Kaseya 2

# Kontrollkonfiguration

## Benutzerhandbuch

**Versión R8**

**Deutsch**

**Oktober 23, 2014**

## Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

# Inhalt

# Einführung

Das **Monitoring**-Modul in **Virtual System Administrator™** stellt sechs Monitoring-Methoden von Rechnern und Protokolldateien zur Verfügung:

- **Meldungen** – Überwacht Ereignisse auf *Agent*-Rechnern.
- **Ereignisprotokoll-Meldungen** – Überwacht Ereignisse in den Ereignisprotokollen der *Agent*-Rechner.
- **Monitor-Sets** – Überwacht den Leistungsstatus auf *Agent*-Rechnern.
- **SNMP-Sets** – Überwachen den Leistungsstatus auf *Geräten ohne Agent*.
- **Systemprüfung** – Überwacht Ereignisse auf *Rechnern ohne Agent*.
- **Protokoll-Monitoring** – Überwacht Ereignisse in *Protokolldateien*.

In diesem Schnellstarthandbuch finden Sie eine Einführung in die fünf wichtigsten Monitoring-Methoden sowie eine allgemeine Einführung in das Thema "Benachrichtigungen". Informationen zum Monitoring von Protokolldateien finden Sie im Schnellstarthandbuch **Schrittweise Konfiguration von Log-Parsern** *(http://help.kaseya.com/webhelp/DE/VSA/R8/DE_logparsers_R8.pdf#zoom=70&navpanes=0)*.

**Hinweis:** Sie haben die Möglichkeit, über den **Standard Solution Package-Setup-Assistenten** *(http://help.kaseya.com/webhelp/DE/SSP/R8/index.asp#11220.htm)* *mithilfe von Richtlinien* schnell und einfach Monitoreinstellungen für eine Organisation zu übernehmen.

**Hinweis:** Eine Einführung in das Monitoring von Rechnern und Geräten *ohne Agents* finden Sie im **Network Monitor-Schnellstarthandbuch** *(http://help.kaseya.com/webhelp/DE/KNM/R8/DE_knmquickstart_R8.pdf#zoom=70&navpanes=0)*.

# Kontrollbedingungen und -konzepte

Für alle Monitoring-Methoden gelten die gleichen Meldungsverwaltungsbedingungen und -konzepte.

## Meldungen und Alarme

- **Meldungen** – Eine Meldung wird erstellt, wenn die Leistung eines Rechners oder Geräts mit einem vordefinierten Kriterium oder einer „Meldungsbedingung“ übereinstimmt.
- **Alarme** – *Alarme* sind eine grafische Methode, um den Benutzer zu benachrichtigen, dass ein *Alarm* aufgetreten ist. In vielen grafischen Anzeigen im VSA wird im Falle einer Meldung standardmäßig im VSA ein rotes Ampelsymbol angezeigt. Liegt kein Alarm vor, wird ein grünes Ampelsymbol angezeigt. Diese Symbole können angepasst werden.
- **Protokolle** – Zwei Protokolle unterscheiden zwischen Meldungen und Alarmen.
  - **Alarmprotokoll** – Verfolgt sämtliche *Alarme, die von einer Meldung erstellt wurden.*
  - **Monitor-Aktionsprotokoll** – Verfolgt sämtliche *erstellten Meldungen*, unabhängig davon, ob ein Alarm oder ein anderer Aktionstyp als Reaktion auf die Meldung ergriffen wurde.

## Aktionen

**Erstellen eines Alarms** ist nur ein *Aktionstyp*, der ergriffen werden kann, wenn eine Meldung auftritt. Die anderen Aktionstypen sind Benachrichtigungen. Diese umfassen **das Senden einer E-Mail** oder **Erstellen eines Tickets**. Ein vierter Aktionstyp ist das **Ausführen eines Agent-Verfahrens**, um automatisch auf die Meldung zu reagieren. Diese vier Arten von Aktionen werden als **ATSE-Code** bezeichnet. Der ATSE-Code gibt an, welche Arten von Aktionen für die definierte Meldung aktiv sind, unabhängig davon, ob sie einer Rechner-ID, einer Gruppen-ID oder einem SNMP-Gerät zugewiesen sind.

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = Agent-Verfahren ausführen
- E = **E**-Mail-Empfänger

Keine der ATSE-Aktionen wird benötigt. Die Meldung und die ATSE-Aktion (einschließlich keine Aktion) werden im Bericht Info Center > Monitor – Monitor-Aktionsprotokoll ausgegeben.

## Meldungstypen

Zu den Arten von Meldungen gehören:

- Ermittlung > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/R8/index.asp#1944.htm)*
- Sicherung > Sicherungsmeldungen
- Monitor > Meldungen – Dies sind spezielle „festgelegte“ Meldungen, die sofort auf einen Rechner angewendet werden können.
- Monitor > Monitor zuweisen
- Monitor > SNMP-Traps-Meldung
- Monitor > SNMP zuweisen
- Monitor > Systemprüfungen
- Monitor > Analyse-Übersicht
- Monitor > Analysesätze zuweisen
- Patch-Management > Patch-Meldungen
- Fernsteuerung > Externe Meldungen
- Sicherheit > Alarmsätze anwenden

Andere Zusatzmodule verfügen über Meldungen, die hier nicht aufgelistet sind.

## Sechs Monitoring-Methoden

Jede der sechs Monitoring-Methoden in **Virtual System Administrator™** ist entweder *ereignisbasiert* oder *statusbasiert*.

- Ereignisbasiert
  - **Meldungen** – Überwacht Ereignisse auf *Agent*-Rechnern.
  - **Ereignisprotokoll-Meldungen** – Überwacht Ereignisse in den Ereignisprotokollen der *Agent*-Rechner
  - **Systemprüfung** – Überwacht Ereignisse auf Rechnern *ohne Agent*
  - **Protokoll-Monitoring** – Überwacht Ereignisse in *Protokolldateien*.
- Statusbasiert
  - **Monitor-Sets** – Überwacht den Leistungsstatus auf *Agent*-Rechnern
  - **SNMP-Sets** – Überwachen den Leistungsstatus auf *Geräten ohne Agent*

## Ereignisbasierte Meldungen

Meldungen, Systemprüfung, **Ereignisprotokoll-Meldungen** *(siehe 7)* und Protokoll-Monitoring stellen **ereignisbasierte Meldungen** dar, die nur vereinzelt auftreten. So kann beispielsweise eine Sicherung fehlschlagen. Auch wenn die Sicherung später erfolgreich ist, ist das Fehlschlagen ein historisches Ereignis im Alarmprotokoll. Wird ein Alarm für diesen Ereignistyp erstellt, *bleibt der Alarm im Alarmprotokoll „offen", selbst wenn die Meldungsbedingung wiederhergestellt ist.* Sie verwenden in der Regel die Seite Alarmübersicht, um Alarme zu überprüfen, die von ereignisbasierten Meldungen erstellt wurden. Wurde das Problem gelöst, „schließen" Sie den Alarm.

Ereignisbasierte Meldungen sind für gewöhnlich leichter zu konfigurieren, da die einzigen Möglichkeiten darin bestehen, ob ein oder mehrere Ereignis(se) innerhalb einer vorgegebenen Zeitspanne eingetreten sind oder nicht.

## Statusbasierte Meldungen

Monitor-Set-Zähler, -Dienste und -Prozesse sowie SNMP-Set-Objekte liegen gegenwärtig entweder innerhalb ihres erwarteten Statusbereichs oder außerhalb dieses Bereichs, worauf *dynamisch* durch grüne oder rote Alarmsymbole in Dashlet-Überwachungen hingewiesen wird. Diese werden als **statusbasierte Meldungen** bezeichnet.

- *Falls gegenwärtig eine Meldungsbedingung vorliegt, wird in Monitor-Dashlets ein rotes Alarmsymbol angezeigt.*
- *Falls gegenwärtig keine Meldungsbedingung vorliegt, wird in Kontroll-Dashlets ein grünes Alarmsymbol angezeigt.*

Wenn Sie einen Alarm für statusbasierte Meldungen erstellen, werden Alarmeinträge im Alarmprotokoll erstellt, die den ereignisbasierten Alarmen entsprechen. Diese können dann geschlossen werden. Da statusbasierte Meldungen jedoch in der Regel dynamisch in eine Meldungsbedingung ein- und aus dieser austreten, empfiehlt es sich, nicht jedes Mal, wenn dies geschieht, einen Alarm zu erstellen. Verwenden Sie stattdessen das Dashlet Netzwerkstatus, um den *aktuellen Status* der statusbasierten Meldungen zu identifizieren. Sobald das Problem auf dem Rechner oder Gerät behoben wurde, wechselt der Meldungsstatus automatisch auf ein grünes Symbol zurück. Sie müssen die Meldung in diesem Dashlet nicht manuell „schließen".

> **Hinweis:** Wenn Sie herkömmliche Alarme speziell für Monitor-Sets und Offline-Meldungen erstellen, können diese beiden Meldungstypen bei Wiederherstellung geschlossen werden. Weitere Informationen erhalten Sie im Kontrollkästchen **Autom. Schließen für Alarme und Tickets aktivieren** auf der Seite System > Konfigurieren.

Die Konfiguration von statusbasierten Alarmen erfordert in der Regel etwas mehr Überlegung als die von ereignisbasierten Alarmen, da mit diesen der Grad der Leistung gemessen wird und nicht nur ein einfaches Versagen.

## Dashboards und Dashlets

Die Seite **Dashboard-Liste** ist die primäre Oberfläche des VSA, um Kontrolldaten, einschließlich Meldungen und Alarme, anzuzeigen. Über die Seite **Dashboard-Liste** werden konfigurierbare Kontrollfenster namens **Dashboard-Ansichten** gepflegt. Jedes Dashboard enthält einen oder mehrere Fensterbereiche mit Kontrolldaten, die als **Dashlets** bezeichnet werden. Jeder VSA-Benutzer kann seine eigenen angepassten Dashboards erstellen. Zu den Arten von Dashlets gehören:

- Alarmliste
- Alarm-Netzwerkstatus
- Alarm Rotator
- Alarm Ticker
- Netzwerkstatus
- Gruppenalarmstatus
- Monitor-Set-Status
- Monitorstatus
- Rechner online
- Top N – Monitoralarmliste

## Überprüfen von Alarmen

Alle Meldungsbedingungen, für die das Kontrollkästchen **Alarm erstellen** aktiviert ist – sowohl status- als auch ereignisbasierte Alarme – werden im **Alarmprotokoll** aufgezeichnet. Ein im Alarmprotokoll aufgeführter Alarm weist nicht unbedingt auf den *aktuellen Status* eines Rechners oder Geräts hin, sondern ist vielmehr eine *Aufzeichnung* eines Alarms, der *in der Vergangenheit* aufgetreten ist. Ein Alarmprotokoll-Datensatz bleibt solange `Open`, bis Sie ihn schließen.

Erstellte Alarme können geprüft, `geschlossen` oder **gelöscht...** werden. Verwenden Sie hierzu die folgenden Optionen:

- Monitor > Alarm-Übersicht
- Monitor > Dashboard-Liste > beliebiges Alarm-Übersichtsfenster in einem Dashlet
- Agent > Agent-Protokolle > Alarmprotokoll
- Live Connect > Agent-Daten > Agent-Protokolle > Alarmprotokoll

Erstellte Alarme können auch mit folgenden Optionen geprüft werden:

- Monitor > Dashboard-Liste > Alarmliste
- Monitor > Dashboard-Liste > Alarm-Netzwerkstatus
- Monitor > Dashboard-Liste > Alarm Rotator
- Monitor > Dashboard-Liste > Alarm Ticker
- Monitor > Dashboard-Liste > Gruppenalarmstatus
- Monitor > Dashboard-Liste > Monitor-Set-Status
- Monitor > Dashboard-Liste > Monitorstatus
- Monitor > Dashboard-Liste > Top N – Anzahl der Monitoralarme
- Monitor > Dashboard-Liste > KES-Status
- Monitor > Dashboard-Liste > KES-Bedrohungen
- Info Center > Reporting > Berichte > Monitoring > Protokolle > Alarmprotokoll
- Info Center > Reporting > Berichte > Monitoring > Monitor-Aktionsprotokoll

## Prüfen der Leistung (mit oder ohne Erstellen von Alarmen)

Sie können den *aktuellen Status* der Leistungsergebnisse von Monitor-Sets und SNMP-Sets *mit oder ohne Erstellen von Alarmen* prüfen. Verwenden Sie hierfür folgende Optionen:

- Monitor > Live Counter
- Monitor > Monitor-Protokoll
- Monitor > SNMP-Protokoll

- Monitor > Dashboard > Netzwerkstatus
- Monitor > Dashboard > Gruppenalarmstatus
- Monitor > Dashboard > Monitor-Set-Status
- Info Center > Reporting > Berichte > Monitoring > Protokolle

### Alarme aussetzen

Das Auslösen von Alarmen kann ausgesetzt werden. Über die Seite **Alarme aussetzen** können Sie Alarme für vorgegebene Zeitspannen, einschließlich wiederkehrender Zeitperioden, aussetzen. Dadurch können Sie Aufrüstungs- und Pflegeaufgaben durchführen, ohne einen Alarm auszulösen. Wenn Alarme für eine Rechner-ID ausgesetzt sind, *sammelt der Agent weiterhin Daten, generiert jedoch keine zugehörigen Alarme*.

### Gruppenalarme

Alarme für Meldungen, Ereignisprotokoll-Meldungen, Systemprüfung und Protokoll-Monitoring werden automatisch einer **Gruppenalarm**-Kategorie zugewiesen. Beim Auslösen eines Alarms wird auch der zugehörige Gruppenalarm ausgelöst. Die Gruppenalarm-Kategorien für Monitor-Sets und SNMP-Sets werden bei der Definition der Sets manuell zugewiesen. Gruppenalarme werden im Dashlet Gruppenalarmstatus der Seite Monitor > **Dashboard-Liste** angezeigt. Sie können neue Gruppen über die Registerkarte **Gruppenalarm-Spaltennamen** in Monitor > Monitorlisten erstellen. Gruppenalarmspalten werden Monitor-Sets über Monitor-Set definieren zugewiesen.

# Benachrichtigungen

Über die Seite **Meldungen** können Sie im Handumdrehen Meldungen für typische Meldungsbedingungen definieren, die in einer IT-Umgebung vorgefunden werden. So ist beispielsweise geringer Plattenspeicherplatz ein häufiges Problem bei verwalteten Rechnern. Bei Auswahl des Meldungstyps `Low Disk` wird ein einzelnes zusätzliches Feld angezeigt, in dem Sie den `% free space`-Schwellenwert definieren können. Anschließend können Sie diese Meldung unmittelbar auf jede auf der Seite **Meldungen** angezeigte Rechner-ID anwenden und die Reaktion auf die Meldung festlegen.

Es stehen Ihnen verschiedene Arten von Alarmen zur Verfügung.

## Alarmtypen

- Auf der Seite **Meldungen – Übersicht** wird angezeigt, welche Meldungen für welchen Rechner aktiviert sind. Sie können Einstellungen anwenden oder löschen bzw. aktivierte Meldungseinstellungen kopieren.
- Die Seite **Meldungen – Agent-Status** löst eine Meldung aus, wenn ein Agent offline ist, erstmals online geht, oder wenn jemand die Fernsteuerung des ausgewählten Rechners deaktiviert hat.
- Die Seite **Meldungen – Anwendungsänderungen** löst eine Meldung aus, wenn auf ausgewählten Rechnern eine Anwendung installiert oder entfernt wird.
- Die Seite **Meldungen – Dateien abrufen** löst eine Meldung aus, wenn der Befehl **getFile()** oder **getFileInDirectoryPath()** eines Verfahrens ausgeführt und nach dem Hochladen der Datei festgestellt wird, dass diese sich von der auf dem Kaseya Server gespeicherten Kopie unterscheidet. Liegt auf dem Kaseya Server keine vorherige Kopie vor, wird der Alarm erstellt.
- Die Seite **Meldungen – Hardwareänderungen** löst eine Meldung aus, wenn sich die Hardwarekonfiguration auf den ausgewählten Rechnern ändert. Die ermittelten Hardwareänderungen umfassen das Hinzufügen oder Entfernen von RAM, PCI-Geräten und Plattenlaufwerken.
- Die Seite **Meldungen – Geringer Plattenspeicher** löst eine Meldung aus, wenn der verfügbare Plattenspeicher unter einen vorgegebenen Prozentsatz des freien Plattenspeicherplatzes fällt.
- Die Seite **Meldungen – Ereignisprotokolle** löst eine Meldung aus, wenn ein Ereignisprotokolleintrag für einen ausgewählten Rechner vorgegebenen Kriterien entspricht. Nach Auswahl des **Ereignisprotokolltyps** können Sie die durch den **Ereignissatz** und die **Ereigniskategorie** vorgegebenen Meldungsbedingungen filtern.
- Die Seite **Meldungen – Fehlgeschlagene Agent-Verfahren** löst eine Meldung aus, wenn die Ausführung eines Agent-Verfahrens auf einem verwalteten Rechner fehlschlägt.
- Die Seite **Meldungen – Schutzverletzung** löst eine Meldung aus, wenn eine Datei geändert wird oder eine Schutzverletzung auf einem verwalteten Rechner festgestellt wird.
- Die Seite **Neuer Agent installiert** löst eine Meldungen aus, wenn auf einem verwalteten Rechner ein neuer Agent durch ausgewählte *Rechnergruppen* installiert wird.
- Die Seite **Meldungen – Patch-Meldung** löst eine Meldung für Patch-Managementereignisse auf verwalteten Rechnern aus.
- Die Seite **Meldungen – Sicherungsmeldung** löst eine Meldung für Sicherungsereignisse auf verwalteten Rechnern aus.
- Die Seite **Meldungen – System** löst eine Meldungen für ausgewählte Ereignisse auf dem *Kaseya Server* aus.

## So erstellen Sie einen Alarm:

Das gleiche allgemeine Verfahren gilt für alle Alarmtypen.

1. Wählen Sie eine Alarmfunktion aus der Dropdown-Liste **Alarmfunktion auswählen** aus.

2. Aktivieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Meldungsbedingung die entsprechenden Aktionen auszuführen:
   - **A**larm erstellen
   - **T**icket erstellen
   - **S**kript ausführen
   - **E**-Mail-Empfänger
3. Legen Sie weitere E-Mail-Parameter fest.
4. Legen Sie weitere alarmspezifische Parameter fest. Diese sind abhängig von der jeweils ausgewählten Alarmfunktion unterschiedlich.
5. Markieren Sie die Seitenzeilen, auf die der Alarm angewendet werden soll.
6. Klicken Sie auf die Schaltfläche **Apply**.

### So brechen Sie einen Alarm ab:

1. Wählen Sie eine oder mehrere Seitenzeilen aus.
2. Klicken Sie auf die Schaltfläche **Löschen**.
   Die neben der Seitenzeile aufgeführten Alarminformationen werden gelöscht.

# Ereignisprotokoll-Benachrichtigungen

Auf der Seite **Ereignisprotokollbenachrichtigungen** finden Sie erweiterte Benachrichtigungsarten, für die eine spezielle Konfiguration nötig ist. Ausgangspunkt ist ein gutes Verständnis von **Ereignisprotokollen**.

# Ereignisprotokolle

Ein **Ereignisprotokolldienst** wird auf Windows-Betriebssystemen ausgeführt. (Er steht nicht für Win9x zur Verfügung.) Über den Ereignisprotokolldienst können Ereignisprotokollnachrichten von Windows-basierten Programmen und Komponenten ausgegeben werden. Diese Ereignisse werden in den auf jedem Rechner gespeicherten Ereignisprotokollen gespeichert. Die Ereignisprotokolle verwalteter Rechner können in der Kaseya Server-Datenbank gespeichert werden und als Basis aller Meldungen und Berichte dienen. Sie können auch archiviert werden.

Abhängig vom jeweiligen Betriebssystem stehen die folgenden **Ereignisprotokolltypen** zur Verfügung:

- Anwendungsprotokoll
- Sicherheitsprotokoll
- Systemprotokoll
- Verzeichnisdienstprotokoll
- Dateireplikationsdienstprotokoll
- DNS-Serverprotokoll

Windows-Ereignisse werden über die folgenden **Ereignisprotokollkategorien** weiter klassifiziert:

- Fehler
- WARNUNG
- Informationen
- Erfolgs-Audit
- Fehler-Audit
- Kritisch – betrifft nur Vista, Windows 7 und Windows Server 2008
- Ausführlich – betrifft nur Vista, Windows 7 und Windows Server 2008

Ereignisprotokolle werden von den folgenden VSA-Seiten verwendet bzw. referenziert:

- Monitor > Agent-Protokolle
- Monitor > Ereignisprotokoll-Meldungen
- Monitor > Ereignisprotokoll-Meldungen > Ereignissätze bearbeiten
- Monitor > Listen nach Scan aktualisieren
- Agent > Protokollverlauf
- Agent > Ereignisprotokolleinstellungen
- Agent > Agent-Protokolle
- Berichte > Protokolle
- Live-Connect > Ereignisanzeige
- Schnellanzeige > Ereignisanzeige
- System > Datenbanksichten > vNtEventLog

# Erstellen von Ereignissätzen aus Ereignisprotokolleinträgen

Ein Monitor-Assistent-  -Symbol wird neben dem Ereignisprotokolleintrag im VSA und in **Live Connect** angezeigt. Wenn Sie den Cursor über das Monitorassistent-Symbol eines Protokolleintrags bewegen, wird ein Assistent angezeigt. Der Assistent ermöglicht Ihnen auf Basis dieses Protokolleintrags ein neues Kriterium für den Ereignissatz zu erstellen. Das neue Ereignissatz-Kriterium kann zu jedem neuen oder bestehenden Ereignissatz hinzugefügt werden. Der neue oder geänderte Ereignissatz wird sofort auf den Rechner angewendet, der die Quelle dieses Protokolleintrags war. Wird ein bestehender Ereignissatz geändert, so sind alle Rechner davon betroffen, denen dieser Ereignissatz zugeordnet ist. Das Monitor-Assistent-Symbol wird angezeigt in:

- Agent > Agent-Protokolle
- Live Connect > Ereignisanzeige
- Live Connect > Agent-Daten > Ereignisprotokoll

Siehe Monitor > Ereignisprotokoll-Meldungen – hier ist jedes im Assistenten angezeigte Feld beschrieben.

# Beispiel-Ereignissätze

Es wird eine stetig wachsende Liste von Beispiel-Ereignissätzen zur Verfügung gestellt. Die Namen der Beispiel-Ereignissätze beginnen mit ZC. Sie können die Beispiel-Ereignissätze bearbeiten. Doch empfehlenswerter ist es, einen Beispiel-Ereignissatz zu kopieren und die Kopie zu bearbeiten. Die Beispiel-Ereignissätze werden bei jeder Aktualisierung der Beispielsätze im Rahmen eines Pflegezyklus überschrieben.

# Ereignissätze zuweisen

Sie können Ereignis-Sets über die Seite "Monitor > Ereignisprotokollbenachrichtigungen" bestimmten Zielrechner-IDs zuweisen.

### Ereignisprotokollalarm erstellen

1. Wählen Sie auf der Seite Monitor > **Ereignisprotokoll-Meldungen** die Registerkarte **Ereignissatz zuweisen** aus.
2. Wählen Sie ein Element aus der Dropdown-Liste **Ereignisprotokolltyp auswählen** aus.

3. Wählen Sie den Ereignissatz-Filter aus, der zum Filtern der Ereignisse verwendet wird, die Meldungen auslösen. Standardmäßig ist `<All Events>` ausgewählt.

   **Hinweis:** Sie können einen neuen Ereignissatz erstellen oder einen vorhandenen Ereignissatz durch Klicken auf die Schaltfläche **Bearbeiten** bearbeiten.

4. Aktivieren Sie das Kontrollkästchen neben einer der folgenden **Ereigniskategorien**:
   - Fehler
   - WARNUNG
   - Informationen
   - Erfolgs-Audit
   - Fehler-Audit
   - Kritisch – betrifft nur Vista, Windows 7 und Windows Server 2008
   - Ausführlich – betrifft nur Vista, Windows 7 und Windows Server 2008

   **Hinweis:** Rote Zeichen zeigen eine deaktivierte Protokollierung an. Die Sammlung der Ereignisprotokolle kann vom VSA für einen bestimmten Rechner deaktiviert worden sein. Dies richtet sich nach den mit Agent > Ereignisprotokolleinstellungen definierten Einstellungen. Für bestimmte Rechner sind möglicherweise nicht alle Ereigniskategorien (EWISFCV) verfügbar, wie beispielsweise die Ereigniskategorien Kritisch und Verbose. **Ereignisprotokoll-Meldungen werden auch generiert, wenn die Ereignisprotokolle nicht von VSA gesammelt werden.**

5. Geben Sie die *Häufigkeit* der Meldungsbedingung an, die zum Auslösen einer Meldung erforderlich ist:
   - **Warnen, wenn dieses Ereignis ein einziges Mal eintritt**
   - **Warnen, wenn dieses Ereignis <N> Mal innerhalb von <N> <Perioden>** eintritt.
   - **Warnen, wenn dieses Ereignis nicht innerhalb von <N> <Perioden>** eintritt.
   - **Zusätzliche Alarme nicht beachten für <N> <Perioden>**.
6. Klicken Sie auf die Optionsfelder **Hinzufügen** oder **Ersetzen**.
   - Durch **Hinzufügen** wird der ausgewählte Ereignissatz zur Liste der Ereignissätze hinzugefügt, die bereits ausgewählten Rechnern zugeordnet sind.
   - Durch **Ersetzen** wird die gesamte Liste an zugewiesenen Ereignissätzen auf ausgewählten Rechnern mit dem ausgewählten Ereignissatz ersetzt.
7. Wählen Sie die Registerkarte **Meldungsaktionen einrichten**, um die Aktionen auszuwählen, die als Reaktion auf die angegebenen Meldungsbedingungen ergriffen werden.
8. Klicken Sie auf **Anwenden**, um die ausgewählten Ereignistypmeldungen ausgewählten Rechner-IDs zuzuweisen.

   **Hinweis:**Klicken Sie auf **Entfernen**, um alle Ereignissatzmeldungen von ausgewählten Rechner-IDs zu entfernen. Sie müssen nicht auf die Schaltfläche **Anwenden** klicken.

# Ereignissätze bearbeiten

In Schritt 2 des obigen Verfahrens **Ereignisprotokollalarm erstellen** werden Sie aufgefordert, einen Ereignissatz auszuwählen. Nachstehend wird erläutert, wie Sie Ereignissätze bearbeiten.

**Ereignissätze bearbeiten** filtert das Auslösen von Meldungen basierend auf dem Monitoring von Ereignissen in Ereignisprotokollen, die durch das Windows-Betriebssystem eines verwalteten Rechners gepflegt werden. Sie können einer Rechner-ID mehrere Ereignissätze zuweisen.

Ereignissätze enthalten eine oder mehrere **Bedingungen**. Jede Bedingung enthält Filter für verschiedene Felder in einem **Ereignisprotokolleintrag**. Die Feld sind **Quelle**, **Kategorie**, **Ereignis-ID**, **Benutzer** und **Beschreibung**. Ein **Ereignisprotokoll** *(siehe 7)*eintrag muss alle Feldfilter einer Bedingung erfüllen, um als Übereinstimmung zu gelten. Ein Feld mit einem Sternchen (*) bedeutet, dass jede Zeichenfolge, selbst eine leere Zeichenfolge, als Übereinstimmung gilt. Eine Übereinstimmung auch nur *einer* der Bedingungen in einem Ereignissatz ist ausreichend, um eine Meldung für einen Rechner auszulösen, auf den dieser Ereignissatz angewendet wurde.

**Hinweis:** Werden einem Ereignissatz zwei Bedingungen hinzugefügt, so werden diese normalerweise als eine OR-Anweisung interpretiert. Wird für eine eine Übereinstimmung erzielt, wird ein Alarm ausgelöst. Die Ausnahme ist, wenn die Option **Warnen, wenn dieses Ereignis nicht innerhalb von<N> <Perioden> eintritt** aktiviert wurde. In diesem Falls sollten die zwei Bedingungen als eine AND-Anweisung interpretiert werden. Beide Bedingungen dürfen *nicht* innerhalb der angegebenen Zeitspanne auftreten, um eine Meldung auszulösen.

**Hinweis:** Sie können Ereignisprotokolle direkt anzeigen. Klicken Sie auf einem Windows-Rechner auf **Start**, **Systemsteuerung**, **Verwaltung** und dann auf **Ereignisanzeige**. Klicken Sie auf **Anwendung**, **Sicherheit** oder **System**, um die Ereignisse in diesem Protokoll anzuzeigen. Doppelklicken Sie auf ein Ereignis, um dessen **Eigenschaften**-Fenster anzuzeigen. Sie können Text im **Eigenschaften**-Fenster jedes Ereignisses kopieren und in die **Ereignissatz bearbeiten**-Felder einfügen.

### So erstellen Sie einen neuen Ereignissatz:

1. Wählen Sie die Seite Monitor > **Ereignisprotokoll-Meldungen** aus.
2. Wählen Sie einen **Ereignisprotokolltyp** aus der zweiten Dropdown-Liste.
3. Wählen Sie `<New Event Set>` aus der Dropdown-Liste **Ereignisse für Übereinstimmungen oder Übergehung definieren**. Das Popup-Fenster **Ereignissatz bearbeiten** wird eingeblendet. Zum Erstellen eines neuen Ereignissatzes haben Sie die folgenden Möglichkeiten:
   - Eingabe eines neuen Namens und Klicken auf die Schaltfläche **Neu**
   - Einfügen der Ereignissatzdaten als Text
   - Importieren der Ereignissatzdaten aus einer Datei
4. Wenn Sie einen neuen Namen eingeben und auf **Neu** klicken, werden im Fenster **Ereignissatz bearbeiten** die fünf zum Filtern von Ereignissen verwendeten Eigenschaften angezeigt.
5. Klicken Sie auf **Hinzufügen**, um dem Ereignissatz ein neues Ereignis hinzuzufügen.
6. Klicken Sie auf **Übergehen**, um ein Ereignis anzugeben, das *keinen* Alarm auslösen sollte.
7. Sie können Ereignissätze wahlweise **umbenennen**, **löschen** oder **exportieren**.

### Übergehen-Bedingungen

Wenn ein Ereignisprotokolleintrag einer oder mehreren **Übergehen-Bedingungen** in einem Ereignissatz entspricht, wird *durch keinen Ereignissatz* ein Alarm ausgelöst, selbst wenn mehrere Ereignissätze einem Ereignisprotokolleintrag entsprechen. Da Übergehen-Bedingungen *alle Ereignissätze* außer Kraft setzen, ist es ratsam, nur einen Ereignissatz für alle Übergehen-Bedingungen zu definieren. Auf diese Weise müssen Sie nur an einer Stelle suchen, wenn Sie den Verdacht haben, dass eine Übergehen-Bedingung das Verhalten aller Ihrer Meldungen beeinflusst. Sie müssen den Ereignissatz mit einer Übergehen-Bedingung zunächst einer Rechner-ID zuweisen, bevor diese Bedingung alle anderen Ereignissätze, die der gleichen Rechner-ID zugewiesen wurden, außer Kraft setzen kann.

*Übergehen-Bedingungen setzen nur Ereignisse des gleichen Protokolltyps außer Kraft.* Wenn Sie also ein „Übergehen-Set“ für alle Übergehen-Bedingungen erstellen, muss dieses mehrmals auf die gleiche Rechner-ID angewendet werden, nämlich *für jeden Protokolltyp einmal*. Ein Übergehen-Satz, der beispielsweise nur auf Ereignisse des Systemprotokolltyps angewendet wurde, setzt keine Ereignisbedingungen des Anwendungs- und Sicherheitsprotokolltyps außer Kraft.

1. Wählen Sie die Seite Monitor > **Ereignisprotokoll-Meldungen** aus.

2. Aktivieren Sie das Kontrollkästchen **Fehler** und wählen Sie `<All Events>` aus der Ereignissatzliste aus. Klicken Sie auf **Anwenden**, um allen ausgewählten Rechner-IDs diese Einstellung zuzuweisen. Damit weisen Sie das System an, für jeden Fehlerereignistyp eine Meldungen zu generieren. Notieren Sie den zugewiesenen Protokolltyp.
3. Erstellen Sie einen „Übergehen-Ereignissatz“, der alle Ereignisse festlegt, die Sie übergehen möchten, und weisen Sie diesen den gleichen Rechner-IDs zu. Der Protokolltyp muss dem in Schritt 2 angegebenen Protokolltyp entsprechen.

### Sternchen (*) als Stellvertreterzeichen verwenden

Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.Zum Beispiel:

```
*yourFilterWord1*yourFilterWord2*
```

Dies ergäbe eine Übereinstimmung und würde einen Alarm für ein Ereignis mit der folgenden Zeichenfolge auslösen:

```
"This is a test. yourFilterWord1 as well as yourFilterWord2 are in the description."
```

### Bearbeitungsereignisse exportieren und importieren

Sie können Ereignissatz-Datensätze als XML-Dateien exportieren und aus diesen importieren.

- Sie können einen vorhandenen Ereignissatz-Datensatz über das Popup-Fenster **Ereignissatz bearbeiten** in eine XML-Datei *exportieren*.
- Sie können eine Ereignissatz-XML-Datei durch Auswahl des Werts `<Import Event Set>` oder `<New Event Set>` aus der Ereignissatz-Dropdown-Liste *importieren*.

Beispiel:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<event_sets>
 <set_elements setName="Test Monitor Set" eventSetId="82096018">
   <element_data ignore="0" source="*SourceValue*"
     category="*CategoryValue*" eventId="12345"
     username="*UserValue*" description="*DescriptionValue*"/>
 </set_elements>
</event_sets>
```

# Systemprüfungen

Der VSA kann auch Rechner überwachen, *auf denen kein Agent installiert ist*. Diese Funktion wird auf einer einzelnen Seite namens **Systemprüfung** durchgeführt. Rechner ohne einen Agent werden als **externe Systeme** bezeichnet. Einem Rechner mit einem Agent wird die Aufgabe zugewiesen, die Systemprüfung auf dem externen System durchzuführen. Durch eine Systemprüfung wird normalerweise festgestellt, ob ein externes System verfügbar ist oder nicht. Es gibt folgende Arten von Systemprüfungen: Webserver, DNSserver, Portverbindung, Ping und benutzerdefiniert.

# Monitor-Sets

**Monitorsets** verwenden Windows-basierte **Leistungszähler**, um Informationen darüber zu liefern, wie gut Ihr Betriebssystem bzw. Anwendungen, Services oder Treiber funktionieren. Zählerdaten können Ihnen helfen, Engpässe im System zu identifizieren und die System- und Anwendungsleistung genau abzustimmen. Ein Server kann beispielsweise weiterhin arbeiten, ohne dass Fehler oder Warnungen in den Ereignisprotokollen generiert werden. Dennoch beschweren sich die Benutzer, dass die Reaktionszeit des Servers langsam ist.

> **Hinweis:** Die Zähler in VSA-Monitorsets basieren nicht auf Protokolldateien, sondern auf statusbasierten Echtzeitdaten. Weitere Informationen finden Sie unter **Alarme** *(siehe 2)*.

### Leistungsobjekte, Instanzen und Zähler

Beim Einrichten von Zählerschwellenwerten in **Monitor-Sets** *(siehe 12)* ist zu beachten, wie Windows und der VSA die zu überwachenden Komponenten identifizieren:

- **Leistungsobjekt** – Eine logische Sammlung von Zählern, die mit einer Ressource oder einen Dienst verknüpft sind, der überwacht werden kann. Zum Beispiel: Prozesse, Arbeitsspeicher, physikalische Festplatten und Server haben alle ihre eigenen Sätze vordefinierter Zähler.
- **Leistungsobjekt-Instanz** – Ein Begriff, mit dem zwischen mehreren Leistungsobjekten des gleichen Typs auf einem Computer unterschieden wird. Zum Beispiel: mehrere Prozessoren oder mehrere physikalische Festplatten. Der VSA lässt Sie dieses Feld überspringen, falls nur eine Instanz eines Objekts vorliegt.
- **Leistungszähler** – Ein mit einem Leistungsobjekt und gegebenenfalls mit der Instanz verknüpftes Datenelement. Jeder ausgewählte Zähler stellt einen Wert das, der einem bestimmen Aspekt der Leistung entspricht, die für das Leistungsobjekt und die Instanz definiert wurden.

# Monitor-Sets

Ein Monitor-Set ist ein Satz von **Zählerobjekten**, **Zählern**, **Zählerinstanzen**, **Diensten** und **Prozessen**, anhand derer die Leistung von Rechnern überwacht werden kann. In der Regel wird jedem/jeder Objekt/Instanz/Zähler, Dienst oder Prozess in einem Monitor-Set ein Schwellenwert zugewiesen. Sie können Alarme festlegen, die ausgelöst werden, wenn einer der Schwellenwerte im Monitor-Set überschritten wird. Ein Monitor-Set sollte als eine logische Gruppierung von Faktoren, die überwacht werden sollen, verstanden werden. Eine solche logische Gruppierung könnte beispielsweise die Überwachung alle zum Ausführen eines Exchange Server erforderlichen Zähler und Dienste sein. Sie können jedem Rechner, auf dem das Betriebssystem Windows 2000 oder höher ausgeführt wird, ein Monitor-Set zuweisen.

Das allgemeine Verfahren zum Arbeiten mit Monitor-Sets ist wie folgt:

1. Sie können die Objekte, Instanzen und Zähler von Monitor-Sets über Monitorlisten wahlweise auch manuell aktualisieren und prüfen.
2. Erstellen und pflegen Sie Monitor-Sets über Monitor > Monitor-Sets.
3. Weisen Sie Monitor-Sets über Monitor > Monitor zuweisen bestimmten Rechner-IDs zu.
4. Wahlweise können Sie Standard-Monitor-Sets als *individualisierte Monitor-Sets* anpassen.
5. Die wahlweise Anpassung von Standard-Monitor-Sets erfolgt über *Auto-Lernen*.
6. Überprüfen Sie Monitor-Sets über folgende Befehle:
   - Monitor > Monitor-Protokoll
   - Monitor > Live Counter
   - Monitor > Dashboard > Netzwerkstatus
   - Monitor > Dashboard > Gruppenalarmstatus
   - Monitor > Dashboard > Monitor-Set-Status
   - Info Center > Reporting > Berichte > Monitor > Monitor-Set-Bericht
   - Info Center > Reporting > Berichte > Monitor > Monitor-Aktionsprotokoll

# Beispiel-Monitor-Sets

Der VSA stellt eine stetig wachsende Liste von Beispiel-Monitor-Sets zur Verfügung. Die Namen der

Beispiel-Monitor-Sets beginnen mit ZC. Sie können die Beispiel-Monitor-Sets bearbeiten. Doch empfehlenswerter ist es, ein Beispiel-Monitor-Set zu kopieren und die Kopie zu bearbeiten. Die Beispiel-Monitor-Sets werden bei jeder Aktualisierung der Beispielsätze im Rahmen eines Pflegezyklus überschrieben.

# Monitorsets definieren

Jeder Monitorset wird über vier Registerkarten definiert.

- Auf der Registerkarte **Zählerschwellenwerte** definieren Sie Meldungsbedingungen für alle mit einem Monitor-Set verknüpften Leistungsobjekte/Instanzen/Zähler. Dabei handelt es sich um die gleichen Leistungsobjekte, Instanzen und Zähler, die auch beim Ausführen der Datei `PerfMon.exe` auf einem Windows-Rechner angezeigt werden.
- Auf der Registerkarte **Dienstprüfung** werden Meldungsbedingungen für einen Dienst definiert, wenn der Dienst auf einer Rechner-ID gestoppt wurde und wahlweise versucht wird, den gestoppten Dienst erneut zu starten. *Der Dienst muss auf Automatisch gesetzt werden, um von einem Monitor-Set erneut gestartet zu werden.*
- Auf der Registerkarte **Prozessstatus** werden Meldungsbedingungen basierend auf der Tatsache, ob ein Prozess auf einer Rechner-ID gestartet oder gestoppt wurde, definiert.
- Auf der Registerkarte **Monitorsymbole** wählen Sie Monitorsymbole aus, die bei Auftreten verschiedener Alarmstatus auf der Seite Monitor-Protokoll angezeigt werden.

### ZählerSchwellenwerte konfigurieren

Nachdem Sie über "Monitor > **Monitorsets**" ein neues Monitorset hinzugefügt haben, können Sie auf der Registerkarte **Zähler-Schwellenwerte** Zähler-Schwellenwerte hinzufügen bzw. bearbeiten.

Klicken Sie auf **Hinzufügen** oder das Bearbeitungssymbol  , um einen Assistenten aufzurufen, der Sie durch die sechs Schritte zum Hinzufügen oder Bearbeiten eines Leistungszählers führt.

1. Wählen Sie ein **Objekt**, einen **Zähler** und gegebenenfalls eine **Instanz** aus den jeweiligen Dropdown-Listen aus.
   - Falls nur eine Instanz eines Leistungsobjekts vorliegt, kann das Feld **Instanz** normalerweise ignoriert werden.
   - Die zum Auswählen der Leistungsobjekte, -zähler und -instanzen verwendeten Dropdown-Listen basieren auf der „Masterliste“, die auf der Seite Monitorlisten gepflegt wird. Wird ein(e) Objekt/Instanz/Zähler in der entsprechenden Dropdown-Liste nicht angezeigt, können diese über **Objekt hinzufügen**, **Zähler hinzufügen** bzw. **Instanz hinzufügen** manuell hinzugefügt werden.
   - Unabhängig vom Bereich der Zählerinstanzen, die von einem Monitor-Set festgelegt wurden, zeigt die Seite Monitor-Protokoll nur die Instanzen an, die auf einem bestimmten Rechner vorhanden sind. Neu hinzugefügte Zählerinstanzen – zum Beispiel das Hinzufügen eines entfernbaren Datenträgers zu einem Rechner – werden kurze Zeit nach der Erkennung auf der Seite **Monitor-Protokoll** angezeigt, wenn sie im für die Überwachung festlegten Bereich eines Monitor-Sets enthalten sind.
   - Sind mehrere Instanzen vorhanden, können Sie eine Instanz mit der Bezeichnung `_Total` hinzufügen. Mit der Instanz `_Total` geben Sie an, dass Sie den *kombinierten* Wert aller anderen Instanzen eines Leistungsobjekts *als einen einzelnen Zähler* überwachen möchten.
   - Sind mehrere Instanzen vorhanden, können Sie mithilfe der Registerkarte Monitorlisten > **Zählerinstanz** eine Zählerinstanz mit der Bezeichnung `*ALL` zur Liste der unterstützten Instanzen hinzufügen. Sobald sie zum gewünschten Zähler hinzugefügt wurde, wird der Wert `*ALL` in der Dropdown-Liste der diesem Zähler zugeordneten Instanzen angezeigt. Mit der Instanz `*ALL` können Sie alle Instanzen des gleichen Leistungsobjekts *unter Verwendung einzelner Zähler* überwachen.

2. Sie können wahlweise den **Namen** und die **Beschreibung** des Standard-Zählerobjekts ändern.
3. Wählen Sie die erfassten Protokolldaten aus. Falls ein numerischer Wert zurückgegeben wird, können Sie ungewünschte Protokolldaten ausblenden, indem Sie unmittelbar über oder unter dem Erfassungsschwellenwert einen Erfassungsbetreiber festlegen.
   - **Erfassungsbetreiber** – Wenn eine Zeichenfolge zurückgegeben wird, lauten die Optionen `Changed`, `Equal` oder `NotEqual`. Für numerische Rückgabewerte lauten die Optionen `Equal`, `NotEqual`, `Over` oder `Under`.
   - **Erfassungsschwellenwert** – Legen Sie einen festen Wert fest, mit dem der Rückgabewert verglichen wird. Verwenden Sie den ausgewählten **Erfassungsbetreiber**, um festzulegen, welche Protokolldaten erfasst werden.
   - **Beispielintervall** – Bestimmt, wie häufig die Daten vom Agent an den Kaseya Server gesendet werden.
4. Geben Sie an, wann eine Meldungsbedingung eintritt.
   - **Alarm-Operator** – Wenn eine Zeichenfolge zurückgegeben wird, lauten die Optionen `Changed`, `Equal` oder `NotEqual`. Für numerische Rückgabewerte lauten die Optionen `Equal`, `NotEqual`, `Over` oder `Under`.
   - **Alarmschwellenwert** – Legen Sie einen festen Wert fest, mit dem der Rückgabewert verglichen wird. Verwenden Sie den ausgewählten **Alarm-Operator**, um festzulegen, wann eine Meldungsbedingung eintritt.
   - **Dauer** – Geben Sie die Zeitspanne an, die die Rückgabewerte fortlaufend den Alarmschwellenwert überschreiten müssen, um die Meldungsbedingung zu generieren. Viele Meldungsbedingungen lösen nur dann einen Alarm aus, wenn das Alarmniveau über eine längere Dauer hinweg konstant bleibt.
   - **Zusätzliche Alarme übergehen für** – Unterdrücken Sie weitere Meldungsbedingungen für das gleiche Problem für die angegebene Zeitspanne. Dadurch vermeiden Sie Verwirrung, wenn für das gleiche Problem zahlreiche Meldungsbedingungen bestehen.
5. **Warnen innerhalb eines Alarmschwellenwerts von X%** – Zeigen Sie wahlweise eine Warnungs-Meldungsbedingung an, wenn der zurückgegebene Wert innerhalb eines vorgegebenen Prozentsatzes des **Alarmschwellenwerts** liegt. Das Warnsymbol ist ein gelbes Ampelsymbol .
6. Aktivieren Sie auf Wunsch einen **Trendalarm**. Trendalarme geben anhand von historischen Daten eine Prognose, wann die nächste Meldungsbedingung eintritt.
   - **Verlauf aktiviert?** – Wenn Ja, wird basierend auf den letzten 2500 aufgezeichneten Datenpunkten eine lineare Regressions-Trendlinie berechnet.
   - **Trendfenster** – Die Zeitspanne, um die die berechnete Trendlinie in die Zukunft verlängert wird. Wenn die vorausgesagte Trendlinie innerhalb der festgelegten zukünftigen Zeitspanne den Alarmschwellenwert überschreitet, wird eine Trendmeldungsbedingung generiert. In der Regel sollte ein Trendfenster auf die Zeitspanne eingestellt werden, die für die Vorbereitung auf eine Meldungsbedingung benötigt wird. Beispiel: Ein Benutzer benötigt 10 Tage Vorwarnung, bevor eine Festplatte die Meldungsbedingung erreicht. Dies gibt ihm ausreichend Zeit für die Bestellung, Lieferung und Installation einer größeren Festplatte.
   - **Zusätzliche Trendalarme übergehen für** – Unterdrückt weitere Trendmeldungsbedingungen für das gleiche Problem für die angegebene Zeitspanne.
   - Trendalarme werden als ein orangefarbenes Symbol angezeigt.

   Warnstatus-Meldungsbedingungen und Trendstatus-Meldungsbedingungen erzeugen keine Alarmeinträge im Alarmprotokoll, sie ändern jedoch das Aussehen des Alarmsymbols in verschiedenen Anzeigefenstern. Sie können einen Trendalarmbericht über Berichte > Monitor generieren.

## Dienstprüfung konfigurieren

Kontrolldienste verwenden einen Monitorset wie folgt. Klicken Sie auf **Hinzufügen** oder das

Bearbeitungssymbol , um einen **Dienstprüfung**-Datensatz zu pflegen.

1. **Dienst** – Wählt den zu überwachenden Dienst aus der Dropdown-Liste aus.
   - Die Dropdown-Liste basiert auf der „Masterliste“, die auf der Seite Monitorlisten gepflegt wird. Falls ein Dienst nicht in der Dropdown-Liste aufgeführt wird, können Sie ihn manuell über **Dienst hinzufügen** hinzufügen.
   - Sie können mithilfe der Registerkarte Monitorlisten > **Dienste** ein Sternchen (`*`) als Platzhalter zu den Spalten **Name** oder **Beschreibung** in der Liste der unterstützten Dienste hinzufügen. Der Platzhalterdienst wird nach dem Hinzufügen in der Dropdown-Liste der Dienste angezeigt. Durch Festlegen des Dienstes `*SQL SERVER*` werden beispielsweise alle Dienste überwacht, die die Zeichenfolge `SQL SERVER` im Dienstnamen haben.
   - Sie können mithilfe der Registerkarte Monitorlisten > **Dienste** einen Dienst mit der Bezeichnung `*ALL` zu den Spalten **Name** oder **Beschreibung** in der Liste der unterstützten Dienste hinzufügen. Der Wert `*ALL` wird nach dem Hinzufügen in der Dropdown-Liste der Dienste angezeigt. Die Auswahl des Dienstes `*ALL` bedeutet, dass Sie alle Dienste überwachen möchten.

     **Hinweis:** Abgleichen aktivieren muss aktiviert sein, damit ein Dienstbereich mit dem Platzhalterzeichen * angegeben werden kann.
2. **Beschreibung** – Beschreibt den Dienst und den Grund für das Monitoring.
3. **Neustartversuche** – Gibt an, wie oft das System versuchen soll, den Dienst neu zu starten.
4. **Neustartintervall** – Die Zeitspanne, die zwischen Neustartversuchen gewartet werden soll. Für manche Dienste wird mehr Zeit benötigt.
5. **Zusätzliche Alarme übergehen für** – Unterdrückt weitere Meldungsbedingungen für die angegebene Zeitspanne.

### Prozessstatus konfigurieren

Klicken Sie auf **Hinzufügen** oder das Bearbeitungssymbol , um einen **Prozessstatus**-Datensatz zu pflegen.

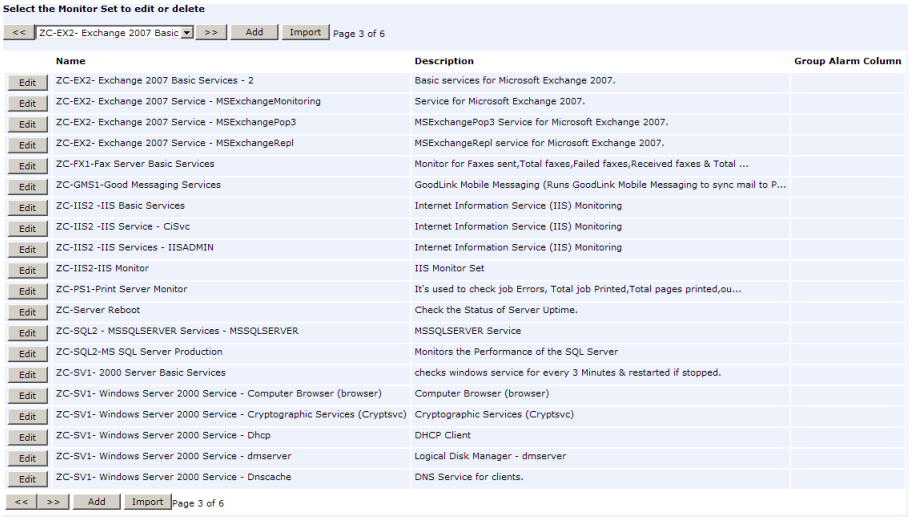
1. **Prozess** – Wählt den zu überwachenden Prozess aus der Dropdown-Liste aus. Die Dropdown-Liste basiert auf der „Masterliste“, die auf der Seite Monitorlisten gepflegt wird. Falls ein Prozess nicht in der Dropdown-Liste aufgeführt wird, können Sie ihn manuell über **Prozess hinzufügen** hinzufügen.
2. **Beschreibung** – Beschreibt den Prozess und den Grund für das Monitoring.
3. **Alarm bei Übergang** – Löst eine Meldungsbedingung aus, wenn ein Prozess (Anwendung) gestartet oder gestoppt wird.
4. **Zusätzliche Alarme übergehen für** – Unterdrückt weitere Meldungsbedingungen für die angegebene Zeitspanne.

# ZählerSchwellenwerte einstellen – Ein Beispiel

In diesem Beispiel sehen Sie anhand des Monitorsets `ZC-PS1-Print Server Monitor`, wie Zähler-Schwellenwerte für Monitorsets definiert werden.

1. Klicken Sie auf "Monitor > **Monitorsets**", um die erste Seite der in Ihrem VSA verfügbaren Monitorsets angezeigt zu bekommen. In diesem Fall wurden Beispiel-Monitorsets in VSA geladen. Die Namen der Beispiel-Monitorsets haben das Präfix ZC. Das Laden der Beispiel-Sets in VSA erfolgt über "System > **Konfigurieren**".

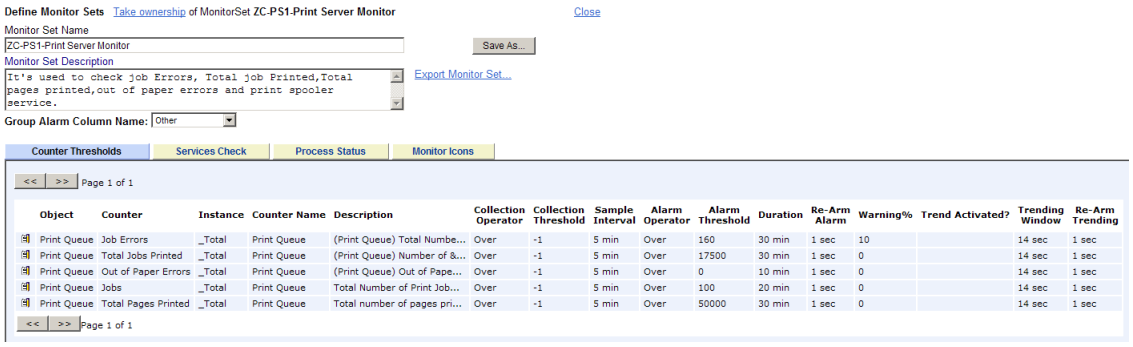
2. Klicken Sie auf die Schaltfläche **Bearbeiten** neben dem Monitorset `ZC-PS1-Print Server Monitor`.




3. Die Seite **Monitorsets definieren** wird angezeigt. Als erstes wird die Registerkarte **ZählerSchwellenwerte** angezeigt, die wir überprüfen wollen. In dieser Tabellenansicht werden die Einstellungen angezeigt, die für jeden der Zähler definiert wurden. Falls Sie einen Zähler bearbeiten möchten, klicken Sie auf das Bearbeitungssymbol in der linken Spalte. Dadurch wird der Bearbeitungsassistent für diesen Zähler eingeblendet.

> **Hinweis:** Sie haben die Möglichkeit, Beispiel-Monitorsets mit dem Präfix ZC zu bearbeiten; allerdings werden diese Beispiel-Monitorsets überschrieben, wenn die Aktualisierung über ''System > Konfigurieren'' aktiviert wurde. Falls Sie einen ZC-Beispiel-Monitorset bearbeiten möchten und sichergehen möchten, dass Ihre Änderungen erhalten bleiben, erstellen Sie eine Kopie des ZC-Beispiel-Monitorsets und nehmen die Änderungen an dieser Kopie vor.

Wir möchten die Einstellungen aller Zähler in diesem Monitorset überprüfen. Daher bleiben wir in der Tabellenansicht.




4. Überprüfen wir zunächst die ersten fünf Spalten der Registerkarte **ZählerSchwellenwerte** für diesen Monitorset.

   In diesem Fall beziehen sich alle Zähler auf dasselbe `Print Queue`-Objekt. Monitorsets sind nicht auf ein einzelnes Leistungsobjekt beschränkt. Es bietet sich jedoch an, die Zähler in einem einzelnen Monitorset unter Bezug auf eine bestimmte Windows-Funktion logisch zu gruppieren.

   Die Spalte **Instanz** ist im Grunde genommen eine Unterkategorie des Objekts, nicht der Zähler. Zähler werden für eine Kombination von Objekt und Instanz definiert. Die Instanzen des Objekts `Print Queue` sind beispielsweise die Namen bestimmter Drucker, an die der Zielrechner Druckaufträge senden kann, sowie eine Instanz namens `_Total`.

Die Instanz `_Total` kombiniert den numerischen Wert aller Zählerdaten von allen Druckern und summiert diese. Sie fungiert jedoch auch als eine Art "Stellvertreterinstanz". Ohne die Instanz `_Total` müssten Sie jede Instanz mit einem exakten Druckernamen aufrufen, was das Anwenden ein und desselben Monitorsets auf verschiedene Rechner erheblich erschweren würde. Der wahre Vorteil der Instanz `_Total` liegt in diesem Fall darin, dass Sie feststellen können, *ob bei irgendwelchen Druckern Druckerfehler vorliegen*. Sobald Sie diese Informationen haben, können Sie dem spezifischen Grund nachgehen.

| Object | Counter | Instance | Counter Name | Description |
|---|---|---|---|---|
| Print Queue | Job Errors | _Total | Print Queue | (Print Queue) Total Numbe... |
| Print Queue | Total Jobs Printed | _Total | Print Queue | (Print Queue) Number of &... |
| Print Queue | Out of Paper Errors | _Total | Print Queue | (Print Queue) Out of Pape... |
| Print Queue | Jobs | _Total | Print Queue | Total Number of Print Job... |
| Print Queue | Total Pages Printed | _Total | Print Queue | Total number of pages pri... |

5. Der nächste Satz von Spalten beschreibt die Sammlungs- und AlarmSchwellenwert-Einstellungen. Beachten Sie, dass die Werte für **Sammlungs-Operator** und **Schwellenwert der Sammlung** alle auf `Over -1` gesetzt sind. Das Sammlungskriterium `Over -1` wird häufig verwendet, um sicherzustellen, dass jeder Wert (einschließlich null) erfasst wird – unabhängig davon, ob jemals ein Alarmschwellenwert erreicht wird oder nicht. Dadurch wird sichergestellt, dass Sie alle von einem Zähler generierten Daten überprüfen können.

   Der Zähler gibt alle fünf Minuten einen neuen Wert aus, wie durch die Spalte **Abfrageintervall** festgelegt.

   Es sind hohe **Alarmschwellenwerte** für die Zähler `Total Jobs Printed` und `Total Pages Printed` eingestellt. Dies ist angebracht, da für einen Drucker mit hohem Druckvolumen diese hohe Anzahl von Druckaufträgen und gedruckten Seiten mühelos erreicht wird.

   Die **Alarmschwellenwerte** für `Jobs` und `Job Errors` sind bedeutend niedriger. Der Zähler `Jobs` gibt die Anzahl der derzeit verarbeiteten Aufträge an. Daher ist es ganz logisch, dass dieser Wert klein ist. Der Zähler `Job Errors` gibt die Anzahl der Fehler in Druckaufträgen an, die seit dem letzten Start des Druckerservers aufgetreten sind. Ein Drucker mit hohem Druckvolumen wird diesen AlarmSchwellenwert sehr schnell überschreiten, falls ein Problem mit dem Drucker vorliegt.

   Der Schwellenwert für den Zähler `Out of Paper Errors` liegt bei null. Dies ist der normale Wert, wenn seit dem letzten Start des Druckerservers kein "Kein Papier'-Fehler aufgetreten ist. Wenn auch nur *ein einziger* "Kein Papier'-Fehler auftritt, d. h. wenn der Zählerwert `Over 0` liegt, wird eine Benachrichtigung ausgelöst, der den Benutzer darauf hinweist, dass im Drucker Papier nachgelegt werden muss.

| Counter | Collection Operator | Collection Threshold | Sample Interval | Alarm Operator | Alarm Threshold | Duration | Re-Arm Alarm |
|---|---|---|---|---|---|---|---|
| Job Errors | Over | -1 | 5 min | Over | 160 | 30 min | 1 sec |
| Total Jobs Printed | Over | -1 | 5 min | Over | 17500 | 30 min | 1 sec |
| Out of Paper Errors | Over | -1 | 5 min | Over | 0 | 10 min | 1 sec |
| Jobs | Over | -1 | 5 min | Over | 100 | 20 min | 1 sec |
| Total Pages Printed | Over | -1 | 5 min | Over | 50000 | 30 min | 1 sec |

6. Die letzten fünf Spalten geben Warn- und Tendenzalarme an. Der Warnalarm wird als ein Prozentsatz angegeben. Für den Zähler `Jobs Errors` wird ein Warnalarm ausgelöst, wenn der Wert des Zählers 10 % seines Alarmschwellenwerts erreicht.

   Falls ein Tendenzalarm aktiviert ist, wird eine Tendenzlinie basierend auf den erfassten Daten berechnet. Falls die Tendenzlinie aufzeigt, dass der AlarmSchwellenwert innerhalb der Zeitspanne **Verlaufsfenster** überschritten wird, wird ein Tendenzalarm ausgelöst.

   Generell werden Warn- und Tendenzalarme nur dann verwendet, wenn eine Ressource kritisch ist oder bereits untersucht wird. In der Regel sollte ein Trendfenster auf die Zeitspanne eingestellt werden, die ggf. für die Vorbereitung auf eine Benachrichtigungsbedingung benötigt wird.

Warnstatus-Alarmbedingungen und Tendenzstatus-Alarmbedingungen erzeugen keine Alarme im Alarmprotokoll, sie ändern jedoch das Aussehen des Alarmsymbols in verschiedenen Anzeigefenstern. Über "Infocenter > Reporting > Berichte > Monitor" können Sie einen Tendenzalarmbericht erzeugen.

| Counter | Warning% | Trend Activated? | Trending Window | Re-Arm Trending |
|---|---|---|---|---|
| Job Errors | 10 | | 14 sec | 1 sec |
| Total Jobs Printed | 0 | | 14 sec | 1 sec |
| Out of Paper Errors | 0 | | 14 sec | 1 sec |
| Jobs | 0 | | 14 sec | 1 sec |
| Total Pages Printed | 0 | | 14 sec | 1 sec |

# Monitorsets zuweisen

Über "Monitor > **Monitoring zuweisen** können Sie Monitorsets bestimmten Rechner-IDs zuweisen. Sie haben die Möglichkeit, angewendete Monitorsets auf zwei Weisen anzupassen:

- Individualisierte Monitorsets
- Automatisch lernen

# Individualisierte Monitor-Sets

Sie können die Monitor-Set-Einstellungen für einen einzelnen Rechner *individualisieren*.

1. Wählen Sie mit Monitor > **Monitor zuweisen** ein *Standard*-Monitor-Set aus der `<Select Monitor Set>`-Dropdown-Liste aus.
2. Weisen Sie dieses Standard-Monitor-Set einer Rechner-ID zu. Der Name des Monitor-Sets wird in der Spalte **Monitor-Set**angezeigt.
3. Klicken Sie auf das individualisierte Monitor-Set-Symbol  in der Spalte **Monitor-Set**, um die gleichen Optionen wie beim Definieren eines Standard-Monitor-Sets anzuzeigen. *Bei einem individualisierten SNMP-Set wird dem Namen des SNMP-Sets ein (IND) Präfix vorangestellt.*
4. Sie können den Namen oder die Beschreibung des individualisierten Monitor-Sets auf Wunsch ändern. Klicken Sie anschließend auf **Speichern**. Durch Bereitstellung eines eindeutigen Namens und einer Beschreibung kann ein individualisiertes Monitor-Set in Berichten und Protokolldateien identifiziert werden.
5. Nehmen Sie Änderungen an den Kontrolleinstellungen des individualisierten Monitor-Sets vor und klicken Sie auf **Einspeichern**. Änderungen gelten nur für den einzelnen Rechner, dem das individualisierte Monitor-Set zugewiesen ist.

> **Hinweis:** Änderungen an einem Standard-Monitor-Set haben keine Auswirkungen auf die individualisierten Monitor-Sets, die davon kopiert wurden.

# Auto-Lernen – Monitor-Sets

Sie können **Auto-Lernen**-Alarmschwellenwerte für jedes Standard-Monitor-Set aktivieren, das Sie ausgewählten Rechner-IDs zuweisen. Damit werden Alarmschwellenwerte basierend auf tatsächlichen Leistungsdaten auf die einzelnen Rechner abgestimmt.

Jeder zugewiesene Rechner generiert Leistungsdaten für die angegebene Zeitspanne. Während dieser Zeitspanne werden keine Alarme ausgelöst. Am Ende der Auto-Lernen-Sitzung wird der Alarmschwellenwert für jeden zugewiesenen Rechner basierend auf der tatsächlichen Leistung des

Rechners automatisch abgestimmt. Sie können die Alarmschwellenwerte, die durch **Auto-Lernen** berechnet wurden, manuell anpassen oder eine weitere **Auto-Lernen**-Sitzung ausführen. **Auto-Lernen** kann nicht mit individualisierten Monitor-Sets verwendet werden.

# SNMP-Sets

Bestimmte Netzwerkgeräte wie Drucker, Router, Firewalls, Server und UPS-Geräte bieten keine Unterstützung für die Installation eines Agent. Ein VSA-Agent, der auf einem verwalteten Rechner im gleichen Netzwerk wie das Gerät installiert ist, kann jedoch durch Verwendung des **Simple Network Management Protocol (SNMP)** von diesem Gerät lesen bzw. darauf schreiben.

# Grundlagen des SNMP-Monitorings

Wie man VSA für das Monitoring von SNMP-Geräten nutzt, lernen Sie am schnellsten, indem Sie einem Gerät ein vordefiniertes "SNMP-Set" zuweisen und sich die Ergebnisse ansehen. Sobald Sie sich mit der relativ einfachen Basiskonfiguration vertraut gemacht haben, können Sie sich auch die erweiterten SNMP-Features ansehen.

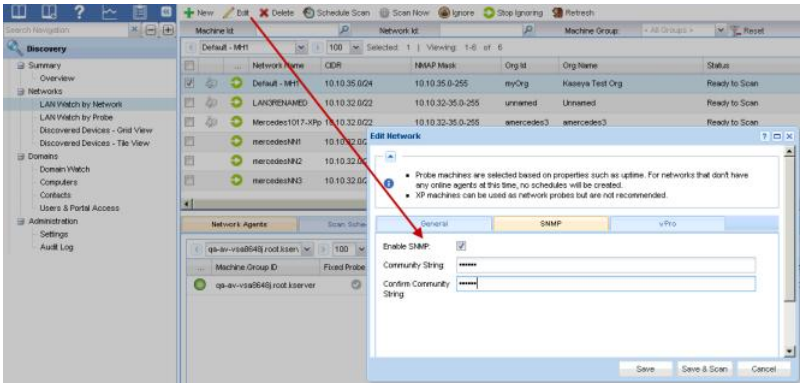
Wenn Sie noch keine Erfahrung im Monitoring von SNMP-fähigen Geräten haben, empfehlen wir Ihnen, in drei Schritten vorzugehen:

1. Ermitteln Sie über "Ermittlung > **LAN-Watch"** *(siehe 19)* SNMP-Geräte.
2. Weisen Sie den ermittelten Geräten über "Monitoring > **SNMP zuordnen"** *(siehe 20)* vordefinierte SNMP-Sets zu.
3. Lassen Sie sich über "Monitoring > **SNMP-Protokoll" SNMP-Alarme anzeigen.** *(siehe 22)*

## LAN-Watch und SNMP

**LAN-Watch nach Netzwerk** bzw. **LAN-Watch nach Sonde** im Modul **Discovery** verwendet einen vorhandenen VSA -Agent auf einem verwalteten Rechner, um in regelmäßigen Abständen das lokale Netzwerk (LAN) auf allen Geräten zu scannen, die seit der letzten Ausführung von LAN-Watch neu mit diesem LAN verbunden worden sind.

*Der LAN-Watch-Ermittlungsrechner gibt eine SNMP-Anforderung an die SNMP-Geräte aus, die er im selben LAN ermittelt.* Sie müssen daher *zuerst* LAN-Watch ausführen, um daraufhin auf SNMP-fähige Geräte in VSA zugreifen zu können.




So schließen Sie SNMP-Geräte in den Ermittlungsscan über LAN-Watch mit ein:

1. Wählen Sie eine Rechner-ID auf dem LAN, auf dem Sie SNMP-Geräte ermitteln wollen.
2. Aktivieren Sie das Kontrollkästchen **SNMP aktivieren**.
3. Geben Sie einen `community name` in die Felder **Communitynamen lesen** und **Bestätigen** ein.

Ein Community-Name fungiert als Anmeldeinformation für den Zugang zu einem SNMP-fähigen Gerät. Der Standardname der Community mit Lesezugriff ist in der Regel `public` (in Kleinbuchstaben); allerdings sind nicht alle Geräte gleich konfiguriert. Wenn Sie nicht sicher sind, welchen Community-Namen Sie verwenden sollen, müssen Sie gegebenenfalls den Community-Namen auf dem Geräte sofort ermitteln oder zurücksetzen.

4. Klicken Sie auf die Schaltfläche **Planen und scannen** im unteren Bereich des Dialogs **Netzwerk bearbeiten**. Der Scan wird daraufhin umgehend gestartet.
5. Prüfen Sie ermittelte SNMP-fähige Geräte über die Seite Monitoring > **SNMP zuweisen** *(siehe 20)*.

# SNMP zuordnen

SNMP-Geräte werden erst auf der Seite "Monitor > **SNMP zuordnen**" angezeigt, *nachdem* **LAN-Watch** *(siehe 19)* auf dem Ermittlungsrechner ausgeführt wurde.

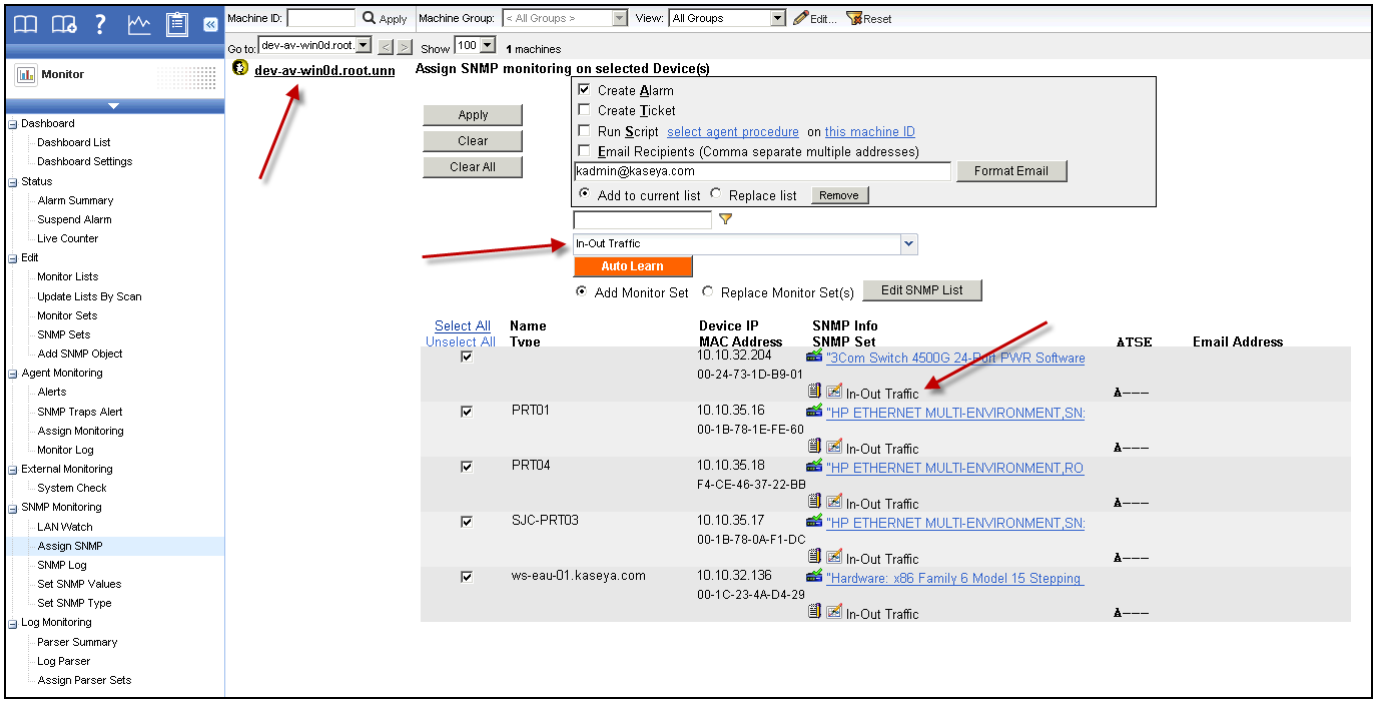
So ordnen Sie auf der Seite **SNMP zuordnen** das Monitoring eines SNMP-fähigen Geräts zu:

1. Wählen Sie auf der linken Seite den Ermittlungsrechner aus. Daraufhin werden alle SNMP-fähigen Geräte im selben lokalen Netzwerk (LAN) angezeigt.
2. Wählen Sie ein SNMP-Set aus der Drop-down-Liste aus.

> **Hinweis:** Enthält die Drop-down-Liste keine SNMP-Sets, gehen Sie zur Seite **SNMP-Sets**, wählen Sie eine SNMP-Set aus und klicken Sie dann auf die Schaltfläche **Speichern unter**, um eine Kopie davon zu erstellen. Erstellen Sie zu Experimentierzwecken eine Kopie eines SNMP-Sets, das dem Gerät ähnelt, das Sie überwachen möchten. Wenn Sie beispielsweise einen Router überwachen möchten, erstellen Sie eine Kopie eines SNMP-Sets für Router. Wenn Sie einen Drucker überwachen möchten, erstellen Sie eine Kopie eines SNMP-Sets für Drucker usw. Wenn Sie zum ersten Mal mit einem SNMP-Set arbeiten, ist es nicht von Bedeutung, wenn einige Objekte im SNMP-Set nicht auf das Gerät zutreffen, das Sie überwachen möchten. Sie können **Ihre Kopie eines SNMP-Sets jederzeit bearbeiten** *(siehe 24)* – egal, ob Sie sie bereits einem Rechner zugewiesen haben oder nicht.

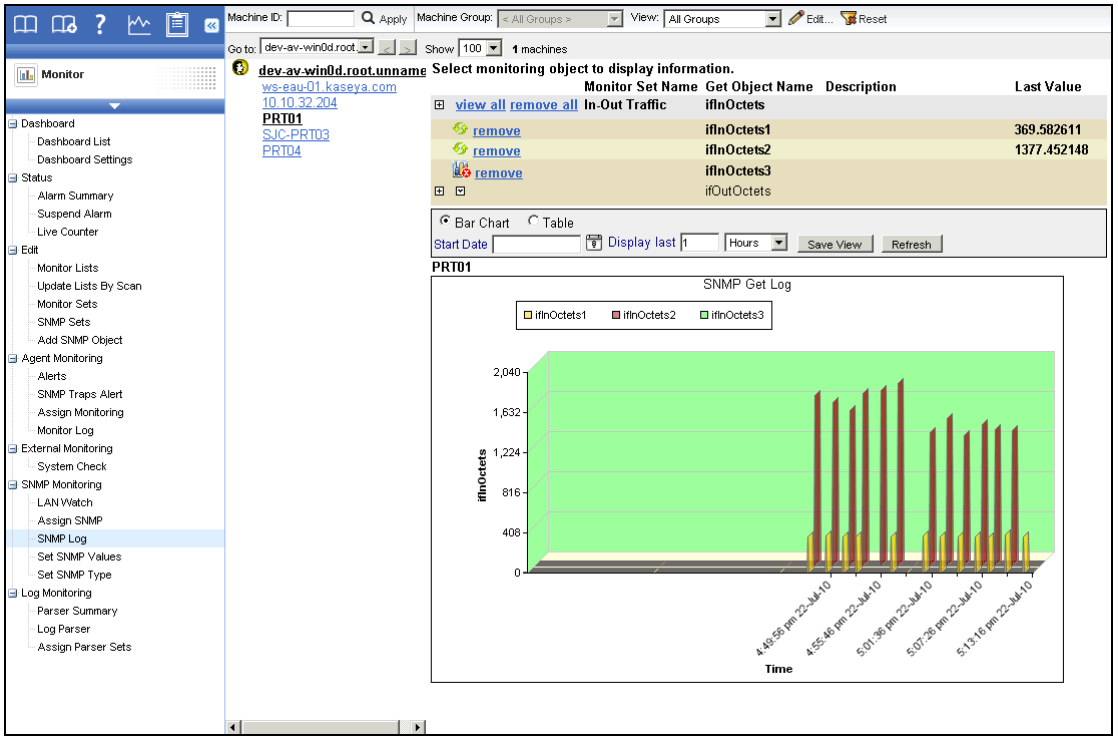
3. Wählen Sie ein oder mehrere SNMP-fähige Geräte aus.
4. Klicken Sie auf die Schaltfläche **Apply**.

5. Es dauert etwa 15 Minuten, bis SNMP-fähige Geräte SNMP-Monitoringdaten an VSA übermitteln. Die Monitoringergebnisse können Sie sich auf der Seite **SNMP-Protokoll** *(siehe 22)* ansehen.



# SNMP-Protokoll

Auf der Seite **SNMP-Protokoll** werden die Ergebnisse des Monitorings SNMP-fähiger Geräte als Grafik oder in Tabellenform angezeigt, nachdem sie über **SNMP zuordnen** *(siehe 20)* einem Gerät zugeordnet wurden. Nachdem ein SNMP-Set einem Gerät zugeordnet wurde, dauert es etwa 15 Minuten, bis die entsprechenden Daten auf der Seite angezeigt werden. Einige Objekte im SNMP-Set übermitteln möglicherweise keine Daten. Dies kann der Fall sein, wenn ein bestimmtes Objekt im SNMP-Set nicht für das jeweilige Gerät geeignet ist. Möglich ist auch, dass das Objekt zwar für das Gerät geeignet, aber gerade inaktiv ist. Navigieren Sie durch die verschiedenen Objekte im SNMP-Set auf dieser Seite, bis Sie eines finden, das Daten übermittelt. Machen Sie sich damit vertraut, wie Sie mithilfe der verschiedenen Steuerungselemente die Anzeige der Daten verändern können.




So wählen Sie aus, welche Daten angezeigt werden sollen:

1. Klicken Sie auf einen Rechner-ID-Link, um alle mit einer Rechner-ID verknüpften SNMP-Geräte anzuzeigen.
2. Klicken Sie auf eine IP-Adresse oder den Namen eines SNMP-Geräts, um alle SNMP-Sätze und MIB-Objekte anzuzeigen, die diesem SNMP-Gerät zugewiesen sind.
3. Klicken Sie auf das Erweiterungssymbol ⊞, um die Erfassungs- und Schwellenwerteinstellungen für ein MIB-Objekt anzuzeigen.
4. Klicken Sie auf die Pfeiltaste nach unten ⊡, um die Protokolldaten des MIB-Objekts als Diagramm oder Tabelle anzuzeigen.
5. Aktivieren Sie das Optionsfeld **Balkendiagramm** oder **Tabelle**, um die Protokolldaten im gewünschten Format anzuzeigen.

SNMP-Kontrollobjekte können mehrere Instanzen enthalten und gemeinsam in einem Diagramm oder einer Tabelle angezeigt werden. Ein Netzwerkschalter kann beispielsweise 12 Ports umfassen. Jeder ist eine Instanz und kann Protokolldaten enthalten. Alle 12 Instanzen können zu einem Diagramm oder einer Tabelle zusammengefasst werden. SNMP-Balkendiagramme liegen im 3D-Format vor, was die Ansicht mehrerer Instanzen ermöglicht.

# SNMP-Konzepte

Bevor Sie versuchen, ein SNMP-Set zu bearbeiten, sollten Sie sich zunächst mit den folgenden SNMP-Konzepten vertraut machen.

## Drei Arten von SNMP-Meldungen

VSA unterstützt drei Arten von SNMP-Meldungen.

1. **GET-'Lesen'-Nachricht** – Das SNMP-fähige Gerät reagiert auf eine GET-SNMP-Anforderung von einer SNMP-Verwaltungssoftware (wie z. B. einem VSA-Agent auf einem Rechner). *Die meisten SNMP-Funktionen in VSA – einschließlich SNMP-Sets – umfassen GET-Nachrichten.*
2. **SET-'Schreiben'-Nachricht** – SNMP-Verwaltungssoftware wie z. B. VSA schreibt einen Wert in das MIB-Objekt auf einem SNMP-fähigen Gerät. Dies kann entweder zu Referenzzwecken geschehen, oder um das Verhalten des Geräts zu verändern. Eine VSA-Seite führt SET-Nachrichten aus: **SNMP-Werte einrichten**.
3. **TRAP-'Warten'-Nachricht** – Nachrichten werden ohne vorherige Anforderung infolge eines bestimmten Ereignisses von einem SNMP-fähigen Gerät an einen "wartenden" Agent versandt. Eine VSA-Seite konfiguriert SNMP-TRAP-Nachrichten und reagiert darauf: **SNMP-Traps-Benachrichtigung** (siehe 32).

## MIB-Objekte

Wenn Sie die SNMP-Sets, die VSA für das Monitoring von SNMP-Geräten nutzt, bearbeiten möchten, sollten Sie zumindest über ein grundlegendes Verständnis von MIB-Objekten und MIB-Dateien verfügen. Sind Ihnen diese Konzepte bereits vertraut, überspringen Sie diesen Abschnitt und gehen Sie zum Kapitel **SNMP-Sets bearbeiten** *(siehe 24)*.

Jedes SNMP-fähige Gerät reagiert ausschließlich auf ganz bestimmte SNMP-Anforderungen. Jede SNMP-Anforderung wird eindeutig durch eine Objekt-ID oder **OID** identifiziert. Beispiel: Eine OID mit der Bezeichnung `ifInOctets` wird durch die zahlenbasierte OID `.1.3.6.1.2.1.2.2.1.10` wiedergegeben. Die entsprechende zeichenbasierte OID für `ifInOctets` lautet `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets`.

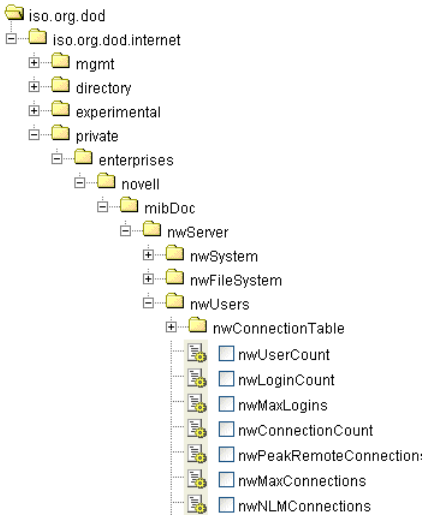
Jeder Gerätehersteller veröffentlicht die OIDs, die seine SNMP-fähigen Geräte in Form einer **MIB-Datei** unterstützen, weshalb OIDs meist als **MIB-Objekte** bezeichnet werden. Die MIB-Dateien können in eine MIB-Verwaltungsanwendung wie z. B. VSA importiert werden. Viele der gängigsten MIB-Objekte sind in VSA bereits vorinstalliert. Es müssen also in der Regel nur dann MIB-Objekte importiert werden, wenn das Gerät ganz spezielle MIB-Objekte erfordert.

Innerhalb von VSA sind die MIB-Objekte zu **SNMP-Sets** zusammengefasst. Nach der Durchführung eines LAN-Watches werden einem SNMP-fähigen Gerät SNMP-Sets im selben lokalen Netzwerk (LAN) zugewiesen, die der Überwachung der Leistung des Geräts dienen.

### MIB-Baumstruktur

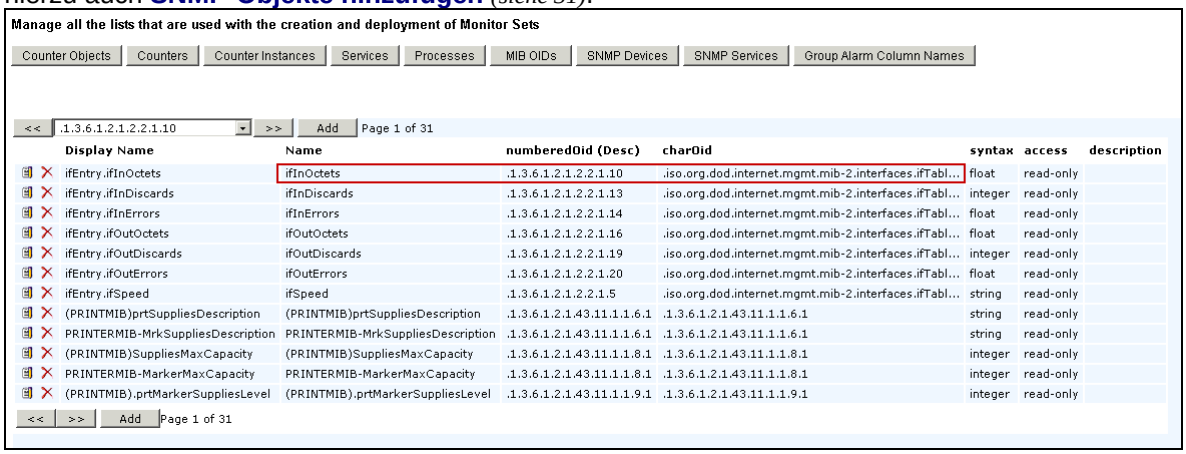
Hersteller haben versucht, die Identifizierung der MIB-Objekte, die sie für ihre Geräte verwenden, zu standardisieren, indem Sie sie in einer MIB-Baumstruktur organisiert haben. So nutzen beispielsweise verschiedene Router oft fast dieselben MIB-Objekte und unterscheiden sich diesbezüglich nur in ein paar speziellen MIB-Objekten, die ausschließlich das jeweilige Produkt unterstützen.

Sie können entweder die ziffernbasierte OID oder die zeichenbasierte OID verwenden, um die Position eines MIB-Objekts im MIB-Baum zu bestimmen. Nachfolgend sehen Sie ein Beispiel einer zeichenbasierten MIB-Baumstruktur.




### MIB-Objekte auf der Seite "Monitor-Listen"

In VSA können Sie eine Liste aller derzeit verfügbaren MIB-Objekte einsehen, die in ein SNMP-Set aufgenommen werden können. Wählen Sie hierzu die Seite "Monitoring > **Monitor-Listen**" aus und klicken Sie dann auf die Schaltfläche **MIB-OIDs**. Daraufhin bekommen Sie eine Tabelle angezeigt, die der untenstehenden Tabelle ähnelt. Sie können der Liste MIB-Objekte hinzufügen, indem Sie MIB-Dateien zur Unterstützung eines bestimmten SNMP-fähigen Geräts in VSA importieren. Siehe hierzu auch **SNMP-Objekte hinzufügen** *(siehe 31)*.




# Bearbeiten von SNMP-Sets

## SNMP-Sets – Teil 1

Wählen Sie in VSA "Monitoring> **SNMP-Sets**" und daraufhin ein bestimmtes SNMP-Beispielset aus, um eine Tabellenansicht mit mehreren Spalten zu erhalten, die der untenstehenden Abbildung ähnelt.

Dieses SNMP-Beispielset zeigt ein Paar MIB-Objekte, die zum übergeordneten MIB-Objekt `IFEntry.` gehören. `IFEntry`-Objekte überwachen den Datenfluss zu und von einem Gerät, wie z. B. über ein am Port eines Switchers eingestecktes Kabel. Wenn es um TCP/IP geht, wird dieser Punkt im Datenfluss als *Schnittstelle* des Geräts bezeichnet; `IFEntry` bedeutet also "Schnittstelleneingang".

Das MIB-Objekt `ifInOctets` bezieht sich speziell auf die Anzahl von 8-Bit-Bytes – in diesem Fall auch "Oktetts" genannt –, die in eine einzelne Schnittstelle fließen. Das MIB-Objekt `ifOutOctets` steht für die Anzahl an 8-Bit-Bytes, die aus einer einzelnen Schnittstelle heraus fließen.

Allein mithilfe dieser beiden MIB-Objekte können Sie die Aus- und Eingangsdatenrate einer Netzwerkverbindung überwachen und für den Fall, dass der Datenfluss einen bestimmten Wert übersteigt, einen Alarmschwellenwert zuweisen.

| MIBObject | SNMP Version | SNMP Instance | Data Type | Name | Description |
|---|---|---|---|---|---|
| ifEntry.ifInOctets | 1 | 1-3 | ratePerSecond | ifInOctets | |
| ifEntry.ifOutOctets | 1 | 1-3 | ratePerSecond | ifOutOctets | |

**MIB-Objekt** – Die MIB-Objekt-ID besteht aus den letzten beiden Elementen der zugehörigen zeichenbasierten OID. In der ersten Zeile lautet die komplette zeichenbasierte OID für dieses MIB-Objekt beispielsweise `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets`. Darum wird in der ersten Spalte der Tabelle `ifEntry.ifInOctets` angezeigt.

**SNMP-Version** – Bei SNMP handelt es sich um ein sich weiterentwickelndes Protokoll. Version 1 wird von allen Geräten unterstützt (Standard). Version 2c definiert mehr Attribute, wie z. B. zusätzliche Datentypen und verschlüsselt die Pakete, die an den SNMP-Agent und von diesem übermittelt werden. *Wählen Sie Version 2c nur dann aus, wenn Sie sicher sind, dass das Gerät die Version 2c unterstützt.*

**SNMP-Instanz** –Es kann mehrere Instanzen eines MIB-Objekts auf einem einzigen Gerät geben. Ein Switcher hat beispielsweise zahlreiche Ports. Sie haben die Möglichkeit anzugeben, welche Instanzen auf einem Gerät Sie überwachen möchten, z. B. `1-5,6` oder `1,3,7`. Gibt es nur eine Instanz eines MIB-Objekts auf einem Gerät, geben Sie `0` oder gar nichts an.

**Wert gespeichert als** – Gibt das MIB-Objekt einen Zahlenwert aus, können Sie wählen, ob der Wert als **Gesamtwert** oder als **Rate pro Sekunde** ausgegeben werden soll. Normalerweise ist beim Schnittstellenmonitoring eher die Flussrate der Ein- und Ausgangsdaten an einem Port relevant, weshalb `IfInOctets` und `IfOutOctets` auf "Rate pro Sekunde" eingestellt sind. Bei MIB-Objekten, die anstatt einer Zahl eine Zeichenfolge ausgeben, wird dieses zusätzliche Feld in den SNMP-Sets nicht angezeigt.

**Name und Beschreibung** – Hierbei handelt es sich um Anzeigenamen und -beschreibung eines MIB-Objekts. Sie können die Standardeinstellungen hierfür unter "Monitoring > **Monitor-Liste**" ändern, oder Anzeigenamen und -beschreibung innerhalb eines SNMP-Sets ändern.

# SNMP-Sets – Teil 2

Die nächsten Spalten in der Tabellenansicht geben den *Schwellenwert für die Sammlung* und den *Alarmschwellenwert* für die Werte an, die das Gerät an VSA übermittelt.

| Name | Collection Operator | Collection Threshold | SNMP Timeout | Alarm Operator | Alarm Threshold | Duration | Re-Arm Alarm |
|---|---|---|---|---|---|---|---|
| ifInOctets | Over | -1 | 2 sec | Over | 1000000 | 30 sec | 1 days |
| ifOutOctets | Over | -1 | 2 sec | Over | 1000000 | 30 sec | 1 days |

## Sammlung

Verringern Sie den Umfang der gesammelten Protokolldaten in VSA, indem Sie den Schwellenwert für die Sammlung so festlegen, dass Sie nur Daten übermittelt bekommen, wenn Sie diese auch wirklich benötigen. Wenn Sie alle Daten erhalten möchten und der **Sammlungs-Operator** auf `Over` gesetzt ist, setzen Sie den **Schwellenwert für die Sammlung** auf `-1`, um alle Werte über -1 zu erhalten.

- **Sammlungs-Operator** – Für in Form von Zeichenfolgen übermittelte Werte stehen die Optionen `Changed`, `Equal` oder `NotEqual` (im Verhältnis zum **Schwellenwert für die Sammlung**) zur

Verfügung. Für numerisch übermittelte Werte stehen die Optionen `Equal`, `NotEqualOver` oder `Under` (im Verhältnis zum **Schwellenwert für die Sammlung**) zur Verfügung.

- **SNMP-Timeout** – Geben Sie die Anzahl der Perioden an, die der Agent auf eine Antwort vom SNMP-Gerät warten soll, bevor er aufgibt. Zwei Sekunden sind der Standardwert.

### Alarme

Legen Sie fest, wann eine Benachrichtigungsbedingung vorliegt. Dies bedeutet nicht unbedingt, dass auch wirklich ein Alarm ausgelöst wird. Ob und wann bei Vorliegen einer Benachrichtigungsbedingung eine Benachrichtigung ausgelöst wird, wird festgelegt, wenn das SNMP-Set einem Gerät zugewiesen wird.

- **Alarm-Operator** – Für in Form von Zeichenfolgen übermittelte Werte stehen die Optionen `Changed`, `Equal` oder `NotEqual` (im Verhältnis zum **Alarmschwellenwert**) zur Verfügung. Für numerisch übermittelte Werte stehen die Optionen `Equal`, `NotEqual`, `Over`, `Under` oder `Percent Of` zur Verfügung. Wird die Option `Percent Of` ausgewählt, wird ein neues Feld namens **Prozentobjekt** angezeigt. Das **Prozentobjekt** dient als 100 %-Richtwert für Vergleichszwecke.
- **Dauer** – Geben Sie an, über welche Zeitspanne hinweg die übermittelten Werte den Benachrichtigungsschwellenwert kontinuierlich überschreiten müssen, damit eine Benachrichtigungsbedingung eintritt. Viele Benachrichtigungsbedingungen lösen erst dann eine Benachrichtigung aus, wenn der Schwellenwert über längere Zeit hinweg überschritten wird.
- **Benachrichtigung scharf schalten** – Unterdrücken Sie weitere Benachrichtigungsbedingungen für dasselbe Problem innerhalb desselben Zeitraums. Dadurch vermeiden Sie Verwirrung durch zahlreiche Benachrichtigungsbedingungen für ein und dasselbe Problem.

## SNMP-Sets – Teil 3

Die letzten Spalten in der Tabellenansicht eines SNMP-Sets werden angezeigt, *bevor* eine Benachrichtigungsbedingung eintritt. Sie werden seltener genutzt als die bereits erläuterten Spalten.

**Warnalarme** und **Trendalarme** erzeugen keine Alarmeinträge im Alarmprotokoll, sie ändern jedoch das Aussehen des Alarmsymbols in verschiedenen Anzeigefenstern. Sie können einen Trendalarmbericht über "Berichte > Monitoring" generieren.

| Name | Warning% | Trend Activated? | Trending Window | Re-Arm Trending |
|---|---|---|---|---|
| ifInOctets | 10 | No - Trending is not need... | 14 days | 1 days |
| ifOutOctets | 10 | No - Trending is not need... | 14 days | 1 days |

### Warnalarme

- **Warnung %** – Sie können sich optional eine *Warnbenachrichtigungsbedingung* anzeigen lassen, wenn der übermittelte Wert um einen bestimmten Prozentsatz vom **Benachrichtigungsschwellenwert** abweicht. Anstatt eines Alarms wird ein Warnsymbol angezeigt.

### Trendalarme

Trendbenachrichtigungen versuchen anhand von Verlaufsdaten vorherzusehen, wann die nächste Benachrichtigungsbedingung eintreten wird.

- **Verlauf aktiviert?** – Wenn Ja, wird basierend auf den letzten 2500 aufgezeichneten Datenpunkten eine lineare Regressions-Tendenzlinie kalkuliert.
- **Verlaufsfenster** – Die Zeitspanne, um die die kalkulierte Tendenzlinie in die Zukunft verlängert wird. Überschreitet die vorhergesagte Trendlinie innerhalb der festgelegten Zeitspanne den Benachrichtigungsschwellenwert, wird eine Trendbenachrichtigungsbedingung erzeugt. In der Regel sollte ein Trendfenster auf die Zeitspanne eingestellt werden, die ggf. für die Vorbereitung auf eine Benachrichtigungsbedingung benötigt wird.

- **Trendbenachrichtigung scharf stellen** – Unterdrückt alle weiteren Trendbenachrichtigungsbedingungen für dasselbe Problem innerhalb derselben Zeitspanne.

# Erweiterte SNMP-Features

Voraussetzung für das manuelle Bearbeiten eines SNMP-Sets ist, dass Sie wissen, welche MIB-Objekte zu einem Gerät gehören sollten und welche nicht und dass Sie die Sammlungs- und Alarmschwellenwerte kennen, die dem Gerät idealerweise zugewiesen werden sollten. Doch was tun, wenn Sie sich bei einem bestimmten Gerät diesbezüglich nicht sicher sind? Unter "Monitoring > **SNMP zuordnen** *(siehe 20)*" finden Sie zwei erweiterte Ermittlungsfeatures, die ihnen weiterhelfen können:

- **Quick Sets** (siehe 27) – Es wird ein eingeschränkter SNMP-Ermittlungsdurchlauf auf einem SNMP-Gerät gestartet, um diejenigen MIB-Objekte auf dem Gerät zu ermitteln, die aktiv genutzt werden. Sie haben die Möglichkeit, nur die MIB-Objekte mit Werten auszuwählen und ein "Quick Set" zu erstellen, um sofort mit dem Monitoring des Geräts beginnen zu können. Beim Erstellen des Quick Sets wird für jedes MIB-Objekt stets der letzte Wert angezeigt.
- **Automatisch lernen** (siehe 29) – Sie können den beim Erstellen eines Quick Sets ursprünglich angezeigten Wert – oder die in einem Standard-SNMP-Set vordefinierten Werte – verwenden und einfach das Beste hoffen. Oder Sie aktivieren das automatische Lernen für ein bestimmtes Quick Set oder Standardset und lassen den Monitoring-Agent die passenden Schwellenwerte für Sie berechnen. Die standardmäßig festgelegte Dauer eines Lernzyklus beträgt eine Stunde. Während dieser Zeit bestimmt die Funktion "Automatisch lernen" den von einem MIB-Objekt auf einem Gerät übermittelten Durchschnittswert und legt die Schwellenwerte für die Sammlung sowie die Benachrichtigungsbedingungen fest. Sie haben die Möglichkeit, die Kriterien für das automatische Lernen zu verändern oder nach Beendigung des Lernzyklus Änderungen an den sich ergebenden Berechnungen vorzunehmen, wenn Sie möchten.

Weiterhin werden im Abschnitt **Erweiterte SNMP-Features** die folgenden Themen behandelt:

- **Individualisierte SNMP-Sätze** (siehe 30) – Damit bezeichnet man SNMP-Standardsätze, die auf ein einzelnes Gerät angewendet und dann manuell angepasst wurden.
- **SNMP-Typen** (siehe 30) – Damit bezeichnet man eine Methode, SNMP-Standardsätze, basierend auf dem während eines LAN-Watch festgestellten **SNMP-Typs** *(siehe 30)*, automatisch Geräten zuzuweisen.
- **SNMP-Objekte hinzufügen** (siehe 31) – Fügen Sie für ein SNMP-Set MIB-Objekte zu VSA hinzu, falls diese noch nicht verfügbar sind.
- **SNMP-Traps** (siehe 32) – Konfiguriert Benachrichtigungen für einen verwalteten Rechner, der auf SNMP-Traps "wartet", für den Fall, dass der Rechner eine **SNMP-Trap**-Nachricht erkennt.

## SNMP-Schnellsätze

Auf der Seite **SNMP-Info** wird eine Liste der MIB-Objekte angezeigt, die von dem jeweils ausgewählten SNMP-Gerät bereitgestellt werden. Diese MIB-Objekte werden durch Ausführen eines beschränkten SNMP-Durchlaufs auf allen ermittelten SNMP-Geräten ermittelt, wann immer ein **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/R8/index.asp#1944.htm)* stattfindet. Sie können die Liste der ermittelten MIB-Objekte verwenden, um sofort ein gerätespezifisches SNMP-Set mit der Bezeichnung **Schnellset** zu erstellen und auf das Gerät anzuwenden. Schnellsets entsprechen nach der Erstellung den Standardsets. Sie werden in Ihrem privaten Ordner in Monitor > **SNMP-Sets** und in der Dropdown-Liste in Monitor > **SNMP zuweisen** angezeigt. Ein `(QS)`-Präfix erinnert Sie daran, wie das Schnellset erstellt wurde. Wie beliebige andere Standardsets können Schnellsets für ein einzelnes Gerät *individualisiert*, mit **Auto-Lernen** *(siehe 29)* verwendet, für andere Benutzer freigegeben und über den VSA auf ähnliche Geräte angewendet werden.

1. Ermitteln Sie SNMP-Geräte über Monitor > **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/R8/index.asp#1944.htm)*.
2. Weisen Sie SNMP-Sets über Monitor > SNMP zuweisen den ermittelten Geräten zu.

3. Klicken Sie auf der Seite **SNMP zuweisen** auf den Hyperlink unterhalb des Namens des Geräts (SNMP-Info-Link), um einen Dialog anzuzeigen.
   - Klicken Sie auf **Gefundene MIB-Objekte** und wählen Sie mindestens ein MIB-Objekt aus, das auf dem gerade ausgewählten SNMP-Gerät gefunden wurde.
   - Klicken Sie auf **Schnellset-Elemente** und bearbeiten Sie bei Bedarf die Alarmschwellenwerte für ausgewählte MIB-Objekte.
   - Geben Sie in der Kopfzeile des Dialogfelds den Namen nach dem Präfix **(QS)** ein.
   - Klicken Sie auf die Schaltfläche **Anwenden**, um das Schnellset auf das Gerät anzuwenden.
4. Zeigen Sie vom Schnellset zurückgegebene SNMP-Monitordaten über Monitor > SNMP-Protokoll genau so an, wie Sie es bei einem anderen Standard-SNMP-Set tun würden.
5. Die Pflege des neuen Schnellsets kann wahlweise mit Monitor > SNMP-Sets erfolgen.

Über die folgenden Registerkarten auf der Seite **SNMP-Info-Link** können Sie ein SNMP-Schnellset konfigurieren.

### Registerkarte „Ermittelte MIB-Objekte“

Auf der Registerkarte **Ermittelte MIB-Objekte** werden alle beim letzten SNMP-Durchlauf ermittelten Objektsätze angezeigt, die für das angewählte SNMP-Gerät gelten. Sie können über diese Registerkarte Objekte und Instanzen zu einem SNMP-Schnellset für dieses Gerät hinzufügen.

- **Instanz hinzufügen** – Klicken Sie auf diese Option, um diese Instanz dieses Objekts zu einem SNMP-Schnellset hinzuzufügen, das auf der Registerkarte **SNMP-Set** des gleichen Fensters angezeigt wird.
- **Alle Instanzen hinzufügen** – Klicken Sie auf diese Option, um alle Instanzen dieses Objekts zu einem SNMP-Schnellset hinzuzufügen, das auf der Registerkarte **SNMP-Set** des gleichen Fensters angezeigt wird.
- **SNMP-Objekt** – Der Name des SNMP-Objekts. Wenn kein Name für das Objekt angegeben wird, wird die numerische OID-Bezeichnung angezeigt.
- **Instanz** – Die Instanz des Objekts. Viele Objekte haben mehrere Instanzen, von denen jedes einen anderen Wert haben kann. Als verschiedene Instanzen zählen beispielsweise die Ports eines Routers oder die Ablagefächer eines Druckers. Das Feld ist leer, wenn die letzte Ziffer der OID Null ist, was darauf hinweist, dass es nur ein Mitglied dieses Objekts gibt. Wenn eine Instanz nicht leer oder eine beliebige Zahl ungleich Null ist, so existieren mehrere Instanzen dieses Objekts für das Gerät. Sie können das Monitoring mehrerer Instanzen eines Objekts festlegen, indem Sie einen Zahlenbereich wie beispielsweise `1-5,6` oder `1,3,7` angeben. Sie können auch `All` eingeben.
- **Aktueller SNMP-Wert** – Der beim letzten SNMP-Durchlauf von der Objekt/Instanz-Kombination zurückgegebene Wert

### Schnellset-Elemente – Registerkarte

Auf der Registerkarte **Schnellset-Elemente** konfigurieren Sie die ausgewählten Objekte und Instanzen, die in das SNMP-Schnellset eingeschlossen werden sollen. Klicken Sie auf das Bearbeitungssymbol  , um die SNMP-Kontrollattribute für die ausgewählten Objekte zu definieren. Sie können auch mithilfe der Schaltfläche **Hinzufügen** ein neues Objekt hinzufügen und die gleichen Attribute festlegen.

- **SNMP-Objekt** – Der SNMP-Objektname oder die OID-Nummer.
- **SNMP-Instanz** – Die letzte Zahl einer Objekt-ID kann auch als eine Wertetabelle statt eines einzelnen Werts ausgedrückt werden. Falls die Instanz ein einzelner Wert ist, geben Sie `0` ein. Wenn die Instanz eine Wertetabelle ist, geben Sie einen Zahlenbereich ein, wie beispielsweise `1-5,6` oder `1,3,7`. Sie können auch `All` eingeben.
- **Alarm-Operator** – Wenn eine Zeichenfolge zurückgegeben wird, lauten die Optionen `Changed`, `Equal` oder `NotEqual`. Für numerische Rückgabewerte lauten die Optionen `Equal`, `NotEqual`, `Over` oder `Under`.
- **Alarmschwellenwert** – Legt einen festen Wert fest, mit dem der Rückgabewert verglichen wird, und verwendet den ausgewählten **Alarm-Operator**, um festzulegen, wann ein Alarm ausgelöst wird.

- **Wert zurückgegeben als** – Wenn das MIB-Objekt einen numerischen Wert zurückgibt, können Sie angeben, ob dieser Wert als eine **Summe** oder als eine **Rate pro Sekunde** zurückgegeben werden soll.
- **Aktueller SNMP-Wert** – Der beim letzten SNMP-Durchlauf von der Objekt/Instanz-Kombination zurückgegebene Wert

## Auto-Lernen - SNMP-Sets

Sie können **Auto-Lernen**-Alarmschwellenwerte für jedes beliebige SNMP-Set bzw. -Schnellset aktivieren, das Sie ausgewählten SNMP-Geräten zuweisen. Damit werden Alarmschwellenwerte basierend auf tatsächlichen Leistungsdaten auf die einzelnen SNMP-Geräte abgestimmt.

Jedes zugewiesene SNMP-Gerät generiert Leistungsdaten für die angegebene Zeitspanne. Während dieser Zeitspanne werden keine Alarme ausgelöst. Am Ende der **Auto-Lernen**-Sitzung wird der Alarmschwellenwert für jedes zugewiesene SNMP-Gerät basierend auf der tatsächlichen Leistung des SNMP-Geräts automatisch abgestimmt. Sie können die Alarmschwellenwerte, die durch **Auto-Lernen** berechnet wurden, manuell anpassen oder eine weitere **Auto-Lernen**-Sitzung ausführen. **Auto-Lernen** kann nicht mit individualisierten SNMP-Sets verwendet werden

So wenden Sie **Auto-Lernen**-Einstellungen auf ausgewählte SNMP-Geräte an:

1. Wählen Sie ein *Standard*-SNMP-Set aus der `<Select SNMP Set>`-Dropdown-Liste aus. Sie können auch auf das Bearbeitungssymbol eines SNMP-Sets klicken, der bereits einem Gerät zugeordnet ist, um den Identifikator in die `<Select SNMP Set>`-Dropdown-Liste zu übertragen.
2. Klicken Sie auf **Auto-Lernen**, um das Popup-Fenster Auto-Lernen einzublenden. Definieren Sie mithilfe eines Assistenten die Parameter, die zum Berechnen der Alarmschwellenwerte verwendet werden.
3. Weisen Sie dieses Standard-SNMP-Set, das durch Ihre **Auto-Lernen**-Parameter abgeändert wurde, ausgewählten SNMP-Geräten zu, falls dies noch nicht geschehen ist.

Sobald **Auto-Lernen** auf eine Rechner-ID angewendet und für die vorgegebene Zeitspanne ausgeführt wurde, können Sie für ein bestimmtes SNMP-Gerät auf das Auto-Lernen-überschreiben-Symbol klicken und die berechneten Alarmschwellenwerte manuell anpassen. Sie können auch **Auto-Lernen** in einer neuen Sitzung unter Verwendung der tatsächlichen Leistungsdaten erneut ausführen, um die Alarmschwellenwerte neu zu berechnen.

Verwenden Sie das folgende Verfahren, um SNMP-Auto-Lernen-Einstellungen im Popup-Fenster **Auto-Lernen** zu konfigurieren:

Klicken Sie auf das Bearbeitungssymbol , um einen Assistenten aufzurufen, der Sie durch die drei Schritte zum Bearbeiten von Auto-Lernen-Alarmschwellenwerten führt.

1. Aktivieren Sie ggf. **Automatisch lernen** für dieses SNMP-Objekt, indem Sie `Yes - Include` auswählen. Wenn `No - Do not include` ausgewählt ist, sind keine weiteren Auswahlen in diesem Assistenten möglich.
   - **Zeitspanne** – Geben Sie an, wie lange Leistungsdaten erfasst und zur automatischen Berechnung der Alarmschwellenwerte verwendet werden sollen. Während dieser Zeitspanne werden keine Alarme gemeldet.
2. Zeigt das **SNMP-Objekt** des geänderten Alarmschwellenwerts an. Diese Option kann nicht geändert werden.
3. Geben Sie Parameter für die Wertberechnung ein.
   - **Berechnung** – Geben Sie einen Parameter für die Wertberechnung ein. Mögliche Optionen: `MIN`, `MAX` oder `AVG`. Bei Auswahl von `MAX` wird beispielsweise der maximale Wert berechnet, der für ein SNMP-Objekt während der oben angegebenen **Zeitspanne** erfasst wurde.
   - **% Anstieg** – Fügen Sie diesen Anstieg zu dem oben berechneten **Berechnung**swert hinzu, wobei der **Berechnung**swert 100% darstellt. Der resultierende Wert stellt den Alarmschwellenwert dar.

- **Minimum** – Legen Sie einen Mindestwert für den Alarmschwellenwert fest. Dieser Wert wird automatisch als *zwei Standardabweichungen unter* dem berechneten **Berechnung**swert kalkuliert, doch dieser Wert kann manuell überschrieben werden.
- **Maximum** – Legen Sie einen Maximalwert für den Alarmschwellenwert fest. Dieser Wert wird automatisch als *zwei Standardabweichungen über* dem berechneten **Berechnung**swert kalkuliert, doch dieser Wert kann manuell überschrieben werden.

## Individualisierte SNMP-Sets

Sie können die SNMP-Set-Einstellungen für einen einzelnen Rechner *individualisieren*.

1. Wählen Sie ein *Standard*-SNMP-Set aus der `<Select Monitor Set>`-Dropdown-Liste aus.
2. Weisen Sie dieses Standard-SNMP-Set einem SNMP-Gerät zu. Der Name des SNMP-Sets wird in der Spalte **SNMP-Info/SNMP-Set** angezeigt.
3. Klicken Sie auf das individualisierte SNMP-Set-Symbol  in der Spalte **SNMP-Info/SNMP-Set**, um die gleichen Optionen wie beim Definieren eines Standard-SNMP-Sets anzuzeigen. *Bei einem individualisierten SNMP-Set wird dem Namen des SNMP-Sets ein (IND) Präfix vorangestellt.*
4. Nehmen Sie Änderungen an dem neuen individualisierten SNMP-Set vor. Diese Änderungen gelten nur für das einzelne SNMP-Gerät, dem dieses SNMP-Set zugewiesen wurde.

> **Hinweis:** Änderungen an einem SNMP-Set haben keine Auswirkungen auf die individualisierten SNMP-Sets, die davon kopiert wurden.

## SNMP-Typen

Die meisten SNMP-Geräte werden mithilfe des MIB-Objekts `system.sysServices.0` als ein bestimmter SNMP-Gerätetyp klassifiziert. Beispielsweise identifizieren sich einige Router selbst generisch als Router, indem sie den Wert `77` für das MIB-Objekt `system.sysServices.0` zurückgeben. Sie können den vom MIB-Objekt `system.sysServices.0` zurückgegebenen Wert verwenden, um SNMP-Sets automatisch zu Geräten zuzuweisen, sobald sie von einem LAN-Watch erkannt wurden.

> **Hinweis:** Die gesamte OID für `system.sysServices.0` ist `.1.3.6.1.2.1.1.7.0` oder `.iso.org.dod.internet.mgmt.mib-2.system.sysServices`.

Weisen Sie folgendermaßen SNMP-Sets bestimmten Geräten *automatisch nach Typ* zu:

1. Fügen Sie SNMP-*Typen* über die Registerkarte **SNMP-Gerät** in Monitor > Monitorlisten hinzu bzw. bearbeiten Sie sie.
2. Fügen Sie den vom MIB-Objekt `system.sysServices.0` zurückgegebenen *und mit dem jeweiligen SNMP-Typ verknüpften* Wert hinzu bzw. bearbeiten Sie ihn mithilfe der Registerkarte **SNMP-Dienste** in Monitor > **Monitorlisten**.
3. Verknüpfen Sie einen SNMP-*Typ* über die Dropdown-Liste **Automatische Bereitstellung auf** in Monitor > SNMP-Sets > SNMP-Set definieren mit einem SNMP-*Set*.
4. Führen Sie einen **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/R8/index.asp#1944.htm)* durch. Während des LAN-Watch werden SNMP-Sets automatisch zugewiesen, um von SNMP-Sets überwacht zu werden, wenn das SNMP-Gerät einen Wert für das MIB-Objekt `system.sysServices.0` zurückgibt, der dem SNMP-Typ entspricht, der mit diesen SNMP-Sets verknüpft ist.

Weisen Sie folgendermaßen SNMP-Sets bestimmten Geräten *manuell* zu:

- Mit Monitor > SNMP-Typ konfigurieren können Sie einen SNMP-Typ einem SNMP-Gerät zuweisen. In diesem Fall beginnt das System automatisch mit dem Monitoring dieses SNMP-Geräts anhand dieses SNMP-Sets.

# Hinzufügen von SNMP-Objekten

Wenn Sie Objekte zum Einschluss in ein SNMP-Set auswählen, haben Sie die Möglichkeit, ein neues SNMP-Objekt hinzuzufügen. In den meisten Fällen ist dies nicht erforderlich, da die benötigten Objekte normalerweise bei einem **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/R8/index.asp#1944.htm)* ermittelt werden. Falls Sie jedoch ein SNMP-Objekt manuell aus einer MIB-Datei hinzufügen, so können Sie dies über Monitor > SNMP-Objekt hinzufügen oder durch Klicken auf die Schaltfläche **Objekt hinzufügen...** beim Konfigurieren eines SNMP-Sets tun.

Die Seite **SNMP MIB-Baumstruktur** lädt eine Management Information Base (MIB)-Datei und zeigt diese als eine erweiterbare *Baumstruktur* von MIB-Objekten an. Alle MIB-Objekte werden gemäß ihrer Position in der MIB-Baumstruktur klassifiziert. Sobald diese Baumstruktur geladen wurde, können Sie die MIB-Objekte auswählen, die Sie auf Ihrem VSA installieren möchten. SNMP-Gerätehersteller stellen für gewöhnlich MIB-Dateien für die von ihnen hergestellten Geräte auf ihren Websites zur Verfügung.

**Hinweis:** Sie können die komplette Liste der bereits installierten MIB-Objekte überprüfen, indem Sie die Registerkarte **MIB OIDs** in Monitor > Monitorliste aufrufen. Dies ist die Liste der MIB-Objekte, die Sie gegenwärtig in ein SNMP-Set einschließen können.

Falls ein Hersteller Ihnen eine MIB-Datei zur Verfügung gestellt hat, können Sie die folgenden Schritte ausführen:

1. Laden Sie die MIB-Datei des Herstellers durch Klicken auf **MIB... laden**. Möglicherweise wird eine Meldung angezeigt, dass abhängige Dateien vorliegen, die zuerst geladen werden müssen. Diese werden wahrscheinlich ebenfalls vom Hersteller bereitgestellt.
2. Klicken Sie auf die ⊞ Erweiterungssymbole in der MIB-Baumstruktur *(siehe unten stehende Beispielabbildung)* und ermitteln Sie die gewünschten Kontrollelemente. Aktivieren Sie jedes entsprechende Kontrollkästchen.
3. Klicken Sie auf **MIB-Objekte hinzufügen**, um die ausgewählten Elemente aus Schritt 2 in die MIB-Objektliste zu verschieben.
4. Konfigurieren Sie die Einstellungen für das neue SNMP-Objekt innerhalb eines SNMP-Sets.
5. Die Anzahl der MIB-Objekte im Verzeichnis kann schnell unhandlich werden. Sobald die gewünschten MIB Objekte hinzugefügt wurden, kann die MIB-Datei entfernt werden.

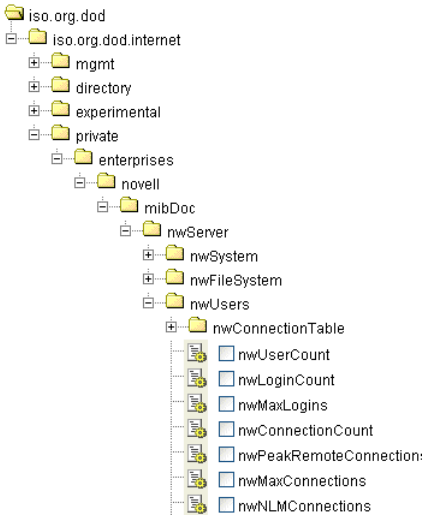
## MIB laden

Klicken Sie auf **MIB laden...**, um nach einer MIB-Datei zu suchen und diese hochzuladen. Wenn beim Hinzufügen eines MIB-Objekts die folgenden standardmäßigen MIB II-Dateien nicht vorliegen, die von den meisten MIBs benötigt werden, werden diese automatisch geladen: `snmp-tc`, `snmp-smi`, `snmp-conf`, `rfc1213`, `rfc1759`. Nachdem diese Dateien geladen wurden, kann die MIB-Baumstruktur am unteren Rand der Seite **SNMP-Objekt hinzufügen** geöffnet werden. Navigieren Sie in dieser Baumstruktur, um nach den neuen Objekten zu suchen, die der Benutzer auswählen kann. Die meisten MIBs privater Hersteller werden im Ordner `Private` installiert. *Siehe nachstehende Beispielabbildung*.

**Hinweis:** Die MIB-Datei kann jederzeit geladen und entfernt werden. Dies hat *keinen* Einfluss auf MIB-Objekte, die in SNMP-Sets verwendet werden.

### MIB-Baumstruktur

Die MIB-Baumstruktur repräsentiert alle gegenwärtig geladenen MIB-Dateiobjekte, aus denen der Benutzer eine Auswahl treffen kann.

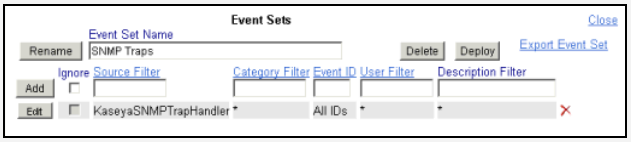



## SNMP-Traps

Die Seite **SNMP-Traps-Meldung** konfiguriert Meldungen für einen verwalteten Rechner und agiert als SNMP-Trap-Listener, wenn eine **SNMP-Trap**-Meldung erkannt wird.

Wenn **SNMP-Traps-Meldung** mit einem verwalteten Rechner verknüpft ist, wird auf diesem Rechner ein Dienst mit der Bezeichnung `Kaseya SNMP Trap Handler` gestartet. Dieser Dienst sucht nach SNMP-Trap-Meldungen, die von SNMP-fähigen Geräten auf dem gleichen LAN gesendet wurden. Wird eine SNMP-Trap-Meldung vom Dienst empfangen, wird eine SNMP-Trap-`Warning` zum `Application`-Ereignisprotokoll des verwalteten Rechners hinzugefügt. Die **Quelle** dieser `Application`-Ereignisprotokolleinträge ist immer `KaseyaSNMPTrapHandler`.

**Hinweis:** Erstellen Sie einen Ereignissatz, der `KaseyaSNMPTrapHandler` als **Quelle** enthält. Verwenden Sie Sternchen `*` für die anderen Kriterien, wenn Sie die Ereignisse nicht weiter filtern möchten.



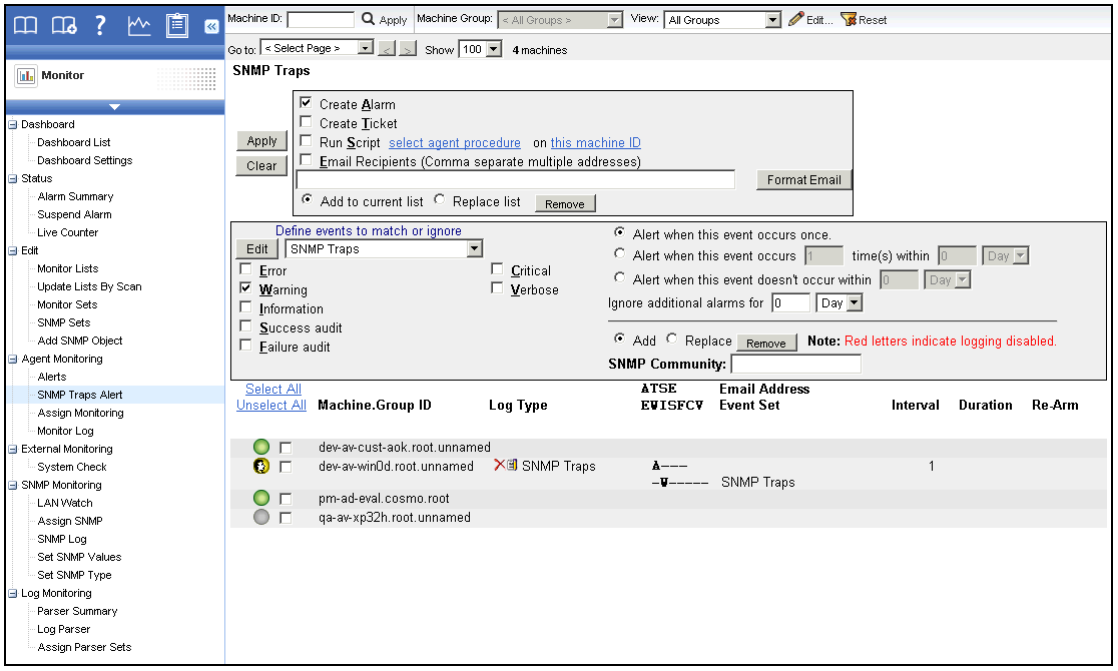

**Hinweis:** SNMP verwendet den Standard-UDP-Port 162 für SNMP-Trap-Meldungen. Achten Sie darauf, dass dieser Port offen ist, wenn eine Firewall aktiviert ist.

### SNMP-Traps-Meldung erstellen

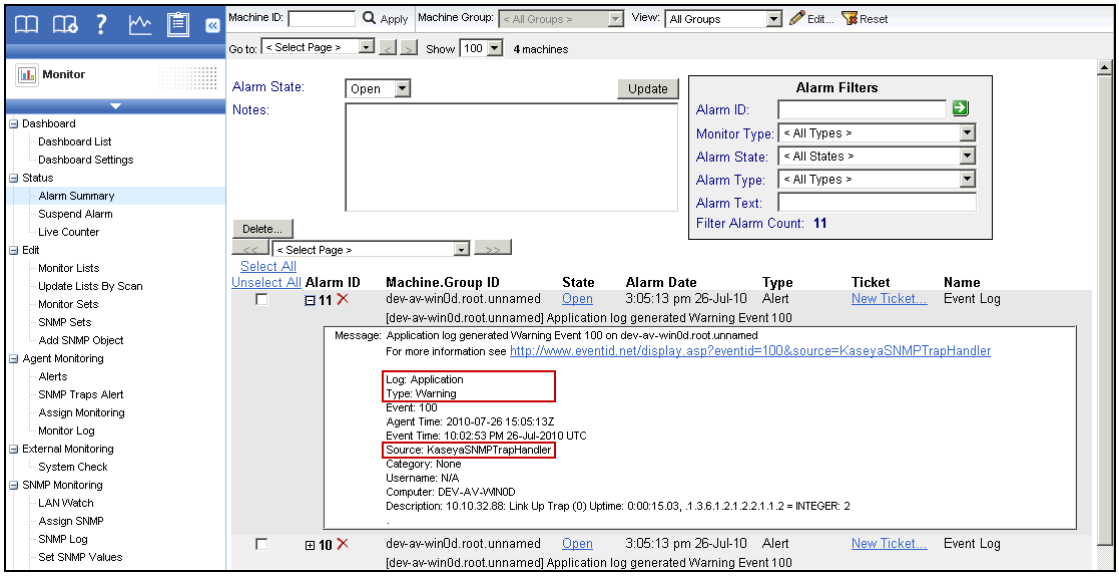
1. Wählen Sie die Seite Monitor > **SNMP-Traps-Meldung** aus.
2. Wählen Sie den **Ereignissatz**-Filter aus, der zum Filtern der Ereignisse verwendet wird, die Meldungen auslösen. Wählen Sie keinen Ereignissatz aus, in den *alle* SNMP-Trap-Ereignisse eingeschlossen werden sollen.
3. Aktivieren Sie das Kontrollkästchen neben der **Ereigniskategorie** `Warning`. *Keine anderen Ereigniskategorien werden von SNMP-Trap-Alarm verwendet.*

**Hinweis:** Rot markierte **Ereigniskategorien** (EWISFCV) geben an, dass diese Ereigniskategorien nicht vom VSA gesammelt werden. **Ereignisprotokoll-Meldungen werden auch generiert, wenn die Ereignisprotokolle nicht von VSA gesammelt werden.**

4. Geben Sie die *Häufigkeit* der Meldungsbedingung an, die zum Auslösen einer Meldung erforderlich ist:
   - **Warnen, wenn dieses Ereignis ein einziges Mal eintritt**
   - **Warnen, wenn dieses Ereignis <N> Mal innerhalb von <N> <Perioden>** eintritt.
   - **Warnen, wenn dieses Ereignis nicht innerhalb von <N> <Perioden>** eintritt.
   - **Zusätzliche Alarme nicht beachten für <N> <Perioden>**.
5. Klicken Sie auf die Optionsfelder **Hinzufügen** oder **Ersetzen** und anschließend auf **Anwenden**, um die ausgewählten Ereignistypmeldungen den ausgewählten Rechner-IDs zuzuweisen.
6. Klicken Sie auf **Entfernen**, um alle ereignisbasierten Meldungen von ausgewählten Rechner-IDs zu entfernen.
7. Ignorieren Sie das Feld **SNMP-Community**. *Diese Option ist noch nicht implementiert.*




Sie haben die Möglichkeit, Benachrichtigungen für SNMP-Trap-Benachrichtigungen über "Monitoring > Benachrichtigungsübersicht" zu prüfen.



# Inhaltsverzeichnis