



SNMP の設定

この章は、次の項で構成されています。

- [SNMPについて, on page 1](#)
- [SNMPの注意事項および制約事項, on page 6](#)
- [SNMPのデフォルト設定, on page 7](#)
- [SNMPの設定 \(8 ページ\)](#)
- [SNMP ローカルエンジン ID の設定, on page 23](#)
- [SNMPの無効化 \(24 ページ\)](#)
- [SNMP 設定の確認, on page 25](#)

SNMPについて

簡易ネットワーク管理プロトコル (SNMP) は、SNMP マネージャとエージェント間の通信用メッセージフォーマットを提供する、アプリケーションレイヤプロトコルです。SNMPでは、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共に言語が提供されます。

SNMP機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- **SNMP マネージャ** : SNMP を使用してネットワークデバイスのアクティビティを制御し、モニタリングするシステム
- **SNMP エージェント** : デバイスのデータを維持し、必要に応じてこれらのデータを管理システムに報告する、管理対象デバイス内のソフトウェアコンポーネント。Cisco Nexus デバイスはエージェントおよび MIB をサポートします。SNMP エージェントをイネーブルにするには、マネージャとエージェントの関係を定義する必要があります。
- **MIB (Management Information Base; 管理情報ベース)** : SNMP エージェントの管理対象オブジェクトの集まり

**Note**

Cisco Nexus デバイスは、イーサネット MIB の SNMP セットをサポートしません。

Cisco Nexus デバイスは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。

SNMPはRFC 3410 で定義されています (<http://tools.ietf.org/html/rfc3410>) 、RFC 3411（<http://tools.ietf.org/html/rfc3411>）、RFC 3412（<http://tools.ietf.org/html/rfc3412>）、RFC 3413（<http://tools.ietf.org/html/rfc3413>）、RFC 3414（<http://tools.ietf.org/html/rfc3414>）、RFC 3415（<http://tools.ietf.org/html/rfc3415>）、RFC 3416（<http://tools.ietf.org/html/rfc3416>）、RFC 3417（<http://tools.ietf.org/html/rfc3417>）、RFC 3418（<http://tools.ietf.org/html/rfc3418>）、および RFC 3584（<http://tools.ietf.org/html/rfc3584>）。

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求を SNMP マネージャから送信する必要はありません。通知は、不正なユーザ認証、再起動、接続の切断、隣接ルータとの接続の切断、その他の重要なイベントを表示します。

Cisco NX-OS は、トラップまたはインフォームとして SNMP 通知を生成します。トラップは、エージェントからホスト レシバーテーブルで指定された SNMP マネージャに送信される、非同期の非確認応答メッセージです。インフォームは、SNMP エージェントから SNMP マネージャに送信される非同期メッセージで、マネージャは受信したという確認応答が必要です。

トラップの信頼性はインフォームより低くなります。SNMP マネージャはトラップを受信しても確認応答 (ACK) を送信しないからです。このため、トラップが受信されたかどうかをスイッチが判断できません。インフォーム要求を受信する SNMP マネージャは、SNMP 応答プロトコルデータユニット (PDU) でメッセージの受信を確認応答します。Cisco NX-OS デバイスが応答を受信しない場合、インフォーム要求を再び送信できます。

複数のホスト レシバーバーに通知を送信するよう Cisco NX-OS を構成できます。

SNMPv3

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュアアクセスを実現します。SNMPv3 が提供するセキュリティ機能は次のとおりです。

- ・メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- ・認証：メッセージのソースが有効かどうかを判別します。
- ・暗号化：許可されていないソースにより判読されないように、パケットの内容のスクランブルを行います。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティ のレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル

セキュリティ レベルは、SNMP メッセージを開示から保護する必要があるかどうか、およびメッセージを認証するかどうか判断します。セキュリティ モデル内のさまざまなセキュリティ レベルは、次のとおりです。

- noAuthNoPriv : 認証または暗号化を実行しないセキュリティ レベル。このレベルは、SNMPv3 ではサポートされていません。
- authNoPriv : 認証は実行するが、暗号化を実行しないセキュリティ レベル。
- authPriv : 認証と暗号化両方を実行するセキュリティ レベル。

SNMPv1、SNMPv2c、および SNMPv3 の 3 つのセキュリティ モデルを使用できます。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

Table 1: SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティストリング	なし	コミュニティストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティストリング	なし	コミュニティストリングの照合を使用して認証します。

■ ユーザーベースのセキュリティ モデル

モデル	レベル	認証	暗号化	結果
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	未対応	Hash-Based Message Authentication Code (HMAC) メッセージ ダイジェスト 5 (MD5) アルゴリズムまたは HMAC Secure Hash Algorithm (SHA) アルゴリズムに基づいて認証します。
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格 (DES) の 56 ビット暗号化、および暗号ブロック鎖 (CBC) DES (DES-56) 標準に基づいて認証します。

■ ユーザーベースのセキュリティ モデル

SNMPv3 ユーザーベース セキュリティ モデル (USM) は SNMP メッセージ レベル セキュリティを参照し、次のサービスを提供します。

- ・メッセージの完全性：メッセージが不正な方法で変更または破壊されず、データ シーケンスが悪意なく起こり得る範囲を超えて変更されていないことを保証します。
- ・メッセージの発信元の認証：データを受信したユーザーが提示した ID の発信元を確認します。
- ・メッセージの機密性：情報が使用不可であること、または不正なユーザ、エンティティ、またはプロセスに開示されないことを保証します。

SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。

Cisco NX-OS は、次の 2 つの SNMPv3 認証プロトコルを使用します：

- HMAC-MD5-96 認証プロトコル
- HMAC-SHA-96 認証プロトコル

Cisco NX-OS は、SNMPv3 メッセージ暗号化用プライバシープロトコルの1つとして、Advanced Encryption Standard (AES) を使用し、RFC 3826 に準拠します。

priv オプションで、SNMP セキュリティ暗号化方式として、DES または 128 ビット AES 暗号化を選択できます。 **priv** オプションと **aes-128** トークンを併用すると、このプライバシーパスワードは 128 ビットの AES キー番号を生成するためのパスワードになります。AES priv パスワードは、8 文字以上の長さにできます。パスフレーズをクリアテキストで指定する場合、最大 64 文字を指定できます。ローカライズドキーを使用する場合は、最大 130 文字を指定できます。



Note 外部の AAA サーバーを使用して SNMPv3 を使う場合、外部 AAA サーバーのユーザー設定でプライバシープロトコルに AES を指定する必要があります。

CLI および SNMP ユーザの同期

SNMPv3 ユーザー管理は、Access Authentication and Accounting (AAA) サーバー レベルで集中化できます。この中央集中型ユーザー管理により、Cisco NX-OS の SNMP エージェントは AAA サーバーのユーザー認証サービスを利用できます。ユーザー認証が検証されると、SNMP PDU の処理が進行します。AAA サーバはユーザ グループ名の格納にも使用されます。SNMP はグループ名を使用して、スイッチでローカルに使用できるアクセス ポリシーまたはロール ポリシーを適用します。

ユーザー グループ、ロール、またはパスワードの構成が変更されると、SNMP と AAA の両方のデータベースが同期化されます。

Cisco NX-OS は、次のようにユーザー構成を同期化します。

- **auth snmp-server user** コマンドで指定されたパスフレーズは、CLI ユーザーのパスワードになります。
- **username** コマンドで指定されたパスワードは、**auth** および **priv** SNMP ユーザーのパスフレーズになります。
- SNMP または CLI を使用してユーザーを作成または削除すると、SNMP と CLI の両方でユーザーが作成または削除されます。
- ユーザーとロールの対応関係の変更は、SNMP と CLI で同期化されます。
- ロール変更 (CLI からの削除または変更) は、SNMP と同期化されます。



Note パスフレーズまたはパスワードをローカライズしたキーおよび暗号形式で設定した場合、Cisco NX-OS はユーザー情報 (パスワード、ルールなど) を同期させません。



Note UCSS グループは業界全体で使用されている標準的な SNMP 用語なので、SNMP に関する説明では、「ロール」ではなく「グループ」を使用します。

SNMP アクセス権は、グループ別に編成されます。SNMP 内の各グループは、CLI を使用する場合のロールに似ています。各グループは 3 つのアクセス権により定義されます。つまり、読み取りアクセス、書き込みアクセス、および通知アクセスです。それぞれのアクセスを、各グループでイネーブルまたはディセーブルに設定できます。

ユーザ名が作成され、ユーザのロールが管理者によって設定され、ユーザがそのロールに追加されていれば、そのユーザはエージェントとの通信を開始できます。

SNMP の注意事項および制約事項

SNMP には、次の注意事項および制限事項があります。

- SNMP SET を使用して構成されたコマンドは、SNMP SET のみを使用して削除する必要があります。コマンドラインインターフェイス (CLI) または NX-API を使用して構成されたコマンドは、CLI または NX-API のみを使用して削除する必要があります。
- アクセス コントロール リスト (ACL) は、スイッチに設定されたローカル SNMPv3 ユーザのみに適用できます。ACL は、認証、許可、アカウンティング (AAA) サーバに保存されるリモート SNMPv3 ユーザに適用できません。
- Cisco NX-OS は、イーサネット MIB への読み取り専用アクセスをサポートします。詳細については次の URL にアクセスして、Cisco NX-OS の MIB サポートリストを参照してください <ftp://ftp.cisco.com/pub/mibs/supportlists/nexus3000/Nexus3000MIBSupportList.html>。
- Cisco NX-OS は SNMPv3 noAuthNoPriv セキュリティ レベル (Security Level) をサポートしません。
- SNMP SET を使用して構成されたコマンドは、SNMP SET のみを使用して削除する必要があります。コマンドラインインターフェイス (CLI) または NX-API を使用して構成されたコマンドは、CLI または NX-API のみを使用して削除する必要があります。
- Cisco Nexus 3600 シリーズスイッチは、*snmpwalk* 要求に対して最大 10000 個のフラッシュ ファイルをサポートします。
- Cisco NX-OS リリース 10.3(3)F 以降では、SNMPv3 ユーザー パスワードのタイプ 6 暗号化が次の制限付きでサポートされています。
 - タイプ 6 暗号化は、次の点に注意した場合にのみ成功します。
 - **feature password encryption aes {tam}** が有効になっているかどうかに関係なく、OMP ピアのフラッピングが発生します。
 - プライマリ キーが構成されていること。

- 次のオプションは、SNMPv3 ユーザーの構成時に指定されます。 **pwd_type 6** オプション
- プライマリキーの構成を変更すると、SNMPはデータベースに保存されているすべてのタイプ6ユーザーを再暗号化します。ただし、SNMP機能は以前と同じように動作します。
- プライマリキーの設定は、スイッチに対してローカルです。ユーザーが1つのスイッチからタイプ6で構成された実行データを取得し、別のプライマリキーが構成されている別のスイッチに適用すると、同じユーザーのSNMP機能が別のスイッチでは動作しない可能性があります。
- タイプ6が設定されている場合は、タイプ6がサポートされていないリリースにダウングレードする前に、構成を削除するか、タイプ6オプションを再構成してください。
- ISSUの場合、以前のイメージ (localizedkey、localizedV2key構成が存在する) からタイプ6暗号化がサポートされている新しいイメージに移行すると、SNMPは既存のキーをタイプ6暗号化に変換しません。
- 既存のSALT暗号化からタイプ6暗号化への変換は、**encryption re-encrypt obfuscated** コマンドを使用してサポートされます。
- 中断を伴うアップグレードや **reload-ascii** コマンドによる ASCII ベースのリロードを実行すると、プライマリキーが失われ、タイプ6ユーザーのSNMP機能に影響を与えます。
- ユーザーが **encryption re-encrypt obfuscated** コマンドを使用して再暗号化を強制すると、SNMPはタイプ6以外のSNMPユーザーからのすべてのパスワードをタイプ6モードに暗号化します。

**Note**

SNMPは、**encryption delete type6** コマンドをサポートしていません。同じことを示すsyslog警告メッセージも表示されます。

SNMP のデフォルト設定

Table 2: デフォルトの **SNMP** パラメータ

パラメータ	デフォルト
ライセンス通知	イネーブル
linkUp/Down 通知タイプ	ietf-extended

SNMP の設定

SNMP 送信元インターフェイスの設定

特定のインターフェイスを使用するように SNMP を設定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **snmp-server source-interface {inform | trap} type slot/port**
3. switch(config)# **show snmp source-interface**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバルコンフィギュレーション モードを開始します。
ステップ 2	switch(config)# snmp-server source-interface {inform trap} type slot/port	すべての SNMP パケットの送信元インターフェイスを設定します。次のリストに、 <i>interface</i> の有効な値を示します。 <ul style="list-style-type: none"> • ethernet • loopback • mgmt • port-channel • vlan
ステップ 3	switch(config)# show snmp source-interface	設定済みの SNMP 送信元インターフェイスを表示します。

例

次に、SNMP 送信元インターフェイスを設定する例を示します。

```
switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server source-interface inform ethernet 1/10
switch(config)# snmp-server source-interface trap ethernet 1/10
switch(config)# show snmp source-interface
-----
Notification           source-interface
-----
trap                  Ethernet1/10
```

inform

Ethernet1/10

SNMP ユーザの設定



Note Cisco NX-OS で SNMP ユーザーを構成するために使用するコマンドは、Cisco IOS でユーザーを構成するために使用されるものとは異なります。

SUMMARY STEPS

1. **configure terminal**
2. **snmp-server user name [pwd_type 6] [auth {md5 | sha | sha-256 | sha-384 | sha-512} passphrase [auto] [priv [aes-128] passphrase] [engineID id] [localizedkey] | [localizedV2key]]**
3. (Optional) **switch# show snmp user**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config) #</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server user name [pwd_type 6] [auth {md5 sha sha-256 sha-384 sha-512} passphrase [auto] [priv [aes-128] passphrase] [engineID id] [localizedkey] [localizedV2key]] Example: <pre>switch(config) # snmp-server user Admin pwd_type 6 auth sha abcd1234 priv abcdefgh</pre>	認証およびプライバシー パラメータのある SNMP ユーザを設定します。パスフレーズには最大 64 文字の英数字を使用できます。大文字と小文字が区別されます。If you use the localizedkey キーワードを使用する場合は、パスフレーズに大文字と小文字を区別した英数字を 130 文字まで使用できます。 localizedkey - localizedkey キーワードを使用する場合は、パスフレーズに大文字と小文字を区別した英数字を 130 文字まで使用できます。プレーンテキスト パスワードの代わりに、 localizedkey キーワードを使用してハッシュされたパスワード (show running config コマンドからコピーするか、snmpv3 ベースのオープン ソース ハッシュ ジェネレーターツールを使用してオフラインで生成したもの、ハッシュ

SNMP ユーザの設定

	Command or Action	Purpose
		<p>シユ化されたパスワードのオフラインでの生成, on page 11 を参照) を構成できます。</p> <p>Note</p> <p>ローカライズされたキーを使用する場合は、ハッシュ値の前に 0x を追加します。たとえば、0x84a716329158a97ac9f22780629bc26c。</p> <p>localizedV2key - localizedV2key キーを使用する場合、パスフレーズは大文字と小文字を区別した、最大 130 文字の英数字文字列にすることができます。先頭に 0x を付ける必要はありません。これは暗号化されたデータであり、オフラインでは生成できないため、show run コマンドを使用して localizedv2key を収集します。</p> <p>engineID の形式は、12 桁のコロンで区切った 10 進数字です。</p> <p>Note</p> <ul style="list-style-type: none"> Cisco NX-OS リリース 10.1(1) 以降、AES-128 は SNMPv3 のデフォルトのプライバシー プロトコルです。 Cisco NX-OS リリース 10.3(3)F 以降、pwd_type 6 SNMP ユーザー パスワードにタイプ 6 暗号化を提供するために キーワードがサポートされています。
ステップ 3	(Optional) switch# show snmp user Example: switch(config) # show snmp user	1 人または複数の SNMP ユーザーに関する情報を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: switch(config) # copy running-config startup-config	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

Example

次に、SNMP ユーザーを構成する例を示します。

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
```

ハッシュ化されたパスワードのオフラインでの生成

snmpv3 ベースのオープンソースハッシュジェネレータツールを使用して、ハッシュ化されたパスワードをオフラインで生成する手順は、次のとおりです。



(注) 例として挙げられている ID はサンプルの ID で、手順を説明するためだけのものです。

- スイッチから SNMP engineID を取得します。

```
switch# show snmp engineID
```

サンプル出力 :

```
Local SNMP engineID: [Hex] 8000000903D4C93CEA31CC
[Dec] 128:000:000:009:003:212:201:060:234:049:204
```

- SNMPv3 ベースのオープンソースハッシュジェネレータを使用して、ハッシュ化されたパスワードをオフラインで生成します。

```
Linux$ snmpv3-hashgen --auth Hello123 --engine 8000000903D4C93CEA31CC --user1 --mode
priv --hash md5
```

サンプル出力 :

```
User: user1
Auth: Hello123 / 84a716329158a97ac9f22780629bc26c
Priv: Hello123 / 84a716329158a97ac9f22780629bc26c
Engine: 8000000903D4C93CEA31CC
ESXi USM String:
u1/84a716329158a97ac9f22780629bc26c/84a716329158a97ac9f22780629bc26c/priv
```

- auth および priv の値を使用して、スイッチのパスワードを構成します。

```
snmp-server user user1 auth md5 0x84a716329158a97ac9f22780629bc26c priv des
0x84a716329158a97ac9f22780629bc26c localizedkey
```

SNMP メッセージ暗号化の適用

着信要求に認証または暗号化が必要となるよう SNMP を設定できます。デフォルトでは、SNMP エージェントは認証および暗号化を行わないでも SNMPv3 メッセージを受け付けます。プライバシーを適用する場合、Cisco NX-OS は、**noAuthNoPriv** または **authNoPriv** のいずれかのセキュリティ レベル パラメータを使用するすべての SNMPv3 PDU 要求に対して、許可エラーで応答します。

SNMP メッセージの暗号化を特定のユーザーに強制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
switch(config)# snmp-server user name enforcePriv	このユーザーに対して SNMP メッセージ暗号化を適用します。

■ SNMPv3 ユーザに対する複数のロールの割り当て

SNMP メッセージの暗号化をすべてのユーザーに強制するには、グローバルコンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
switch(config)# snmp-server globalEnforcePriv	すべてのユーザーに対して SNMP メッセージ暗号化を適用します。

SNMPv3 ユーザに対する複数のロールの割り当て

SNMP ユーザーを作成した後で、そのユーザーに複数のロールを割り当てることができます。



Note 他のユーザーにロールを割り当てる能够るのは、network-admin ロールに属するユーザーだけです。

コマンド	目的
switch(config)# snmp-server user name group	この SNMP ユーザーと設定されたユーザー ロールをアソシエートします。

SNMP コミュニティの作成

SNMPv1 または SNMPv2c の SNMP コミュニティを作成できます。

コマンド	目的
switch(config)# snmp-server community name group {ro rw}	SNMP コミュニティ ストリングを作成します。

SNMP 要求のフィルタリング

アクセスコントロールリスト (ACL) をコミュニティに割り当てて、着信 SNMP 要求にフィルタを適用できます。割り当てた ACL により着信要求パケットが許可される場合、SNMP はその要求を処理します。ACL により要求が拒否される場合、SNMP はその要求を廃棄して、システム メッセージを送信します。

ACL は次のパラメータで作成します。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元ポート
- 宛先ポート

- プロトコル (UDP または TCP)

ACL は、 UDP および TCP を介する IPv4 および IPv6 の両方に適用されます。 ACL を作成したら、 ACL を SNMP コミュニティに割り当てます。



ヒント ACL の作成の詳細については、使用している Cisco Nexus シリーズ ソフトウェアの NX-OS セキュリティ コンフィギュレーション ガイドを参照してください。

ACL をコミュニティに割り当てて SNMP 要求をフィルタするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
<pre>switch(config)# snmp-server community <i>community name</i> use-acl <i>acl-name</i></pre> <p>Example:</p> <pre>switch(config)# snmp-server community public use-acl my_acl_for_public</pre>	SNMP コミュニティに IPv4 ACL または IPv6 ACL を割り当てて SNMP 要求をフィルタします。

SNMP 通知レシーバの設定

複数のホスト レシーバに対して SNMP 通知を生成するよう Cisco NX-OS を構成できます。

グローバル コンフィギュレーション モードで SNMPv1 トランプのホスト レシーバを設定できます。

コマンド	目的
<pre>switch(config)# snmp-server host <i>ip-address</i> traps version 1 <i>community</i> [udp_port <i>number</i>]</pre>	SNMPv1 トランプのホスト レシーバを設定します。 <i>ip-address</i> は、 IPv4 アドレスまたは IPv6 アドレスである場合があります。 コミュニティは、最大 255 文字の英数字で指定できます。 UDP ポート番号の範囲は 0 ~ 65535 です。

グローバル コンフィギュレーション モードで SNMPv2c トランプまたはインフォームのホスト レシーバを設定できます。

コマンド	目的
<pre>switch(config)# snmp-server host <i>ip-address</i> {traps informs} version 2c <i>community</i> [udp_port <i>number</i>]</pre>	SNMPv2c トランプまたはインフォームのホスト レシーバを設定します。 <i>ip-address</i> は、 IPv4 アドレスまたは IPv6 アドレスである場合があります。 コミュニティは、最大 255 文字の英数字で指定できます。 UDP ポート番号の範囲は 0 ~ 65535 です。

■ VRF を使用する SNMP 通知レシーバの設定

グローバル コンフィギュレーションモードで SNMPv3 ト ラップまたはインフォームのホスト レシーバを設定できます。

コマンド	目的
<code>switch(config)# snmp-server host ip-address {traps informs} version 3 {auth noauth priv} username [udp_port number]</code>	SNMPv2c ト ラップまたはインフォームのホスト レシーバを設定します。 <code>ip-address</code> は、 IPv4 アドレスまたは IPv6 アドレスである場合があります。ユーザー名は、最大 255 文字の英数字で指定できます。 UDP ポート番号の範囲は 0 ~ 65535 です。



Note SNMP マネージャは SNMPv3 メッセージを認証して解読するために、Cisco Nexus デバイスの SNMP engineID に基づいてユーザー クレデンシャル (authKey/PrivKey) を調べる必要があります。

次に、SNMPv1 ト ラップのホスト レシーバを設定する例を示します。

```
switch(config)# snmp-server host 192.0.2.1 traps version 1 public
```

次に、SNMPv2 インフォームのホスト レシーバを設定する例を示します。

```
switch(config)# snmp-server host 192.0.2.1 informs version 2c public
```

次に、SNMPv3 インフォームのホスト レシーバを設定する例を示します。

```
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
```

VRF を使用する SNMP 通知レシーバの設定

設定された VRF をホスト レシーバに接続するように Cisco NX-OS を設定できます。SNMP 通知レシーバの VRF 到達可能性およびフィルタリング オプションを設定すると、SNMP によって CISCO-SNMP-TARGET-EXT-MIB の `cExtSnmpTargetVrfTable` にエントリが追加されます。



(注) VRF 到達可能性またはフィルタリング オプションを設定する前に、ホストを設定する必要があります。

手順の概要

1. `switch# configure terminal`
2. `switch# snmp-server host ip-address use-vrf vrf_name [udp_port number]`
3. (任意) `switch(config)# copy running-config startup-config`

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch# snmp-server host ip-address use-vrf vrf_name [udp_port number]	特定の VRF を使用してホスト レシーバと通信するように SNMP を設定します。IP アドレスは、IPv4 または IPv6 アドレスを使用できます。VRF 名には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ~ 65535 です。このコマンドによって、CISCO-SNMP-TARGET-EXT-MB の ExtSnmpTargetVrfTable にエントリが追加されます。
ステップ 3	(任意) switch(config)# copy running-config startup-config	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、IP アドレス 192.0.2.1 の SNMP サーバー ホストを「Blue」という名前の VRF を使用するように設定する例を示します。

```
switch# configuration terminal
switch(config)# snmp-server host 192.0.2.1 use-vrf Blue
switch(config)# copy running-config startup-config
```

VRFに基づく SNMP 通知のフィルタリング

通知が発生した VRF に基づいて、Cisco NX-OS 通知をフィルタリングするように設定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **snmp-server host ip-address filter-vrf vrf_name [udp_port number]**
3. (任意) switch(config)# **copy running-config startup-config**

■ インバンドアクセスのための SNMP の設定

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# snmp-server host ip-address filter-vrf vrf_name [udp_port number]	設定された VRF に基づいて、通知ホスト レシーバへの通知をフィルタリングします。IP アドレスは、IPv4 または IPv6 アドレスを使用できます。VRF 名には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ~ 65535 です。 このコマンドによって、CISCO-SNMP-TARGET-EXT-MB の ExtSnmpTargetVrfTable にエントリが追加されます。
ステップ 3	(任意) switch(config)# copy running-config startup-config	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、VRF に基づいて SNMP 通知のフィルタリングを設定する例を示します。

```
switch# configuration terminal
switch(config)# snmp-server host 192.0.2.1 filter-vrf Red
switch(config)# copy running-config startup-config
```

インバンドアクセスのための SNMP の設定

次のものを使用して、インバンドアクセス用に SNMP を設定できます。

- コンテキストのない SNMP v2 の使用：コンテキストにマッピングされたコミュニティを使用できます。この場合、SNMP クライアントはコンテキストについて認識する必要はありません。
- コンテキストのある SNMP v2 の使用：SNMP クライアントはコミュニティ、たとえば、<community>@<context> を指定して、コンテキストを指定する必要があります。
- SNMP v3 の使用：コンテキストを指定できます。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **snmp-server context context-name vrf vrf-name**

3. switch(config)# **snmp-server community** *community-name* **group** *group-name*
4. switch(config)# **snmp-server mib community-map** *community-name* **context** *context-name*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configuration terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# snmp-server context <i>context-name</i> vrf <i>vrf-name</i>	管理VRFまたはデフォルトVRFにSNMPコンテキストをマッピングします。カスタムVRFはサポートされません。 名前には最大32の英数字を使用できます。
ステップ 3	switch(config)# snmp-server community <i>community-name</i> group <i>group-name</i>	SNMPv2cコミュニティとSNMPコンテキストにマッピングし、コミュニティが属するグループを識別します。名前には最大32の英数字を使用できます。
ステップ 4	switch(config)# snmp-server mib community-map <i>community-name</i> context <i>context-name</i>	SNMPv2cコミュニティをSNMPコンテキストにマッピングします。名前には最大32の英数字を使用できます。

例

次のSNMPv2の例は、コンテキストにsnmpdefaultという名前のコミュニティをマッピングする方法を示しています。

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server context def vrf default
switch(config)# snmp-server community snmpdefault group network-admin
switch(config)# snmp-server mib community-map snmpdefault context def
switch(config)#

```

次のSNMPv2の例は、マッピングされていないコミュニティcommを設定し、インバンドアクセスする方法を示しています。

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server context def vrf default
switch(config)# snmp-server community comm group network-admin
switch(config)#

```

次のSNMPv3の例は、v3ユーザーネームとパスワードを使用する方法を示しています。

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server context def vrf default
switch(config)#

```

SNMP 通知のイネーブル化

通知をイネーブルまたはディセーブルにできます。通知名を指定しないと、Cisco NX-OS は通知をすべてイネーブルにします。



Note 値は、**snmp-server enable traps** CLI コマンドを使用すると、構成通知ホストトレシーバーによっては、トラップとインフォームの両方をイネーブルにできます。

次の表に、Cisco NX-OS MIB の通知を有効にする CLI コマンドを示します。

Table 3: SNMP 通知のイネーブル化

MIB	関連コマンド
すべての通知	snmp-server enable traps
CISCO-ERR-DISABLE-MIB	snmp-server enable traps show interface status
Q-BRIDGE-MIB	snmp-server enable traps show mac address-table
CISCO-SWITCH-QOS-MIB	snmp-server enable traps show hardware internal buffer info pkt-stats
BRIDGE-MIB	snmp-server enable traps bridge newroot snmp-server enable traps bridge topologychange
CISCO-AAA-SERVER-MIB	snmp-server enable traps aaa
ENTITY-MIB、 CISCO-ENTITY-FRU-CONTROL-MIB、 CISCO-ENTITY-SENSOR-MIB	snmp-server enable traps entity snmp-server enable traps entity fru
CISCO-LICENSE-MGR-MIB	snmp-server enable traps license
IF-MIB	snmp-server enable traps link
CISCO-PSM-MIB	snmp-server enable traps port-security
SNMPv2-MIB	snmp-server enable traps snmp snmp-server enable traps snmp authentication
CISCO-FCC-MIB	snmp-server enable traps fcc
CISCO-DM-MIB	snmp-server enable traps fdomain
CISCO-NS-MIB	snmp-server enable traps fcns
CISCO-FCS-MIB	snmp-server enable traps fcs discovery-complete snmp-server enable traps fcs request-reject

MIB	関連コマンド
CISCO-FDMI-MIB	snmp-server enable traps fDMI
CISCO-FSPF-MIB	snmp-server enable traps fSPF
CISCO-PSM-MIB	snmp-server enable traps port-security
CISCO-RSCN-MIB	snmp-server enable traps rscn snmp-server enable traps rscn els snmp-server enable traps rscn ils
CISCO-ZS-MIB	snmp-server enable traps zone snmp-server enable traps zone default-zone-behavior-change snmp-server enable traps zone enhanced-zone-db-change snmp-server enable traps zone merge-failure snmp-server enable traps zone merge-success snmp-server enable traps zone request-reject snmp-server enable traps zone unsupp-mem
CISCO-CONFIG-MAN-MIB Note ccmCLIRunningConfigChanged 通知を除き、MIB オブジェクトをサポートしていません。	snmp-server enable traps config



Note ライセンス通知は、デフォルトではイネーブルです。

グローバル コンフィギュレーション モードで指定の通知をイネーブルにするには、次の作業を行います。

コマンド	目的
switch(config)# snmp-server enable traps	すべての SNMP 通知をイネーブルにします。
switch(config)# snmp-server enable traps aaa [server-state-change]	AAA SNMP 通知をイネーブルにします。
switch(config)# snmp-server enable traps entity [fru]	ENTITY-MIB SNMP 通知をイネーブルにします。
switch(config)# snmp-server enable traps license	ライセンス SNMP 通知をイネーブルにします。

リンクの通知の設定

コマンド	目的
switch(config)# snmp-server enable traps port-security	ポートセキュリティ SNMP 通知をイネーブルにします。
switch(config)# snmp-server enable traps snmp [authentication]	SNMP エージェント通知をイネーブルにします。

リンクの通知の設定

デバイスに対して、イネーブルにする linkUp/linkDown 通知を設定できます。次のタイプの linkUp/linkDown 通知をイネーブルにできます。

- **cieLinkDown** : シスコ拡張リンク ステート ダウン通知をイネーブルにします。
- **cieLinkUp** : シスコ拡張リンク ステート アップ通知をイネーブルにします。
- **cisco-xcvr-mon-status-chg** : シスコ インターフェイス トランシーバ モニター ステータス変更通知をイネーブルにします。
- **delayed-link-state-change** : 遅延リンク ステート 変更をイネーブルにします。
- **extended-linkUp** : IETF 拡張リンク ステート アップ通知をイネーブルにします。
- **extended-linkDown** : IETF 拡張リンク ステート ダウン通知をイネーブルにします。
- **linkDown** : IETF リンク ステート ダウン通知をイネーブルにします。
- **linkUp** : IETF リンク ステート アップ通知をイネーブルにします。

手順の概要

1. **configure terminal**
2. **snmp-server enable traps link [cieLinkDown | cieLinkUp | cisco-xcvr-mon-status-chg | delayed-link-state-change] | extended-linkUp | extended-linkDown | linkDown | linkUp]**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	<pre>snmp-server enable traps link [cieLinkDown cieLinkUp cisco-xcvr-mon-status-chg delayed-link-state-change] extended-linkUp extended-linkDown linkDown linkUp]</pre> <p>例 :</p> <pre>switch(config)# snmp-server enable traps link cieLinkDown</pre>	リンク SNMP 通知をイネーブルにします。

インターフェイスでのリンク通知のディセーブル化

個別のインターフェイスで linkUp および linkDown 通知をディセーブルにできます。これにより、フラッピングインターフェイス（アップとダウン間の移行を繰り返しているインターフェイス）に関する通知を制限できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config -if)# **no snmp trap link-status**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface type slot/port	変更するインターフェイスを指定します。
ステップ 3	switch(config -if)# no snmp trap link-status	インターフェイスの SNMP リンクステート トラブルをディセーブルにします。この機能は、デフォルトでイネーブルにされています。

TCP での SNMP に対するワンタイム認証のイネーブル化

TCP セッション上で SNMP に対するワンタイム認証をイネーブルにできます。

コマンド	目的
switch(config)# snmp-server tcp-session [auth]	TCP セッション上で SNMP に対するワンタイム認証をイネーブルにします。この機能はデフォルトで無効に設定されています。

■ SNMP スイッチの連絡先および場所の情報の割り当て

SNMP スイッチの連絡先および場所の情報の割り当て

スイッチの連絡先情報（スペースを含めず、最大 32 文字まで）およびスイッチの場所を割り当てるすることができます。

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **snmp-server contact** *name*
3. switch(config)# **snmp-server location** *name*
4. (Optional) switch# **show snmp**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# configuration terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# snmp-server contact <i>name</i>	sysContact (SNMP 担当者名) を設定します。
ステップ 3	switch(config)# snmp-server location <i>name</i>	sysLocation (SNMP ロケーション) を設定します。
ステップ 4	(Optional) switch# show snmp	1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	(Optional) switch# copy running-config startup-config	この設定変更を保存します。

コンテキストとネットワーク エンティティ間のマッピング設定

プロトコルインスタンス、VRF などの論理ネットワーク エンティティに対する SNMP コンテキストのマッピングを設定できます。

SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]
3. switch(config)# **snmp-server mib community-map** *community-name* **context** *context-name*
4. (Optional) switch(config)# **no snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# configuration terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# snmp-server context context-name [instance instance-name] [vrf vrf-name] [topology topology-name]	SNMP コンテキストをプロトコル インスタンス、VRF、またはトポロジにマッピングします。名前には最大 32 の英数字を使用できます。
ステップ 3	switch(config)# snmp-server mib community-map community-name context context-name	SNMPv2c コミュニティを SNMP コンテキストにマッピングします。名前には最大 32 の英数字を使用できます。
ステップ 4	(Optional) switch(config)# no snmp-server context context-name [instance instance-name] [vrf vrf-name] [topology topology-name]	SNMP コンテキストとプロトコル インスタンス、VRF、またはトポロジ間のマッピングを削除します。名前には最大 32 の英数字を使用できます。 Note コンテキスト マッピングを削除する目的で、インスタンス、VRF、またはトポロジを入力しないでください。 instance 、 vrf 、または topology キーワードを使用すると、コンテキストとゼロ長ストリング間のマッピングが設定されます。

SNMP ローカル エンジン ID の設定

Cisco NX-OS リリース 7.0 (3) F3 (1) 以降では、ローカル デバイスにエンジン ID を構成できます。

SUMMARY STEPS

1. **configure terminal**
2. **snmp-server engineID local engineid-string**
3. **show snmp engineID**
4. **[no] snmp-server engineID local engineid-string**
5. **copy running-config startup-config**

■ SNMP の無効化

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config) #</pre>	グローバルコンフィギュレーションモードを開始します。
ステップ 2	snmp-server engineID local engineid-string Example: <pre>switch(config) # snmp-server engineID local AA:BB:CC:1A:2C:10</pre>	ローカルデバイスの SNMP engineID を変更します。ローカルエンジン ID は、コロンで指定された 16 進数オクテットのリストとして設定する必要があります。ここでは 10 ~ 64 の範囲の偶数 16 進数文字が使用され、2 つの 16 進数文字ごとにコロンで区切れます。たとえば、i80:00:02:b8:04:61:62:63 です。
ステップ 3	show snmp engineID Example: <pre>switch(config) # show snmp engineID</pre>	設定されている SNMP エンジンの ID を表示します。
ステップ 4	[no] snmp-server engineID local engineid-string Example: <pre>switch(config) # no snmp-server engineID local AA:BB:CC:1A:2C:10</pre>	ローカルエンジン ID を無効にし、自動生成されたデフォルトのエンジン ID を設定します。
ステップ 5	Required: copy running-config startup-config Example: <pre>switch(config) # copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

SNMP の無効化

手順の概要

1. **configure terminal**
2. **switch(config) # no snmp-server protocol enable**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ1	configure terminal 例： switch# configure terminal switch(config) #	グローバル コンフィギュレーション モードを開始します。
ステップ2	switch(config) # no snmp-server protocol enable 例： no snmp-server protocol enable	SNMP を無効にします。 SNMP は、デフォルトで無効になっています。

SNMP 設定の確認

SNMP 設定情報を表示するには、次の作業を行います。

コマンド	目的
show snmp	SNMP ステータスを表示します。
show snmp community	SNMP コミュニティ ストリングを表示します。
show interface snmp-ifindex	すべてのインターフェイスについて (IF-MIB から) SNMP の ifIndex 値を表示します。
show running-config snmp [all]	SNMP の実行コンフィギュレーションを表示します。
show snmp engineID	SNMP engineID を表示します。
show snmp group	SNMP ロールを表示します。
show snmp sessions	SNMP セッションを表示します。
show snmp context	SNMP コンテキスト マッピングを表示します。
show snmp host	設定した SNMP ホストの情報を表示します。
show snmp source-interface	設定した発信元インターフェイスの情報を表示します。
show snmp trap	イネーブルまたはディセーブルである SNMP 通知を表示します。
show snmp user	SNMPv3 ユーザを表示します。

■ SNMP 設定の確認

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。