SNMP の設定

SNMP の概要

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 はネットワークデバイスのモニタリングや管理のための標準化されたフレームワークと共通言語を提供します。

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（SNMP agent）]：Cisco UCS 内のソフトウェア コンポーネントであり、Cisco UCS のデータを維持し、必要に応じて SNMP マネージャにデータをレポートする管理対象デバイスです。Cisco UCS には、エージェントと MIB 収集が含まれます。SNMP エージェントを有効にしてマネージャとエージェント間のリレーションシップを作成するには、Cisco UCS Manager で SNMP を有効にして設定します。
- 管理情報ベース：SNMP エージェントの一連の管理対象オブジェクト。Cisco UCS リリース 1.4(1) 以降では、以前よりも多くの MIB をサポートしています。

Cisco UCS 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 は次のように定義されています。

- RFC 3410（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）
- 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 UCS Manager 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。SNMP マネージャはトラップ受信時に確認応答を送信せず、Cisco UCS Manager はトラップが受信されたかどうかを確認できないため、トラップの信頼性はインフォームよりも低くなります。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します。Cisco UCS Manager が PDU を受信しない場合、インフォーム要求を再送できます。

SNMP セキュリティ レベルおよび権限

SNMPv1、SNMPv2c、および SNMPv3 はそれぞれ別のセキュリティ モデルを表します。セキュリティ モデルと選択したセキュリティ 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。

セキュリティ レベルは、SNMP トラップに関連付けられているメッセージを表示するために必要な特権を決定します。権限のレベルによって、メッセージが情報開示の保護を必要とするか、またはメッセージが認証されるかが決定されます。サポートされるセキュリティ レベルは、実装されているセキュリティ モデルによって異なります。SNMP セキュリティ レベルは、次の権限の 1 つ以上をサポートします。

- noAuthNoPriv：認証なし、暗号化なし
- authNoPriv：認証あり、暗号化なし
- authPriv：認証あり、暗号化あり

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。

SNMP セキュリティ モデルとレベルのサポートされている組み合わせ

次の表に、セキュリティ モデルとレベルの組み合わせを示します。

表 *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。
v3	noAuthNoPriv	ユーザ名	未対応	ユーザ名の照合を使用して認証します。
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連鎖（CBC）DES（DES-56）標準に基づいた認証を提供します。

SNMPv3 セキュリティ機能

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 は、管理操作および暗号化 SNMP メッセー

ジを実行するために、設定されているユーザーのみを承認します。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ていないこと、悪意なく起こり得る範囲を超えてデータ シーケンスが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：メッセージ送信者の ID を確認できることを保証します。
- メッセージの機密性および暗号化：不正なユーザ、エンティティ、プロセスに対して情報を利用不可にしたり開示しないようにします。

Cisco UCS での SNMP サポート

Cisco UCS は、SNMP に対して以下のサポートを提供します。

MIB のサポート

Cisco UCS は、MIB への読み取り専用アクセスをサポートします。

Cisco UCS で使用可能な特定の MIB およびその入手先については、B シリーズ サーバーは http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html を、C シリーズは http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/c-series/b_UCS_Standalone_C-Series_MIBRef.html を参照してください。

SNMPv3 ユーザーの認証プロトコル

Cisco UCS は、SNMPv3 ユーザーに次の認証プロトコルをサポートします。

- HMAC-MD5-96（MD5）
- HMAC-SHA-96（SHA）

SNMPv3 ユーザーの AES プライバシー プロトコル

Cisco UCS は、SNMPv3 メッセージ暗号化用のプライバシー プロトコルの 1 つとして Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠しています。

プライバシー パスワード（priv オプション）では、SNMP セキュリティ暗号化方式として DES または 128 ビット AES を選択できます。AES-128 の設定を有効にして、SNMPv3 ユーザー用のプライバシー パスワードを含めると、Cisco UCS Manager はそのプライバシー パスワードを使用して 128 ビット AES キーを生成します。AES priv パスワードは、8 文字以上にします。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。

このようなユーザーを展開するには、[AES-128] 暗号化を有効にします。

SNMP の有効化と SNMP プロパティの設定

Cisco UCS ドメインからの SNMP メッセージには、システム名ではなくファブリック インターコネクト名が表示されます。

Procedure

ステップ 1 [ナビゲーション]ペインで、[管理者]をクリックします。

ステップ 2 **[すべて]** > **[通信管理]** > **[通信サービス]**を展開します。

ステップ 3 [通信サービス（Communication Services）] タブを選択します。

ステップ 4 [SNMP] 領域で、次のフィールドに入力します。

名前	説明
[管理状態（Admin State）] フィールド	次のいずれかになります。 • **有効** • **無効** システムに SNMP サーバとの統合が含まれる場合にだけこのサービスをイネーブルにします。 **[管理状態（Admin State）]** が有効になっている場合は、Cisco UCS Manager GUIにこのセクションの残りのフィールドが表示されます。

ステップ 5 **[Save Changes]**をクリックします。

What to do next

SNMP トラップおよびユーザを作成します。

SNMP トラップの作成

手順

ステップ 1 [ナビゲーション]ペインで、[管理者]をクリックします。

ステップ 2 **[すべて]** > **[通信管理]** > **[通信サービス]**を展開します。

ステップ 3 [Communication Services] タブを選択します。

ステップ 4 [SNMP Traps] 領域で、[+] をクリックします。

ステップ 5 [Create SNMP Trap] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[ホスト名（または IP アドレス）（Hostname (or IP Address)）] フィールド	Cisco UCS Manager がトラップを送信する SNMP ホストのホスト名または IP アドレス。 SNMP ホストには IPv4 アドレスまたは IPv6 アドレスを使用できます。ホスト名を IPv4 アドレスの完全修飾ドメイン名にすることもできます。
[コミュニティ/ユーザ名（Community/Username）] フィールド	Cisco UCS Manager が SNMP ホストにトラップを送信するときに含める、SNMP v1 または v2c コミュニティ名、または SNMP v3 ユーザ名。これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。 1 ～ 32 文字の英数字文字列を入力します。@（アット マーク）、\（バックスラッシュ）、"（二重引用符）、?(疑問符)、&（アンパサンド）、または空のスペースは使用しないでください。
[ポート（Port）] フィールド	トラップのために Cisco UCS Manager が SNMP ホストと通信するポート。 1 ～ 65535 の整数を入力します。デフォルトのポートは 162 です。
[バージョン（Version）] フィールド	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 • **V1** • **V2c** • **V3**
[タイプ（Type）] フィールド	送信するトラップのタイプ。バージョンに **V2c** または **V3** を選択する場合、送信するトラップのタイプは次のいずれかになります。 • **[Traps]** • **情報**
[v3 特権（v3 Privilege）] フィールド	バージョンとして [V3] を選択した場合に、トラップに関連付ける権限。次のいずれかになります。 • [認証（Auth）]：認証あり、暗号化なし • [認証なし（Noauth）]：認証なし、暗号化なし • [秘密（Priv）]：認証あり、暗号化あり

（注）　最大 8 つのホストを SNMP トラップに追加できます。

ステップ 6 [OK] をクリックします。
ステップ 7 **[Save Changes]**をクリックします。

SNMP トラップの削除

手順

ステップ 1 [ナビゲーション]ペインで、[管理者]をクリックします。
ステップ 2 **[すべて]** > **[通信管理]** > **[通信サービス]**を展開します。
ステップ 3 [Communication Services] タブを選択します。
ステップ 4 [SNMP Traps] 領域で、削除するユーザに対応するテーブルの行をクリックします。
ステップ 5 テーブルの右側の [Delete] アイコンをクリックします。
ステップ 6 確認ダイアログボックスが表示されたら、**[はい]**をクリックします。
ステップ 7 **[Save Changes]**をクリックします。

SNMPv3 ユーザの作成

手順

ステップ 1 [ナビゲーション]ペインで、[管理者]をクリックします。
ステップ 2 **[すべて]** > **[通信管理]** > **[通信サービス]**を展開します。
ステップ 3 [Communication Services] タブを選択します。
ステップ 4 [SNMP Users] 領域で、[+] をクリックします。
ステップ 5 [Create SNMP User] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	SNMP ユーザーに割り当てられるユーザー名。 32 文字までの文字または数字を入力します。名前は文字で始まる必要があり、_（アンダースコア）、.（ピリオド）、@（アット マーク）、-（ハイフン）も指定できます。 （注）　ローカル側で認証されたユーザ名と同一の SNMP ユーザ名を作成することはできません。

名前	説明
[Auth Type] フィールド	許可タイプ。これはできるだけ**SHA**です。
Use aes-128] フィールド	かどうか、ユーザは、aes-128 暗号化を使用します。
[パスワード（Password）] フィールド	このユーザのパスワード。
[Confirm Password] フィールド	確認のためのパスワードの再入力。
[Privacy Password] フィールド	このユーザのプライバシー パスワード。
[Confirm Privacy Password] フィールド	確認のためのプライバシー パスワードの再入力。

ステップ 6 [OK] をクリックします。

ステップ 7 **[Save Changes]**をクリックします。

SNMPv3 ユーザの削除

手順

ステップ 1 [ナビゲーション]ペインで、[管理者]をクリックします。

ステップ 2 **[すべて]** > **[通信管理]** > **[通信サービス]**を展開します。

ステップ 3 [Communication Services] タブを選択します。

ステップ 4 [SNMP Users] 領域で、削除するユーザに対応するテーブルの行をクリックします。

ステップ 5 テーブルの右側の [Delete] アイコンをクリックします。

ステップ 6 確認ダイアログボックスが表示されたら、**[はい]**をクリックします。

ステップ 7 **[Save Changes]**をクリックします。

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。