SNMPの管理（クラスタ管理者のみ）

ONTAP 9

NetApp
April 24, 2024

目次

SNMPの管理（クラスタ管理者のみ）

SNMPの概要

クラスタの SVM を監視するように SNMP を設定すると、問題を発生前に回避したり、発生時に対応したりすることができます。SNMP の管理には、 SNMP ユーザを設定し、すべての SNMP イベントの SNMP トラップの送信先（管理ワークステーション）を設定する必要があります。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 SVM に、読み取り専用 SNMP ユーザを作成して管理できます。データ LIF は、 SVM で SNMP 要求を受信するように設定する必要があります。

SNMP ネットワーク管理ワークステーションまたはマネージャは、 SVM SNMP エージェントに情報を照会できます。SNMP エージェントは情報を収集し、 SNMP マネージャに転送します。SNMP エージェントは、特定のイベントが発生するたびにトラップ通知も生成します。SVM 上の SNMP エージェントの権限は読み取り専用権限であるため、設定操作や、トラップに応答して対処するために使用することはできません。ONTAP は SNMP バージョン v1 、 v2c 、および v3 と互換性のある SNMP エージェントを備えています。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。

ONTAP システムでの SNMP サポートの詳細については、を参照してください "TR-4220 ：『 SNMP Support in Data ONTAP 』"。

MIBの概要

MIB （管理情報ベース）は、 SNMP のオブジェクトとトラップが記述されたテキストファイルです。

MIB は、ストレージシステムの管理データの構造を表し、 Object Identifier （ OID ；オブジェクト識別子）を含む階層状のネームスペースを使用します。各 OID は、 SNMP を使用して読み取り可能な変数を識別します。

MIB は構成ファイルではなく、 ONTAP はこれらのファイルを読み取らないため、 SNMP 機能は MIB による影響を受けません。ONTAP には次の MIB ファイルがあります。

- ネットアップのカスタムMIB (`netapp.mib`)

ONTAP は、 IPv6 （ RFC 2465 ）、 TCP （ RFC 4022 ）、 UDP （ RFC 4113 ）、および ICMP （ RFC 2466 ）の MIB をサポートします。これらの MIB では IPv4 と IPv6 の両方のデータが表示されます。

ONTAP では、のオブジェクト識別子（OID）とオブジェクトの簡略名の簡単な相互参照も提供されています `traps.dat` ファイル。

> ONTAP の MIB および「 traps.dat 」ファイルの最新バージョンは、NetApp Support Siteから入手できます。ただし、サポートサイトにあるファイルのバージョンが、お使いの ONTAP バージョンの SNMP 機能に必ずしも対応しているとは限りません。これらのファイルは、最新バージョンの ONTAP の SNMP 機能の評価用に提供されています。

SNMP トラップ

SNMP トラップは、 SNMP エージェントから SNMP マネージャに非同期通知として送信されたシステム監視

情報をキャプチャします。

SNMP トラップには、標準、ビルトイン、およびユーザ定義の 3 種類があります。ユーザ定義トラップは、ONTAP ではサポートされていません。

トラップを使用して、 MIB に定義された運用上のしきい値または障害を定期的にチェックすることができます。しきい値に到達するか、障害が検出されると、 SNMP エージェントは、イベントを警告するメッセージ（トラップ）をトラップホストに送信します。

> ONTAP は、 SNMPv1 トラップ、および ONTAP 9.1 以降の SNMPv3 トラップをサポートしています。ONTAP は、 SNMPv2c トラップおよび INFORM をサポートしていません。

標準 SNMP トラップ

これらのトラップは RFC 1215 で定義されています。ONTAP でサポートされている SNMP トラップは、coldStart 、 warmStart 、 linkDown 、 linkUp 、および authenticationFailure の 5 つです。

> authenticationFailure トラップは、デフォルトで無効になっています。を使用する必要があります `system snmp authtrap` トラップをイネーブルにするコマンド。詳細については、次のマニュアルページを参照してください。 "ONTAP 9 のコマンド"

組み込みの SNMP トラップ

ビルトイントラップは ONTAP に事前定義されたトラップで、イベントの発生時にトラップホストリストのネットワーク管理ステーションに自動的に送信されます。diskFailedShutdown 、 cpuTooBusy 、volumeNearlyFull など、これらのトラップはカスタム MIB で定義されています。

各ビルトイントラップは、一意のトラップコードで識別されます。

SNMP コミュニティを作成して LIF に割り当てます

SNMPv1 および SNMPv2c を使用する場合に管理ステーションと Storage Virtual Machine （ SVM ）間の認証メカニズムとして機能する、 SNMP コミュニティを作成できます。

データSVMにSNMPコミュニティを作成することで、などのコマンドを実行できます `snmpwalk` および `snmpget` （データLIF）。

このタスクについて

- 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。

- ONTAP でサポートされるのは、読み取り専用のコミュニティです。
- デフォルトでは、データLIFに割り当てられている「data」ファイアウォールポリシーでは、SNMPサービスがに設定されています `deny`。

  新しいファイアウォールポリシーを作成し、SNMPサービスをに設定する必要があります `allow` データSVMのSNMPユーザを作成する場合。

ONTAP 9.10.1以降では、ファイアウォールポリシーは廃止され、完全にLIFのサービスポリシーに置き換えられました。詳細については、を参照してください "LIF のファイアウォールポリシーを設定します"。

- 管理 SVM とデータ SVM の両方に、 SNMPv1 ユーザと SNMPv2c ユーザの SNMP コミュニティを作成できます。
- SVMはSNMP標準の一部ではないため、データLIFでのクエリにはネットアップのルートOID（1.3.6.1.4.1.789）を含める必要があります。次に例を示します。 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

手順

1. を使用してSNMPコミュニティを作成します `system snmp community add` コマンドを実行します次のコマンドは、管理 SVM cluster-1 に SNMP コミュニティを作成する方法を示しています。

   ```
   system snmp community add -type ro -community-name comty1 -vserver
   cluster-1
   ```

   次のコマンドは、データ SVM vs1 に SNMP コミュニティを作成する方法を示しています。

   ```
   system snmp community add -type ro -community-name comty2 -vserver vs1
   ```

2. system snmp community show コマンドを使用して、コミュニティが作成されたことを確認します。

   次のコマンドは、 SNMPv1 および SNMPv2c 用に作成された 2 つのコミュニティを表示します。

   ```
   system snmp community show
   cluster-1
   rocomty1
   vs1
   rocomty2
   ```

3. を使用して、「data」ファイアウォールポリシーでSNMPがサービスとして許可されているかどうかを確認します `system services firewall policy show` コマンドを実行します

   次のコマンドは、デフォルトの「 data 」ファイアウォールポリシーでは SNMP サービスが許可されていないことを示しています（ SNMP サービスは「 mgmt 」ファイアウォールポリシーでのみ許可されています）。

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. を使用したアクセスを許可する新しいファイアウォールポリシーを作成します `snmp` を使用してサービスを提供します `system services firewall policy create` コマンドを実行します

   次のコマンドは、「data1」という名前の新しいデータファイアウォールポリシーを作成して、を許可します `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. firewall-policy パラメータを指定して「 network interface modify 」コマンドを使用し、ファイアウォール

ポリシーをデータ LIF に適用します。

次のコマンドは、新しい「 data1 」ファイアウォールポリシーを LIF 「 datalif1 」に割り当てます。

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

クラスタに **SNMPv3** ユーザを設定します

SNMPv3 は、 SNMPv1 や SNMPv2c に比べて安全なプロトコルです。SNMPv3 を使用するには、 SNMP マネージャから SNMP ユーティリティを実行するための SNMPv3 ユーザを設定する必要があります。

ステップ

「 security login create コマンド」を使用して SNMPv3 ユーザを作成します。

次の情報を入力するように求められます。

- エンジン ID ：デフォルトで、推奨値はローカルエンジン ID です
- 認証プロトコル
- 認証パスワード
- プライバシープロトコル
- プライバシープロトコルのパスワード

結果

SNMPv3 ユーザは、ユーザ名とパスワードを使用して SNMP マネージャからログインし、 SNMP ユーティリティのコマンドを実行できます。

SNMPv3 セキュリティパラメータ

SNMPv3 には認証機能が備わっており、この機能を選択すると、コマンドの呼び出し時に、ユーザ名、認証プロトコル、認証キー、および必要なセキュリティレベルの入力が必要になります。

次の表に、 SNMPv3 セキュリティパラメータを示します。

パラメータ	コマンドラインオプション	説明
エンジン ID	-e engineID	SNMP エージェントのエンジン ID 。デフォルト値はローカルのエンジン ID （推奨）です。
securityName の略	-u 名	ユーザ名は 32 文字以内にする必要があります。
authProtocol の略	• a ｛ none	md5

sha	SHA-256 }	認証タイプには、 none 、 md5 、 SHA 、または SHA-256 を指定できます。
authKey	• パスフレーズ	8 文字以上の長さのパスフレーズ
セキュリティレベル	-l { authNoPriv	AuthPriv
noAuthNoPriv }	セキュリティレベルには、「 Authentication 、 No Privacy 」、「 Authentication 、 Privacy 」、「 No Authentication 、 No Authentication 」のいずれかを指定できます。 プライバシーなし。	privProtocol の略
-x { none	des	aes128 }
プライバシープロトコルには、 none 、 des 、または aes128 を指定できます	プライベートパスワード	-X パスワード

さまざまなセキュリティレベルの例

次に、さまざまなセキュリティレベルで作成されたSNMPv3ユーザが、などのSNMPクライアント側コマンドを使用する例を示します `snmpwalk`をクリックして、クラスタオブジェクトを照会します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

> を使用する必要があります `snmpwalk` 認証プロトコルがSHAの場合は5.3.1以降。

セキュリティレベル： **authPriv**

authPriv セキュリティレベルの SNMPv3 ユーザを作成した場合の出力を次に示します。

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

FIPS モード

```
security login create -username snmpv3user -application snmp -authmethod
usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

snmpwalk テストを実行します

この SNMPv3 ユーザが snmpwalk コマンドを実行した場合の出力を次に示します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

セキュリティレベル： **authNoPriv**

authNoPriv セキュリティレベルの SNMPv3 ユーザを作成した場合の出力を次に示します。

```
security login create -username snmpv3user1 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

FIPS モード

FIPSでは、プライバシープロトコルに* none *を選択することはできません。そのため、authNoPriv SNMPv3ユーザをFIPSモードで設定することはできません。

snmpwalk テストを実行します

この SNMPv3 ユーザが snmpwalk コマンドを実行した場合の出力を次に示します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

セキュリティレベル： **noAuthNoPriv**

noAuthNoPriv セキュリティレベルの SNMPv3 ユーザを作成した場合の出力を次に示します。

```
security login create -username snmpv3user2 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

FIPS モード

FIPSでは、プライバシープロトコルに* none *を選択することはできません。

snmpwalk テストを実行します

この SNMPv3 ユーザが snmpwalk コマンドを実行した場合の出力を次に示します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

SNMP 通知を受信するトラップホストを設定します

クラスタで SNMP トラップが生成されたときに通知（ SNMP トラップ PDU ）を受信するトラップホスト（ SNMP マネージャ）を設定できます。SNMP トラップホストのホスト名または IP アドレス（ IPv4 または IPv6 ）を指定できます。

作業を開始する前に

- クラスタで SNMP トラップと SNMP トラップが有効になっている必要があります。

> 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。

- クラスタでトラップホスト名を解決するように DNS が設定されている必要があります。
- 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。
- ONTAP 9.1 以降のバージョンでは、トラップホストの作成時に、事前定義されているユーザベースのセキュリティモデル（ USM ）の認証とプライバシーのクレデンシャルを指定しておく必要があります。

ステップ

SNMP トラップホストを追加します。

```
system snmp traphost add
```

> トラップを送信できるのは、少なくとも 1 つの SNMP 管理ステーションがトラップホストとして指定されているときのみです。

次のコマンドは、 yyy.example.com という新しい SNMPv3 トラップホストを既知の USM ユーザとともに追加します。

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

次のコマンドは、トラップホストの IPv6 アドレスを指定して、そのホストを追加します。

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

SNMP を管理するためのコマンド

を使用できます `system snmp` SNMP、トラップ、およびトラップホストを管理するコマンド。を使用できます `security` SVMごとにSNMPユーザを管理するコマンド。を使用できます `event` SNMPトラップに関連するイベントを管理するコマンド。

SNMP を設定するためのコマンド

状況	使用するコマンド
クラスタで SNMP を有効にします	`options -option-name snmp.enable -option-value on` 管理（ mgmt ）ファイアウォールポリシーで SNMP サービスが許可されている必要があります。SNMP が許可されているかどうかを確認するには、 system services firewall policy show コマンドを使用します。
クラスタで SNMP を無効にします	`options -option-name snmp.enable -option-value off`

SNMP v1 、 v2c 、および v3 ユーザを管理するコマンド

状況	使用するコマンド
SNMP ユーザを設定する	`security login create`
SNMP ユーザを表示します	`security snmpusers and security login show -application snmp`
SNMP ユーザを削除する	`security login delete`
SNMP ユーザのログイン方法のアクセス制御ロール名を変更します	`security login modify`

連絡先と場所の情報を提供するコマンド

状況	使用するコマンド
クラスタの連絡先の詳細を表示または変更する	`system snmp contact`
クラスタの場所の詳細を表示または変更する	`system snmp location`

SNMP コミュニティを管理するコマンド

状況	使用するコマンド
1 つの SVM 、またはクラスタのすべての SVM に読み取り専用（ ro ）コミュニティを追加する	`system snmp community add`
1 つまたはすべてのコミュニティを削除します	`system snmp community delete`
すべてのコミュニティのリストを表示します	`system snmp community show`

SVMはSNMP標準の一部ではないため、データLIFでのクエリにはネットアップのルートOID（1.3.6.1.4.1.789）を含める必要があります。次に例を示します。 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

SNMP オプションの値を表示するコマンド

状況	使用するコマンド
クラスタの連絡先、連絡先、トラップホストを送信するようにクラスタが設定されているかどうか、トラップホストのリスト、コミュニティとアクセス制御の種類のリストなど、すべての SNMP オプションの現在の値を表示します	`system snmp show`

SNMP のトラップおよびトラップホストを管理するコマンド

状況	使用するコマンド
クラスタからの SNMP トラップの送信を有効にします	`system snmp init -init 1`
クラスタからの SNMP トラップの送信を無効にします	`system snmp init -init 0`
クラスタの特定のイベントに関する SNMP 通知を受信するトラップホストを追加します	`system snmp traphost add`

トラップホストを削除します	`system snmp traphost delete`
トラップホストのリストを表示します	`system snmp traphost show`

SNMP トラップに関連するイベントを管理するコマンド

状況	使用するコマンド
SNMP トラップ（ビルトイン）が生成されたイベントを表示します	`event route show` を使用します `-snmp-support true` SNMP関連のイベントのみを表示するためのパラメータ。 を使用します `instance -messagename <message>` パラメータを使用して、イベントが発生した理由と対処方法の詳細な概要 を表示します。 個々の SNMP トラップイベントを特定の送信先トラップホストにルーティングすることはできません。すべての SNMP トラップイベントが、すべての送信先トラップホストに送信されます。
SNMP トラップ履歴レコードのリストを表示します。 SNMP トラップに送信されたイベント通知です	`event snmphistory show`
SNMP トラップ履歴レコードを削除します	`event snmphistory delete`

詳細については、を参照してください `system snmp`、 `security`および `event` コマンドについては、マニュアルページを参照してください。 "ONTAP 9 のコマンド"