterstützt.

5.10.2.1 Mibs, Communities & Benutzer

Die Registerkarte "Mibs, Communities & Benutzer" konfiguriert, welche MIB-Dateien geladen werden sollen, welche Communities akzeptiert werden sollen und konfiguriert auch SNMP v3-Benutzer.



Alle Felder können doppelt angeklickt werden, um vorhandene Werte zu bearbeiten.

Mibs

Damit OIDs korrekt interpretiert werden können, müssen MIBs konfiguriert werden, die mit den empfangenen Traps übereinstimmen. Welche MIBs zu laden sind, hängt davon ab, von welchen Geräten der Dämon Traps empfangen wird. Standard-MIBs können aus dem Internet heruntergeladen werden,

wohingegen herstellerspezifische MIBs in der Regel vom Hersteller bezogen werden, z.B. von der Website des Herstellers.

Sie können bis zu 128 MIB-Dateien angeben, beim Hinzufügen von MIBs können mehrere MIB-Dateien ausgewählt werden.

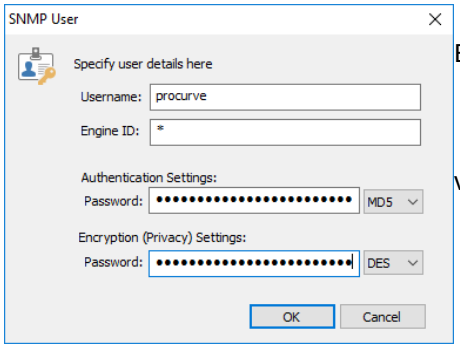
Stellen Sie sicher, dass sich alle hinzugefügten MIB-Dateien auf einem physischen Laufwerk und nicht auf einem Netzlaufwerk befinden und dass das Konto, unter dem der "Netzwerkdienste"-Dienst läuft ("LocalSystem" standardmäßig), über Berechtigungen zum Lesen der Datei(en) verfügt.

Gemeinschaften

SNMP v1- und v2c-Traps verwenden Community-Namen zur Authentifizierung; geben Sie hier Community-Namen an, für die Traps akzeptiert werden sollen. Traps, die einen Community-Namen verwenden, der nicht aufgeführt ist, werden verworfen.

SNMP v3-Benutzer

Eingehende v3-Traps müssen authentifiziert werden, um akzeptiert zu werden.



Benutzer von SNMP v3 unterstützen die folgenden Eigenschaften:

- Benutzername (erforderlich)
- EngineID (optional, eine normalerweise eindeutige Kennung vom Netzwerkgerät)
- Authentifizierungspasswort und -algorithmus
- Verschlüsselungspasswort und -algorithmus

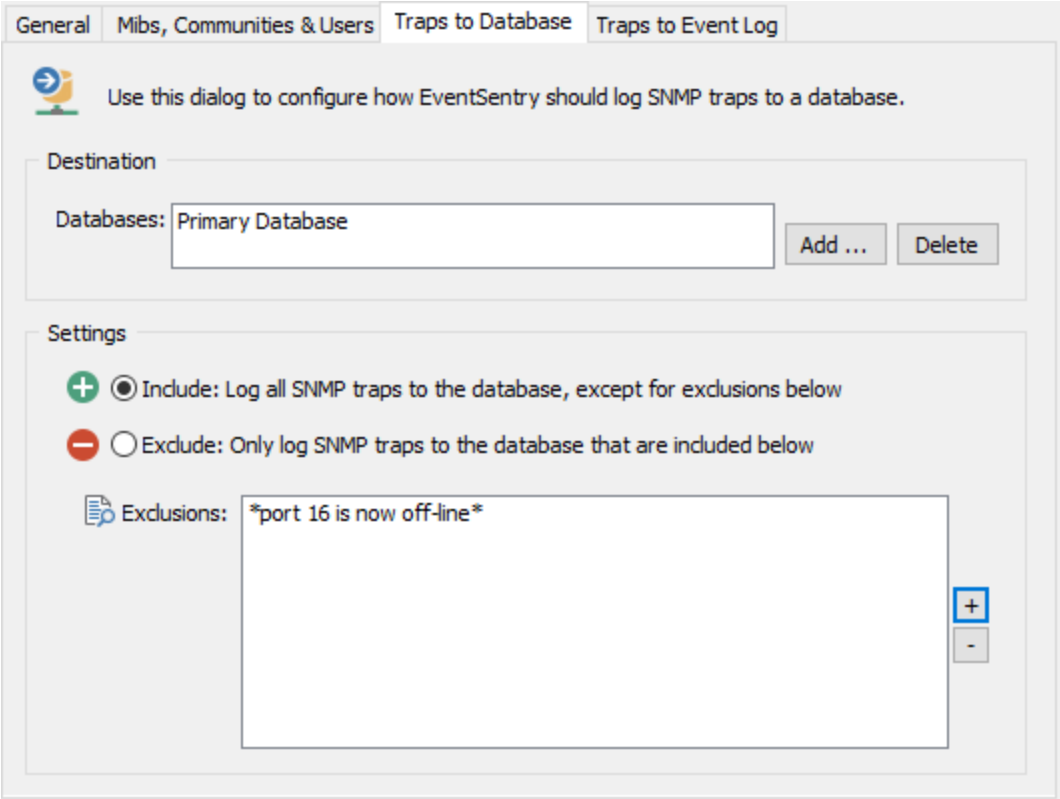
Authentifizierung und Verschlüsselung

Bei der Übertragung von SNMP v3-Traps über ein Netzwerk können Sie wählen, ob Sie sich authentifizieren möchten, um die Authentizität des Absenders sicherzustellen, und/oder ob Sie den Trap verschlüsseln möchten, um sicherzustellen, dass der Inhalt des Traps für Dritte nicht sichtbar ist. Die Verschlüsselung von Traps ist besonders wichtig bei der Übertragung von Traps über ein unsicheres Medium wie das Internet. Die folgenden Authentifizierungs- und Verschlüsselungsalgorithmen werden derzeit unterstützt:

Authentifizierung: MD5, SHA
Verschlüsselung: DES, AES, 3DES

5.10.2.2 Datenbank-Konsolidierung

Um Traps in einer Datenbank zu protokollieren, klicken Sie auf die Registerkarte "Traps zur Datenbank" und fügen Sie eine oder mehrere Datenbanken zur Liste der Datenbanken hinzu, indem Sie auf die Schaltfläche "Hinzufügen" klicken.



Einstellungen

Standardmäßig werden alle empfangenen SNMP-Traps an die angegebene(n) Datenbank(en) gesendet. Um dieses Verhalten zu ändern, können Sie entweder bestimmte Nachrichten vom Hinzufügen zur Datenbank ausschließen (alle einschließen, einige ausschließen) oder nur bestimmte SNMP-Traps an die Datenbank senden.

Include: Log all SNMP traps to the database, except for exclusions below

Dies ist die Standardeinstellung, und es werden alle Traps an die Datenbank gesendet. Traps, die unten aufgeführte Zeichenfolgen enthalten, werden nicht an die Datenbank gesendet. Auf diese Weise können Sie Platz in der Datenbank sparen, indem Sie nicht benötigte Nachrichten herausfiltern.

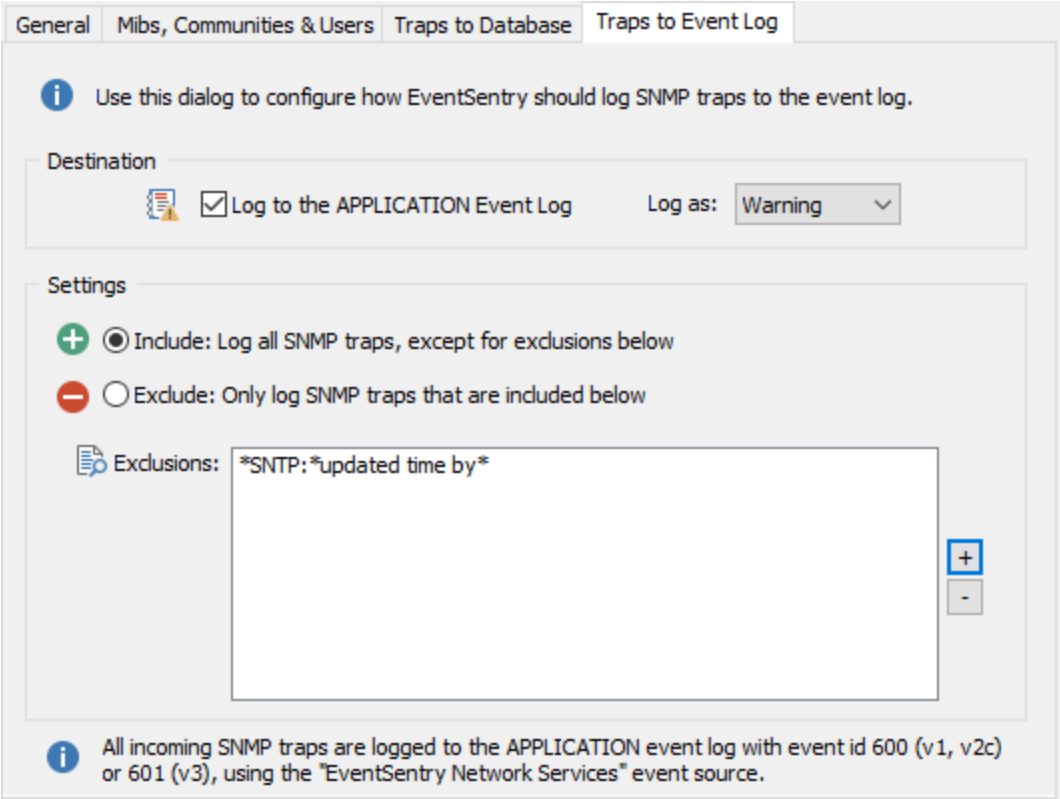
Exclude: Only log SNMP traps to the database that are included below

Diese Einstellung ist restriktiver und sendet nur SNMP-Traps an die Datenbank, die unten aufgeführt sind. Auf diese Weise können Sie nur Nachrichten an die Datenbank senden, die Ihren Filtern entsprechen.

Fügen Sie bei der Angabe einer teilweisen Textübereinstimmung vor und/oder nach dem Suchtext ein nachgestelltes Sternchen hinzu. EventSentry wertet die von Ihnen angegebenen Zeichenfolgen gegen die Trap-ID sowie die numerischen OIDs, Text-OIDs und die tatsächlichen Werte aller Trap-Bindungen aus.

5.10.2.3 Traps zum Ereignisprotokoll

Um SNMP-Traps im Ereignisprotokoll zu protokollieren, klicken Sie auf die Registerkarte "Traps zum Ereignisprotokoll", aktivieren Sie das Kontrollkästchen "Im Ereignisprotokoll der Anwendung protokollieren" und geben Sie den Schweregrad an, unter dem eingehende Traps protokolliert werden sollen.



EventSentry protokolliert alle Traps im Anwendungsereignisprotokoll mit den folgenden Ereigniseigenschaften:

SNMP Version	Event Source	Event ID
v1, v2c	EventSentry Network Services	600
v3	EventSentry Network Services	601

Einstellungen

Standardmäßig werden keine eingehenden SNMP-Traps im Ereignisprotokoll protokolliert. Klicken Sie auf das Symbol +, um Zeichenfolgen hinzuzufügen, die Alarme für das Ereignisprotokoll auslösen.

Include: Log all SNMP traps, except for exclusions below

Bei dieser Einstellung werden alle SNMP-Traps im Ereignisprotokoll aufgezeichnet. SNMP-Traps mit Zeichenfolgen, die unten aufgeführt sind, werden nicht im Ereignisprotokoll protokolliert.

Exclude: Only log SNMP traps that are included below

Dies ist die Standardeinstellung und protokolliert im Ereignisprotokoll nur SNMP-Traps, die mit den unten aufgeführten Zeichenfolgen übereinstimmen. Dadurch können Sie nur Inhalte an das Ereignisprotokoll senden, die mit Ihren Filtern übereinstimmen.

Fügen Sie bei der Angabe einer teilweisen Textübereinstimmung vor und/oder nach dem Suchtext ein nachgestelltes Sternchen hinzu. EventSentry wertet die von Ihnen angegebenen Zeichenfolgen gegen die Trap-ID sowie die numerischen OIDs, Text-OIDs und die tatsächlichen Werte aller Trap-Bindungen aus.

5.10.3 ARP Daemon

Die ARP-Daemon-Komponente hört den gesamten Netzwerkverkehr an einer oder mehreren Schnittstellen ab und bietet folgende Funktionalität

- Sammelt Statistiken über MAC-Adressen, die im Netzwerk verwendet werden
- Gibt Warnmeldungen aus, wenn neue MAC-Adressen gefunden werden
- Gibt Warnmeldungen aus, wenn die Zuordnungen von IP- und MAC-Adressen geändert werden

Der ARP-Daemon durchläuft eine anfängliche Lernperiode von 2 Wochen, nach der er davon ausgeht, dass er über eine brauchbare Grundlinie aller Netzwerkgeräte im Netzwerk verfügt und bei neu gefundenen MAC-Adressen einen Alarm auslöst (falls aktiviert).

Der ARP-Daemon benötigt einen WinPcap-kompatiblen Treiber, um den Netzwerkverkehr zu erfassen. Npcap ist derzeit der Treiber der Wahl, da sich der ursprüngliche WinPcap-Treiber nicht mehr in aktiver Entwicklung befindet.

WICHTIG: Stellen Sie bei der Installation sicher, dass "Install Npcap in WinPcap API-compatible Mode" markiert ist.

Merkmale

Statistik
Bietet Echtzeitinformationen über die Verwendung und Änderungen von MAC-Adressen.

- Wann wurde eine MAC-Adresse zum ersten und letzten Mal im Netzwerk gesehen?
- Mit welcher IP-Adresse ist eine MAC-Adresse verbunden?
- Mit mit mit Hostname ist eine MAC-Adresse verbunden?
- Mit welchem Anbieter ist eine MAC-Adresse verbunden?

Warnungen
Der ARP-Dämon liefert nicht nur statistische Informationen über das Netzwerk, sondern gibt auch unter folgenden Umständen Warnungen aus

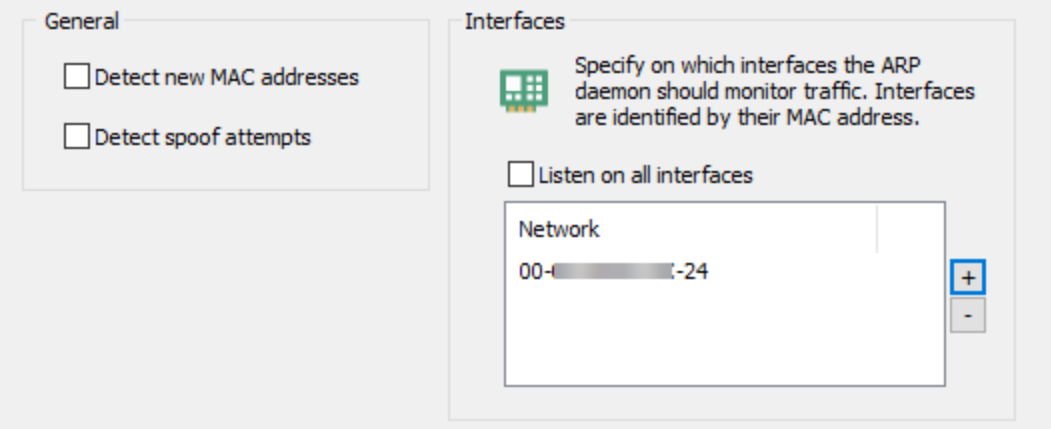
- Eine neue MAC-Adresse wurde außerhalb der anfänglichen Lernperiode entdeckt
- Eine MAC-Adresse registriert sich selbst mit einer IP-Adresse, die bereits mit einer anderen MAC-Adresse registriert ist (möglicher ARP-Spoof-Versuch)

Setup

Allgemein
Damit die ARP-Daemon-Komponente ausgeführt werden kann, muss entweder "Neue MAC-Adressen erkennen" oder "Spoof-Versuche erkennen" geprüft werden.

Netzwerkschnittstellen
Konfigurieren Sie, auf welcher(n) Schnittstelle(n) der ARP-Dämon auf Netzwerkverkehr lauschen soll, indem Sie eine oder mehrere MAC-Adressen angeben. Obwohl dies nicht unbedingt erforderlich ist, werden die besten Ergebnisse erzielt, wenn die Schnittstelle(n), die der ARP-Dämon abhört, mit einem Switch-Port verbunden ist (sind), der den gesamten Netzwerkverkehr des Switches empfängt. Ein Port auf dem Switch, der den gesamten Netzwerkverkehr empfängt (im Gegensatz zur Standardeinstellung,

bei der er nur Verkehr empfängt, der an die registrierten MAC-Adressen gerichtet ist), wird normalerweise als **Monitor-Port** bezeichnet.



5.10.3.1 Ereignisprotokoll & Datenbank

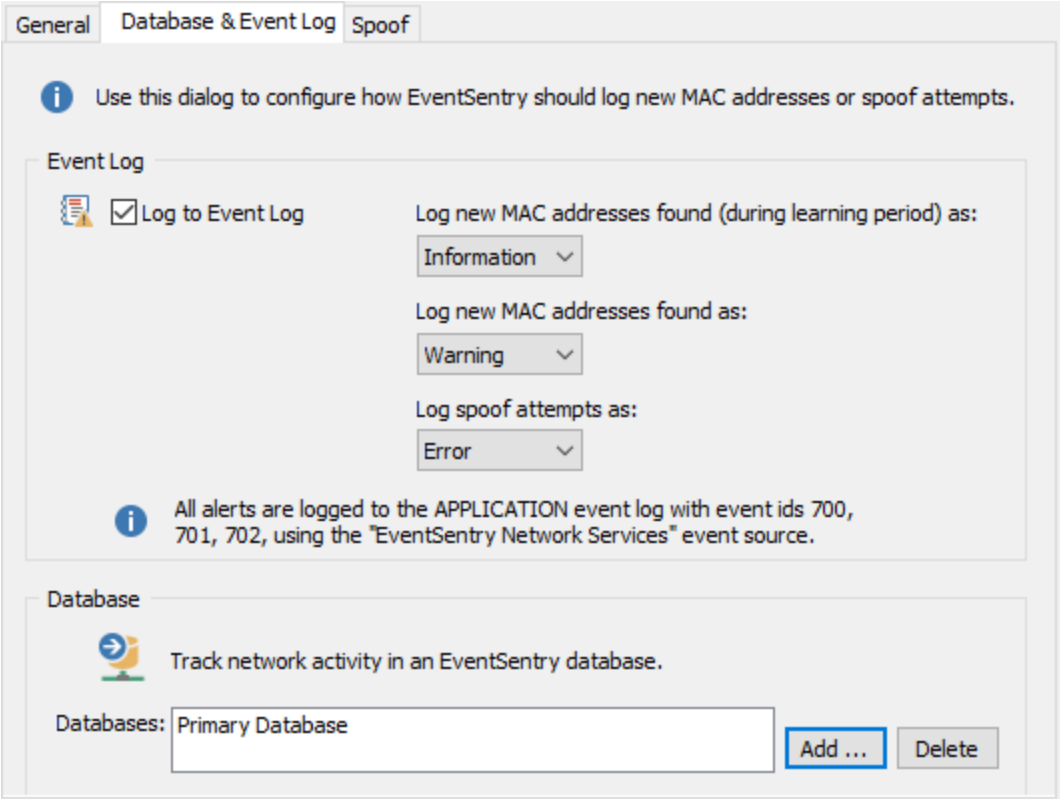
Ereignisprotokoll

Wenn diese Option aktiviert ist, werden Warnungen im Ereignisprotokoll protokolliert, wenn eine neue MAC-Adresse gefunden wird oder wenn ein ARP-Spoofing-Versuch erkannt wird.

Es wird empfohlen, ARP-Spoofing-Versuche als Fehler zu protokollieren, insbesondere in sicherheitsempfindlichen Umgebungen. Siehe "Spoof-Erkennung" für weitere Konfigurationsoptionen und Möglichkeiten zum Ausschließen falsch positiver Ergebnisse.

Datenbank

Konfigurieren Sie eine oder mehrere Datenbanken, in denen die Historie der MAC-Adresse sowie der aktuelle Status der MAC-Adresse gespeichert wird.



5.10.3.2 Spoof-Erkennung

Die ARP-Spoof-Erkennung kann Sie alarmieren, wenn ein Gerät im Netzwerk versucht, Datenverkehr stillschweigend von einem legitimen Host (in der Regel ein Router) auf einen illegitimen Host umzuleiten, in der Regel mit dem Ziel, vertrauliche Informationen zu erfassen oder den normalen Betrieb zu stören. Weitere Informationen finden Sie unter ARP-Spoofing.

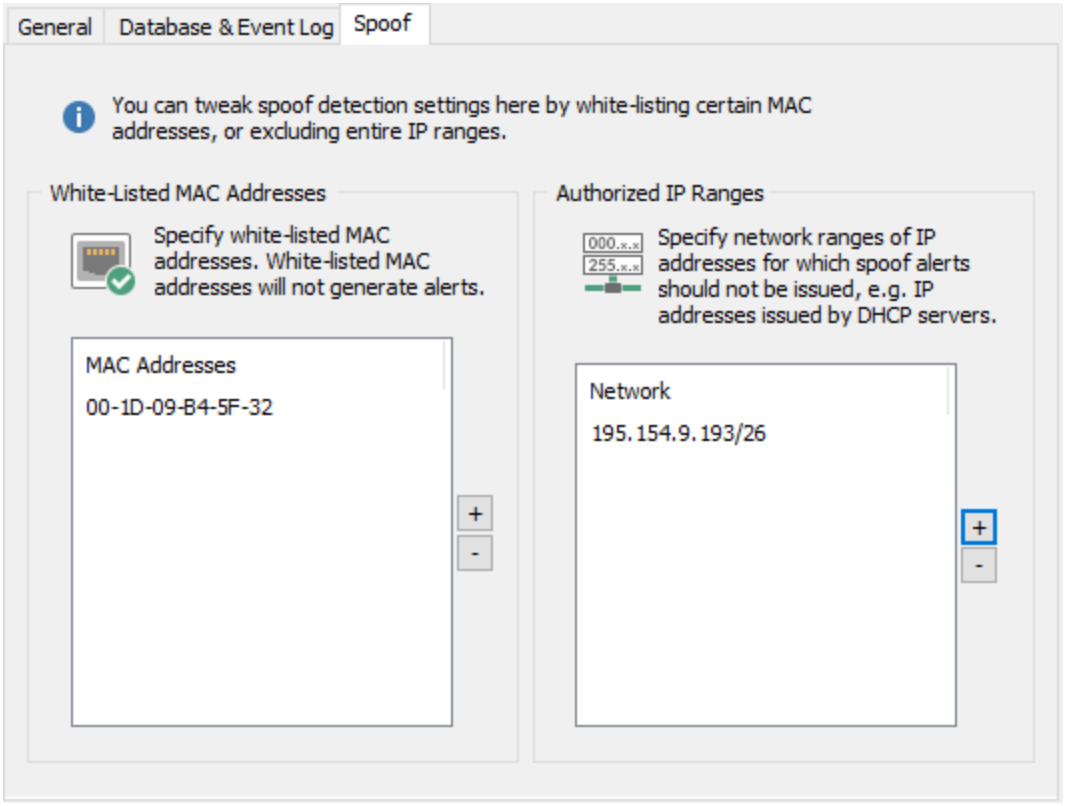
Ein gewisser legitimer Netzwerkverkehr kann als ARP-Spoofing-Versuch erscheinen, daher ist es wichtig, diese Funktion anzupassen, um Fehlalarme zu vermeiden.

White-Listed-MAC-Adressen

MAC-Adressen von legitimen Netzwerkgeräten wie Routern und Gateways sollten auf die weiße Liste gesetzt werden, da sie ihre MAC-Adressen normalerweise mit nicht-lokalen IP-Adressen verknüpfen. Es wird auch empfohlen, die MAC-Adresse jedes anderen Netzwerkgeräts, das regelmäßig Fehlalarme verursacht, auf die weiße Liste zu setzen.

Autorisierte IP-Bereiche

Hosts mit dynamischen IP-Adressen (DHCP) können häufig zu Fehlalarmen führen. Daher sollten alle von DHCP-Servern verwendeten IP-Bereiche in die Liste der "autorisierten IP-Bereiche" aufgenommen werden, um Fehlalarme zu vermeiden. Dies ist im Allgemeinen kein Sicherheitsproblem, da Gateways und Server in der Regel keine über DHCP zugewiesenen IP-Adressen haben.



5.10.4 NetFlow

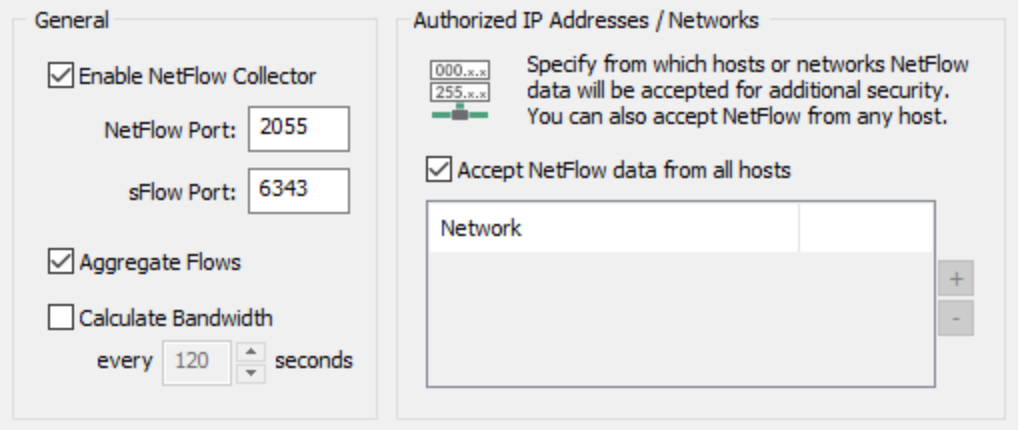
EventSentry kann die folgenden Ablaufprotokolle parsen:

- NetFlow v1
- NetFlow v5
- NetFlow v9
- IPFIX
- sFlow

Die NetFlow-Überwachung unterstützt die folgenden Funktionen:

- Visualisierung, einschließlich Geolokalisierung, der gesamten über NetFlow gesendeten Netzwerkkommunikation
- Echtzeitwarnungen für Verkehr von/nach bestimmten IP-Bereichen, Ländern, Staaten, Städten, Postleitzahlen oder Orten
- Korrelation mit Netzwerk-Anmeldedaten, um den Netzwerkverkehr mit Benutzernamen zu verknüpfen (erfordert die Überwachung von Workstations mit EventSentry)

NetFlow ist eine separat lizenzierte Komponente, für die eine NetFlow-Lizenz erforderlich ist. Die NetFlow-Funktionalität ist während einer Evaluierung (bei der die NetFlow-Funktionalität automatisch aktiviert wird) oder wenn mindestens eine NetFlow-Lizenz installiert ist, verfügbar.



Um den NetFlow-Collector zu aktivieren, markieren Sie das Kontrollkästchen **NetFlow-Collector aktivieren** auf der Registerkarte "Allgemein" und konfigurieren Sie entweder die **Datenbank-** oder die Ereignisprotokollfunktion. Der standardmäßige NetFlow-Port ist 2055, der standardmäßige sFlow-Port ist 6343. Beide können bei Bedarf auf einen anderen Port geändert werden. Nachdem Sie den NetfFlow Collector aktiviert haben, können Sie Ihre NetFlow-Geräte so konfigurieren, dass sie Daten über die konfigurierten NetFlow-Anschlüsse an den EventSentry-Server weiterleiten.

Aggregierte Flows

Um Speicherplatz in der Datenbank zu sparen, kann der NetFlow-Collector mehrere Flows gruppieren, die in dichter Folge empfangen werden. Bei Aktivierung dieser Option können einzelne Paketdetails verloren gehen, der Datenbankspeicherplatz wird jedoch erheblich reduziert.

Bandbreite berechnen

Ermittelt die Bandbreitennutzung einer Schnittstelle und bietet zusätzliche Metriken im Vergleich zur herkömmlichen SNMP-basierten Bandbreitenüberwachung. Das Bandbreitenintervall bestimmt, wie oft Bandbreitenstatistiken in der Datenbank gespeichert werden.

- Auslastung (in %)
- Bytes
- Pakete
- Bytes pro Paket

Nutzung

Die Berechnung der Auslastung einer Schnittstelle setzt voraus, dass die NetFlow-Komponente die maximale Geschwindigkeit einer Schnittstelle kennt (welche sie versucht automatisch über SNMP zu ermitteln). Die maximale Geschwindigkeit einer Schnittstelle kann auch über Variablen angegeben werden, wenn die Geschwindigkeit der Schnittstelle nicht ermittelt werden kann oder wenn die maximale Geschwindigkeit der Schnittstelle nicht die tatsächlich verfügbare Bandbreite widerspiegelt (z.B. hat ein Router eine 1Gb-Schnittstelle, aber nur 100MBit verfügbar). Die Geschwindigkeiten werden in MBit angegeben.

Bandbreitennutzung, die weniger als 0,0001% beträgt, wird immer als 0,0001% protokolliert. Wenn die Bandbreitennutzung nicht berechnet werden kann wird eine Auslastung von 0% protokolliert.

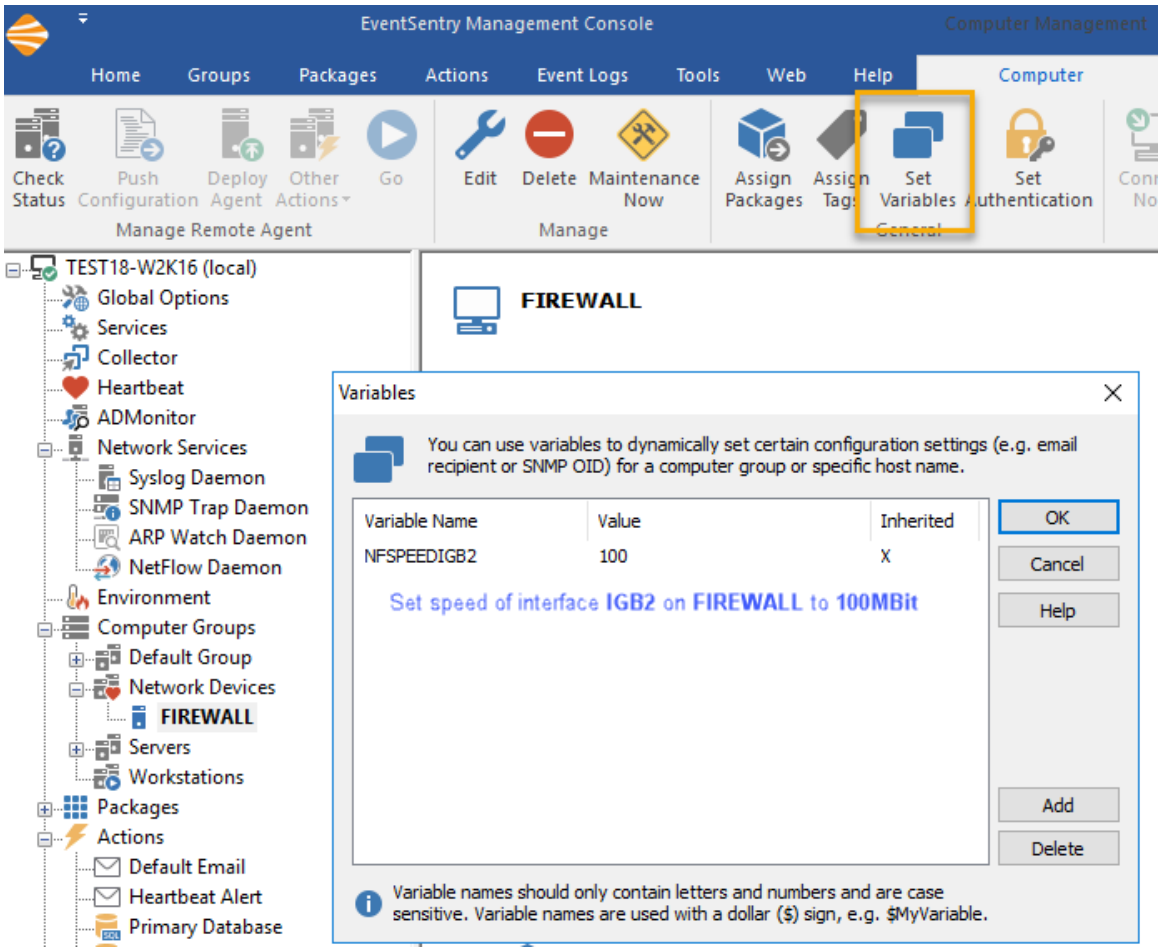
Die folgenden Variablen werden unterstützt:

- NFSPEED
- NFSPEED*[INTERFACENAME]*

Um eine Variable zu setzen muss zunächst der NetFlow-Exporter zu einer Gruppe in der Verwaltungskonsole hinzugefügt und die erforderlichen SNMP-Authentifizierungs-Credentials gesetzt werden. Sobald der Zugriff auf den NetFlow-Exporter bestätigt ist (Gruppen -> Status prüfen), kann eine Variable zugewiesen werden, indem man den NetFlow-Exporter auswählt und im Ribbon auf "Set Variables" klickt.

Das Gerät, das NetFlow-Daten sendet, muss zu einer Gruppe in der Verwaltungskonsole hinzugefügt werden, bevor ihm eine Variable zugewiesen werden kann. Die IP-Adresse des Geräts sollte hinzugefügt werden, wenn Reverse-Lookup im DNS nicht verfügbar ist.

Um eine neue Variable hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie sowohl einen Variablennamen als auch einen Wert an. Wenn die Geschwindigkeit über die NFSPEED-Variable eingestellt wird, dann wird die konfigurierte Geschwindigkeit auf jede Schnittstelle des NetFlow-Exporters angewendet. Um die Geschwindigkeit für eine bestimmte Schnittstelle einzustellen, muss die Schnittstelle an den Variablennamen angehängt werden. Um z.B. die maximal verfügbare Bandbreite der eth0-Schnittstelle auf 100MBit einzustellen, kann die Variable **NFSPEEDETH0** auf **100** gesetzt werden. Die Schnittstellennamen werden normalerweise auf der Inventarseite des Hosts in den Web Reports angezeigt.



Zuweisen einer benutzerdefinierten Schnittstellengeschwindigkeit

Die NetFlow-Komponente protokolliert während des Starts die folgenden Ereignisse unter der Ereignisquelle **Netzwerkdienste**, um zu bestätigen, welche Schnittstellengeschwindigkeiten wirksam sind:

1005: Die Schnittstellengeschwindigkeit wurde über SNMP bestimmt
1006: Die Schnittstellengeschwindigkeit wurde über eine Variable
1007: Die Schnittstelle konnte nicht über SNMP bestimmt werden und wurde nicht mit einer Variablen eingestellt, die Bandbreitennutzung kann derzeit nicht berechnet werden

Bytes
Speichert die Anzahl der Bytes, die während des Erfassungsintervalls von der Schnittstelle gesendet und empfangen wurden.

Pakete
Speichert die Anzahl der Pakete, die während des Erfassungsintervalls von der Schnittstelle gesendet und empfangen wurden.

Bytes pro Paket
Berechnet die durchschnittliche Paketgröße während des Sammelintervalls.

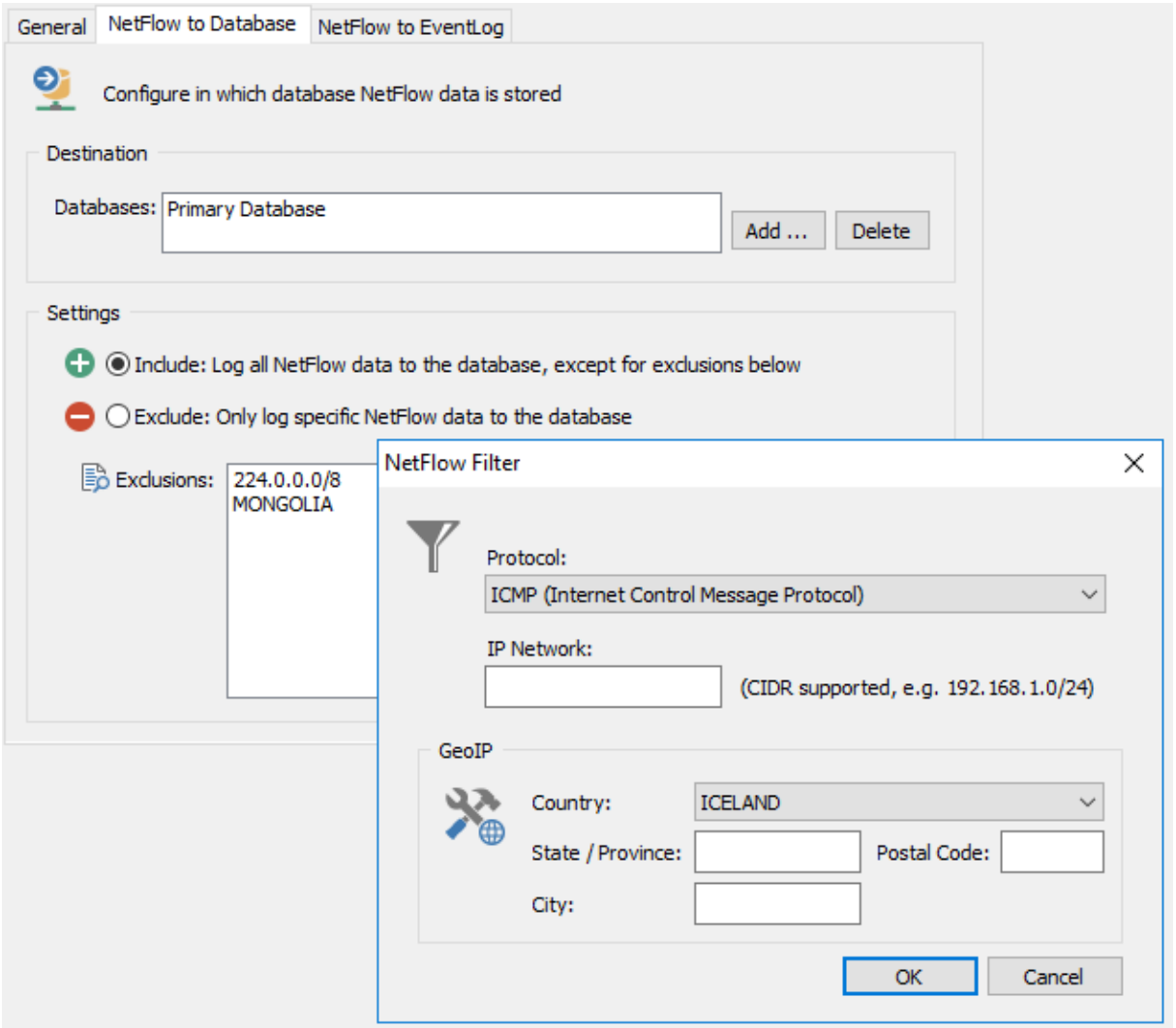
Die Überwachung der durchschnittlichen Paketgröße kann nützlich sein, um ungewöhnliche Aktivitäten in einem Netzwerk zu erkennen, z.B. wenn die durchschnittliche Größe ungewöhnlich hoch oder niedrig ist.

Autorisierte IP-Adressen / Netzwerke

Um die Sicherheit zu erhöhen müssen Sie angeben, von welchen Hosts der NetFlow-Collektor Pakete akzeptiert. Hostnamen sind in dieser Liste nicht erlaubt, es dürfen nur IP-Adressen angegeben werden welche die CIDR-Notation unterstützten.

5.10.4.1 Datenbank-Konsolidierung

Um NetFlow-Daten in einer Datenbank zu konsolidieren, klicken Sie auf die Registerkarte "NetFlow zur Datenbank" und fügen Sie eine oder mehrere Datenbanken zur Liste der Datenbanken hinzu, indem Sie auf die Schaltfläche "Hinzufügen" klicken.



Einstellungen

Standardmäßig werden alle empfangenen NetFlow-Daten an die angegebene(n) Datenbank(en) gesendet. Um dieses Verhalten zu ändern, können Sie entweder bestimmte Daten vom Hinzufügen zur Datenbank ausschließen (alle einschließen, einige ausschließen) oder nur bestimmte NetFlow-Daten an die Datenbank senden.

Regeln können basierend auf bewerten:

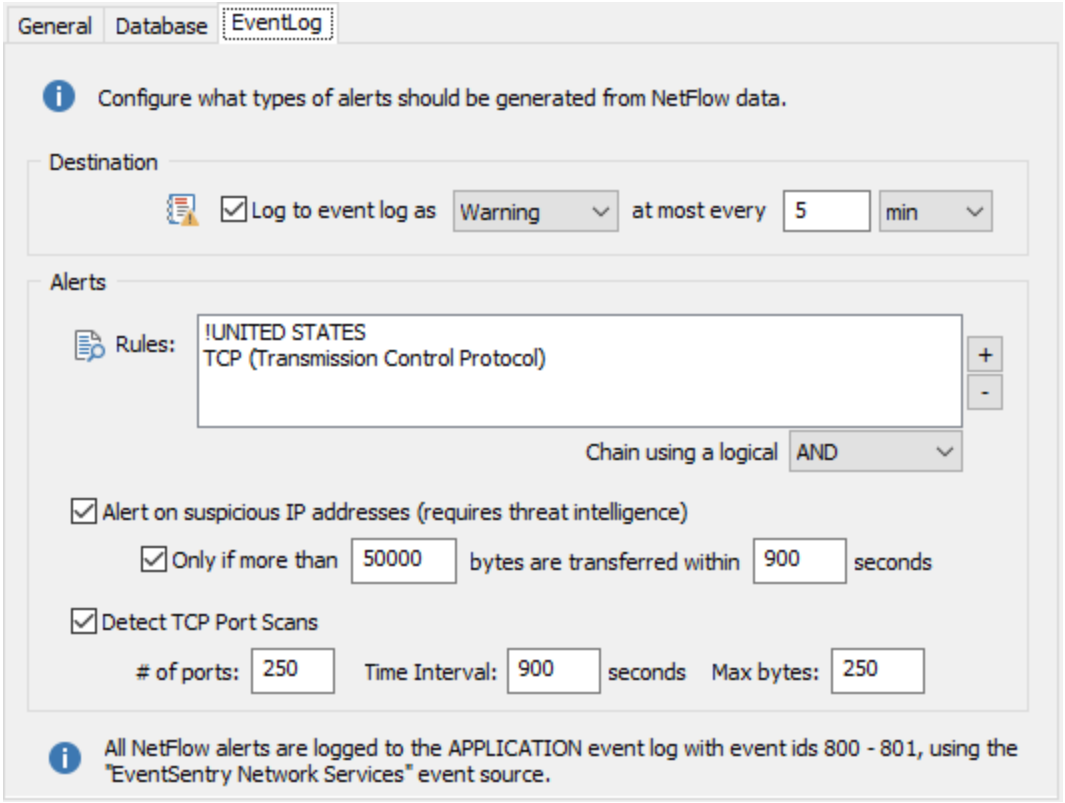
- Das Protokoll
- Die IP-Adresse
- Geolokalisierung (Land, Bundesland, Stadt, Postleitzahl)

Include: Log all NetFlow data to the database, except for exclusions below
Dies ist die Standardeinstellung und speichert alle NetFlow-Daten in der Datenbank. NetFlow-Daten, die unter "Exklusionen" aufgeführt sind, werden von der Verarbeitung ausgeschlossen. Zum Beispiel kann der Verkehr zu/von bestimmten IP-Adressen oder Geolokationen exkludiert werden.

Exclude: Only log specific NetFlow data to the database
Diese Einstellung ist restriktiver und speichert nur NetFlow-Daten in der Datenbank, die den unter "Inklusionen" aufgeführten Regeln entsprechen.

5.10.4.2 NetFlow zum Ereignisprotokoll

Um NetFlow-Daten im Ereignisprotokoll zu protokollieren, klicken Sie auf die Registerkarte "NetFlow to Event Log", aktivieren Sie das Kontrollkästchen "Log to the APPLICATION Event Log" und geben Sie den Schweregrad an, unter dem NetFlow-Daten protokolliert werden sollen. Um eine Überflutung des Anwendungsereignisprotokolls mit NetFlow-bezogenen Warnmeldungen zu vermeiden, kann die Häufigkeit von NetFlow-Warnmeldungen begrenzt werden.

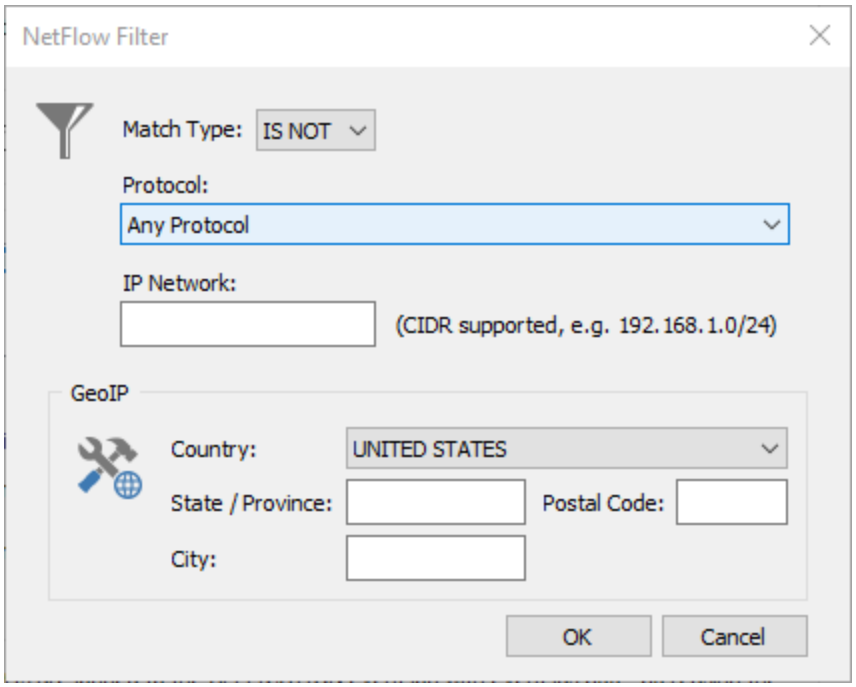


Alarmlogik

Enthält die Regeln, nach denen NetFlow-Verkehrsinformationen im Ereignisprotokoll protokolliert werden sollen. Regeln können basierend auf auswerten:

- Das Protokoll
- Die IP-Adresse
- Geolokalisierung (Land, Bundesland, Stadt, Postleitzahl)

Mehrere Regeln können entweder mit den logischen Operatoren AND oder OR kombiniert werden. Einzelne Regeleinträge können durch Auswahl des Übereinstimmungstyps "IS NOT" negiert werden (siehe unten).



Warnung bei verdächtigen IP-Adressen

Protokolliert Ereignis 820 (EventSentry Network Services / NetFlow) im Ereignisprotokoll, wenn eine verdächtige IP-Adresse festgestellt wurde. Der Alarm enthält die Quell- und Ziel-IP-Adresse, den betroffenen Port, die Anzahl der Bedrohungen und die Details der Bedrohung.

Nur wenn mehr als ...

Protokolliert das Ereignis 830 (EventSentry Network Services / NetFlow), wenn innerhalb des angegebenen Zeitintervalls mehr als die angegebene Anzahl von Bytes zu/von einer verdächtigen IP-Adresse übertragen werden. Dies kann potenziell unregelmäßige Netzwerkaktivitäten wie APTs erkennen und auch dazu beitragen, potenzielle Fehlalarme zu reduzieren. Bei Aktivierung dieser Funktion wird die Ereignis-ID 820 nicht mehr protokolliert.

Erkennen von TCP-Port-Scans

Protokolliert Ereignis 801 (EventSentry Network Services / NetFlow) im Ereignisprotokoll, wenn ein potenzieller Port-Scan erkannt wurde:

# of ports: Die Anzahl der verschiedenen Ports, mit denen ein Remote-Host versuchen muss, eine Verbindung herzustellen, um einen Alarm auszulösen (Standard ist 250)

Time Interval: Das Zeitintervall (in Sekunden), in dem der Port-Scan erfolgen muss (Standard sind 900 Sekunden)
Max Bytes: Netzwerkpakete müssen kleiner oder gleich dieser Größe sein, um als Teil eines potentiellen Port-Scans zu zählen (Standard ist 250).

5.11 ADMonitor

Die optional lizenzierte ADMonitor-Komponente überwacht Änderungen an allen Active Directory-Objekten bis hinunter auf die Attributebene (z.B. Benutzerkonten, Computerkonten, Gruppenrichtlinienobjekte) unabhängig von den aktuellen Audit-Einstellungen in einer Windows-Domäne.

Die Komponente ADMonitor muss nicht auf einem Domänencontroller installiert werden und hat gegenüber der nativen Ereignisprotokollüberwachung folgende Vorteile

1. Funktioniert unabhängig von den aktuellen Audit-Einstellungen (siehe Banner unten)
2. Erkennt Änderungen an der Gruppenrichtlinie
3. Zeigt Änderungen jeder Attributänderung an
4. Zeigt Vor- und Nachwerte von Attributen an
5. Zeigt an, wer die Änderung vorgenommen hat
6. Deutlich geringerer Speicherbedarf als die Erfassung aller Verzeichnisdienst-Ereignisse (Ereignisprotokoll)
7. Kann E-Mails zum Ablauf des Passworts direkt an den Endbenutzer versenden

Für ADMonitor wird ein gewisses Auditing empfohlen, um festzustellen, welcher Benutzer eine bestimmte Änderung in Active Directory vorgenommen hat.

Neben der Erfassung von AD- und Gruppenrichtlinien-Änderungen bietet ADMonitor auch eine aktuelle Liste aller Benutzerobjekte, die Abfragen zur Isolierung von Benutzern mit abgelaufenen Kennwörtern, Benutzern, die Administratoren sind, und mehr unterstützen:

- Administrator?
- Deaktiviert?
- Ist das Passwort so eingestellt, dass es nie abläuft?
- Ist das Passwort abgelaufen?
- Muss das Passwort geändert werden?
- Ist der Benutzer ausgesperrt?
- Wann wurde der Benutzer erstellt?
- Wann hat sich der Benutzer zuletzt angemeldet?

Um die letzte AD-Anmeldung eines Benutzers zu ermitteln, verwendet die ADMonitor-Users Seite entweder den **Zeitstempel lastLogonTimestamp** oder **msDS-LastSuccessfulInteractiveLogonTime** Active Directory, je nachdem, welcher Zeitpunkt aktueller ist.

Bitte beachten Sie, dass **msDS-LastSuccessfulInteractiveLogonTime** im Allgemeinen genauer ist, aber eine GPO-Einstellung erfordert, die bei jeder Anmeldung eines Benutzers ein Popup-Fenster anzeigt.

ADMonitor vs. Account Management-Verfolgung

Für Benutzer, die bereits die EventSentry Account-Management Funktionalität in Security & Compliance nutzen, bietet ADMonitor zusätzliche Details zu Änderungen an Active Directory-Objekten, wie z. B. Vor- und Nachwerte von Attributen.

Da die ADMonitor-Komponente nur Änderungen an Active Directory (Domänenbenutzer usw.) überwacht, wird die Verwendung der Account Management Tracking nach wie vor für Mitgliedsserver und Workstations empfohlen, um auch Benutzer- und Gruppenänderungen an der lokalen Sicherheitsdatenbank zu erkennen.

5.11.1 Installation

Die ADMonitor-Komponente wird durch den Konfigurationsassistenten installiert, der während der Installation und/oder des Upgrades von EventSentry automatisch ausgeführt wird. Um die ADMonitor-Komponente hinzuzufügen, nachdem EventSentry bereits installiert ist, starten Sie den Konfigurationsassistenten über das Startmenü.

ADMonitor besteht aus den folgenden Komponenten:

- EventSentry ADMonitor-Dienst
- EventSentryADMonitor-Domänenkonto
- C:\Programmdateien (x86)\EventSentry\ADMonitor-Dateien

Die Komponente ADMonitor kann nur auf Rechnern installiert werden, die Teil einer Domäne sind.

Servicekonto EventSentryADMonitor / Manuelle Einrichtung
Der EventSentry-Konfigurationsassistent erstellt während der Installation automatisch das EventSentryADMonitor-Dienstkonto in der Domäne; dieses Konto ist für die korrekte Funktion der ADMonitor-Komponente erforderlich.

Da der EventSentryADMonitor-Benutzer Domain Admins und Enterprise Admins (nur bei Überwachung von Subdomänen) Berechtigungen benötigt, muss der Benutzer, der die EventSentry-Installation ausführt, Teil der Domänenadministrator-Gruppe sein; andernfalls muss der Benutzer von einem Domänenadministrator erstellt werden.

Um den EventSentryADMonitor-Benutzer manuell zu erstellen, folgen Sie den nachstehenden Anweisungen:

1. Öffnen Sie Active Directory-Benutzer und -Computer und erstellen Sie einen Benutzer mit dem Namen **EventSentryADMonitor**.
2. Fügen Sie das EventSentryADMonitor-Benutzerkonto zur Gruppe der **Domain Admins** (und **Enterprise Admins** wenn Subdomänen überwacht werden) hinzu.
3. Öffnen Sie auf dem Host, auf dem EventSentry installiert ist, die Anwendung **Dienste** und suchen Sie den **EventSentry ADMonitor**-Dienst.
4. Geben Sie die Eigenschaften des Dienstes ein, und setzen Sie das Dienstkonto auf der Registerkarte **Anmelden** vom **EventSentryADMonitor**-Dienst. Starten Sie den Dienst neu.

Deinstallation
ADMonitor wird als Teil des EventSentry-Deinstallationsprozesses automatisch entfernt. Die folgenden Anweisungen beschreiben, wie Sie nur die ADMonitor-Komponente deinstallieren können:

- Klicken Sie im Dialogfeld ADMonitor in der Verwaltungskonsole auf Deinstallieren

- Löschen Sie das Unterverzeichnis ADMonitor aus dem Installationsordner von EventSentry (z. B. C: \Programme (x86)\EventSentry\ADMonitor)

Die ADMonitor-Komponente kann mit dem EventSentry-Konfigurationsassistenten (erneut) installiert werden.

5.11.2 Konfiguration

Die ADMonitor-Komponente erfordert nur sehr wenig Anpassung und konfiguriert sich während der Installation automatisch wie folgt:

- Überwacht die Domäne, zu der der Computer gehört
- Findet den nächstgelegenen Domänencontroller
- Lädt alle Active Directory-Objekte sowie das Schema zum Erhalt einer Baseline herunter. Die Offline-AD-Datenbank wird im Unterverzeichnis ADMonitor\DB gespeichert.
- Speichert alle zukünftigen Änderungen an Objekten und Gruppenrichtlinien in der ausgewählten oder Standard-Datenbankaktion.

Grundlegende Konfiguration
Das Dialogfeld ADMonitor in der Verwaltungskonsole unterstützt die Einstellung der Zieldatenbank für alle AD-Änderungen, die Steuerung des Dienstes und die Überprüfung, ob der ADMonitor-Dienst ordnungsgemäß funktioniert.

Erweiterte Konfiguration
Die ADMonitor-Komponente unterstützt zusätzliche Konfigurationsoptionen, die mit der EventSentry ADMonitor-Konsolenanwendung konfiguriert werden können.

5.11.3 Utilities

Die EventSentry ADMonitor-Komponente umfasst drei Dienstprogramme, die zur Fehlerbehebung verwendet werden können, und wenn Funktionalität nicht über die Web Reports verfügbar ist. Für die meisten Benutzer ist die Berichtsfunktionalität in den Web-Reports ausreichend und empfehlenswert.

Die Namen der drei Dienstprogramme sind unten aufgelistet und können entweder über die Schaltfläche ADMonitor in der Kategorie Home des Ribbon oder über das Startmenü gestartet werden.

EventSentry ADMonitor Console

Die Konsole unterstützt die folgenden zusätzlichen Funktionen, die nicht über die EventSentry-Verwaltungskonsole verfügbar sind:

1. Überwacht zusätzliche Domänen
2. Einrichten globaler Filter zum Ignorieren bestimmter AD-Änderungen
3. Sofortige Benachrichtigungen über AD-Änderungen einrichten
4. Verwaltung von Datendateien zur Einsparung von Speicherplatz

EventSentry ADMonitor Viewer

Der Viewer interagiert direkt mit der internen Datenbank und ermöglicht die Überprüfung aller AD-Änderungen ohne den EventSentry-Web Reports.

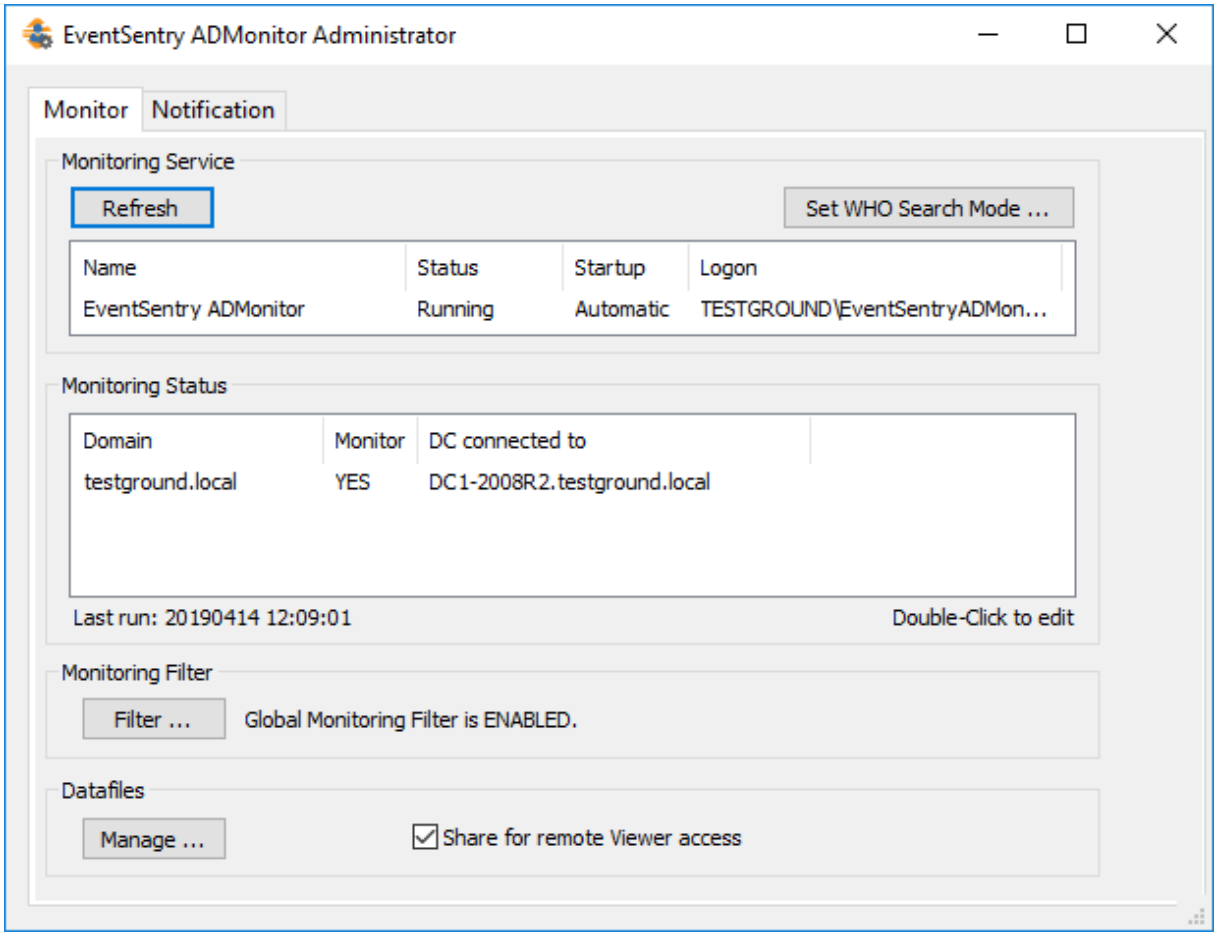
EventSentry ADMonitor Reporting

Unterstützt die Erstellung und Planung von Berichten für Daten, die möglicherweise nicht über die EventSentry-Web Reports verfügbar sind, z. B. eine Liste aller Organisationseinheiten in einer Domäne.

5.11.3.1 ADMonitor Konsole

Mit der Konsolenanwendung können Benutzer Folgendes konfigurieren:

- Umschalten der Überwachung von Unter- oder übergeordneten Domänen
- Filtern von AD Änderungen
- Alarme einrichten
- Verwalten von Datendateien

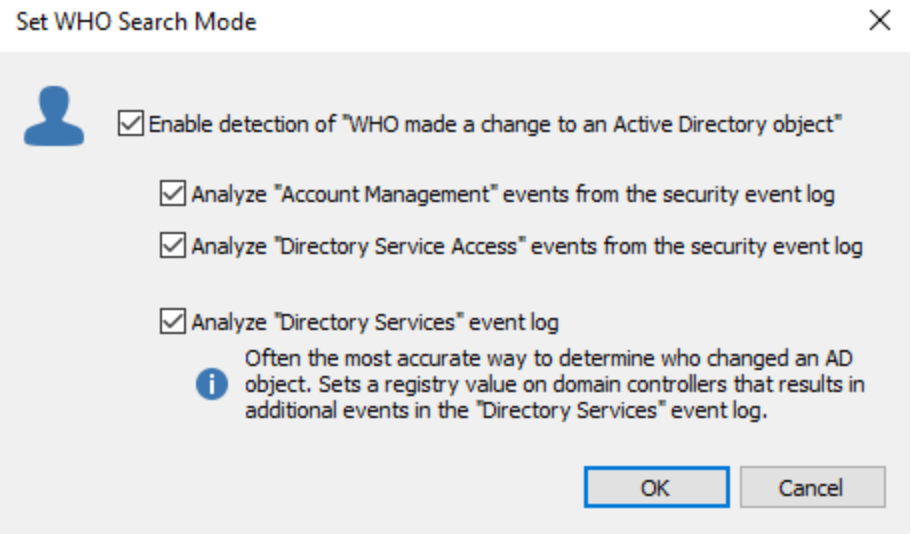


Überwachungsdienst

Zeigt den Status der ADMonitor-Dienst zusammen mit dem Benutzerkonto, unter dem der Dienst läuft

WHO-Suchmodus einstellen

ADMonitor unterstützt mehrere Methoden, um festzustellen, wer eine Änderung an einem AD-Objekt vorgenommen hat. Dies ist im Dialogfeld **WHO-Suchmodus einstellen** konfigurierbar.



Das Kontrollkästchen *Enable Detection of "WHO made a change to an Active Directory object"* schaltet einfach die empfohlenen Standardeinstellungen um, das Kontrollkästchen selbst ist nicht an eine tatsächliche Einstellung gebunden. Die Einstellungen werden über die 3 untergeordneten Kontrollkästchen unten gesteuert:

Analyze "Account Management" events from the security event log
Verwendet Ereignisse aus dem Sicherheitsereignisprotokoll mit der Kategorie "Kontoverwaltung".

Analyze "Directory Service Access" events from the security event log
Verwendet Ereignisse aus dem Sicherheitsereignisprotokoll mit der Kategorie "Directory Service Access".

Analyze "Directory Services" event log
Verwendet Ereignisse aus dem "Directory Services"-Ereignisprotokoll (nur auf Domänencontrollern verfügbar), für die eine zusätzliche Diagnoseprotokollierung in diesem Ereignisprotokoll aktiviert werden muss; ADMonitor aktiviert dies automatisch. Die Menge der zusätzlich protokollierten Ereignisse hängt vom Netzwerk, der installierten Software von Drittanbietern und der Benutzeraktivität ab. Dies ist die genaueste Methode, um festzustellen, wer eine Änderung an einem Objekt vorgenommen hat.

Wenn Sie diese Einstellung aktivieren, wird die zusätzliche Protokollierung unter **HKLM\System\CurrentControlSet\Services\NTDS\Diagnostics** aktiviert, was sich auf den Umfang der im Ereignisprotokoll "Directory Services" erzeugten Ereignisse auswirkt.

Überwachung des Status / Überwachung zusätzlicher Domänen
Zusätzliche Domänen können überwacht werden, wenn der Host, auf dem ADMonitor installiert ist, Teil einer Domäne mit übergeordneten oder untergeordneten Domänen ist. Standardmäßig wird nur die Domäne überwacht, in der der Computer, auf dem ADMonitor ausgeführt wird. Zusätzliche Domänen werden im Bereich **Überwachungsstatus** angezeigt, aber standardmäßig nicht überwacht. Die Überwachung zusätzlicher Domänen kann durch Doppelklicken auf die Domäne und Aktivieren des Kontrollkästchens "Monitor subdomain.maindomain.com" aktiviert werden.

Globale Filter
Standardmäßig werden alle Änderungen an AD-Attributen und Objekten aufgezeichnet. Um Rauschen zu unterdrücken, kann der globale Filter verwendet werden, um bestimmte Änderungen herauszufiltern,

zum Beispiel Änderungen an bestimmten Objekten oder Attributen. So werden z.B. Änderungen an den Attributen **lastLogonTimestamp** und **msDS-LastSuccessfulInteractiveLogonTime** standardmäßig ignoriert, um das Rauschen in der AD-Änderungshistorie zu reduzieren.

Filter können durch Klicken auf die Schaltfläche "Filter" konfiguriert werden.

Verwaltung von Datendateien

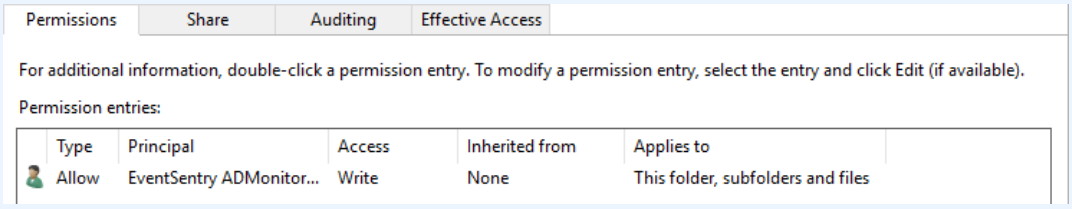
Da ADMonitor alle Änderungen an AD-Objekten im lokalen Cache speichert, kann eine Verwaltung der Daten erforderlich sein:

- Alte Dateien löschen
- Alte Dateien komprimieren
- Dateien an einen anderen Speicherort verschieben (lokale oder Netzwerkfreigabe)

Unabhängig von der gewählten Option läuft die Datendateiverwaltung immer um 2:30 Uhr.

Durch Aktivieren des Kontrollkästchens "Für entfernten Viewer-Zugriff freigeben" wird das lokale DB-Unterverzeichnis als **EventSentryADMonitorDB$** (eine versteckte Freigabe) mit Lesezugriff für **Domain-Administratoren** freigegeben. Diese Freigabe wird vom ADMonitor Viewer für den Fernzugriff auf archivierte Datendateien verwendet. Folglich sollte diese Aktion auf dem Host ausgeführt werden, auf dem sich die Datendateien befinden. Wenn Sie das Kontrollkästchen deaktivieren, wird die Freigabe wieder entfernt.

Wenn Sie **Netzwerkspeicher** wählen, muss die Zielfreigabe dem Benutzer **von EventSentryADMonitor** Schreibzugriff erlauben. Zur Erhöhung der Sicherheit wird dringend empfohlen, nur Schreibzugriff auf das **Verzeichnis** zuzulassen (Schreibzugriff auf Freigaben wird nicht unterstützt), wie in der Abbildung unten gezeigt.



Benachrichtigungen

Der empfohlene Weg, Änderungen an AD-Objekten zu überprüfen, ist über die Web-Reports, die sowohl On-Demand-Suchen als auch Berichte & Jobs unterstützen. Für Fälle, in denen sofortige Benachrichtigungen zu AD-Objekten erforderlich sind, können Benachrichtigungen in der Konsole auf der Registerkarte Benachrichtigungen eingerichtet werden.

5.11.3.1.1 Globale Überwachungsfilter

Globale Überwachungsfilter können verwendet werden, um bestimmte Änderungen an Objekten herauszufiltern, die nicht auditiert werden müssen. Änderungen, die durch einen globalen Filter gefiltert werden, werden weiterhin im lokalen ADMonitor-Cache aufgezeichnet, erscheinen aber nicht im ADMonitor Viewer oder in Web-Reports.

Die folgende Tabelle listet die Arten von Auslösern und Kriterien auf, die zum Filtern von Änderungen verwendet werden können. Beachten Sie, dass mehrere Bedingungen kombiniert werden können, z.B. kann eine Objektänderung mit einer Attributänderung kombiniert werden.

Trigger Options

Search What	Description	Search Operator
Object	Filter out general changes to objects, usually combined with additional conditions.	was created was modified was deleted was created or modified was created or deleted was modified or deleted
Attribute	Filter out changes to attributes, such as attribute values or attribute names.	is equal is not equal contains does not contain BIT is set BIT is not set was created, modified or deleted was created was modified was rewritten was created or modified was created or rewritten was modified or rewritten is found is not found
Classname	Filter out changes based on the class name.	is equal is not equal contains does not contain
Object-Name	Filter out changes based on the object name.	is equal is not equal contains does not contain
Object-GUID	Filter out changes based on the object GUID.	is equal is not equal contains does not contain
Who	Filter out changes based on who performed the change.	is equal is not equal contains does not contain
Organizational Unit	Filter out changes based on the organizational unit where the change occurred.	contains does not contain

Filter verwalten

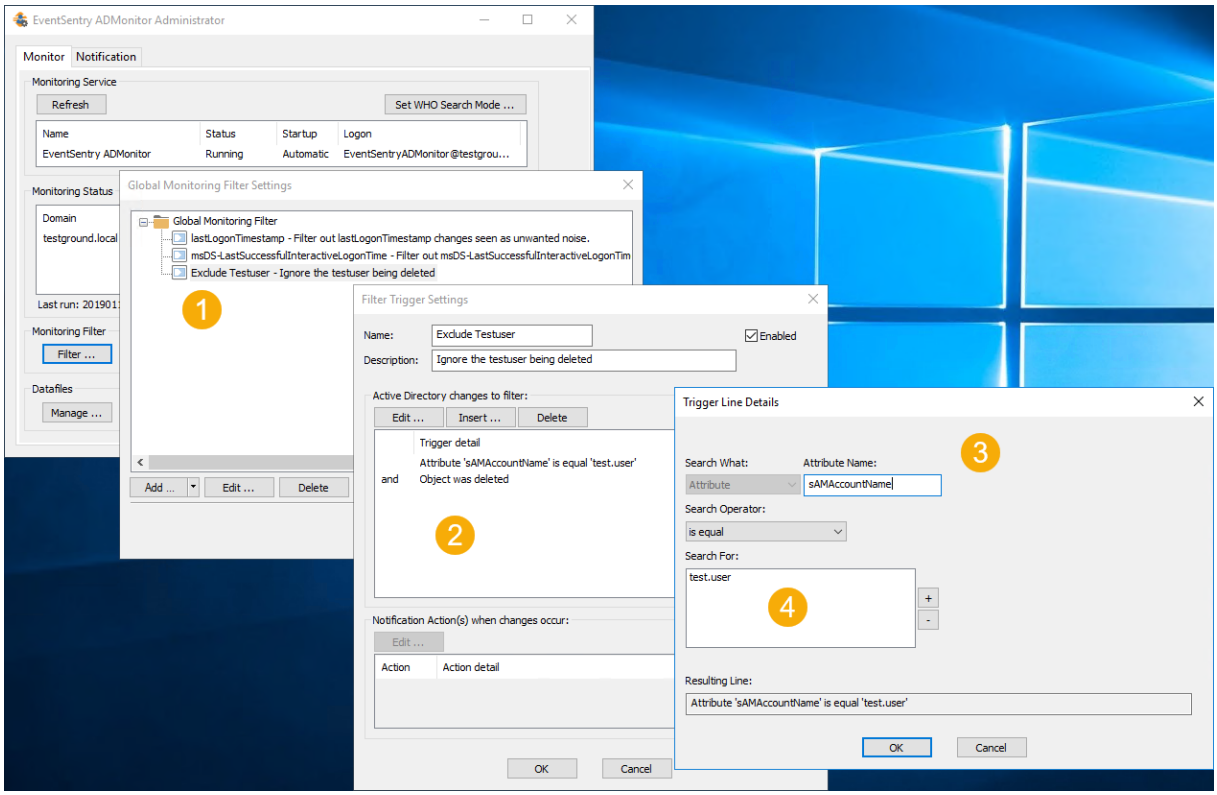
Globale Überwachungsfilter-Einstellungen

Vorhandene Filter werden im Dialogfeld "Global Monitoring Filter Settings" (1 unten) angezeigt und über die Schaltflächen Add, Edit und Delete verwaltet. Das Hinzufügen oder Bearbeiten eines bestehenden Filters ruft das Dialogfeld "**Filter-Triggereinstellungen"** (2 unten) auf, in dem der Triggername, die Beschreibung und die Triggerliste angezeigt werden.

Filter-Trigger-Einstellungen

Die Trigger selbst werden unter Trigger-Detail (2) aufgelistet und über die Schaltflächen Bearbeiten, Einfügen und Löschen verwaltet. Das Einfügen oder Bearbeiten eines vorhandenen Triggers ruft das Dialogfeld Triggerzeilen-Details (3) auf, in dem der Trigger konfiguriert wird.

Details zur Auslöselinie
Die obige Tabelle zeigt die möglichen unterstützten Trigger-Optionen, mehrere Elemente in der Liste "Suchen nach" (4) sind ODER-verknüpft.



In den meisten Fällen kann das Viewer-Dienstprogramm verwendet werden, um einen Filter zu testen und sicherzustellen, dass er wie erwartet funktioniert.

5.11.3.2 ADMonitor Viewer

Die ADMonitor Viewer-Anwendung bietet eine zusätzliche Methode zum Anzeigen von AD-Änderungen, ohne dass die Web-Reports erforderlich sind. Der ADMonitor-Viewer greift direkt auf den lokalen AD-Cache zu und ermöglicht Benutzern die Anzeige aller AD-Änderungen, die seit der Installation von ADMonitor aufgetreten sind. Beachten Sie, dass der Viewer Folgendes **nicht** anzeigt:

- Änderungen an den Gruppenrichtlinien (erfordert Web-Reports)
- Liste von Objekten wie Benutzern und/oder Gruppen (erfordert ADMonitor Reporting oder Web-Reports)

Die Ergebnisse können auch gedruckt und im HTML- und CSV-Format exportiert werden.

Verbinden

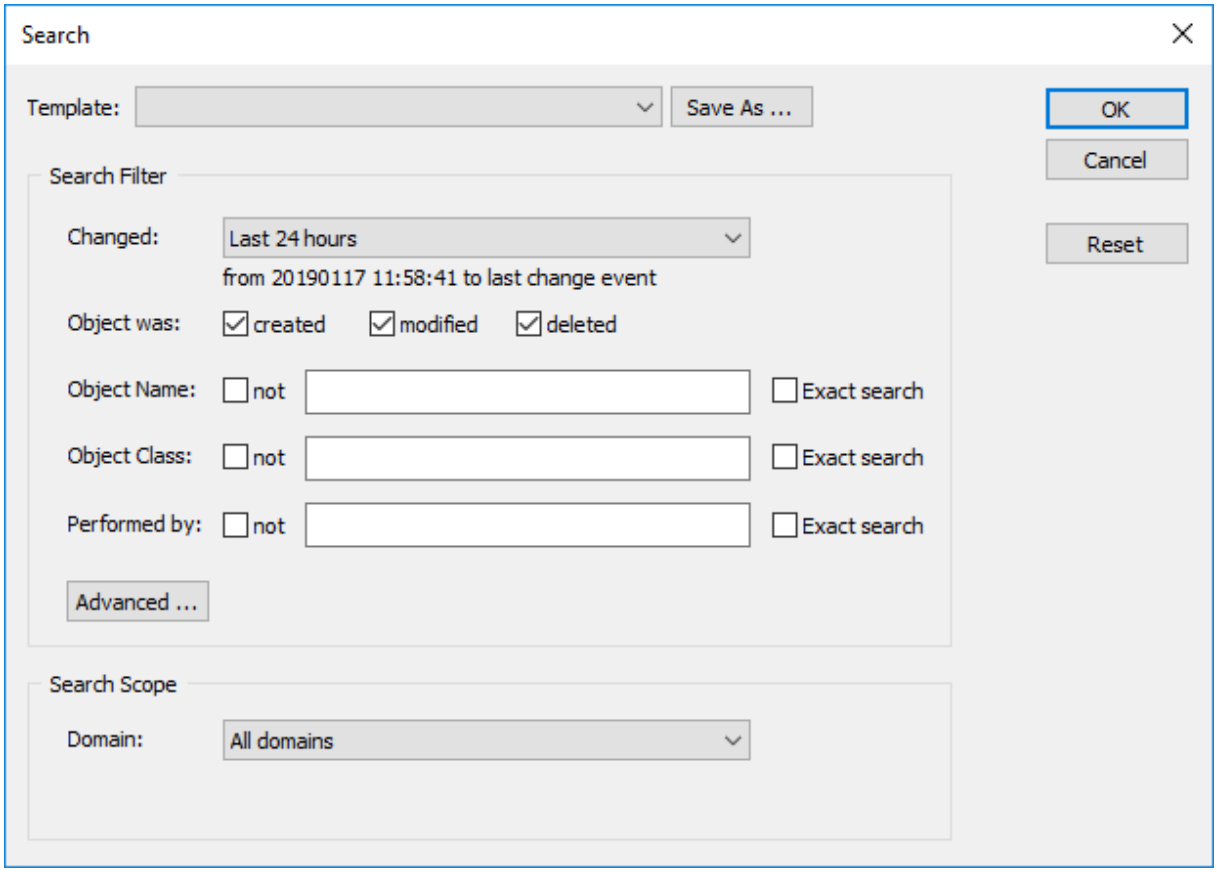
Der Viewer kann entweder eine Verbindung mit dem lokalen ADMonitor-Cache (Standard) oder mit einem entfernten Archiv herstellen, wenn die Datendateiverwaltung aktiviert wurde. Der Zugriff auf ein entferntes Archiv setzt voraus, dass die **EventSentryADMonitorDB$** verfügbar ist und dass der aktuell angemeldete Benutzer zur Gruppe der **Domänen-Admins** gehört.

Suchen

Nachdem eine Verbindung hergestellt wurde, kann der Benutzer im Suchdialog festlegen, welche Änderungsereignisse angezeigt werden sollen. Standardmäßig werden alle Objektänderungen der letzten 24 Stunden aus allen Domänen zurückgegeben. Häufig verwendete Suchkriterien können als Vorlage gespeichert werden. Die Suche kann eingeschränkt werden durch:

- Typs
- Objekt-Name
- Objekt-Klasse
- Benutzer, der die Änderung durchgeführt hat
- Domäne

Erweiterte Suchen, die die Attribute eines Objekts auswerten, sind ebenfalls verfügbar.



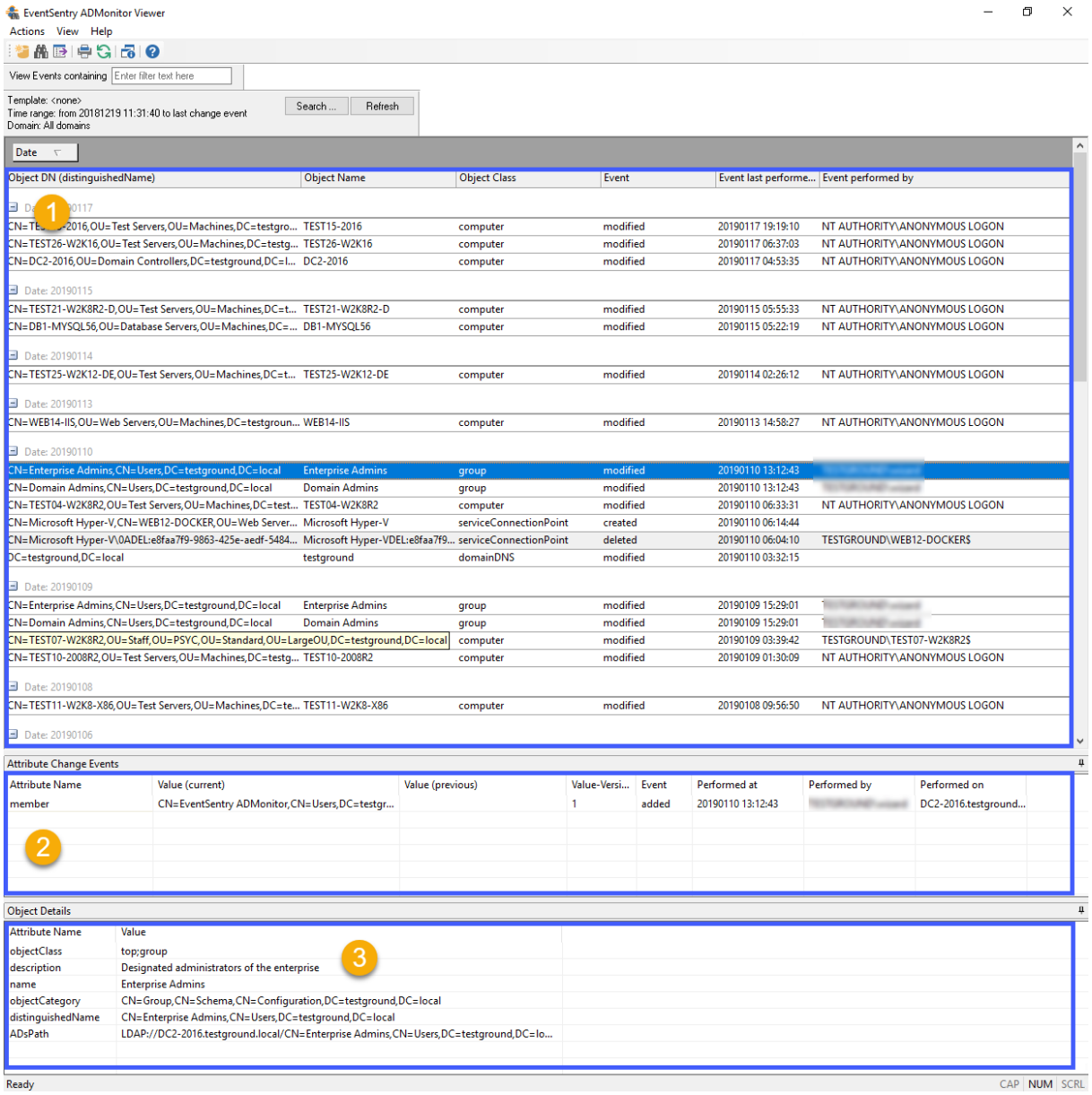
Sortieren/Gruppieren von Ergebnissen

Suchergebnisse werden standardmäßig nach ihrem Zeitstempel sortiert, aber eine benutzerdefinierte Sortierreihenfolge kann durch Ziehen einer der verfügbaren Spalten in den dunkelgrauen Kopfbereich angewendet werden. Such-/Gruppenbedingungen können durch Ziehen des Feldes außerhalb der grauen Kopfzeile entfernt werden.

Ergebnisse interpretieren

Die Suchergebnisse werden im Hauptdialog des Anzeigers angezeigt, der in drei Abschnitte unterteilt ist:

- Objekt-Änderungen
- Attribut-Änderungsereignisse
- Objekt-Details



Zusätzlich kann das Attribut-Fenster (kann deaktiviert werden) eine Beschreibung und Details anzeigen, wenn ein Attribut ausgewählt wird.

Objekt-Änderungen (1)

Zeigt eine Liste der Objekte an, die während des ausgewählten Suchzeitraums geändert wurden, einschließlich des Änderungstyps, des Objekt-DN, des Namens, der Klasse und der Zeitstempel.

Attribut-Änderungsereignisse (2)
Alle Attribute, die im Rahmen einer Objektänderung geändert wurden, werden in diesem Bereich angezeigt, da Objektänderungen in der Regel aus einer oder mehreren Attributänderungen bestehen. Zu den Attributänderungen gehören der Attributname und der Änderungstyp, aktuelle und frühere Werte einschließlich Versionsnummern sowie Zeitstempel. Wenn der Attribut-Beraterdialog sichtbar ist, wird eine Beschreibung eines Attributs angezeigt, wenn verfügbar.

Objekt-Details (3)
Zeigt alle Attribute an, die mit dem ausgewählten Objekt verknüpft sind, wie z.B. objectClass, displayName, Name und andere.

5.11.3.3 ADMonitor Reporting

Active Directory- und Gruppenrichtlinien-Änderungen zusammen mit einer Liste des aktuellen Benutzerstatus werden über die EventSentry Web Reports bereitgestellt, die empfohlene Methode für die ADMonitor-Berichterstattung.

Die ADMonitor-Berichtsanwendung unterstützt eine Reihe von geplanten und abrufbaren Berichten, die möglicherweise nicht über die EventSentry Web Reports verfügbar sind. Die ADMonitor-Reportinganwendung bietet Berichte wie

- Eine Liste aller Computer, Gruppen oder Organisationseinheiten
- Eine Liste von Benutzern, die sich nie angemeldet haben
- Eine Liste der Benutzer, für die Anmelde- oder Arbeitsstundenbeschränkungen gelten

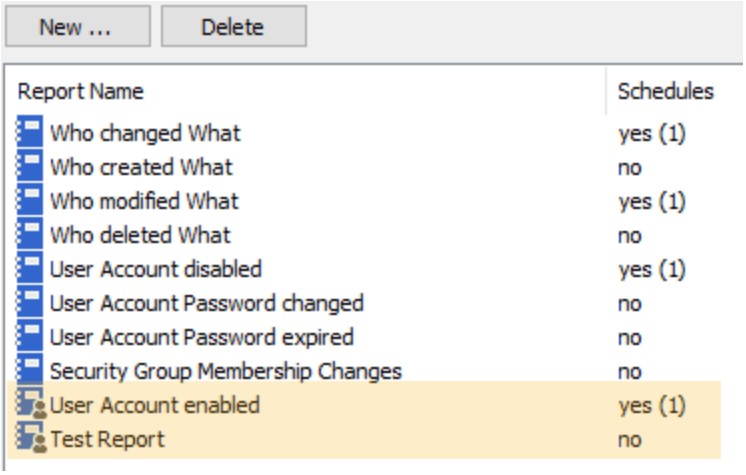
Änderungen an Active Directory und Gruppenrichtlinien sowie eine Liste der aktuellen Benutzer kann über die EventSentry Web Reports abgerufen werden.

Die Berichte sind entweder in *Objektstatus-* oder Objektänderungsberichte unterteilt und können so geplant werden, dass sie zu einer bestimmten Tageszeit ausgeführt werden. Berichte werden immer im HTML-Format generiert.

Berichtstyp	On-Demand ausführen?	Zeitplan?	Erstellen & Anpassen
Objekt ändern	Nein	Ja	Ja
Objekt-Status	Ja	Nein	Nein

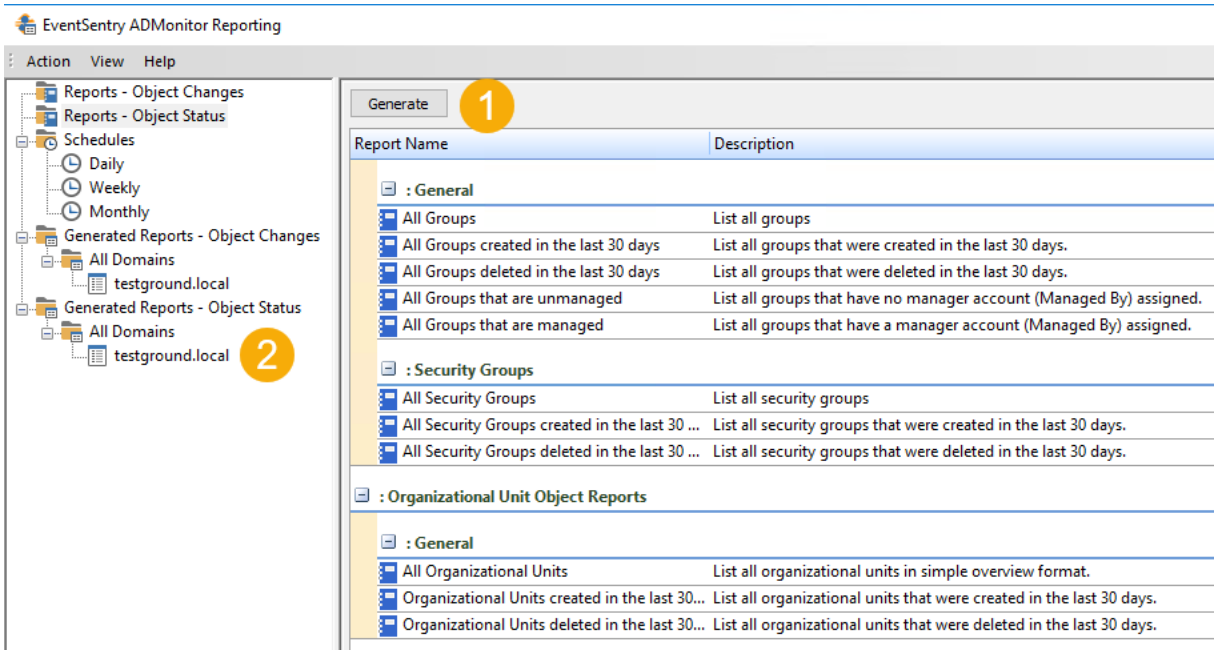
Berichte - Objektänderungen
Die Berichtsanwendung enthält eine Reihe von Standard-Berichten, und mit der Schaltfläche **Neu** können zusätzliche Berichte erstellt werden. Objektänderungsberichte können nicht auf Anforderung ausgeführt werden, sie können nur mit einem Tages-, Wochen- oder Monatsplan geplant werden.

Eingebaute Berichte, die mit EventSentry ausgeliefert werden, können nicht geändert werden. Um einen vorhandenen Bericht anzupassen, erstellen Sie einen neuen Bericht - unter Verwendung eines integrierten Berichts als Vorlage - und passen Sie dann stattdessen den neuen Bericht an. Von Benutzern erstellte Berichte sind leicht durch ein anderes Berichtssymbol zu unterscheiden, das ein Benutzersymbol enthält - siehe Screenshot unten.



Berichte - Objektstatus

Objektstatusberichte unterstützen nur vordefinierte Berichte und können durch Auswahl eines Berichts und Klicken auf die Schaltfläche **Generate (1)** ausgeführt werden. Generierte Berichte werden im Abschnitt **Generated Reports - Object Status (2**) angezeigt.



Generating object status reports on demand

Zeitpläne

Daily

AD-Änderungen vom vorherigen Kalendertag enthalten.

Weekly

Enthält AD-Änderungen gegenüber der vorherigen Kalenderwoche (Mo - So).

Monthly

Sie enthalten AD-Änderungen aus dem vorhergehenden Kalendermonat (1. - 28/29/30/31. April).

Es ist wichtig zu beachten, dass die Zeitspanne für Wochen- und Monatspläne immer für einen Kalendertag/eine Kalenderwoche/einen Kalendermonat gilt und **nicht** für die vorhergehenden 7 oder 28/29/30/31 Tage. Ein Monatsbericht, der am 18. April generiert wird, wird immer Daten aus dem Monat März enthalten.

6 Web Reports

Das webbasierte Reporting, offiziell "EventSentry Web Reports", macht alle gesammelten und konsolidierten Daten visuell verfügbar. Die Web-Reports können entweder als Teil der EventSentry-Hauptinstallation oder separat mit einem eigenständigen Installationsprogramm installiert werden.

Die Web Reports können auf jedem Host im Netzwerk installiert werden, solange dieser direkten Netzwerkzugriff auf den Datenbankserver hat. Die folgenden Plattformen werden für die java-basierten Web Reports unterstützt:

- Fenster
- Linux
- Mac OSX

Das Installationsprogramm für Web Reports kann im Kundenbereich heruntergeladen werden, eine Live-Demo ist unter https://demo.eventsentry.com verfügbar.

Die Java-basierten Web Reports ersetzen die IIS-basierten Web Reports aus früheren Versionen von EventSentry und führen eine Vielzahl neuer Funktionen ein, darunter Jobs, ein granularer Suchsyntax und verbesserte Berichtsoptionen.

Sprachen

Unterstützung für mehrere Sprachen, einschließlich Deutsch und Spanisch, ist in den Web Reports verfügbar. Bitte kontaktieren Sie uns unter support@netikus.net, wenn Sie eine Übersetzung in Ihrer Sprache beisteuern möchten.

Browser-Unterstützung

Die Web Reports funktionieren mit den meisten modernen Browsern, siehe Anforderungen für weitere Informationen. Mobile Geräte auf den Plattformen iOS und Android werden ebenfalls vollständig unterstützt.

Die Web Reports erfordern keine Browser-Plug-ins auf den Clients (z.B. Java, Flash oder Silverlight).

Zugriffskontrolle

Der Zugriff auf die Web Reports kann eingeschränkt werden, so dass nur Benutzer mit gültigen Zugangsdaten auf die webbasierten Berichte zugreifen können. Benutzer und Gruppen werden immer innerhalb der Web Reports erstellt, aber die Authentifizierung kann optional auf einen LDAP-Server verschoben werden. Die Zugriffssteuerung ermöglicht es, Benutzer auf bestimmte Funktionen zu beschränken (z.B. einen Benutzer auf Leistungsberichte zu beschränken) oder nur Daten von bestimmten Computern anzuzeigen (z.B. einen Benutzer darauf zu beschränken, nur Logs von nicht klassifizierten Servern anzuzeigen).

SSL/TLS-Unterstützung
Der Webverkehr zu und von den Web Reports kann mit SSL / TLS verschlüsselt werden, indem Sie die Anweisungen in KB-Artikel 371 befolgen.

Java
Die Web Reports erfordern Java 8 (nur auf dem Server, auf dem die Web Reports installiert sind). EventSentry installiert und pflegt Java automatisch als Teil seiner Update-/Patch-Zyklen, seine Java-Installation ist für andere Anwendungen auf dem Server nicht zugänglich.

6.1 Seiten

Die Mehrheit der Seiten in den Web Reports hat einen von 4 Seitentypen:

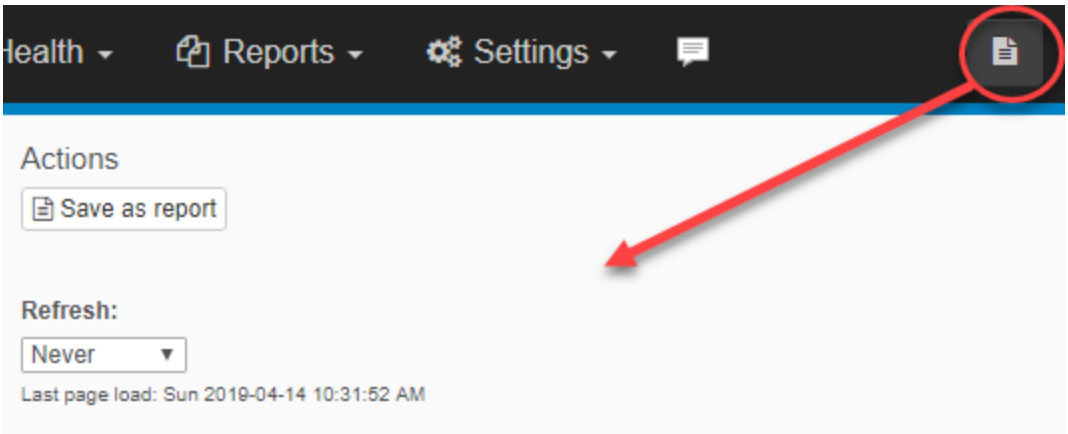
- Dashboard (Netzwerk-Dashboard, Computer-Dashboard)
- Zusammenfassung
- Details
- Trends

Alle anderen Seitentypen sind einzigartig, einschließlich der Seiten Netzwerkstatus, Gesundheitsmatrix, Benutzer-/ IP-Suchseiten, Berichte, Wartungsassistent und andere.

Seiten-Optionen
Alle Standard-Suchseiten haben die Möglichkeit

- als Bericht gespeichert werden
- automatisch aktualisiert werden
- Berichte für diesen Seitentyp anzeigen

Um auf die Seitenoption zuzugreifen, klicken Sie auf die Schaltfläche mit den drei weißen Linien oben rechts auf der Seite, wie unten dargestellt.



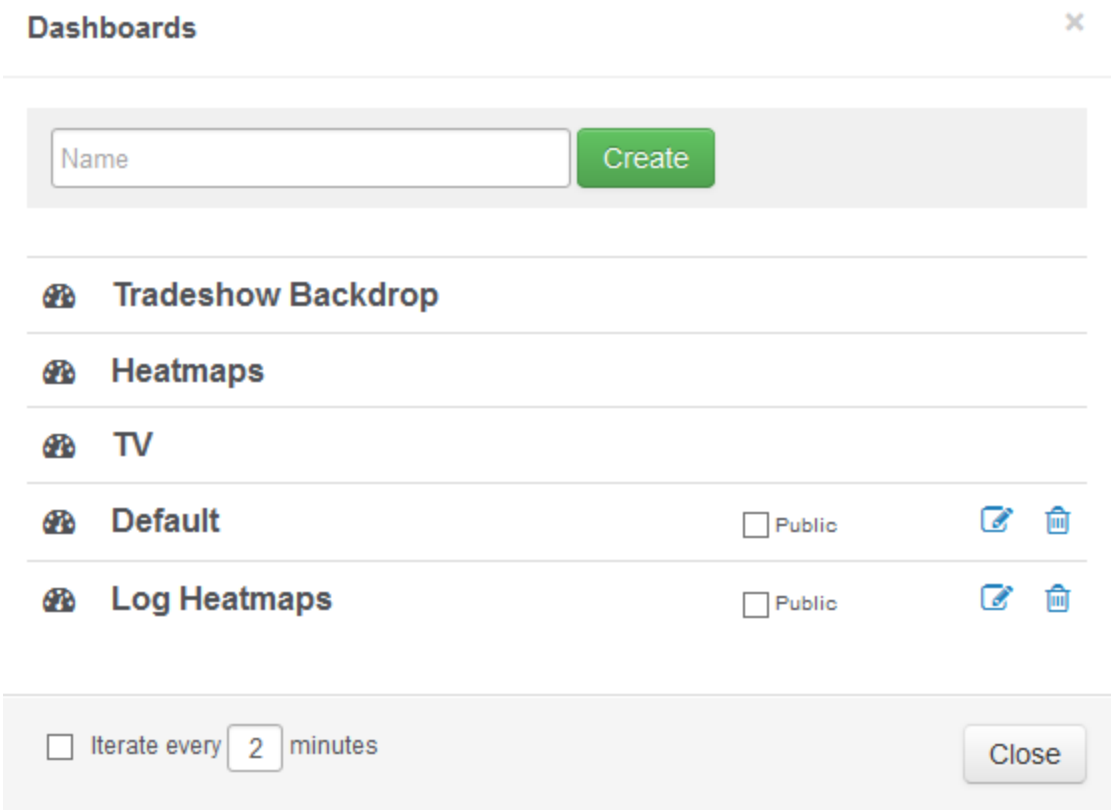
6.1.1 Dashboard-Seiten

Die Netzwerk- und Computer-Dashboard-Seiten sind anpassbare Ansichten einer weiteren Kachel, die aktuelle Protokolleinträge, Trends, Systemzustandsberichte und mehr anzeigen. Die Dashboards für den Netzwerkstatus und die Gesundheitsmatrix werden separat besprochen:

- Netzwerk-Status
- Gesundheits-Matrix

Mehrere Dashboards

Das Network Dashboard unterstützt mehrere Dashboards, die von den Benutzern gemeinsam genutzt und zwischen ihnen iteriert werden können.



TV-Modus: Klicken Sie auf die Schaltfläche TV-Modus, um das Dashboard in den Vollbildmodus zu versetzen. Die Bildschirmfläche kann weiter maximiert werden, indem der Vollbildmodus des Webbrowsers verwendet wird. Bitte beachten Sie, dass die Iteration durch mehrere Dashboards den Vollbildmodus des Webbrowsers verlässt.

Erstellen eines neuen Dashboards: Um ein neues Dashboard hinzuzufügen, klicken Sie auf den Link [Ändern] oben links auf dem Bildschirm und wählen Sie **Bearbeiten**. Geben Sie im daraufhin angezeigten Bildschirm im Feld "Name" einen Namen für das neue Dashboard an und klicken Sie auf **Erstellen**.

Gemeinsame Nutzung eines Dashboards: Ein Dashboard kann von mehreren Benutzern genutzt werden, indem Sie das Kontrollkästchen "Public" aktivieren. Dieses Dashboard erscheint dann in der Liste der Dashboards für alle anderen Benutzer. Bereits von anderen Benutzern freigegebene Dashboards erscheinen in der Liste ohne die Schaltflächen "Bearbeiten" und "Löschen".

Iteration: Anstatt nur ein Dashboard anzuzeigen, kann die Dashboard-Seite automatisch alle X Minuten zwischen allen verfügbaren Dashboards iterieren. Aktivieren Sie das Kontrollkästchen "Alle Iterationen" und konfigurieren Sie ein Zeitintervall. Der TV-Modus ist auf den meisten Plattformen nicht verfügbar, solange die Iteration aktiviert ist.

Dashboards bearbeiten: Dashboards können mit der Schaltfläche "Bearbeiten" neben dem Papierkorb umbenannt werden, Dashboards können durch Klicken auf die Schaltfläche "Papierkorb" gelöscht werden.

Kacheln (Tiles)

Die Netzwerk- und Computer-Dashboards unterscheiden zwischen den folgenden Typen:

- Status
- Geschichte (History)
- Gauges
- NetFlow
- ADMonitor

Status

Den aktuellen Status einer bestimmten Metrik anzeigen, z.B. den Netzwerkstatus oder einen Leistungszähler. Die meisten Statuskacheln zeigen entweder "OK" an wenn keine Probleme identifiziert wurden, oder die Liste der Warnungen und/oder Fehler.

Geschichte

Zeigt die jüngsten Änderungen/Ereignisse zu einer überwachten Metrik an, wie z. B. die jüngsten Änderungen des Dienststatus.

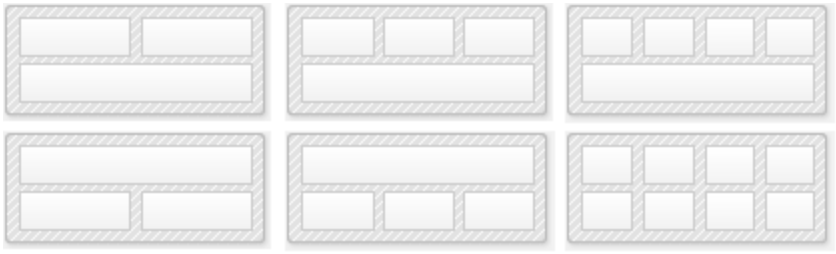
Messgeräte

Zeigen Sie den aktuellen Status von Leistung, Plattenplatz oder Umgebungssensorwert an. Messwerte sind nur auf dem Netzwerk-Dashboard verfügbar.

Siehe Kacheltypen für weitere Informationen.

Gestaltung

Das Layout kann durch Angabe der Anzahl der Spalten (2 - 4) und der Position der Kachel in voller Breite (oben oder unten) angepasst werden. Die Kachel in voller Breite kann optional auch deaktiviert werden, was nützlich ist, wenn Sie keine Kachel in voller Breite verwenden. Der folgende Screenshot zeigt einige der verfügbaren Layout-Optionen.



6.1.1.1 Tile Types

Status

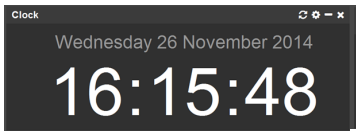
- Heartbeat-Status
- Festplattenplatz-Warnungen
- Leistung (höchste & niedrigste Werte)
- Prozessleistung
- Dienstleistungen
- Informationen zur Garantie
- Verwaltete Hardware

Geschichte

- Aktivste Maschinen
- Heartbeat-Geschichte
- Trends (Audit-Fehlschläge, Fehler, Syslog)
- Ereignisse
- Software-Änderungen
- Generische Suche

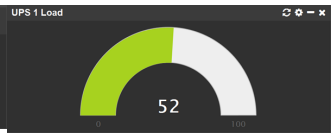
Gauges

Gauges sind auf dem Netzwerkstatus-Dashboard verfügbar und helfen bei der Visualisierung von Leistungs-, Festplattenspeicher- oder Umgebungsdaten. Die folgenden Typen sind verfügbar:



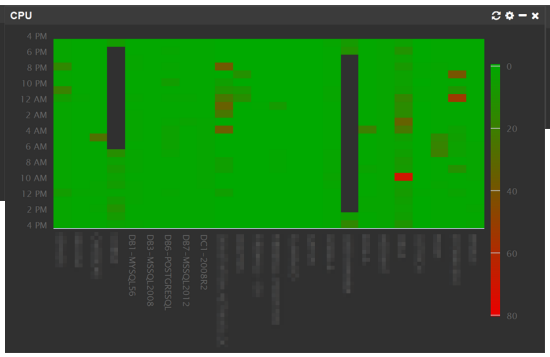
Digitale Uhr

Bullet

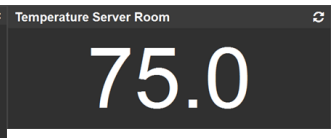


Meter

Analoge Uhr



Heatmap



Nummer

Wärmebildkarten

Visualisieren Leistungsdaten und Log-Volumen der letzten 24 Stunden auf einzigartige Weise, wobei die x-Achse jeden verfügbaren Host und die y-Achse 24 Datenpunkte anzeigt, einen für jede Stunde. Die Skala (auf der rechten Seite angezeigt) des Diagramms ist dynamisch und reicht vom niedrigsten bis zum höchsten beobachteten Wert. Die Heatmap macht es extrem einfach, Anomalien in der Leistung zu erkennen und Daten von einer Gruppe von Hosts zu protokollieren. Im Gegensatz zu Trenddiagrammen visualisiert die Heatmap große Datenmengen - auch über eine große Anzahl von Hosts hinweg - sehr gut.

NetFlow

Enthält Kacheln zur Visualisierung von NetFlow-Daten, einschließlich

- Bedrohungen
- Karten
- Trends
- Netzwerk-Verkehr
- Top-Talker
- Bandbreite

- Wichtigste Ports

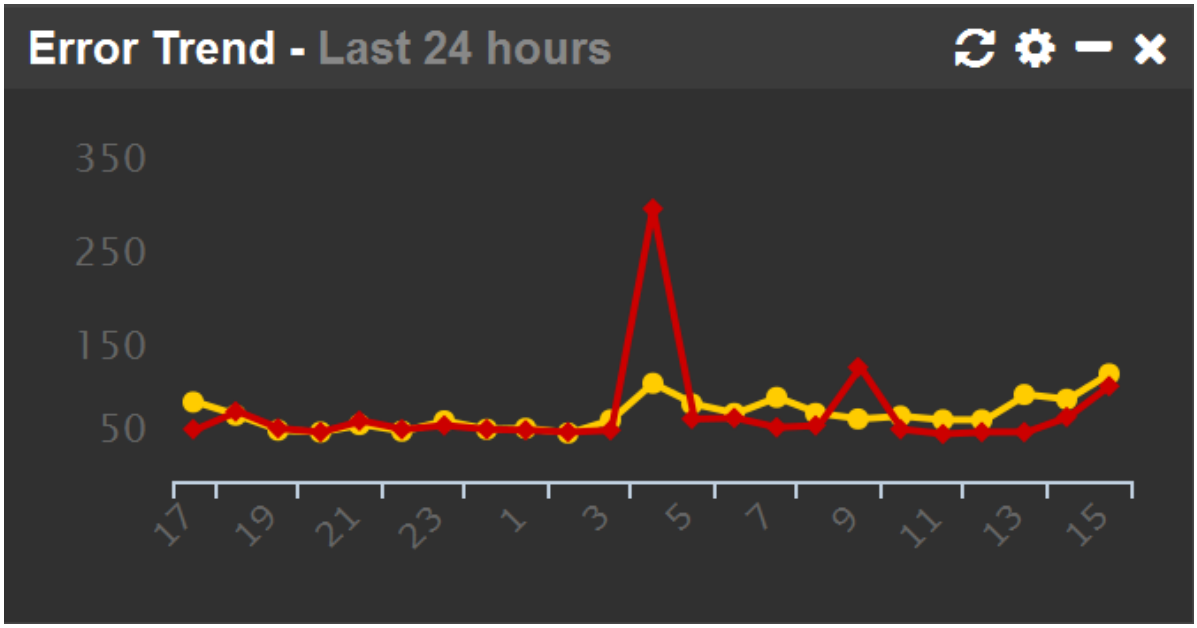
ADMonitor
Enthält Kacheln, die Active Directory-Daten zusammenfassen, einschließlich

- Statistik
- Änderungen durch Benutzer
- Änderungen durch Computer
- Änderungen der Gruppenrichtlinien

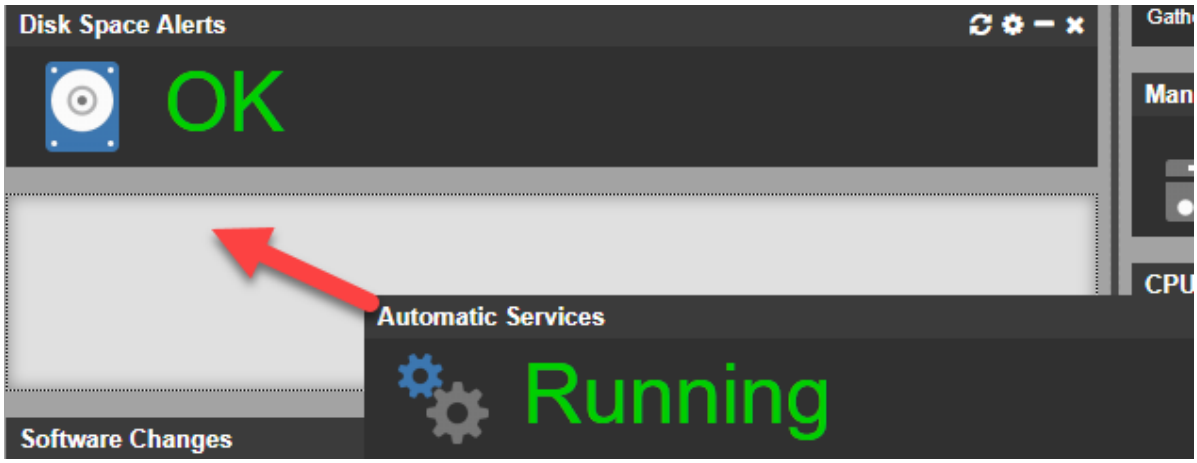
Management
Dashboards unterstützen Kacheln in einfacher Breite und in voller Breite, und einzelne Kacheln können frei auf der Seite platziert werden. Kacheln in voller Breite müssen jedoch im Bereich der vollen Breite platziert werden, was über die Option "Layout" konfiguriert wird.

Kacheln werden durch Klicken auf die Schaltfläche "Hinzufügen" in der unteren linken Ecke hinzugefügt, eine Kachel kann durch Klicken auf die Schaltfläche "X" in der oberen rechten Ecke der Kachel entfernt werden. Kacheln können durch Anklicken des "Strich"-Symbols in der Menüleiste minimiert und durch Anklicken des Doppelpfeil-Symbols aktualisiert werden.

> Alle Kacheln sind für das Netzwerk-Dashboard verfügbar, aber nur eine kleine Untermenge von Kacheln ist für das Computer-Dashboard verfügbar.

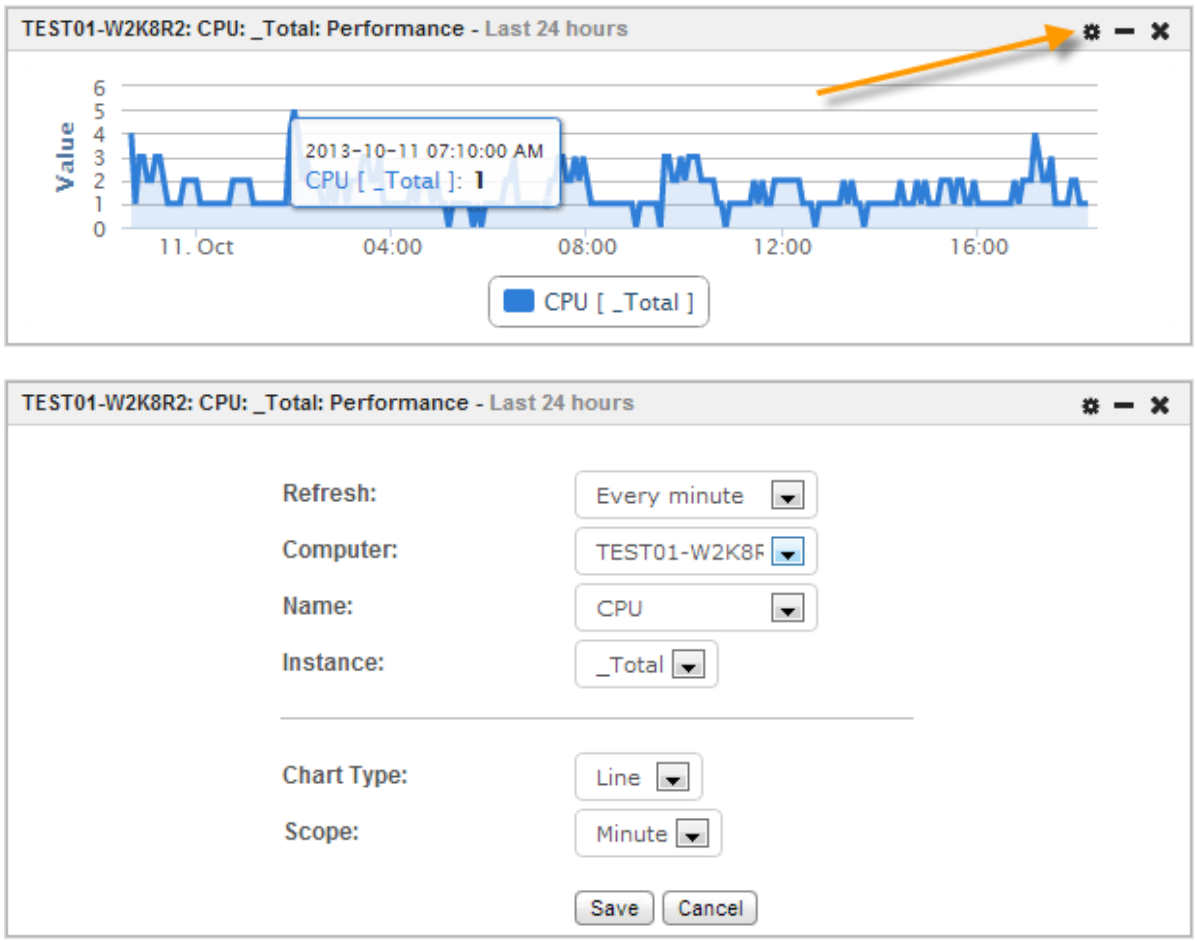


Kacheln verschieben
Eine Kachel kann verschoben werden, indem sie mit der Maus an eine neue Position gezogen wird, bis ein grauer Hintergrund sichtbar wird. Der graue Hintergrund zeigt an, wo die neue Position der Kachel sein wird. In der Abbildung unten wird die Kachel "Automatische Dienste" unter die Kachel "Disk Alerts" verschoben, wo der graue Hintergrund sichtbar wird.



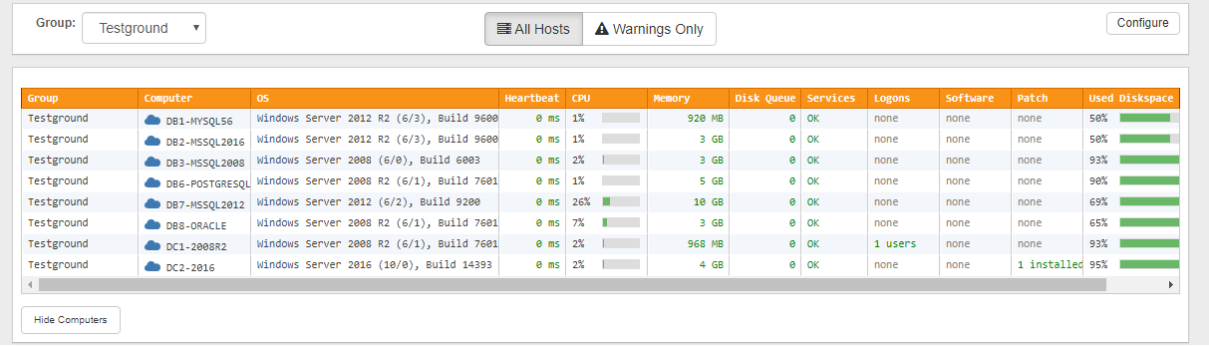
Kacheln anpassen

Einmal zum Dashboard hinzugefügte Kacheln können durch Klicken auf das Symbol für den äußersten linken Gang in der Menüleiste angepasst werden. Die meisten Kacheln erlauben die Anpassung des automatischen Aktualisierungsintervalls, des Computers, von dem die Daten bezogen werden sollen, und kachelspezifischer Einstellungen. Der folgende Screenshot zeigt eine Leistungskachel und ihre Konfiguration.



6.1.1.2 Netzwerk-Status

Die Netzwerk-Statusseite bietet einen effizienten Überblick über den Gesamtzustand aller überwachten Server und Workstations in Ihrem Netzwerk. Standardmäßig zeigt die Netzwerk-Statusseite den aktuellen Wert von 3 wichtigen Leistungszählern (CPU-, Speicher- und Festplattenauslastung) an, kann aber so angepasst werden, dass auch der aktuelle Status von zusätzlichen Leistungszählern angezeigt wird.



Group	Computer	OS	Heartbeat	CPU	Memory	Disk Queue	Services	Logons	Software	Patch	Used Diskspace
Testground	DB1-MYSQL56	Windows Server 2012 R2 (6/3), Build 9600	0 ms	1%	920 MB	0	OK	none	none	none	50%
Testground	DB2-MSSQL2016	Windows Server 2012 R2 (6/3), Build 9600	0 ms	1%	3 GB	0	OK	none	none	none	50%
Testground	DB3-MSSQL2008	Windows Server 2008 (6/0), Build 6003	0 ms	2%	3 GB	0	OK	none	none	none	93%
Testground	DB6-POSTGRESQL	Windows Server 2008 R2 (6/1), Build 7601	0 ms	1%	5 GB	0	OK	none	none	none	90%
Testground	DB7-MSSQL2012	Windows Server 2012 (6/2), Build 9200	0 ms	26%	10 GB	0	OK	none	none	none	69%
Testground	DB8-ORACLE	Windows Server 2008 R2 (6/1), Build 7601	0 ms	7%	3 GB	0	OK	none	none	none	65%
Testground	DC1-2008R2	Windows Server 2008 R2 (6/1), Build 7601	0 ms	2%	968 MB	0	OK	1 users	none	none	93%
Testground	DC2-2016	Windows Server 2016 (10/0), Build 14393	0 ms	2%	4 GB	0	OK	none	none	1 installed	95%

> Einige Spalten sind anklickbar und werden beim Anklicken auf eine andere Seite übertragen (z.B. wird durch Anklicken von "Computer" auf das "Computer-Dashboard" übertragen).

Felder

Heartbeat: Antwortzeit des Remote-Hosts in ms, oder "FEHLER", wenn der Host offline ist.

Dienstleistungen: Zeigt OK an, wenn alle für den automatischen Start konfigurierten Dienste laufen, andernfalls wird die Anzahl der gestoppten Dienste angezeigt.

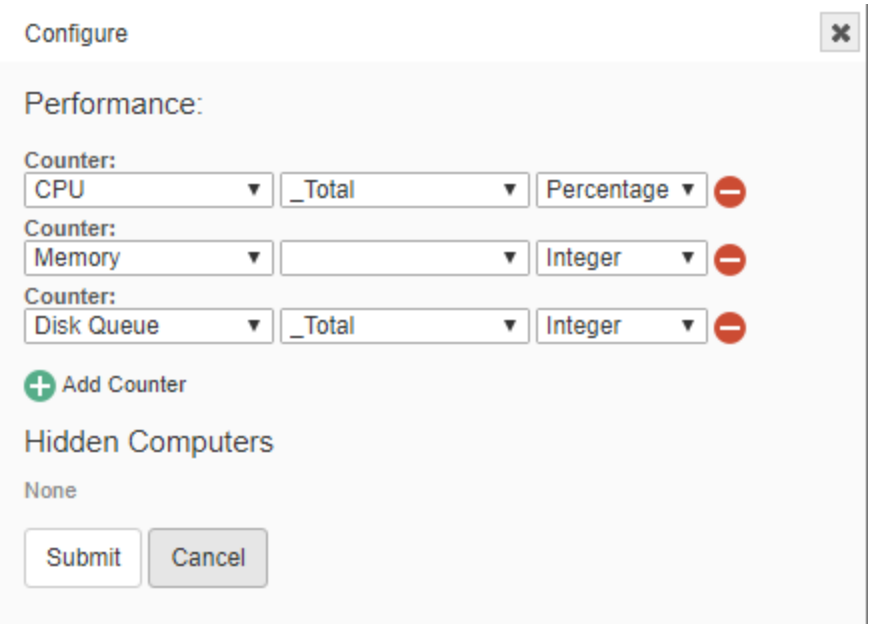
Anmelden: Dieser Wert zeigt an, wie viele Benutzer derzeit an der Maschine angemeldet sind.

Software: Dieser Wert zeigt die Anzahl der heute installierten Anwendungen oder Patches an.

Anpassung

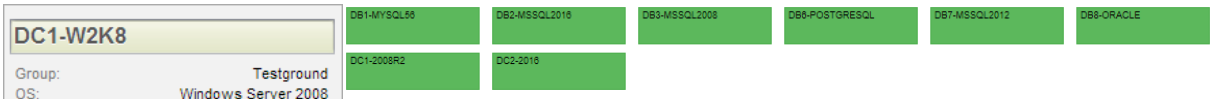
Wenn Sie auf "Nur Warnungen anzeigen" klicken, werden nur Hosts angezeigt, bei denen sich mindestens eine überwachte Komponente in einem Warn- oder Fehlerstatus befindet.

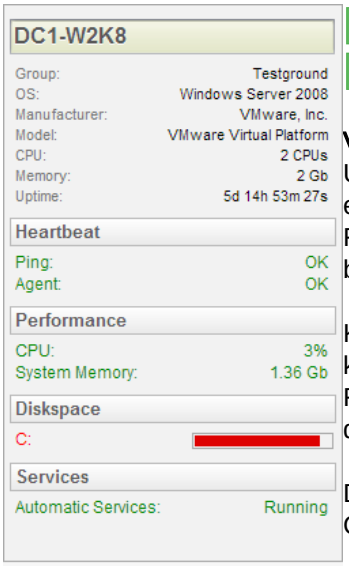
Wenn Sie auf "Konfigurieren" klicken, wird der Konfigurationsdialog aufgerufen, der die Anpassung bestehender Leistungszähler sowie das Hinzufügen neuer Leistungszähler ermöglicht.



6.1.1.3 Health Matrix

Die Health-Matrix ist eine neue und einzigartige Möglichkeit, den Gesundheitszustand eines großen Netzwerks darzustellen und gleichzeitig so wenig Bildschirmfläche wie möglich in Anspruch zu nehmen.

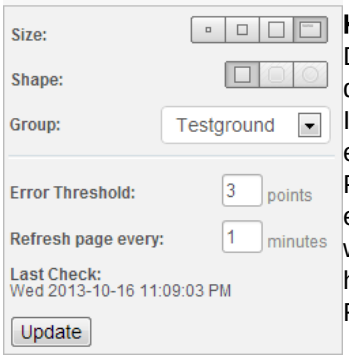




Verwendung
Um detaillierte Informationen über einen Host anzuzeigen, klicken Sie einfach auf die Kachel und überprüfen Sie die Details im linken Fensterbereich. Alle Elemente, die sich derzeit in einem Warnstatus befinden, werden in rot angezeigt.

Kachelgröße und -form, Fehlerschwelle und die Aktualisierungsintervalle können im linken Fensterbereich konfiguriert werden. Änderungen der Fehlerschwelle und der Aktualisierungsintervalle müssen durch Drücken der Schaltfläche "Aktualisieren" bestätigt werden.

Die Ausgabe kann mit der Dropdown-Liste "Gruppe" auf eine bestimmte Gruppe gefiltert werden.

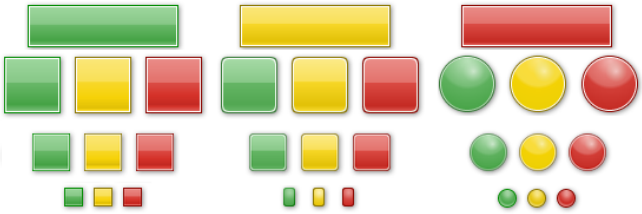


Kachel-Farben
Der allgemeine Gesundheitszustand eines überwachten Hosts wird durch die Farbe seines Quadrats / Rechtecks / Kreises angezeigt (abhängig von Ihrer Konfiguration). Der Gesundheitszustand eines Hosts wird mit Hilfe eines Punktesystems berechnet. Jedes überwachte Element (z.B. Dienst, Plattenplatz, Leistungszähler), das sich in einem Warnstatus befindet, erhält einen Punkt. Hosts ohne (0) Punkte haben einen grünen Status, während Hosts mit 1 Punkt (konfigurierbar) einen orangen (Warn-)Status haben. Hosts mit 2 oder mehr (konfigurierbaren) Punkten haben einen Fehlerstatus mit einer roten Farbe.

Status	Points	Description
	0	All monitored components are OK
	1	One monitored component is NOT OK
	2+	More than one component is NOT OK

Description is based on the default error threshold of "2"

Icons

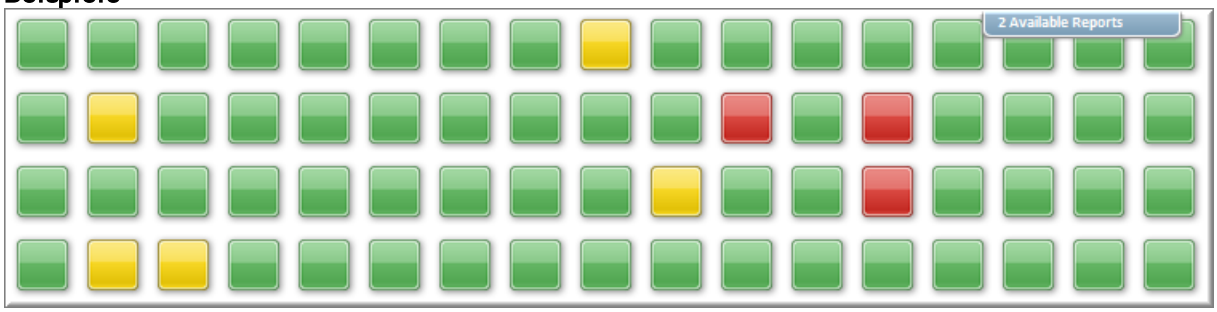


Sowohl die Icon-/Kachelform als auch die für Hosts verwendete Größe sind konfigurierbar. Sie können zwischen einem Rechteck, einem Quadrat, einem Quadrat mit abgerundeten Kanten und einem Kreis wählen. Mit Ausnahme der Rechteckform sind alle Formen in den Größen klein, mittel und groß erhältlich.

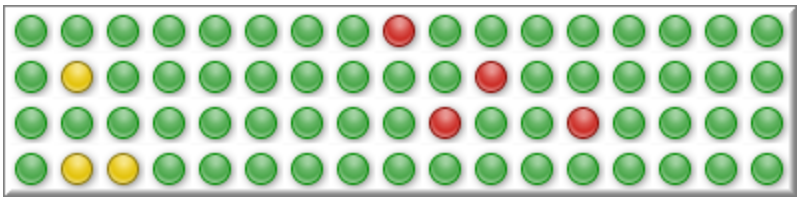
Die Rechteckform ist die einzige Form, die den Hostnamen innerhalb des Symbols anzeigt. Bei allen anderen Formen wird der Hostname abgerufen, indem Sie mit der Maus über das Symbol fahren.

Die Form und Größe des mit den Steuerelementen unteren Bildschirmseite g werden. Bitte beachten S eine globale Einstellung i alle Healthmatrix-Berichte

Beispiele



Health-Matrix mit mittlerer quadratischer Größe, die 68 Computer anzeigt und nur etwa 756 x 188 Pixel benötigt



68 Computer, die hier nur etwa 397 x 96 Pixel benötigen

6.1.2 Zusammenfassung & Details

Alle Seiten, die Logdaten (z.B. Ereignisprotokoll, Protokolldateien, Syslog, SNMP-Traps, ...) und EventSentry-Protokolldaten (z.B. Software-Installationsverlauf, Datei-Prüfsummenverlauf) abrufen, zeigen Daten sowohl in einer "Zusammenfassung" als auch in einer "Details"-Ansicht an.

Beide Ansichten greifen auf die gleichen Daten zu, zeigen die Daten aber unterschiedlich an. Die "Zusammenfassung"-Ansicht bietet einen kategorisierten Überblick über die gesammelten Daten auf hoher Ebene, um dem Benutzer ein schnelles Verständnis der Art der Daten zu ermöglichen, die in der Datenbank gesammelt wurden. Beide Ansichten haben einen gemeinsamen Seitenkopf, der das Such-(Abfrage-)Feld und das 24-Stunden-Trend-Diagramm enthält.

Die "Detailansicht" ermöglicht den Zugriff auf die Rohdaten und damit eine detaillierte Untersuchung der gesammelten Protokolldaten.

Empfohlene Vorgehensweise bei der Untersuchung von Protokolldaten:

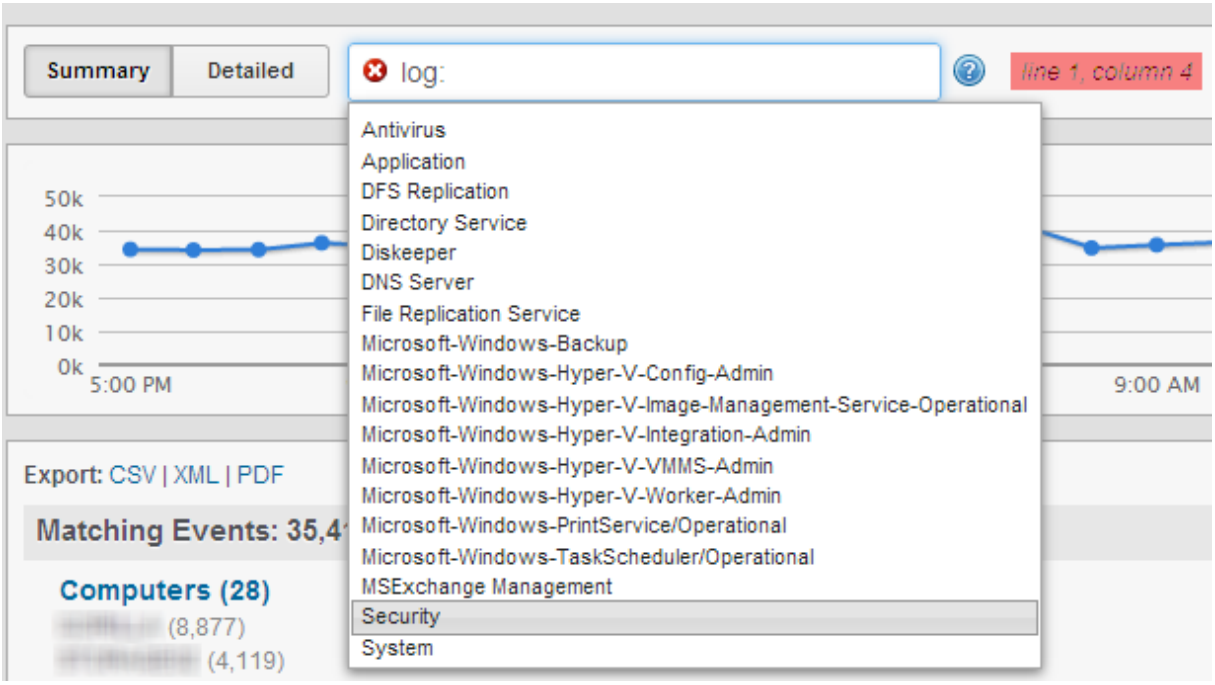
1. Zugriff auf die Ansicht "Zusammenfassung" der jeweiligen Protokolldaten
2. Einschränken der Suche indem entweder die Schaltfläche "X" verwendet oder eine Abfrage erstellt wird
3. Anpassen des Datums-/Zeitbereichs und der Resultate
4. Wechseln in die "Detailansicht"

Zeitspanne
Verwenden Sie das Dropdown-Menü für die Zeitauswahl, um den Zeitbereich der angezeigten Daten anzupassen, "Custom" ermöglicht die Auswahl einer beliebten Zeitspanne.

Sprache der Abfrage
Die Web Reports verwenden die Apache Lucene Query Parser-Syntax. Sie können grundlegende Abfragen erstellen, indem Sie entweder Elemente ausschließen (wenn Sie sich in der Zusammenfassungsansicht befinden) oder indem Sie mit der Maus auf das Suchfeld klicken, ein Feld auswählen und einen Suchwert angeben. Weitere Informationen und Beispiele finden Sie unter Abfragesyntax.

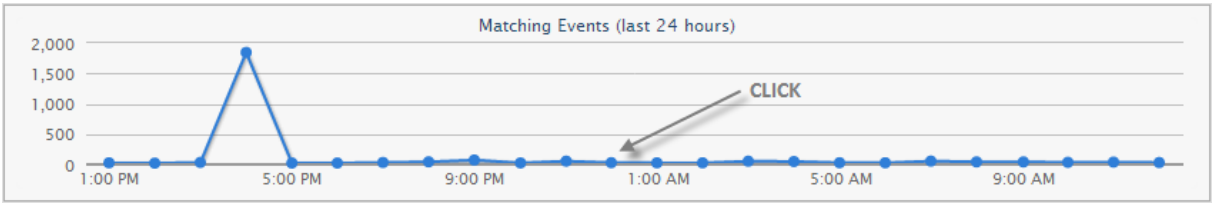
Sie können weiterhin auf das Suchfeld klicken und Ihre Abfrage sequentiell aufbauen bis sie abgeschlossen ist. Wenn Sie eine Abfrage nur mit der Maus erstellen, werden Elemente standardmäßig mit einem logischen "UND" verknüpft.

Wenn die Abfragesyntax unvollständig oder falsch ist, zeigt das Suchfeld auf der linken Seite ein rotes X Symbol, sowie auf der rechten Seite Details über den Ort des Fehlers. Das Suchfeld zeigt ein grünes Häkchen an wenn die Abfragesyntax korrekt ist.

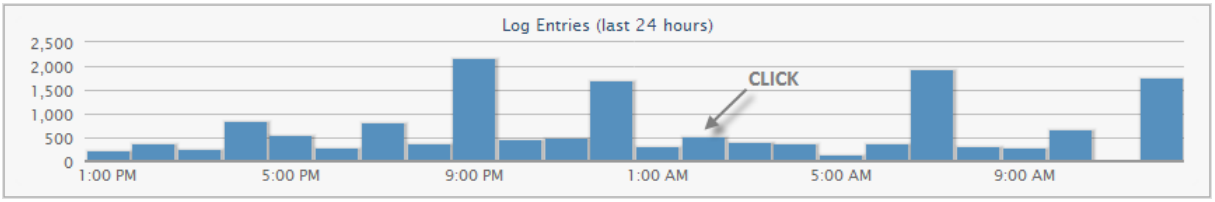


24-Stunden-Trend

Der 24-Stunden-Trend zeigt eine Trendlinie für die aktuelle Abfrage über die letzten 24 Stunden (unabhängig vom gewählten Zeitlimit). Durch Klicken auf einen Datenpunkt auf der Trendlinie wird die Suche auf diese Stunde des Tages eingegrenzt. Abhängig von der Funktion ist die Trendlinie entweder eine Linie oder ein Balkendiagramm.



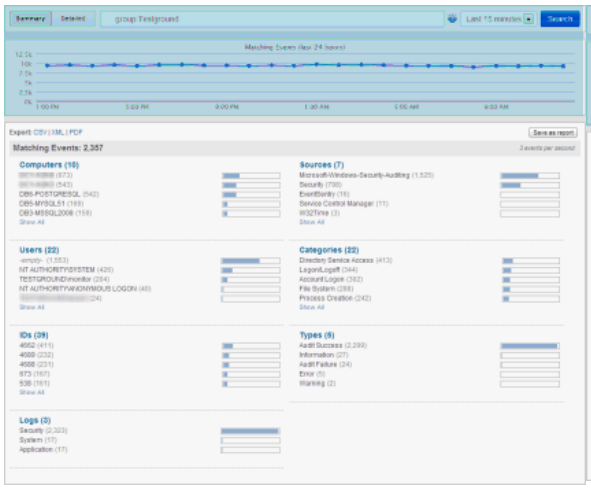
Trenddiagramm für Ereignisprotokoll-Suche



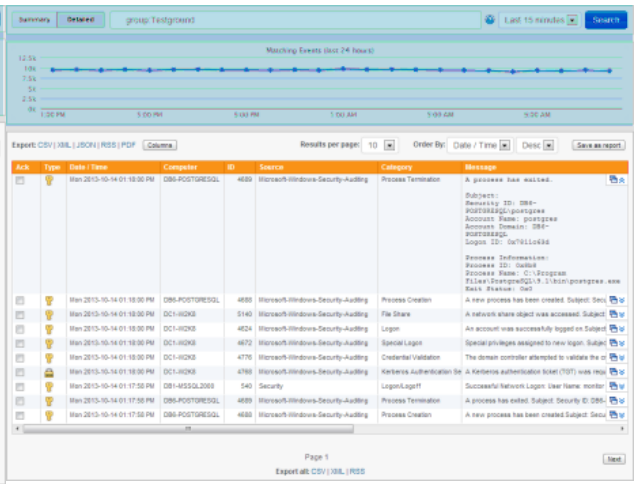
Trenddiagramm für die Suche in Protokolldateien

> Die Trendlinie zeigt **immer** Daten der letzten 24 Stunden an, unabhängig vom aktuell gewählten Zeitbereich.

Die untenstehenden Bildschirmfotos zeigen die Zusammenfassung und die Detailansicht derselben Daten nebeneinander. Beide Ansichten enthalten die Suchleiste, die Auswahl des Zeitraums und das Diagramm.



Zusammenfassende Ansicht



Detaillierte Ansicht

6.1.2.1 Abfrage-Syntax

Die Web Reports verwenden die Apache Lucene Query Parser-Syntax, die `Feld:Wert`-Paare für die Kernsyntax verwendet. Die folgenden Beispiele veranschaulichen die gebräuchlichste Syntax anhand von Beispielen.

Alle Ereignisse vom Security Ereignisprotokoll:

log:Security
Events from the "Security" event log

Sie können nach unterschiedlichen Werten des gleichen Feldes suchen, indem Sie die Werte innerhalb einer Klammer gruppieren:

log:(Application OR System)
Events from either the Application or System event log

Durchsuchen Sie mehrere Felder, indem Sie sie mit dem logischen Operator **AND** oder **OR** kombinieren:

log:Application AND source:EventSentry
Events from the Application event log with event source "EventSentry"

Schließen Sie Ergebnisse aus, indem Sie ihnen ein Minus voranstellen:

log:Security AND id:(-5447)
Events from the Security event log except events with event id 5447

Verwenden Sie den Platzhalter **?**, um ein einzelnes Zeichen abzugleichen, verwenden Sie den Platzhalter *****, um 0 oder mehr Zeichen abzugleichen:

log:Security AND category:Process*
Events from the Security event log with any category that starts with "Process"

Verwenden Sie Anführungszeichen, wenn Sie nach Textzeichenfolgen suchen, die ein oder mehrere Leerzeichen enthalten:

log:Security AND category:"Process Creation"
Events from the Security event log with category "Process Creation"

Der Feldname kann bei der Suche im Standardfeld weggelassen werden (z. B. die Ereignismeldung bei der Suche im Ereignisprotokoll):

john.johnson* OR *jack.jackson
Events containing "john.johnson" or "jack.jackson"

Beschränken Sie numerische Felder auf einen Wertebereich mit Klammern:

log:Security AND id:[4727 TO 4730]
Ereignisse für Gruppenwechsel global sicherheitsrelevanter Gruppen

name:"Applications*CPU" AND value:[5 TO *]
Leistungsstatus: Listet alle Prozesse auf, die eine CPU-Auslastung von 5% oder mehr haben

6.1.2.2 Zusammenfassung

Alle Seiten, die Daten in Textform zurückgeben (z.B. Ereignisprotokolldaten, Syslog-Daten, SNMP-Daten, Dateiprüfsummendaten usw.), bieten sowohl eine "Zusammenfassung" als auch eine "Details"-Ansicht der Daten. Die Zusammenfassungsansicht gruppiert Daten aus allen relevanten Datenfeldern, um einen Überblick über die Daten zu geben, die von der aktuell ausgewählten Funktion gesammelt wurden.

Auf Seiten, die historische Daten anzeigen (im Gegensatz zu Seiten, die aktuelle Daten anzeigen, wie z.B. "Leistungsstatus"), bietet die Zusammenfassungsansicht auch eine Zeitleiste, um die Verteilung der Daten über die letzten 24 Stunden zu visualisieren.

Summary / Detailed
Schaltet zwischen Zusammenfassung und Detailansicht um. Jede benutzerdefinierte Abfrage wird auf beide Ansichten angewendet. Durch Klicken auf die Dropdown-Liste "Letzte Stunde" wird der Zeitraum für den aktuellen Bericht geändert.

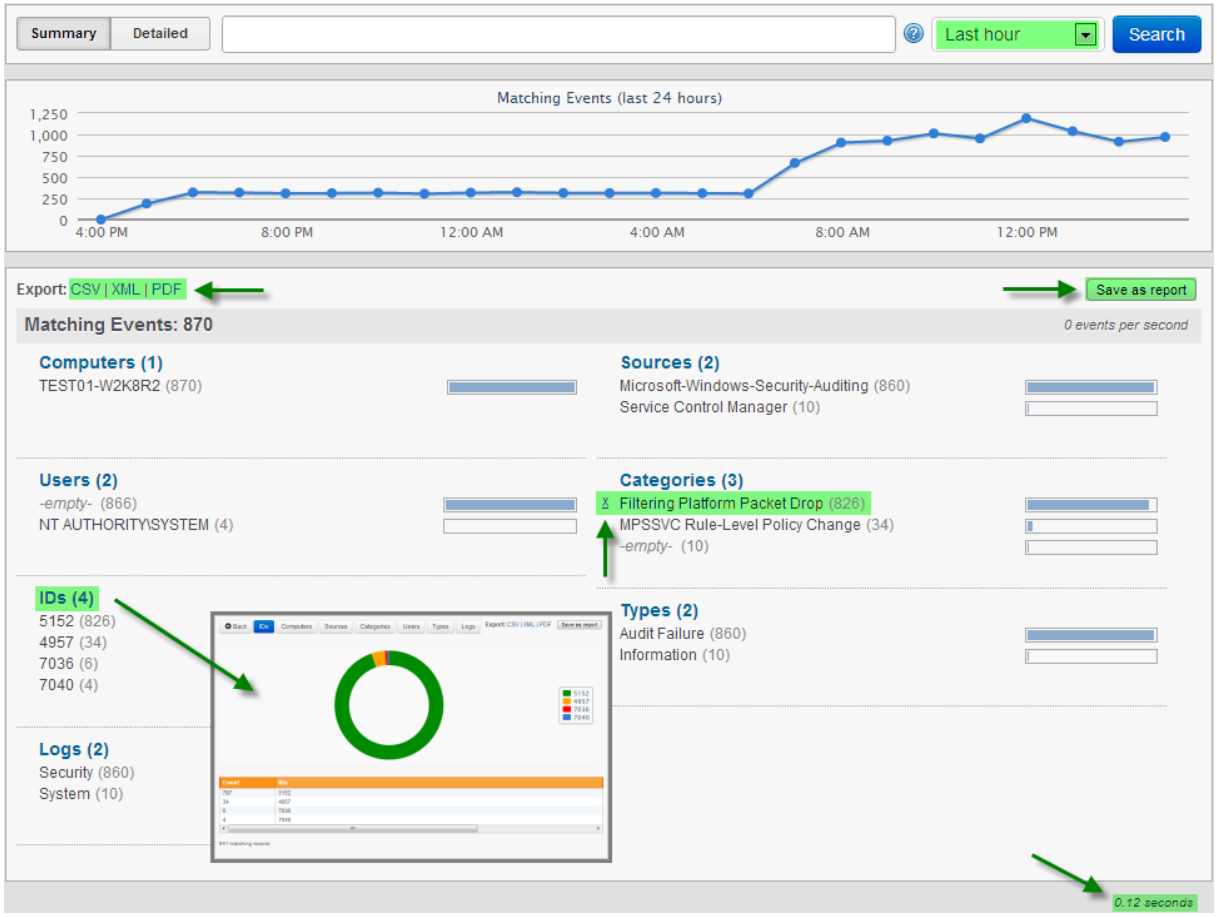
Export-Optionen
Daten können im CSV- (comma separated values), XML- und PDF-Format exportiert werden. Häufig abgerufene Suchanfragen können über den Link "Als Bericht speichern" als Bericht gespeichert werden. Berichte können als Standardansicht für eine Seite festgelegt und mit Jobs geplant werden.

Gruppenleiter
Durch Klicken auf eine beliebige Gruppenüberschrift wird auf die Seite "Gruppenausgabe" gewechselt, auf der ein Torten- oder gestapeltes Balkendiagramm angezeigt wird.

Einschließlich Elemente
Wenn Sie auf ein Element klicken, wird die Abfrage aktualisiert und die Seite neu geladen, so dass nur Datensätze, die mit diesem Element übereinstimmen, zurückgegeben werden.

Artikel ausschließen
Wenn Sie in der Zusammenfassungsansicht mit der Maus über ein Element fahren, erscheint ein kleines X neben dem Text. Wenn Sie auf das "X" klicken, wird die Seite aktualisiert und dieses Element ausgeschlossen.

Unten rechts wird die Ladezeit der Seite angezeigt.



6.1.2.3 Details

Paginierung

Die Ausgabe in der Detailansicht ist paginiert, wobei bis zu 500 Datensätze auf einer einzigen Seite angezeigt werden können. Wenn mehr Datensätze verfügbar sind, als auf eine Seite passen, wird eine Schaltfläche "Nächster" (und "Vorheriger" auf Seiten 2 und höher) angezeigt. Die Gesamtzahl der Seiten ist nicht verfügbar, da zu diesem Zeitpunkt nur eine Teilergebnisse aus der Datenbank abgerufen werden.

Ausgabe anpassen

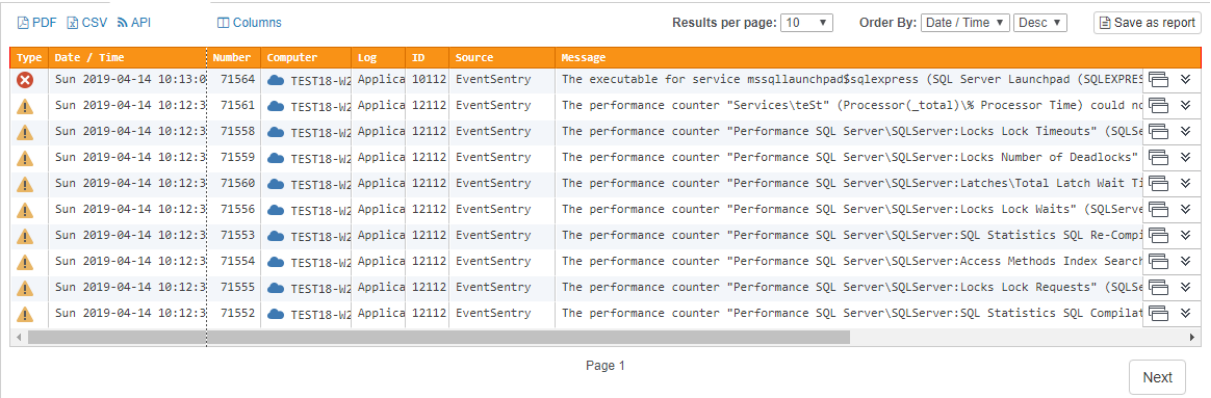
Die Sichtbarkeit der Spalten kann mit der Schaltfläche "Spalten" umgeschaltet werden. Wenn Sie auf "Speichern" klicken, wird die Spaltenauswahl für alle zukünftigen Suchvorgänge dieser Seite beibehalten. Die Ausgabe kann nach jedem verfügbaren Feld in aufsteigender oder absteigender Reihenfolge sortiert werden.

Anzeige von Aufzeichnungsdetails

Wenn verfügbar, können die Aufzeichnungsdetails durch Klicken auf die blaue Doppelpfeil-Schaltfläche (rechts) dargestellt erweitert werden. Bei der Ansicht von Ereignisprotokolldaten können die Aufzeichnungsdetails des Ereignisprotokolls auch durch Klicken auf das Doppelfenstersymbol angezeigt werden.

Export-Optionen

Die Daten können entweder für die aktuelle Seite (wie oben links verfügbar) oder für die gesamte (nicht dargestellte) Ergebnismenge exportiert werden. Die Daten können im CSV-, XML-, JSON-, RSS- und PDF-Format exportiert werden (das PDF-Format ist nur für die aktuelle Seite verfügbar).



6.1.3 Trends

Visuelle Trends visualisieren numerische Daten aus den folgenden Merkmalen:

- Leistung
- Plattenplatz
- Umgebung (Temperatur + Luftfeuchtigkeit)
- Ping-Antwort
- NetFlow-Bandbreite

Alle Trendseiten können ins PDF-Format exportiert werden.

Hostname & Feature-Auswahl
Alle Trendseiten zeigen die Auswahl des Hostnamens oben links, mit erweiterten Konfigurationsoptionen speziell für die Funktion rechts darunter.

Zeit/Datumsbereich
Der Zeit-/Datumsbereich für den Trend wird oben rechts ausgewählt und reicht von "15 Minuten" bis "Letztes Jahr". Wählen Sie "Zusammenfassung", um drei kombinierte Diagramme für die

- Letzte 12 Stunden
- Letzte 2 Tage
- Letzte Woche

Ein benutzerdefinierter Bereich kann mit der Option "Benutzerdefinierter Bereich" gewählt werden.

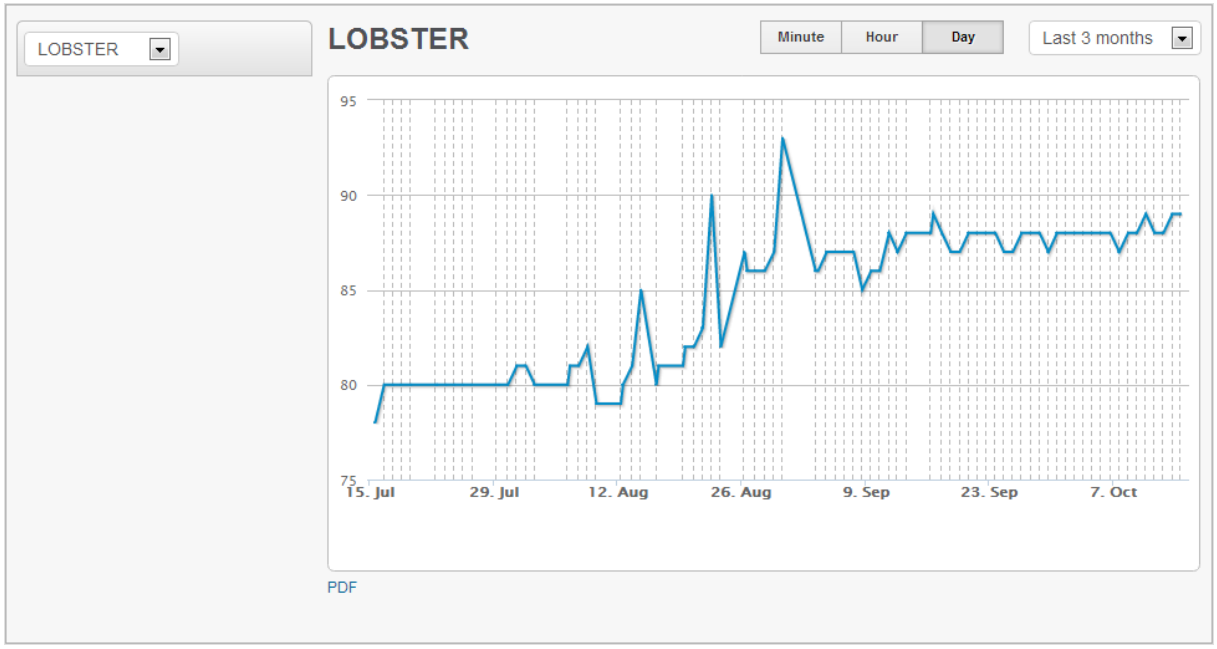
> Die Ansicht "Zusammenfassung" ist die empfohlene Anfangsansicht und bietet die beste Datenpräsentation.

Diagramm-Genauigkeit
Die Genauigkeit des Diagramms kann, sofern genügend Daten verfügbar sind, mit den Schaltflächen "Minute | Stunde | Tag" kontrolliert werden:

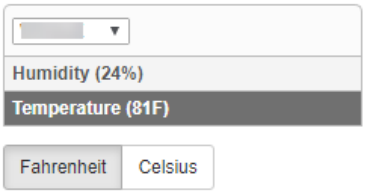
- Tag (geringste Genauigkeit, schnellste Ladezeit)

- Stunde (genaue, durchschnittliche Ladezeit)
- Minute (genaueste, längste Ladezeit)

> "Stunde" ist für die meisten Diagramme eine vernünftige Wahl, außer für Diagramme, die mehr als einen Monat umfassen. "Minute" wird nur für kurze Zeiträume von etwa einem Tag empfohlen.



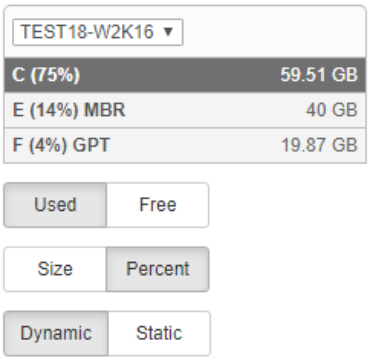
6.1.3.1 Funktionsspezifische Trendseiten



Umwelt

Alle verfügbaren Sensoren (Temperatur, Feuchte oder beide) werden unterhalb des Host-Namens angezeigt, einschließlich ihrer aktuellsten Messwerte.

Die Maßeinheit für die Temperatur kann zwischen Fahrenheit und Celsius umgeschaltet werden.



Festplattenplatz

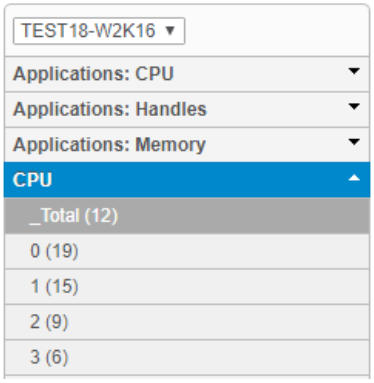
Alle überwachten Laufwerke werden unterhalb des Host-Namens angezeigt, einschließlich des Volume-Namens, des prozentualen Anteils des verwendeten Speicherplatzes und des gesamten Speicherplatzes des Volumes auf der rechten Seite.

Die Diagramme können folgend konfiguriert werden:

- Genutzten oder verfügbaren freien Speicherplatz anzeigen
- Prozent oder Größe anzeigen

Dynamisch vs. Statisch

"Statisch" zeigt den vollen Bereich auf der Y-Achse an (z.B. 0 - 100% bei Auswahl von "Prozent"), während "Dynamisch" die Y-Achse auf der Grundlage der im Diagramm angezeigten Daten dynamisch skaliert.



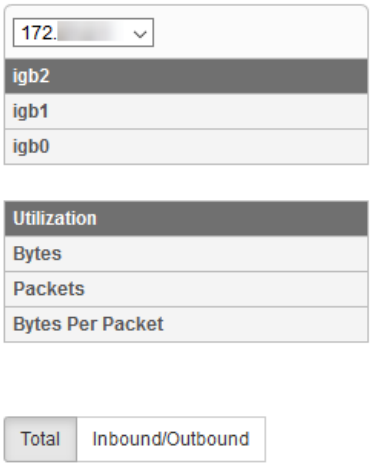
Leistung

Alle auf dem ausgewählten Host verfügbaren Leistungsindikatoren, einschließlich ihrer neuesten Werte, werden unterhalb des Hostnamens angezeigt.

Leistungsindikatoren mit mehreren Instanzen können angeklickt werden, wodurch alle verfügbaren Instanzen erweitert und angezeigt werden. Instanzen oder Zähler, die sich in einem Alarmzustand befinden, werden in rot angezeigt.

Das Klicken auf "Zähler / Counter" wechselt in die Leistungszähler-zentrierte Ansicht, welche die Leistungshistorie eines oder mehrerer Computer eines Counters in einem Diagramm anzeigt.

Sie können in ein Diagramm zoomen, indem Sie eine Te Diagramms mit der Maus auswählen. Klicken Sie einfach r Maustaste auf den Anfang des Zeitbereichs, halten Sie sie bewegen Sie die Maus nach rechts, lassen Sie die linke M wenn der gewünschte Bereich ausgewählt wurde.



NetFlow-Bandbreite

Zeigt die IP-Adresse des NetFlow-Exporters zusammen mit allen Schnittstellen, für die NetFlow-Bandbreiteninformationen verfügbar sind.

Für jede Schnittstelle sind die folgenden Metriken verfügbar:

- Auslastung in Prozent (nur verfügbar, wenn NetFlow die Geschwindigkeit der Schnittstelle bestimmen kann, entweder manuell oder über SNMP)
- Bytes
- Pakete
- Bytes pro Paket

Total zeigt die kombinierte Anzahl der eingehenden und ausgehenden Bytes an. Diagramme, die zwischen ausgehenden und eingehenden Bytes unterscheiden, sind nur verfügbar, wenn sie vom Exporteur unterstützt werden, andernfalls sind die Diagramme für eingehende/ausgehende Bytes leer.

Qualität des Netzwerks

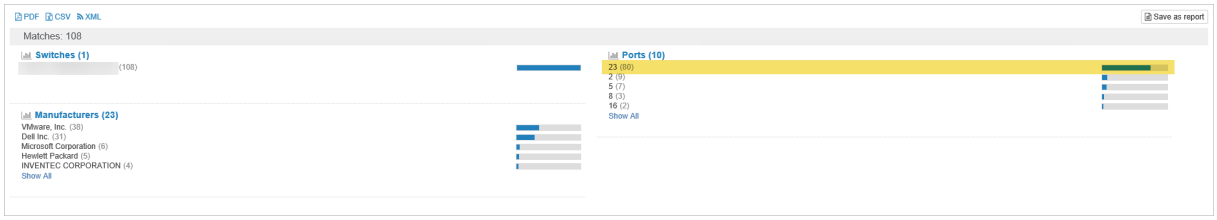
Wählen Sie einen Host aus, um die Ping-Antwortzeit des ausgewählten Zeitraums anzuzeigen.

6.1.4 Inventar

6.1.4.1 Switch

Zeigt alle überwachten Switches und ihre Zuordnung von Port zu MAC-Adressen.

Entfernen von Duplikaten
Wenn Switches kaskadiert werden (was in der Regel der Fall ist), tauchen einige MAC-Adressen mehrfach auf - sowohl auf dem Uplink als auch auf dem eigentlichen Port, mit dem sie verbunden sind. Uplink-Ports sind normalerweise leicht zu identifizieren, da die meisten Geräte damit verbunden sind. In der Abbildung unten ist Port **23** ein Uplink-Port.



Up-Link-Ports können leicht aus der Ergebnismenge entfernt werden, indem Sie auf das "X"-Symbol links neben dem Port klicken. Dies kann für alle überwachten Switches wiederholt werden, und es kann eine Standardberichtsseite erstellt werden, auf der diese Einträge standardmäßig immer ausgelassen werden.

Einzelheiten
Die Detailansicht zeigt alle inventarisierten Switch-Ports, einschließlich Hostname, IP-Adresse, MAC-Adresse und MAC-Adressenanbieter. Die IP-Adresse und/oder Host-Namen sind nur verfügbar, wenn diese Informationen aus anderen Quellen bezogen werden können, wie z.B. von den Agenten gemeldete Daten, ARP-Dämon und anderen.

6.2 Seiteneigenschaften

Einige Seiten weisen einzigartige Merkmale auf, die im Folgenden beschrieben werden:

Status - Heartbeat
Um die Netzwerkverfügbarkeit eines weiteren Hosts anzuzeigen, wechseln Sie in die Detailansicht und überprüfen Sie die Spalten Betriebszeit, Ausfallzeit, verstrichene Zeit und Verfügbarkeit.

Status - Performance
Standardmäßig zeigt die Detailansicht der Leistungsstatusseite den zuletzt erfassten Wert eines Leistungszählers an. Wenn der Zeitbereich von "Aktuell" auf einen bestimmten Zeitbereich wie "Heute" geändert wird, wird stattdessen der Durchschnitt aus allen Werten über diesen Zeitraum berechnet.

Protokolle - Getrennte Protokolldateien
Formatierte Log-Dateien sind mit einer Log-Datei-Definition verbunden, die ausgewählt werden muss, um die gesammelten Daten korrekt abzubilden. Da sich Änderungen der Protokolldateidefinitionen auf die Ausgabe auswirken können, speichert EventSentry eine Historie aller Revisionen. Um Daten anzuzeigen, die mit einer anderen als der aktuellen Revision erfasst wurden, muss die richtige Revision ausgewählt werden. Revisionen werden der Reihe nach gezählt, wobei die erste (älteste) Revision Revision 1 ist.

Konformität - Prozesse
Die Spalte "Dauer" in der Detailansicht unterstützt den Bereichsoperator im Abfragefeld. Zum Beispiel zeigt **Duration:[180 TO *]** nur Prozesse an, die 3 Minuten oder länger liefen.

Einhaltung - Richtlinienänderungen - Audit-Richtlinie
Unter Windows 2003 und früher listet alle 9 verfügbaren Richtlinienkategorien und ihre effektiven Werte für Erfolg und Misserfolg auf. Unter Windows 2008 und später sind deutlich mehr Auditierungskategorien enthalten als in früheren Versionen von Windows, und daher werden nur die Kategorien aufgelistet, deren Werte sich geändert haben. Daher enthalten die Felder **Unterkategorie** und **Unterkategorie-GUID** detaillierte Informationen über die geänderte Richtlinie.

Compliance - Richtlinienänderungen - Vertrauensbeziehungen
Die Spalte "SID-Filterung" zeigt an, ob die SID-Filterung für den Trust aktiviert ist oder nicht.

Geschichte - Uptime
Der Verlauf der Betriebszeit wird vom Agenten nach dem Neustart oder Einschalten eines Servers oder einer Workstation aktualisiert. Daher spiegelt diesr Betriebszeitbericht nicht die aktuelle Betriebszeit eines Hosts wider - prüfen Sie stattdessen die Seite Inventar - Computer.

Inventarisierung - Computer
Die Computer-Inventarisierungsseite zeigt detaillierte Hardware-Informationen über einen Host, einschließlich Modell- und Seriennummern, installierter Speicher, Controller und Netzwerkkarten, Festplatten und vieles mehr. Die Registerkarten Software, Prozesse und Änderungen sind nur auf Windows-Hosts verfügbar, die mit einem Agenten überwacht werden.

Hardware von DELL oder HP
Ein Garantiefeld zeigt an, wann die Garantie für einen Computer abgelaufen ist oder abläuft, einschließlich zusätzlicher Informationen über die Art der für diesen Computer verfügbaren Garantie. Wenn die Verwaltungssoftware des Herstellers (z.B. DELL OpenManage) installiert ist, dann sind zusätzliche Informationen über Serverkomponenten wie Netzteile, Systemlüfter, Temperatursensoren und mehr auf der Registerkarte **Managed Hardware** verfügbar.

Nicht-Windows-Hosts über SNMP überwacht
Auf Hosts, die über SNMP überwacht werden, ist nur die Registerkarte "Hardware" verfügbar, und es wird nur eine Teilmenge der Informationen im Vergleich zu Windows-Hosts angezeigt.

6.3 Berichte & Jobs

Häufige Suchanfragen können von fast allen Seiten (mit Ausnahme der meisten Seiten unter "Dashboards" und "Einstellungen") als Bericht gespeichert werden. Berichte können auch so geplant werden, dass sie automatisch mit Jobs ausgeführt werden.

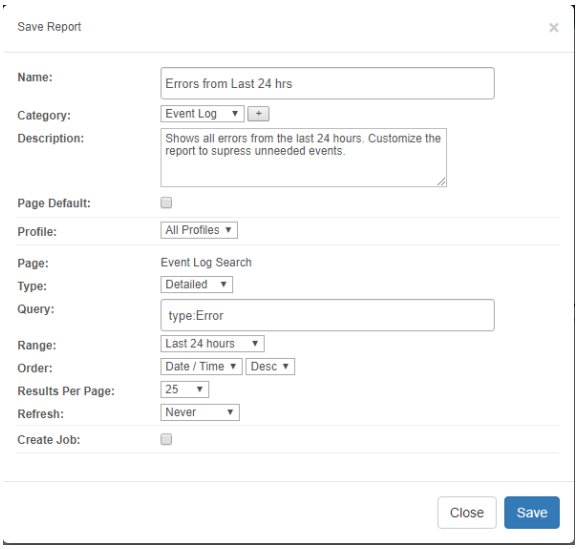
Um einen Bericht zu erstellen, führen Sie eine beliebige Seite aus, passen Sie sie an und klicken Sie auf die Schaltfläche "Als Bericht speichern". Wenn die Schaltfläche "Als Bericht speichern" nicht verfügbar ist, klicken Sie auf die Schaltfläche "Optionen"  oben rechts auf der Seite.

Bei der Erstellung eines neuen Berichts können die folgenden Felder angegeben werden:

- Name des Berichts
- Bericht Kategorie
- Beschreibung (optional)
- Seite Standard
- Job erstellen

Standardseite

Jeder Seite in den Web Reports kann ein Bericht "Page Default" zugeordnet werden. Wenn einer Seite (z.B. Heartbeat- Status, Trends - Leistung) ein Standardbericht zugeordnet ist, dann wird dieser Bericht (anstelle der Standardansicht "Zusammenfassung") geladen, wenn die Seite aufgerufen wird. Es kann also nur einen "Seitenvorgabe-Bericht" pro Seite geben.



Berichte bearbeiten

Vorhandene Berichte können über die Seite "Berichte - Berichte auflisten" verwaltet werden, wo man alle konfigurierten Berichte bearbeiten, ausführen, löschen und überprüfen kann. Alle Eigenschaften eines Berichts, mit Ausnahme des Seitentyps, können bearbeitet werden, nachdem ein Bericht erstellt wurde. Nur Berichte, die mit dem derzeit aktiven Profil verknüpft sind, oder Berichte, die für "Alle Profile" konfiguriert sind, werden aufgelistet.

Überprüfung / Review

Wenn ein Bericht regelmäßig überprüft werden muss, kann "Eine Überprüfung erfordern" konfiguriert werden. Berichte, die nicht im erforderlichen Zeitraum ausgeführt wurden, erscheinen sowohl im Widget "Überfällige Berichte" auf dem Netzwerk-Dashboard als auch auf der Seite "Berichte auflisten". Ein Bericht kann für eine Überprüfung konfiguriert werden, indem Sie auf die Schaltfläche "Überprüfung" auf der Seite "Berichte auflisten" klicken.

Eingebaute Berichte

EventSentry wird mit einer Reihe von eingebauten Berichten ausgeliefert, die beim ersten Klicken auf die Registerkarte "Eingebaute Berichte" geladen werden. Eingebaute Berichte verhalten sich wie reguläre Berichte und können bearbeitet, gelöscht usw. werden.

Profile

Standardmäßig ist ein Bericht automatisch mit dem aktuellen Profil verknüpft und wird nur in der Berichtsliste für dieses Profil angezeigt. Ein Bericht kann entweder mit einem einzelnen Profil (Voreinstellung) oder mit allen Profilen verknüpft werden.

Stellenangebote

Wenn ein Bericht erstellt oder bearbeitet wird, kann durch Ankreuzen des Kontrollkästchens "Create Job" sofort ein Job erstellt werden. Jobs können auch auf der Seite "Berichte - Jobs" verwaltet werden.

Bestehende Berichte können über die Seite "Berichte - Berichte auflisten" verwaltet werden.

Kopieren von Berichten auf verschiedene Computer

Berichte von allen Profilen werden in der Datei "reports.xml" gespeichert, die sich im Unterverzeichnis "WebReports\conf" des EventSentry Installationsverzeichnisses befindet. Die XML-Datei kann durch einfaches Ersetzen der Datei "reports.xml" zu/von einem anderen Host kopiert werden.

Berichthistorie

Jedes Mal, wenn ein Bericht manuell (und nicht als Teil eines Jobs) ausgeführt wird, werden Details über die Ausführung des Berichts in die Berichtshistorie aufgenommen. Die folgenden Informationen über einen Bericht sind unter "Berichte - Berichtshistorie" verfügbar:

- Datum/Uhrzeit
- Name des Berichts
- Benutzername
- Ladezeit
- Zurückgegebene Ergebnisse (falls zutreffend)

6.3.1 Jobs

Jobs führen automatisch Berichte in einem bestimmten Intervall aus und werden per E-Mail an einen oder mehrere Empfänger gesendet.

Wenn Sie auf die Schaltfläche "Job hinzufügen" in der oberen rechten Ecke der Seite "Jobs" klicken, wird ein Bericht erstellt. Wie Berichte können Jobs auf der "Jobs"-Seite mit den Links "Bearbeiten" und "Löschen" bearbeitet oder gelöscht werden.

Format
Berichte können entweder im HTML-, PDF- oder CSV-Format gesendet werden.

Leere Berichte senden
Wenn diese Option auf "Ja" gesetzt ist, werden Berichte auch dann gesendet, wenn sie keine Daten enthalten (wenn der zugrunde liegende Bericht keine Datensätze liefert). Bei der Einstellung "Nein" werden Berichte nur dann per E-Mail versandt, wenn sie mindestens einen Datensatz enthalten.

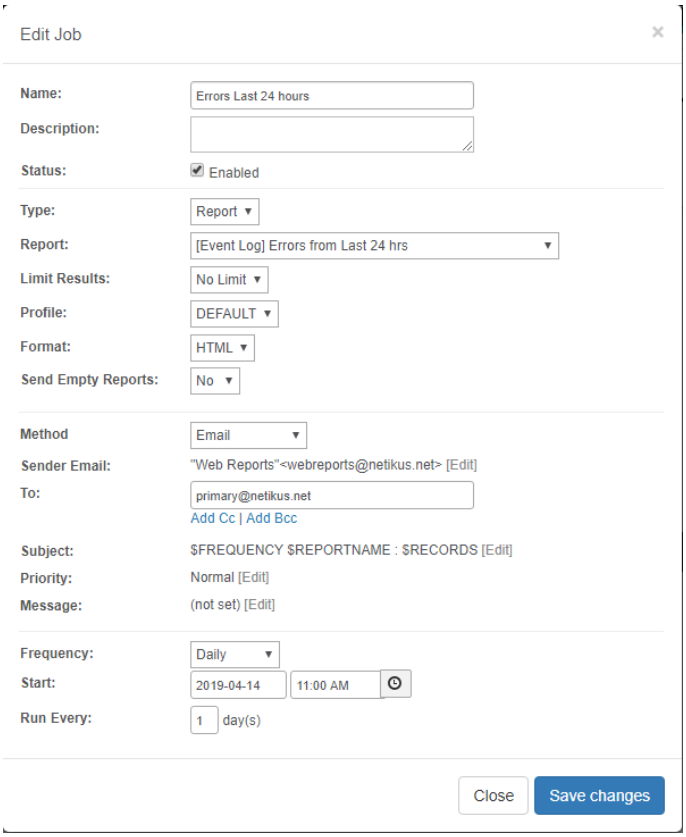
Profile
Wenn ein Bericht mit "Alle Profile" verknüpft ist, dann muss der Job das Profil festlegen, unter dem der Bericht ausgeführt werden soll. Wenn der Bericht bereits mit einem bestimmten Profil verknüpft ist, dann verwendet der Job auch dieses Profil.

E-Mail
E-Mails, die von einem Auftrag versendet werden, können stark angepasst werden, indem der Absender, die CC- und BCC-Empfänger, der Betreff und der Nachrichtentext festgelegt werden. Die folgenden Variablen werden im Betreff unterstützt:

- $FREQUENCY
- $REPORTNAME
- $RECORDS

Häufigkeit
Aufträge können einmal oder in konfigurierbaren Frequenzen gesendet werden:

- Minutenweise
- Stündlich
- Täglich
- Wöchentlich
- Monatlich



6.3.1.1 ADMonitor-Benutzerpasswort-Erinnerungen

Da ADMonitor weiß, wann das Passwort eines Benutzers abläuft, kann er täglich E-Mails zum Ablauf des Passworts direkt an den Endbenutzer senden, wenn das Passwort kurz vor dem Ablauf steht. Die einzige Voraussetzung ist, dass es eine vorhersehbare Möglichkeit gibt, die E-Mail-Adresse des Endbenutzers unter Verwendung eines der in den Web Reports verfügbaren Benutzerattribute dynamisch aufzubauen.

E-Mails zum Ablauf des Passworts werden auf der Seite Berichte -> Jobs im Abschnitt "E-Mail-Benutzer-Passwort-Ablauferinnerungen" konfiguriert. Neue Erinnerungs-E-Mails werden mit dem Link "Add Reminder" hinzugefügt, und es können mehrere Erinnerungs-E-Mails konfiguriert werden (z.B. um verschiedene Domänen anzusprechen).

Erinnern bei Ablauf (Tage)
Sendet eine E-Mail, wenn das Passwort innerhalb der gewählten Anzahl von Tagen abläuft.

E-Mail-Attribut bevorzugen, falls verfügbar
AD enthält ein E-Mail-Attribut. Wenn ein E-Mail-Attribut aktiviert und konfiguriert ist, wird dies zuerst für die Email Adresse verwendet.

E-Mail-Format
Wenn das E-Mail-Attribut bei einem Benutzer nicht gesetzt ist, muss die E-Mail-Adresse dynamisch unter Verwendung der verfügbaren Variablen aufgebaut werden:

$UPN
$FIRSTNAME
$LASTNAME
$FIRSTNAME_INITIAL
$LASTNAME_INITIAL
$SAM

Diese Funktion kann nicht verwendet werden, wenn die E-Mail-Adresse nicht mit den verfügbaren Variablen definiert werden kann (z.B. mit einem mittleren Anfangsbuchstaben).

Filter
Die E-Mail-Funktion zur Passworterinnerung listet standardmäßig alle aktiven Benutzerkonten auf, kann aber so eingeschränkt werden, dass sie nur für eine bestimmte Domäne oder nur für administrative Benutzer gilt.

6.4 Wartung

Der Wartungsabschnitt bietet Funktionen zur Wartung und Verwaltung der EventSentry Datenbank.

Wartungs-Assistent
Der Wartungsassistent löscht alte Daten aus der Datenbank, siehe Wartungsassistent für weitere Informationen.

Verwendung der Datenbank
Diese Seite zeigt, wie viel Platz in der EventSentry Datenbank verbraucht wird, aufgeschlüsselt nach Funktionen. Die für jede Datenbank verfügbaren Statistiken können variieren. Die Seite ist für die integrierten Datenbanken PostgreSQL und Microsoft SQL Server® verfügbar.

Agenten-Status
Diese Seite zeigt das letzte Mal, als ein Agent auf einem überwachten Host Daten in die Datenbank geschrieben hat, aufgeschlüsselt nach den folgenden Merkmalen:

- Ereignisprotokoll
- Heartbeat
- Leistung
- Disks

- Umwelt

6.4.1 Wartungs-Assistent

Der **Wartungsassistent** ermöglicht alte Daten aus der EventSentry Datenbank zu löschen. Daten können auch automatisch mit einem Befehlszeilen-Dienstprogramm entfernt werden.

Alle mit dem Wartungsassistenten gelöschten Daten werden dauerhaft entfernt, und es gibt keine Möglichkeit, die Daten zurückzubekommen, es sei denn, Sie verfügen über eine funktionierende Datenbanksicherung. Der Wartungsassistent wird für alle Aufgaben nach dem Login/Passwort des Datenbankadministrators (z.B. postgres, sa, ...) fragen.

Allgemein

Leistungsindikator:	Entfernt alle Verweise auf den/die ausgewählten Leistungszähler
Logischer Antrieb:	Entfernt alle Verweise auf das/die ausgewählte(n) logische(n) Laufwerk(e) auf dem ausgewählten Host
Binäre Daten:	Entfernt **alle** binären Daten
Virtuelle Maschine	Entfernt Informationen zu virtuellen Maschinen
Log-Datei	Entfernt Protokolldatei-Definitionen

Gastgeber

Alle Instanzen:	Entfernt alle Daten des/der ausgewählten Hosts
Bestimmte Instanzen:	Entfernt eine oder mehrere Instanzen des ausgewählten Hosts (z. B. nur alle Ereignisprotokolldaten entfernen)

- Computer werden von der Verwaltungskonsole als "verwaist" gekennzeichnet, wenn ein Computer aus einer mit Active Directory verknüpften Gruppe aus Active Directory entfernt wird. Durch Klicken auf das Kontrollkästchen "Verwaiste Computer" werden automatisch alle Computer ausgewählt, die als verwaist markiert sind.

- Wenn alle oder einige Instanzen entfernt werden, werden standardmäßig nur Computer angezeigt, auf denen ein Agent ausgeführt wird. Um Hosts zu entfernen, auf denen kein Agent ausgeführt wird, klicken Sie auf das Kontrollkästchen "Hosts ohne Agent einbeziehen". In den meisten Fällen wird dadurch die Anzahl der angezeigten Hosts deutlich erhöht.

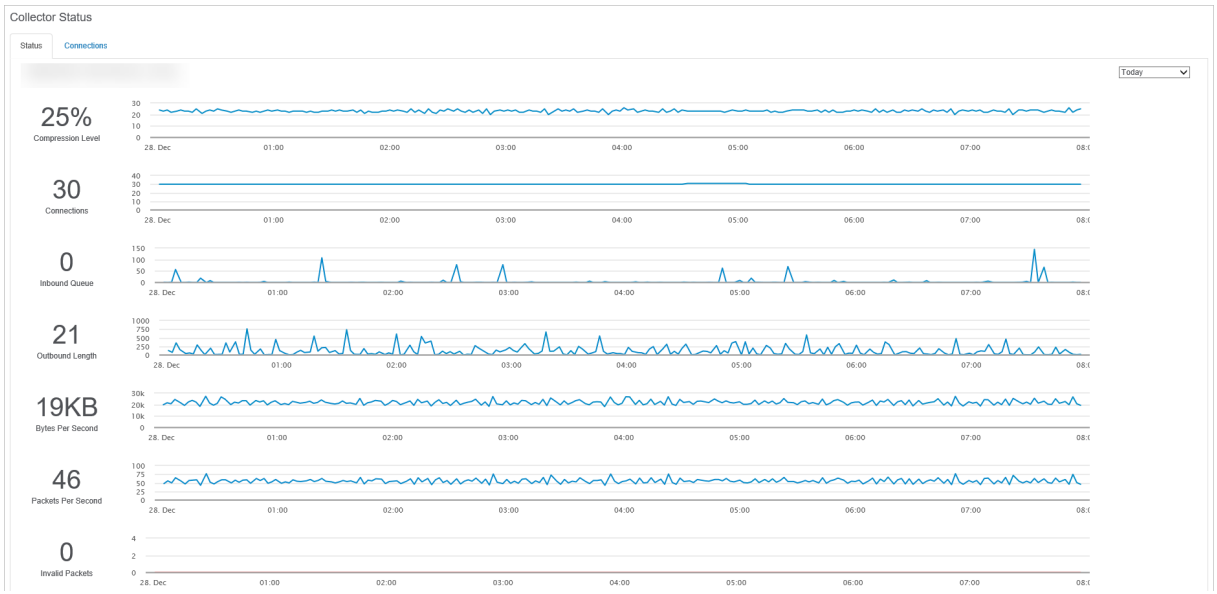
Abstimmung

Mit dem Tuning können Sie Daten, die älter als eine bestimmte Anzahl von Tagen sind, aus allen oder ausgewählten Instanzen entfernen. Beispielsweise können alle Dateizugriffs- und Prozessverfolgungsdaten, die älter als 90 Tage sind, entfernt werden. Das Tuning kann entweder auf alle oder nur auf ausgewählte Hosts angewendet werden.

Anstatt die Daten sofort zu bereinigen, kann mit der SQL-Schaltfläche in Schritt 3 ein Satz von SQL-Anweisungen generiert werden. Die SQL-Anweisungen können dann zu einem späteren Zeitpunkt ausgeführt werden.

6.4.2 Collector Status

Die Collectorß Statusseite bietet Leistungs- und Integritätsstatistiken für jeden installierten Collector. In der Collector-Konfiguration für diese Seite muss "Collect Statistics" aktiviert sein, um Informationen anzuzeigen.



Kompressionsstufe
Die Komprimierungsrate.

Verbindungen
Die Anzahl der mit dem Collector verbundenen Agenten.

Eingehende Warteschlange
Die Anzahl der Pakete, die vom Collector empfangen, aber noch nicht zur Verarbeitung dekodiert wurden. Eine anhaltend hohe Zahl kann darauf hindeuten, dass der Collector nicht über genügend CPU-Ressourcen verfügt, um Pakete zu verarbeiten.

Ausgangswarteschlange
Die Anzahl der Datenelemente, die erfolgreich aus der Eingangswarteschlange dekodiert, aber noch nicht an die Aktion (meistens eine Datenbank= gesendet wurden. Die Anzahl der Objekte in der Warteschlange sollte gering sein, eine große Länge der Ausgangswarteschlange deutet normalerweise auf ein Performance-Problem mit der Datenbank hin.

Bytes pro Sekunde
Die Anzahl der empfangenen Bytes pro Sekunde.

Pakete pro Sekunde
Die Anzahl der Pakete pro Sekunde. Jedes Paket kann ein oder mehrere Datenelemente (z.B. Ereignisprotokolleintrag, Leistungsdaten usw.) enthalten.

Ungültige Pakete
Ein Paket gilt als ungültig, wenn es nicht entschlüsselt werden kann. Ungültige Pakete können auftreten, wenn es eine (signifikante) Versionsabweichung zwischen dem Collector und den Agenten gibt. Diese Zahl sollte immer 0 sein.

6.5 Einstellungen

6.5.1 Profile

Profile unterstützen mehrere Datenbankverbindungen innerhalb einer einzigen Installation der Web Reports. Standardmäßig wird nur ein Profil eingerichtet. Mehrere Profile sind in einer Vielzahl von Szenarien nützlich:

- Umschalten zwischen einer primären und einer Archivdatenbank oder zwischen mehreren Datenbanken
- Umschalten zwischen Datenbanken verschiedener Kunden ("Multi-Tenancy")

Im Allgemeinen legt ein Profil die Sprache, die Eigenschaften der Datenbankverbindung sowie die E-Mail-Einstellungen (die vor allem für Jobs verwendet werden) fest.

> Wenn die Zugriffskontrolle aktiviert ist, können Benutzer auf ein oder mehrere Profile beschränkt werden.

Sie können zwischen den Profilen wechseln, indem Sie auf den Profilnamen ("EVENTSENTRY" als Voreinstellung) auf dem linken oberen Bildschirm der Web Reports klicken, wie unten dargestellt:

Profil-Einstellungen
Standard-Profil
Dies ist das Profil, das standardmäßig geladen wird, wenn mehrere Profile vorhanden sind.

UTC
Diese Einstellung muss mit der Einstellung in den "Globalen Optionen" der Verwaltungskonsole übereinstimmen. Wenn Agenten Daten im UTC-Datum/Zeit-Format schreiben, zeigen die Web Reports alle Zeitstempel in der lokalen Zeitzone an, wie unter "Einstellungen" konfiguriert.

Erstellen und Löschen von Profilen
Erstellen eines neuen Profils: Um ein neues Profil zu erstellen, navigieren Sie zu "Einstellungen - Profile" und klicken Sie oben links auf "Neues Profil erstellen" . Geben Sie alle erforderlichen Profileinstellungen an und klicken Sie unten auf die Schaltfläche "Submit".

Löschen eines Profils: Um ein Profil zu löschen, wechseln Sie zunächst zu dem Profil, das Sie löschen möchten, indem Sie auf den Profilnamen oben links klicken. Navigieren Sie dann zu "Einstellungen - Profile" und klicken Sie auf die Schaltfläche "Aktuelles Profil löschen".

6.5.2 Zugriffskontrolle

Der Zugriff auf die Web-Reports kann eingeschränkt werden, so dass nur authentifizierte und autorisierte Benutzer Zugriff haben. Die Zugriffskontrolle unterstützt auch Multi-Tenancy, indem sie Benutzern nur Zugriff auf Daten von bestimmten Hosts gewährt.

Die Zugriffskontrolle unterstützt Folgendes:

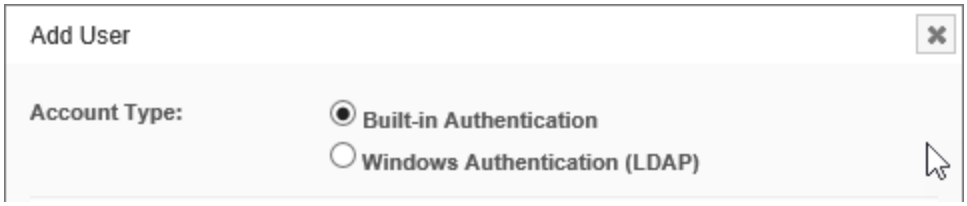
- Benutzer und Gruppen erstellen
- Benutzer über LDAP(S) authentifizieren
- Beschränken Sie Benutzer auf eine Reihe von Bereichen in den Web-Reports
- Zugriff auf Profile kontrollieren
- Blockieren bestimmter Bereiche in Web-Reports von Benutzern
- Benutzer darauf beschränken, nur Daten von bestimmten Hosts anzuzeigen

> Der **Standardbenutzername** für den ersten Benutzer ist **"admin"**, wenn die Zugriffskontrolle aktiviert wird.

Die Zugriffskontrolle kann aktiviert werden, wenn Sie EventSentry und die Web-Reports zum ersten Mal einrichten, oder jederzeit danach, indem Sie zu Einstellungen -> Zugriffskontrolle navigieren. Wenn die Zugriffskontrolle aktiviert wird, muss mindestens ein Benutzer angelegt werden ("admin" standardmäßig).

LDAP

Standardmäßig verwenden Benutzerkonten eine integrierte Authentifizierung, wobei das Benutzerkennwort von den Web-Reports verwaltet wird. Wenn eine Windows Active Directory-Infrastruktur verfügbar ist, empfiehlt es sich, die LDAP-Unterstützung zu aktivieren, damit die Benutzer nicht mehrere Passwörter verwalten müssen. Wenn die LDAP-Unterstützung aktiviert wird, kann die Authentifizierung auf einen LDAP(S)-Server ausgelagert werden, wenn ein Konto vom Typ "Windows-Authentifizierung (LDAP)" erstellt wird.



Um die LDAP-Unterstützung zu aktivieren, schalten Sie die LDAP-Unterstützung auf "Aktiviert", klicken Sie auf den Link "LDAP-Server konfigurieren" und geben Sie die IP-Adresse oder den Hostnamen eines Domänencontrollers an, auf dem LDAP ausgeführt wird.

Benutzer verwalten

Benutzer werden durch Anklicken der entsprechenden Benutzer-Symbole im Register "Benutzer" hinzugefügt und entfernt. Wenn die LDAP-Unterstützung aktiviert ist, können Benutzer entweder mit der eingebauten Authentifizierung oder mit der Windows-Authentifizierung aktiviert werden (siehe "LDAP" oben). Beim Erstellen von Benutzern können Sie folgendes angeben:

- Benutzername
- Vollständiger Name
- Passwort (nur bei eingebauter Authentifizierung)
- E-Mail-Adresse (zur Passwort-Wiederherstellung, nur integrierte Authentifizierung)

Gruppen verwalten

Gruppen werden hinzugefügt und entfernt, indem Sie auf die entsprechenden Gruppensymbole in der Registerkarte "Gruppen" klicken. Die gleichen Privilegien und

Berechtigungen, die Benutzern zugewiesen werden können, können auch Gruppen zugewiesen werden.

6.5.2.1 Berechtigungen & Privilegien

Standardmäßig sind für Benutzerkonten und -gruppen alle Berechtigungen aktiviert und sie haben Zugriff auf alle Seiten, Berichte und Computer.

> Alle Informationen in diesem Kapitel gelten sowohl für Benutzerkonten als auch für Gruppen.

Privilegien

Die folgenden zwei Privilegien sind verfügbar:

- Konten verwalten: Ermöglicht es einem Benutzer oder einer Gruppe, Benutzer anzulegen, zu bearbeiten und zu löschen. Dies sollte nur Administratoren zugewiesen werden.
- Profile verwalten: Erlaubt die Verwaltung von Profilen: Erlaubt einem Benutzer oder einer Gruppe, Profile zu erstellen, zu bearbeiten und zu löschen.

Zulassen vs. Gesperrt

Seiten, Berichte oder Computer können entweder zugelassen oder gesperrt werden. Wenn ein Element (z.B. "Ereignisprotokoll-Suche") zur Liste Erlaubt hinzugefügt wird, wird die Liste Authorisiert aktiv, und der Benutzer oder die Gruppe darf nur auf Seiten zugreifen, die sich in der Liste Authorisiert befinden - die Liste Blockiert ist deaktiviert.

Wenn ein Element zur Liste "Blockiert" hinzugefügt wird, wird die Liste "Blockiert ..." aktiv, und dem Benutzer oder der Gruppe wird nur der Zugriff auf Seiten verweigert, die sich auf der Liste "Blockiert ..." befinden.

> Wenn ein Benutzer oder eine Gruppe nur Zugriff auf eine begrenzte Anzahl von Seiten, Berichten oder Computern haben soll, dann sollten diese der jeweiligen "Authorisiert"-Liste hinzugefügt werden. Wenn ein Benutzer oder eine Gruppe Zugriff auf die Mehrzahl der Web Reports haben soll, Sie aber bestimmte Seiten, Berichte oder Computer blockieren möchten, dann sollten diese Elemente der jeweiligen "Blockiert ..."-Liste hinzugefügt werden.

Seiten

Erlauben oder blockieren Sie jede Seite in den Web Reports. Seiten, auf die der Benutzer oder die Gruppe keinen Zugriff hat (entweder weil sie nicht erlaubt oder weil sie blockiert ist), werden im Menü nicht angezeigt.

Berichte

Erlauben oder blockieren Sie jeden Bericht in den Web Reports.

Computer

Erlauben oder blockieren Sie Computer von Ergebnissen, dies gilt für alle Seiten und Berichte.

Benutzer- vs. Gruppenberechtigungen

Berechtigungen, wie authorisierte oder blockierte Seiten, werden akkumuliert, wenn ein Benutzer Mitglied mehrerer Gruppen ist oder wenn Berechtigungen sowohl auf Benutzer- als auch auf Gruppenebene zugewiesen werden. Blockierte Funktionen (z.B. blockierte Seiten, blockierte Berichte oder blockierte Computer) haben immer Vorrang vor erlaubten Funktionen.

Die folgende Tabelle zeigt, wie verschiedene Berechtigungen auf Benutzerebene und Mehrfachgruppenmitgliedschaft zu den effektiven Berechtigungen zusammengeführt werden:

Beispiele	Benutzer-Berechtigungen		Gruppe 1 Berechtigungen		Gruppe 2 Berechtigungen		Effektive Berechtigungen	
	Erlaubte Seiten	Blockierte Seiten	Erlaubte Seiten	Blockierte Seiten	Erlaubte Seiten	Blockierte Seiten	Erlaubte Seiten	Blockierte Seiten
Beispiel #1	Disk Trends		Performance Trends		Syslog Search		Disk Trends	all others
	Disk Status						Disk Status	
							Performance Charts	
							Syslog Search	
Beispiel #2		Event Log Search		Syslog Search		Software Installed	all other	Event Search
						Software History		Syslog Search
								Software Installed
								Software History
Beispiel #3	Computer Dashboard					Maintenance Wizard	Computer Dashboard	all other
						Database Usage		

Effektive Berechtigungen

6.5.3 Präferenzen

Zeitzone
Wenn UTC aktiviert ist, konfigurieren Sie die Zeitzone, in der alle Zeiten angezeigt werden sollen.

Erscheinungsbild
Konfigurieren Sie das grundlegende Farbschema.

Die Einstellungen sind spezifisch für ein Benutzerkonto, es sei denn, die Zugriffskontrolle ist deaktiviert; in diesem Fall gilt sie global.

7 Zusätzliche Tipps und Ressourcen

This chapter contains additional information not directly related to EventSentry but useful for event log and system monitoring:

Database Tips

- Tuning the EventSentry database
- Purging records periodically
- Encrypting Network Traffic with MSSQL

Event Log Reference

- 1. Windows NT Security Event Descriptions
- 2. Windows 2000 Security Event Descriptions
- 3. Common events from systems in the field

7.1 Datenbank-Tipps

Dieses Kapitel enthält Tipps und Tricks für alle datenbankbezogenen Aufgaben.

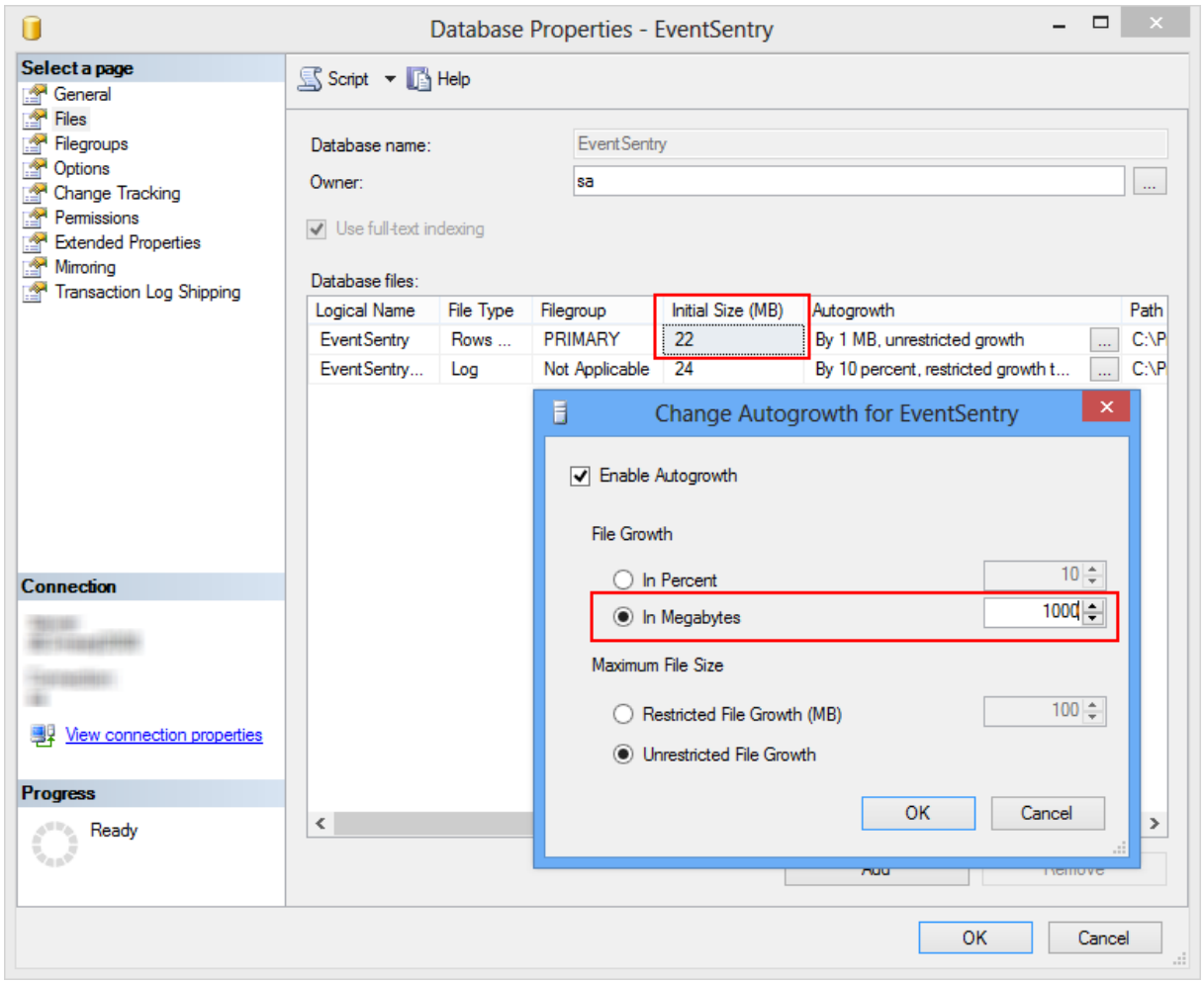
- Tuning der EventSentry-Datenbank
- Periodisches Bereinigen von Datensätzen (Beispiel für MS SQL Server)
- Encrypting Network Traffic with MSSQL

7.1.1 Tuning der EventSentry-Datenbank

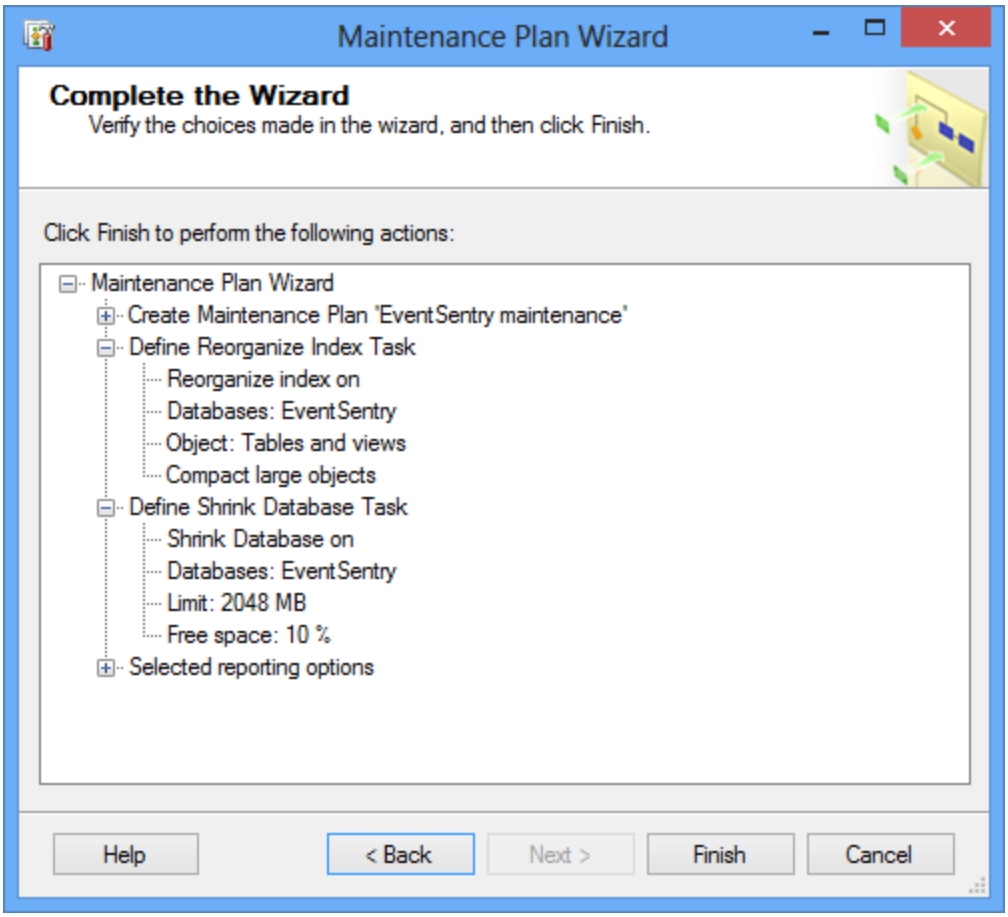
Die EventSentry-Datenbank ist so konzipiert, dass sie große Datenmengen aufnehmen kann und dennoch schnelle Antworten auf Anfragen liefert. Wenn Sie große Datenmengen erwarten (z.B. mehr als 1 Million Datensätze), ist es jedoch trotzdem wichtig, dass Sie Maßnahmen ergreifen, um sicherzustellen, dass die Datenbank jederzeit optimiert ist. Nachstehend finden Sie Empfehlungen für verschiedene unterstützte Datenbanken, wenn Sie mit großen Datenmengen rechnen.

Microsoft SQL-Server®

1. Achten Sie beim Anlegen der Datenbank darauf, dass Sie die anfängliche Datenbankgröße ausreichend hoch einstellen. Dadurch wird die Gesamtleistung verbessert, da die Datenbank-Engine die Datendateien nicht ständig erweitern muss. Dies gilt sowohl für die Datendateien als auch für die Größe des Transaktionsprotokolls. Außerdem sollten Sie die Wachstumsrate der Dateien eher größer als kleiner konfigurieren. Die folgenden Screenshots zeigen einen guten Ausgangspunkt für potenziell große Datenbanken:



2. Reorganisieren Sie die Tabellen regelmäßig, vor allem aber nachdem Sie alte Datensätze bereinigen oder verschieben. SQL Server bietet eine Funktion namens **Wartungsplan**, mit der Sie eine Datenbank-Wartung regelmäßig oder nach Bedarf planen können. Denken Sie daran, dass eine Datenbankreorganisation vorübergehend mehr Plattenplatz beanspruchen kann. Stellen Sie daher immer sicher, dass Sie genügend Plattenplatz für die Datenbank und das Transaktionsprotokoll zur Verfügung haben. Der Wartungsplan-Assistent kann gestartet werden, indem Sie mit der rechten Maustaste auf die Datenbank klicken und "Maintenance Plan" aus dem Untermenü "All Tasks" wählen. Der untenstehende Screenshot zeigt eine empfohlene Konfiguration.



7.1.2 Daten löschen

Die Tabellen zur Konsolidierung der Ereignisprotokolle und zur Prozessverfolgung könnten nach einer Weile zu groß werden. Sie können Ihr System so konfigurieren, dass Datensätze, die nicht mehr relevant sind, periodisch bereinigt werden, z.B. nach 12 Monaten. Dieses Kapitel zeigt:

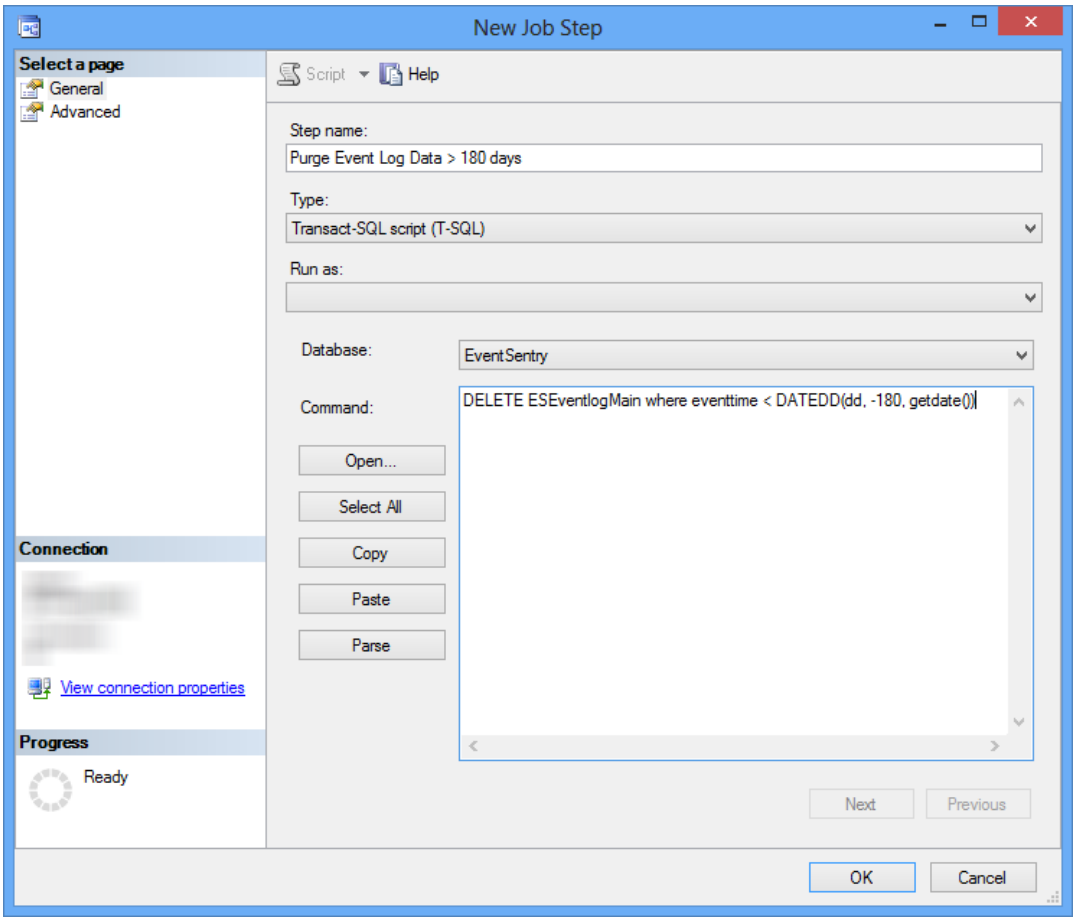
- Verwendung des mitgelieferten Datenbank-Bereinigungsdienstprogramms zur **automatischen Bereinigung von Datensätzen** in allen unterstützten Datenbanken
- Einrichten geplanter Jobs auf Microsoft SQL Server® zur Automatisierung des Löschens von Datensätzen

EventSentry enthält eine Befehlszeilenanwendung, die Datensätze aus der EventSentry-Datenbank bereinigen kann. Das Dienstprogramm kann mit Hilfe des EventSentry-Anwendungsplaners oder des Windows-Taskplaners für eine regelmäßige Ausführung geplant werden. Weitere Informationen finden Sie unter Automatisches Bereinigen von Datensätzen.

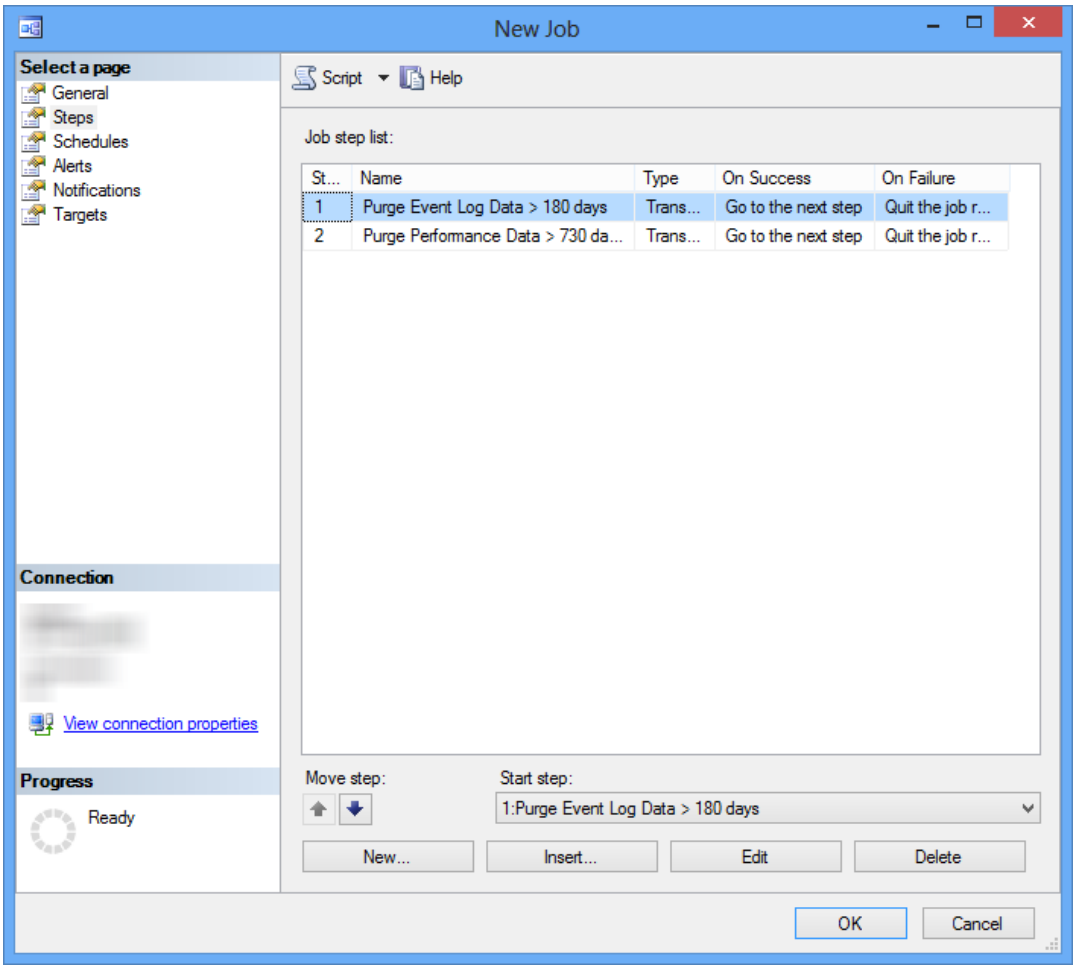
Einrichten eines automatischen Jobs (Microsoft SQL Server® 2005 und höher)

1. Öffnen Sie das "Microsoft SQL Server® Management Studio" und navigieren Sie zu "SQL Server Agent" -> "Jobs".
2. Klicken Sie mit der rechten Maustaste auf "Jobs" und wählen Sie "Neuer Job ...".

3. Geben Sie einen Namen für den Job an (z.B. "EventSentry Database Purge") und klicken Sie auf "Steps" im linken Fensterbereich.
4. Klicken Sie im Fenster "Schritte" auf die Schaltfläche "Neu...".
5. Geben Sie dem Schritt einen beschreibenden Namen und fügen Sie eine der folgenden SQL-Anweisungen ein. Sie können mehrere SQL-Anweisungen angeben, diese aber durch eine GO-Anweisung in einer einzigen Zeile trennen. Sie können die SQL-Anweisungen aus dem letzten Schritt des webbasierten Wartungsassistenten beziehen.

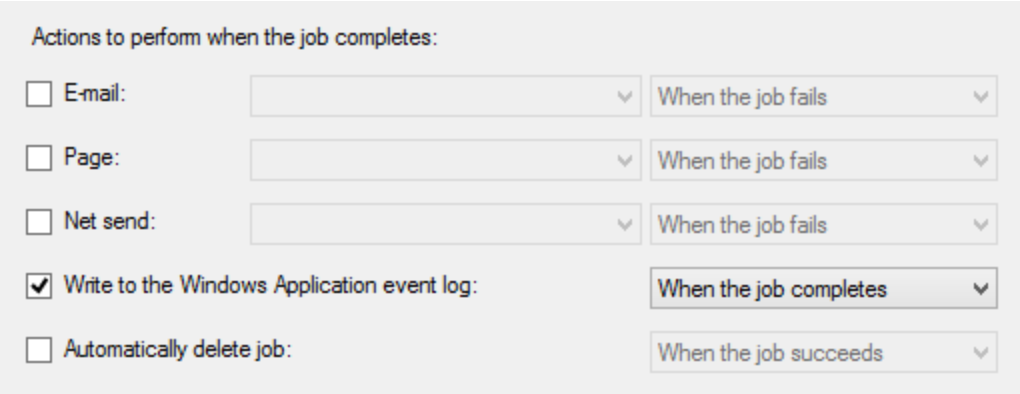


6. Stellen Sie sicher, dass die richtige Datenbank ausgewählt ist.
7. Klicken Sie auf die Registerkarte "Erweitert" und wählen Sie "Gehe zum nächsten Schritt" für die Einstellung "Aktion bei Fehler". Klicken Sie auf **"OK"**.
8. Fügen Sie bei Bedarf einen weiteren Schritt hinzu.



Es wird empfohlen, Daten häufig zu löschen (wobei bei jedem Löschen kleinere Datenmengen betroffen sind), um die Auswirkungen des Löschens auf die Datenbank zu verringern. Anstatt beispielsweise einen Job zum Löschen von Datensätzen, die älter als 180 Tage sind, einmal im Monat einzurichten, sollten Sie den Job so einrichten, dass er mindestens einmal pro Woche ausgeführt wird. Auf diese Weise wirkt sich jeder Job auf weniger Daten aus und ist somit schneller abgeschlossen.

9. Klicken Sie auf "Zeitpläne" und fügen Sie einen neuen Zeitplan hinzu.
10. Geben Sie dem Zeitplan einen Namen (z.B. "Wöchentlich") und konfigurieren Sie den Zeitplan.
11. Klicken Sie auf "Benachrichtigungen", um die Fehlerberichterstattung zu aktivieren. Markieren Sie das Kästchen "In das Ereignisprotokoll der Windows-Anwendung schreiben" und wählen Sie "Wenn der Auftrag abgeschlossen ist". Sie können diese Option ändern und ein Ereignis nur dann protokollieren, wenn der Auftrag fehlschlägt.



12. Klicken Sie auf **OK**, um den Zeitplan hinzuzufügen.

7.1.2.1 Daten automatisch löschen

Sie können Datensätze aus **PostgreSQL-** und MSSQL-Datenbanken mit der Befehlszeilenanwendung **es_db_purge.exe** automatisch löschen. Sie können dieses Tool entweder nach Belieben ausführen, oder Sie können es automatisch so planen, dass es regelmäßig (z.B. jeden Sonntag) ausgeführt wird, um den Prozess der permanenten Entfernung alter Daten vollständig zu automatisieren.

Mit dem Dienstprogramm können Sie angeben, welche Funktion Sie bereinigen möchten (z.B. Ereignisprotokolldaten und Leistungsdaten) und wie viele Tage Sie behalten möchten (z.B. 180 Tage).

Das Datenbank-Bereinigungsdienstprogramm arbeitet über ODBC (auf die gleiche Weise wie alle anderen Komponenten, die mit Datenbanken verbunden sind) und kann mit Befehlszeilenargumenten konfiguriert werden.

Alle durch diese Anwendung bereinigten Daten werden **dauerhaft gelöscht** und sind nur zugänglich, wenn sie von einer funktionierenden Sicherung wiederhergestellt werden.

Siehe Datenbank-Bereinigungsdienstprogramm für weitere Informationen.

7.1.3 Archivierung von Ereignisprotokolldaten

Die Konsolidierung von Ereignisprotokolleinträgen in einer zentralen Datenbank kann eine Herausforderung für Datenbankserver sein, die nicht ausreichend dimensioniert sind, insbesondere in mittleren und größeren Netzwerken, in denen die EventSentry-Datenbank leicht auf Hunderte von Gigabyte oder sogar Terabyte anwachsen kann. Wenn der Datenbankserver unter zu hohem Druck steht, können bestimmte EventSentry-Komponenten anfangen, Daten in eine Warteschlange zu stellen, und Suchanfragen in den Web Reports können länger dauern.

Obwohl EventSentry keine Funktion zur automatischen Archivierung von Ereignissen in einer separaten Archivierungsdatenbank bietet, kann EventSentry so konfiguriert werden, dass Protokolldaten in **zwei Datenbanken** geschrieben werden: Eine Datenbank für den schnellen Zugriff (diese Datenbank löscht regelmäßig ältere Daten) und eine weitere Datenbank für die Langzeitarchivierung. Aufgrund der Flexibilität von EventSentry können Sie für diese Aufgabe sogar zwei verschiedene Datenbanktypen verwenden. Zum Beispiel kann eine Microsoft SQL Server®-Datenbank zur Speicherung von Sofortdaten

(z.B. der letzten 60 Tage) und eine PostgreSQL-Datenbank zur Speicherung von Daten für die Langzeitspeicherung (z.B. 2 Jahre) verwendet werden.

Die folgenden drei EventSentry-Funktionen unterstützen dies:

1. **Filter:** Die Filterregeln von EventSentry können dasselbe Ereignis an mehrere Benachrichtigungen weiterleiten, zum Beispiel an zwei verschiedene Datenbanken.
2. **Benachrichtigungen:** EventSentry ermöglicht die Einrichtung mehrerer Benachrichtigungen desselben Typs, z.B. an mehrere Datenbanken.
3. **Profile:** Die Web-Reports unterstützen mehrere Profile, so dass von derselben URL aus auf mehrere Datenbanken zugegriffen werden kann.

Die nachstehenden Anweisungen gehen davon aus, dass eine Datenbankkonsolidierung bereits eingerichtet ist.

1. Eine Aktion erstellen
EventSentry benötigt eine Aktion, um Ereignisse an eine Datenbank weiterzuleiten. Klicken Sie in der EventSentrz Konsole auf den Container "Actions" in der linken Baumansicht. Verwenden Sie dann entweder den Ribbon um eine Aktion hinzuzufügen, oder klicken Sie mit der rechten Maustaste auf den Aktionscontainer und wählen Sie *Hinzufügen*. Geben Sie einen beschreibenden Namen für die Aktion ein, z.B. "Sekundärdatenbank" oder "Langzeitdatenbank".

Klicken Sie im daraufhin erscheinenden Dialog auf die Schaltfläche *Datenbank initialisieren oder aktualisieren*, um den Konfigurationsassistenten im Datenbankinitialisierungsmodus zu starten. Folgen Sie einfach dem Assistenten, der eine Initialisierung des Schemas auf einer neuen Datenbank erstellen wird.

Wenn Sie die erste EventSentry-Datenbank auf einem DB-Server erstellen, stellen Sie sicher, dass Sie die Kennwörter sowohl für die Benutzer **eventsentry_svc** als auch **eventsentry_web** dokumentieren.

Wenn der Konfigurationsassistent abgeschlossen ist, konfiguriert er automatisch die Datenbankeigenschaften für die Aktion. Klicken Sie auf die Schaltfläche "Test", um sicherzustellen, dass die Konfiguration der Aktion gültig ist.

2. Ändern oder Erstellen einer zusätzlichen Filterregel
Sobald die neue Datenbank initialisiert ist, können Ereignisse an sie weitergeleitet werden. Der einfachste Weg, Ereignisse an eine 2. Datenbank weiterzuleiten, besteht darin, die bereits vorhandene Filterregel zu modifizieren, die Ihre Ereignisse an Ihre primäre Datenbank weiterleitet.

Bearbeiten Sie jede Filterregel im Paket "Database Consolidation" und fügen Sie die neue Meldung zur Liste *Aktionen* hinzu. Wenn Sie die Liste der Aktionen nicht sehen können, werden Ihre Aktionen von der Paketebene geerbt, und Sie müssen die Paketdetails ändern. Klicken Sie mit der rechten Maustaste auf das übergeordnete Paket und wählen Sie *Edit*. Fügen Sie dort die neue Aktion zur Aktionsliste des Abschnitts *"Overrides"* hinzu.

Sie können auch eine zusätzliche Filterregel erstellen, anstatt die bestehende zu modifizieren, um die Struktur zu verbessern. Nach dem Speichern und Verschieben der Konfiguration werden die ausgewählten Ereignisse in beide Datenbanken geschrieben.

Sie können auch andere Funktionen anpassen, die mehrere Datenbanken unterstützen, einschließlich

- Log-Datei-Überwachung
- Leistungsüberwachung
- Validierungs-Skripte

3. Periodisches Löschen von Daten
Sobald die Daten in beide Datenbanken geschrieben sind, muss ein Purge Plan erstellt werden, der auf den folgenden Faktoren basiert:

- Wie lange die Daten in der Schnellzugriffsdatenbank aufbewahrt werden sollen, zum Beispiel 60 Tage.
- Wie lange die Daten in der Archivierungsdatenbank aufbewahrt werden sollen, z.B. 60 Tage. Dies hängt von den Compliance- oder Verwaltungsanforderungen ab.
- Welcher Datenbankserver für den Schnellzugriff und welcher für die Archivdatenbank ausgewählt werden soll. Dies ist normalerweise eine offensichtliche Wahl.

Sobald Sie diese Faktoren bestimmt haben, können Sie beide Datenbanken so einrichten, dass die Datensätze periodisch gelöscht werden. Weitere Informationen finden Sie unter Daten löschen und Daten automatisch löschen.

4. Erstellen eines neuen Profils in den Web Reports
Mit Profilen können Sie zusätzliche Datenbankverbindungen und/oder Schnittstelleneinstellungen einrichten. Nachdem ein zusätzliches Profil erstellt wurde, können Sie einfach auf dieses zugreifen, indem Sie es in der Dropdown-Liste oben links auswählen. Profile werden über den Profileditor oder durch direktes Bearbeiten der Datei configuration.xml erstellt.

Klicken Sie im Menü der Web Reports auf das Zahnradsymbol, wählen Sie Profile und klicken Sie links auf *Neues Profil erstellen*. Weisen Sie dem Profil im Abschnitt *Profilname* einen aussagekräftigen Namen zu und konfigurieren Sie die Datenbankverbindung entsprechend. Bitte stellen Sie auch sicher, dass andere Einstellungen (z.B. die UTC-Einstellungen und E-Mail-Einstellungen) korrekt konfiguriert sind.

Sobald Sie unten auf der Seite auf Submit klicken, können Sie einfach zwischen Ihrer primären und sekundären Datenbank wechseln, indem Sie das Pulldown-Menü oben links wählen.

7.1.4 Microsoft SQL Server

7.1.4.1 Encrypting Network Traffic with MSSQL //OLD: Encrypting Network Traffic with MSSQL

Most ODBC drivers, including Microsoft SQL Server®, transmit network traffic in clear text which can be a problem in security sensitive environments. Microsoft SQL Server® supports protocol encryption which encrypts all traffic between the client (=EventSentry agent) and the Microsoft SQL Server®.

Using protocol encryption requires the following prerequisites:

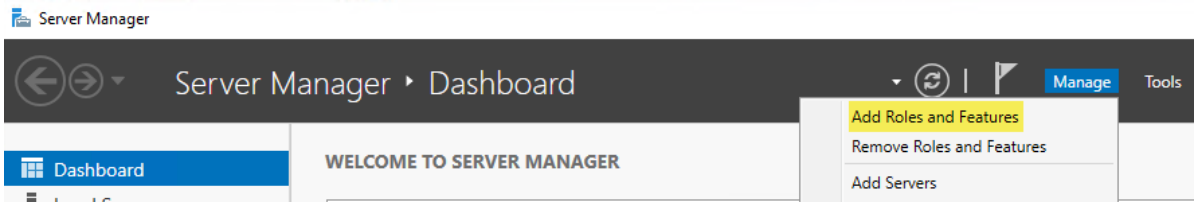
- Certificate Services installed on machine running in your domain
- Latest SQL Server ODBC drivers installed on all clients (Microsoft® ODBC Driver 13.1 for SQL Server)

This chapter will guide you through the process of setting up Active Directory Certificate Services and requesting a certificate so that SQL server can use protocol encryption. This chapter is based on using Windows Server 2016 for the OS and Microsoft SQL Server® 2016/Microsoft SQL Server® 2019 for the database

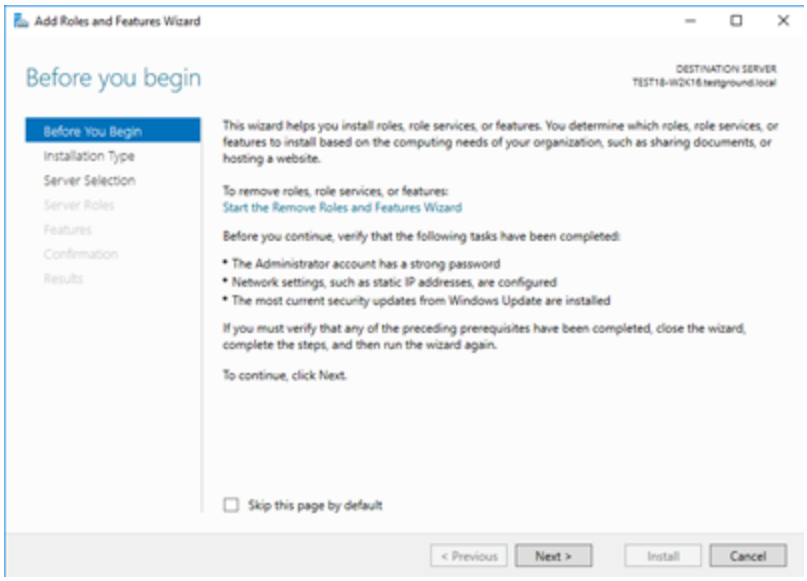
1. Installing Certificate Services

You will only need to follow these steps if you do not have certificate services running in your domain. If you already have a certificate server in your domain then you can skip step 1.

Navigate to "Start -> Administrative Tools -> Server Manager -> Manage -> Add Roles and Features":



Which will launch the “Add Roles and Features Wizard” similar to this:



Step-by-step instructions for installing the Active Directory Certificate Services

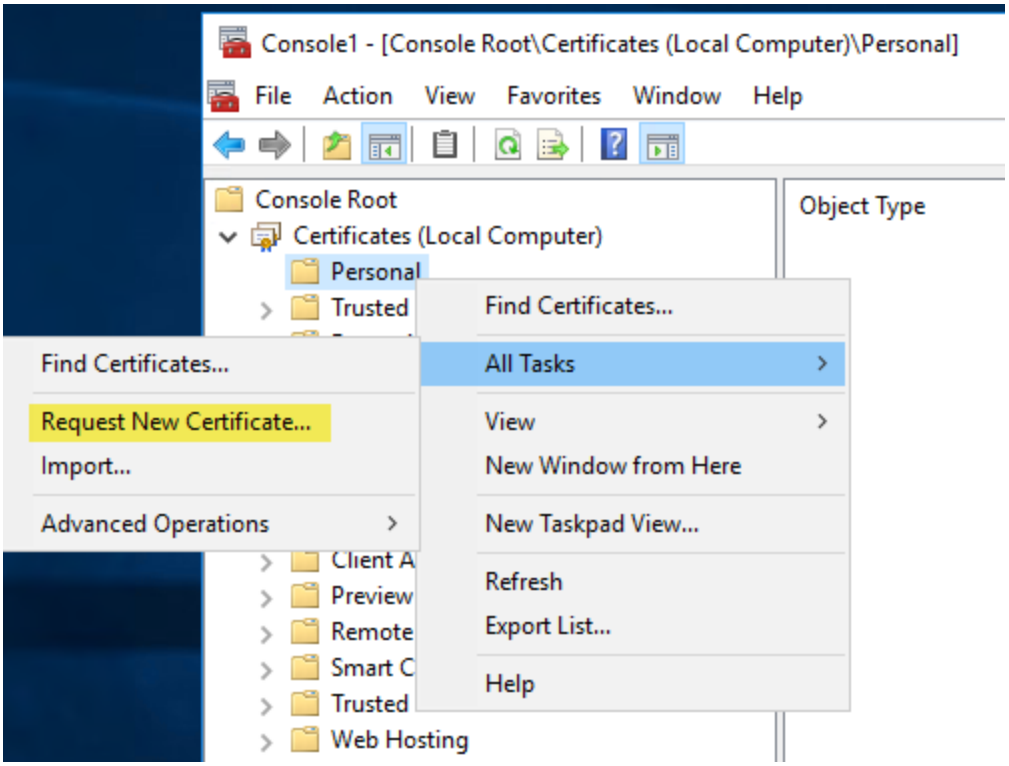
2. Configuring the MMC snap-in

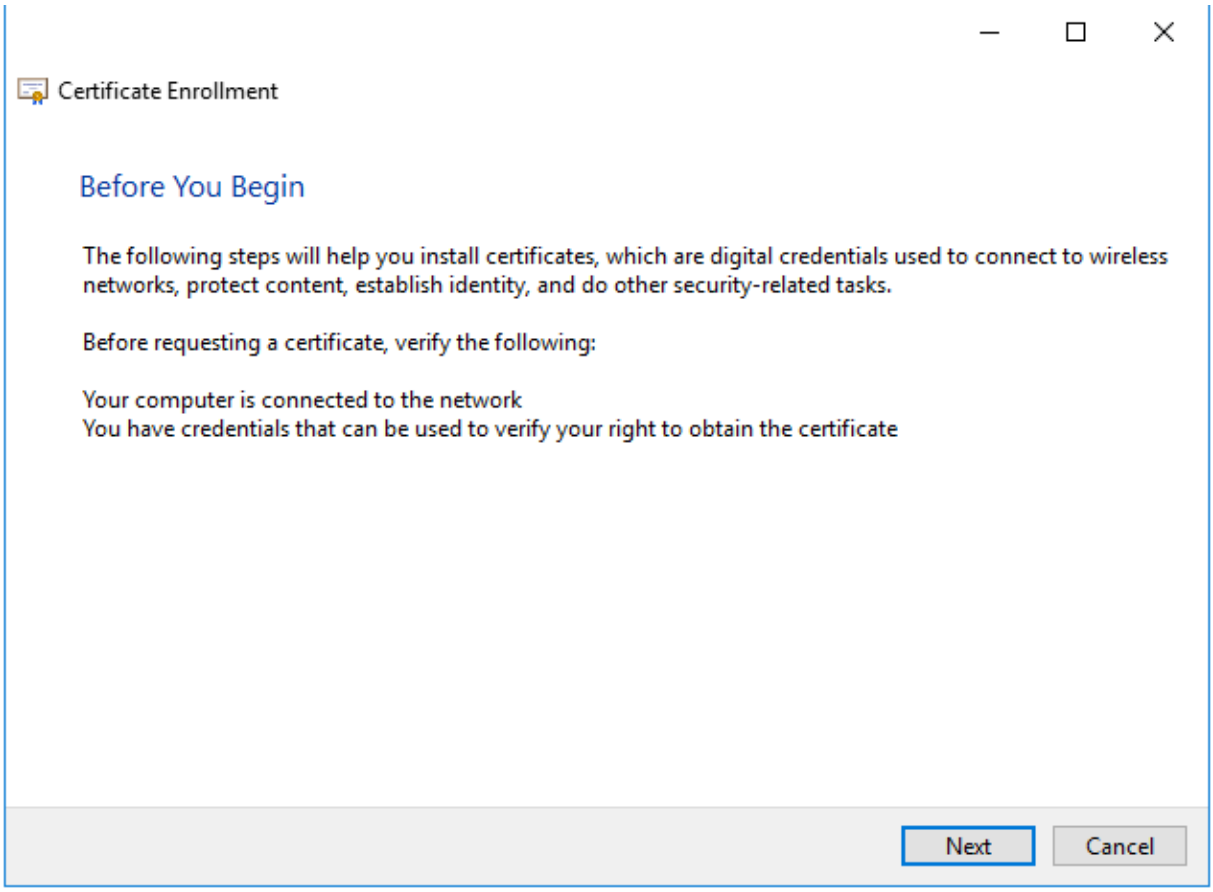
In order to manage/create certificates you need to configure an MMC for the certificate services. To open the Certificates snap-in, follow these steps:

- To open the MMC console, click Start, and then click Run. In the Run dialog box type: **mmc**
- On the Console menu, click Add/Remove Snap-in....
- Click Add, and then click Certificates. Click Add again.
- You are prompted to open the snap-in for the current user account, the service account, or for the computer account. Select the **Computer Account**.
- Select **Local computer**, and then click Finish.
- Click Close in the Add Standalone Snap-in dialog box.
- Click OK in the Add/Remove Snap-in dialog box. Your installed certificates are located in the **Certificates** folder in the **Personal** container.

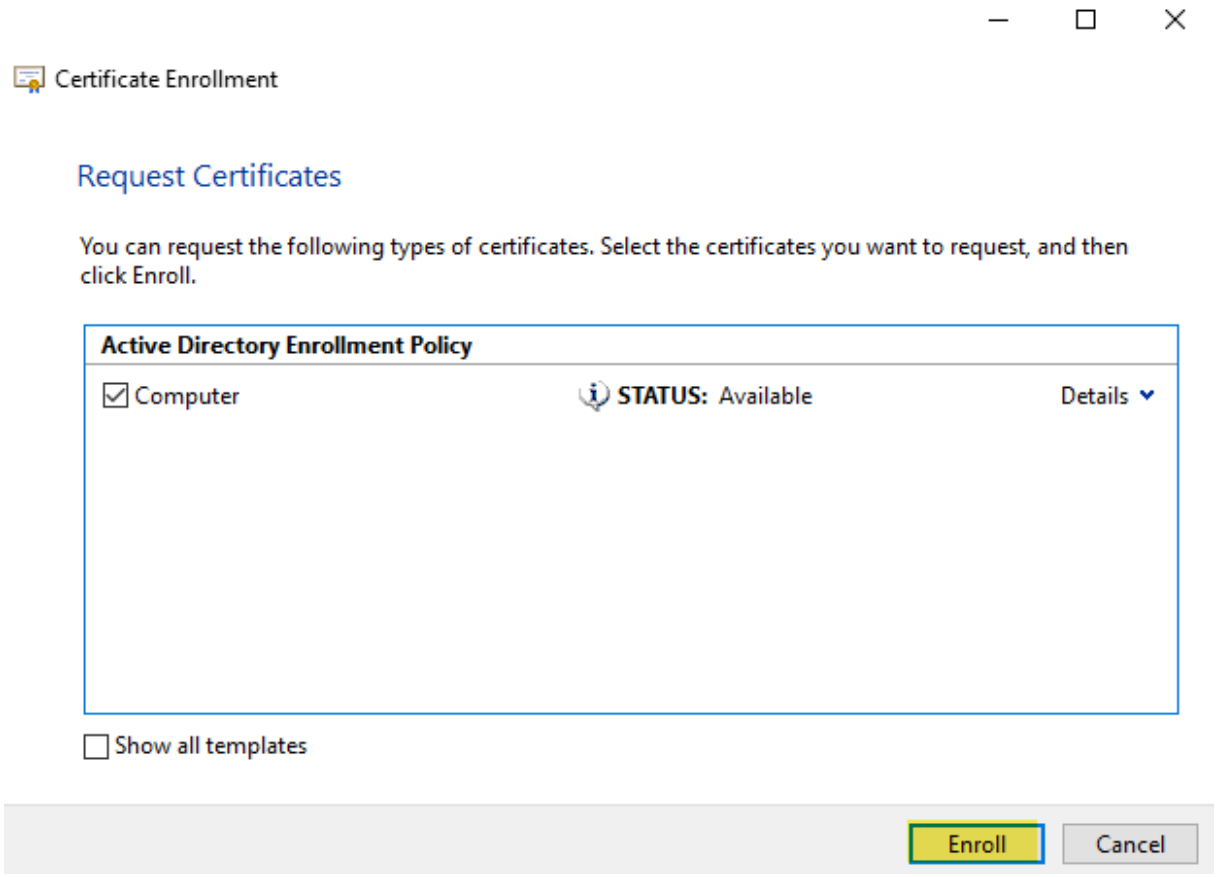
3. Installing a certificate on the server

In the MMC, click to select the Personal folder in the left-hand pane. Right-click in the right-hand pane, point to All Tasks, and then click Request New Certificate....which will bring up the dialogs shown below:





The **Certificate Request Wizard** dialog box opens. Click Next. Select Computer as the Certificate type.



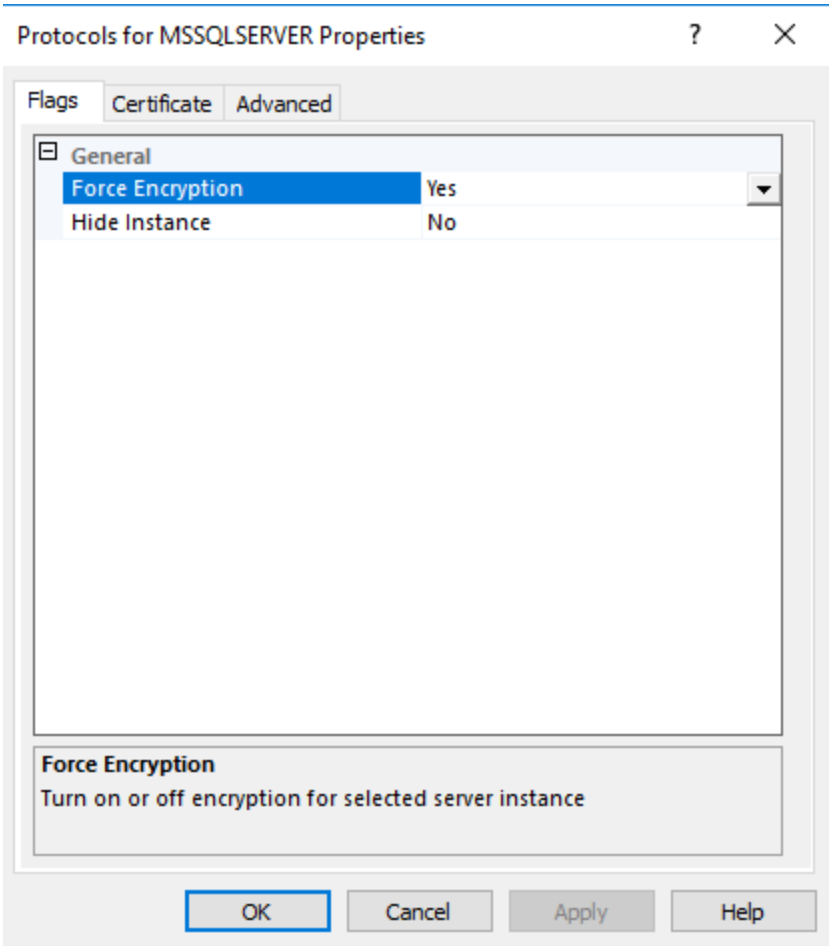
After the wizard finishes, you will see the certificate in the folder with the fully qualified computer domain name.

4. Requiring database encryption for all communication

Once the certificate is installed you can configure the SQL Server to "Force protocol encryption".

• **For SQL Server 2016/2019**

Navigate to “Start -> Microsoft SQL Server 20xx -> SQL Server 20xx Configuration Manager.” Expand "SQL Server Network Configuration". Right click on "Protocols for MSSQLSERVER" and choose Properties. Set "Force Encryption" to "Yes" then click on the Certificate tab where you have to select the certificate you created above.



When not using the collector, all clients communicating with the SQL Server will need an up-to-date SQL Server ODBC driver installed in order to support encryption. If a machine is unable to communicate with the database server after you enabled encryption, installing the latest OBCD driver from Microsoft® ODBC Driver 13.1 for SQL Server will usually resolve the problem.

----------OLD_TEXT----------
Most ODBC drivers, including Microsoft SQL Server®, transmit network traffic in clear text which can be a problem in security sensitive environments. Microsoft SQL Server® supports protocol encryption which encrypts all traffic between the client (=EventSentry agent) and the Microsoft SQL Server®.

Using protocol encryption requires the following prerequisites:

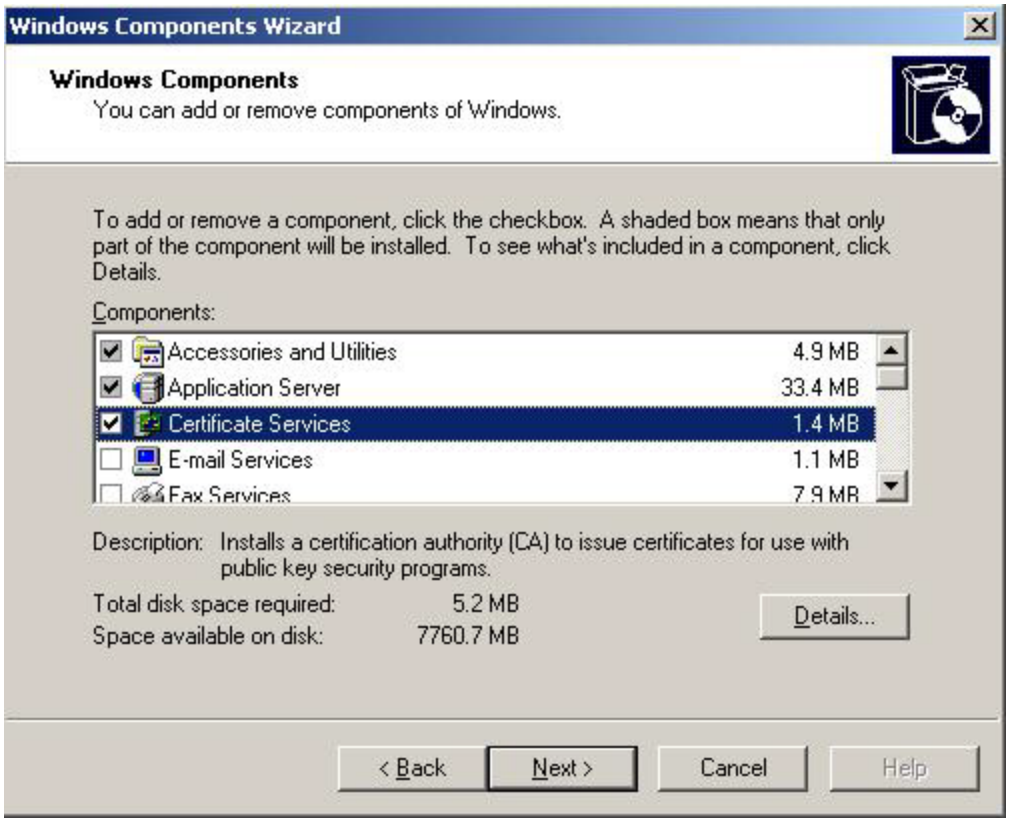
- Certificate Services installed on machine running SQL Server
- Latest SQL Server ODBC drivers installed on all clients (MDAC)

This chapter will guide you through the process of setting up Certificate Services and requesting a certificate so that SQL server can use protocol encryption. This chapter is based on using Windows Server 2003 for the OS and Microsoft SQL Server® 2000/Microsoft SQL Server® 2005 for the database.

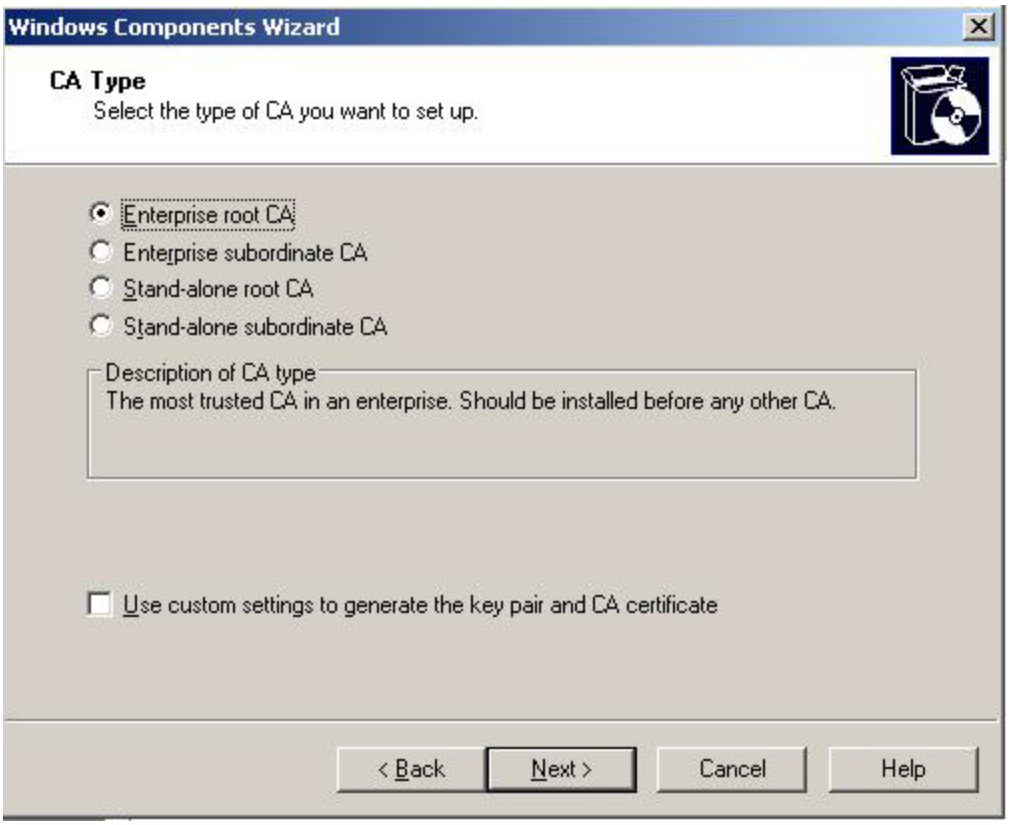
1. Installing Certificate Services

You will only need to follow these steps if you do not have certificate services running in your domain. If you already have a certificate server in your domain then you can skip step 1.

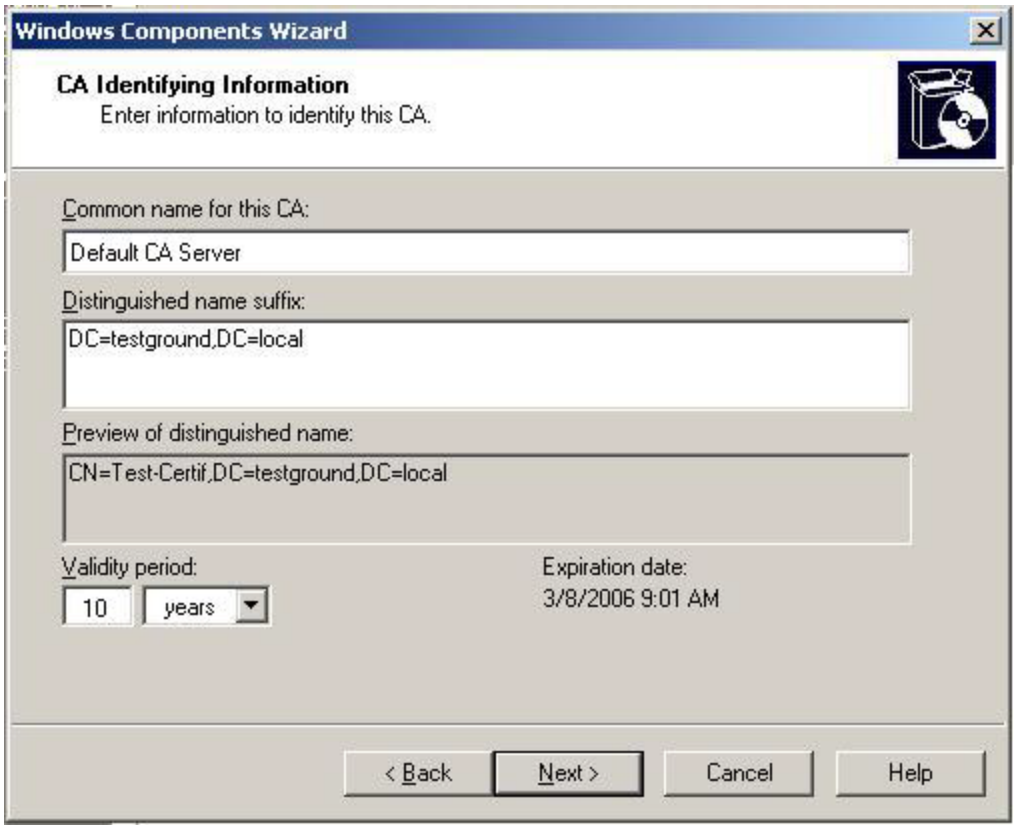
Navigate to "Start -> Settings -> Control Panel -> Add/Remove Programs" and click "Add/Remove Windows Components" which will bring up a screen similar to the one shown below:



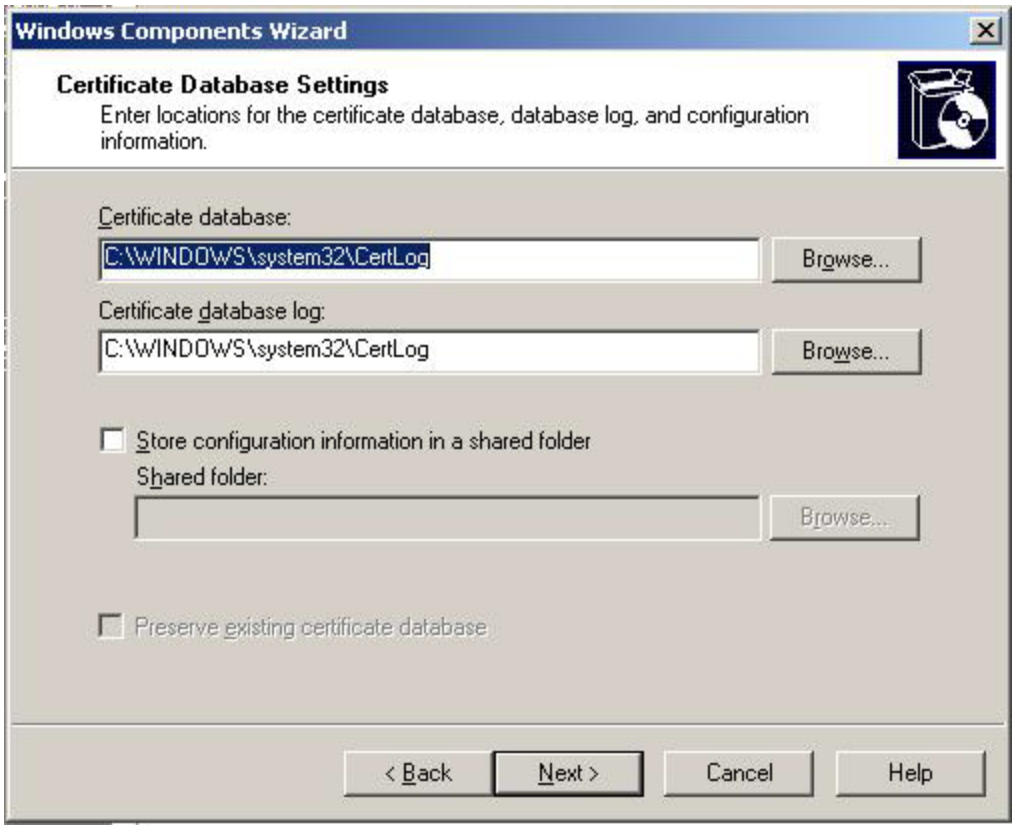
Check "Certificate Services" and click next. Click "Yes" on the confirmation dialog if the imposed restrictions are OK. On the next screen select the appropriate certificate authority type for your network. Please refer to the Windows Server documentation for more information. In our example we will be installing an "Enterprise Root CA" since it is the first CA server:

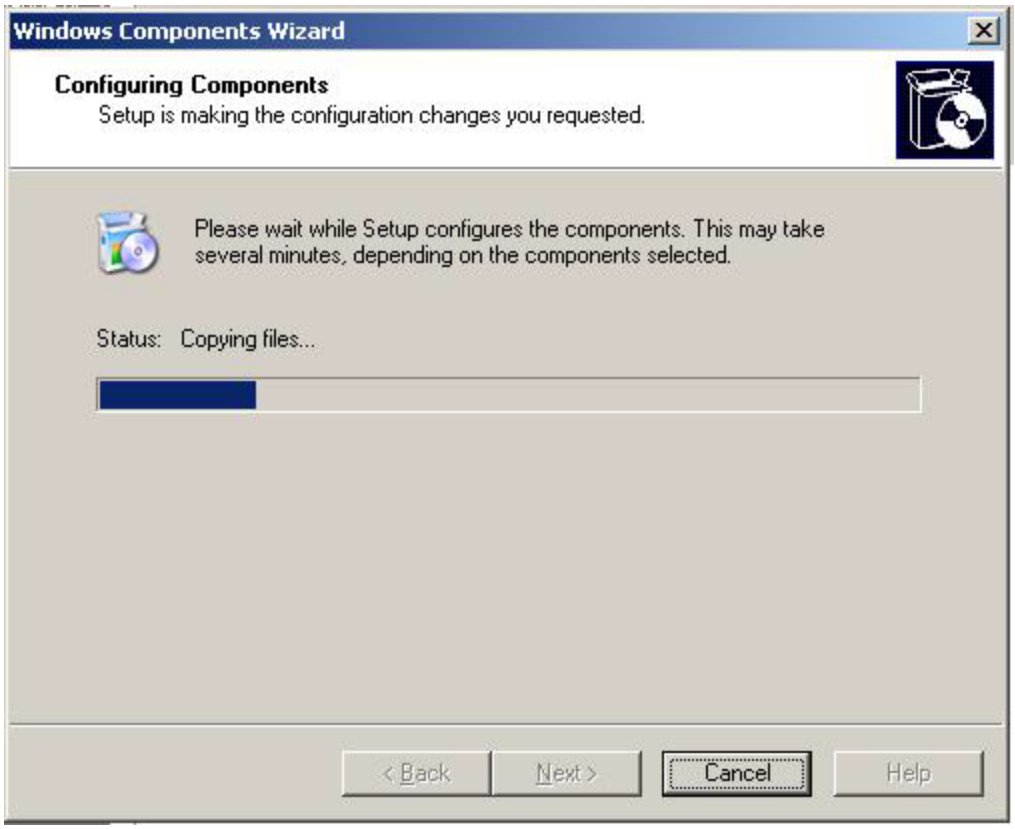


Please note that the following screenshots might look differently depending on the type of CA you select here (the screenshots shown are based on the "Enterprise root CA" selection). On the next screen enter the "CA Identifying Information". Make sure that you enter a good common CA name and a specify a validity period that is long enough:



After clicking Next confirm the following dialogs and click "Finish" to complete the setup of the CA.





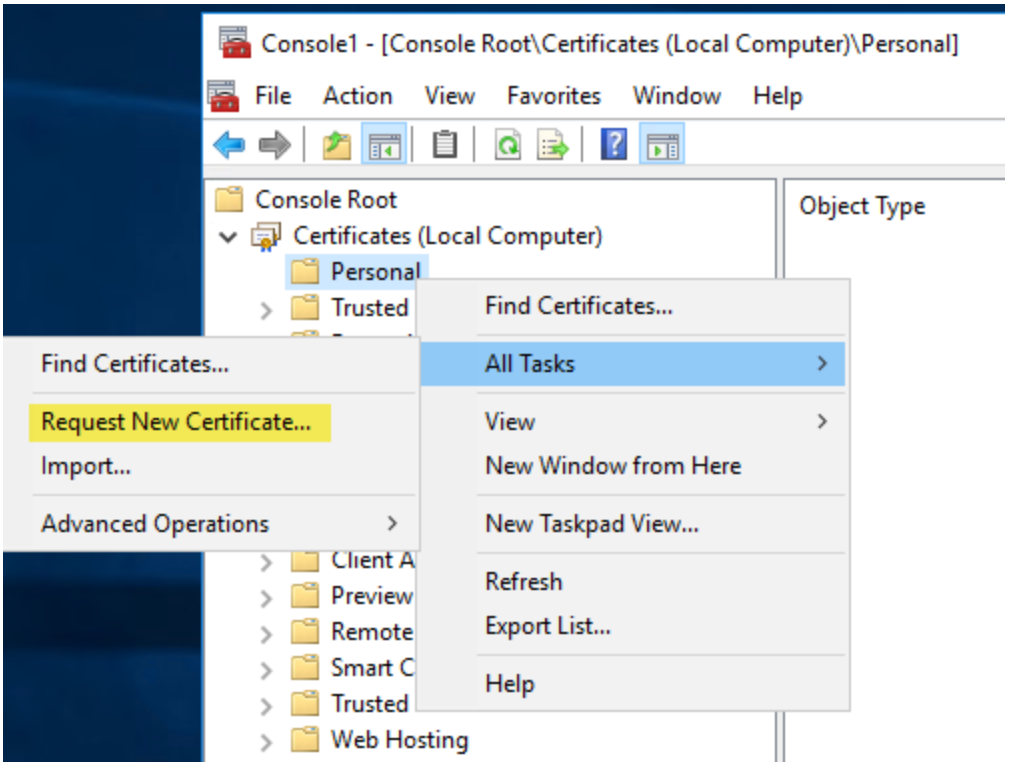
2. Configuring the MMC snap-in

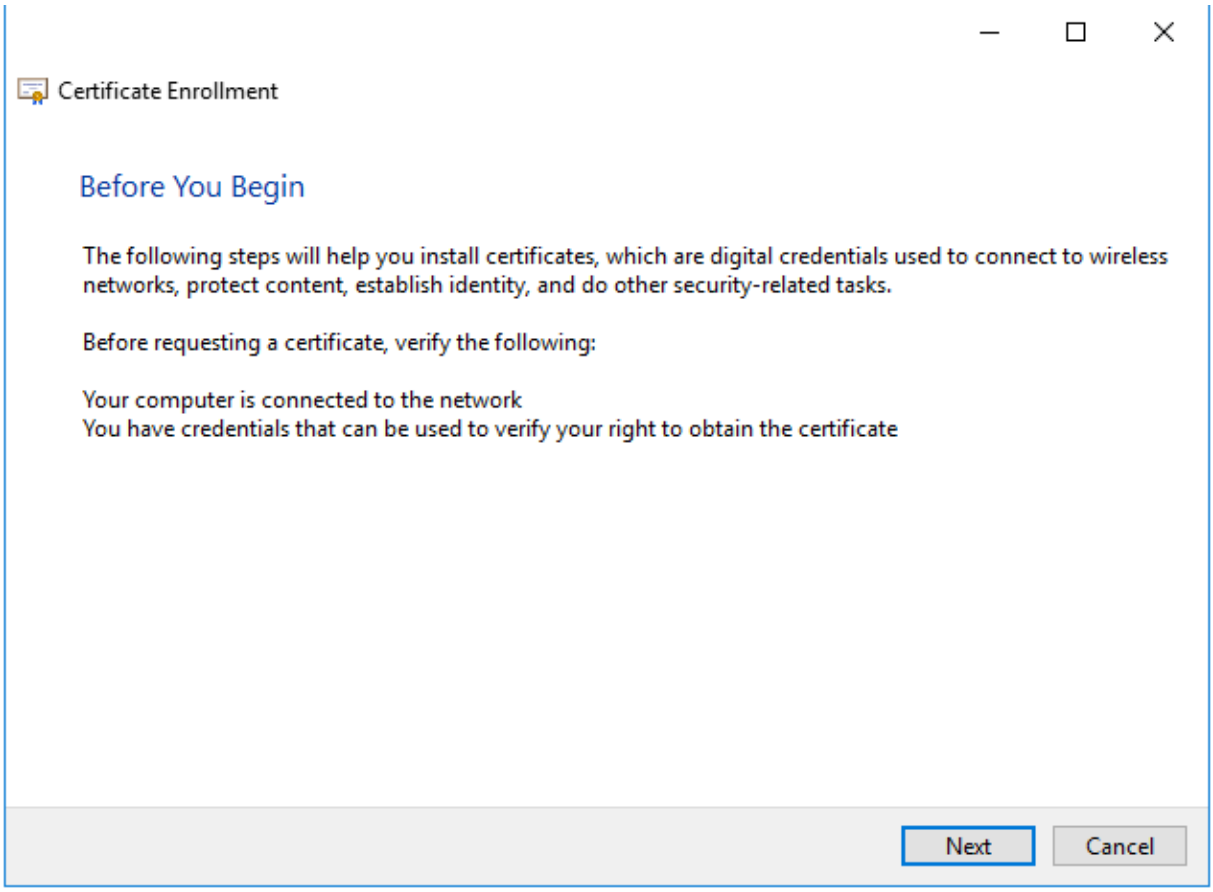
In order to manage/create certificates you need to configure an MMC for the certificate services. To open the Certificates snap-in, follow these steps:

- To open the MMC console, click Start, and then click Run. In the Run dialog box type: **mmc**
- On the Console menu, click Add/Remove Snap-in....
- Click Add, and then click Certificates. Click Add again.
- You are prompted to open the snap-in for the current user account, the service account, or for the computer account. Select the **Computer Account**.
- Select **Local computer**, and then click Finish.
- Click Close in the Add Standalone Snap-in dialog box.
- Click OK in the Add/Remove Snap-in dialog box. Your installed certificates are located in the **Certificates** folder in the **Personal** container.

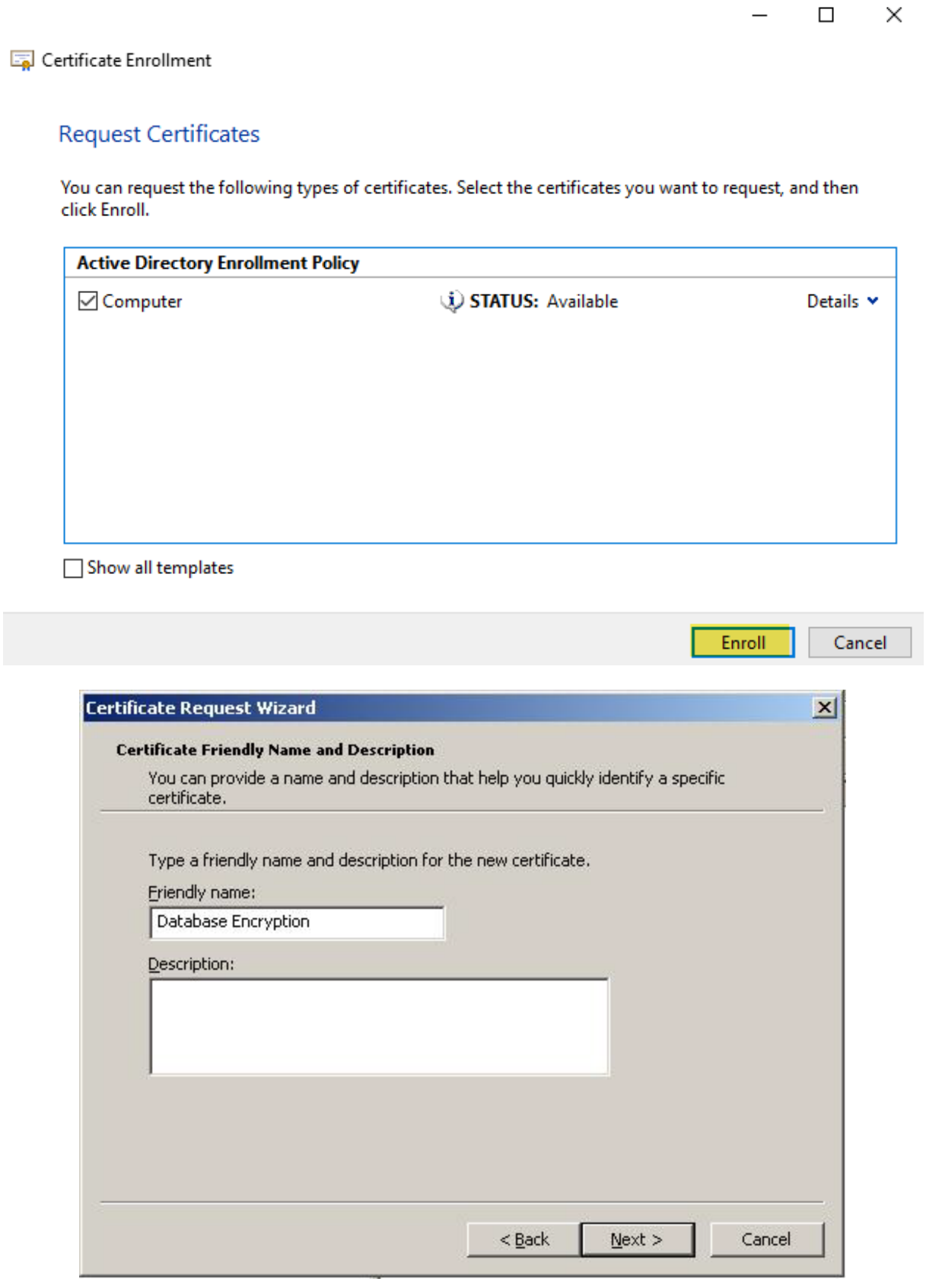
3. Installing a certificate on the server

In the MMC, click to select the Personal folder in the left-hand pane. Right-click in the right-hand pane, point to All Tasks, and then click Request New Certificate....which will bring up the dialogs shown below:





The **Certificate Request Wizard** dialog box opens. Click Next. Select Computer as the Certificate type.

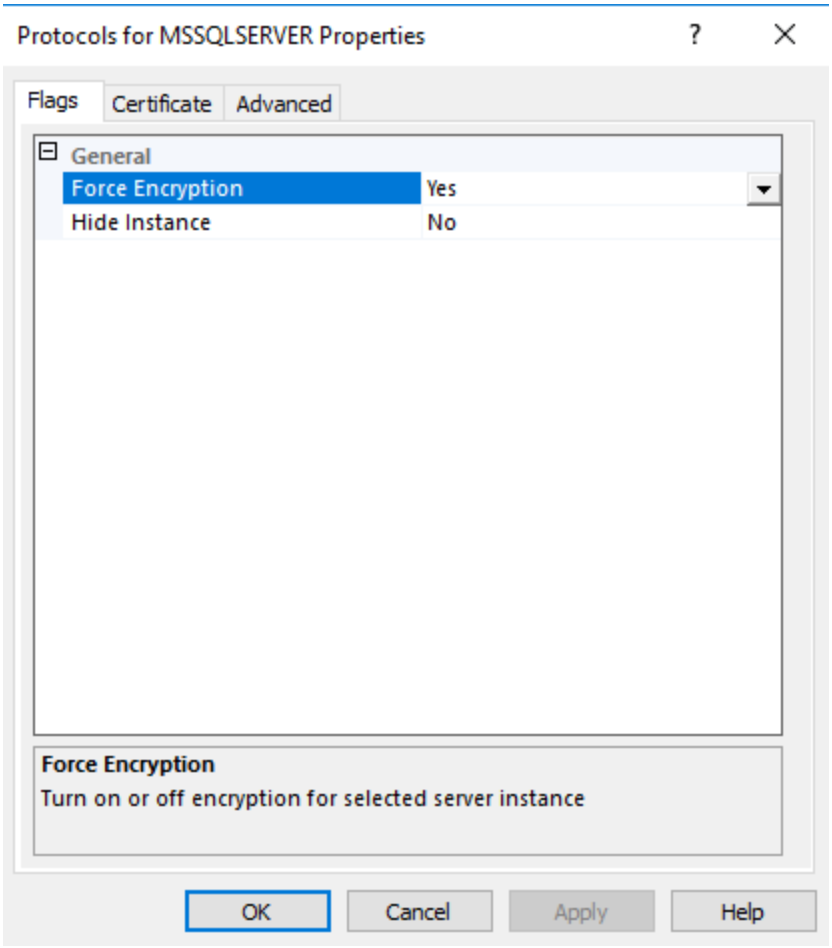


In the **Friendly Name** text box you can type a friendly name for the certificate or leave the text box blank, and then complete the wizard. After the wizard finishes, you will see the certificate in the folder with the fully qualified computer domain name.

4. Requiring database encryption for all communication

Once the certificate is installed you can configure the SQL Server to "Force protocol encryption".

Navigate to "Start -> Programs -> Microsoft SQL Server 2005-> Configuration Tools" and open the "SQL Server Configuration Manager". Expand "SQL Server 2005 Network Configuration". Right click on "Protocols for MSSQLSERVER" and choose Properties. Set "Force Encryption" to "Yes" then click on the Certificate tab where you have to select the certificate you created above.



When not using the collector, all clients communicating with the SQL Server will need an up-to-date SQL Server ODBC driver installed in order to support encryption. If a machine is unable to communicate with the database server after you enabled encryption, installing the latest MDAC (Microsoft Data Access Components) from MDAC Downloads will usually resolve the problem.

----------OLD_TEXT----------
Most ODBC drivers, including Microsoft SQL Server®, transmit network traffic in clear text which can be a problem in security sensitive environments. Microsoft SQL Server® supports protocol encryption which encrypts all traffic between the client (=EventSentry agent) and the Microsoft SQL Server®.

Using protocol encryption requires the following prerequisites:

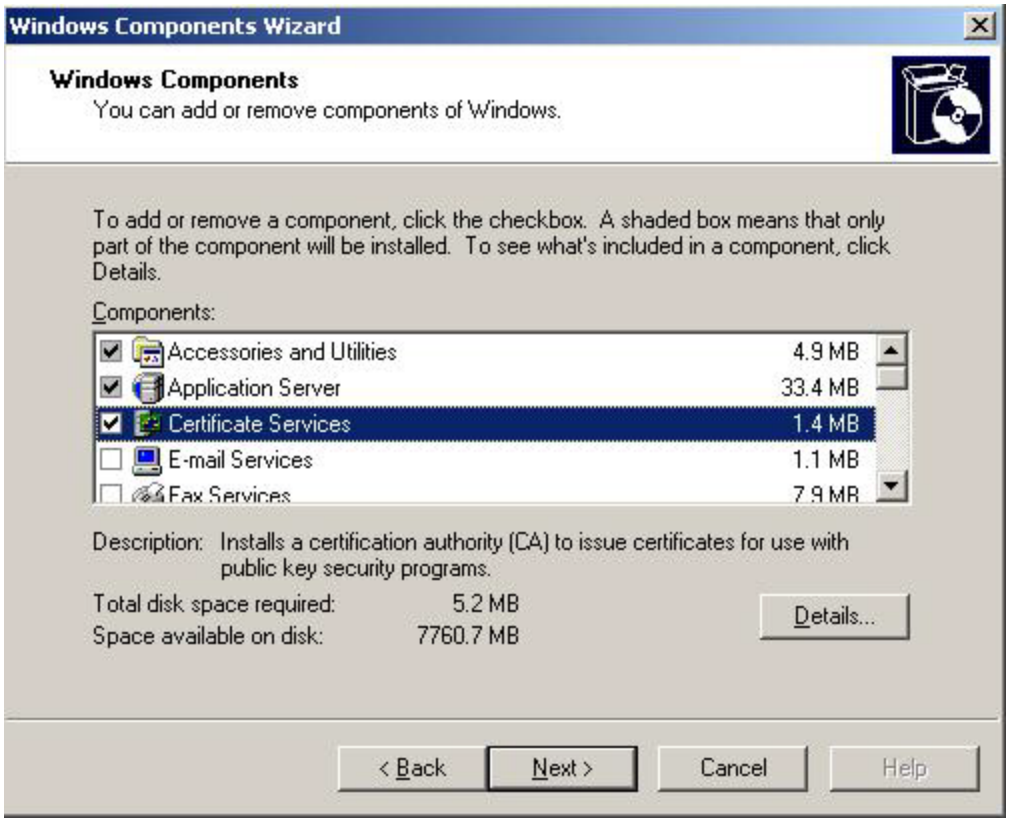
- Certificate Services installed on machine running SQL Server
- Latest SQL Server ODBC drivers installed on all clients (MDAC)

This chapter will guide you through the process of setting up Certificate Services and requesting a certificate so that SQL server can use protocol encryption. This chapter is based on using Windows Server 2003 for the OS and Microsoft SQL Server® 2000/Microsoft SQL Server® 2005 for the database.

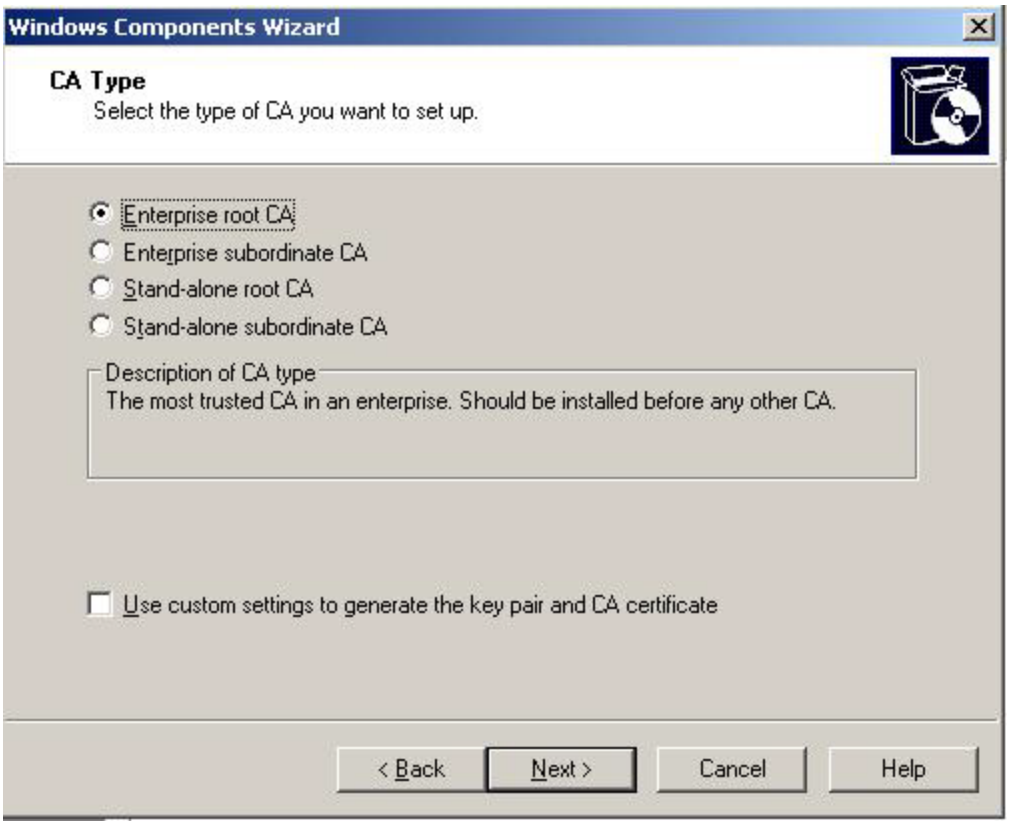
1. Installing Certificate Services

You will only need to follow these steps if you do not have certificate services running in your domain. If you already have a certificate server in your domain then you can skip step 1.

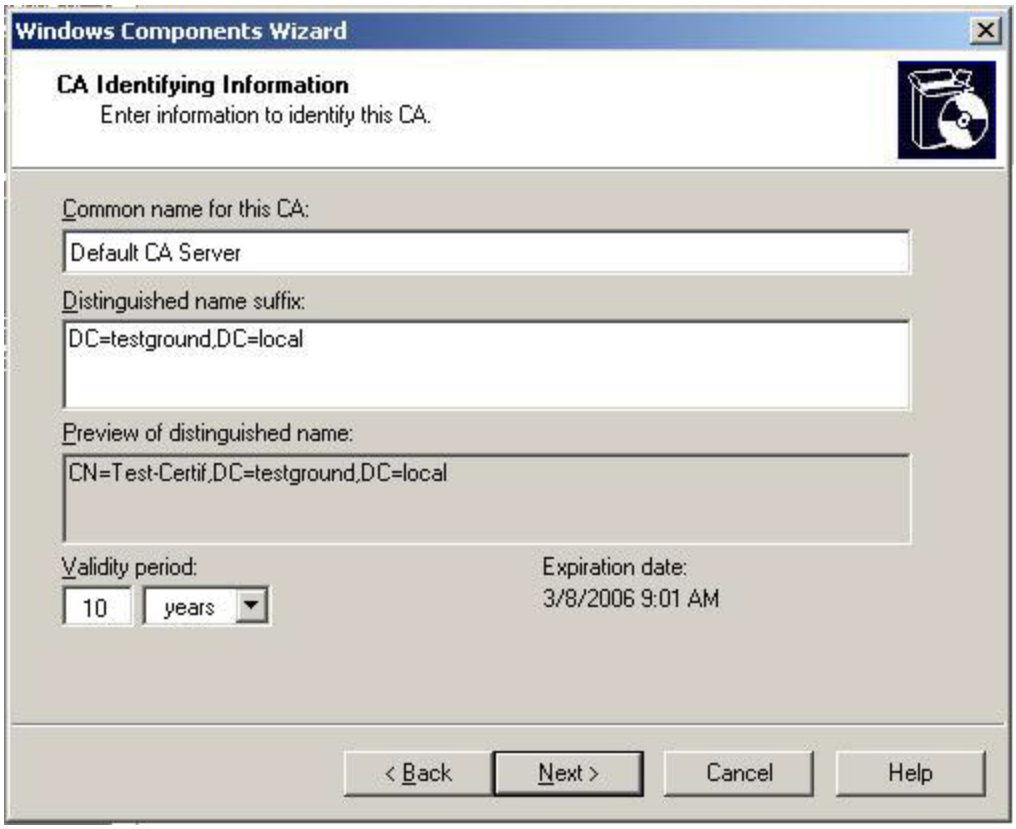
Navigate to "Start -> Settings -> Control Panel -> Add/Remove Programs" and click "Add/Remove Windows Components" which will bring up a screen similar to the one shown below:



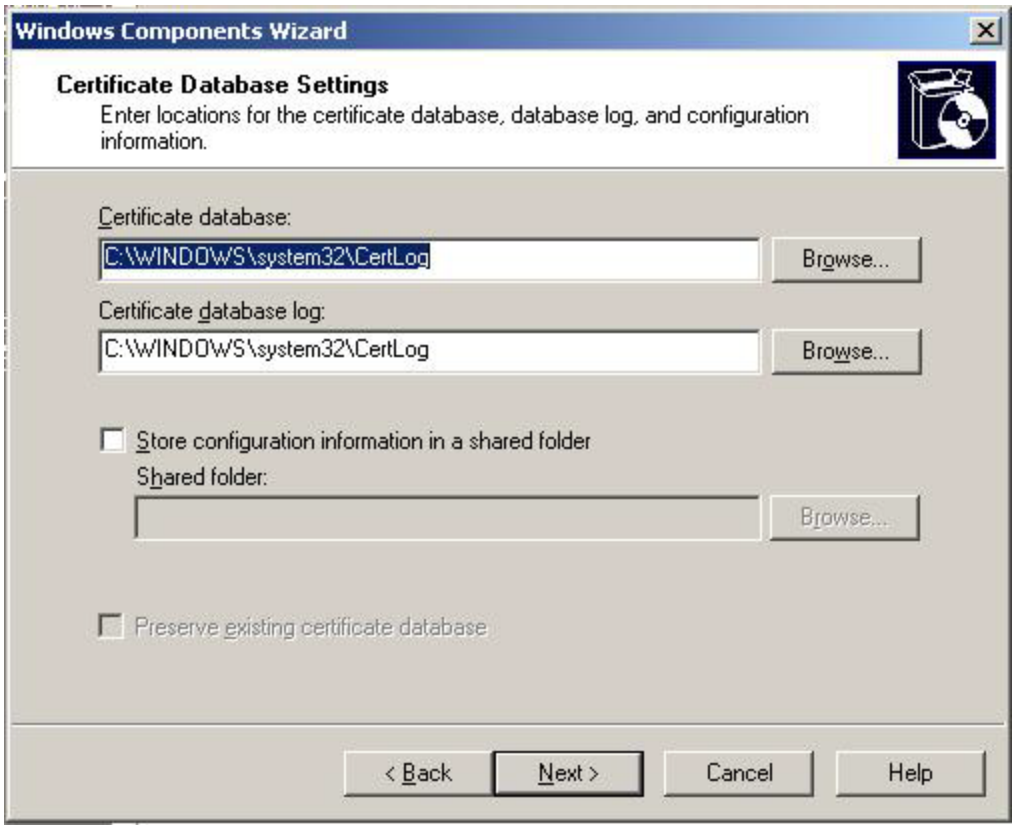
Check "Certificate Services" and click next. Click "Yes" on the confirmation dialog if the imposed restrictions are OK. On the next screen select the appropriate certificate authority type for your network. Please refer to the Windows Server documentation for more information. In our example we will be installing an "Enterprise Root CA" since it is the first CA server:

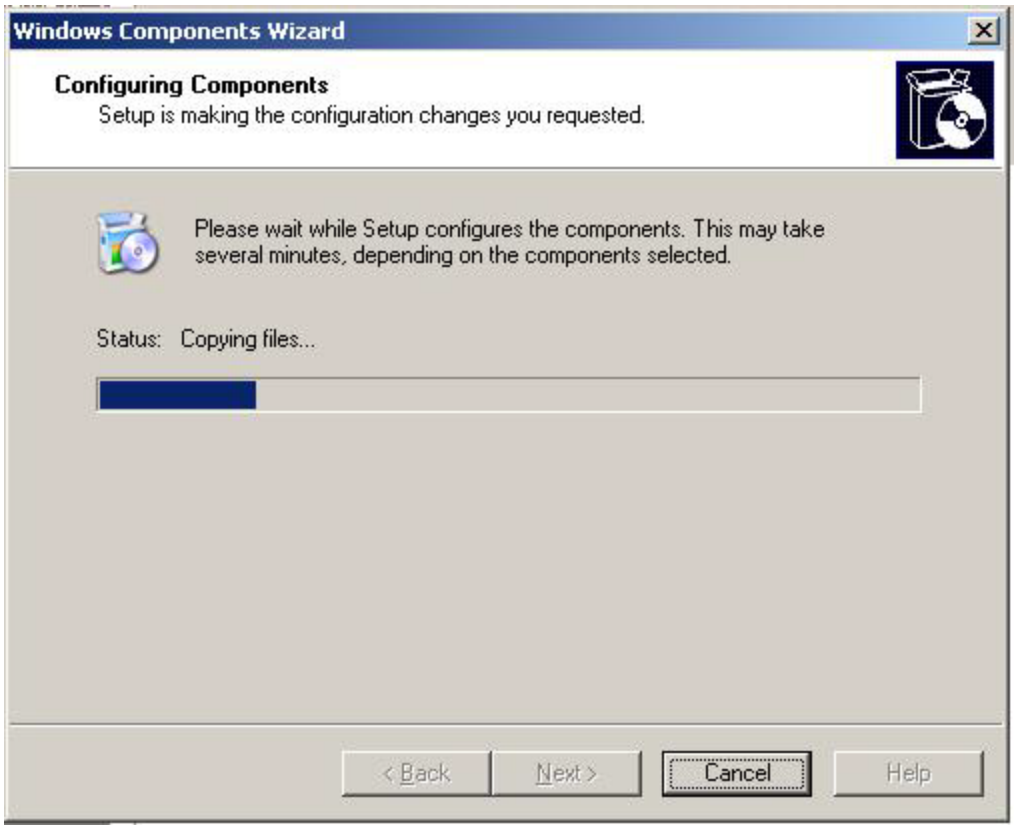


Please note that the following screenshots might look differently depending on the type of CA you select here (the screenshots shown are based on the "Enterprise root CA" selection). On the next screen enter the "CA Identifying Information". Make sure that you enter a good common CA name and a specify a validity period that is long enough:



After clicking Next confirm the following dialogs and click "Finish" to complete the setup of the CA.





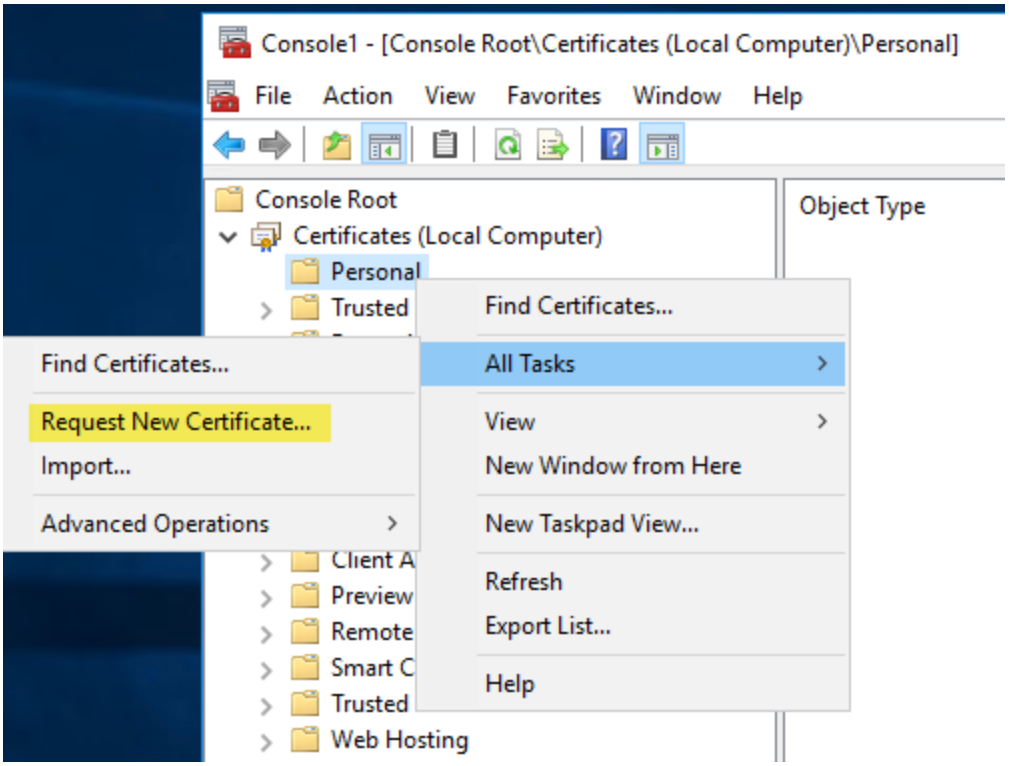
2. Configuring the MMC snap-in

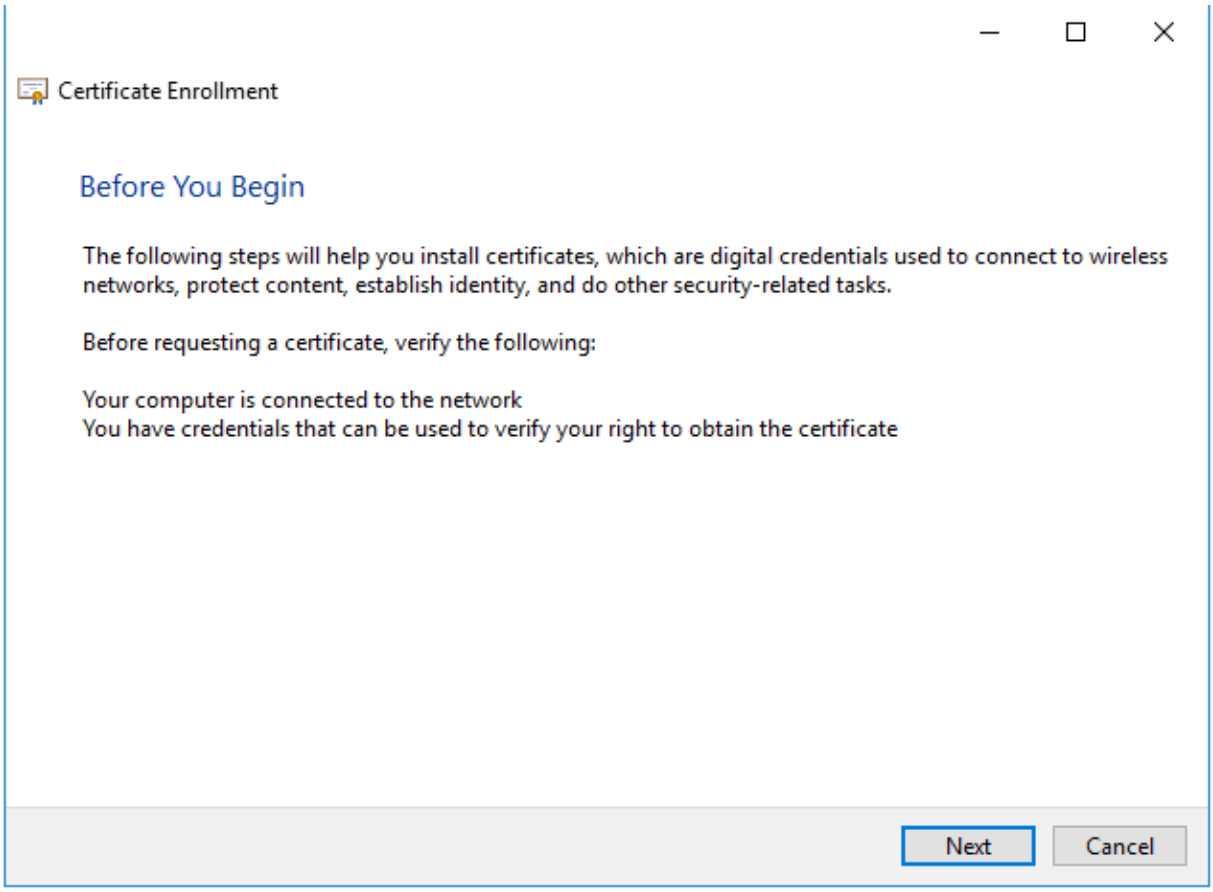
In order to manage/create certificates you need to configure an MMC for the certificate services. To open the Certificates snap-in, follow these steps:

- To open the MMC console, click Start, and then click Run. In the Run dialog box type: **mmc**
- On the Console menu, click Add/Remove Snap-in....
- Click Add, and then click Certificates. Click Add again.
- You are prompted to open the snap-in for the current user account, the service account, or for the computer account. Select the **Computer Account**.
- Select **Local computer**, and then click Finish.
- Click Close in the Add Standalone Snap-in dialog box.
- Click OK in the Add/Remove Snap-in dialog box. Your installed certificates are located in the **Certificates** folder in the **Personal** container.

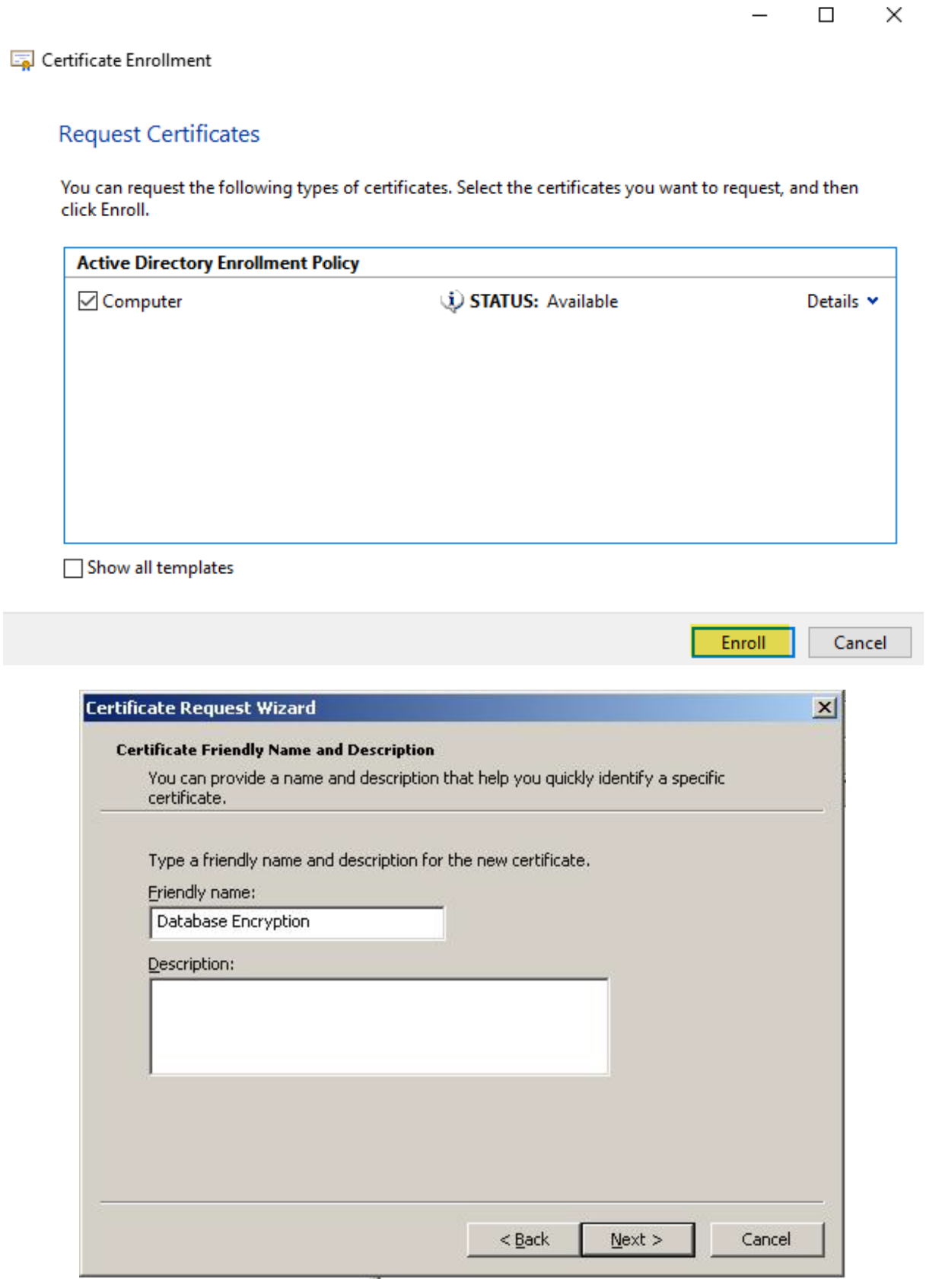
3. Installing a certificate on the server

In the MMC, click to select the Personal folder in the left-hand pane. Right-click in the right-hand pane, point to All Tasks, and then click Request New Certificate....which will bring up the dialogs shown below:





The **Certificate Request Wizard** dialog box opens. Click Next. Select Computer as the Certificate type.

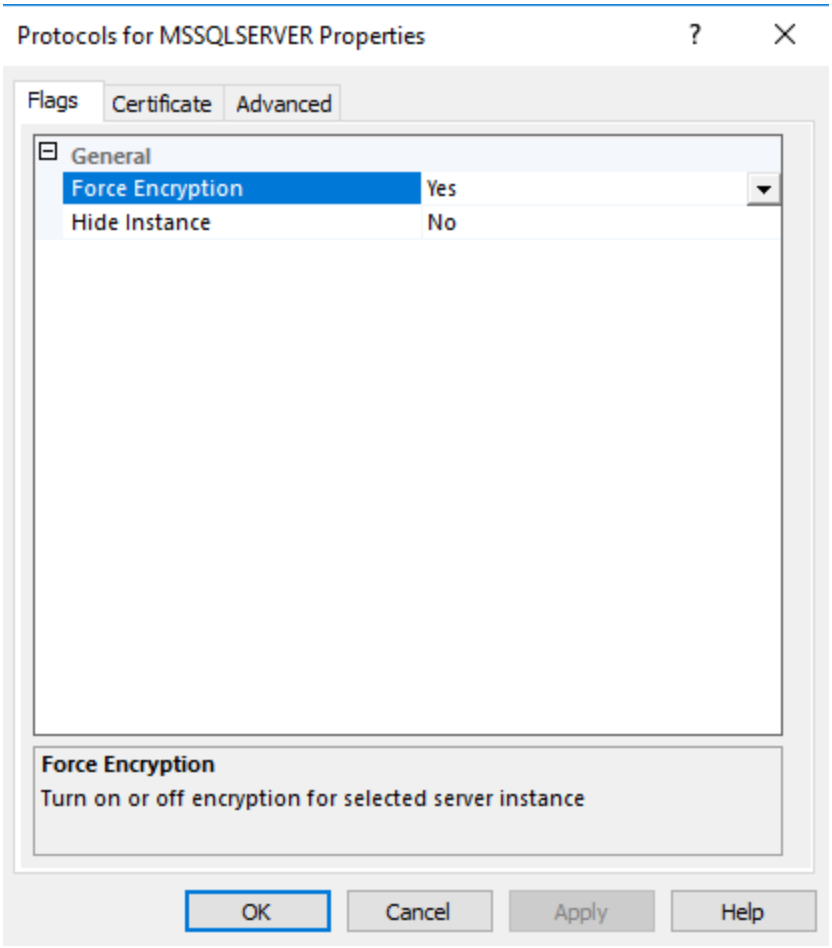


In the **Friendly Name** text box you can type a friendly name for the certificate or leave the text box blank, and then complete the wizard. After the wizard finishes, you will see the certificate in the folder with the fully qualified computer domain name.

4. Requiring database encryption for all communication

Once the certificate is installed you can configure the SQL Server to "Force protocol encryption".

Navigate to "Start -> Programs -> Microsoft SQL Server 2005-> Configuration Tools" and open the "SQL Server Configuration Manager". Expand "SQL Server 2005 Network Configuration". Right click on "Protocols for MSSQLSERVER" and choose Properties. Set "Force Encryption" to "Yes" then click on the Certificate tab where you have to select the certificate you created above.



When not using the collector, all clients communicating with the SQL Server will need an up-to-date SQL Server ODBC driver installed in order to support encryption. If a machine is unable to communicate with the database server after you enabled encryption, installing the latest MDAC (Microsoft Data Access Components) from MDAC Downloads will usually resolve the problem.

7.2 Event Log Reference

7.2.1 Security Events

7.2.1.1 Legacy Operating Systems

7.2.1.1.1 Windows NT Security Events

Windows NT security event descriptions from the security event log. These events will appear with the **security** event source.

```
   Event ID: 512
       Type: Success Audit
Description: Windows NT is starting up.
```

```
   Event ID: 513
       Type: Success Audit
Description: Windows NT is shutting down. All logon sessions will be
             terminated by this shutdown.

   Event ID: 514
       Type: Success Audit
Description: An authentication package has been loaded by the Local
             Security Authority. This authentication package will be
             used to authenticate logon attempts.
             Authentication Package Name: %1

   Event ID: 515
       Type: Success Audit
Description: A trusted logon process has registered with the Local
             Security Authority. This logon process will be trusted to
             submit logon requests.
             Logon Process Name: %1

   Event ID: 516
       Type: Success Audit
Description: Internal resources allocated for the queuing of audit
             messages have been exhausted, leading to the loss of some
             audits.
             Number of audit messages discarded: %1

   Event ID: 517
       Type: Success Audit
Description: The audit log was cleared
             Primary User Name: %1      Primary Domain: %2
             Primary Logon ID: %3       Client User Name: %4
             Client Domain: %5          Client Logon ID: %6

   Event ID: 518
       Type: Success Audit
Description: A notification package has been loaded by the Security
             Account Manager. This package will be notified of any
             account or password changes.
             Notification Package Name: %1

   Event ID: 528
       Type: Success Audit
Description: Successful Logon:
             User Name: %1            Domain: %2
             Logon ID: %3             Logon Type: %4
             Logon Process: %5        Authentication Package: %6
             Workstation Name: %7

   Event ID: 529
       Type: Failure Audit
Description: Logon Failure:
             Reason: Unknown user name or bad password
             User Name: %1             Domain: %2
             Logon Type: %3            Logon Process: %4
             Authentication Package: %5 Workstation Name: %6
```

```
   Event ID: 530
       Type: Failure Audit
Description: Logon Failure:
             Reason: Account logon time restriction violation
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 531
       Type: Failure Audit
Description: Logon Failure:
             Reason: Account currently disabled
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 532
       Type: Failure Audit
Description: Logon Failure:
             Reason: The specified user account has expired
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 533
       Type: Failure Audit
Description: Logon Failure:
             Reason: User not allowed to logon at this computer
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 534
       Type: Failure Audit
Description: Logon Failure:
             Reason: The user has not been granted the requested logon
             type at this machine
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 535
       Type: Failure Audit
Description: Logon Failure:
             Reason: The specified account's password has expired
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 536
       Type: Failure Audit
Description: Logon Failure:
             Reason: The NetLogon component is not active
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6
```

```
   Event ID: 537
       Type: Failure Audit
Description: Logon Failure:
             Reason: An unexpected error occurred during logon
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 538
       Type: Success Audit
Description: User Logoff:
             User Name: %1            Domain: %2
             Logon ID: %3             Logon Type: %4

   Event ID: 539
       Type: Failure Audit
Description: Logon Failure:
             Reason: Account locked out
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 560
       Type: Success Audit
Description: Object Open:
             Object Server: %1          Object Type: %2
             Object Name: %3            New Handle ID: %4
             Operation ID: {%5,%6}
             Process ID: %7             Primary User Name: %8
             Primary Domain: %9         Primary Logon ID: %10
             Client User Name: %11      Client Domain: %12
             Client Logon ID: %13       Accesses %14
             Privileges %15

   Event ID: 561
       Type: Success Audit
Description: Handle Allocated:
             Handle ID: %1              Operation ID: {%2,%3}
             Process ID: %4

   Event ID: 562
       Type: Success Audit
Description: Handle Closed:
             Object Server: %1          Handle ID: %2
             Process ID: %3

   Event ID: 563
       Type: Success Audit
Description: Object Open for Delete:
             Object Server: %1          Object   Type: %2
             Object Name: %3            New Handle ID: %4
             Operation ID: {%5,%6}
             Process ID: %7             Primary User Name: %8
             Primary Domain: %9         Primary Logon ID: %10
             Client User Name: %11      Client Domain: %12
```

```
             Client Logon ID: %13       Accesses %14
             Privileges %15

   Event ID: 564
       Type: Success Audit
Description: Object Deleted:
             Object Server: %1          Handle ID: %2
             Process ID: %3

   Event ID: 576
       Type: Success Audit
Description: Special privileges assigned to new logon:
             User Name: %1             Domain: %2
             Logon ID: %3              Assigned: %4

   Event ID: 577
       Type: Success Audit
Description: Privileged Service Called:
             Server: %1              Service: %2
             Primary User Name: %3      Primary Domain: %4
             Primary Logon ID: %5       Client User Name: %6
             Client Domain: %7          Client Logon ID: %8
             Privileges: %9

   Event ID: 578
       Type: Failure Audit
Description: Privileged object operation:
             Object Server: %1          Object Handle: %2
             Process ID: %3             Primary User Name: %4
             Primary Domain: %5         Primary Logon ID: %6
             Client User Name: %7       Client Domain: %8
             Client Logon ID: %9        Privileges: %10

   Event ID: 592
       Type: Success Audit
Description: A new process has been created:
             New Process ID: %1         Image File Name: %2
             Creator Process ID: %3     User Name: %4
             Domain: %5                 Logon ID: %6

   Event ID: 593
       Type: Success Audit
Description: A process has exited:
             Process ID: %1             User Name: %2
             Domain: %3              Logon ID: %4

   Event ID: 594
       Type: Success Audit
Description: A handle to an object has been duplicated:
             Source Handle ID: %1       Source Process ID: %2
             Target Handle ID: %3       Target Process ID: %4

   Event ID: 595
       Type: Success Audit
Description: Indirect access to an object has been obtained:
             Object   Type: %1          Object Name: %2
```

```
              Process ID: %3              Primary User Name: %4
              Primary Domain: %5          Primary Logon ID: %6
              Client User Name: %7        Client Domain: %8
              Client Logon ID: %9         Accesses: %10

   Event ID: 608
       Type: Success Audit
Description: User Right Assigned:
              User Right: %1              Assigned To: %2
              Assigned By:
              User Name: %3               Domain: %4
              Logon ID: %5

   Event ID: 609
       Type: Success Audit
Description: User Right Removed:
              User Right: %1              Removed From: %2
              Removed By:
              User Name: %3               Domain: %4
              Logon ID: %5

   Event ID: 610
       Type: Success Audit
Description: New Trusted Domain:
              Domain Name: %1             Domain ID: %2
              Established By:
              User Name: %3               Domain: %4
              Logon ID: %5

   Event ID: 611
       Type: Success Audit
Description: Removing Trusted Domain:
              Domain Name: %1             Domain ID: %2
              Removed By:
              User Name: %3               Domain: %4
              Logon ID: %5

   Event ID: 612
       Type: Success Audit
Description: Audit Policy Change:
              New Policy:
              Success   Failure
                %1         %2    System
                %3         %4    Logon/Logoff
                %5         %6    Object Access
                %7         %8    Privilege Use
                %9        %10    Detailed Tracking
               %11        %12    Policy Change
               %13        %14    Account Management
              Changed By:
              User Name: %15              Domain Name: %16
              Logon ID: %17

   Event ID: 624
       Type: Success Audit
Description: User Account Created:
```

```
             New Account Name: %1       New Domain: %2
             New Account ID: %3         Caller User Name: %4
             Caller Domain: %5          Caller Logon ID: %6
             Privileges %7

   Event ID: 625
       Type: Success Audit
Description: User Account Type Change:
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3      New Type: %4
             Caller User Name: %5       Caller Domain: %6
             Caller Logon ID: %7

   Event ID: 626
       Type: Success Audit
Description: User Account Enabled:
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3      Caller User Name: %4
             Caller Domain: %5          Caller Logon ID: %6

   Event ID: 627
       Type: Success Audit
Description: Change Password Attempt:
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3      Caller User Name: %4
             Caller Domain: %5          Caller Logon ID: %6
             Privileges: %7

   Event ID: 628
       Type: Success Audit
Description: User Account password set:
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3      Caller User Name: %4
             Caller Domain: %5          Caller Logon ID: %6

   Event ID: 629
       Type: Success Audit
Description: User Account Disabled:
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3      Caller User Name: %4
             Caller Domain: %5          Caller Logon ID: %6

   Event ID: 630
       Type: Success Audit
Description: User Account Deleted:
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3      Caller User Name: %4
             Caller Domain: %5          Caller Logon ID: %6
             Privileges: %7

   Event ID: 631
       Type: Success Audit
Description: Global Group Created:
             New Account Name: %1       New Domain: %2
             New Account ID: %3         Caller User Name: %4
             Caller Domain: %5          Caller Logon ID: %6
```

```
             Privileges: %7

   Event ID: 632
       Type: Success Audit
Description: Global Group Member Added:
             Member: %1                 Target Account Name: %2
             Target Domain: %3          Target Account ID: %4
             Caller User Name: %5       Caller Domain: %6
             Caller Logon ID: %7        Privileges: %8

   Event ID: 633
       Type: Success Audit
Description: Global Group Member Removed:
             Member: %1                 Target Account Name: %2
             Target Domain: %3          Target Account ID: %4
             Caller User Name: %5       Caller Domain: %6
             Caller Logon ID: %7        Privileges: %8

   Event ID: 634
       Type: Success Audit
Description: Global Group Deleted:
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3      Caller User Name: %4
             Caller Domain: %5          Caller Logon ID: %6
             Privileges: %7

   Event ID: 635
       Type: Success Audit
Description: Local Group Created:
             New Account Name: %1       New Domain: %2
             New Account ID: %3         Caller User Name: %4
             Caller Domain: %5          Caller Logon ID: %6
             Privileges: %7

   Event ID: 636
       Type: Success Audit
Description: Local Group Member Added:
             Member: %1                 Target Account Name: %2
             Target Domain: %3          Target Account ID: %4
             Caller User Name: %5       Caller Domain: %6
             Caller Logon ID: %7        Privileges: %8

   Event ID: 637
       Type: Success Audit
Description: Local Group Member Removed:
             Member: %1                 Target Account Name: %2
             Target Domain: %3          Target Account ID: %4
             Caller User Name: %5       Caller Domain: %6
             Caller Logon ID: %7        Privileges: %8

   Event ID: 638
       Type: Success Audit
Description: Local Group Deleted:
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3      Caller User Name: %4
             Caller Domain: %5          Caller Logon ID: %6
```

```
              Privileges: %7

   Event ID: 639
       Type: Success Audit
Description: Local Group Changed:
              Target Account Name: %1    Target Domain: %2
              Target Account ID: %3      Caller User Name: %4
              Caller Domain: %5          Caller Logon ID: %6
              Privileges: %7

   Event ID: 640
       Type: Success Audit
Description: General Account Database Change:
              Type of change: %1         Object Type: %2
              Object Name: %3            Object ID: %4
              Caller User Name: %5       Caller Domain: %6
              Caller Logon ID: %7

   Event ID: 641
       Type: Success Audit
Description: Global Group Changed:
              Target Account Name: %1    Target Domain: %2
              Target Account ID: %3      Caller User Name: %4
              Caller Domain: %5          Caller Logon ID: %6
              Privileges: %7

   Event ID: 642
       Type: Success Audit
Description: User Account Changed:
              Target Account Name: %1    Target Domain: %2
              Target Account ID: %3      Caller User Name: %4
              Caller Domain: %5          Caller Logon ID: %6
              Privileges: %7

   Event ID: 643
       Type: Success Audit
Description: Domain Policy Changed:
              Domain: %1                 Domain ID: %2
              Caller User Name: %3       Caller Domain: %4
              Caller Logon ID: %5        Privileges: %6

   Event ID: 644
       Type: Success Audit
Description: User Account Locked Out
               Target Account Name:  %1   Target Account ID: %2
               Caller Machine Name:  %3   Caller User Name:  %4
               Caller Domain:      %5     Caller Logon ID:  %6
```

7.2.1.1.2 Windows 2000 Security Events

Windows 2000 security event descriptions from the security event log. These events will appear with the **security** event source. Most of of the event descriptions listed here also apply to Windows XP and Windows Server 2003.

```
   Event ID: 512 (0x0200)
       Type: Success Audit
```

```
Description: Windows NT is starting up.

   Event ID: 513 (0x0201)
       Type: Success Audit
Description: Windows NT is shutting down.
             All logon sessions will be terminated by this shutdown.

   Event ID: 514 (0x0202)
       Type: Success Audit
Description: An authentication package has been loaded by the Local Security
Authority.
             This authentication package will be used to authenticate logon attempts.
             Authentication Package Name: %1

   Event ID: 515 (0x0203)
       Type: Success Audit
Description: A trusted logon process has registered with the Local Security Authority.
             This logon process will be trusted to submit logon requests.
             Logon Process Name: %1

   Event ID: 516 (0x0204)
       Type: Success Audit
Description: Internal resources allocated for the queuing of audit messages have been
             exhausted, leading to the loss of some audits.
             Number of audit messages discarded: %1

   Event ID: 517 (0x0205)
       Type: Success Audit
Description: The audit log was cleared
             Primary User Name: %1     Primary Domain:   %2
             Primary Logon ID:  %3     Client User Name: %4
             Client Domain:     %5     Client Logon ID:  %6

   Event ID: 518 (0x0206)
       Type: Success Audit
Description: An notification package has been loaded by the Security Account Manager.
             This package will be notified of any account or password changes.
             Notification Package Name: %1

   Event ID: 528 (0x0210)
       Type: Success Audit
Description: Successful Logon:
             User Name: %1             Domain: %2
             Logon ID: %3              Logon Type: %4
             Logon Process: %5         Authentication Package: %6
             Workstation Name: %7

   Event ID: 529 (0x0211)
       Type: Failure Audit
Description: Logon Failure
             Reason: Unknown user name or bad password
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 530 (0x0212)
```

```
       Type: Failure Audit
Description: Logon Failure
             Reason: Account logon time restriction violation
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 531 (0x0213)
       Type: Failure Audit
Description: Logon Failure
             Reason: Account currently disabled
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 532 (0x0214)
       Type: Failure Audit
Description: Logon Failure
             Reason: The specified user account has expired
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 533 (0x0215)
       Type: Failure Audit
Description: Logon Failure
             Reason: User not allowed to logon at this computer
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 534 (0x0216)
       Type: Failure Audit
Description: Logon Failure
             Reason:The user has not been granted the requested
             logon type at this machine
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 535 (0x0217)
       Type: Failure Audit
Description: Logon Failure
             Reason: The specified account's password has expired
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 536 (0x0218)
       Type: Failure Audit
Description: Logon Failure
             Reason: The NetLogon component is not active
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6
```

```
   Event ID: 537 (0x0219)
       Type: Failure Audit
Description: Logon Failure
             Reason: An unexpected error occurred during logon
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 538 (0x021A)
       Type: Success Audit
Description: User Logoff
             User Name: %1              Domain: %2
             Logon ID: %3               Logon Type: %4.

   Event ID: 539 (0x021B)
       Type: Failure Audit
Description: Logon Failure
             Reason: Account locked out
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6

   Event ID: 540 (0x021c)
       Type: Success Audit
Description: Successful Network Logon
             User Name: %1              Domain: %2
             Logon ID: %3               Logon Type: %4
             Logon Process: %5          Authentication Package: %6
             Workstation Name: %7

   Event ID: 541 (0x021d)
       Type: Success Audit
Description: IKE security association established.
             Mode: %1                   Peer Identity: %2
             Filter: %3                 Parameters: %4

   Event ID: 542 (0x021e)
       Type: Success Audit
Description: IKE security association ended.
             Mode: Data Protection (Quick mode)
             Filter: %1                 Inbound SPI: %2
             Outbound SPI: %3

   Event ID: 543 (0x021f)
       Type: Success Audit
Description: IKE security association ended.
             Mode: Key Exchange (Main mode)
             Filter: %1

   Event ID: 544 (0x0220)
       Type: Failure Audit
Description: IKE security association establishment failed because peer could not
             authenticate. The certificate trust could not be established.
             Peer Identity: %1          Filter: %2

   Event ID: 545 (0x0221)
```

```
       Type: Failure Audit
Description: IKE peer authentication failed.
             Peer Identity: %1          Filter: %2

   Event ID: 546 (0x0222)
       Type: Failure Audit
Description: IKE security association establishment failed because peer
             sent invalid proposal.
             Mode: %1                   Filter: %2
             Attribute: %3              Expected value: %4
             Received value: %5

   Event ID: 547 (0x0223)
       Type: Failure Audit
Description: IKE security association negotiation failed.
             Mode:          %1          Filter: %2
             Failure Point: %3          Failure Reason: %4

   Event ID: 560 (0x0230)
       Type: Success Audit
Description: Object Open
             Object Server: %1          Object Type: %2
             Object Name: %3            New Handle ID: %4
             Operation ID:{%5,%6}       Process ID: %7
             Primary User Name: %8      Primary Domain: %9
             Primary Logon ID: %10      Client User Name: %11
             Client Domain: %12         Client Logon ID: %13
             Accesses %14               Privileges %15

   Event ID: 561 (0x0231)
       Type: Success Audit
Description: Handle Allocated
             Handle ID: %1              Operation ID:{%2,%3}
             Process ID: %4

   Event ID: 562 (0x0232)
       Type: Success Audit
Description: Handle Closed
             Object Server: %1          Handle ID: %2
             Process ID: %3

   Event ID: 563 (0x0233)
       Type: Success Audit
Description: Object Open for Delete
             Object Server: %1          Object Type: %2
             Object Name: %3            New Handle ID: %4
             Operation ID:{%5,%6}       Process ID: %7
             Primary User Name: %8      Primary Domain: %9
             Primary Logon ID: %10      Client User Name: %11
             Client Domain: %12         Client Logon ID: %13
             Accesses %14               Privileges %15

   Event ID: 564 (0x0234)
       Type: Success Audit
Description: Object Deleted
             Object Server: %1          Handle ID: %2
```

```
              Process ID: %3

   Event ID: 565 (0x0235)
       Type: Success Audit
Description: Object Open
              Object Server: %1          Object Type: %2
              Object Name: %3            New Handle ID: %4
              Operation ID:{%5,%6}       Process ID: %7
              Primary User Name: %8      Primary Domain: %9
              Primary Logon ID: %10      Client User Name: %11
              Client Domain: %12         Client Logon ID: %13
              Accesses %14               Privileges %15
              Properties:%16%17%18%19%20%21%22%23%24%25

   Event ID: 566 (0x0236)
       Type: Success Audit
Description: Object Operation
              Operation Type %1          Object Type: %2
              Object Name: %3            Handle ID: %4
              Operation ID:{%5,%6}       Primary User Name: %7
              Primary Domain: %8         Primary Logon ID: %9
              Client User Name: %10      Client Domain: %11
              Client Logon ID: %12       Requested Accesses %13

   Event ID: 576 (0x0240)
       Type: Success Audit
Description: Special privileges assigned to new logon:
              User Name: %1              Domain: %2
              Logon ID: %3               Assigned: %4

   Event ID: 577 (0x0241)
       Type: Success Audit
Description: Privileged Service Called
              Server: %1                 Service: %2
              Primary User Name: %3      Primary Domain: %4
              Primary Logon ID: %5       Client User Name: %6
              Client Domain: %7          Client Logon ID: %8
              Privileges: %9

   Event ID: 578 (0x0242)
       Type: Success Audit
Description: Privileged object operation
              Object Server: %1          Object Handle: %2
              Process ID: %3             Primary User Name: %4
              Primary Domain: %5         Primary Logon ID: %6
              Client User Name: %7       Client Domain: %8
              Client Logon ID: %9        Privileges: %10

   Event ID: 592 (0x0250)
       Type: Success Audit
Description: A new process has been created
              New Process ID: %1         Image File Name: %2
              Creator Process ID: %3     User Name: %4
              Domain: %5                 Logon ID: %6

   Event ID: 593 (0x0251)
```

```
       Type: Success Audit
Description: A process has exited
             Process ID: %1             User Name: %2
             Domain: %3                 Logon ID: %4

   Event ID: 594 (0x0252)
       Type: Success Audit
Description: A handle to an object has been duplicated
             Source Handle ID: %1       Source Process ID: %2
             Target Handle ID: %3       Target Process ID: %4

   Event ID: 595 (0x0253)
       Type: Success Audit
Description: Indirect access to an object has been obtained
             Object Type: %1            Object Name: %2
             Process ID: %3             Primary User Name: %4
             Primary Domain: %5         Primary Logon ID: %6
             Client User Name: %7       Client Domain: %8
             Client Logon ID: %9        Accesses: %10

   Event ID: 608 (0x0260)
       Type: Success Audit
Description: User Right Assigned
             User Right: %1             Assigned To: %2
Assigned By  User Name: %3              Domain: %4
             Logon ID: %5

   Event ID: 609 (0x0261)
       Type: Success Audit
Description: User Right Removed
             User Right: %1             Removed From: %2
Removed By:  User Name: %3              Domain: %4
             Logon ID: %5

   Event ID: 610 (0x0262)
       Type: Success Audit
Description: New Trusted Domain
             Domain Name: %1            Domain ID: %2
Established By:
             User Name: %3              Domain: %4
             Logon ID: %5

   Event ID: 611 (0x0263)
       Type: Success Audit
Description: Removing Trusted Domain
             Domain Name: %1            Domain ID: %2
Removed By:  User Name: %3              Domain: %4
             Logon ID: %5

   Event ID: 612 (0x0264)
       Type: Success Audit
Description: Audit Policy Change
             New Policy:
             Success   Failure
               %1        %2    System
               %3        %4    Logon/Logoff
```

```
                %5         %6    Object Access
                %7         %8    Privilege Use
                %9        %10    Detailed Tracking
               %11        %12    Policy Change
               %13        %14    Account Management
              Changed By:
              User Name: %15             Domain Name: %16
              Logon ID: %17

   Event ID: 613 (0x0265)
       Type: Success Audit
Description: IPSec policy agent started
              Ipsec Policy Agent: %1     Policy Source:  %2
              Event Data: %3

   Event ID: 614 (0x0266)
       Type: Success Audit
Description: IPSec policy agent disabled
              Ipsec Policy Agent: %1     Event Data:  %2

   Event ID: 615 (0x0267)
       Type: Success Audit
Description: IPSEC PolicyAgent Service:  %1
              Event Data: %1

   Event ID: 616 (0x0268)
       Type: Failure Audit
Description: IPSec policy agent encountered a potentially serious failure.
              Event Data: %1

   Event ID: 617 (0x0269)
       Type: Success Audit
Description: Kerberos Policy Changed
Changed By:  User Name: %1              Domain Name: %2
              Logon ID: %3
                Changes made: %4

                '-'  means no changes, otherwise each change is shown as:
                Parameter Name: (new value) (old value)

   Event ID: 618 (0x026a)
       Type: Success Audit
Description: Encrypted Data Recovery Policy Changed
Changed By:  User Name: %1              Domain Name: %2
              Logon ID: %3
                Changes made: %4

                '-'  means no changes, otherwise each change is shown as:
                Parameter Name: new value (old value)

   Event ID: 619 (0x026b)
       Type: Success Audit
Description: Quality of Service Policy Changed
Changed By:  User Name: %1              Domain Name: %2
              Logon ID: %3
                Changes made: %4
```

```
              '-'  means no changes, otherwise each change is shown as:
              Parameter Name: new value (old value)

   Event ID: 620 (0x026C)
Description: Trusted Domain Information Modified:
             Domain Name: %1            Domain ID: %2
Modified By: User Name: %3              Domain: %4
             Logon ID: %5

   Event ID: 624 (0x0270)
       Type: Success Audit
Description: User Account Created
             New Account Name: %1       New Domain: %2
             New Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges %7

   Event ID: 625 (0x0271)
Description: User Account Type Change
       Type: Success Audit
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             New Type: %4               Caller User Name: %5
             Caller Domain: %6          Caller Logon ID: %7

   Event ID: 626 (0x0272)
Description: User Account Enabled
       Type: Success Audit
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6

              Note: Windows 2000 does not log event ID 626 explicitly.
              Results are logged as a part of event ID 642 in the description of the
message.

   Event ID: 627 (0x0273)
       Type: Success Audit
Description: Change Password Attempt
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 628 (0x0274)
       Type: Success Audit
Description: User Account password set
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6

   Event ID: 630 (0x0276)
       Type: Success Audit
```

```
Description: User Account Deleted:
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 631 (0x0277)
       Type: Success Audit
Description: Security Enabled Global Group Created
             New Account Name: %1       New Domain: %2
             New Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 632 (0x0278)
       Type: Success Audit
Description: Security Enabled Global Group Member Added
             Member Name: %1            Member ID: %2
             Target Account Name: %3    Target Domain: %4
             Target Account ID: %5
             Caller User Name: %6       Caller Domain: %7
             Caller Logon ID: %8        Privileges: %9

   Event ID: 633 (0x0279)
       Type: Success Audit
Description: Security Enabled Global Group Member Removed
             Member Name: %1            Member ID: %2
             Target Account Name: %3    Target Domain: %4
             Target Account ID: %5
             Caller User Name: %6       Caller Domain: %7
             Caller Logon ID: %8        Privileges: %9

   Event ID: 634 (0x027A)
       Type: Success Audit
Description: Security Enabled Global Group Deleted
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 635 (0x027B)
       Type: Success Audit
Description: Security Enabled Local Group Created
             New Account Name: %1       New Domain: %2
             New Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 636 (0x027C)
       Type: Success Audit
Description: Security Enabled Local Group Member Added
             Member Name: %1            Member ID: %2
             Target Account Name: %3    Target Domain: %4
             Target Account ID: %5
             Caller User Name: %6       Caller Domain: %7
             Caller Logon ID: %8        Privileges: %9
```

```
   Event ID: 637 (0x027D)
       Type: Success Audit
Description: Security Enabled Local Group Member Removed
             Member Name: %1            Member ID: %2
             Target Account Name: %3    Target Domain: %4
             Target Account ID: %5
             Caller User Name: %6       Caller Domain: %7
             Caller Logon ID: %8        Privileges: %9

   Event ID: 638 (0x027E)
       Type: Success Audit
Description: Security Enabled Local Group Deleted
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 639 (0x027F)
       Type: Success Audit
Description: Security Enabled Local Group Changed
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 640 (0x0280)
       Type: Success Audit
Description: General Account Database Change
             Type of change: %1         Object Type: %2
             Object Name: %3            Object ID: %4
             Caller User Name: %5       Caller Domain: %6
             Caller Logon ID: %7

   Event ID: 641 (0x0281)
       Type: Success Audit
Description: Security Enabled Global Group Changed
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 642 (0x0282)
       Type: Success Audit
Description: User Account Changed
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 643 (0x0283)
       Type: Success Audit
Description: Domain Policy Changed: %1 modified
             Domain: %2                 Domain ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7
```

```
   Event ID: 644 (0x0284)
       Type: Success Audit
Description: User Account Locked Out
             Target Account Name: %1    Target Account ID: %3
             Caller Machine Name: %2
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6

   Event ID: 645 (0x0285)
       Type: Success Audit
Description: Computer Account Created
             New Account Name: %1       New Domain: %2
             New Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges %7

   Event ID: 646 (0x0286)
       Type: Success Audit
Description: Computer Account Changed
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %5       Caller Domain: %6
             Caller Logon ID: %7        Privileges: %8

   Event ID: 647 (0x0287)
       Type: Success Audit
Description: Computer Account Deleted
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 648 (0x0288)
       Type: Success Audit
Description: Security Disabled Local Group Created
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 649 (0x0289)
       Type: Success Audit
Description: Security Disabled Local Group Changed
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 650 (0x028A)
       Type: Success Audit
Description: Security Disabled Local Group Member Added
             Member Name: %1            Member ID: %2
             Target Account Name: %3    Target Domain: %4
             Target Account ID: %5
             Caller User Name: %6       Caller Domain: %7
```

```
             Caller Logon ID: %8        Privileges: %9

   Event ID: 651 (0x028B)
       Type: Success Audit
Description: Security Disabled Local Group Member Removed
             Member Name: %1            Member ID: %2
             Target Account Name: %3    Target Domain: %4
             Target Account ID: %5
             Caller User Name: %6       Caller Domain: %7
             Caller Logon ID: %8        Privileges: %9

   Event ID: 652 (0x028C)
       Type: Success Audit
Description: Security Disabled Local Group Deleted
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 653 (0x028D)
       Type: Success Audit
Description: Security Disabled Global Group Created
             New Account Name: %1       New Domain: %2
             New Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 654 (0x028E)
       Type: Success Audit
Description: Security Disabled Global Group Changed
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 655 (0x028F)
       Type: Success Audit
Description: Security Disabled Global Group Member Added
             Member Name: %1            Member ID: %2
             Target Account Name: %3    Target Domain: %4
             Target Account ID: %5
             Caller User Name: %6       Caller Domain: %7
             Caller Logon ID: %8        Privileges: %9

   Event ID: 656 (0x0290)
       Type: Success Audit
Description: Security Disabled Global Group Member Removed
             Member Name: %1            Member ID: %2
             Target Account Name: %3    Target Domain: %4
             Target Account ID: %5
             Caller User Name: %6       Caller Domain: %7
             Caller Logon ID: %8        Privileges: %9

   Event ID: 657 (0x0291)
       Type: Success Audit
Description: Security Disabled Global Group Deleted
```

```
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 658 (0x0292)
       Type: Success Audit
Description: Security Enabled Universal Group Created
             New Account Name: %1       New Domain: %2
             New Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 659 (0x0293)
       Type: Success Audit
Description: Security Enabled Universal Group Changed
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 660 (0x0294)
       Type: Success Audit
Description: Security Enabled Universal Group Member Added
             Member Name: %1            Member ID: %2
             Target Account Name: %3    Target Domain: %4
             Target Account ID: %5
             Caller User Name: %6       Caller Domain: %7
             Caller Logon ID: %8        Privileges: %9

   Event ID: 661 (0x0295)
       Type: Success Audit
Description: Security Enabled Universal Group Member Removed
             Member Name: %1            Member ID: %2
             Target Account Name: %3    Target Domain: %4
             Target Account ID: %5
             Caller User Name: %6       Caller Domain: %7
             Caller Logon ID: %8        Privileges: %9

   Event ID: 662 (0x0296)
       Type: Success Audit
Description: Security Enabled Universal Group Deleted
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 663 (0x0297)
       Type: Success Audit
Description: Security Disabled Universal Group Created
             New Account Name: %1       New Domain: %2
             New Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 664 (0x0298)
```

```
       Type: Success Audit
Description: Security Disabled Universal Group Changed
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 665 (0x0299)
       Type: Success Audit
Description: Security Disabled Universal Group Member Added
             Member Name: %1            Member ID: %2
             Target Account Name: %3    Target Domain: %4
             Target Account ID: %5
             Caller User Name: %6       Caller Domain: %7
             Caller Logon ID: %8        Privileges: %9

   Event ID: 666 (0x029A)
       Type: Success Audit
Description: Security Disabled Universal Group Member Removed
             Member Name: %1            Member ID: %2
             Target Account Name: %3    Target Domain: %4
             Target Account ID: %5
             Caller User Name: %6       Caller Domain: %7
             Caller Logon ID: %8        Privileges: %9

   Event ID: 667 (0x029B)
       Type: Success Audit
Description: Security Disabled Universal Group Deleted
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %4       Caller Domain: %5
             Caller Logon ID: %6        Privileges: %7

   Event ID: 668 (0x029C)
       Type: Success Audit
Description: Group Type Changed
             Target Account Name: %1    Target Domain: %2
             Target Account ID: %3
             Caller User Name: %5       Caller Domain: %6
             Caller Logon ID: %7        Privileges: %8

   Event ID: 669 (0x029D)
       Type: Success Audit
Description: Add SID History
             Source Account Name: %1    Source Account ID: %2
             Target Account Name: %3    Target Domain: %4
             Target Account ID: %5
             Caller User Name: %6       Caller Domain: %7
             Caller Logon ID: %8        Privileges: %9

   Event ID: 670 (0x029E)
       Type: Success Audit
Description: Add SID History
             Source Account Name: %1    Target Account Name: %2
             Target Domain: %3          Target Account ID: %4
             Caller User Name: %5       Caller Domain: %6
```

```
              Caller Logon ID: %7        Privileges: %8

   Event ID: 672 (0x02a0)
       Type: Success Audit
Description: Authentication Ticket Granted
              User Name: %1              Supplied Realm Name: %2
              User ID: %3                Service Name: %4
              Service ID: %5             Ticket Options: %6
              Ticket Encryption Type: %7 Pre-Authentication Type: %8
              Client Address: %9

   Event ID: 673 (0x02a1)
       Type: Success Audit
Description: Service Ticket Granted
              User Name: %1              User Domain: %2
              Service Name: %3           Service ID: %4
              Ticket Options: %5         Ticket Encryption Type: %6
              Client Address: %7

   Event ID: 674 (0x02a2)
       Type: Success Audit
Description: Ticket Granted Renewed
              User Name: %1              User Domain: %2
              Service Name: %3           Service ID: %4
              Ticket Options: %5         Ticket Encryption Type: %6
              Client Address: %7

   Event ID: 675 (0x02a3)
       Type: Failure Audit
Description: Pre-authentication failed
              User Name: %1              User ID: %2
              Service Name: %3           Pre-Authentication Type: %4
              Failure Code: %5           Client Address: %6

   Event ID: 676 (0x02a4)
       Type: Failure Audit
Description: Authentication Ticket Request Failed
              User Name: %1              Supplied Realm Name: %2
              Service Name: %3           Ticket Options: %4
              Failure Code: %5           Client Address: %6

   Event ID: 677 (0x02a5)
       Type: Failure Audit
Description: Service Ticket Request Failed:
Description: Authentication Ticket Request Failed
              User Name: %1              Supplied Realm Name: %2
              Service Name: %3           Ticket Options: %4
              Failure Code: %5           Client Address: %6

   Event ID: 678 (0x02a6)
       Type: Success Audit
Description: Account Mapped for Logon by: %1
              Client Name: %2            Mapped Name:%3

   Event ID: 679 (0x02a7)
       Type: Failure Audit
```

```
Description: The name: %2 could not be mapped for logon by: %1

   Event ID: 680 (0x02a8)
       Type: Success Audit
Description: Account Used for Logon by: %1
             Account Name: %2           Workstation: %3

   Event ID: 681 (0x02a9)
       Type: Failure Audit
Description: The logon to account: %2 by: %1 from workstation: %3 failed. The error
code was: %4

   Event ID: 682 (0x02aa)
       Type: Success Audit
Description: Session reconnected to winstation:
             User Name: %1              Domain: %2
             Logon ID: %3               Session Name: %4
             Client Name: %5            Client Address: %6

   Event ID: 683 (0x02ab)
       Type: Success Audit
Description: Session disconnected from winstation:
             User Name: %1              Domain: %2
             Logon ID: %3               Session Name: %4
             Client Name: %5            Client Address: %6
```

7.2.1.2 Windows 2003 Security Events

Account Logon Events

Event ID: 672
Description: An authentication service (AS) ticket was successfully issued and validated.

Event ID: 673
A ticket granting service (TGS) ticket was granted. A TGS is a ticket issued by the Kerberos version 5 ticket-granting service TGS that allows a user to authenticate to a specific service in the domain.

Event ID: 674
A security principal renewed an AS ticket or TGS ticket.

Event ID: 675
Pre-authentication failed. This event is generated on a Key Distribution Center (KDC) when a user types in an incorrect password.

Event ID: 676
Authentication ticket request failed. This event is not generated in Windows XP Professional or in members of the Windows Server family.

Event ID: 677
A TGS ticket was not granted. This event is not generated in Windows XP Professional or in the members of the Windows Server family.

Event ID: 678
An account was successfully mapped to a domain account.

Event ID: 681
Logon failure. A domain account logon was attempted. This event is not generated in Windows XP Professional or in members of the Windows Server family.

Event ID: 682
A user has reconnected to a disconnected terminal server session.

Event ID: 683
A user disconnected a terminal server session without logging off.

Account Management Events

Event ID: 624
A user account was created.

Event ID: 627
A user password was changed.

Event ID: 628
A user password was set.

Event ID: 630
A user account was deleted.

Event ID: 631

A global group was created.

Event ID: 632
A member was added to a global group.

Event ID: 633
A member was removed from a global group.

Event ID: 634
A global group was deleted.

Event ID: 635
A new local group was created.

Event ID: 636
A member was added to a local group.

Event ID: 637
A member was removed from a local group.

Event ID: 638
A local group was deleted.

Event ID: 639
A local group account was changed.

Event ID: 641
A global group account was changed.

Event ID: 642
A user account was changed.

Event ID: 643
A domain policy was modified.

Event ID: 644
A user account was automatically locked.

Event ID: 645
A computer account was created.

Event ID: 646
A computer account was changed.

Event ID: 647
A computer account was deleted.

Event ID: 648
A local security group with security disabled was created.

Note: SECURITY_DISABLED in the formal name means that this group cannot be used to grant permissions in access checks.

Event ID: 649
A local security group with security disabled was changed.

Event ID: 650
A member was added to a security-disabled local security group.

Event ID: 651
A member was removed from a security-disabled local security group.

Event ID: 652
A security-disabled local group was deleted.

Event ID: 653
A security-disabled global group was created.

Event ID: 654
A security-disabled global group was changed.

Event ID: 655
A member was added to a security-disabled global group.

Event ID: 656
A member was removed from a security-disabled global group.

Event ID: 657
A security-disabled global group was deleted.

Event ID: 658
A security-enabled universal group was created.

Event ID: 659
A security-enabled universal group was changed.

Event ID: 660
A member was added to a security-enabled universal group.

Event ID: 661
A member was removed from a security-enabled universal group.

Event ID: 662
A security-enabled universal group was deleted.

Event ID: 663
A security-disabled universal group was created.

Event ID: 664
A security-disabled universal group was changed.

Event ID: 665
A member was added to a security-disabled universal group.

Event ID: 666
A member was removed from a security-disabled universal group.

Event ID: 667
A security-disabled universal group was deleted.

Event ID: 668
A group type was changed.

Event ID: 684
The security descriptor of administrative group members was set.

Note: Every 60 minutes on a domain controller, a background thread searches all members of administrative groups (such as domain, enterprise, and schema administrators) and applies a fixed security descriptor on them. This event is logged.

Event ID: 685
Name of an account was changed.

Directory Service Access Events

Event ID: 566
A generic object operation took place.

Audit Logon Events

Event ID: 528
A user successfully logged on to a computer.

Event ID: 529
Logon failure. A logon attempt was made with an unknown user name or a known user name with a bad password.

Event ID: 530
Logon failure. A logon attempt was made outside the allowed time.

Event ID: 531
Logon failure. A logon attempt was made using a disabled account.

Event ID: 532
Logon failure. A logon attempt was made using an expired account.

Event ID: 533
Logon failure. A logon attempt was made by a user who is not allowed to log on at the specified computer.

Event ID: 534
Logon failure. The user attempted to log on with a password type that is not allowed.

Event ID: 535
Logon failure. The password for the specified account has expired.

Event ID: 536
Logon failure. The Net Logon service is not active.

Event ID: 537
Logon failure. The logon attempt failed for other reasons.

Note: In some cases, the reason for the logon failure may not be known.

Event ID: 538
The logoff process was completed for a user.

Event ID: 539
Logon failure. The account was locked out at the time the logon attempt was made.

Event ID: 540
A user successfully logged on to a network.

Event ID: 541
Main mode Internet Key Exchange (IKE) authentication was completed between the local computer and the listed peer identity (establishing a security association), or quick mode has established a data channel.

Event ID: 542
A data channel was terminated.

Event ID: 543
Main mode was terminated.

Note: This might occur as a result of the time limit on the security association expiring (the default is eight hours), policy changes, or peer termination.

Event ID: 544
Main mode authentication failed because the peer did not provide a valid certificate or the signature was not validated.

Event ID: 545
Main mode authentication failed because of a Kerberos failure or a password that is not valid.

Event ID: 546
IKE security association establishment failed because the peer sent a proposal that is not valid. A packet was received that contained data that is not valid.

Event ID: 547
A failure occurred during an IKE handshake.

Event ID: 548
Logon failure. The security identifier (SID) from a trusted domain does not match the account domain SID of the client.

Event ID: 549
Logon failure. All SIDs corresponding to untrusted namespaces were filtered out during an authentication across forests.

Event ID: 550
Notification message that could indicate a possible denial-of-service (DoS) attack.

Event ID: 551
A user initiated the logoff process.

Event ID: 552
A user successfully logged on to a computer using explicit credentials while already logged on as a different user.

Event ID: 682
A user has reconnected to a disconnected terminal server session.

Event ID: 683
A user disconnected a terminal server session without logging off.

Note: This event is generated when a user is connected to a terminal server session over the network. It appears on the terminal server.

Object Access Events

Event ID: 560
Access was granted to an already existing object.

Event ID: 562
A handle to an object was closed.

Event ID: 563
An attempt was made to open an object with the intent to delete it.

Note: This is used by file systems when the FILE_DELETE_ON_CLOSE flag is specified in Createfile().

Event ID: 564
A protected object was deleted.

Event ID: 565
Access was granted to an already existing object type.

Event ID: 567
A permission associated with a handle was used.

Note: A handle is created with certain granted permissions (Read, Write, and so on). When the handle is used, up to one audit is generated for each of the permissions that were used.

Event ID: 568
An attempt was made to create a hard link to a file that is being audited.

Event ID: 569
The resource manager in Authorization Manager attempted to create a client context.

Event ID: 570
A client attempted to access an object.

Note: An event will be generated for every attempted operation on the object.

Event ID: 571
The client context was deleted by the Authorization Manager application.

Event ID: 572
The Administrator Manager initialized the application.

Event ID: 772
The Certificate Manager denied a pending certificate request.

Event ID: 773
Certificate Services received a resubmitted certificate request.

Event ID: 774
Certificate Services revoked a certificate.

Event ID: 775
Certificate Services received a request to publish the certificate revocation list (CRL).

Event ID: 776
Certificate Services published the CRL.

Event ID: 777
A certificate request extension was made.

Event ID: 778
One or more certificate request attributes changed.

Event ID: 779
Certificate Services received a request to shut down.

Event ID: 780
Certificate Services backup started.

Event ID: 781
Certificate Services backup completed.

Event ID: 782
Certificate Services restore started.

Event ID: 783
Certificate Services restore completed.

Event ID: 784
Certificate Services started.

Event ID: 785
Certificate Services stopped.

Event ID: 786
The security permissions for Certificate Services changed.

Event ID: 787
Certificate Services retrieved an archived key.

Event ID: 788
Certificate Services imported a certificate into its database.

Event ID: 789
The audit filter for Certificate Services changed.

Event ID: 790
Certificate Services received a certificate request.

Event ID: 791
Certificate Services approved a certificate request and issued a certificate.

Event ID: 792
Certificate Services denied a certificate request.

Event ID: 793

Certificate Services set the status of a certificate request to pending.

Event ID: 794
The certificate manager settings for Certificate Services changed.

Event ID: 795
A configuration entry changed in Certificate Services.

Event ID: 796
A property of Certificate Services changed.

Event ID: 797
Certificate Services archived a key.

Event ID: 798
Certificate Services imported and archived a key.

Event ID: 799
Certificate Services published the certificate authority (CA) certificate to Microsoft Active Directory directory service.

Event ID: 800
One or more rows have been deleted from the certificate database.

Event ID: 801
Role separation enabled.

Audit Policy Change Events

Event ID: 608
A user right was assigned.

Event ID: 609
A user right was removed.

Event ID: 610
A trust relationship with another domain was created.

Event ID: 611
A trust relationship with another domain was removed.

Event ID: 612
An audit policy was changed.

Event ID: 613
An Internet Protocol security (IPSec) policy agent started.

Event ID: 614
An IPSec policy agent was disabled.

Event ID: 615
An IPSec policy agent changed.

Event ID: 616
An IPSec policy agent encountered a potentially serious failure.

Event ID: 617
A Kerberos version 5 policy changed.

Event ID: 618
Encrypted Data Recovery policy changed.

Event ID: 620
A trust relationship with another domain was modified.

Event ID: 621
System access was granted to an account.

Event ID: 622
System access was removed from an account.

Event ID: 623
Auditing policy was set on a per-user basis

Event ID: 625
Auditing policy was refreshed on a per-user basis.

Event ID: 768
A collision was detected between a namespace element in one forest and a namespace element in another forest.

Note: When a namespace element in one forest overlaps a namespace element in another forest, it can lead to ambiguity in resolving a name belonging to one of the namespace elements. This overlap is also called a collision. Not all parameters are valid for each entry type. For example, fields such as DNS name, NetBIOS name, and SID are not valid for an entry of type 'TopLevelName.'

Event ID: 769
Trusted forest information was added.

Note: This event message is generated when forest trust information is updated and one or more entries are added. One event message is generated for each added, deleted, or modified entry. If multiple entries are added, deleted, or modified in a single update of the forest trust information, all the generated event messages are assigned a single unique identifier called an operation ID. This allows you to determine that the multiple generated event messages are the result of a single operation. Not all parameters are valid for each entry type. For example, parameters such as DNS name, NetBIOS name and SID are not valid for an entry of type "TopLevelName."

Event ID: 770
Trusted forest information was deleted.

Note: See event description for event 769.

Event ID: 771
Trusted forest information was modified.

Note: See event description for event 769.

Event ID: 805
The event log service read the security log configuration for a session.

Privilege Use Events

Event ID: 576
Specified privileges were added to a user's access token.

Note: This event is generated when the user logs on.

Event ID: 577
A user attempted to perform a privileged system service operation.

Event ID: 578
Privileges were used on an already open handle to a protected object.

Detailed Tracking Events

Event ID: 592
A new process was created.

Event ID: 593
A process exited.

Event ID: 594
A handle to an object was duplicated.

Event ID: 595
Indirect access to an object was obtained.

Event ID: 596
A data protection master key was backed up.

Note: The master key is used by the CryptProtectData and CryptUnprotectData routines, and Encrypting File System (EFS). The master key is backed up each time a new one is created. (The default setting is 90 days.) The key is usually backed up by a domain controller.

Event ID: 597
A data protection master key was recovered from a recovery server.

Event ID: 598
Auditable data was protected.

Event ID: 599
Auditable data was unprotected.

Event ID: 600
A process was assigned a primary token.

Event ID: 601
A user attempted to install a service.

Event ID: 602
A scheduler job was created.

Audit System Events

Event ID: 512
Windows is starting up.

Event ID: 513
Windows is shutting down.

Event ID: 514
An authentication package was loaded by the Local Security Authority.

Event ID: 515
A trusted logon process has registered with the Local Security Authority.

Event ID: 516
Internal resources allocated for the queuing of security event messages have been exhausted, leading to the loss of some security event messages.

Event ID: 517
The audit log was cleared.

Event ID: 518
A notification package was loaded by the Security Accounts Manager.

Event ID: 519
A process is using an invalid local procedure call (LPC) port in an attempt to impersonate a client and reply or read from or write to a client address space.

Event ID: 520
The system time was changed.

Note: This audit normally appears twice.

7.2.1.3 Windows 2008 Security Events

Category: Account Logon

Subcategory: Credential Validation

ID	Message
4774	An account was mapped for logon.
4775	An account could not be mapped for logon.
4776	The domain controller attempted to validate the credentials for an account.
4777	The domain controller failed to validate the credentials for an account.

Subcategory: Kerberos Service Ticket Operations

ID	Message
4768	A Kerberos authentication ticket (TGT) was requested.
4769	A Kerberos service ticket was requested.
4770	A Kerberos service ticket was renewed.
4771	Kerberos pre-authentication failed.
4772	A Kerberos authentication ticket request failed.

Category: Account Management

Subcategory: Application Group Management

ID	Message
4783	A basic application group was created.
4784	A basic application group was changed.
4785	A member was added to a basic application group.

4786 A member was removed from a basic application group.
4787 A non-member was added to a basic application group.
4788 A non-member was removed from a basic application group.
4789 A basic application group was deleted.
4790 An LDAP query group was created.

Subcategory: Computer Account Management

ID	Message
4742	A computer account was changed.
4743	A computer account was deleted.

Subcategory: Distribution Group Management

ID	Message
4744	A security-disabled local group was created.
4745	A security-disabled local group was changed.
4746	A member was added to a security-disabled local group.
4747	A member was removed from a security-disabled local group.
4748	A security-disabled local group was deleted.
4749	A security-disabled global group was created.
4750	A security-disabled global group was changed.
4751	A member was added to a security-disabled global group.
4752	A member was removed from a security-disabled global group.
4753	A security-disabled global group was deleted.
4759	A security-disabled universal group was created.
4760	A security-disabled universal group was changed.
4761	A member was added to a security-disabled universal group.
4762	A member was removed from a security-disabled universal group.

Subcategory: Other Account Management Events

ID	Message
4782	The password hash an account was accessed.
4793	The Password Policy Checking API was called.

Subcategory: Security Group Management

ID	Message
4727	A security-enabled global group was created.
4728	A member was added to a security-enabled global group.
4729	A member was removed from a security-enabled global group.
4730	A security-enabled global group was deleted.
4731	A security-enabled local group was created.
4732	A member was added to a security-enabled local group.
4733	A member was removed from a security-enabled local group.
4734	A security-enabled local group was deleted.
4735	A security-enabled local group was changed.
4737	A security-enabled global group was changed.
4754	A security-enabled universal group was created.
4755	A security-enabled universal group was changed.
4756	A member was added to a security-enabled universal group.
4757	A member was removed from a security-enabled universal group.
4758	A security-enabled universal group was deleted.
4764	A group’s type was changed.

Subcategory: User Account Management

ID	Message
4720	A user account was created.
4722	A user account was enabled.
4723	An attempt was made to change an account's password.
4724	An attempt was made to reset an account's password.
4725	A user account was disabled.
4726	A user account was deleted.
4738	A user account was changed.
4740	A user account was locked out.
4765	SID History was added to an account.
4766	An attempt to add SID History to an account failed.
4767	A user account was unlocked.
4780	The ACL was set on accounts which are members of administrators groups.
4781	The name of an account was changed:
4794	An attempt was made to set the Directory Services Restore Mode.
5376	Credential Manager credentials were backed up.
5377	Credential Manager credentials were restored from a backup.

Category: Detailed Tracking

Subcategory: DPAPI Activity

ID	Message
4692	Backup of data protection master key was attempted.
4693	Recovery of data protection master key was attempted.
4694	Protection of auditable protected data was attempted.
4695	Unprotection of auditable protected data was attempted.

Subcategory: Process Creation

ID	Message
4688	A new process has been created.
4689	A process has exited.
4696	A primary token was assigned to process.

Subcategory: RPC Events

ID	Message
5712	A Remote Procedure Call (RPC) was attempted.

Category: DS Access

Subcategory: Detailed Directory Service Replication

ID	Message
4928	An Active Directory replica source naming context was established.
4929	An Active Directory replica source naming context was removed.
4930	An Active Directory replica source naming context was modified.
4931	An Active Directory replica destination naming context was modified.
4934	Attributes of an Active Directory object were replicated.
4935	Replication failure begins.
4936	Replication failure ends.
4937	A lingering object was removed from a replica.

Subcategory: Directory Service Access

ID Message
4662 An operation was performed on an object.

Subcategory: Directory Service Changes
ID Message
5136 A directory service object was modified.
5137 A directory service object was created.
5138 A directory service object was undeleted.
5139 A directory service object was moved.

Note: The following event in the Directory Service Changes subcategory is available only in Windows Vista Service Pack 1 and in Windows Server 2008.
ID Message
5141 A directory service object was deleted.

Subcategory: Directory Service Replication
ID Message
4932 Synchronization of a replica of an Active Directory naming context has begun.
4933 Synchronization of a replica of an Active Directory naming context has ended.

Category: Logon/Logoff

Subcategory: IPsec Extended Mode
ID Message
4978 During Extended Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
4979 IPsec Main Mode and Extended Mode security associations were established.
4980 IPsec Main Mode and Extended Mode security associations were established.
4981 IPsec Main Mode and Extended Mode security associations were established.
4982 IPsec Main Mode and Extended Mode security associations were established.
4983 An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.
4984 An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.

Subcategory: IPsec Main Mode
ID Message
4646 IKE DoS-prevention mode started.
4650 An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used.
4651 An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.
4652 An IPsec Main Mode negotiation failed.
4653 An IPsec Main Mode negotiation failed.
4655 An IPsec Main Mode security association ended.
4976 During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
5049 An IPsec Security Association was deleted.
5453 An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.

Subcategory: IPsec Quick Mode

ID Message
4654 An IPsec Quick Mode negotiation failed.
4977 During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
5451 An IPsec Quick Mode security association was established.
5452 An IPsec Quick Mode security association ended.

Subcategory: Logoff
ID Message
4634 An account was logged off.
4647 User initiated logoff.

Subcategory: Logon
ID Message
4624 An account was successfully logged on.
4625 An account failed to log on.
4648 A logon was attempted using explicit credentials.
4675 SIDs were filtered.

Note All the events in the Network Policy Server subcategory are available only in Windows Vista Service Pack 1 and in Windows Server 2008.

Subcategory: Network Policy Server
ID Message
6272 Network Policy Server granted access to a user.
6273 Network Policy Server denied access to a user.
6274 Network Policy Server discarded the request for a user.
6275 Network Policy Server discarded the accounting request for a user.
6276 Network Policy Server quarantined a user.
6277 Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.
6278 Network Policy Server granted full access to a user because the host met the defined health policy.
6279 Network Policy Server locked the user account due to repeated failed authentication attempts.
6280 Network Policy Server unlocked the user account.

Subcategory: Other Logon/Logoff Events
ID Message
4649 A replay attack was detected.
4778 A session was reconnected to a Window Station.
4779 A session was disconnected from a Window Station.
4800 The workstation was locked.
4801 The workstation was unlocked.
4802 The screen saver was invoked.
4803 The screen saver was dismissed.
5378 The requested credentials delegation was disallowed by policy.
5632 A request was made to authenticate to a wireless network.
5633 A request was made to authenticate to a wired network.

Subcategory: Special Logon
ID Message
4964 Special groups have been assigned to a new logon.

Category: Object Access

Subcategory: Application Generated

ID	Message
4665	An attempt was made to create an application client context.
4666	An application attempted an operation:
4667	An application client context was deleted.
4668	An application was initialized.

Subcategory: Certification Services

ID	Message
4868	The certificate manager denied a pending certificate request.
4869	Certificate Services received a resubmitted certificate request.
4870	Certificate Services revoked a certificate.
4871	Certificate Services received a request to publish the certificate revocation list (CRL).
4872	Certificate Services published the certificate revocation list (CRL).
4873	A certificate request extension changed.
4874	One or more certificate request attributes changed.
4875	Certificate Services received a request to shut down.
4876	Certificate Services backup started.
4877	Certificate Services backup completed.
4878	Certificate Services restore started.
4879	Certificate Services restore completed.
4880	Certificate Services started.
4881	Certificate Services stopped.
4882	The security permissions for Certificate Services changed.
4883	Certificate Services retrieved an archived key.
4884	Certificate Services imported a certificate into its database.
4885	The audit filter for Certificate Services changed.
4886	Certificate Services received a certificate request.
4887	Certificate Services approved a certificate request and issued a certificate.
4888	Certificate Services denied a certificate request.
4889	Certificate Services set the status of a certificate request to pending.
4890	The certificate manager settings for Certificate Services changed.
4891	A configuration entry changed in Certificate Services.
4892	A property of Certificate Services changed.
4893	Certificate Services archived a key.
4894	Certificate Services imported and archived a key.
4895	Certificate Services published the CA certificate to Active Directory Domain Services.
4896	One or more rows have been deleted from the certificate database.
4897	Role separation enabled:
4898	Certificate Services loaded a template.

Subcategory: File Share

ID	Message
5140	A network share object was accessed.

Subcategory: File System

ID	Message
4664	An attempt was made to create a hard link.
4985	The state of a transaction has changed.
5051	A file was virtualized.

Subcategory: Filtering Platform Connection

ID Message
5031 The Windows Firewall Service blocked an application from accepting incoming connections on the network.
5152 The Windows Filtering Platform blocked a packet.
5153 A more restrictive Windows Filtering Platform filter has blocked a packet.
5154 The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.
5155 The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.
5156 The Windows Filtering Platform has allowed a connection.
5157 The Windows Filtering Platform has blocked a connection.
5158 The Windows Filtering Platform has permitted a bind to a local port.
5159 The Windows Filtering Platform has blocked a bind to a local port.

Subcategory: Handle Manipulation

ID Message
4656 A handle to an object was requested.
4658 The handle to an object was closed.
4690 An attempt was made to duplicate a handle to an object.

Subcategory: Other Object Access Events

ID Message
4671 An application attempted to access a blocked ordinal through the TBS.
4691 Indirect access to an object was requested.
4698 A scheduled task was created.
4699 A scheduled task was deleted.
4700 A scheduled task was enabled.
4701 A scheduled task was disabled.
4702 A scheduled task was updated.
5888 An object in the COM+ Catalog was modified.
5889 An object was deleted from the COM+ Catalog.
5890 An object was added to the COM+ Catalog.

Subcategory: Registry

ID Message
4657 A registry value was modified.
5039 A registry key was virtualized.

Subcategory: Subcategory

Note The following event may be generated by any resource manager when enabling its subcategory. For example, the following event may be generated by the Registry resource manager or the File System resource manager.
ID Message
4659 A handle to an object was requested with intent to delete.
4660 An object was deleted.
4661 A handle to an object was requested.
4663 An attempt was made to access an object.

Category: Policy Change

Subcategory: Audit Policy Change

ID	Message
4715	The audit policy (SACL) on an object was changed.
4719	System audit policy was changed.
4902	The Per-user audit policy table was created.
4904	An attempt was made to register a security event source.
4905	An attempt was made to unregister a security event source.
4906	The CrashOnAuditFail value has changed.
4907	Auditing settings on object were changed.
4908	Special Groups Logon table modified.
4912	Per User Audit Policy was changed.

Subcategory: Authentication Policy Change

ID	Message
4706	A new trust was created to a domain.
4707	A trust to a domain was removed.
4713	Kerberos policy was changed.
4716	Trusted domain information was modified.
4717	System security access was granted to an account.
4718	System security access was removed from an account.
4739	Domain Policy was changed.
4864	A namespace collision was detected.
4865	A trusted forest information entry was added.
4866	A trusted forest information entry was removed.
4867	A trusted forest information entry was modified.

Subcategory: Authorization Policy Change

ID	Message
4704	A user right was assigned.
4705	A user right was removed.
4714	Encrypted data recovery policy was changed.

Subcategory: Filtering Platform Policy Change

ID	Message
4709	IPsec Services was started.
4710	IPsec Services was disabled.
4711	May contain any one of the following: • PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer. • PAStore Engine applied Active Directory storage IPsec policy on the computer. • PAStore Engine applied local registry storage IPsec policy on the computer. • PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer. • PAStore Engine failed to apply Active Directory storage IPsec policy on the computer. • PAStore Engine failed to apply local registry storage IPsec policy on the computer. • PAStore Engine failed to apply some rules of the active IPsec policy on the computer. • PAStore Engine failed to load directory storage IPsec policy on the computer. • PAStore Engine loaded directory storage IPsec policy on the computer. • PAStore Engine failed to load local storage IPsec policy on the computer. • PAStore Engine loaded local storage IPsec policy on the computer. • PAStore Engine polled for changes to the active IPsec policy and detected no changes.
4712	IPsec Services encountered a potentially serious failure.
5040	A change has been made to IPsec settings. An Authentication Set was added.
5041	A change has been made to IPsec settings. An Authentication Set was modified.

5042 A change has been made to IPsec settings. An Authentication Set was deleted.
5043 A change has been made to IPsec settings. A Connection Security Rule was added.
5044 A change has been made to IPsec settings. A Connection Security Rule was modified.
5045 A change has been made to IPsec settings. A Connection Security Rule was deleted.
5046 A change has been made to IPsec settings. A Crypto Set was added.
5047 A change has been made to IPsec settings. A Crypto Set was modified.
5048 A change has been made to IPsec settings. A Crypto Set was deleted.
5440 The following callout was present when the Windows Filtering Platform Base Filtering Engine started.
5441 The following filter was present when the Windows Filtering Platform Base Filtering Engine started.
5442 The following provider was present when the Windows Filtering Platform Base Filtering Engine started.
5443 The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.
5444 The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.
5446 A Windows Filtering Platform callout has been changed.
5448 A Windows Filtering Platform provider has been changed.
5449 A Windows Filtering Platform provider context has been changed.
5450 A Windows Filtering Platform sub-layer has been changed.
5456 PAStore Engine applied Active Directory storage IPsec policy on the computer.
5457 PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.
5458 PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.
5459 PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.
5460 PAStore Engine applied local registry storage IPsec policy on the computer.
5461 PAStore Engine failed to apply local registry storage IPsec policy on the computer.
5462 PAStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem.
5463 PAStore Engine polled for changes to the active IPsec policy and detected no changes.
5464 PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services.
5465 PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully.
5466 PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied.
5467 PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used.
5468 PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no longer being used.
5471 PAStore Engine loaded local storage IPsec policy on the computer.
5472 PAStore Engine failed to load local storage IPsec policy on the computer.
5473 PAStore Engine loaded directory storage IPsec policy on the computer.
5474 PAStore Engine failed to load directory storage IPsec policy on the computer.
5477 PAStore Engine failed to add quick mode filter.

Subcategory: MPSSVC Rule-Level Policy Change
ID Message

4944 The following policy was active when the Windows Firewall started.
4945 A rule was listed when the Windows Firewall started.
4946 A change has been made to Windows Firewall exception list. A rule was added.
4947 A change has been made to Windows Firewall exception list. A rule was modified.
4948 A change has been made to Windows Firewall exception list. A rule was deleted.
4949 Windows Firewall settings were restored to the default values.
4950 A Windows Firewall setting has changed.
4951 A rule has been ignored because its major version number was not recognized by Windows Firewall.
4952 Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.
4953 A rule has been ignored by Windows Firewall because it could not parse the rule.
4954 Windows Firewall Group Policy settings have changed. The new settings have been applied.
4956 Windows Firewall has changed the active profile.
4957 Windows Firewall did not apply the following rule:
4958 Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer:

Subcategory: Other Policy Change Events

ID Message
4909 The local policy settings for the TBS were changed.
4910 The group policy settings for the TBS were changed.
5063 A cryptographic provider operation was attempted.
5064 A cryptographic context operation was attempted.
5065 A cryptographic context modification was attempted.
5066 A cryptographic function operation was attempted.
5067 A cryptographic function modification was attempted.
5068 A cryptographic function provider operation was attempted.
5069 A cryptographic function property operation was attempted.
5070 A cryptographic function property modification was attempted.
5447 A Windows Filtering Platform filter has been changed.
6144 Security policy in the group policy objects has been applied successfully.
6145 One or more errors occurred while processing security policy in the group policy objects.

Subcategory: Subcategory

Note The following event may be generated by any resource manager when enabling its subcategory. For example, the following event may be generated by the Registry resource manager or the File System resource manager.

ID Message
4670 Permissions on an object were changed.

Category: Privilege Use

Subcategory: Sensitive Privilege Use / Non Sensitive Privilege Use

ID Message
4672 Special privileges assigned to new logon.
4673 A privileged service was called.
4674 An operation was attempted on a privileged object.

Category: System

Subcategory: IPsec Driver

ID Message

4960 IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.

4961 IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.

4962 IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.

4963 IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.

4965 IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.

5478 IPsec Services has started successfully.

5479 IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.

5480 IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.

5483 IPsec Services failed to initialize RPC server. IPsec Services could not be started.

5484 IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.

5485 IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.

Subcategory: Other System Events

ID Message

5024 The Windows Firewall Service has started successfully.

5025 The Windows Firewall Service has been stopped.

5027 The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.

5028 The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.

5029 The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.

5030 The Windows Firewall Service failed to start.

5032 Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.

5033 The Windows Firewall Driver has started successfully.

5034 The Windows Firewall Driver has been stopped.

5035 The Windows Firewall Driver failed to start.

5037 The Windows Firewall Driver detected critical runtime error. Terminating.

5058 Key file operation.

5059 Key migration operation.

Subcategory: Security State Change
ID Message
4608 Windows is starting up.
4609 Windows is shutting down.
4616 The system time was changed.
4621 Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.

Subcategory: Security System Extension
ID Message
4610 An authentication package has been loaded by the Local Security Authority.
4611 A trusted logon process has been registered with the Local Security Authority.
4614 A notification package has been loaded by the Security Account Manager.
4622 A security package has been loaded by the Local Security Authority.
4697 A service was installed in the system.

Subcategory: System Integrity
ID Message
4612 Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
4615 Invalid use of LPC port.
4618 A monitored security event pattern has occurred.
4816 RPC detected an integrity violation while decrypting an incoming message.
5038 Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.
5056 A cryptographic self test was performed.
5057 A cryptographic primitive operation failed.
5060 Verification operation failed.
5061 Cryptographic operation.
5062 A kernel-mode cryptographic self test was performed.

7.2.1.4 Windows 2012 Security Events

Category	Subcategory	Event ID	Message Summary	Minimum Operating System Requirement
System	Security State Change	4608	Windows is starting up.	Windows Vista, Windows Server 2008
		4609	Windows is shutting down.	
	Security System Extension	4610	An authentication package has been loaded by the Local Security Authority.	
		4611	A trusted logon process has been registered with the Local Security Authority.	
	System Integrity	4612	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.	
	Security System Extension	4614	A notification package has been loaded by the Security Account Manager.	
	System Integrity	4615	Invalid use of LPC port.	
	Security State Change	4616	The system time was changed.	
	System Integrity	4618	A monitored security event pattern has occurred.	
	Security State Change	4621	Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.	
	Security System Extension	4622	A security package has been loaded by the Local Security Authority.	

Logon/Logoff	Logon	4624	An account was successfully logged on.	
		4625	An account failed to log on.	
		4626	User/Device claims information.	Windows 8, Windows Server 2012
	Group Membership	4627	Group membership information.	Windows 10
	Logoff	4634	An account was logged off.	Windows Vista, Windows Server 2008
	IPsec Main Mode	4646	%1	
	Logoff	4647	User initiated logoff.	
	Logon	4648	A logon was attempted using explicit credentials.	
	Other Logon/Logoff Events	4649	A replay attack was detected.	
	IPsec Main Mode	4650	An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used.	
		4651	An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.	
		4652	An IPsec Main Mode negotiation failed.	
		4653	An IPsec Main Mode negotiation failed.	
	IPsec Quick Mode	4654	An IPsec Quick Mode negotiation failed.	
	IPsec Main Mode	4655	An IPsec Main Mode security association ended.	
Object Access	Handle Manipulation	4656	A handle to an object was requested.	
	Registry	4657	A registry value was modified.	
	Handle Manipulation	4658	The handle to an object was closed.	
	SAM	4659	A handle to an object was requested with intent to delete.	
	Kernel	4659	A handle to an object was requested with intent to delete.	
	SAM	4660	An object was deleted.	
	Kernel	4660	An object was deleted.	
	SAM	4661	A handle to an object was requested.	
	Kernel	4661	A handle to an object was requested.	
DS Access	Directory Service Access	4662	An operation was performed on an object.	
Object Access	SAM	4663	An attempt was made to access an object.	
	Kernel	4663	An attempt was made to access an object.	
	File System	4664	An attempt was made to create a hard link.	
	Application Generated	4665	An attempt was made to create an application client context.	
		4666	An application attempted an operation:	
		4667	An application client context was deleted.	
		4668	An application was initialized.	
Policy Change	Subcategory (special)	4670	Permissions on an object were changed.	
Object Access	Other Object Access Events	4671	An application attempted to access a blocked ordinal through the TBS.	
Privilege Use	Sensitive Privilege Use / Non Sensitive Privilege Use	4672	Special privileges assigned to new logon.	
		4673	A privileged service was called.	
		4674	An operation was attempted on a privileged object.	
Logon/Logoff	Logon	4675	SIDs were filtered.	
Detailed Tracking	Process Creation	4688	A new process has been created.	
	Process Termination	4689	A process has exited.	
Object Access	Handle Manipulation	4690	An attempt was made to duplicate a handle to an object.	

	Other Object Access Events	4691	Indirect access to an object was requested.	
Detailed Tracking	DPAPI Activity	4692	Backup of data protection master key was attempted.	
		4693	Recovery of data protection master key was attempted.	
		4694	Protection of auditable protected data was attempted.	
		4695	Unprotection of auditable protected data was attempted.	
	Process Creation	4696	A primary token was assigned to process.	
System	Security System Extension	4697	A service was installed in the system.	
Object Access	Other Object Access Events	4698	A scheduled task was created.	
		4699	A scheduled task was deleted.	
		4700	A scheduled task was enabled.	
		4701	A scheduled task was disabled.	
		4702	A scheduled task was updated.	
Policy Change	Authorization Policy Change	4703	A user right was adjusted.	Windows 10
		4704	A user right was assigned.	Windows Vista, Windows Server 2008
		4705	A user right was removed.	
		4706	A new trust was created to a domain.	
		4707	A trust to a domain was removed.	
	Filtering Platform Policy Change	4709	IPsec Services was started.	
		4710	IPsec Services was disabled.	
		4711	May contain any one of the following: PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer. PAStore Engine applied Active Directory storage IPsec policy on the computer. PAStore Engine applied local registry storage IPsec policy on the computer. PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer. PAStore Engine failed to apply Active Directory storage IPsec policy on the computer. PAStore Engine failed to apply local registry storage IPsec policy on the computer. PAStore Engine failed to apply some rules of the active IPsec policy on the computer. PAStore Engine failed to load directory storage IPsec policy on the computer. PAStore Engine loaded directory storage IPsec policy on the computer. PAStore Engine failed to load local storage IPsec policy on the computer. PAStore Engine loaded local storage IPsec policy on the computer. PAStore Engine polled for changes to the active IPsec policy and detected no changes.	
	Filtering Platform Policy Change	4712	IPsec Services encountered a potentially serious failure.	
	Authentication Policy Change	4713	Kerberos policy was changed.	
	Authorization Policy Change	4714	Encrypted data recovery policy was changed.	
	Audit Policy Change	4715	The audit policy (SACL) on an object was changed.	
	Authentication Policy Change	4716	Trusted domain information was modified.	
		4717	System security access was granted to an account.	
		4718	System security access was removed from an account.	
	Audit Policy Change	4719	System audit policy was changed.	

Account Management	User Account Management	4720	A user account was created.	
		4722	A user account was enabled.	
		4723	An attempt was made to change an account's password.	
		4724	An attempt was made to reset an account's password.	
		4725	A user account was disabled.	
		4726	A user account was deleted.	
	Security Group Management	4727	A security-enabled global group was created.	
		4728	A member was added to a security-enabled global group.	
		4729	A member was removed from a security-enabled global group.	
		4730	A security-enabled global group was deleted.	
		4731	A security-enabled local group was created.	
		4732	A member was added to a security-enabled local group.	
		4733	A member was removed from a security-enabled local group.	
		4734	A security-enabled local group was deleted.	
		4735	A security-enabled local group was changed.	
		4737	A security-enabled global group was changed.	
	User Account Management	4738	A user account was changed.	
Policy Change	Authentication Policy Change	4739	Domain Policy was changed.	
Account Management	User Account Management	4740	A user account was locked out.	
	Computer Account Management	4742	A computer account was changed.	
		4743	A computer account was deleted.	
	Distribution Group Management	4744	A security-disabled local group was created.	
		4745	A security-disabled local group was changed.	
		4746	A member was added to a security-disabled local group.	
		4747	A member was removed from a security-disabled local group.	
		4748	A security-disabled local group was deleted.	
		4749	A security-disabled global group was created.	
		4750	A security-disabled global group was changed.	
		4751	A member was added to a security-disabled global group.	
		4752	A member was removed from a security-disabled global group.	
		4753	A security-disabled global group was deleted.	
	Security Group Management	4754	A security-enabled universal group was created.	
		4755	A security-enabled universal group was changed.	
		4756	A member was added to a security-enabled universal group.	
		4757	A member was removed from a security-enabled universal group.	
		4758	A security-enabled universal group was deleted.	
	Distribution Group Management	4759	A security-disabled universal group was created.	
		4760	A security-disabled universal group was changed.	
		4761	A member was added to a security-disabled universal group.	
		4762	A member was removed from a security-disabled universal group.	
	Security Group Management	4764	A group's type was changed.	
	User Account Management	4765	SID History was added to an account.	
		4766	An attempt to add SID History to an account failed.	
		4767	A user account was unlocked.	
Account Logon	Kerberos Authentication Service	4768	A Kerberos authentication ticket (TGT) was requested.	
	Kerberos Service Ticket Operations	4769	A Kerberos service ticket was requested.	
		4770	A Kerberos service ticket was renewed.	
	Kerberos Authentication	4771	Kerberos pre-authentication failed.	

	Service	4772	A Kerberos authentication ticket request failed.	
		4773	A Kerberos service ticket request failed.	
	Credential Validation	4774	An account w as mapped for logon.	
		4775	An account could not be mapped for logon.	
		4776	The domain controller attempted to validate the credentials for an account.	
		4777	The domain controller failed to validate the credentials for an account.	
Logon/Logoff	Other Logon/Logoff Events	4778	A session w as reconnected to a Window Station.	
		4779	A session w as disconnected from a Window Station.	
Account Management	User Account Management	4780	The ACL w as set on accounts w hich are members of administrators groups.	
		4781	The name of an account w as changed:	
	Other Account Management Events	4782	The passw ord hash an account w as accessed.	
	Application Group Management	4783	A basic application group w as created.	
		4784	A basic application group w as changed.	
		4785	A member w as added to a basic application group.	
		4786	A member w as removed from a basic application group.	
		4787	A non-member w as added to a basic application group.	
		4788	A non-member w as removed from a basic application group.	
		4789	A basic application group w as deleted.	
		4790	An LDAP query group w as created.	
		4791	A basic application group w as changed.	
		4792	An LDAP query group w as deleted.	
	Other Account Management Events	4793	The Passw ord Policy Checking API w as called.	
	User Account Management	4794	An attempt w as made to set the Directory Services Restore Mode.	
		4797	An attempt w as made to query the existence of a blank passw ord for an account.	Window s 8, Window s Server 2012
	Security Group Management	4798	A user's local group membership w as enumerated.	Window s 10
		4799	A security-enabled local group membership w as enumerated.	
Logon/Logoff	Other Logon/Logoff Events	4800	The w orkstation w as locked.	Window s Vista, Window s Server 2008
		4801	The w orkstation w as unlocked.	
		4802	The screen saver w as invoked.	
		4803	The screen saver w as dismissed.	
System	System Integrity	4816	RPC detected an integrity violation w hile decrypting an incoming message.	
Policy Change	Audit Policy Change	4817	Auditing settings on an object w ere changed.	Window s 7, Window s Server 2008 R2
Object Access	Central Access Policy Staging	4818	Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy	Window s 8, Window s Server 2012
Policy Change	Other Policy Change Events	4819	Central Access Policies on the machine have been changed.	
Account Logon	Kerberos Authentication Service	4820	A Kerberos Ticket-granting-ticket (TGT) w as denied because the device does not meet the access control restrictions.	
	Kerberos Service Ticket Operations	4821	A Kerberos service ticket w as denied because the user, device, or both does not meet the access control restrictions.	Window s 8.1, Window s Server 2012 R2
	Credential Validation	4822	NTLM authentication failed because the account w as a member of the Protected User group.	
		4823	NTLM authentication failed because access control restrictions are required.	

	Kerberos Authentication Service	4824	Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group.	
Logon/Logoff	Other Logon/Logoff Events	4825	A user was denied the access to Remote Desktop.	Windows Vista SP2, Windows Server 2008 SP2
Policy Change	Other Policy Change Events	4826	Boot Configuration Data loaded.	Windows 10
	Authentication Policy Change	4864	A namespace collision was detected.	Windows Vista, Windows Server 2008
		4865	A trusted forest information entry was added.	
		4866	A trusted forest information entry was removed.	
		4867	A trusted forest information entry was modified.	
Object Access	Certification Services	4868	The certificate manager denied a pending certificate request.	
		4869	Certificate Services received a resubmitted certificate request.	
		4870	Certificate Services revoked a certificate.	
		4871	Certificate Services received a request to publish the certificate revocation list (CRL).	
		4872	Certificate Services published the certificate revocation list (CRL).	
		4873	A certificate request extension changed.	
		4874	One or more certificate request attributes changed.	
		4875	Certificate Services received a request to shut down.	
		4876	Certificate Services backup started.	
		4877	Certificate Services backup completed.	
		4878	Certificate Services restore started.	
		4879	Certificate Services restore completed.	
		4880	Certificate Services started.	
		4881	Certificate Services stopped.	
		4882	The security permissions for Certificate Services changed.	
		4883	Certificate Services retrieved an archived key.	
		4884	Certificate Services imported a certificate into its database.	
		4885	The audit filter for Certificate Services changed.	
		4886	Certificate Services received a certificate request.	
		4887	Certificate Services approved a certificate request and issued a certificate.	
		4888	Certificate Services denied a certificate request.	
		4889	Certificate Services set the status of a certificate request to pending.	
		4890	The certificate manager settings for Certificate Services changed.	
		4891	A configuration entry changed in Certificate Services.	
		4892	A property of Certificate Services changed.	
		4893	Certificate Services archived a key.	
		4894	Certificate Services imported and archived a key.	
		4895	Certificate Services published the CA certificate to Active Directory Domain Services.	
		4896	One or more rows have been deleted from the certificate database.	
		4897	Role separation enabled:	
		4898	Certificate Services loaded a template.	
		4899	A Certificate Services template was updated.	
		4900	Certificate Services template security was updated.	
Policy Change	Audit Policy Change	4902	The Per-user audit policy table was created.	
		4904	An attempt was made to register a security event source.	
		4905	An attempt was made to unregister a security event source.	
		4906	The CrashOnAuditFail value has changed.	
		4907	Auditing settings on object were changed.	

		4908	Special Groups Logon table modified.	
	Other Policy Change Events	4909	The local policy settings for the TBS were changed.	
		4910	The group policy settings for the TBS were changed.	
	Authorization Policy Change	4911	Resource attributes of the object were changed.	Windows 8, Windows Server 2012
	Audit Policy Change	4912	Per User Audit Policy was changed.	Windows Vista, Windows Server 2008
	Authorization Policy Change	4913	Central Access Policy on the object was changed.	Windows 8, Windows Server 2012
DS Access	Detailed Directory Service Replication	4928	An Active Directory replica source naming context was established.	Windows Vista, Windows Server 2008
		4929	An Active Directory replica source naming context was removed.	
		4930	An Active Directory replica source naming context was modified.	
		4931	An Active Directory replica destination naming context was modified.	
	Directory Service Replication	4932	Synchronization of a replica of an Active Directory naming context has begun.	
		4933	Synchronization of a replica of an Active Directory naming context has ended.	
	Detailed Directory Service Replication	4934	Attributes of an Active Directory object were replicated.	
		4935	Replication failure begins.	
		4936	Replication failure ends.	
		4937	A lingering object was removed from a replica.	
Policy Change	MPSSVC Rule-Level Policy Change	4944	The following policy was active when the Windows Firewall started.	
		4945	A rule was listed when the Windows Firewall started.	
		4946	A change has been made to Windows Firewall exception list. A rule was added.	
		4947	A change has been made to Windows Firewall exception list. A rule was modified.	
		4948	A change has been made to Windows Firewall exception list. A rule was deleted.	
		4949	Windows Firewall settings were restored to the default values.	
		4950	A Windows Firewall setting has changed.	
		4951	A rule has been ignored because its major version number was not recognized by Windows Firewall.	
		4952	Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.	
		4953	A rule has been ignored by Windows Firewall because it could not parse the rule.	
		4954	Windows Firewall Group Policy settings have changed. The new settings have been applied.	
		4956	Windows Firewall has changed the active profile.	
		4957	Windows Firewall did not apply the following rule:	
		4958	Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer:	
System	IPsec Driver	4960	IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.	
		4961	IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.	

		4962	IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.	
		4963	IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.	
Logon/Logoff	Special Logon	4964	Special groups have been assigned to a new logon.	
System	IPsec Driver	4965	IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.	
Logon/Logoff	IPsec Main Mode	4976	During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.	
	IPsec Quick Mode	4977	During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.	
	IPsec Extended Mode	4978	During Extended Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.	
		4979	IPsec Main Mode and Extended Mode security associations were established.	
		4980	IPsec Main Mode and Extended Mode security associations were established.	
		4981	IPsec Main Mode and Extended Mode security associations were established.	
		4982	IPsec Main Mode and Extended Mode security associations were established.	
		4983	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.	
		4984	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.	
Object Access	File System	4985	The state of a transaction has changed.	
System	Other System Events	5024	The Windows Firewall Service has started successfully.	
		5025	The Windows Firewall Service has been stopped.	
		5027	The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.	
		5028	The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.	
		5029	The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.	
		5030	The Windows Firewall Service failed to start.	
Object Access	Filtering Platform Connection	5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.	
System	Other System Events	5032	Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.	
		5033	The Windows Firewall Driver has started successfully.	
		5034	The Windows Firewall Driver has been stopped.	
		5035	The Windows Firewall Driver failed to start.	

		5037	The Windows Firewall Driver detected critical runtime error. Terminating.	
	System Integrity	5038	Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.	
Object Access	Registry	5039	A registry key was virtualized.	
Policy Change	Filtering Platform Policy Change	5040	A change has been made to IPsec settings. An Authentication Set was added.	
		5041	A change has been made to IPsec settings. An Authentication Set was modified.	
		5042	A change has been made to IPsec settings. An Authentication Set was deleted.	
		5043	A change has been made to IPsec settings. A Connection Security Rule was added.	
		5044	A change has been made to IPsec settings. A Connection Security Rule was modified.	
		5045	A change has been made to IPsec settings. A Connection Security Rule was deleted.	
		5046	A change has been made to IPsec settings. A Crypto Set was added.	
		5047	A change has been made to IPsec settings. A Crypto Set was modified.	
		5048	A change has been made to IPsec settings. A Crypto Set was deleted.	
Logon/Logoff	IPsec Main Mode	5049	An IPsec Security Association was deleted.	
System	Other System Events	5050	An attempt to programmatically disable the Windows Firewall was rejected because this API is not supported on Windows Vista.	
Object Access	File System	5051	A file was virtualized.	
System	System Integrity	5056	A cryptographic self test was performed.	
		5057	A cryptographic primitive operation failed.	
	Other System Events	5058	Key file operation.	
		5059	Key migration operation.	
	System Integrity	5060	Verification operation failed.	
		5061	Cryptographic operation.	
		5062	A kernel-mode cryptographic self test was performed.	
Policy Change	Other Policy Change Events	5063	A cryptographic provider operation was attempted.	
		5064	A cryptographic context operation was attempted.	
		5065	A cryptographic context modification was attempted.	
		5066	A cryptographic function operation was attempted.	
		5067	A cryptographic function modification was attempted.	
		5068	A cryptographic function provider operation was attempted.	
		5069	A cryptographic function property operation was attempted.	
		5070	A cryptographic function property modification was attempted.	
System	Other System Events	5071	Key access denied by Microsoft key distribution service.	Windows 8, Windows Server 2012
Object Access	Certification Services	5120	OCSP Responder Service Started.	Windows Vista, Windows Server 2008
		5121	OCSP Responder Service Stopped.	
		5122	A Configuration entry changed in the OCSP Responder Service.	
		5123	A configuration entry changed in the OCSP Responder Service.	
		5124	A security setting was updated on OCSP Responder Service.	
		5125	A request was submitted to OCSP Responder Service.	
		5126	Signing Certificate was automatically updated by the OCSP Responder Service.	

		5127	The OCSP Revocation Provider successfully updated the revocation information.	
DS Access	Directory Service Changes	5136	A directory service object was modified.	
		5137	A directory service object was created.	
		5138	A directory service object was undeleted.	
		5139	A directory service object was moved.	
Object Access	File Share	5140	A network share object was accessed.	
DS Access	Directory Service Changes	5141	A directory service object was deleted.	Windows Vista SP1, Windows Server 2008
Object Access	File Share	5142	A network share object was added.	Windows 7, Windows Server 2008 R2
		5143	A network share object was modified.	
		5144	A network share object was deleted.	
	Detailed File Share	5145	A network share object was checked to see whether the client can be granted desired access.	
	Filtering Platform Packet Drop	5146	The Windows Filtering Platform has blocked a packet.	Windows 8, Windows Server 2012
		5147	A more restrictive Windows Filtering Platform filter has blocked a packet.	
	Other Object Access Events	5148	The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.	Windows 7, Windows Server 2008 R2
		5149	The DoS attack has subsided and normal processing is being resumed.	
	Filtering Platform Connection	5150	The Windows Filtering Platform has blocked a packet.	
		5151	A more restrictive Windows Filtering Platform filter has blocked a packet.	
	Filtering Platform Packet Drop	5152	The Windows Filtering Platform blocked a packet.	Windows Vista, Windows Server 2008
		5153	A more restrictive Windows Filtering Platform filter has blocked a packet.	
	Filtering Platform Connection	5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.	
		5155	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.	
		5156	The Windows Filtering Platform has allowed a connection.	
		5157	The Windows Filtering Platform has blocked a connection.	
		5158	The Windows Filtering Platform has permitted a bind to a local port.	
		5159	The Windows Filtering Platform has blocked a bind to a local port.	
	File Share	5168	Spn check for SMB/SMB2 failed.	Windows 7, Windows Server 2008 R2
DS Access	Directory Service Access	5169	A directory service object was modified.	Windows 10
Account Management	User Account Management	5376	Credential Manager credentials were backed up.	Windows Vista, Windows Server 2008
		5377	Credential Manager credentials were restored from a backup.	
Logon/Logoff	Other Logon/Logoff Events	5378	The requested credentials delegation was disallowed by policy.	
Policy Change	Filtering Platform Policy Change	5440	The following callout was present when the Windows Filtering Platform Base Filtering Engine started.	
		5441	The following filter was present when the Windows Filtering Platform Base Filtering Engine started.	
		5442	The following provider was present when the Windows Filtering Platform Base Filtering Engine started.	
		5443	The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.	

		5444	The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.	
		5446	A Windows Filtering Platform callout has been changed.	
	Other Policy Change Events	5447	A Windows Filtering Platform filter has been changed.	
	Filtering Platform Policy Change	5448	A Windows Filtering Platform provider has been changed.	
		5449	A Windows Filtering Platform provider context has been changed.	
		5450	A Windows Filtering Platform sub-layer has been changed.	
Logon/Logoff	IPsec Quick Mode	5451	An IPsec Quick Mode security association was established.	
		5452	An IPsec Quick Mode security association ended.	
	IPsec Main Mode	5453	An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.	
Policy Change	Filtering Platform Policy Change	5456	PAStore Engine applied Active Directory storage IPsec policy on the computer.	
		5457	PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.	
		5458	PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.	
		5459	PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.	
		5460	PAStore Engine applied local registry storage IPsec policy on the computer.	
		5461	PAStore Engine failed to apply local registry storage IPsec policy on the computer.	
		5462	PAStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem.	
		5463	PAStore Engine polled for changes to the active IPsec policy and detected no changes.	
		5464	PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services.	
		5465	PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully.	
		5466	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied.	
		5467	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used.	
		5468	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no longer being used.	
		5471	PAStore Engine loaded local storage IPsec policy on the computer.	
		5472	PAStore Engine failed to load local storage IPsec policy on the computer.	
		5473	PAStore Engine loaded directory storage IPsec policy on the computer.	
		5474	PAStore Engine failed to load directory storage IPsec policy on the computer.	
		5477	PAStore Engine failed to add quick mode filter.	
System	IPsec Driver	5478	IPsec Services has started successfully.	

		5479	IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.	
		5480	IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.	
		5483	IPsec Services failed to initialize RPC server. IPsec Services could not be started.	
		5484	IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.	
		5485	IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.	
Logon/Logoff	Other Logon/Logoff Events	5632	A request was made to authenticate to a wireless network.	
		5633	A request was made to authenticate to a wired network.	
Detailed Tracking	RPC Events	5712	A Remote Procedure Call (RPC) was attempted.	
Object Access	Other Object Access Events	5888	An object in the COM+ Catalog was modified.	
		5889	An object was deleted from the COM+ Catalog.	
		5890	An object was added to the COM+ Catalog.	
Policy Change	Other Policy Change Events	6144	Security policy in the group policy objects has been applied successfully.	
		6145	One or more errors occurred while processing security policy in the group policy objects.	
Logon/Logoff	Network Policy Server	6272	Network Policy Server granted access to a user.	Windows Vista SP1, Windows Server 2008
		6273	Network Policy Server denied access to a user.	
		6274	Network Policy Server discarded the request for a user.	
		6275	Network Policy Server discarded the accounting request for a user.	
		6276	Network Policy Server quarantined a user.	
		6277	Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.	
		6278	Network Policy Server granted full access to a user because the host met the defined health policy.	
		6279	Network Policy Server locked the user account due to repeated failed authentication attempts.	
		6280	Network Policy Server unlocked the user account.	
System	System Integrity	6281	Code Integrity determined that the page hashes of an image file are not valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error	Windows 7, Windows Server 2008 R2
	Other System Events	6400	BranchCache: Received an incorrectly formatted response while discovering availability of content.	
		6401	BranchCache: Received invalid data from a peer. Data discarded.	
		6402	BranchCache: The message to the hosted cache offering it data is incorrectly formatted.	
		6403	BranchCache: The hosted cache sent an incorrectly formatted response to the client.	

		6404	BranchCache: Hosted cache could not be authenticated using the provisioned SSL certificate.	
		6405	BranchCache: %2 instance(s) of event id %1 occurred.	
		6406	%1 registered to Windows Firewall to control filtering for the following: %2	
		6407	1%	
		6408	Registered product %1 failed and Windows Firewall is now controlling the filtering for %2	
		6409	BranchCache: A service connection point object could not be parsed.	Windows 8.1, Windows Server 2012 R2
	System Integrity	6410	Code integrity determined that a file does not meet the security requirements to load into a process.	
	Plug and Play Events	6416	A new external device was recognized by the System	Windows 10
	System Integrity	6417	The FIPS mode crypto selftests succeeded.	Windows 10 [Version 1511]
		6418	The FIPS mode crypto selftests failed.	
	Plug and Play Events	6419	A request was made to disable a device	
		6420	A device was disabled.	
		6421	A request was made to enable a device.	
		6422	A device was enabled.	
		6423	The installation of this device is forbidden by system policy	
		6424	The installation of this device was allowed, after having previously been forbidden by policy.	

7.2.2 Common Events

The following chapters list common event records that we collected from live systems in the field. It lists events from various types, both informational and critical. This list is neither complete nor to be used as a reference but instead can be used to get an idea of what types of events are logged to event logs.

Please send "interesting" events to support@netikus.net so that they can be included in this list, thank you.

1. Active Directory / DNS / WINS
2. System Events
3. Security
4. IIS / MSSQL / Exchange
5. Application Management
6. Hardware

7.2.2.1 Active Directory / DNS / WINS

These events are logged by Active Directory / DNS / WINS and indicate status information, errors or problems with the DNS or Active Directory.

Event Log	ID	Type	Source	Category	Message
DNS Server	4001	Error	DNS		The DNS server was unable to open zone *yzone.mydomain.com* in the Active Directory. This DNS Server is configured to obtain and use information from the directory for this zone and is unable to load the zone without it. Check that the Active Directory is functioning properly and reload the zone. The event data is the error code.
DNS Server	9999	Warning	DNS		The DNS server has encountered numerous run-time events. These are usually caused by the reception of bad or unexpected packets, or from problems with or excessive replication traffic. The data is the number of suppressed events encountered in the last 15 minute interval.
DNS Server	5504	Warning	DNS		The DNS server encountered an invalid domain name in a packet from *12.23.34.23* . The packet is rejected.
Application	100	Information	ESE	General	Information Store (*2256*) *00.6249.0000* started.
Application	300	Information	ESENT	Logging/Recovery	wins (*1672*) The database engine is initiating recovery steps.
Application	302	Information	ESENT	Logging/Recovery	wins (*1672*) The database engine has successfully completed recovery steps.

Strings in italic may vary depending on what triggered the event

7.2.2.2 System Events

These events are logged by the Operating System and mostly indicate errors or problems with the system. Please note that even critical messages might just be logged as **Information** events.

Event Log	ID	Type	Source	Category	Message
System	16	Warning	Automatic Updates	Download	Unable to connect: Windows is unable to connect to the Automatic Updates service and therefore cannot download and install updates according to the set schedule. Windows will continue to try to establish a connection.
System	6005	Information	EventLog		The Event Log service was started.
System	6006	Information	EventLog		The Event Log service was stopped.
System	6009	Error	EventLog		The previous system shutdown at *6:32:01 AM* on *1/1/2004* was unexpected.
System	6009	Information	EventLog		Microsoft (R) Windows 2000 (R) 5.0 2195 Service Pack *4 Uniprocessor* Free.
System	1073	Warning	USER32		The attempt to reboot *WORKSTATION73* failed.
System	29223	Information	LSASRV		This server is now a Domain Controller.
System	40960	Warning	LSASRV	SPNEGO (Negotiator)	The Security System detected an authentication error for the server LDAP/*myserver1.mydomain.com@mydomain.com*. The failure code from authentication protocol Kerberos was "The attempted login is invalid. This is either due to a bad username or authentication information.".
System	40961	Warning	LSASRV	SPNEGO (Negotiator)	The Security System could not establish a secured connection with the server LDAP/*myserver1.mydomain.com@mydomain.com*. No authentication protocol was available.
System	3034	Warning	MRxSmb		The redirector was unable to initialize security context or query context attributes.
System	3019	Warning	MRxSmb		The redirector failed to determine the connection type.

System	2511	Error	Server		The server service was unable to recreate the share *myshare* because the directory *c:\mydata* no longer exists.
System	2506	Error	Server		The value named IRPStackSize in the server's Registry key LanmanServer\Parameters was invalid. The value was ignored, and processing continued.
System	2012	Error	Srv		The server has encountered a network error.
System	16650	Error	SAM		The account-identifier allocator failed to initialize properly. The recod data contains the NT error code that caused the failure.

				Windows 2000 will retry the initialization until it succeeds; until that time, account creating will be denied on this Domain Controller. Please look for other SAM event logs that may indicate the exact reason for the failure.
System	64	Warning	w32time	Because of repeated network problems, the time service has not been able to find a domain controller to synchronize with for a long time. To reduce network traffic, the time service will wait 960 minutes before trying again. No synchronization will take place during this interval, even if network connectivity is restored. Accumulated time errors may cause certain network operations to fail. To tell the time service that network connectivity has been restored and that it should resynchronize, execute "w32tm /s" from the command line.
System	54	Warning	w32time	The Windows Time Service was not able to find a Domain Controller. A time and date update was not possible.
System	24	Warning	w32time	Time Provider NtpClient: No valid response has been received from domain controller *mydc.mydomain.com* after 8 attempts to contact it. This domain controller will be discarded as a time source and NtpClient will attempt to discover a new domain controller from which to synchronize.
System	20050	Error	RemoteAccess	The user *DOMAIN\Ingmar* connected to port *VPN2-120* has been disconnected because no network protocols were successfully negotiatated.
System	20189	Warning	RemoteAccess	The user *Intruder* connected from *12.23.34.55* but failed an authentication attempt due to the following reason (*112*).
System	1001	Information	Save Dump	The computer has rebooted from a bugcheck. The bugcheck was *0x000000d1 (0x00000002 0x00000009 0x00000000 0xf1c21934*). Microsoft Windows 2000 [v15.2195]. A dump was saved in *C:\WINNT\MEMORY.DMP*.
System	1003	Warning	Dhcp	Your computer was not able to renew its address from the network (from the DHCP Server) for the Network Card with network address 00053C08910F. The following error occurred: *The operation was canceled by the user. Your computer will continue to try and obtain an address on its own from the network address (DHCP) server.*

Strings in italic may vary depending on what triggered the event

7.2.2.3 Security

These events are logged by the security sub-system of Windows. For a complete list of possible events see "Windows 2000 Security Event Descriptions".

Event Log	ID	Type	Source	Category	Message
Security	596	Audit Failure	Security	Detailed Tracking	Backup of data protection master key. Key Identifier: 38b2f717-214b-4c2a-00e0-0ee945fa4616 Recovery Server: Recovery Key ID: Failure Reason: 0x32
Security	615	Audit Failure	Security	Policy Change	IPSec Services: IPSec Services failed to get the complete list of network interfaces on the machine. This can be a potential security hazard to the machine since some of the network interfaces may not get the protection as desired by the applied IPSec filters. Please run IPSec monitor snap-in to further diagnose the problem.
Security	612	Audit Success	Security	Policy Change	Audit Policy Change: New Policy: Success Failure + + Logon/Logoff + + Object Access - + Privilege Use + + Account Management + + Policy Change + + System - + Detailed Tracking + + Directory Service Access + + Account Logon Changed By: User Name *SHEEP* $ Domain Name *NETIKUS* Logon ID: (0x0,0x3E7)
Security	627	Audit Failure	Security	Account Management	Change Password Attempt: Target Account Name: Administrator Target Domain: SHEEP Target Account ID: SHEEP\Administrator Caller User Name: SHEEP$ Caller Domain: NETIKUS Caller Logon ID: (0x0,0x3E7) Privileges: -

Strings in italic may vary depending on what triggered the event

7.2.2.4 IIS / MSSQL / Exchange

These events are logged by IIS, Exchange Server and MSSQL server. Most Microsoft server applications (Backoffice) log extensive information to the event log and can thus be monitored very nicely with EventSentry.

Event Log	ID	Type	Source	Category	Message
Application	2219	Warning	MSExchange MTA	Field Engineering	The MTA is running recovery on the internal message database because the MTA was not shut down cleanly. This operation may take some time. Status updates will be written to the Windows 2000 Event Log. [DB Server MAIN BASE 1 0 14 ( )
Application	5	Error	MSExchange ES	General	An unexpected MAPI error occurred. Error returned was 0x [800401548]
Application	12002	Error	MSExchange IS	Content Engine	Error 8004011B-82000387 occurred while processing message <> from somebody@aol.com '
Application	1025	Warning	MSExchange IS Mailbox Store	General	An error occurred on database "First Storage Group\Mailbox Store (SERVER1)". Function name or description of problem: Restrict/SetSearchCriteria Error: -1102 Warning: fail to apply search optimization to folder (FID 1-3619001) Retrying without optimization.
System	2	Information	IISCTLS		IIS stop command received from user DOMAIN\User . The logged data is the status code.
System	4	Information	IISCTLS		IIS kill command received from user DOMAIN\User . The logged data is the status code.
System	105	Error	W3SVC		The server was unable to register the administration tool discovery information. The administration tool may not be able to see this server. The data is the error code.
System	100	Warning	W3SVC		The server was unable to logon the Windows NT account 'myaccount' due to the following error: Logon failure: unknown user name or bad password. The data is the error code.
Application	1051	Error	IMAP4SVC	General	Unexpected error condition: call to function EncryptCtx::CheckServerCert() resulted in error code 800cc000 .
System	50	Error	TermDD		The RDP protocol component X.224 detected an error in the protocol stream and has disconnected the client.
System	36871	Error	Schannel		A fatal error occurred while creating an SSL server credential.
System	36872	Warning	Schannel		No suitable default server credential exists on this system. This will prevent server applications that expect to make use of the system default credentials from accepting SSL connections. An example of such an application is the diretory server. Applications that manage their own credentials, such as the internet information server, are not affected by this.

System	36874	Error	Schannel		An SSL connection request was received from a remote client application, but none of the ciper suites supported by the client application are supported by the server. Ths SSL connection request has failed.
Application	17052	Information	MSSQL*Inst* *nce*		Error: 154557, Severity: 0, State: 1 Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
Application	17055	Information	MSSQL*Inst* *nce*		19013: SQL server listening on *TCP, Shared Memory,* *amed Pipes* .
Application	17055	Information	MSSQL*Inst* *nce*		17126: SQL Server is ready for client connections
Application	17055	Information	MSSQL*Inst* *nce*		19013: SQL Server listening on *34.234.34.32 3431*
Application	208	Information	SQLSERVERAGENT		SQL Server Scheduled Job *EventSentry Database* *urge* ' (0x3DF88F31AB6B4C4F8FD0574F29FF3B48) - Status: Succeeded - Invoked on: 2004-06-22 11:30:00 - Message: The job succeeded. The Job was invoked by Schedule *2 (Default*). The last step to run was step *1 (Delete records older than 90 days*).

Strings in italic may vary depending on what triggered the event

7.2.2.5 Application Management

These events concern services and applications.

Event Log	ID	Type	Source	Message
System	26	Information	Application Popup	Application Popup: Service Control Manager : At least one service or driver failed during system startup. Use Event Viewer to examine the event log for details.
System	26	Information	Application Popup	Application popup: *somefile.exe* - Application Error : The instruction at "*0x00000000* " referenced memory at "*0x00000000* ". The memory could not be *read* ". Click on OK to terminate the program
System	7000	Error	Service Control Manager	The *Simple Mail Transport Protocal (SMTP)* service failed to start due to the following error: *The system cannot find the file specified* .
System	7031	Error	Service Control Manager	The *Simple Mail Transport Protocol (SMTP)* service terminated unexpectedly. It has done this *1* time(s). The following corrective action will be taken in *0* milliseconds: *No action* .
System	4381	Information	NTServicePack	Windows *2000* Service Pack *4* was installed.
System	4377	Information	NTServicePack	Windows *2000* Hotfix *KB25119* was installed.
Security	592	Audit Success	Detailed Tracking	A new process has been created: New Process ID: 724 Image File Name: *C:\Program Files\EventSentry\eventsentry_gui.exe* Creator Process ID: 1044 User Name: *Administrator* Domain: *GOAT* Logon ID: (0x0,0xB6A9)
Security	593	Audit Success	Detailed Tracking	A process has exited: Process ID: 724 User Name: *GOAT$* Domain: *NETIKUS* Logon ID: (0x0,0x3E7)

Strings in italic may vary depending on what triggered the event

7.2.2.6 Hardware

These events are logged by hardware drivers, such as SCSI controllers, network card drivers etc. An event log entry is often the first indication that a hardware problem exists.

Event Log	ID	Type	Source	Message
System	4	Warning	b57w2k	Broadcom NetXtreme Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
Application	1001	Warning	DPTELOG	The DISK at (0,0,0,0) returned SCSI status: Check Condition at Sun May 23 16:38:56 2004.
Application	1002	Error	DPTELOG	Non-corrected ECC RAM error found for device (0, 0, 0, 0) at Fri Jun 04 14:14:32 2004. RAM address: 0x809F2800
Application	1027	Warning	UPS Event	UPS disconnect! Cannot retrieve information from the UPS.
System	1	Error	afasa	\Device\Afa0: SMART WARNING: ID (0:2:0) =FPT_EXCEEDED
System	11	Error	Disk	The driver detected a controller error on \Device\Harddisk0\Partition2

Strings in italic may vary depending on what triggered the event

7.3 Beispiele & Vorlagen

Eine umfassendere Liste von Konfigurationsbeispielen und Anweisungen finden Sie im Abschnitt How-To auf eventsentry.com.

7.3.1 Filter-Beispiele

Dieser Abschnitt listet Filterbeispiele auf:

Beispiel 1: Standard-Filter

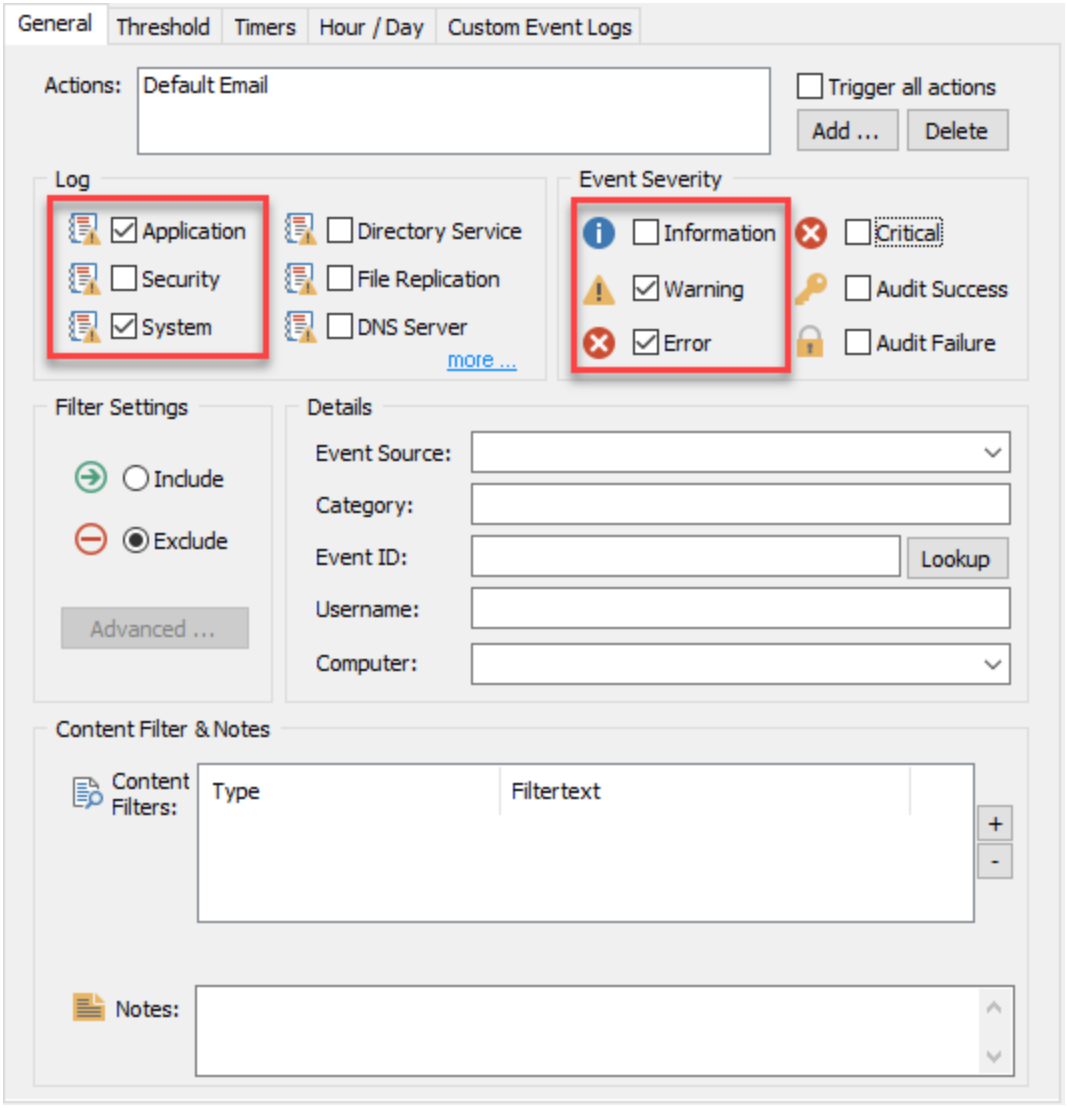
Beispiel 2: Filter für Ereignisquelle

Beispiel 3: Filter für Ereignisquelle und mehrere Ereignis-IDs

7.3.1.1 Beispiel 1: Standard-Filter

Dieser **Include** Filter überwacht das Anwendungs- und Systemereignisprotokoll auf WARNUNG- und FEHLER-Meldungen und benachrichtigt bei Übereinstimmung eine Aktion namens "Default Email".

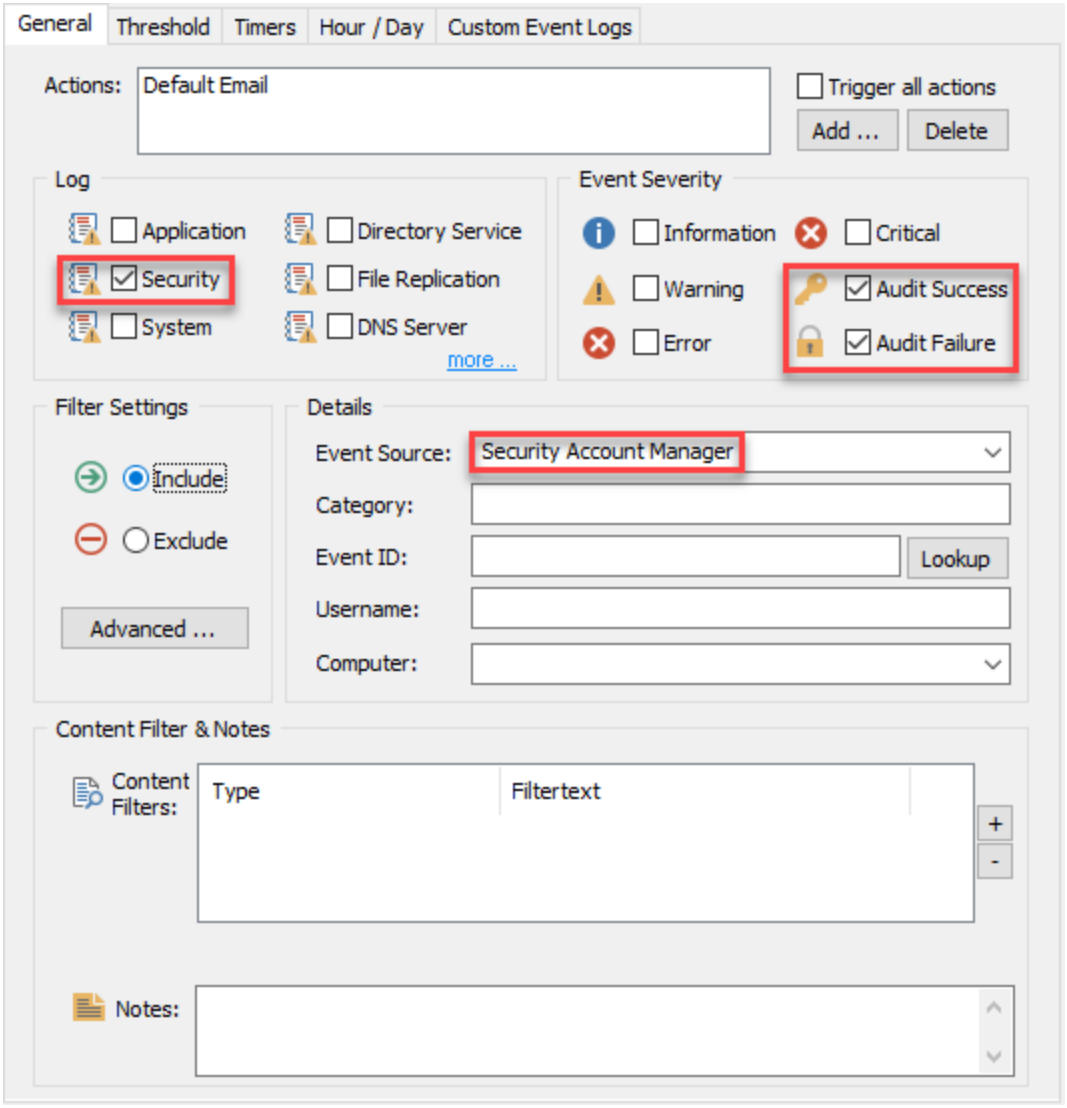
Da alle Felder im Abschnitt "**Details**" leer bleiben, wird jede Quelle, Kategorie, ID oder jeder Benutzername diesem Filter entsprechen.



7.3.1.2 Example 2: Event Source

Dieser **Include** Filter überwacht das Sicherheitsereignisprotokoll auf AUDIT-SUCCESS- und AUDIT-FAILURE-Meldungen und benachrichtigt bei Übereinstimmung ein Ziel namens "Default Email".

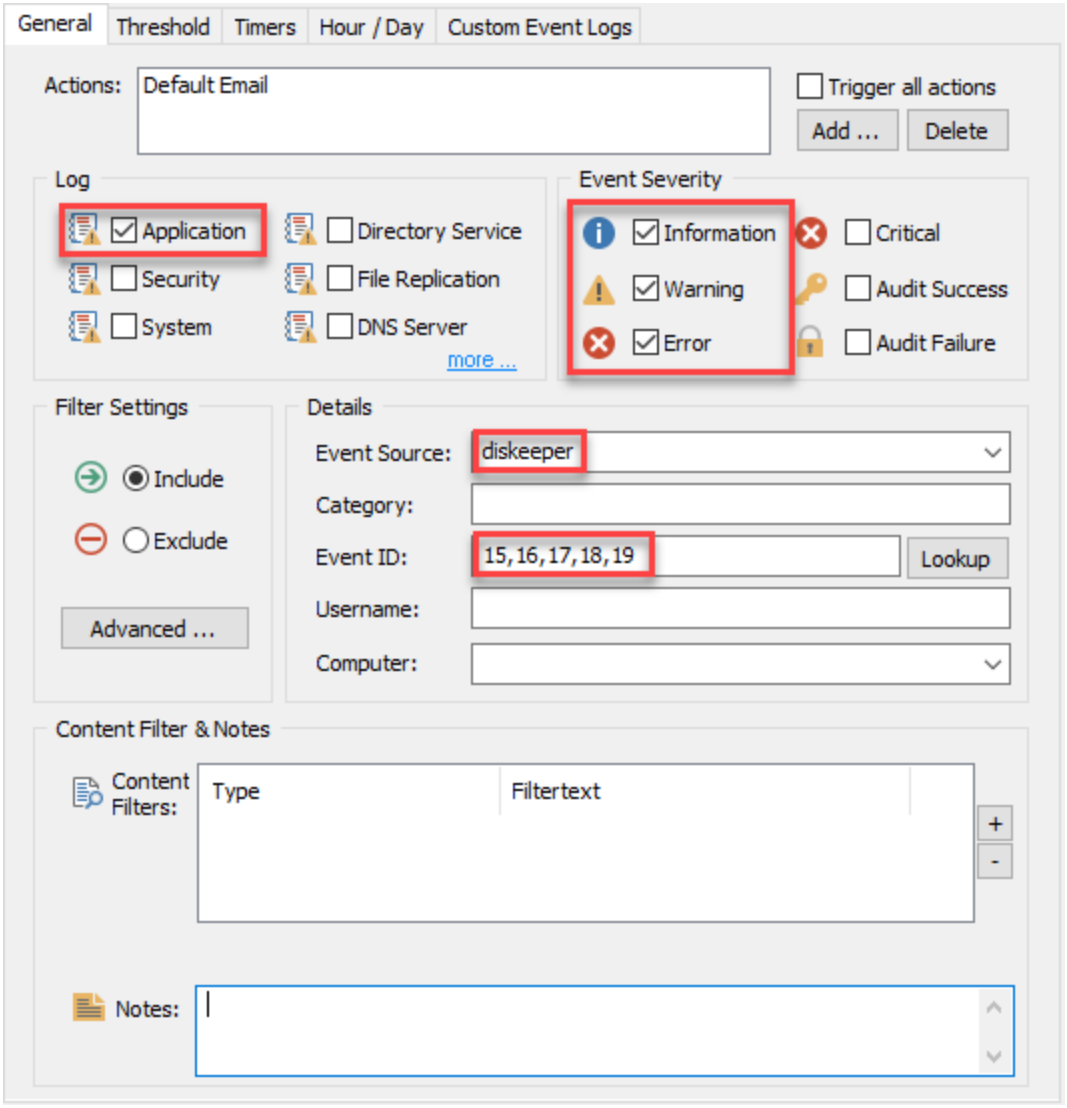
Nur Ereignisse aus der Quelle "Security Account Manager" werden von diesem Filter verarbeitet.



7.3.1.3 Beispiel 3: Ereignisquelle & Ereignis-ID

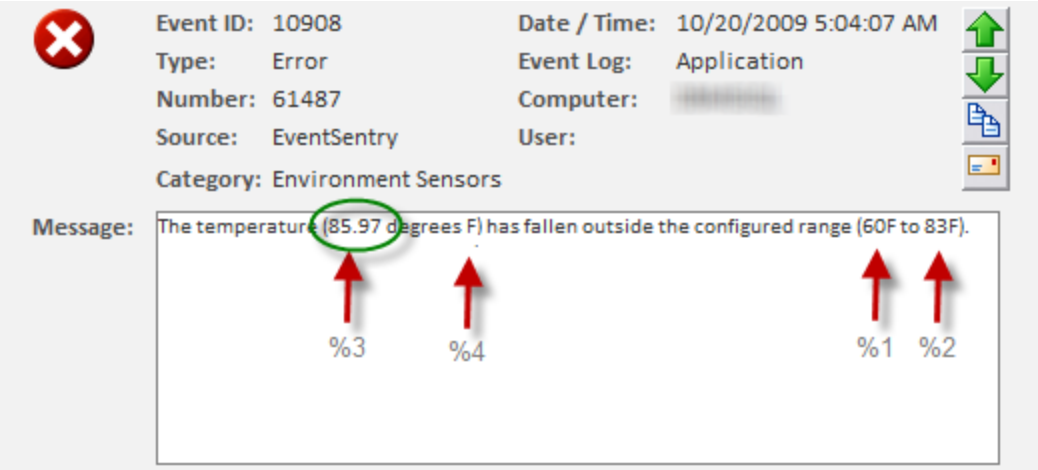
Dieser **Include** Filter überwacht das Ereignisprotokoll der Anwendung auf INFORMATIONEN, WARNUNGEN und FEHLERMELDUNGEN und benachrichtigt bei Übereinstimmung eine Aktion namens "Default Email".

Zusätzlich passen nur Ereignisse aus der Quelle "Diskeeper" mit den Ereignis-IDs 15,16,17,18 und 19 auf diesen Filter.



7.3.1.4 Beispiel 4: Inhaltsfilter mit Einfügungetext

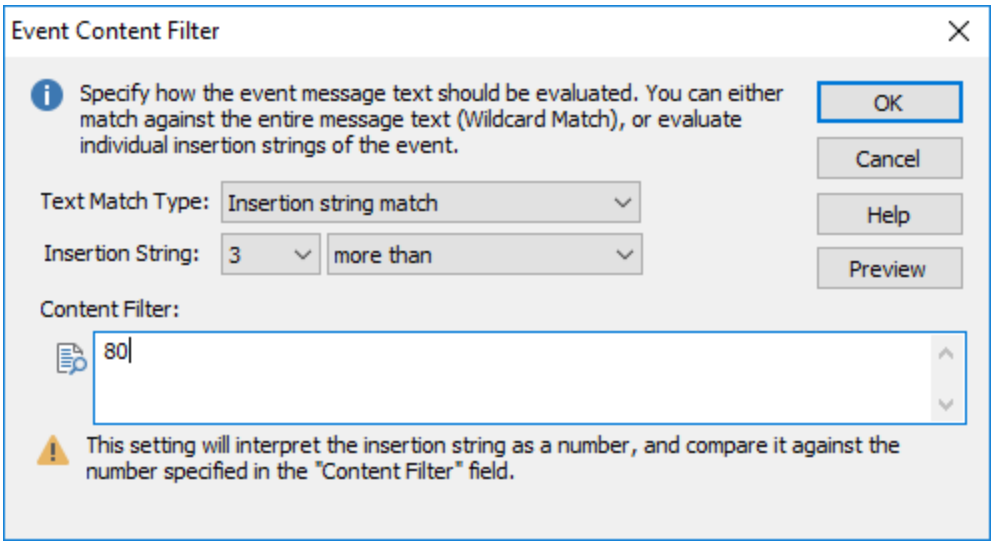
Der Zweck dieses Filters besteht darin, eine Aktion auszulösen, wenn der EventSentry Temperatursensor 80 Grad F überschreitet. Ein typisches Ereignis würde so aussehen:



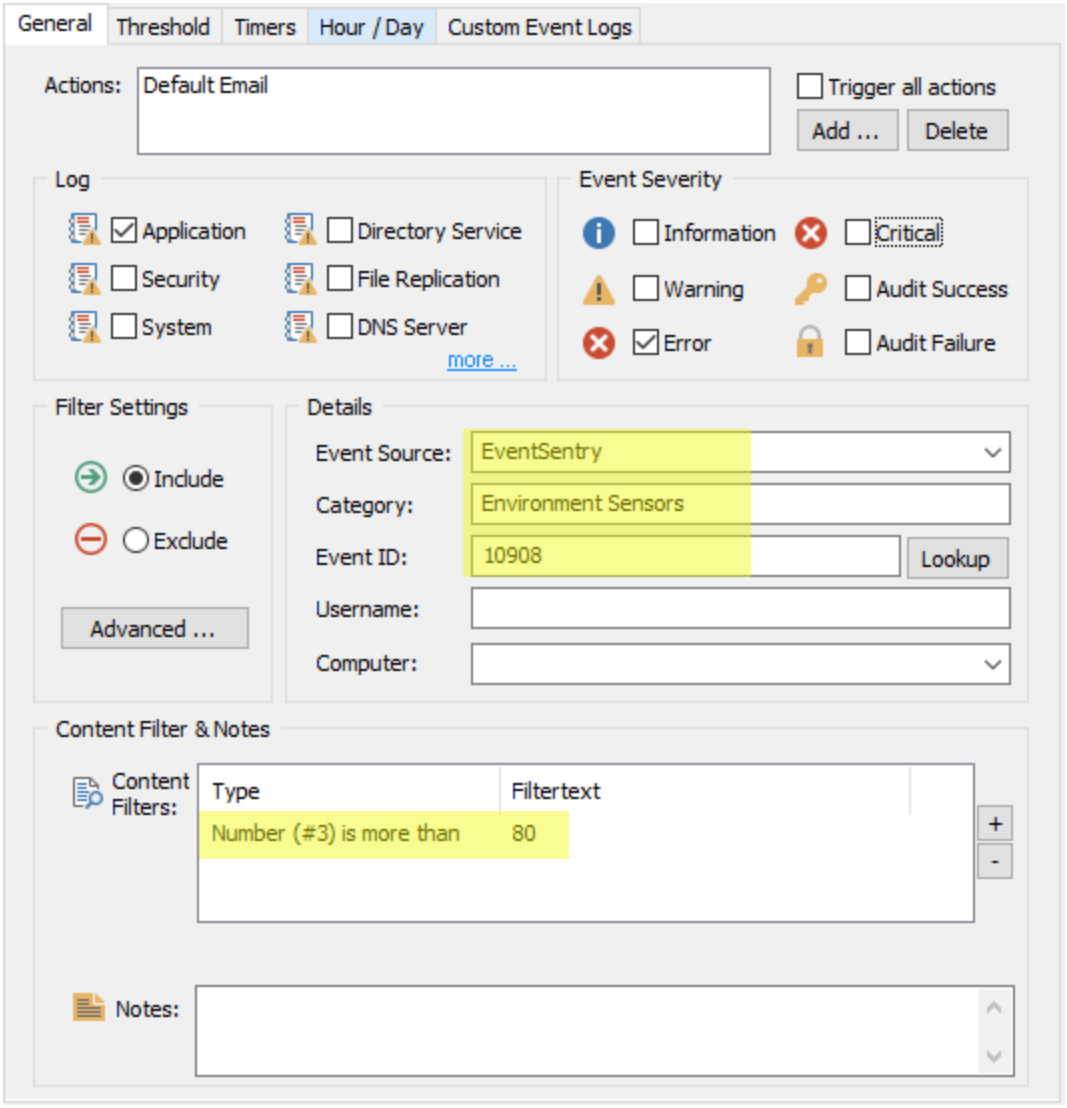
Betrachtet man das Ereignis 10908 mit dem Event Message Browser, so zeigt sich Folgendes:

```
The temperature (%3 degrees %4) has fallen outside the configured range (%
                                1%4 to %2%4).
```

Da der Einfügungetext #3 durch die Temperatur ersetzt wird, werden wir einen Inhaltsfilter erstellen, der den dritten Einfügungetext betrachtet.



Da es sich bei dem Einfügungetext #3 um eine Zahl handelt, können wir, wie oben gezeigt, den Vorteil des numerischen Vergleichs nutzen. Der Hauptfilterdialog sieht dann ähnlich aus wie dieser:



7.3.2 Beispiele für zusammenfassende Benachrichtigungen

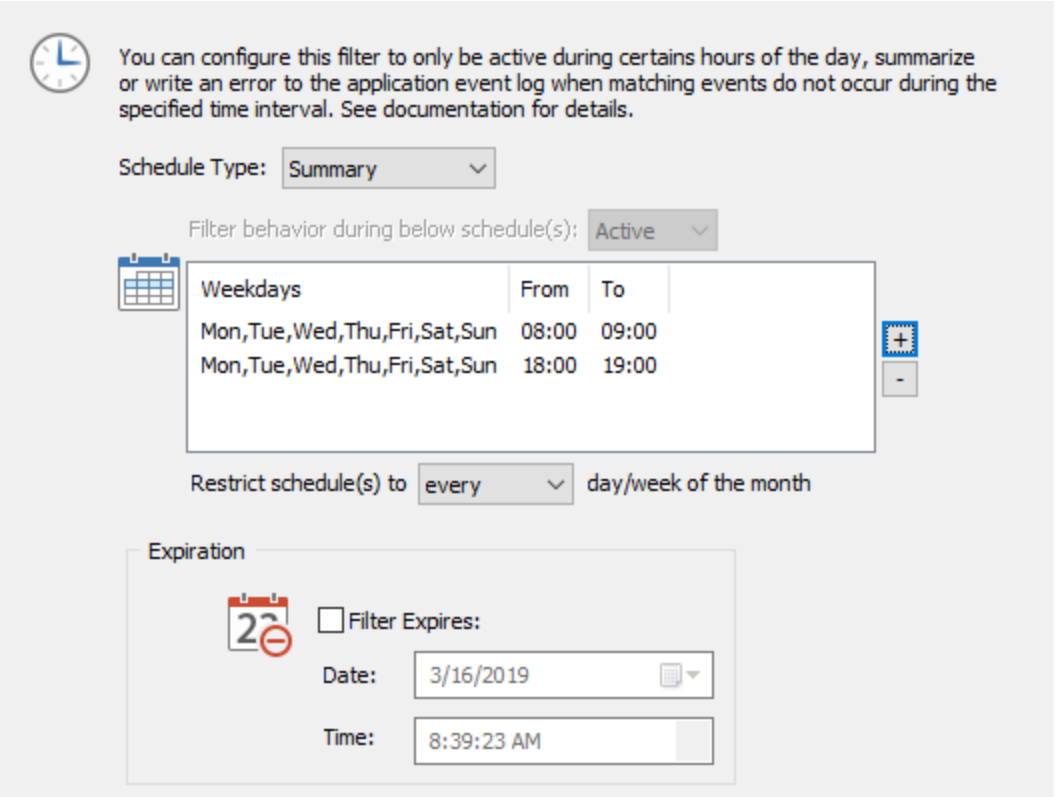
Dieser Abschnitt listet Beispiele für Zusammenfassende Benachrichtigungen auf:

Beispiel 1: Tägliche Zusammenfassung

Beispiel 2: Tägliche Zusammenfassung mit Nachrichten

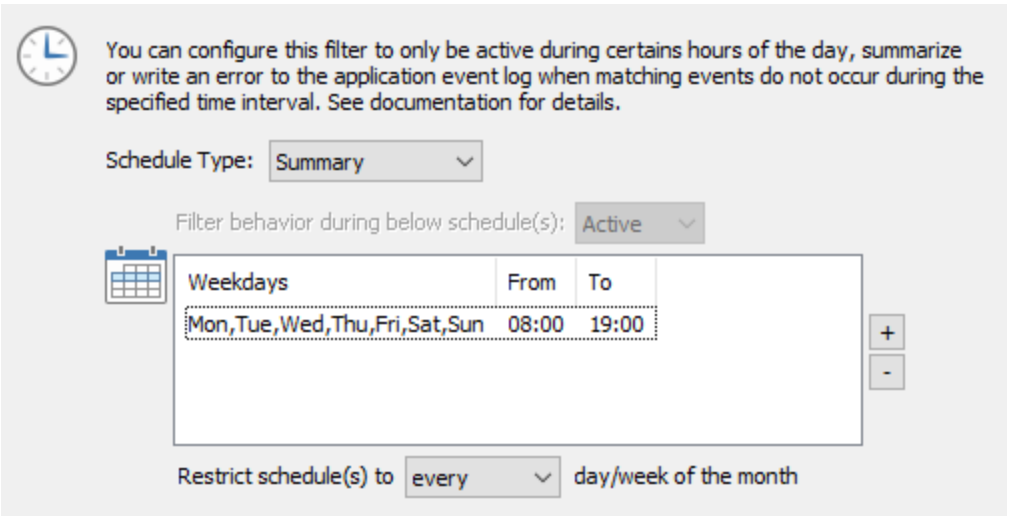
7.3.2.1 Beispiel 1: Tägliche Zusammenfassung

Dieser Benachrichtigungsfilter benachrichtigt die angegebene Aktion (nicht gezeigt) jeden Tag um **9 Uhr und 19 Uhr**. Bitte beachten Sie, dass die Benachrichtigungen immer am Ende der aktiven Stunde verschickt werden, in diesem Fall also **um 9 Uhr** und **19 Uhr**. Die um 9 Uhr morgens gesendete E-Mail enthält Ereignisse, die dem Filter entsprechen und zwischen 8 und 9 Uhr morgens aufgetreten sind; die um 19 Uhr gesendete E-Mail enthält Ereignisse, die zwischen 18 und 19 Uhr aufgetreten sind.



7.3.2.2 Beispiel 2: Tägliche Zusammenfassung mit Nachrichten

Dieser Beispiel-Benachrichtigungsfilter benachrichtigt die angegebene Aktion (nicht gezeigt) jeden Tag um **19 Uhr.** Die E-Mail enthält alle Ereignisse, die dem Filter entsprechen und zwischen 8 Uhr morgens und 19 Uhr abends auftreten.



7.4 Compliance

7.4.1 Matrix

The matrix below shows which compliance sections are covered by EventSentry (tracking) features.

Report Title

Feature: Path to the query page in the EventSentry web reports
Report: Name of the built-in report, if available and applicable. Reports are accessed through EVENT -> REPORTS

Active Directory Administrator Logons

Feature: Compliance -> Logon Tracking -> Console Logons
Report: Administrative Console Logons

PCI	10.1	10.2	10.3	10.5	10.6	10.7								
FISMA / NIST 800 53	AC-13	AU-2	AU-3	AU-6	AU-7	AU-9								
ISO17799	0.5	10.1.3	10.10.1	10.10.2	10.10.3	10.10.4	11.5.1	11.5.2	11.5.3	13.2.3	15.1.3	15.2.1	15.3.1	
Cobit	PO 4.11	PO 7.8	AI 2.3	AI 2.4	AI 4.2	DS 5.3	DS 5.4	DS 5.5	ME 2.3	ME 2.5	ME 3.4	ME 4.5		
HIPAA	164.306	164.308a	164.312a	164.312b	164.312d									

Active Directory General Object Changes

Feature: Event -> Event Search
Report: Active Directory General Object Changes

PCI	6.4	10.1	10.2	10.3	10.5	10.6	10.7							
FISMA / NIST 800 53	AC-13	AU-3	AU-6	AU-7										
ISO17799	0.5	10.1.2	10.1.3	10.10.1	10.10.2	10.10.3	10.10.4	11.1.1	12.5.1	13.2.1	13.2.3	15.1.3	15.2.1	15.3.1
Cobit	PO 4.11	AI 2.3	AI 2.4	AI 4.2	AI 6.4	AI 6.5	DS 5.5	ME 2.3	ME 2.5	ME 3.4	ME 4.5	ME 4.7		
HIPAA	164.306	164.308a	164.312a	164.312b										

Active Directory Group Member Additions

Feature: Compliance -> Account Changes -> Group Account
Report: Active Directory Security Group Changes

PCI	6.4	7.1	10.1	10.2	10.3	10.5	10.6	10.7						
FISMA / NIST 800 53	AC-2	AC-13	AU-2	AU-3	AU-6	AU-7	AU-9							
ISO17799	0.5	10.1.2	10.1.3	10.10.1	10.10.3	10.10.4	12.5.1	13.2.1	13.2.3	15.1.3	15.2.1	15.3.1		
Cobit	PO 4.11	PO 7.8	AI 2.3	AI 2.4	AI 4.2	AI 6.4	AI 6.5	DS 5.4	DS 5.5	ME 2.3	ME 3.4	ME 4.4	ME 4.5	ME 4.7

HIPAA	164.306	164.308a	164.310a	164.312b													

Active Directory Group Member Deletions

Feature: Compliance -> Account Changes -> Group Account
Report: Active Directory Security Group Changes

PCI	6.4	7.1	10.1	10.2	10.3	10.5	10.6	10.7									
FISMA / NIST 800 53	AC-2	AC-13	AU-2	AU-3	AU-6	AU-7	AU-9										
ISO17799	0.5	8.3.3	10.1.2	10.10.1	10.10.2	10.10.3	10.10.4	11.1.1	12.5.1	13.2.1	13.2.3	15.1.3	15.2.1	15.3.1			
Cobit	PO 4.11	PO 7.8	AI 2.3	AI 2.4	AI 4.2	AI 6.4	AI 6.5	DS 5.4	DS 5.5	ME 2.3	ME 2.5	ME 3.4	ME 4.4	ME 4.5	ME 4.7		
HIPAA	164.306	164.308a	164.310a	164.312b													

Active Directory New or Enabled Account

Feature: Compliance -> Account Changes -> User Account
Report: Active Directory User Changes

PCI	7.1	10.1	10.2	10.3	10.5	10.6	10.7										
FISMA / NIST 800 53	AC-2	AC-13	PS-6	AU-2	AU-3	AU-6	AU-7	AU-9									
ISO17799	0.5	10.1.2	10.10.1	10.10.3	10.10.4	12.5.1	15.1.3	15.2.1	15.3.1								
Cobit	PO 4.11	PO 7.8	AI 2.3	AI 2.4	AI 3.2	AI 4.2	DS 5.3	DS 5.4	DS 5.5	ME 2.5							
HIPAA	164.306	164.308a	164.310a	164.312b	164.312d												

Active Directory Users Deleted or Disabled

Feature: Compliance -> Account Changes -> User Account
Report: Active Directory User Changes

PCI	6.4	7.1	10.1	10.2	10.3	10.5	10.6	10.7									
FISMA / NIST 800 53	AC-2	AU-2	AU-3	AU-6	AU-7	AU-9											
ISO17799	0.5	8.3.3	10.1.2	10.10.1	10.10.2	10.10.3	10.10.4	11.1.1	12.5.1	13.2.1	13.2.3	15.1.3	15.2.1	15.3.1			
Cobit	PO 4.11	PO 4.14	PO 7.8	AI 2.4	AI 6.4	DS 5.4	DS 5.5	ME 2.5	ME 3.4	ME 4.7							
HIPAA	164.306	164.308a	164.310a	164.312b	164.312d	164.312e											

Active Directory Group Policy Change Report

Feature: Event -> Event Search
Report: Active Directory Group Policy Changes

PCI	6.4	10.1	10.2	10.3	10.5	10.6	10.7

FISMA / NIST 800 53	AC-3	AC-13	AU-2	AU-3	AU-6	AU-7	AU-9								
ISO17799	0.5	10.1.2	10.1.3	10.10.1	10.10.2	10.10.3	10.10.4	11.1.1	12.5.1	13.2.1	13.2.3	15.1.3	15.2.1	15.3.1	
Cobit	PO 4.11	AI 2.3	AI 2.4	AI 4.2	AI 6.4	AI 6.5	DS 5.5	ME 2.3	ME 2.5	ME 3.4	ME 4.5	ME 4.7			
HIPAA	164.306	164.308a	164.312a	164.312b											

Active Directory Permission Changes

Feature: Event -> Event Search
Report: Active Directory General Object Changes

PCI	6.4	10.1	10.2	10.3	10.5	10.6	10.7
FISMA / NIST 800 53	AC-3	AC-13	AU-2	AU-3	AU-6	AU-7	AU-9
ISO17799	0.5	10.1.2	10.1.3	10.10.1	10.10.2	10.10.3	10.10.4
Cobit	PO 4.11	AI 2.3	AI 4.2	AI 6.4	AI 6.5	DS 5.5	ME 2.5
HIPAA	164.306	164.308a	164.312a	164.312b	164.312d		

ISO17799	12.5.1	13.2.1	13.2.3	15.1.3	15.2.1	15.3.1									
Cobit	ME 3.4	ME 4.5	ME 4.7												

Active Directory User Account Lockouts and Password Resets

Feature: Compliance -> Account Changes -> User Account
Report: Active Directory User Changes

PCI	10.2	10.3	10.5	10.6	10.7		
FISMA / NIST 800 53	AC-2	AC-7	AU-2	AU-3	AU-6	AU-7	AU-9
ISO17799	0.5	10.1.3	10.10.1	10.10.2	10.10.3	10.10.4	11.5.1
Cobit	PO 4.11	AI 3.2	AI 4.2	DS 5.4	DS 5.5	ME 2.5	
HIPAA	164.306	164.308a	164.312a	164.312b	164.312e		

ISO17799	11.5.2	11.5.3	13.2.3	15.1.3	15.2.1	15.3.1									

Active Directory Domain Policy Changes

Feature: Compliance -> Policy Changes -> Domain Policy
Report: Active Directory Domain Policy Changes

PCI	10.1	10.2	10.3	10.5	10.6	10.7	
FISMA / NIST 800 53	AC-3	AC-13	AU-2	AU-3	AU-6	AU-7	AU-9
ISO17799	0.5	10.1.2	10.10.1	10.10.2	10.10.4	12.5.1	13.2.1
Cobit	PO 4.11	AI 2.3	AI 2.4	AI 4.2	AI 6.4	AI 6.5	DS 5.5
HIPAA	164.306	164.308a	164.312a	164.312b	164.312c	164.312d	164.312e

ISO17799	15.1.3	15.2.1	15.3.1												
Cobit	ME 2.3	ME 2.5	ME 3.4	ME 4.5	ME 4.7										

Local Group Member Additions Report

Feature: Compliance -> Account Changes -> Group Account
Report: Member Server Security Group Changes

PCI	6.4	7.1	10.1	10.2	10.3	10.5	10.6	10.7
FISMA / NIST 800 53	AC-2	AC-13	AU-2	AU-3	AU-6	AU-7	AU-9	
ISO17799	0.5	10.1.2	10.1.3	10.10.1	10.10.3	10.10.4	12.5.1	13.2.1
Cobit	PO 4.11	PO 7.8	AI 2.3	AI 2.4	AI 4.2	DS 5.4	DS 5.5	ME 2.3
HIPAA	164.306	164.308a	164.312a	164.312b				

PCI													
FISMA / NIST 800 53													
ISO17799	13.2.3	13.2.4	15.1.1	15.2.1	15.3.1								
Cobit	ME 2.5	ME 3.4	ME 4.4	ME 4.5	ME 4.7								
HIPAA													

Local Group Member Deletions Report

Feature: Compliance -> Account Changes -> Group Account
Report: Member Server User Changes

PCI	6.4	7.1	10.1	10.2	10.3	10.5	10.6	10.7
FISMA / NIST 800 53	AC-2	AC-13	AU-2	AU-3	AU-6	AU-7	AU-9	
ISO17799	0.5	8.3.3	10.1.2	10.10.1	10.10.2	10.10.3	10.10.4	11.1.1
Cobit	PO 4.11	PO 7.8	AI 2.3	AI 2.4	AI 4.2	AI 6.4	AI 6.5	DS 5.4
HIPAA	164.306	164.308a	164.312a	164.312b				

PCI													
FISMA / NIST 800 53													
ISO17799	12.5.1	13.2.1	13.2.3	15.1.1	15.2.1	15.3.1							
Cobit	DS 5.5	ME 2.3	ME 2.5	ME 3.4	ME 4.4	ME 4.5	ME 4.7						
HIPAA													

Local Users Consolidated Changes

Feature: Compliance -> Account Changes -> User Account
Report: Member Server User Changes

PCI	6.4	7.1	10.1	10.2	10.3	10.5	10.6	10.7
FISMA / NIST 800 53	AC-2	AC-13	PS-6	AU-2	AU-3	AU-6	AU-7	AU-9
ISO17799	0.5	10.1.2	10.1.3	10.10.1	10.10.3	10.10.4	12.5.1	13.2.1
Cobit	PO 4.11	PO 7.8	AI 2.3	AI 2.4	AI 3.2	AI 4.2	DS 5.3	DS 5.4
HIPAA	164.306	164.308a	164.312a	164.312b	164.312d			

PCI													
FISMA / NIST 800 53													
ISO17799	13.2.3	15.1.1	15.2.1	15.3.1									
Cobit	DS 5.5	ME 2.5											
HIPAA													

Object Access

Feature: Compliance -> File Access
Report: n/a

PCI	6.4	10.1	10.2	10.3	10.5	10.6	10.7
FISMA / NIST 800 53	AU-3	AU-6	AU-7				
ISO17799	0.5	10.6.1	10.10.1	10.10.2	10.10.3	10.10.4	13.2.1

PCI							
FISMA / NIST 800 53							
ISO17799	13.2.3	15.1.1	15.2.1	15.3.1			

Cobit	PO 4.11	PO 8.6	AI 1.3	AI 2.3	AI 2.4	DS 5.5	ME 2.3	ME 2.5	ME 3.4	ME 4.4
HIPAA	164.306	164.308a	164.312a	164.312b						

Object Deletions

Feature: Compliance -> File Access
Report: n/a

PCI	6.4	10.1	10.2	10.3	10.5	10.6	10.7
FISMA / NIST 800 53	AU-3	AU-6	AU-7	AU-9			
ISO17799	0.5	10.6.1	10.10.1	10.10.3	13.2.3	15.1.3	15.2.1	15.3.1
Cobit	AI 2.3	DS 5.5	DS 9.2	ME 2.3	ME 2.5	ME 3.4	ME 4.4	
HIPAA	164.306	164.308a	164.312a	164.312b				

Permission Changes

Feature: Compliance -> File Access
Report: n/a

PCI	6.4	7.1	10.1	10.2	10.3	10.5	10.6	10.7
FISMA / NIST 800 53	AC-13	AU-2						
ISO17799	0.5	10.6.1	10.10.1	10.10.2	10.10.3	10.10.4	11.1.1	11.6.1
Cobit	AI 2.3	AI 2.4	DS 5.5	ME 2.3	ME 2.5	ME 3.4	ME 4.4	
HIPAA	164.306	164.308a	164.312a	164.312b				

Programs Executed By User

Feature: Compliance -> Process Tracking
Report: n/a

PCI	10.1	10.6						
FISMA / NIST 800 53	MA-3	AC-13	AU-2					
ISO17799	0.5	10.10.1	10.10.2	10.10.3	10.10.4	11.5.4	15.1.2	
Cobit	PO 4.11	AI 1.3	AI 2.3	AI 2.4	DS 5.5	ME 2.5	ME 3.4	ME 4.4
HIPAA	164.306	164.308a	164.312a	164.312b				

Programs Executed Summary

Feature: Compliance -> Process Tracking

Report: n/a

PCI	10.6						
FISMA / NIST 800 53	AU-2						
ISO17799	0.5	10.10.1	10.10.2	10.10.3	11.5.4	15.1.2	
Cobit	PO 5.5	AI 1.3	AI 2.4	DS 5.5	ME 2.5	ME 3.4	ME 4.4
HIPAA	164.306	164.308a	164.312a	164.312b			

User Activity Journal

Feature: Compliance -> Process Tracking
Report: n/a

PCI	10.1	10.2	10.3	10.5	10.6	10.7
FISMA / NIST 800 53	AC-13	AU-2	AU-6	AU-7		
ISO17799	10.10.1	10.10.2	10.10.3	10.10.4	15.1.5	
Cobit	PO 4.11	DS 5.5	ME 2.3	ME 3.4	ME 4.5	
HIPAA						

Major Security Events and Policy changes

Feature: Compliance -> Policy Changes
Report: Active Directory Domain Policy Changes
Active Directory Audit Policy Changes
Active Directory Kerberos Policy Changes
Active Directory Trust Relationship Changes

PCI	6.4	10.1	10.2	10.3	10.5	10.6	10.7			
FISMA / NIST 800 53	AU-2	AU-3	AU-6	AU-7	AU-9					
ISO17799	0.5	10.1.2	10.10.1	10.10.2	10.10.4	12.5.1	13.2.1	15.1.3	15.2.1	15.3.1
Cobit	PO 4.11	AI 2.3	AI 2.4	AI 6.5	DS 5.4	DS 5.5	ME 2.3	ME 2.5	ME 4.5	
HIPAA	164.306	164.308a	164.312a	164.312b						

Domain Account Authentication

Feature: Compliance -> Logons -> Network
Report: Domain Account Authentication

PCI	10.3	10.5	10.7			
FISMA / NIST 800 53	AC-13	AU-2	AU-3	AU-6	AU-7	AU-9

ISO17799	0.5	10.1.3	10.10.1	10.10.2	10.10.3	10.10.4	11.5.2	11.5.3	13.2.3	15.1.3	15.2.1	15.3.1
Cobit	PO 4.11	DS 5.5	ME 2.1	ME 2.5								
HIPAA	164.306	164.308a	164.312a	164.312b	164.312d							

Domain Account Authentication Failure Analysis

Feature: Compliance -> Logons -> Failures
Report: Domain Account Authentication Failure Analysis

PCI	10.2	10.3	10.5	10.6	10.7							
FISMA / NIST 800 53	AC-13	AU-2	AU-3	AU-6	AU-7	AU-9						
ISO17799	0.5	10.1.3	10.10.1	10.10.2	10.10.3	11.5.2	11.5.3	13.2.3	15.1.3	15.2.1	15.3.1	
Cobit	PO 4.11	DS 5.5	ME 2.1	ME 2.5								
HIPAA	164.306	164.308a	164.312a	164.312b	164.312d							

Initial Logon With Servers Accessed

Feature: Compliance -> Logons -> Network
Report: n/a

PCI						
FISMA / NIST 800 53	AC-2	AU-2	AU-3	AU-6	AU-7	AU-9
ISO17799	10.10.1	10.10.2	10.10.3	15.1.5		
Cobit						
HIPAA						

Member Server Authentication

Feature: Compliance -> Logons -> Network
Report: n/a

PCI	10.2	10.3	10.5	10.7								
FISMA / NIST 800 53	AC-13	AU-2	AU-3	AU-6	AU-7	AU-9						
ISO17799	0.5	10.1.3	10.10.1	10.10.2	10.10.3	10.10.4	11.5.2	11.5.3	13.2.3	15.1.3	15.2.1	15.3.1
Cobit	PO 4.11	DS 5.5	ME 2.1	ME 2.5								
HIPAA												

User Authentication And Logon Journal

Feature: Compliance -> Logons -> Network
Report: n/a

PCI						
FISMA / NIST 800 53	AC-2	AU-2	AU-3	AU-6	AU-7	AU-9
ISO17799	10.10.1	10.10.2	10.10.3	15.1.5		
Cobit	PO 4.11	DS 5.5	ME 2.3	ME 3.4	ME 4.5	
HIPAA	164.306	164.308a	164.312a	164.312b	164.312d	

User Logons By Server-Type

Feature: Compliance -> Logons -> By Type
Report: Logons: By Server-Type

PCI	10.1	10.2	10.3	10.5	10.6	10.7
FISMA / NIST 800 53	AC-2	AU-2	AU-3	AU-6	AU-7	AU-9
ISO17799	10.10.1	10.10.2	10.10.3	15.1.5		
Cobit	PO 4.11	DS 5.5	ME 2.3	ME 2.5	ME 3.4	ME 4.5
HIPAA	164.306	164.308a	164.312a	164.312b		

7.4.2 Regulations

Depending on which type of regulatory compliance an organization has to comply with, the following topics can be used as a starting point to determine which reports in EventSentry need to be evaluated and generated on a regular basis.

Once the appropriate reports have been selected, (optionally) customized and a schedule determined, then the Review feature of the reports can be used to ensure that reports are actually being run at the required time intervals.

A blue cell in the table indicates that the report helps fulfill this particular section. For example, the *Active Directory Users Deleted or Disabled*, *Active Directory - User Account Lockouts and Password Resets* and *Active Directory Domain Policy Changes* are relevant for section **164.312e** of **HIPAA**.

7.4.2.1 PCI

	6.4	7.1	10.1	10.2	10.3	10.4	10.5	10.6	10.7	10.8	10.11	10.11	10.12
Active Directory Administrator Logons			■	■	■		■	■	■				
Active Directory General Object Changes	■		■	■	■		■	■	■				
Active Directory Group Member Additions	■	■	■	■	■		■	■	■				
Active Directory Group Member Deletions	■	■	■	■	■		■	■	■				
Active Directory New or Enabled Account		■	■	■	■		■	■	■				
Active Directory Users Deleted or Disabled	■	■	■	■	■		■	■	■				
Active Directory Group Policy Change Report	■		■	■	■		■	■	■				
Active Directory Permission Changes	■		■	■	■		■	■	■				
Active Directory - User Account Lockouts and Password Resets				■	■		■	■	■				

Active Directory - Users Groups and Computers Consolidated Changes	■	■	■	■	■		■	■	■				
Active Directory Domain Policy Changes			■	■	■		■	■	■				
Local Group Member Additions Report	■	■	■	■	■		■	■	■				
Local Group Member Deletions Report	■	■	■	■	■		■	■	■				
Local Users Consolidated Changes	■	■	■	■	■		■	■	■				
Object Access	■		■	■	■		■	■	■				
Object Deletions	■		■	■	■		■	■	■				
Permission Changes	■	■	■	■	■		■	■	■				
Programs Executed By User			■					■					
Programs Executed Summary								■					
User Activity Journal			■	■	■		■	■	■				
Major Security Events and Policy Changes	■		■	■	■		■	■	■				
Domain Account Authentication					■		■		■				
Domain Account Authentication Failure Analysis				■	■		■	■	■				
Initial Logon With Servers Accessed													
Member Server Authentication				■	■		■		■				
User Authentication And Logon Journal													
User Logons By Server - Type			■	■	■		■	■	■				

7.4.2.2 FISMA NIST 800-53

	MA-3	AC-2	AC-3	AC-7	AC-13	PS-6	AU-2	AU-3	AU-6	AU-7	AU-9
Active Directory Administrator Logons					■		■	■	■	■	■
Active Directory General Object Changes					■			■	■	■	
Active Directory Group Member Additions		■			■		■	■	■	■	■
Active Directory Group Member Deletions		■			■		■	■	■	■	■
Active Directory New or Enabled Account		■			■	■	■	■	■	■	■
Active Directory Users Deleted or Disabled		■					■	■	■	■	■
Active Directory Group Policy Change Report			■		■		■	■	■	■	■
Active Directory Permission Changes			■		■		■	■	■	■	■
Active Directory - User Account Lockouts and Password Resets		■		■			■	■	■	■	■
Active Directory - Users Groups and Computers Consolidated Changes		■			■						
Active Directory Domain Policy Changes			■		■		■	■	■	■	■
Local Group Member Additions Report		■			■		■	■	■	■	■
Local Group Member Removal Report		■			■		■	■	■	■	■
Local Users Consolidated Changes		■			■	■	■	■	■	■	■
Object Access								■	■	■	
Object Deletions								■	■	■	■
Permission Changes					■		■				
Programs Executed By User	■				■		■				
Programs Executed Summary							■				
User Activity Journal					■		■		■	■	
Major Security Events and Policy Changes							■	■	■	■	■
Domain Account Authentication					■		■	■	■	■	■
Domain Account Authentication Failure Analysis					■		■	■	■	■	■
Initial Logon With Servers Accessed		■					■	■	■	■	■

Member Server Authentication													
User Authentication And Logon Journal													
User Logons By Server - Type													

7.4.2.3 ISO 17799

	0.5	8.3	10.1.2	10.1.3	10.6.1	10.10.1	10.10.2	10.10.3	10.10.4	11.1.1	11.15.1	11.15.2	11.15.3	11.15.4	11.16.1	12.5.1	13.2.1	13.2.3	15.1.2	15.1.3	15.1.5	15.2.1	15.3.1
		3																					
Active Directory Administrator Logons																							
Active Directory General Object Changes																							
Active Directory Group Member Additions																							
Active Directory Group Member Deletions																							
Active Directory New or Enabled Account																							
Active Directory Users Deleted or Disabled																							
Active Directory Group Policy Change Report																							
Active Directory Permission Changes																							
Active Directory - User Account Lockouts and Password Resets																							
Active Directory - Users Groups and Computers Consolidated Changes																							
Active Directory Domain Policy Changes																							
Local Group Member Additions Report																							
Local Group Member Deletions Report																							
Local Users Consolidated Changes																							
Major Security Events and Policy Changes																							
Object Access Report																							
Object Deleted																							
Permission Changes																							
Programs Executed By User																							
Programs Executed Summary																							
User Activity Journal																							
Domain Account Authentication																							

Domain Account Authentication Failure Analysis	■			■		■	■	■				■	■					■		■		■	■
Initial Logon With Servers Accessed						■	■	■													■		
Member Server Local Account Authentication	■			■		■	■	■	■			■	■					■		■		■	■
User Authentication And Logon Journal						■	■	■													■		
User Logons By Server - Type						■	■	■													■		

7.4.2.4 CobiT / Sarbanes Oxley

	PO 4.11	PO 4.14	PO 5.5	PO 7.8	PO 8.6	AI 1.3	AI 2.3	AI 2.4	AI 3.2	AI 4.2	AI 6.4	AI 6.5	DS 5.3	DS 5.4	DS 5.5	DS 9.2	ME 2.1	ME 2.3	ME 2.5	ME 3.4	ME 4.4	ME 4.5	ME 4.7
Active Directory Administrator Logons	■			■			■	■		■			■	■	■			■	■	■		■	
Active Directory General Object Changes	■						■	■		■	■	■			■			■	■	■		■	■
Active Directory Group Member Additions	■			■			■	■		■	■	■		■	■			■		■	■	■	■
Active Directory Group Member Deletions	■			■			■	■		■	■	■		■	■			■	■	■	■	■	■
Active Directory Users - New or Enabled	■			■			■	■	■	■			■	■	■				■				
Active Directory Users Deleted or Disabled	■	■		■				■			■			■	■				■	■			■
Active Directory Group Policy Change Report	■						■	■		■	■	■			■			■	■	■		■	■
Active Directory Permission Changes	■						■			■	■	■			■				■	■		■	■
Active Directory - User Account Lockouts and Password Resets	■								■	■				■	■				■				
Active Directory - Users Groups and Computers Consolidated Changes	■			■			■	■		■	■	■		■	■			■	■	■	■	■	■
Active Directory Domain Policy Changes	■						■	■		■	■	■			■			■	■	■	■	■	■
Local Group Member Additions Report	■			■			■	■		■				■	■			■	■	■	■	■	■
Local Group Member Deletions Report	■			■			■	■		■	■	■		■	■			■	■	■	■	■	■
Local Users Consolidated Changes	■			■			■	■	■	■			■	■	■				■				
Major Security Events and Policy Changes	■						■	■				■		■	■			■	■			■	
Object Access Report	■				■	■	■	■							■			■	■	■	■		
Object Deleted							■								■	■		■	■	■	■		
Permission Changes							■	■							■			■	■	■	■		
Programs Executed By User Report	■					■	■	■							■				■	■	■		
Programs Executed Summary			■			■		■							■				■	■	■		
Domain Account Authentication Failure Analysis	■														■		■		■				
Domain Account Authentication	■														■		■		■				
User Logons By Server - Type	■														■			■	■	■		■	
User Activity Journal	■														■			■		■		■	

Member Server Local Account Authentication																				

7.4.2.5 HIPAA

	164.306	164.308a	164.312a	164.312b	164.312c	164.312d	164.312e
Active Directory Administrator Logons							
Active Directory General Object Changes							
Active Directory Group Member Additions							
Active Directory Group Member Deletions							
Active Directory New or Enabled Account							
Active Directory Users Deleted or Disabled							
Active Directory Group Policy Change Report							
Active Directory Permission Changes							
Active Directory - User Account Lockouts and Password Resets							
Active Directory - Users Groups and Computers Consolidated Changes							
Active Directory Domain Policy Changes							
Local Group Member Additions Report							
Local Group Member Removal Report							
Local Users Consolidated Changes							
Major Security Events and Policy Changes							
Object Access Report							
Object Deleted							
Permission Changes							
Programs Executed Report							
Programs Executed Summary							
Domain Account Authentication Failure Analysis							
Domain Account Authentication							
User Logons By Server - Type							
User Activity Journal							

7.5 Verschiedenes

7.5.1 File Monitoring vs. File Access Tracking

Die Funktionen Dateiüberwachung (Systemzustand) und Dateizugriffsverfolgung (Sicherheit & Compliance) können zweideutig erscheinen, da sie beide Dateiänderungen überwachen. Die Funktionen sind jedoch recht unterschiedlich und versuchen, unterschiedliche Probleme zu lösen. Die nachstehende Vergleichstabelle umreißt die wichtigsten Unterschiede zwischen diesen Funktionen:

Vergleichs-Übersicht

Feature	Datei-Überwachung	Dateizugriffsverfolgung
Kann Alerts erzeugen, Aktionen auslösen	Ja	Nein
Erfordert, dass NTFS-Auditing für überwachte Ordner aktiviert ist	Nein	Ja

Erfasst den Benutzernamen, der auf die Datei zugegriffen und/oder sie geändert hat	Nein	Ja
Kann den aufrufenden Prozess erfassen, der auf die Datei zugegriffen und/oder sie geändert hat	Nein	Ja, je nach Quelle
Kann den Quellcomputer erfassen, von dem aus auf die Datei zugegriffen wurde und/oder sie verändert wurde	Nein	Ja
Überwacht Prüfsummen	Ja	Ja
Kann den Lesezugriff überwachen	Nein	Ja

Detaillierter Vergleich

System Health -> File Monitoring

Diese Funktion überwacht Dateien in einem oder mehreren bestimmten Verzeichnissen entweder in Echtzeit oder in geplanten Intervallen. Die Dateiüberwachung wurde sowohl mit Blick auf die Sicherheit (Integritätsprüfungen) als auch auf die Systemautomatisierung entwickelt und dient in erster Linie dazu, Warnmeldungen auszugeben oder Aktionen auszulösen, wenn eine Dateiänderung erkannt wird.

Vom Sicherheitsstandpunkt aus gesehen stellt die Dateiüberwachung sicher, dass ausgewählte Dateien (z.B. ausführbare Dateien im SYSTEM32-Verzeichnis, Protokolle von Kreditkartentransaktionen usw.) nicht verändert werden, und dass jede Änderung, die stattfindet, protokolliert wird und optional einen Alarm auslöst.

Aus der Sicht eines Systemadministrators kann es helfen, viele Aufgaben zu automatisieren, die aufgrund von Dateiänderungen in einem Verzeichnis ausgelöst werden. Beispielsweise kann ein Verzeichnis überwacht werden, und jede Datei, die dem Verzeichnis hinzugefügt wird, kann durch eine Prozessaktion automatisch komprimiert werden, oder eine Liste von Benutzern kann benachrichtigt werden, dass eine Datei hinzugefügt wurde. Da Dateiänderungen direkt mit einer Prozessaktion verknüpft werden können, sind die Möglichkeiten, was man tun kann, nur durch die Prozess-/Batchdatei selbst begrenzt.

Ein entscheidender Vorteil der Datei-Überwachungsfunktion ist, dass sie keine zusätzlichen Konfigurationsschritte auf dem Betriebssystem erfordert. Sobald die Datei-

Sicherheit und Compliance -> Dateizugriffsverfolgung

Security & Compliance fängt "Object Access"-Sicherheitsereignisse ab, die vom Betriebssystem erzeugt werden, wenn die Überwachung einer Datei und/oder eines Verzeichnisses aktiviert wurde. Diese Funktion wurde entwickelt, um Verzeichnisse zu überwachen, die vertrauliche oder sicherheitsempfindliche Daten enthalten, und um eine erweiterte Berichterstellung zu ermöglichen, mit der sowohl sicherheits- als auch konformitätsbezogene Anforderungen erfüllt werden können.

Die Dateizugriffsverfolgung kann zwar keine Art von Warnung erzeugen oder Aktionen auslösen, aber sie enthält mehr Informationen über die Dateiänderungen selbst. Der Hauptvorteil besteht darin, dass die Dateizugriffsverfolgung Ihnen oft Auskunft darüber geben kann, wer Änderungen an einer Datei vorgenommen hat und von wo aus.

Je nach Quelle der Dateiänderung können die Daten beispielsweise sowohl den aufrufenden Prozess als auch den Quellcomputer umfassen.

Aufgrund einiger wichtiger architektonischer Unterschiede zwischen den Betriebssystemen von Pre-Vista sind Vista und Windows Server 2008 die bevorzugten Plattformen für diese Funktion, obwohl auch frühere Betriebssysteme unterstützt werden.

Beachten Sie, dass die Dateizugriffsverfolgung voraussetzt, dass die NTFS-Überwachung für jeden Ordner, der überwacht werden soll,

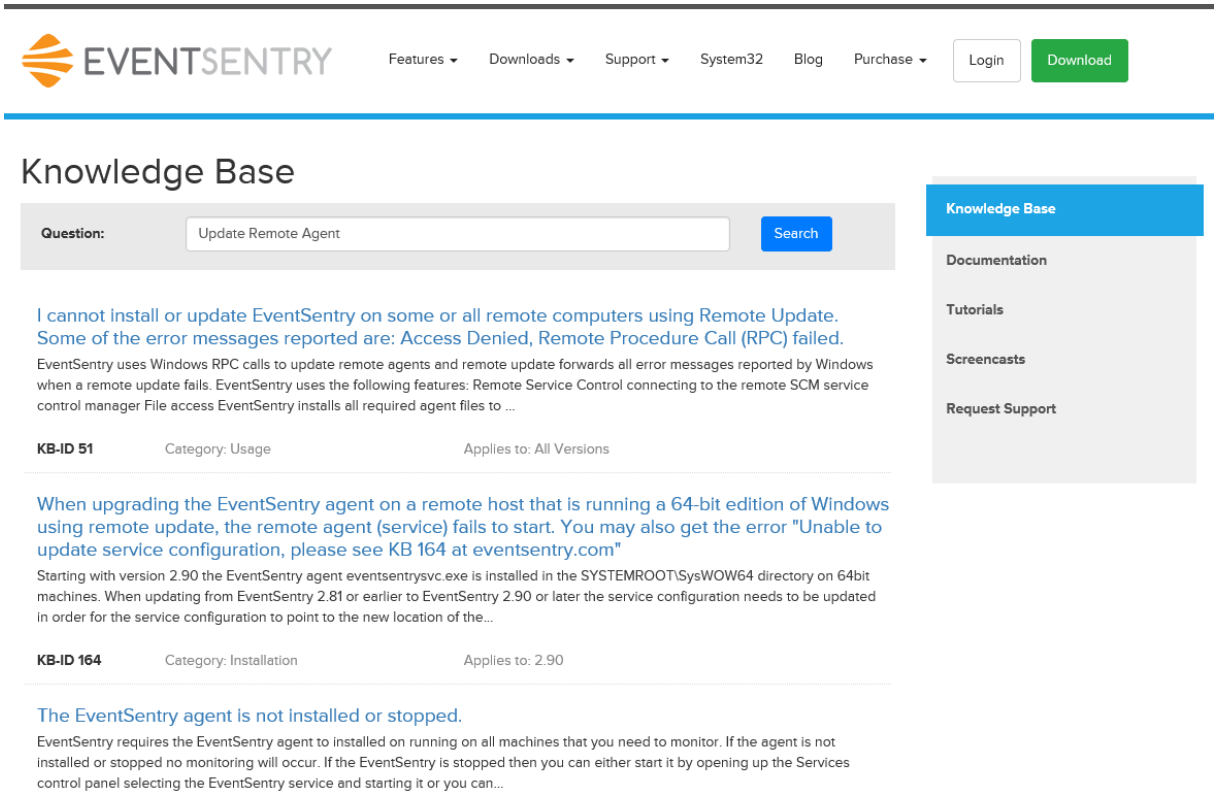
Überwachung konfiguriert und die Konfiguration aktiv ist, wird sie sofort wirksam.

aktiviert ist, siehe Voraussetzungen für die Dateizugriffsverfolgung für weitere Informationen.

8 Support, FAQ & Versionen

8.1 Fehlerbehebung und FAQ

Bitte durchsuchen Sie unsere Knowledge Base unter https://www.eventsentry.com/support/kb nach Antworten auf bekannte Probleme. Unsere Wissensdatenbank wird ständig weiterentwickelt und enthält Antworten auf die am häufigsten gestellten Fragen und Probleme zu EventSentry.



8.2 Fragen oder Probleme?

Bitte beachten Sie, dass wir Ihnen nur die Beantwortung von Support-Anfragen garantieren können, die von **registrierten E-Mail-Adressen** (standardmäßig diejenige, die Sie beim Kauf von EventSentry angegeben haben) gesendet werden.

EventSentry Light Benutzer

Wenn Sie die kostenlose Version von EventSentry, EventSentry Light, verwenden, dann können Sie Unterstützung über die NETIKUS.NET Support-Foren unter https://helpdesk.eventsentry.com/ oder über die Knowledge Base unter http://www.eventsentry.com/support/kb erhalten.

Fragen

Bei Fragen zu EventSentry wenden Sie sich bitte entweder über Email oder Telefon an uns:

- E-Mail an support@netikus.net oder
- Anruf 1-877-NETIKUS (1-877-638-4587)

mit den folgenden Informationen:

- Das Betriebssystem (inkl. Service Pack-Version), auf dem EventSentry läuft
- Die Version von EventSentry
- Ihre Frage

Probleme

Wenn Sie Probleme mit EventSentry haben, können Sie entweder das Fehler-/Problembericht-Feedback-Formular im Feedback-Menü ausfüllen oder

- senden Sie eine E-Mail an support@netikus.net
- Anruf 1-877-NETIKUS (1-877-638-4587)

und enthalten die folgenden Informationen:

- Das Betriebssystem (inkl. Service Pack-Version), auf dem EventSentry läuft
- Die Version von EventSentry
- Eine genaue Beschreibung des Problems. Fügen Sie Informationen bei wie z.B:
  - Tritt dieses Problem bei einer oder mehreren Installationen auf?
  - Ist es einmal aufgetreten oder tritt es wiederholt auf?
  - Was können wir tun, um das Problem zu reproduzieren?

8.3 Version History

This page lists all versions of EventSentry that were released since its initial launch in December 2002 until 2017. A complete version history of all versions is available online.

To learn more about the numbering system click here.

Version 3.4.1 September 2017

Windows Monitoring

- Additional capabilities to detect and prevent against new types of Ransomware infections, including variants that modify the boot sector.
- New software version check identifies outdated software on your network to help you reduce your attack surface. This new feature supplements EventSentry's software inventory component.
- Disk space alerts now include a list of the largest files and folders of a volume
- UPS & Battery monitoring now inventories all attached UPS batteries as well as integrated batteries (laptops) regardless of the manufacturer
- Effective audit settings on a Windows host can sometimes deviate from group policy settings - due to conflicts, errors and so forth. A new Audit Policy Status page periodically inventories the current audit settings so you can verify the actual audit settings.

Network Monitoring

- NetFlow monitoring now supports calculating the bandwidth of an interface, including additional statistics such as packet count, bytes per packet and more.
- Ping response time now provides packet loss stats

Integrations

- EventSentry agents can now be integrated with many open source and commercial log solutions with additional Syslog options - even custom JSON formatting is supported!

Web Reports

- Now available in 64-bit and support larger reports and increased performance
- New user activity tracking page makes seeing all activity by a user as easy as never before!

Version 3.3.1 December 2016

NetFlow

- NetFlow with support for NetFlow v1, v5, v9 & sFlow. NetFlow supports visualization, geolocation, alerts, correlation with workstation logon events to map flows to ActiveDirectory users, filtering and more

Web Reports

- Notes & Documentation: Web reports users can submit notes to document infrastructure updates, maintenance, fixes and more. Documentation files can be uploaded and associated with hosts
- Added ISO 27001:2013 compliance reports
- New security features
- New dashboard tiles
- Treemap visualization available for most pages
- Updated look and improved menu

Management Console

- Deployment: Agents using the collector can receive configuration and agent binary updates automatically through the collector without user intervention.
- Deployment: MSI installers can now be created in a few seconds directly from the management console (requires free WiX Toolset)
- Ability to reset the configuration to post-installation defaults (new v3.3 installations only)
- Remote configuration can now removed when uninstalling an agent even when remote registry service is unavailable
- Version checks and update/patch downloads are now performed over TLS for enhanced security

Agent

- 64-bit agent is now available for 64-bit Windows
- Removed limit and improved management of custom event logs
- Support for chaining events
- Agent / Collector: Emails containing IP addresses sent through collector can be enhanced to display geolocation and reverse lookup data inline.
- Emails from security event log will automatically be enhanced with descriptions for many status and error codes
- Database performance of delimited log files has been significantly improved
- Insertion strings of events can be created or replaced using regular expressions
- Install date of software is now available for most software even if it was installed before EventSentry

- USB drives are now detected in real-time

Other

- Heartbeat Agent: Agent status is now retrieved directly from collector and/or database for faster and more efficient monitoring
- Network Services: Database performance for Syslog component has been improved for MSSQL databases
- Network Services: License count for network devices is now more accurately enforced
- Database: Built-In database now uses PostgreSQL v9.6, optional upgrade path is available
- Configuration: Improved out-of-the-box filter rules for less noise

Version 3.2.1 February 2016

Collector

- Central collector service which enables a 3-tier architecture between an action (e.g. database, email server) and the EventSentry agents
- Supports compression and secure data transmission via TLS encryption

General

- Management Console: Ability to import computers from a network (subnet) scan
- Management Console / Remote Update: Record activity in log files
- Management Console / Remote Update: Toggle fields in result list
- Management Console: Export all configured filters to CSV file
- Switch inventory with switch port to MAC/hostname mapping
- Detection of highest supported USB version

Web Reports

- Additional language support for French, Spanish, Polish, Portuguese and Italian
- Out-of-the-box compliance reports for PCI-DSS, FISMA, Sarbanes Oxley, HIPAA and GLBA
- Improved & faster performance trend reporting with ability to display multiple trend charts on a single page
- New Bulk assignment for easier report management
- Report jobs can be saved to a folder
- Improved host inventory page now shows switch port (if available), USB version and VM hosts (if available)
- Health matrix displays computer notes
- Improved usability throughout
- Improved connection pool support

Version 3.1.1 December 2014

Windows & General Monitoring

- Task Scheduler inventory and change detection
- Large File enumeration
- Inventory of virtual machines (Hyper-V & ESXi)
- HTTP action now supports POST/PUT for better interoperability with web-based APIs
- Disk space monitoring now supports multiple disk space packages assigned to a single host
- Improved remote update / host management, especially of Non-Windows hosts in management console

Heartbeat & SNMP Monitoring

- Process Monitoring support for SNMP-enabled hosts
- Improved router functionality, configure routers based on IP subnet
- Status change detection and uptime calculation is more reliable
- Overall stability improvements in the heartbeat agent

Web Reports

- Support for multiple dashboards, including automatic iteration between dashboards
- Dashboards can be shared
- Support for graphical gauges (Clock, meter, number, bullet)
- New heat-map tile for uniquely visualizing log, syslog and performance data
- New generic search tile supports embedding data from any feature in dashboard
- Support for TV mode and dark/light theme in dashboard
- Various tweaks and improvements to existing dashboard tiles

Version 3.0.1 December 2013

New Web Reports

- Scheduled Jobs: Receive reports via email
- PDF & JSON Output
- UTC Support
- Cross-platform: Supports Windows, Linux and OS X
- Complex queries for all features
- Full API
- Easier installation & setup
- Better dashboards
- Better summary pages
- Do no longer require Flash
- Access control with LDAP integration

Network Monitoring (Heartbeat Agent)

- Poll SNMP counters (integrates with performance monitoring)
- Retrieve disk space information from SNMP-enabled hosts
- Retrieve basic system & hardware information from SNMP-enabled hosts
- Retrieve uptime from SNMP-enabled hosts

Windows Monitoring

- Log file monitoring supports sub folders
- Compliance "Logon By Type" tracking can exclude logons by computer accounts
- Event Log filters can override email subject & message body
- Packages can by dynamically assigned based on platform (32bit vs 64bit)
- Threshold filters can utilize insertion strings
- Disk space prediction feature (predicts when disk will be full)
- Identify reasons why hosts were shut down or rebooted
- Desktop notification supports Growl
- Network notification supports remote desktop services
- Application scheduler support process isolation
- New email format "HTML Modern"

Other

- New management console features ribbon & visual improvements
- New authentication manager

- Many common tasks have been simplified
- Improved built-in event viewer for Application & Services Logs
- ARP daemon detects & tracks new MAC addresses and MAC to IP mappings

Version 2.93 June 2012

New Features:

- New installer for a better installation and upgrade experience
- Now includes a built-in (PostgreSQL) database
- Added support for PostgreSQL 9.x
- ODBC drivers for PostgreSQL and MySQL are now installed automatically (when needed)
- New installation includes performance monitoring packages for Exchange Server and others
- Preliminary support for Windows 8 and Windows Server 2012
- Support for USB-only temperature & humidity sensors
- Introducing the Configuration Assistant, which supersedes the database setup wizard, and introduces additional functionality
- Heartbeat monitoring can now scan hosts in parallel using multiple threads
- Heartbeat monitoring: Maintenance schedule can be set to the "nth" weekday (e.g. 2nd Tuesday)
- Performance Monitoring supports floating point counter values
- Performance Monitoring can log counter data to multiple databases
- Performance Monitoring can combine values from two different counters
- Performance Monitoring can detect leaks in performance counters
- Performance Monitoring can suppress alerts based on past values
- Performance Monitoring alerts are more verbose and include additional information, including counter descriptions
- Process Monitoring: Supports wildcards and can evaluate the command line of a process
- Event Log Backups: Better alerts and alerts now include SHA checksum of .evt(x) files
- Event Log Monitoring: Content filter supports perl regular expression syntax
- Event Log Monitoring: Day/Hour filter can be set to the "nth" weekday (e.g. 2nd Tuesday)
- Event Log Monitoring: For Windows 2008 and later, processing performance has been optimized for higher throughput and lower CPU utilization
- Process Tracking: Now collects process elevation level when UAC is enabled
- Embedded scripts now verify temp file contents with checksum
- Embedded scripts called from the applications scheduler now support command-line arguments
- Hardware Inventory: On DELL & HP servers (when required manufacturer management tools are installed), collects fan speed, redundant power supply status, remote management card information, temperature information, detailed RAID information
- Hardware Inventory: Retrieves warranty information for DELL, HP, IBM and Lenovo hardware
- Hardware Inventory: Retrieves configured UAC level
- Actions: Filter notes can now be posted to HTTP action
- Management Console: Saving configuration is about 10 times faster
- Management Console: Added better keyboard and mouse scroll wheel navigation for better user experience and section 508 compliance
- Management Console: Status of all local EventSentry services is now monitored in the background

- Management Console: Environment monitoring dialog now shows serial ports with descriptions
- Web Reports: Performance Status and Heartbeat Status pages load significantly faster
- IIS: IIS no longer has to be switched to 32-bit mode on 64-bit systems

Bug Fixes:

- Added support for 64-bit event numbers (Vista and later)
- Audit policies for compliance tracking features are now set correctly on Vista and later systems
- Resolved problems in various features when Japanese file names were processed
- Computer names exceeding the maximum NetBIOS length of 15 characters are now properly stored in the database
- Event message text is now properly formatted before submitting to SNPP (Pager) server
- Software Inventory: Internet Explorer is now properly detected on Vista and later
- Software Inventory: Patches are new enumerated even when TrustedInstaller.exe is active
- Event Log Backup: Resolved small memory leak
- Heartbeat Monitoring: Improved reliability
- Heartbeat Monitoring: Resolved memory leaks
- Environment Monitoring: Location is now included in alerts
- Performance Monitoring: Performance Status and other related pages (including network status, mobile apps) now load significantly faster
- Fixed bugs in Console Logon Tracking
- Agent startup speed has been improved when service monitoring is enabled
- File Access Tracking: Fixed issue on Windows 2008 and later
- Network Services: Japanese Syslog messages and SNMP traps are now correctly logged to the event log and database

Version 2.92 April 2011

New Features:

- SNMP trap daemon is introduced and logs v1, v2c and v3 SNMP traps either to the event log or the database
- Syslog daemon has been moved from the EventSentry agent into the "Network Services" service, together with the SNMP daemon. Stability as well as reliability have been improved in the new Syslog daemon
- Performance (optional) as well as environment email alerts now include an attached chart which shows recent performance / environmental data
- Management Console: Clicking a computer icon now displays a summary page
- Event Log Monitoring: Insertion string matching can now match empty strings
- Event Log Monitoring: Number of supported custom event logs has been increased to 30
- Service Monitoring: A recurring alert can be configured when a service remains in the "Stopped" state
- Hardware Inventory: Network adapter speed is now collected, and speed changes are logged to the event log
- Hardware Inventory: Addition and removal of Removable drives (e.g. USB drives) are now detected and logged to the event log
- Hardware Monitoring: The S.M.A.R.T. status of physical drives (when supported) is monitored.
- Disk Space Monitoring: Volumes linked to by junction points are now included when disk space alerts are evaluated / generated. Note: Disk space information in web reports does not yet take junction points into consideration

- Process Monitoring: The number of required instances of a process can now be specified
- Print Tracking: Print tracking now works with Vista and later operating systems
- Network Logon Tracking: When capturing "Logon By Type" events, "Audit Success" can now be excluded
- A new HTTP action submits events to web pages via http or https
- The SMTP action dialog now includes a wizard to build email addresses for common email to SMS gateways
- Additional variable support for the Process, Syslog and Snmp action
- Heartbeat Agent: Improved detection of remote agent status
- Removed: Microsoft Access is no longer officially supported, and no MS Access database is shipped with the installer

Bug Fixes: All bug fixes since the initial 2.91 release have been incorporated into version 2.92, additionally:

- Hosts configured with multiple NICs that are added to the configuration with just the IP address, will properly determine their group membership.
- Print tracking works with Vista, Win7 and Windows 2008

Version 2.91 November 2009

New Features:

- Event Log Monitoring: Filtering capabilities have been improved to allow for insertion string matching, including the ability to interpret insertion strings as numbers, usernames or file names
- Actions: SNMP action now supports v2c and v3 traps
- Service Monitoring: Now collects service account as well as executable, in both alerts as well as reporting
- Service Monitoring: Service history report now shows every service change per line, with easier readability
- Process Tracking: Command line arguments of an active can now be collected
- Logon Tracking: Group information is now collected
- Software Monitoring: Uninstallation events now include same information as installation events
- Software Monitoring: Windows updates are now collected on Vista, Windows 2008 and Windows 7, and more easily searchable in the web reports
- Hardware Monitoring: IP addresses are now collected, and changes updated dynamically in the background
- File Monitoring: Processing of a file's checksum can now be skipped if the size has not changed
- Management Console: Authentication can now be set globally, in addition to being set on a per-group and per-computer level
- Management Console: Computers in AD-linked groups can be sorted.
- Management Console: Notes can now be added to computers
- Environment monitoring: The minimum monitoring interval has been reduced to 5 minutes
- Reporting: Health status of multiple computers can be displayed in a visual health matrix, scalable to display hundreds of computers in a single page
- Reporting: The network status page now allows the customizations of performance counters as well as disks displayed
- Reporting: Reports are more accessible, and can now be accessed from every page
- Reporting: Most pages have been overhauled and improved for improved usability

Performance Enhancements:
- Event Log Monitoring: Filter processing has been improved, resulting in a lower CPU usage
- Checksum generation (File Monitoring, File Access Tracking) has been improved resulting in lower CPU usage

Bug Fixes: All bug fixes since the initial 2.90 release have been incorporated into version 2.91.

- Software Monitoring: Duplicate records of software is not longer shown in the software inventory
- Compliance Tracking: Temp file was used even when its maximum size was set to 0 Mb
- Network Status: This feature has been improved to avoid problems with computers missing, being displayed in the wrong group or not showing up at all
- Disk space Monitoring: Alerts for low disk space are no longer generated when the total disk space is less than the alert (hard) limit to begin with
- Hardware Inventory: Virtual machine detection, as well as Hyper-V detection has been improved for more reliability

Version 2.90 October 2008

New Features:
- Vista, Windows 2008 are monitored with new API
- Event Log Backup feature supports .evtx files
- Database Import Utility supports .evtx files
- New NTP monitoring and synchronization feature
- Event Log Filter Timers now support insertion strings for easier setup & more flexibility
- Scripts can now be embedded into the EventSentry configuration and referenced in application schedules & process actions
- Actions: Jabber action supports chat rooms
- Actions: Process action supports time-based termination and more event logging options
- Actions: Fields in SMTP action can now be customized
- Actions: In addition to controlling services, processes can be terminated (with support for insertion strings)
- Actions: Certain actions can track their trigger history in database
- Actions can now be enabled/disabled based on weekday and time of day
- Compliance: New File Access Tracking feature
- Compliance: Account Management Tracking
- Compliance: Successful & Failed network logon tracking
- Compliance: Audit, Domain & Kerberos policy tracking
- Compliance: Trust Relationship tracking
- Compliance: User & Logon Right change tracking
- Compliance: Improved logon tracking to include domain role and indicate administrative logons
- Compliance: Process tracking includes domain role
- Variables can now be assigned to computers in addition to global & groups
- Service Monitoring: Events now distinguish between services and drivers
- File Monitoring: Can detect alternate data streams (ADS)
- Performance Monitoring: Added "between" condition and "divide by # of processors"
- Software Monitoring: Monitors and records system uptime
- Hardware Inventory: Detects more details about the OS (e.g. editions) as well as hardware

- Management Console: Group-Level Inheritance can be blocked on a per-computer basis
- Management Console: Remote update feature now uses threads for much faster update speeds
- Management Console: Added "Quicktools" to execute any application against a remote computer
- Heartbeat Monitor: Can now utilize credentials set on group or computer items
- Heartbeat Monitor: Can notify you via email when the EventSentry agent is not running
- Web Reports: Extremely granular, built-In authentication has been added
- Web Reports: Users can customize their settings in web reports without affecting global profile settings
- Web Reports: Network Status includes switch to only show erroneous machines
- Web Reports: Network Overview shows disk & performance alerts and event log trends
- Web Reports: Network Overview shows overdue reports and most active machines
- Web Reports: Computer Overview includes event log trend, overview and common errors
- Web Reports: Report management has been improved
- Web Reports: Reports support review as well as a report trigger history
- Web Reports: Right-click menu for column headers allows toggling columns
- Web Reports: Maintenance wizard supports deleting multiple computers at once, and much more
- Web Reports: Database usage page shows storage details of database
- Web Reports: Database can now be created and/or updated using the web reports
- Web Reports: Print output has been significantly improved
- Three completely redesigned widgets using the Yahoo Widget Engine

Bug Fixes:

- Several bug fixes in the database import utility for importing log files
- Issues with filter times have been resolved
- Filter test feature has been improved
- Event Log Monitoring has been improved for better reliability

Version 2.81 September 2007

New Features:

- Database Setup Wizard now supports database connection strings and EventSentry Actions as a destination in addition to System DSNs
- Nessus Import Utility and reporting now supports XML files from Nessus v3 as well
- Web Reports: New "Network Status" overview page
- New SMTP engine now supports TLS/SSL connections
- Event Log Backup files can now be automatically compressed
- Line delimiter can now be specified for non-delimited files as well
- Actions now support a limit feature
- Management Console can automatically check for new versions and patches
- Event Log Database Import utility is now called "Database Import Utility" and supports importing delimited and non-delimited log files
- You can now specify a router for a Heartbeat-Enabled group to suppress duplicate alerts when a router goes down
- Hardware inventory can now distinguish between logical and physical CPUs and show more detailed CPU information
- Web Reports: Computer Overview page supports automatic iteration between computers
- Web Reports: Weekly Logon Reports in Logon Tracking
- Web Reports: Ability to email event records and copy event records to the clipboard

- Web Reports: Calendar popup improved on newer browsers

Bug Fixes:

- Improved SQL queries drastically improve speed of most searches on the web reports
- Detailed hardware inventory information (NIC, memory, etc.) would sometimes not be recorded correctly
- Host names / IP addresses of remote Syslog hosts would not be included in events or the database if the IP address of the remote host could not be resolved
- Resolved bug in environment monitoring dialog
- Computers logging on to Citrix or Terminal Servers would show up in the "Computers" field of the Logon Tracking page
- Active Directory Auto-Refresh: Computers that were removed from AD would not automatically be removed from the corresponding group
- Web Reports: Improved Correlation between logon and process tracking
- Web Reports: Several bug fixes in combination with MySQL, profile editor

Version 2.80 May 2007

New Features:

- Log File Monitoring allows you to monitor both non-delimited and delimited files. You can either consolidate content into the database or receive alerts based on text logged to the log files
- File Monitoring allows you to be notified when files in a monitored directory are changed (includes checksum hashes), and you can either track changes in the database or receive alerts
- Directory Monitoring alerts you when a monitored directory exceeds a preset size
- Jabber notifications allow you to send IM notifications, e.g. using Google Talk!
- The hardware inventory feature now includes detailed information about installed memory and available slots, installed network cards, optical drives and you can remotely power on computers using WakeOnLAN!
- Logon Tracking now includes more detailed information such as remote IP address, session connections/disconnections and workstation unlocks
- The heartbeat agent now supports recurring alerts
- As always we also fixed minor bugs and optimized various aspects of the agent to continuously increase the availability of the agents
- Two new wizards were added for the log file monitoring and for setting up thresholds
- A “filter test” utility has been added that allows you to test events against your filter rules by simply right-clicking an event in the built-in event viewer
- Insertion Strings of events can now be displayed in the subject of an email ($STR1, $STR2, ...)
- System Health features now include an "Alerts" button to easily create filters for events logged by the respective feature
- Package summary pages now include description of packages
- Hardware inventory feature can generate alerts when memory, CPU count or number of installed drives change

Bug Fixes:

- Custom event log settings are now completely transferred to remote machines when pushing the configuration
- Some events would not be transferred correctly with the SNMP action
- On 64-bit systems, EventSentry now shows 32-bit and 64-bit installed software

Version 2.72 8th September 2006

New Features:

- Remote configuration updates do not require the Remote Registry Service anymore, but instead use the ADMIN$ share. A work-around without the ADMIN$ share exists
- Remote update shows the total and average time it took to perform an action
- Event Log Backup Files (.evt) can be imported into the EventSentry database
- Event Message Browser lets you view and test all installed event messages
- Two wizards where added to accomplish common tasks
- Disk space alerts are now cleared after an alert, the volume name is also shown in alerts
- Disk space web-reports can be filtered/grouped on the group level
- Speed of performance charts was improved significantly
- Expanded the "toggle" functionality to most search pages
- A user-configured IP address will now be used on the web reports

Bug Fixes:

- Deleting a database action could incorrectly configure the notifications of existing health and tracking features, including notifications set on the package-level
- Remote update would not work correctly when the EventSentry was not installed locally
- Creating a new package and immediately configuring it to be global would not work
- The automatic configuration backup feature would not correctly delete old files
- A temperature-only sensor could not be configure for a position other than 1
- The temperature and/or humidity sensor would not work correctly
- Remotely connected event logs would sometimes not be restored correctly
- Filters and folders with the same name would crash the GUI
- The event log summary dialog would display incorrect data when connected to remote hosts
- Finding Event IDs works correctly now
- Creating multiple SNPP action notifications was not possible
- Resolved problems with event reports on SQL Server 2005
- Resolved problems with IP address lookup
- Resolved problems with the performance reports

Version 2.71 6th July 2006

New Features:

- Filter Timers for event-log relation
- Additional hardware sensors: Motion-, Smoke- and Water sensors
- Nessus reporting support
- Database purge utility (command-line based)
- Installer now supports MySQL
- Agent: New Shutdown/Reboot and Service Control action
- Agent: Support for more runtime variables in SMTP Header/Footer
- Heartbeat Monitoring: Ping tracking
- Heartbeat Monitoring: Maintenance schedule can be accounted for in uptime statistics
- Improved hardware inventory (now also detects serial numbers, model and graphic adapter/resolution)
- Remote Update utility to automate remote update tasks
- Improved dashboard
- Ability to save the configuration as a HTML file
- Maximum temp file size mechanism change
- Various improvements in the web reports

Bug Fixes:

- Pushing the agent to a remote host running the x64 edition Windows Server 2003 would sometimes not work
- Fixed problems with application scheduler that would not execute certain files properly
- Fixed various small bugs in management console application
- Fixed problem with certain threshold settings
- Fixed bug with performance monitoring
- Fixed XSS vulnerability in web reports
- Fixed minor issues in database setup wizard
- Fixed problem with event log backup assignments
- Fixed problem when computers where added with FQDN instead of NetBIOS name

Version 2.70 9th February 2006

New Features:

- Management console now supports filter, health and tracking package for easier and more flexible administration
- NETIKUS.NET offers standard filter and health packages that can be updated directly from the management console over the Internet
- Performance monitoring to track performance information (e.g. CPU usage, memory usage) in a database and/or receive performance alerts via notifications (e.g. email)
- Filter packages can be configured to be automatically active when one or more services are installed
- Environment monitoring now supports temperature and humidity ranges and also clears previously issued alerts
- Pager support for paging providers that support the SNPP protocol
- Service monitoring now includes database support, allowing you to query service status, history and uptime through the web reports
- Autorun Monitoring is now called "Software Monitoring"
- Software inventory is now included as Software Monitoring now includes database support. This allows you to query installed applications and installation history through the web reports.
- Software monitoring also monitors the ActiveSetup registry key
- 3rd Party Application is now called "Application Scheduler" and supports running custom monitoring tasks in a recurring fashion, e.g. every 30 seconds.
- Logon tracking monitors logon's and logoff's, enabling you to view detailed logon/logoff information about users through the web reports
- Print tracking monitors all print jobs and allows you to see print job data and statistics through the web reports, including the ability to assign cost to print queues for invoicing
- The threshold feature has been simplified and offers new features
- The built-in event log viewer supports opening .evt files, you can also open .evt files directly from explorer
- Remotely connected event logs can automatically be restored after restarting the management console
- The remote update computer list can automatically be sorted
- Heartbeat agent now supports maintenance schedules that can be set for individual computers and/or groups
- Management console supports searching for filters and computers
- Management console can automatically backup the entire configuration at preset intervals
- The completely redesigned web reports now offer a dashboard, event log reports, a profile editor, a maintenance wizard and much more!

Bug Fixes:

- Reduced size of configuration in registry for faster remote updates
- Increased agent stability
- Fixed problems with moving and cutting/pasting filters
- Several problems in the web reports have been fixed
- Duplicate computers cannot be entered anymore and no longer cause problems with the heartbeat agent

Version 2.60 1st June 2005

New Features:

- SNMP Support (sending traps)
- Monitoring of application installation/uninstallation
- Monitoring of machine-based autorun registry keys and directories
- Web reports now feature an uptime calculation page
- Ping option for remote update can be toggled
- System health options can now be set to block inheritance
- Process Monitoring can be configured to start after X seconds
- Various enhancements in the management application, including proxy server support for feedback and news feature
- Added ping dependency in heartbeat monitoring
- Added additional monitoring options in heartbeat monitoring
- Added database backup feature (if database is temporarily unavailable) to heartbeat monitoring
- Agents installed through remote update can now be uninstalled on target machines using "Add/Remove Programs"
- Desktop action notification now supports remote hosts in addition to the local host
- "Online Configuration Update" feature was improved for higher stability
- Map IP address to alias in remote update
- Changed MSI installer from Wise to InstallShield for higher stability and more future features

Bug Fixes:

- Some SIDs were not resolved to usernames correctly
- Clicking on the "Computers" container would show a wrong path in an error message
- Computers would randomely not show up in the web reports computer list
- Saving the configuration would increase the memory usage on the agent, without freeing it (~200kb)
- Some processes in "Process Tracking" would incorrectly show up as "still running" when they had exited
- Bootscan feature of Process Tracking would not record all activity correctly
- Recurring event filters would not work 100% correctly when a schedule would end exactly at midnight
- SMTP Footer would not appear in Mini Emails
- Under certain circumstances on very busy event logs (e.g. security event log on domain controllers) some event records would be skipped and not processed by EventSentry.
- The EventSentry agent would crash under special circumstances when using the summary notification feature.
- When clearing an event log the EventSentry agent would not continue to monitor this log.
- Fixed various issues with SP1 of Windows Server 2003
- Various bug fixes in the management application
- Various bug fixes in the EventSentry agent

- Fixed problems in combination with DEP (data execution prevention) in SP1 of Windows Server 2003

Version 2.50 26th January 2005

New Features:

- Temperature & Humidity monitoring with external device
- Heartbeat monitoring of remote hosts (ES agent monitoring, PING and TCP port checks)
- Local computername may now be added to remote update list
- ODBC Target supports ODBC connection strings in addition to DSN names for easier deployment
- "Audit Process Tracking" can now also be switched off through "Process Tracking" feature
- Recurring event feature lets you define events that you expect to appear (such as a tape backup) during a certain time period, and become notified if they are not
- Computer field added to event log filter properties
- Event Log Backup feature now supports environment variables in file name
- Event Log Full detection now also supports the ODBC, NET SEND, SYSLOG and DESKTOP actions
- GUI: Event Log Viewer supports sorting
- GUI: Remote Update results window allows for sorting
- GUI: Remote Update also sends computer names
- GUI: Remote Update "Computers" container supports sorting and drag/drop
- GUI: Targets support drag/drop
- GUI: Active Directory linked groups now show the actual computers under the "Computers" container and allow for authentication to be set on a per-host level
- GUIDs in event log records are resolved to display name
- Filter Source, Category and Users allow for multiple values, separated by comma
- Filter Source, Category and Users support negation with exclamation mark
- Binary data of events now also available in all notifications, GUI and web reports
- Additional variable support for the FILE action
- ASP and PHP Web reports now work with all supported databases (Access, MSSQL, MySQL, Oracle), the PHP web reports have been switched to use ODBC
- A new Database Wizard now creates all tables, indexes and permissions automatically on MSSQL, MySQL and Oracle
- The new MSI installer optionally creates a virtual IIS directory and/or sets up the MS SQL Server database automatically
- SMTP action now supports an optional header and footer that can be added to every email
- Service Monitoring: Included/Excluded services now support wildcards
- Process Tracking: Included/Excluded processes now support wildcards

Bug Fixes:

- Database layout completely redesigned for faster web reporting
- Event Log Scanning engine significantly improved
- Memory Leak in filter processing removed
- Absolute diskspace limits now work for values > 4Gb
- Selecting a particular set of logical drives would not work
- ASP Web pages corrected to support Access databases without restrictions
- ASP Web pages corrected to support non-US date formats
- Threshold feature incorrectly counting excluded events towards limits
- Filtering of "Filter Text" would not work correctly when filter text attempted to match the last character of an event log record

- Password for group (remote update) not saved correctly
- GUI will not allow more than one instances anymore on computers running Terminal Services to avoid data corruption
- GUI will not freeze while performing remote updates and switching to another application
- Several bug fixes in ASP and PHP web reports
- Unsupported characters were allowed in filter names, resulting in configuration corruption

Version 2.43 22nd July 2004

New Features:

- Process Tracking records all process activity in a database and allows you to see a process history on all monitored hosts
- Service monitoring can control services and maintain a set status. Failed services can now be automatically restarted
- Disk Space Monitoring allows for more granular settings for warnings and database connections
- Disk Space Monitoring will now recognize when new (fixed) disks are added or removed during runtime
- Event Log Backup allows for backups of all event logs for faster configuration
- Database table names can now be specified for each of the features requiring a database (ODBC action, disk space trend collection and detailed process tracking)
- GUI: "Force News Update" reloads latest news
- GUI: Filters can be commented

Bug Fixes:

- Handle leak in eventsenry_svc.exe.
- Memory leak in NonPaged pool when using the TCP syslog action and remote syslog host is not accepting TCP connections
- Launching applications with the "3rd Party Applications" feature might show error "Invalid access to memory location" and the application would not run.
- An error with the summary notification feature could crash the application when a large amount of events (more than the configured maximum) were summarized.
- Right-Click on SYSTEM event log in tray icon opens security log (no other logs are affected)

Version 2.41 7th June 2004

New Features:

- Added $HOSTNAME variable to event log backup feature

Bug Fixes:

- Warning messages in PHP interface removed
- Wrong $DAY, $MONTH and $YEAR variables in event log backup feature
- OLE DB error in index.asp file removed when using an MS Access database

Version 2.40 25th May 2004

Version 1.x Compatability mode will no longer be supported starting with Version 2.40 of EventSentry. If you are still running 1.x agents in your network then you will need to upgrade them to version 2.40.

New Features:

- GUI: Tree in navigation pane restructured for easier navigation, general usability improvements

- GUI: Maximum groups, actions were increased
- GUI: Active Directory Import (with "Link" feature) added
- GUI: Up to 5 remote event logs can be added to navigation pane
- GUI: Change detection added, GUI tries to determine whether changes were made and only prompts to save then
- GUI: Event Log Viewer filter added (filter for errors, warnings, information, audit success & failure)
- GUI: Only active group is sent to remote computers with remote update
- GUI: One-Button remote agent installation
- GUI: Tree status is now also saved/restored when connecting to remote computers
- GUI: ODBC action has a test button now too
- SMTP Target: Mini-Emails can now be customized
- SMTP Target: Dial RAS connections before sending emails
- SYSLOG Target: This action has been optimized and should offer higher throughput
- Custom variables are introduced, variable processing improved
- Variable $EVENTMESSAGE for SMTP subject added
- Automatically backup and clear event logs on a regular basis
- Run command-line applications and log their output to the event log
- Monitor memory consumption of processes to detect possible memory leaks
- Monitor diskspace, including trend change detection
- Trial Version & Full Version are now one product

Bug Fixes:

- GUI: Remote Update: Health settings of a group could be deleted when only updating filters
- GUI: Service Monitoring would not save changes when adding services that don't exist on local machine
- GUI: Feedback forms do not disappear when connection was unsuccessful
- GUI: Renaming groups could yield random results
- SERVICE: Filter processing has been optimized
- SERVICE: Some boot time events could be ignored
- SERVICE: Formatting of event log records has been corrected and improved
- SERVICE: SMTP message now contain a Message ID

Removed Features:

- 1.x Compatability Mode was removed. If you are upgrading from version 1.x then you will need to upgrade to version 2.30 first to preserve existing filters.

Version 2.30 3rd December 2003

New Features:

- EventSentry now monitors services
- Small enhancements in the management interface
- Filter Groups are now referred to as "Groups"
- Filter Groups can be added/removed in Remote Update, System Health and Filters tree
- PHP version of web interface added (ASP + PHP now supported)
- Added links to eventid.net, google, etc. to web files
- Sylog facility/level now mapped to event category for incoming syslog packets

Bug Fixes:

- Long date format problem in event viewer resolved
- Rename problem in GUI resolved
- Import Problem in GUI resolved

Version 2.21 5th November 2003

New Features:

- Syslog target now supports TCP in addition to UDP
- Remote Update speed improved
- Remote Update displays more informative error messages
- Remote Update now supports different credentials
- Added troubleshooting section in help file and GUI for every target
- Numerous enhancements in the management application
- Added EventSentry Quickstart Guide

Bug Fixes:

- Event records containing a single dot per line could cut off email
- Potential problems in wildcard feature
- Problem in built-in Event Log viewer with certain events resolved

Version 2.20 8th September 2003

New Features:

- (X)HTML emails are sent in multi part/alternative including a non-HTML version of the content. This is useful for email clients that are not capable of displaying HTML messages and for filtering (rules) in MS Outlook
- Wildcard support for filters was added
- The following additional variables for the SMTP target were included: $EVENTSOURCE, $EVENTCATEGORY, $EVENTTYPE, $EVENTID
- The $HOSTNAME variable is now supported in the SMTP Sender **email** field
- The built-in event log viewer allows you to query web sites to obtain information on a particular event
- Installer features (Management package) improved

Bug Fixes:

- The syslog hostname (as logged & reported by the syslog daemon) was truncated
- The welcome screen might show an invalid event log summary when connected to a remote machine
- Day/Time summaries are sometimes not read correctly on the fly, a service restart is necessary
- Changing the debug logging level requires a service restart
- Various improvements in the management application

Version 2.11 18th August 2003

New Features:

- A customizable Welcome Screen shows important information such as EventSentry news, event log summary and more
- Display speed of the built-in event viewer was greatly improved
- Invalid filter order is detected by management interface
- For better usability some menu options were renamed
- Sample ASP pages for querying an ODBC database were added
- On German Operating Systems EventSentry logs German messages to the event log

Bug Fixes:

- The service (agent) underwent a major security code review
- Memory usage was reduced and optimized
- Exclude filters using more than one target would not exclude events properly
- Drag & Drop would sometimes not work properly
- Creating filters or targets would fail when clicking with mouse instead of hitting enter
- Remote Update would sometimes not connect to certain machines
- Import Wizard would only import ~250 computers

- Size & positioning issues with desktop notification feature were corrected
- Potential problems in the network target have been resolved
- Problems with the summary notification have been resolved

Version 2.10 3rd July 2003

New Features:
- Custom event logs can now be managed and monitored

Bug Fixes:
- Fixed problems in the built-in event viewer and other minor problems

Version 2.01 18th June 2003

New Features:
- Added check box functionality for remote update
- All groups can now be updated at once

Bug Fixes:
- Fixed problems in the remote update feature (including service installation)
- Fixed problems in built-in Event Viewer

Version 2.00 5th June 2003

New Features:
- Added installer software
- **Completely redesigned** the management interface (GUI)
- Filters can be assigned to multiple targets
- Smtp target enhancements
- Added network target (ala net send)
- Added process target
- Added sound target
- Added desktop target

Bug Fix:
- Permanent summary notification on Windows NT4 might not work due to missing % TEMP% variable

Version 1.15 11th March 2003

New Features:
- Summary features events are now stored throughout service restarts
- Filter option "Filter Text" is not case sensitive anymore

Bug Fixes:
- "Stop processing other filters" didn't work in combination with summary feature under some circumstances
- Other minor bug fixes

Version 1.14 25th February 2003

New Features:
- Targets can now be enabled/disabled
- Multiple concurrent instances of the GUI are prevented

Bug Fixes:
- The "stop processing other filters" option didn't work correctly under some circumstances

- Bootscan would report too many events under some circumstances
- Using ODBC with a MS SQL Server would sometimes not write events to the database
- Excluding filters for particular targets would under some circumstances not work

Version 1.12 10th February 2003

Bug Fixes:

- The filter summary dialog box is cleared/reset under some circumstances
- A filter group update does not correctly set the active filter group on the target computer
- Sending emails with certain mail servers would fail

Version 1.10 4th February 2003

New Features:

- Introduced filter groups (see help for an explanation)
- Added the parallel ASCII-printer target
- Added email importance flags
- Added/improved computer list import/export
- Added GUI tips

Bug Fixes:

- A special kind of event log entry could crash the service
- Database DATETIME field was not used (text was used instead)
- Event log entries would sometimes be ignored
- Fixed GUI ALT-F4 issue.
- Other minor fixes in both GUI and service

Version 1.03 16th January 2003

New Features:

- Added the $HOSTNAME variable for the SMTP subject and FILE filename, added HTML customization options.

Bug Fix:

- If an event log is configured to "overwrite events as needed" and events are being overwritten (because the event log is full) then EventSentry can stop monitoring this particular event log under certain circumstances.

Version 1.02 22nd December 2002

Bug Fix:

- Under some circumstances the GUI could crash when performing any kind of batch update.
- The EventSentry service is not affected by this problem.

Version 1.00 19th December 2002
This was the initial public release of EventSentry.

8.3.1 Version Numbering System

This page explains how version numbers for EventSentry are created. A typical EventSentry version looks like this:

3.4.1

3	**Major Release Number**	This number is increased when EventSentry undergoes a major change, such as the introduction of the new web reports in v3.
.	**Separator**	
4	**Minor Release Number**	This number is increased when a new feature is introduced such as the support for log file monitoring.
1	**Sub-Release Number**	This number is increased when minor features have been added and bugs have been fixed.

9 Vorschläge und zukünftige Features

Zukünftige Features

Es sind viele Produkterweiterungen für EventSentry geplant. Bitte lesen Sie unsere Online-Roadmap für aktuelle Informationen über zukünftige Funktionen und in Entwicklung befindliche Funktionen.

Darüber hinaus wird EventSentry ständig überprüft, um mögliche Probleme zu lösen und bestehende Funktionen zu verbessern und zu optimieren. Wenn Sie weitere Vorschläge haben, klicken Sie bitte hier.

Vorschläge

EventSentry wird ständig überprüft und verbessert, und wir haben in der Vergangenheit viele Funktionen aus Kundenanregungen implementiert!

Wenn Sie eine Funktion vermissen und diese in einer zukünftigen Version sehen möchten, dann starten Sie bitte entweder eine Diskussion in unserem Feature Requests-Forum oder füllen Sie ein Feedback-Formular im Feedback-Menü aus und geben Sie alle oder einige der folgenden Informationen an:

- Eine Beschreibung des Merkmals
- Wie Ihnen diese Funktion helfen würde
- Ein Beispiel

Nachdem wir Ihre Anfrage geprüft haben, werden wir uns mit Ihnen in Verbindung setzen und Ihnen mitteilen, ob und wann wir Ihre Funktion zu EventSentry hinzufügen werden.

10 Credits

Beta Testers

We would like to thank all the individuals who helped us beta test EventSentry. We received many suggestions, ideas, and bug reports that enabled us to make EventSentry a better and more stable product.

Bug Discoverers

We thank everybody who took the time to report problems and/or bugs in EventSentry.

Suggestions

Many thanks to all individuals who sent us suggestions. We have implemented countless customer suggestions over the past years.

Development

We would like to thank Chris Maunder and others from CodeProject for providing sample classes.
Many thanks to PJ Naughter, for the many MFC libraries he provides to the community.
Many thanks to Stephan Brumme for Fast CRC32.

Individuals

Many thanks to Dina, Dieter, Juergen, Mariano, Dietward, Urban, Bud, Rick and Josh who are and have been helping us make EventSentry better, better and better!

Translations

Many thanks to Mihai, Eduardo and Jupiter Technology for helping us translate the web reporting into additional languages.

Projects

EventSentry uses components / software from the following projects:

- PostgreSQL
- The PostgreSQL ODBC driver
- Qt
- GeoIP
- cgminer
- RapidJSON
- Google Protocol Buffers
- PCRE
- Zlib
- Boost
- Crypto++
- WinPCAP
- Tomcat
- Play! Framework
- jQuery
- OpenJDK JRE

10.1 PostgreSQL

```
PostgreSQL is released under the PostgreSQL License, a liberal Open Source
license, similar to the BSD or MIT licenses.

PostgreSQL Database Management System
(formerly known as Postgres, then as Postgres95)

Portions Copyright © 1996-2019, The PostgreSQL Global Development Group

Portions Copyright © 1994, The Regents of the University of California

Permission to use, copy, modify, and distribute this software and its
documentation for any purpose, without fee, and without a written agreement
is hereby granted, provided that the above copyright notice and this
paragraph and the following two paragraphs appear in all copies.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR
DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING
LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS
DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON
AN "AS IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO
PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.
```

10.2 PostgreSQL ODBC

```
/*-------------------------------------------------------------------

  PSQLODBC.DLL - A library to talk to the PostgreSQL DBMS using ODBC.


  Copyright (C) 1998          Insight Distribution Systems
  Copyright (C) 1998 - 2011   The PostgreSQL Global Development Group

  Multibyte support was added by Sankyo Unyu Service, (C) 2001.

  The code contained in this library is based on code written by
  Christian Czezatke and Dan McGuirk, (C) 1996.


  This library is free software; you can redistribute it and/or modify
  it under the terms of the GNU Library General Public License as
  published by the Free Software Foundation; either version 2 of the
  License, or (at your option) any later version.

  This library is distributed in the hope that it will be useful, but
  WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTIBILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
  Library General Public License for more details.

  You should have received a copy of the GNU Library General Public
  License along with this library (see "license.txt"); if not, write to
  the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA
  02139, USA.


  How to contact the authors:

  email:   pgsql-odbc@postgresql.org
  website: http://pgfoundry.org/projects/psqlodbc


-------------------------------------------------------------------*/
```

10.3 Qt

EventSentry uses software from the Qt GUI Toolkit (v5.1x). The Qt source code used in EventSentry can be downloaded from here.

The Qt GUI Toolkit is Copyright (C) 2015 The Qt Company Ltd.
Contact: http://www.qt.io/licensing/

Qt is available under the LGPL.

```
                  GNU LESSER GENERAL PUBLIC LICENSE
                  Version 2.1, February 1999
```

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the

ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.
In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.
The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".
A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs

(which use some of those functions and data) to form executables.
  The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)
  "Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.
  Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.
  1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.
  You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
  2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
    a) The modified work must itself be a software library.
    b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
    c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
    d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.
    (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)
These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you

distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.
Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.
In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative

work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

  Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

  6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

  You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

    a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

    b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

    c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

    d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

    e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

  For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

  It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot

use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute 0the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made

generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.
This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

```
            How to Apply These Terms to Your New Libraries
  If you develop a new library, and you want it to be of the greatest
possible use to the public, we recommend making it free software that
everyone can redistribute and change.  You can do so by permitting
redistribution under these terms (or, alternatively, under the terms of the
ordinary General Public License).
  To apply these terms, attach the following notices to the library.  It is
safest to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least the
"copyright" line and a pointer to where the full notice is found.
    <one line to give the library's name and a brief idea of what it does.>
    Copyright (C) <year>  <name of author>
    This library is free software; you can redistribute it and/or
    modify it under the terms of the GNU Lesser General Public
    License as published by the Free Software Foundation; either
    version 2.1 of the License, or (at your option) any later version.
    This library is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
    Lesser General Public License for more details.
    You should have received a copy of the GNU Lesser General Public
    License along with this library; if not, write to the Free Software
    Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA  02110-1301  USA

Also add information on how to contact you by electronic and paper mail.
You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary.  Here is a sample; alter the names:
  Yoyodyne, Inc., hereby disclaims all copyright interest in the
  library `Frob' (a library for tweaking knobs) written by James Random Hacker.
  <signature of Ty Coon>, 1 April 1990
  Ty Coon, President of Vice
That's all there is to it!
```

10.4 GeoIP

This product includes GeoLite2 data created by MaxMind, available from http://www.maxmind.com.

10.5 cgminer

EventSentry uses code from the cgminer project to calculate sha256 checksums.

```
 * FIPS 180-2 SHA-224/256/384/512 implementation
 * Last update: 02/02/2007
 * Issue date:  04/30/2005
 *
 * Copyright (C) 2013, Con Kolivas <kernel@kolivas.org>
 * Copyright (C) 2005, 2007 Olivier Gay <olivier.gay@a3.epfl.ch>
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
```

```
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the project nor the names of its contributors
 *    may be used to endorse or promote products derived from this software
 *    without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
```

10.6 RapidJSON

```
Copyright (C) 2015 THL A29 Limited, a Tencent company, and Milo Yip.  All rights
reserved.

If you have downloaded a copy of the RapidJSON binary from Tencent, please note that
the RapidJSON binary is licensed under the MIT License.
If you have downloaded a copy of the RapidJSON source code from Tencent, please note
that RapidJSON source code is licensed under the MIT License, except for the third-
party components listed below which are subject to different license terms.  Your
integration of RapidJSON into your own projects may require compliance with the MIT
License, as well as the other licenses applicable to the third-party components
included within RapidJSON. To avoid the problematic JSON license in your own projects,
it's sufficient to exclude the bin/jsonchecker/ directory, as it's the only code under
the JSON license.
A copy of the MIT License is included in this file.

Other dependencies and licenses:

Open Source Software Licensed Under the BSD License:
--------------------------------------------------------------------

The msinttypes r29
Copyright (c) 2006-2013 Alexander Chemeris
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.
* Neither the name of  copyright holder nor the names of its contributors may be used
to endorse or promote products derived from this software without specific prior
written permission.
```

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS AND CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Open Source Software Licensed Under the JSON License:
---

json.org
Copyright (c) 2002 JSON.org
All Rights Reserved.

JSON_checker
Copyright (c) 2002 JSON.org
All Rights Reserved.

Terms of the JSON License:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

The Software shall be used for Good, not Evil.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Terms of the MIT License:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

10.7 Google Protocol Buffers

Copyright 2008 Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

    * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
    * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
    * Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

10.8 PCRE

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 8 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself. The data
in the testdata directory is not copyrighted and is in the public domain.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions, and a just-in-time compiler that can be used to optimize pattern matching. These are both optional features that can be omitted when the library is built.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel
Email local part: ph10
Email domain: cam.ac.uk

University of Cambridge Computing Service,
Cambridge, England.

PCRE JUST-IN-TIME COMPILATION SUPPORT

Written by: Zoltan Herczeg
Email local part: hzmester
Emain domain: freemail.hu

STACK-LESS JUST-IN-TIME COMPILER

Written by: Zoltan Herczeg
Email local part: hzmester
Emain domain: freemail.hu

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

10.9 Zlib

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

10.10 Boost

Boost Software License - Version 1.0 - August 17th, 2003
http://www.boost.org/users/license.html

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

10.11 Crypto++

Compilation Copyright (c) 1995-2016 by Wei Dai. All rights reserved.
This copyright applies only to this software distribution package
as a compilation, and does not imply a copyright on any particular
file in the package.

All individual files in this compilation are placed in the public domain by Wei Dai and other contributors.

I would like to thank the following authors for placing their works into the public domain:

Joan Daemen - 3way.cpp
Leonard Janke - cast.cpp, seal.cpp
Steve Reid - cast.cpp
Phil Karn - des.cpp
Andrew M. Kuchling - md2.cpp, md4.cpp

Colin Plumb - md5.cpp
Seal Woods - rc6.cpp
Chris Morgan - rijndael.cpp
Paulo Baretto - rijndael.cpp, skipjack.cpp, square.cpp
Richard De Moliner - safer.cpp
Matthew Skala - twofish.cpp
Kevin Springle - camellia.cpp, shacal2.cpp, ttmac.cpp, whrlpool.cpp, ripemd.cpp
Ronny Van Keer - sha3.cpp

The Crypto++ Library (as a compilation) is currently licensed under the Boost Software License 1.0.

10.12 WinPCAP

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the Politecnico di Torino, CACE Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.
This product includes software developed by the Kungliga Tekniska Högskolan and its contributors.
This product includes software developed by Yen Yen Lim and North Dakota State University.

Portions Copyright (c) 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors."
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Portions Copyright (c) 1983 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.
Portions Copyright (c) 1995, 1996, 1997 Kungliga Tekniska Högskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the Kungliga Tekniska Högskolan and its contributors."
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,

OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Portions Copyright (c) 1997 Yen Yen Lim and North Dakota State University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by Yen Yen Lim and North Dakota State University"
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Portions Copyright (c) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.
THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
Portions Copyright (C) 1995, 1996, 1997, 1998, and 1999 WIDE Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED
AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Portions Copyright (c) 1996 Juniper Networks, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that: (1) source code distributions retain the above copyright
notice and this paragraph in its entirety, (2) distributions including binary code
include the above copyright notice and this paragraph in its entirety in the
documentation or other materials provided with the distribution. The name of Juniper
Networks may not be used to endorse or promote products derived from this software
without specific prior written permission.
THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES,
INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
FOR A PARTICULAR PURPOSE.
Portions Copyright (c) 2001 Daniel Hartmeier All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:
- Redistributions of source code must retain the above copyright notice, this list of
conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list
of conditions and the following disclaimer in the documentation and/or other materials
provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTOR "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT
SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY
WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.
Portions Copyright 1989 by Carnegie Mellon.

Permission to use, copy, modify, and distribute this program for any purpose and
without fee is hereby granted, provided that this copyright and permission notice
appear on all copies and supporting documentation, the name of Carnegie Mellon not be
used in advertising or publicity pertaining to distribution of the program without
specific prior permission, and notice be given in supporting documentation that
copying and distribution is by permission of Carnegie Mellon and Stanford University.
Carnegie Mellon makes no representations about the suitability of this software for
any purpose. It is provided "as is" without express or implied warranty.

10.13 Tomcat, Play! Framework

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems,
and issue tracking systems that are managed by, or on behalf of, the

Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one

of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.
Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

10.14 jQuery

Copyright JS Foundation and other contributors, https://js.foundation/

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

10.15 OpenJDK JRE

GNU General Public License, version 2, **with the Classpath Exception**
The GNU General Public License (GPL)

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license
document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either

the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate
works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on

the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will

automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying
the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to
refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that
system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA
BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

"CLASSPATH" EXCEPTION TO THE GPL

Certain source files distributed by Oracle America and/or its affiliates are subject to the following clarification and special exception to the GPL, but only where Oracle has expressly included in the particular source file's header the words "Oracle designates this particular file as subject to the "Classpath" exception as provided by Oracle in the LICENSE file that accompanied this code."

Linking this library statically or dynamically with other modules is making a combined work based on this library. Thus, the terms and conditions of the GNU General Public License cover the whole combination.

As a special exception, the copyright holders of this library give you permission to link this library with independent modules to produce an executable, regardless of the license terms of these independent modules, and to copy and distribute the resulting executable under terms of your choice, provided that you also meet, for each linked independent module, the terms and conditions of the license of that module. An independent module is a module which is not derived from or based on this library. If you modify this library, you may extend this exception to your version of the library, but you are not obligated to do so. If you do not wish to do so, delete this exception statement from your version.