Managen von SNMP-Warnmeldungen

SANtricity 11.7

NetApp
February 12, 2024

Inhalt

Managen von SNMP-Warnmeldungen

Konfigurieren von SNMP-Warnmeldungen

Um SNMP-Warnungen (Simple Network Management Protocol) zu konfigurieren, müssen Sie mindestens einen Server identifizieren, auf dem der Ereignismonitor des Speicherarrays SNMP-Traps senden kann. Die Konfiguration erfordert einen Community-Namen oder Benutzernamen und eine IP-Adresse für den Server.

Bevor Sie beginnen

- Ein Netzwerkserver muss mit einer SNMP-Dienstanwendung konfiguriert sein. Sie benötigen die Netzwerkadresse dieses Servers (entweder eine IPv4- oder eine IPv6-Adresse), damit der Ereignismonitor Trap-Meldungen an diese Adresse senden kann. Sie können mehrere Server verwenden (bis zu 10 Server sind zulässig).
- Die Management Information Base (MIB)-Datei wurde kopiert und mit der SNMP-Dienst-Anwendung auf dem Server kompiliert. Diese MIB-Datei definiert die Daten, die überwacht und verwaltet werden.

  Wenn Sie nicht über die MIB-Datei, können Sie sie von der NetApp Support-Website erhalten:

  - Gehen Sie zu "NetApp Support".
  - Klicken Sie auf die Registerkarte **Downloads** und wählen Sie dann **Downloads**.
  - Klicken Sie auf **E-Series SANtricity OS Controller Software**.
  - Wählen Sie **Letzte Version Herunterladen**.
  - Melden Sie sich an.
  - Akzeptieren Sie die Vorsichtserklärung und die Lizenzvereinbarung.
  - Scrollen Sie nach unten, bis Sie die MIB-Datei für Ihren Controller-Typ sehen, und klicken Sie dann auf den Link, um die Datei herunterzuladen.

Über diese Aufgabe

Diese Aufgabe beschreibt, wie Sie den SNMP-Server für Trap-Ziele identifizieren und anschließend Ihre Konfiguration testen.

Schritte

1. Wählen Sie Menü:Einstellungen[Alarme].
2. Wählen Sie die Registerkarte **SNMP** aus.

   Bei der Ersteinrichtung wird auf der Registerkarte SNMP „Configure Communities/Users“ angezeigt.

3. Wählen Sie * Communities/Benutzer Konfigurieren*.

   Das Dialogfeld SNMP-Version auswählen wird geöffnet.

4. Wählen Sie die SNMP-Version für die Alarme aus, entweder **SNMPv2c** oder **SNMPv3**.

   Je nach Auswahl wird das Dialogfeld „Communities konfigurieren“ oder das Dialogfeld „SNMPv3-Benutzer konfigurieren“ geöffnet.

5. Befolgen Sie die entsprechenden Anweisungen für SNMPv2c (Communities) oder SNMPv3 (Benutzer):

- **SNMPv2c (Communities)** — Geben Sie im Dialogfeld „Configure Communities“ eine oder mehrere Community-Strings für die Netzwerkserver ein. Ein Community-Name ist eine Zeichenfolge, die einen bekannten Satz von Management Stations identifiziert und in der Regel von einem Netzwerkadministrator erstellt wird. Es besteht nur aus druckbaren ASCII-Zeichen. Sie können bis zu 256 Communities hinzufügen. Wenn Sie fertig sind, klicken Sie auf **Speichern**.
- **SNMPv3 (Users)** — Klicken Sie im Dialogfeld Configure SNMPv3 Users auf **Add**, und geben Sie anschließend die folgenden Informationen ein:
  - **Benutzername** — Geben Sie einen Namen ein, um den Benutzer zu identifizieren, der bis zu 31 Zeichen lang sein kann.
  - **Engine ID** — Wählen Sie die Engine-ID aus, die zur Generierung von Authentifizierungs- und Verschlüsselungsschlüsseln für Nachrichten verwendet wird, und müssen in der Verwaltungsdomäne eindeutig sein. In den meisten Fällen sollten Sie **Lokal** wählen. Wenn Sie eine nicht-Standardkonfiguration haben, wählen Sie **Benutzerdefiniert** aus. Ein weiteres Feld wird angezeigt, in dem Sie die autoritative Engine-ID als Hexadezimalstring eingeben müssen, wobei eine gerade Anzahl von Zeichen zwischen 10 und 32 Zeichen lang ist.
  - **Authentifizierungsdaten** — Wählen Sie ein Authentifizierungsprotokoll, das die Identität der Benutzer sicherstellt. Geben Sie dann ein Authentifizierungspasswort ein, das erforderlich ist, wenn das Authentifizierungsprotokoll festgelegt oder geändert wird. Das Passwort muss zwischen 8 und 128 Zeichen lang sein.
  - **Datenschutzhinweise** — Wählen Sie ein Datenschutzprotokoll, das zur Verschlüsselung der Inhalte von Nachrichten verwendet wird. Geben Sie dann ein Datenschutzkennwort ein, das erforderlich ist, wenn das Datenschutzprotokoll festgelegt oder geändert wird. Das Passwort muss zwischen 8 und 128 Zeichen lang sein. Wenn Sie fertig sind, klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **Schließen**.

6. Klicken Sie auf der Seite Warnungen auf der Registerkarte SNMP auf **Trap Destinations hinzufügen**.

   Das Dialogfeld Trap-Ziele hinzufügen wird geöffnet.

7. Geben Sie ein oder mehrere Trap-Ziele ein, wählen Sie die zugehörigen Community-Namen oder Benutzernamen aus, und klicken Sie dann auf **Hinzufügen**.
   - **Trap-Ziel** — Geben Sie eine IPv4- oder IPv6-Adresse des Servers ein, auf dem ein SNMP-Dienst ausgeführt wird.
   - **Community-Name oder Benutzername** — Wählen Sie in der Dropdown-Liste den Community-Namen (SNMPv2c) oder den Benutzernamen (SNMPv3) für dieses Trap-Ziel aus. (Wenn Sie nur einen definiert haben, wird der Name bereits in diesem Feld angezeigt.)
   - **Authentifizierungsfehler senden Trap** — Wählen Sie diese Option (das Kontrollkästchen) aus, wenn Sie das Trap-Ziel benachrichtigen möchten, wenn eine SNMP-Anfrage aufgrund eines nicht erkannten Community-Namens oder Benutzernamens abgelehnt wird. Nach dem Klicken auf **Hinzufügen** werden die Trap-Ziele und die zugehörigen Namen auf der Seite **SNMP** auf der Registerkarte **Alarme** angezeigt.
8. Um sicherzustellen, dass ein Trap gültig ist, wählen Sie ein Trap-Ziel aus der Tabelle aus, und klicken Sie dann auf **Trap-Ziel testen**, um einen Test-Trap an die konfigurierte Adresse zu senden.

Ergebnisse

Der Ereignismonitor sendet SNMP-Traps an den/die Server(s), wenn ein alertable Ereignis auftritt.

Fügen Sie Trap-Ziele für SNMP-Warnungen hinzu

Sie können bis zu 10 Server zum Senden von SNMP-Traps hinzufügen.

Bevor Sie beginnen

- Der Netzwerkserver, den Sie hinzufügen möchten, muss mit einer SNMP-Serviceanwendung konfiguriert sein. Sie benötigen die Netzwerkadresse dieses Servers (entweder eine IPv4- oder eine IPv6-Adresse), damit der Ereignismonitor Trap-Meldungen an diese Adresse senden kann. Sie können mehrere Server verwenden (bis zu 10 Server sind zulässig).
- Die Management Information Base (MIB)-Datei wurde kopiert und mit der SNMP-Dienst-Anwendung auf dem Server kompiliert. Diese MIB-Datei definiert die Daten, die überwacht und verwaltet werden.

  Wenn Sie nicht über die MIB-Datei, können Sie sie von der NetApp Support-Website erhalten:

  - Gehen Sie zu "NetApp Support".
  - Klicken Sie auf **Downloads** und wählen Sie dann **Downloads**.
  - Klicken Sie auf **E-Series SANtricity OS Controller Software**.
  - Wählen Sie **Letzte Version Herunterladen**.
  - Melden Sie sich an.
  - Akzeptieren Sie die Vorsichtserklärung und die Lizenzvereinbarung.
  - Scrollen Sie nach unten, bis Sie die MIB-Datei für Ihren Controller-Typ sehen, und klicken Sie dann auf den Link, um die Datei herunterzuladen.

Schritte

1. Wählen Sie Menü:Einstellungen[Alarme].
2. Wählen Sie die Registerkarte **SNMP** aus.

   Die aktuell definierten Trap-Ziele werden in der Tabelle angezeigt.

3. Wählen Sie **Trap Desinations Hinzufügen**.

   Das Dialogfeld Trap-Ziele hinzufügen wird geöffnet.

4. Geben Sie ein oder mehrere Trap-Ziele ein, wählen Sie die zugehörigen Community-Namen oder Benutzernamen aus, und klicken Sie dann auf **Hinzufügen**.
   - **Trap-Ziel** — Geben Sie eine IPv4- oder IPv6-Adresse des Servers ein, auf dem ein SNMP-Dienst ausgeführt wird.
   - **Community-Name oder Benutzername** — Wählen Sie in der Dropdown-Liste den Community-Namen (SNMPv2c) oder den Benutzernamen (SNMPv3) für dieses Trap-Ziel aus. (Wenn Sie nur einen definiert haben, wird der Name bereits in diesem Feld angezeigt.)
   - **Authentifizierungsfehler senden Trap** — Wählen Sie diese Option (das Kontrollkästchen) aus, wenn Sie das Trap-Ziel benachrichtigen möchten, wenn eine SNMP-Anfrage aufgrund eines nicht erkannten Community-Namens oder Benutzernamens abgelehnt wird. Nach dem Klicken auf **Hinzufügen** werden die Trap-Ziele und die zugehörigen Community-Namen oder Benutzernamen in der Tabelle angezeigt.
5. Um sicherzustellen, dass ein Trap gültig ist, wählen Sie ein Trap-Ziel aus der Tabelle aus, und klicken Sie dann auf **Trap-Ziel testen**, um einen Test-Trap an die konfigurierte Adresse zu senden.

Ergebnisse

Der Ereignismonitor sendet SNMP-Traps an den/die Server(s), wenn ein alertable Ereignis auftritt.

Konfigurieren Sie SNMP-MIB-Variablen

Für SNMP-Warnungen können Sie optional Management Information Base (MIB)-Variablen konfigurieren, die in SNMP-Traps angezeigt werden. Diese Variablen können den Namen des Speicher-Arrays, den Speicherort des Arrays und einen Ansprechpartner zurückgeben.

Bevor Sie beginnen

Die MIB-Datei muss kopiert und mit der SNMP-Dienst-Anwendung auf dem Server kompiliert werden.

Wenn Sie keine MIB-Datei haben, können Sie es wie folgt erhalten:

- Gehen Sie zu "NetApp Support".
- Klicken Sie auf **Downloads** und wählen Sie dann **Downloads**.
- Klicken Sie auf **E-Series SANtricity OS Controller Software**.
- Wählen Sie **Letzte Version Herunterladen**.
- Melden Sie sich an.
- Akzeptieren Sie die Vorsichtserklärung und die Lizenzvereinbarung.
- Scrollen Sie nach unten, bis Sie die MIB-Datei für Ihren Controller-Typ sehen, und klicken Sie dann auf den Link, um die Datei herunterzuladen.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie MIB-Variablen für SNMP-Traps definiert werden. Diese Variablen können als Antwort auf SNMP GetRequests folgende Werte zurückgeben:

- `sysName` (Name für das Speicher-Array)
- `sysLocation` (Speicherort des Speicher-Arrays)
- `sysContact` (Name eines Administrators)

Schritte

1. Wählen Sie Menü:Einstellungen[Alarme].
2. Wählen Sie die Registerkarte **SNMP** aus.
3. Wählen Sie **Konfigurieren von SNMP-MIB-Variablen**.

   Das Dialogfeld SNMP-MIB-Variablen konfigurieren wird geöffnet.

4. Geben Sie einen oder mehrere der folgenden Werte ein, und klicken Sie dann auf **Speichern**.
   - **Name** — der Wert für die MIB-Variable `sysName`. Geben Sie beispielsweise einen Namen für das Speicher-Array ein.
   - **Lage** — der Wert für die MIB Variable `sysLocation`. Geben Sie beispielsweise einen Speicherort des Speicher-Arrays ein.
   - **Kontakt** — der Wert für die MIB-Variable `sysContact`. Geben Sie beispielsweise einen Administrator ein, der für das Speicher-Array verantwortlich ist.

Ergebnisse

Diese Werte werden in SNMP-Trap-Meldungen für Storage Array-Warnungen angezeigt.

Communities für SNMPv2c-Traps bearbeiten

Sie können Community-Namen für SNMPv2c-Traps bearbeiten.

Bevor Sie beginnen

Ein Community-Name muss erstellt werden.

Schritte

1. Wählen Sie MENU:Einstellen von[Warnungen].
2. Wählen Sie die Registerkarte **SNMP** aus.

   Die Trap-Ziele und Community-Namen werden in der Tabelle angezeigt.

3. Wählen Sie * Communities Konfigurieren*.
4. Geben Sie den neuen Community-Namen ein und klicken Sie dann auf **Speichern**. Community-Namen können nur aus druckbaren ASCII-Zeichen bestehen.

Ergebnisse

Auf der Registerkarte SNMP der Seite Meldungen wird der aktualisierte Community-Name angezeigt.

Benutzereinstellungen für SNMPv3-Traps bearbeiten

Sie können Benutzerdefinitionen für SNMPv3-Traps bearbeiten.

Bevor Sie beginnen

Für den SNMPv3-Trap muss ein Benutzer erstellt werden.

Schritte

1. Wählen Sie Menü:Einstellungen[Alarme].
2. Wählen Sie die Registerkarte **SNMP** aus.

   Die Trap-Ziele und Benutzernamen werden in der Tabelle angezeigt.

3. Um eine Benutzerdefinition zu bearbeiten, wählen Sie den Benutzer in der Tabelle aus und klicken dann auf **Benutzer konfigurieren**.
4. Klicken Sie im Dialogfeld auf **Einstellungen anzeigen/bearbeiten**.
5. Bearbeiten Sie folgende Informationen:
   - **Benutzername** — Ändern Sie den Namen, der den Benutzer identifiziert, der bis zu 31 Zeichen lang sein kann.
   - **Engine ID** — Wählen Sie die Engine-ID aus, die zur Generierung von Authentifizierungs- und Verschlüsselungsschlüsseln für Nachrichten verwendet wird, und müssen in der Verwaltungsdomäne eindeutig sein. In den meisten Fällen sollten Sie **Lokal** wählen. Wenn Sie eine nicht-Standardkonfiguration haben, wählen Sie **Benutzerdefiniert** aus. Ein weiteres Feld wird angezeigt, in dem Sie die autoritative Engine-ID als Hexadezimalstring eingeben müssen, wobei eine gerade Anzahl von Zeichen zwischen 10 und 32 Zeichen lang ist.
   - **Authentifizierungsdaten** — Wählen Sie ein Authentifizierungsprotokoll, das die Identität der Benutzer sicherstellt. Geben Sie dann ein Authentifizierungspasswort ein, das erforderlich ist, wenn das Authentifizierungsprotokoll festgelegt oder geändert wird. Das Passwort muss zwischen 8 und 128 Zeichen lang sein.

- **Datenschutzhinweise** — Wählen Sie ein Datenschutzprotokoll, das zur Verschlüsselung der Inhalte von Nachrichten verwendet wird. Geben Sie dann ein Datenschutzkennwort ein, das erforderlich ist, wenn das Datenschutzprotokoll festgelegt oder geändert wird. Das Passwort muss zwischen 8 und 128 Zeichen lang sein.

Ergebnisse

Auf der Registerkarte SNMP der Seite Meldungen werden die aktualisierten Einstellungen angezeigt.

Fügen Sie Communities für SNMPv2c-Traps hinzu

Sie können bis zu 256 Community-Namen für SNMPv2c-Traps hinzufügen.

Schritte

1. Wählen Sie Menü:Einstellungen[Alarme].
2. Wählen Sie die Registerkarte **SNMP** aus.

   Die Trap-Ziele und Community-Namen werden in der Tabelle angezeigt.

3. Wählen Sie * Communities Konfigurieren*.

   Das Dialogfeld „Communities konfigurieren“ wird geöffnet.

4. Wählen Sie **Weitere Community hinzufügen**.
5. Geben Sie den neuen Community-Namen ein und klicken Sie dann auf **Speichern**.

Ergebnisse

Der neue Community-Name wird auf der Registerkarte SNMP der Seite Meldungen angezeigt.

Benutzer für SNMPv3-Traps hinzufügen

Sie können bis zu 256 Benutzer für SNMPv3-Traps hinzufügen.

Schritte

1. Wählen Sie Menü:Einstellungen[Alarme].
2. Wählen Sie die Registerkarte **SNMP** aus.

   Die Trap-Ziele und Benutzernamen werden in der Tabelle angezeigt.

3. Wählen Sie **Benutzer Konfigurieren**.

   Das Dialogfeld SNMPv3-Benutzer konfigurieren wird geöffnet.

4. Wählen Sie **Hinzufügen**.
5. Geben Sie die folgenden Informationen ein, und klicken Sie dann auf **Hinzufügen**.
   - **Benutzername** — Geben Sie einen Namen ein, um den Benutzer zu identifizieren, der bis zu 31 Zeichen lang sein kann.
   - **Engine ID** — Wählen Sie die Engine-ID aus, die zur Generierung von Authentifizierungs- und Verschlüsselungsschlüsseln für Nachrichten verwendet wird, und müssen in der Verwaltungsdomäne eindeutig sein. In den meisten Fällen sollten Sie **Lokal** wählen. Wenn Sie eine nicht-Standardkonfiguration haben, wählen Sie **Benutzerdefiniert** aus. Ein weiteres Feld wird angezeigt, in

dem Sie die autoritative Engine-ID als Hexadezimalstring eingeben müssen, wobei eine gerade Anzahl von Zeichen zwischen 10 und 32 Zeichen lang ist.

- **Authentifizierungsdaten** — Wählen Sie ein Authentifizierungsprotokoll, das die Identität der Benutzer sicherstellt. Geben Sie dann ein Authentifizierungspasswort ein, das erforderlich ist, wenn das Authentifizierungsprotokoll festgelegt oder geändert wird. Das Passwort muss zwischen 8 und 128 Zeichen lang sein.
- **Datenschutzhinweise** — Wählen Sie ein Datenschutzprotokoll, das zur Verschlüsselung der Inhalte von Nachrichten verwendet wird. Geben Sie dann ein Datenschutzkennwort ein, das erforderlich ist, wenn das Datenschutzprotokoll festgelegt oder geändert wird. Das Passwort muss zwischen 8 und 128 Zeichen lang sein.

Entfernen Sie Communities für SNMPv2c-Traps

Sie können einen Community-Namen für SNMPv2c-Traps entfernen.

Schritte

1. Wählen Sie Menü:Einstellungen[Alarme].
2. Wählen Sie die Registerkarte **SNMP** aus.

   Die Trap-Ziele und Community-Namen werden auf der Seite **Alerts** angezeigt.

3. Wählen Sie * Communities Konfigurieren*.

   Das Dialogfeld „Communities konfigurieren“ wird geöffnet.

4. Wählen Sie den Community-Namen aus, den Sie löschen möchten, und klicken Sie auf das Symbol **Entfernen** (X) ganz rechts.

   Wenn Trap-Ziele mit diesem Community-Namen verknüpft sind, werden im Dialogfeld Community entfernen bestätigen die betroffenen Trap-Zieladressen angezeigt.

5. Bestätigen Sie den Vorgang, und klicken Sie dann auf **Entfernen**.

Ergebnisse

Der Community-Name und das zugehörige Trap-Ziel werden von der Seite Alerts entfernt.

Benutzer für SNMPv3-Traps entfernen

Sie können einen Benutzer für SNMPv3-Traps entfernen.

Schritte

1. Wählen Sie Menü:Einstellungen[Alarme].
2. Wählen Sie die Registerkarte **SNMP** aus.

   Die Trap-Ziele und Benutzernamen werden auf der Seite Meldungen angezeigt.

3. Wählen Sie **Benutzer Konfigurieren**.

   Das Dialogfeld SNMPv3-Benutzer konfigurieren wird geöffnet.

4. Wählen Sie den Benutzernamen aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.

5. Bestätigen Sie den Vorgang, und klicken Sie dann auf **Löschen**.

Ergebnisse

Der Benutzername und das zugehörige Trap-Ziel werden von der Seite Warnungen entfernt.

Löschen von Trap-Zielen

Sie können eine Trap-Zieladresse löschen, sodass der Event-Monitor des Speicherarrays keine SNMP-Traps mehr an diese Adresse sendet.

Schritte

1. Wählen Sie Menü:Einstellungen[Alarme].
2. Wählen Sie die Registerkarte **SNMP** aus.

   Die Trap-Zieladressen werden in der Tabelle angezeigt.

3. Wählen Sie ein Trap-Ziel aus, und klicken Sie dann rechts oben auf der Seite auf **Löschen**.
4. Bestätigen Sie den Vorgang, und klicken Sie dann auf **Löschen**.

   Die Zieladresse wird nicht mehr auf der Seite „Meldungen“ angezeigt.

Ergebnisse

Das gelöschte Trap-Ziel empfängt keine SNMP-Traps mehr vom Event-Monitor des Speicherarrays.