SNMP-Konfiguration

System Manager Classic

NetApp
April 09, 2024

This PDF was generated from https://docs.netapp.com/de-de/ontap-sm-classic/snmp-config/index.html on April 09, 2024. Always check docs.netapp.com for the latest.

Inhalt

SNMP-Konfiguration 1
Überblick über die SNMP-Konfiguration 1
SNMP-Konfigurationsworkflow 1

SNMP-Konfiguration

Überblick über die SNMP-Konfiguration

Mithilfe der Schnittstelle ONTAP System Manager *classic* mit ONTAP 9.7 oder einer älteren Version können Sie SNMP auf der Cluster-Verwaltungsebene konfigurieren, Communitys, Sicherheitsbenutzer und Traphosts hinzufügen und die SNMP-Kommunikation testen.

Sie sollten die folgenden Verfahren verwenden, wenn Sie SNMP-Zugriff auf ein Cluster wie folgt konfigurieren möchten:

- Sie arbeiten mit Clustern, auf denen ONTAP 9 ausgeführt wird.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.

> In den Verfahren werden einige Schritte ausgeführt, für die Sie die Befehlszeilenschnittstelle verwenden müssen.

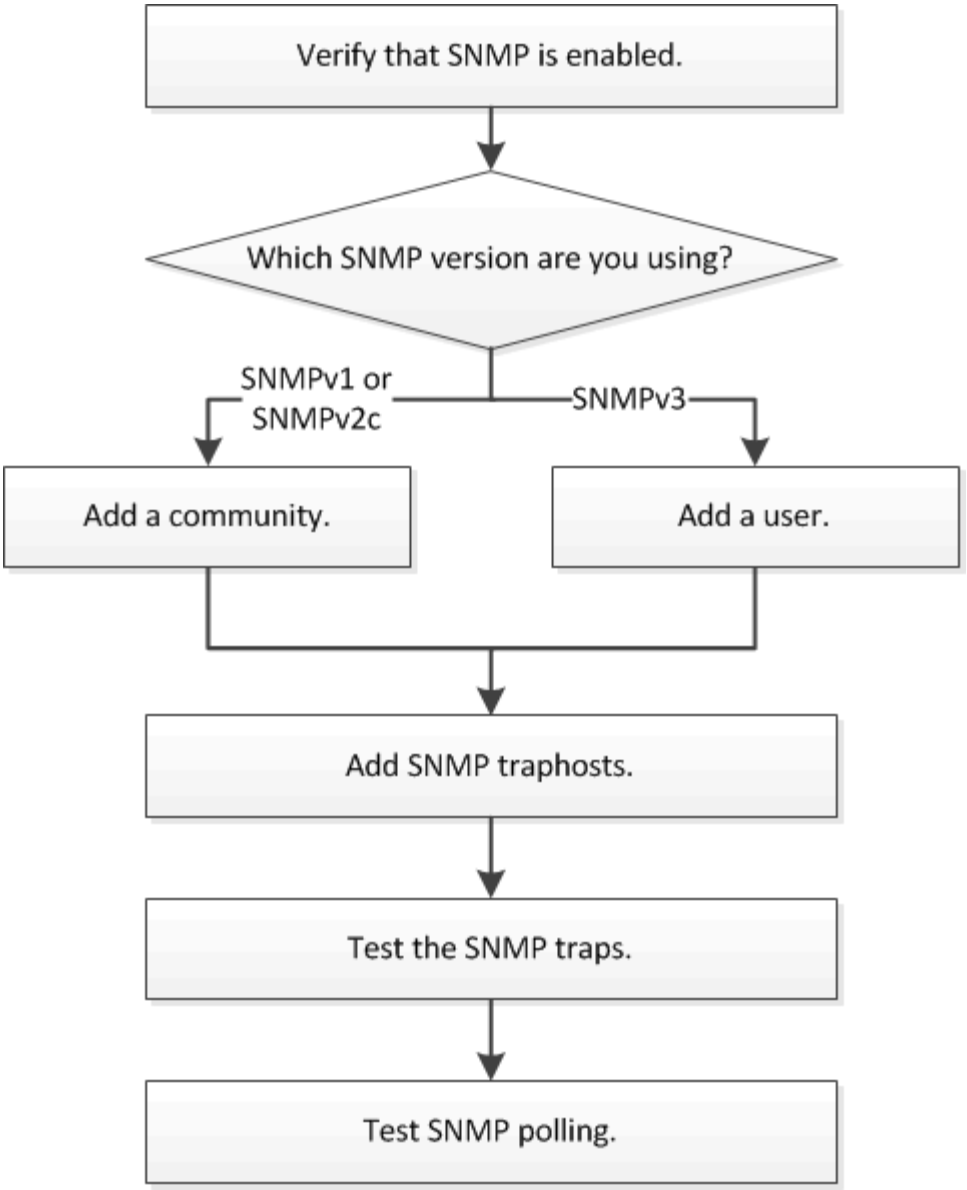
Weitere Möglichkeiten dies in ONTAP zu tun

Sie können SNMP-Zugriff auf ein Cluster konfigurieren, indem Sie für alle Versionen von ONTAP 9 verwenden. Sie sollten das entsprechende Verfahren für Ihre ONTAP-Version verwenden.

So führen Sie diese Aufgaben durch:	Siehe…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	**Verwalten Sie SNMP auf dem Cluster (nur Clusteradministratoren) › Übersicht**
Die ONTAP Befehlszeilenschnittstelle (CLI)	"Befehle zum Verwalten von SNMP"

SNMP-Konfigurationsworkflow

Beim Konfigurieren von SNMP wird SNMP aktiviert, optional eine SNMPv1- oder SNMPv2c-Community konfiguriert, optional ein SNMPv3-Benutzer hinzugefügt, SNMP-Traphosts hinzugefügt und SNMP-Polling und -Traps getestet.



Vergewissern Sie sich, dass SNMP aktiviert ist

Mithilfe der Schnittstelle ONTAP System Manager *classic* mit ONTAP 9.7 oder einer älteren Version können Sie überprüfen, ob SNMP auf dem Cluster aktiviert ist.

Über diese Aufgabe

In allen Versionen von ONTAP ist SNMPv3 standardmäßig auf Clusterebene aktiviert und SNMPv1 und SNMPv2c standardmäßig deaktiviert. SNMPv1 und SNMPv2c sind aktiviert, wenn Sie eine SNMP-Community erstellen.

SNMP ist standardmäßig auf Daten-LIFs deaktiviert. Informationen zur Aktivierung von SNMP auf Daten-LIFs finden Sie unter "Netzwerkmanagement".

Schritte

1. Klicken Sie auf das Nut-Symbol.
2. Navigieren Sie im Fensterbereich **Setup** zum Fenster **SNMP**.

Sie können den aktuellen SNMP-Status für das Cluster anzeigen.

Wenn SNMP nicht aktiviert ist, klicken Sie auf **Aktivieren**.

Fügen Sie eine SNMP Community hinzu

Sie können die klassische Schnittstelle des ONTAP System Manager *classic* mit ONTAP 9.7 oder einer älteren Version verwenden, um eine Community der administrativen Storage Virtual Machine (SVM) für einen Cluster hinzuzufügen, auf dem SNMPv1 oder SNMPv2c ausgeführt wird. System Manager verwendet SNMP-Protokolle SNMPv1 und SNMPv2c sowie eine SNMP-Community, um Storage-Systeme zu erkennen.

Über diese Aufgabe

Dieses Verfahren dient zum Hinzufügen einer SNMP-Community zu der administrativen SVM für den Cluster. Das Verfahren zum Hinzufügen einer SNMP-Community zu einer Daten-SVM wird in beschrieben "Netzwerkmanagement".

Bei Neuinstallationen von ONTAP sind SNMPv1 und SNMPv2c standardmäßig deaktiviert. SNMPv1 und SNMPv2c sind aktiviert, wenn Sie eine SNMP-Community erstellen.

Schritte

1. Klicken Sie im SNMP-Fenster auf **Bearbeiten**, um das Dialogfeld **SNMP-Einstellungen bearbeiten** zu öffnen.
2. Geben Sie auf der Registerkarte **Allgemein** den Ansprechpartner und den Standort für das ONTAP-System an.
3. Klicken Sie auf **Hinzufügen**, geben Sie einen Community-Namen ein und klicken Sie dann im Fenster **Community-Namen** auf **OK**.

   Sie können mehrere Community-Namen hinzufügen. Ein Community-Name darf maximal 32 Zeichen lang sein und darf die folgenden Sonderzeichen nicht enthalten: `, / : " ' |`

4. Wenn Sie das Hinzufügen von Community-Namen beenden, klicken Sie im Dialogfeld **SNMP-Einstellungen bearbeiten** auf **OK**.

Fügen Sie einen SNMPv3-Sicherheitsbenutzer hinzu

Sie können die Schnittstelle ONTAP System Manager *classic* mit ONTAP 9.7 oder früher verwenden, um einen SNMPv3-Benutzer auf Cluster-Ebene hinzuzufügen.

Der SNMPv3-Benutzer kann SNMP-Dienstprogramme über den traphost (SNMP Manager) mit den von Ihnen angegebenen Authentifizierungs- und Datenschutzeinstellungen ausführen. SNMPv3 bietet erweiterte Sicherheit durch Nutzung von Passphrases und Verschlüsselung.

Über diese Aufgabe

Wenn Sie einen SNMPv3-Benutzer auf Cluster-Ebene hinzufügen, kann dieser Benutzer über alle LIFs, auf die die Firewall-Richtlinie „`mgmt`“ angewendet wurde, auf das Cluster zugreifen.

Schritte

1. Klicken Sie im SNMP-Fenster auf **Bearbeiten**, um das Dialogfeld **SNMP-Einstellungen bearbeiten** zu

öffnen.

2. Klicken Sie auf der Registerkarte **SNMPv3** auf **Hinzufügen**, um das Dialogfeld **SNMPv3-Benutzer hinzufügen** zu öffnen.
3. Geben Sie die folgenden Werte ein:

   a. Geben Sie einen SNMPv3-Benutzernamen ein.

      Ein Security-Benutzername darf nicht mehr als 31 Zeichen enthalten und darf die folgenden Sonderzeichen nicht enthalten:

      `, / : " ' |`

   b. Wählen Sie für die Engine-ID den Standardwert aus `Local Engine ID`.

      Die Engine-ID wird verwendet, um Authentifizierungs- und Verschlüsselungsschlüssel für SNMPv3-Nachrichten zu generieren.

   c. Wählen Sie ein Authentifizierungsprotokoll aus, und geben Sie ein Authentifizierungskennwort ein.

      Ein Passwort muss mindestens acht Zeichen lang sein.

   d. Optional: Wählen Sie ein Datenschutzprotokoll aus und geben Sie ein Passwort dafür ein.

4. Klicken Sie im Dialogfeld **SNMPv3-Benutzer hinzufügen** auf **OK**.

   Sie können mehrere Sicherheits-Benutzernamen hinzufügen, indem Sie nach jedem Hinzufügen auf **OK** klicken. Wenn Sie zum Beispiel SNMP verwenden, um verschiedene Anwendungen zu überwachen, die unterschiedliche Berechtigungen erfordern, müssen Sie möglicherweise einen SNMPv3-Benutzer für jede Überwachungs- oder Verwaltungsfunktion hinzufügen.

5. Klicken Sie nach dem Hinzufügen von Benutzernamen im Dialogfeld **SNMP-Einstellungen bearbeiten** auf **OK**.

Fügen Sie einen SNMP traphost hinzu

Sie können die Schnittstelle ONTAP System Manager *classic* mit ONTAP 9.7 oder einer älteren Version verwenden, um einen traphost (SNMP Manager) zum Empfangen von SNMP-Benachrichtigungen (SNMP Trap Protocol Data Units) hinzuzufügen, wenn Traps im Cluster erzeugt werden.

Bevor Sie beginnen

IPv6 muss auf dem Cluster aktiviert sein, wenn Sie SNMP-Traphosts mit IPv6-Adressen konfigurieren.

Über diese Aufgabe

SNMP- und SNMP-Traps sind standardmäßig aktiviert. Der technische Bericht TR-4220 zur SNMP-Unterstützung enthält Listen aller Standardereignisse, die durch SNMP-Traps unterstützt werden.

"Technischer Bericht von NetApp 4220: SNMP-Support in Data ONTAP"

Schritte

1. Klicken Sie im SNMP-Fenster auf **BEARBEITEN**, um das Dialogfeld **SNMP-Einstellungen bearbeiten** zu öffnen.

2. [[step 2-verify-enable-Traps]]Überprüfen Sie auf der Registerkarte **Trap Hosts**, ob das Kontrollkästchen **enable Traps** aktiviert ist, und klicken Sie auf **Add**.
3. [[STEP 3-Enter-traphost-ip]] Geben Sie die traphost-IP-Adresse ein, und klicken Sie dann im Bereich **Trap Hosts** auf **OK**.

   Die IP-Adresse eines SNMP traphosts kann IPv4 oder IPv6 sein.

4. Um einen anderen traphost hinzuzufügen, wiederholen Sie den Vorgang Schritt 2 Und Schritt 3.
5. Wenn Sie das Hinzufügen von Traphosts abgeschlossen haben, klicken Sie im Dialogfeld **SNMP-Einstellungen bearbeiten** auf **OK**.

Testen Sie SNMP-Traps

Sie können die ONTAP System Manager *classic* -Schnittstelle mit ONTAP 9.7 oder früher zum Testen von SNMP-Traps verwenden. Da die Kommunikation mit einem traphost nicht automatisch validiert wird, wenn Sie es hinzufügen, sollten Sie überprüfen, ob SNMP traphost Traps korrekt empfangen kann.

Schritte

1. Navigieren Sie zum Bildschirm **SNMP**.
2. Klicken Sie auf **Trap Host testen**, um einen Trap aus dem Cluster zu erstellen, in dem Sie einen traphost hinzugefügt haben.
3. Überprüfen Sie am traphost-Standort, ob die Trap empfangen wurde.

   Verwenden Sie die Software, die Sie normalerweise verwenden, um den SNMP traphost zu verwalten.

Testen Sie die SNMP-Abfrage

Nachdem Sie SNMP konfiguriert haben, sollten Sie überprüfen, dass Sie den Cluster anfragen können.

Über diese Aufgabe

Um einen Cluster abzufragen, müssen Sie einen Drittanbieter-Befehl wie verwenden `snmpwalk`.

Schritte

1. Senden Sie einen SNMP-Befehl, um den Cluster von einem anderen Cluster abzufragen.

   Verwenden Sie für Systeme, auf denen SNMPv1 ausgeführt wird, den CLI-Befehl `snmpwalk -v version -c community_stringip_address_or_host_name system` Um den Inhalt der MIB (Management Information Base) zu entdecken.

   In diesem Beispiel ist die IP-Adresse der Cluster-Management-LIF, die Sie abfragen, 10.11.12.123. Der Befehl zeigt die angeforderten Informationen aus der MIB an:

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

Verwenden Sie für Systeme, die SNMPv2c ausführen, den CLI-Befehl `snmpwalk -v version -c community_stringip_address_or_host_name system` Um den Inhalt der MIB (Management Information Base) zu entdecken.

In diesem Beispiel ist die IP-Adresse der Cluster-Management-LIF, die Sie abfragen, 10.11.12.123. Der Befehl zeigt die angeforderten Informationen aus der MIB an:

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

Verwenden Sie für Systeme, die SNMPv3 ausführen, den CLI-Befehl `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` Um den Inhalt der MIB (Management Information Base) zu entdecken.

In diesem Beispiel ist die IP-Adresse der Cluster-Management-LIF, die Sie abfragen, 10.11.12.123. Der Befehl zeigt die angeforderten Informationen aus der MIB an:

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

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 IRGENDEINER 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.