



SNMP設定

System Manager Classic

NetApp
June 22, 2024

目次

| | |
|---------------------|---|
| SNMP設定 | 1 |
| SNMP 設定の概要 | 1 |
| SNMPの設定ワークフロー | 1 |

SNMP設定

SNMP 設定の概要

ONTAP 9.7 以前の場合に ONTAP System Manager の *classic* インターフェイスを使用すると、クラスタ管理レベルで SNMP を設定し、コミュニティ、セキュリティユーザ、トラップホストを追加し、SNMP 通信をテストできます。

クラスタへの SNMP アクセスを設定する場合は、次の手順を実行します。

- クラスタで ONTAP 9 を実行している。
- すべての選択肢について検討するのではなく、ベストプラクティスに従う。



これらの手順には、コマンドラインインターフェイスを使用する必要がある手順がいくつかあります。

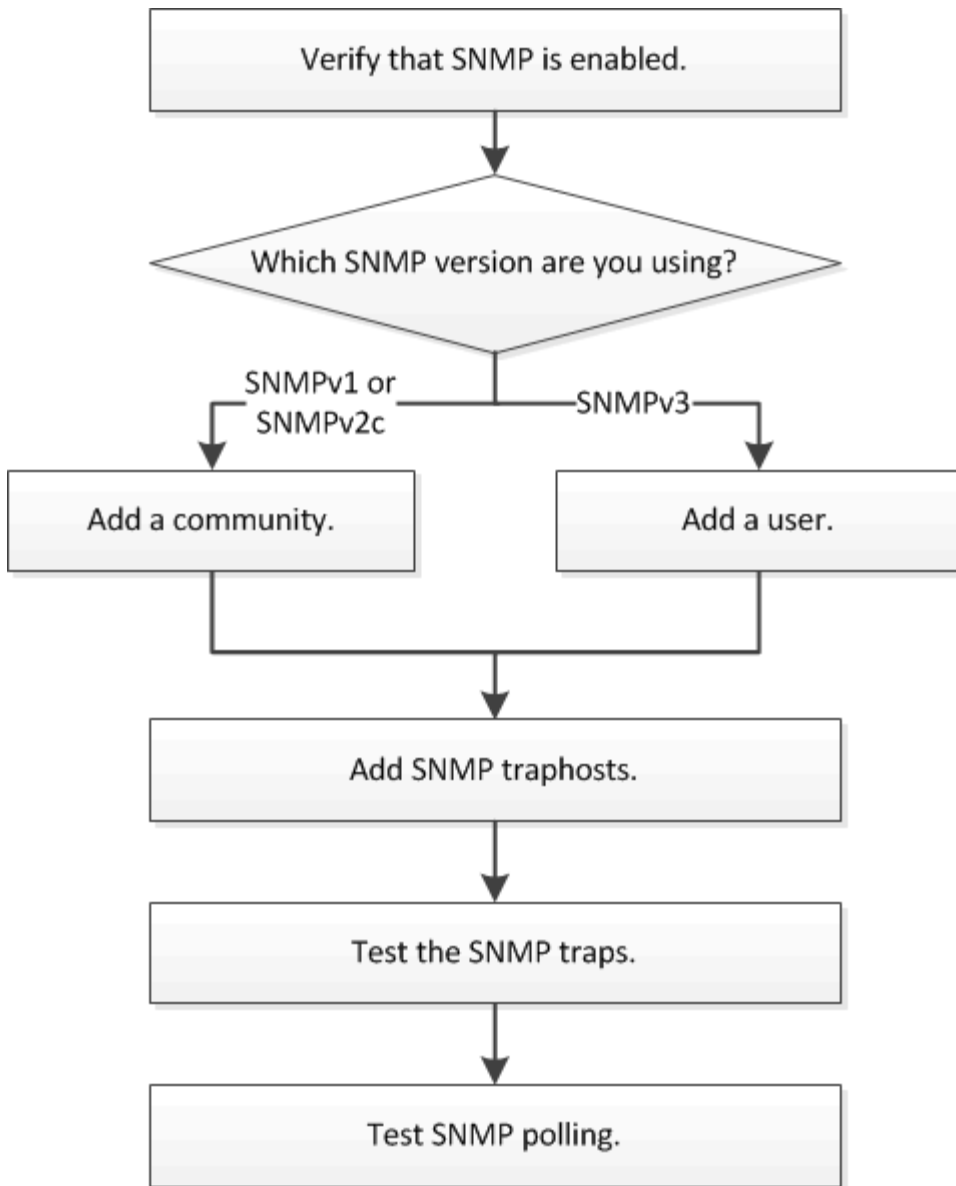
ONTAP でこれを行うその他の方法

ONTAP 9 のすべてのバージョンで、を使用したクラスタへの SNMP アクセスを設定できます。使用している ONTAP のバージョンに適した手順を使用してください。

| 実行するタスク | 参照先 |
|---|--|
| 再設計された System Manager (ONTAP 9.7 以降で使用可能) | "クラスタ上のSNMPの管理(クラスタ管理者のみ)>概要" |
| ONTAP コマンドラインインターフェイス (CLI) | "SNMP を管理するためのコマンド" |

SNMPの設定ワークフロー

SNMP の設定には、SNMP の有効化、SNMPv1 または SNMPv2c コミュニティの設定 (オプション)、SNMPv3 ユーザの追加、SNMP トラップホストの追加、SNMP ポーリングとトラップのテストが含まれます。



SNMP が有効になっていることを確認します

ONTAP 9.7 以前では、ONTAP System Manager の *classic* インターフェイスを使用して、クラスタで SNMP が有効になっているかどうかを確認できます。

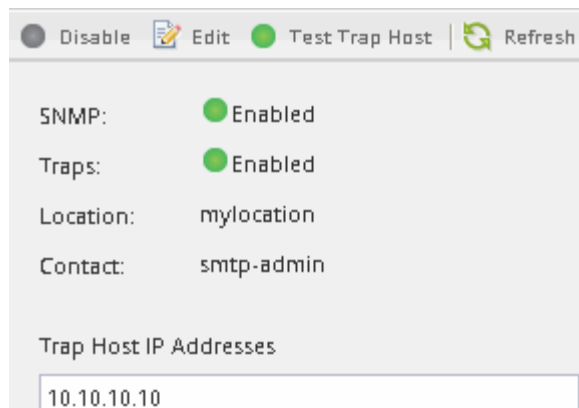
このタスクについて

ONTAP のすべてのバージョンで、SNMPv3 はクラスタレベルでデフォルトで有効になっており、SNMPv1 と SNMPv2c はデフォルトで無効になっています。SNMPv1 と SNMPv2c は、SNMP コミュニティを作成すると有効になります。

データ LIF では、SNMP はデフォルトで無効になっています。データ LIF で SNMP を有効にする方法については、を参照してください "[Network Management の略](#)"。

手順

1. 溝アイコンをクリックします。
2. [Setup] ペインで、[SNMP] ウィンドウに移動します。



クラスタの現在の SNMP ステータスを確認できます。

SNMP が有効になっていない場合は、**Enable** をクリックします。

SNMP コミュニティを追加します

ONTAP 9.7 以前で ONTAP System Manager の *classic* インターフェイスを使用して、SNMPv1 または SNMPv2c を実行しているクラスタの管理 Storage Virtual Machine (SVM) にコミュニティを追加できます。System Manager は、SNMP プロトコル SNMPv1 と SNMPv2c、および SNMP コミュニティを使用して、ストレージシステムを検出します。

このタスクについて

この手順は、クラスタの管理 SVM に SNMP コミュニティを追加するためのものです。データ SVM に SNMP コミュニティを追加するための手順については、を参照してください "[Network Management の略](#)"。

ONTAP の新規インストールでは、SNMPv1 と SNMPv2c はデフォルトで無効になっています。SNMPv1 と SNMPv2c は、SNMP コミュニティを作成すると有効になります。

手順

1. SNMP ウィンドウで、*** Edit *** をクリックして、*** Edit SNMP Settings *** ダイアログボックスを開きます。
2. **[*General]** タブで、ONTAP システムの担当者と場所を指定します。
3. **[* 追加]** をクリックし、コミュニティ名を入力して、**[* コミュニティ名 *]** ウィンドウ枠の *** [OK]** をクリックします。

コミュニティ名は複数追加できます。コミュニティ名の最大文字数は32文字です。次の特殊文字は使用できません。 , / : " ' |

4. コミュニティ名の追加が完了したら、*** Edit SNMP Settings *** (SNMP 設定の編集) ダイアログボックスで *** OK *** をクリックします。

SNMPv3 セキュリティユーザを追加します

ONTAP 9.7 以前では、ONTAP System Manager の *classic* インターフェイスを使用し

て、クラスタレベルで SNMPv3 ユーザを追加できます。

SNMPv3 ユーザは、管理者が指定した認証およびプライバシー設定を使用して、トラップホスト（SNMP マネージャ）から SNMP ユーティリティを実行できます。SNMPv3 は、パスフレーズと暗号化を使用して高度なセキュリティを提供します。

このタスクについて

クラスタレベルで SNMPv3 ユーザを追加すると、このユーザは「mgmt」ファイアウォールポリシーが適用されているすべての LIF を介してクラスタにアクセスできるようになります。

手順

1. SNMP ウィンドウで、* Edit * をクリックして、* Edit SNMP Settings * ダイアログボックスを開きます。
2. **SNMPv3** タブで、* Add * をクリックして、* Add SNMPv3 User * ダイアログボックスを開きます。
3. 次の値を入力します。

- a. SNMPv3 ユーザの名前を入力します。

セキュリティユーザ名は最大 31 文字で、次の特殊文字は使用できません。

, / : " ' |

- b. [エンジンID]で、デフォルト値を選択します。Local Engine ID。

エンジン ID は、SNMPv3 メッセージの認証キーおよび暗号キーの生成に使用されます。

- c. 認証プロトコルを選択し、認証パスワードを入力します。

パスワードは 8 文字以上にする必要があります。

- d. オプション：プライバシープロトコルを選択し、パスワードを入力します。

4. [Add SNMPv3 User*] ダイアログボックスで、**OK** をクリックします。

追加するたびに「* OK」をクリックすると、複数のセキュリティユーザー名を追加できます。たとえば、異なる権限を必要とする複数のアプリケーションを SNMP を使用して監視する場合は、監視や管理の機能ごとに SNMPv3 ユーザを追加する必要があります。

5. ユーザー名の追加が完了したら、* SNMP 設定の編集 * ダイアログボックスの * OK * をクリックします。

SNMP トラップホストを追加します。

ONTAP 9.7以前では、ONTAP System Manager_classic_interfaceを使用して、クラスタでトラップが生成されたときにSNMP通知（SNMPトラッププロトコルデータユニット）を受信するトラップホスト（SNMPマネージャ）を追加できます。

作業を開始する前に

IPv6 アドレスを使用して SNMP トラップホストを設定するには、クラスタで IPv6 を有効にする必要があります。

このタスクについて

SNMP トラップと SNMP トラップはデフォルトで有効になっています。SNMP トラップでサポートされるデフォルトのイベントについては、SNMP サポートに関するネットアップテクニカルレポート TR-4220 を参照してください。

"[ネットアップテクニカルレポート 4220 : 『SNMP Support in Data ONTAP』](#)"

手順

1. SNMP ウィンドウで **edit** をクリックして、* Edit SNMP Settings * ダイアログボックスを開きます。
2. [[stp2-verify-enable-traps] [* Trap Hosts] タブで、[* トラップを有効にする] チェックボックスがオンになっていることを確認し、[追加] をクリックします。
3. [[step3-enter-traphost - ip]] トラップホストの IP アドレスを入力し、* Trap Hosts * ペインで * OK * をクリックします。

SNMP トラップホストの IP アドレスには、IPv4 または IPv6 を使用できます。

4. 別のトラップホストを追加するには、を繰り返します [ステップ2](#) および [手順3](#)。
5. トラップホストの追加が完了したら、* Edit SNMP Settings * (SNMP 設定の編集) ダイアログボックスで * OK * をクリックします。

テスト用の SNMP トラップ

ONTAP 9.7 以前では、ONTAP System Manager の *classic* インターフェイスを使用して SNMP トラップをテストできます。追加したトラップホストとの通信は自動では検証されないため、SNMP トラップホストがトラップを正しく受信できることを確認する必要があります。

手順

1. [SNMP] 画面に移動します。
2. トラップホストのテスト * をクリックして、トラップホストを追加したクラスタからトラップを生成します。
3. トラップホストの場所で、トラップを受信したことを確認します。

SNMP トラップホストの管理に通常使用するソフトウェアを使用してください。

SNMP ポーリングのテスト

SNMP を設定したら、クラスタをポーリングできることを確認する必要があります。

このタスクについて

クラスタをポーリングするには、次のようなサードパーティのコマンドを使用する必要があります。
snmpwalk。

手順

1. SNMP コマンドを送信して、別のクラスタからクラスタをポーリングします。

SNMPv1を実行しているシステムの場合は、CLIコマンドを使用します。snmpwalk -v version -c community_string ip_address_or_host_name system MIB（管理情報ベース）の内容を検出します。

この例では、ポーリングするクラスタ管理 LIF の IP アドレスは 10.11.12.123 です。要求された MIB 情報が表示されます。

```
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
```

SNMPv2cを実行しているシステムの場合は、CLIコマンドを使用します。snmpwalk -v version -c community_string ip_address_or_host_name system MIB（管理情報ベース）の内容を検出します。

この例では、ポーリングするクラスタ管理 LIF の IP アドレスは 10.11.12.123 です。要求された MIB 情報が表示されます。

```
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
```

SNMPv3を実行しているシステムの場合は、CLIコマンドを使用します。snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A password ip_address_or_host_name system MIB（管理情報ベース）の内容を検出します。

この例では、ポーリングするクラスタ管理 LIF の IP アドレスは 10.11.12.123 です。要求された MIB 情報が表示されます。


```
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
```

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。