



Managen von SNMP-Warnmeldungen

SANtricity 11.6

NetApp
February 12, 2024

Inhalt

- Managen von SNMP-Warnmeldungen 1
 - Konfigurieren Sie Communities und Ziele für SNMP-Benachrichtigungen 1
 - Community-Namen für SNMP-Traps bearbeiten 2
 - Fügen Sie Community-Namen für SNMP-Traps hinzu 3
 - Entfernen Sie den Community-Namen für SNMP-Traps 3
 - Konfigurieren Sie SNMP-MIB-Variablen 4
 - Fügen Sie Trap-Ziele für SNMP-Warnungen hinzu 5
 - Löschen von Trap-Zielen 6

Managen von SNMP-Warnmeldungen

Konfigurieren Sie Communities und Ziele für SNMP-Benachrichtigungen

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 und eine IP-Adresse für den Server.

Bevor Sie beginnen

- Ein Netzwerkservers 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).
- Es muss ein Community-Name erstellt werden, der nur aus druckbaren ASCII-Zeichen besteht. Der Community-Name, ein String, der wie ein Kennwort für die Netzwerkservers fungiert, wird in der Regel von einem Netzwerkadministrator erstellt. Es können bis zu 256 Communities erstellt werden.
- 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**.
- Klicken Sie Auf **Software**.
- Suchen Sie Ihre Verwaltungssoftware (z. B. SANtricity-System-Manager), und klicken Sie dann rechts auf **Los!**.
- Klicken Sie auf der neuesten Version auf **Anzeigen & Download**.
- Klicken Sie unten auf der Seite auf **Weiter**.
- Akzeptieren Sie die EULA.
- Scrollen Sie nach unten, bis Sie **MIB-Datei für SNMP-Traps** 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 **Einstellungen > Alarmer**.
2. Wählen Sie die Registerkarte **SNMP** aus.

Wenn noch keine Community konfiguriert ist, wird auf der Registerkarte SNMP „Configure Communities“ angezeigt.

3. Wählen Sie * Communities Konfigurieren*.

Das Dialogfeld **Configure Communities** wird geöffnet.

4. Geben Sie im Feld **Community Name** eine oder mehrere Community-Strings für die Netzwerkserver ein, und klicken Sie dann auf **Speichern**.

Auf der Seite Warnungen wird „Fallziele hinzufügen“ angezeigt.

5. Wählen Sie **Trap-Ziele Hinzufügen**.

Das Dialogfeld **Trap-Ziele hinzufügen** wird geöffnet.

6. Geben Sie ein oder mehrere Trap-Ziele ein, wählen Sie die zugehörigen Community-Namen 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** — Wählen Sie im Dropdown-Menü den Community-Namen für dieses Trap-Ziel aus. (Wenn Sie nur einen Community-Namen 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 abgelehnt wird. Nach dem Klicken auf **Hinzufügen** werden die Trap-Ziele und die zugehörigen Community-Namen auf der Seite **SNMP** auf der Registerkarte **Alarme** angezeigt.
7. 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.

Community-Namen für SNMP-Traps bearbeiten

Sie können Community-Namen für SNMP-Traps bearbeiten und einen anderen Community-Namen einem SNMP-Trap-Ziel zuordnen.

Bevor Sie beginnen

Es muss ein Community-Name erstellt werden, der nur aus druckbaren ASCII-Zeichen besteht. Der Community-Name, ein String, der wie ein Kennwort für die Netzwerkserver fungiert, wird von einem Netzwerkadministrator erstellt.

Schritte

1. Wählen Sie **Einstellungen > Alarme**.
2. Wählen Sie die Registerkarte **SNMP** aus.

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

3. Bearbeiten Sie Community-Namen wie folgt:
 - Um einen Community-Namen zu bearbeiten, wählen Sie **Communities konfigurieren**. Geben Sie den neuen Community-Namen ein und klicken Sie dann auf **Speichern**. Community-Namen können nur aus druckbaren ASCII-Zeichen bestehen.
 - Um einen Community-Namen einem neuen Trap-Ziel zuzuordnen, wählen Sie den Community-Namen aus der Tabelle aus, und klicken Sie dann rechts auf das Symbol **Bearbeiten** (Bleistift). Wählen Sie im

Dropdown-Menü Community Name einen neuen Community-Namen für ein SNMP-Trap-Ziel aus und klicken Sie dann auf das Symbol **Speichern** (Häkchen).



Wenn Sie die Änderungen abbrechen möchten, wählen Sie das Symbol **Abbrechen** (X).

Ergebnisse

Die Registerkarte **SNMP** der Seite **Alerts** zeigt die aktualisierten Communities an.

Fügen Sie Community-Namen für SNMP-Traps hinzu

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

Bevor Sie beginnen

Der/die Community-Name(n) muss erstellt werden. Der Community-Name, ein String, der wie ein Kennwort für die Netzwerkserver fungiert, wird in der Regel von einem Netzwerkadministrator erstellt. Es besteht nur aus druckbaren ASCII-Zeichen.

Schritte

1. Wählen Sie **Einstellungen** > **Alarmer**.
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 Seite **Alerts** auf der Registerkarte **SNMP** angezeigt.

Entfernen Sie den Community-Namen für SNMP-Traps

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

Schritte

1. Wählen Sie **Einstellungen** > **Alarmer**.
2. Wählen Sie die Registerkarte **SNMP** aus.

Die Trap-Ziele und die Community-Namen werden auf der Seite Meldungen angezeigt.

3. Wählen Sie * Communities Konfigurieren*.

Das Dialogfeld **Configure Communities** 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.

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**.
- Klicken Sie Auf **Software**.
- Suchen Sie Ihre Verwaltungssoftware (z. B. SANtricity-System-Manager), und klicken Sie dann rechts auf **Los!**.
- Klicken Sie auf **Ansicht & Download** auf der neuesten Version.
- Klicken Sie unten auf der Seite auf **Weiter**.
- Akzeptieren Sie die EULA.
- Scrollen Sie nach unten, bis Sie **MIB-Datei für SNMP-Traps** 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 **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.

Fügen Sie Trap-Ziele für SNMP-Warnungen hinzu

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

Bevor Sie beginnen

- Der Netzwerkservers, 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).
- Es muss ein Community-Name erstellt werden, der nur aus druckbaren ASCII-Zeichen besteht. Der Community-Name, ein String, der wie ein Kennwort für die Netzwerkservers fungiert, wird in der Regel von einem Netzwerkadministrator erstellt. Es können bis zu 256 Communities erstellt werden.
- 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**.
- Klicken Sie Auf **Software**.
- Suchen Sie Ihre Verwaltungssoftware (z. B. SANtricity-System-Manager), und klicken Sie dann rechts auf **Los!**.
- Klicken Sie auf **Ansicht & Download** auf der neuesten Version.
- Klicken Sie unten auf der Seite auf **Weiter**.
- Akzeptieren Sie die EULA.
- Scrollen Sie nach unten, bis Sie **MIB-Datei für SNMP-Traps** sehen, und klicken Sie dann auf den Link, um die Datei herunterzuladen.

Schritte

1. Wählen Sie **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 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** — Wählen Sie im Dropdown-Menü den Community-Namen für dieses Trap-Ziel aus. (Wenn Sie nur einen Community-Namen 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 abgelehnt wird. Nach dem Klicken auf **Hinzufügen** werden die Trap-Ziele und die zugehörigen Community-Namen 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.

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 **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 **Alerts** angezeigt.

Ergebnisse

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

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.