コミュニケーション サービスの設定

この章は、次の項で構成されています。

セキュアおよび非セキュアなブラウザの UCS Manager

以下に定義する通信サービスを使用してサードパーティ アプリケーションを Cisco UCS に接続できます。

Cisco UCS Manager は、次のサービスに対する IPv4 および IPv6 アドレス アクセスの両方をサポートします。

- CIM XML
- HTTP
- HTTPS
- SNMP
- SSH
- Telnet

Cisco UCS Manager では、Web ブラウザから [Cisco UCS KVM Direct] 起動ページへのアウトオブバンドIPv4アドレスアクセスをサポートしています。このアクセスを提供するには、次のサービスをイネーブルにする必要があります。

- CIMC Web サービス

通信サービス	説明
CIM XML	Common Information Model（CIM XML）サービスはデフォルトはディセーブルであり、読み取り専用モードでのみ利用できます。デフォルトのポートは 5988 です。 CIM XML は、Distributed Management Task Force によって定義された CIM 情報を交換するための標準ベースのプロトコルです。
CIMC Web サービス	このサービスは、デフォルトでディセーブルになります。 このサービスをイネーブルにすると、ユーザは直接サーバに割り当てられるか、またはサービス プロファイルを介しサーバに関連付けられたアウトオブバンドの管理IPアドレスの1つを使用して直接サーバCIMCにアクセスできます。 （注） CIMC Web サービスは全体的にイネーブルまたはディセーブルにすることのみが可能です。個別の CIMC IP アドレスに対し KVM ダイレクト アクセスを設定できません。
HTTP	デフォルトでは、HTTP はポート 80 でイネーブルになっています。 Cisco UCS Manager GUI は HTTP または HTTPS のブラウザで実行できます。HTTP を選択した場合、すべてのデータはクリア テキスト モードで交換されます。 セキュアなブラウザ セッションを確立するため、HTTPS をイネーブルにし、HTTP をディセーブルにすることを推奨します。 デフォルトでは、Cisco UCS では同等の HTTPS にリダイレクトするブラウザ リダイレクトを実装しています。この動作は変更しないことを推奨します。 （注） Cisco UCS バージョン 1.4(1) にアップグレードすると、セキュアなブラウザへのブラウザのリダイレクトはデフォルトでは発生しなくなります。HTTP ブラウザからの同等の HTTPS ブラウザへリダイレクトするには、Cisco UCS Manager で [Redirect HTTP to HTTPS] をイネーブルにします。

通信サービス	説明
HTTPS	デフォルトでは、HTTPS はポートでイネーブルになっています。 HTTPS を使用すると、すべてのデータはセキュアなサーバを介して暗号化モードで交換されます。 セキュアなブラウザ セッションを確立するため、HTTPS だけを使用するようにし、HTTP 通信はディセーブルにするかリダイレクトすることを推奨します。
SMASH CLP	このサービスは読み取り専用アクセスに対してイネーブルになり、**show** コマンドなど、プロトコルの一部のサブセットをサポートします。これをディセーブルにすることはできません。 このシェル サービスは、Distributed Management Task Force によって定義された標準の 1 つです。
SNMP	デフォルトでは、このサービスはディセーブルになっています。イネーブルの場合、デフォルトのポートは 161 です。コミュニティと少なくとも 1 つの SNMP トラップを設定する必要があります。 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。
SSH	このサービスは、ポート 22 でイネーブルになります。これはディセーブルにできず、デフォルトのポートを変更することもできません。 このサービスは Cisco UCS Manager CLI へのアクセスを提供します。
Telnet	デフォルトでは、このサービスはディセーブルになっています。 このサービスは Cisco UCS Manager CLI へのアクセスを提供します。

CIM-XML の設定

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [Communication Management] > [Communication Services] 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 [CIM-XML] 領域で、[Enabled] オプション ボタンをクリックします。

[CIM-XML] 領域が展開して、デフォルトの [Port] 番号 5988 を表示します。このポート番号は変更できません。

ステップ 5 [Save Changes] をクリックします。

HTTP の設定

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [Communication Management] > [Communication Services] を展開します。

ステップ 3 [Communication Services] タブをクリックします。

ステップ 4 [HTTP] 領域で、[Enabled] オプション ボタンをクリックします。
[HTTP] 領域が展開され、利用可能な設定オプションが表示されます。

ステップ 5 （任意） [Port] フィールドで、 Cisco UCS Manager GUI が HTTP に使用するデフォルトのポートを変更します。
デフォルトのポートは 80 です。

ステップ 6 （任意） [Redirect HTTP to HTTPS] フィールドで、[Enabled] オプション ボタンをクリックします。
HTTP ログインの HTTPS ログインへのリダイレクションをイネーブルにするには、HTTPS も設定して有効にする必要があります。いったんイネーブルにすると、HTTPS をディセーブルにするまではリダイレクションをディセーブルにできません。

（注） HTTP を HTTPS にリダイレクトする場合、Cisco UCS Manager GUI へのアクセスに HTTP は使用できません。リダイレクションは、HTTP をディセーブルにして、自動的に HTTPS にリダイレクトします。

ステップ 7 [Save Changes] をクリックします。

HTTPS の設定

証明書、キー リング、トラスト ポイント

HTTPS では、公開キー インフラストラクチャ（PKI）のコンポーネントを使用して、クライアントのブラウザと Cisco UCS Manager などの 2 つのデバイス間でセキュアな通信を確立します。

暗号キーとキー リング

各 PKI デバイスは、内部キー リングに非対称の Rivest-Shamir-Adleman（RSA）暗号キーのペア（1 つはプライベート、もう 1 つはパブリック）を保持します。いずれかのキーで暗号化されたメッセージは、もう一方のキーで復号化できます。暗号化されたメッセージを送信する場合、送信者は受信者の公開キーで暗号化し、受信者は独自の秘密キーを使用してメッセージを復号化します。送信者は、独自の秘密キーで既知のメッセージを暗号化（「署名」とも呼ばれます）して公開キーの所有者を証明することもできます。受信者が該当する公開キーを使用してメッセージを正常に復号化できる場合は、送信者が対応する秘密キーを所有していることが証明されます。暗号キーの長さはさまざまであり、通常の長さは 512 ビット ～ 2048 ビットです。一般的に、短いキーよりも長いキーの方がセキュアになります。Cisco UCS Manager では、最初に 1024 ビットのキー ペアを含むデフォルトのキー リングが提供されます。その後、追加のキー リングを作成できるようになります。

クラスタ名が変更されたり、証明書が期限切れになったりした場合は、デフォルトのキー リング証明書を手動で再生成する必要があります。

この操作は、UCS Manager CLI のみで使用できます。

証明書

セキュアな通信を準備するには、まず2つのデバイスがそれぞれのデジタル証明書を交換します。証明書は、デバイスの ID に関する署名済み情報とともにデバイスの公開キーを含むファイルです。暗号化された通信をサポートするために、デバイスは独自のキー ペアと独自の自己署名証明書を生成できます。リモート ユーザが自己署名証明書を提示するデバイスに接続する場合、ユーザはデバイスの ID を簡単に検証することができず、ユーザのブラウザは最初に認証に関する警告を表示します。デフォルトでは、Cisco UCS Manager にはデフォルトのキー リングからの公開キーを含む組み込み用自己署名証明書が含まれます。

トラスト ポイント

Cisco UCS Manager に強力な認証を提供するために、デバイスの ID を証明する信頼できるソース（つまり、トラスト ポイント）からサードパーティ証明書を取得し、インストールできます。サードパーティ証明書は、発行元トラスト ポイント（ルート認証局（CA）、中間 CA、またはルート CA につながるトラスト チェーンの一部となるトラスト アンカーのいずれか）によって署名されます。新しい証明書を取得するには、Cisco UCS Manager で証明書要求を生成し、トラスト ポイントに要求を送信する必要があります。

重要 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

キー リングの作成

Cisco UCS Manager は、デフォルト キー リングを含め、最大 8 個のキー リングをサポートします。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [Key Management] を展開します。

ステップ 3 [Key Management] を右クリックし、[Create Key Ring] を選択します。

ステップ 4 [Create Key Ring] ダイアログボックスで、次の手順を実行します。

a) [Name] フィールド で、キー リングの一意の名前を入力します。

b) [Modulus] フィールド で、次のいずれかのオプション ボタンを選択し、SSL キー長をビット単位で指定します。

- Mod512
- Mod1024
- Mod1536
- Mod2048
- Mod2560
- Mod3072
- Mod3584
- Mod4096

c) [OK] をクリックします。

次の作業

このキー リングの証明書要求を作成します。

キー リングの証明書要求の作成

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [Key Management] を展開します。

ステップ 3 証明書要求を作成するキー リングをクリックします。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ 5 [General] タブで [Create Certificate Request] をクリックします。

ステップ 6 [Create Certificate Request] 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
[DNS] フィールド	ネットワークに割り当てられたドメイン名（すべてのホストに共通）。
[Locality] フィールド	証明書を要求している会社の本社が存在する市または町。 最大64文字まで入力できます。任意の文字、数字、スペース、および次の特殊文字を使用できます：,（カンマ）、.（ピリオド）、@（アットマーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。
[State] フィールド	証明書を要求している会社の本社が存在する州または行政区分。 最大64文字まで入力できます。任意の文字、数字、スペース、および次の特殊文字を使用できます：,（カンマ）、.（ピリオド）、@（アットマーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。
[Country] フィールド	会社所在国の国コード。 2 文字のアルファベットを入力します。
[Organization Name] フィールド	証明書を要求している組織。 最大64文字まで入力できます。任意の文字、数字、スペース、および次の特殊文字を使用できます：,（カンマ）、.（ピリオド）、@（アットマーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。
[Organization Unit Name] フィールド	組織ユニット 最大64文字まで入力できます。任意の文字、数字、スペース、および次の特殊文字を使用できます：,（カンマ）、.（ピリオド）、@（アットマーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。
[Email] フィールド	要求に関連付けられている電子メール アドレス。
[Password] フィールド	この要求に対するオプションのパスワード。
[Confirm Password] フィールド	パスワードを指定した場合は、確認のためにそのパスワードを再入力します。
[Subject] フィールド	ファブリック インターコネクトの完全修飾ドメイン名。

ステップ 7 IP アドレスを割り当てるには、[IPv4] または [IPv6] のタブをクリックします。この選択は、Cisco UCS Manager をセットアップするときのファブリック インターコネクトの設定に応じて行います。

- [IPv4] タブをクリックし、次のフィールドに値を入力します。

名前	説明
[IP Address] フィールド	Cisco UCS ドメインの IPv4 アドレス。
[FI-A IP] フィールド	ファブリック インターコネクト A の IPv4 アドレス。
[FI-B IP] フィールド	ファブリック インターコネクト B の IPv4 アドレス。

- [IPv6] タブをクリックし、次のフィールドに値を入力します。

名前	説明
[IP Address] フィールド	Cisco UCS ドメインの IPv6 アドレス。
[FI-A IP] フィールド	ファブリック インターコネクト A の IPv6 アドレス。
[FI-B IP] フィールド	ファブリック インターコネクト B の IPv6 アドレス。

ステップ 8 [OK] をクリックします。

ステップ 9 [Request] フィールドから証明書要求のテキストをコピーし、ファイルに保存します。

ステップ 10 証明書要求を含むファイルをトラスト アンカーまたは認証局に送信します。

次の作業

トラストポイントを作成し、トラストアンカーから受け取ったトラストの証明書の証明書チェーンを設定します。

トラスト ポイントの作成

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [Key Management] を展開します。

ステップ 3 [Key Management] を右クリックし、[Create Trusted Point] を選択します。

ステップ 4 [Create Trusted Point] 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
[Name] フィールド	トラスト ポイントの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Certificate Chain] フィールド	このトラスト ポイントの証明書情報。 **重要** 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

ステップ 5 [OK] をクリックします。

次の作業

トラスト アンカーまたは認証局から証明書を受信したら、キー リングにインポートします。

キー リングへの証明書のインポート

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [Key Management] を展開します。

ステップ 3 証明書のインポート先となるキー リングをクリックします。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ 5 [Certificate] 領域で、次のフィールドに値を入力します。

a) [Trusted Point] ドロップダウン リストから、この証明書を付与したトラスト アンカーのトラスト ポイントを選択します。
b) [Certificate] フィールドに、トラスト アンカーまたは認証局から受け取った証明書のテキストを貼り付けます。

重要 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

ヒント この領域のフィールドが表示されない場合は、見出しの右側の展開アイコンをクリックします。

ステップ 6 [Save Changes] をクリックします。

次の作業

キー リングを使用して HTTPS サービスを設定します。

HTTPS の設定

注意 HTTPS で使用するポートとキー リングの変更を含め、HTTPS の設定を完了した後、トランザクションを保存またはコミットするとすぐに、現在のすべての HTTP および HTTPS セッションは警告なく閉じられます。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [Communication Management] > [Communication Services] 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 [HTTPS] 領域で、[Enabled] オプション ボタンをクリックします。
[HTTPS] 領域が展開され、利用可能な設定オプションが表示されます。
ステップ 5 次のフィールドに入力します。

名前	説明
[Admin State] フィールド	次のいずれかになります。 • イネーブル • Disabled [Admin State] がイネーブルの場合は、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。

名前	説明
[Port] フィールド	HTTPS 接続に使用するポート。 1～65535 の整数を入力します。デフォルトでは、HTTPS はポートでイネーブルになっています。
[Operational Port] フィールド	Cisco UCS Manager がシステム レベルの HTTPS 通信を行うために必要なポート。 このポートは変更できません。
[Key Ring] ドロップダウン リスト	HTTPS 接続のキー リング。
[Cipher Suite Mode] フィールド	Cisco UCS ドメインで使用される暗号スイート セキュリティのレベル。次のいずれかになります。 • High Strength • Medium Strength • Low Strength • [Custom]：ユーザ定義の暗号スイート仕様の文字列を指定できます。
[Cipher Suite] フィールド	[Cipher Suite Mode] フィールドで [Custom] を選択した場合は、このフィールドでユーザ定義の暗号スイート仕様の文字列を指定します。 暗号スイート仕様の文字列は最大256文字まで使用できますが、OpenSSL 暗号スイート仕様に準拠する必要があります。次を除き、スペースや特殊文字は使用できません。！（感嘆符）、+（プラス記号）、-（ハイフン）、および：（コロン）。詳細については、http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite を参照してください。 たとえば、Cisco UCS Manager がデフォルトとして使用する中強度仕様の文字列は次のようになります。 ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL

ステップ 6 [Save Changes] をクリックします。

キーリングの削除

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [Key Management] を展開します。
ステップ 3 削除するキー リングを右クリックし、[Delete] を選択します。
ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

トラスト ポイントの削除

はじめる前に

トラスト ポイントがキー リングによって使用されていないことを確認してください。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [Key Management] を展開します。
ステップ 3 削除するトラスト ポイントを右クリックし、[Delete] を選択します。
ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 5 [OK] をクリックします。

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 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通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：Cisco UCS 内のソフトウェア コンポーネントです。Cisco UCS のデータを維持し、必要に応じて SNMP マネージャにレポートします。Cisco UCS にはエージェントと MIB のコレクションが含まれます。SNMP エージェントをイネーブル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 をイネーブルにして設定します。
- Managed Information Base（MIB）：SNMP エージェントの管理対象オブジェクトの集合。Cisco UCS リリース 1.4(1) 以降では、それ以前のリリースより大量の 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応答します。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 モデルは、選択したセキュリティ レベルと結合され、SNMP メッセージの処理中に適用されるセキュリティ メカニズムを決定します。

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。

モデル	レベル	認証	暗号化	結果
v3	noAuthNoPriv	ユーザ名	なし	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	なし	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、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。SNMPv3 ユーザベース 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、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：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、B シリーズ サーバの場合は http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html を、C シリーズ サーバの場合は 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 ユーザの認証プロトコル

Cisco UCS は、SNMPv3 ユーザ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 プライバシー パスワードは最小で 8 文字です。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。

SNMP のイネーブル化および 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。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [Communication Management] > [Communication Services] 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] 領域で、次のフィールドに入力します。

名前	説明
[Admin State] フィールド	次のいずれかになります。 • イネーブル • Disabled 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。 [Admin State] がイネーブルの場合は、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。
[Port] フィールド	Cisco UCS Manager が SNMP ホストと通信するポート。デフォルト ポートは変更できません。
[Community/Username] フィールド	Cisco UCS Manager が SNMP ホストに送信するトラップ メッセージに含まれるデフォルトの SNMP v1 または v2c コミュニティ名あるいは SNMP v3 ユーザ名。 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）または空欄スペースは使用しないでください。デフォルトは public です。
[System Contact] フィールド	SNMP の実装を担当するシステムの連絡先。 電子メール アドレス、名前、電話番号など、255 文字までの文字列を入力します。
[System Location] フィールド	SNMP エージェント（サーバ）が実行するホストの場所。 最大 510 文字の英数字を入力します。

ステップ 5 [Save Changes] をクリックします。

次の作業

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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [Communication Management] > [Communication Services] 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
[Hostname]（または [IP Address]）フィールド	Cisco UCS Manager がトラップを送信する必要のある 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。ホスト名は 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。
[Community/Username] フィールド	Cisco UCS Manager がトラップを SNMP ホストに送信するときに含める SNMP v1/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）または空欄スペースは使用しないでください。
[Port] フィールド	Cisco UCS Manager がトラップの 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 ポートは 162 です。
[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

名前	説明
[Type] フィールド	送信するトラップのタイプ。次のいずれかになります。 • バージョンとして [V2c] または [V3] を選択した場合は [Traps]。 • バージョンとして [V2c] を選択した場合は [informs]。 （注） バージョンとして [v2c] を選択した場合にのみインフォーム通知を送信できます。
[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。 • [Auth]：認証あり、暗号化なし • [Noauth]：認証なし、暗号化なし • [Priv]：認証あり、暗号化あり

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 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [Communication Management] > [Communication Services] 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、[Yes] 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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [All] > [Communication Management] > [Communication Services] 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
[Name] フィールド	SNMP ユーザに割り当てられるユーザ名。 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。
[Auth Type] フィールド	許可タイプ。次のいずれかになります。 • MD5 • SHA
[Use AES-128] チェックボックス	オンにすると、このユーザに AES-128 暗号化が使用されます。
[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 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [Communication Management] > [Communication Services] 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、[Yes] をクリックします。
ステップ 7 [Save Changes] をクリックします。

Telnet のイネーブル化

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [Communication Management] > [Communication Services] を展開します。
ステップ 3 [Communication Services] タブをクリックします。
ステップ 4 [Telnet] 領域で、[Enabled] オプション ボタンをクリックします。
ステップ 5 [Save Changes] をクリックします。

CIMC Web サービスのイネーブル化

CIMC Web サービスはデフォルトでイネーブルとなっています。ディセーブルにしている場合は、次の手順を行ってサービスをイネーブルにします。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [Communication Management] > [Communication Services] 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 [CIMC Web Service] 領域で、[Enabled] オプション ボタンをクリックします。
ステップ 5 [Save Changes] をクリックします。

通信サービスのディセーブル化

（注） 他のネットワーク アプリケーションとのインターフェイスに必要ない通信サービスは、すべてディセーブルにすることを推奨します。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [All] > [Communication Management] > [Communication Services] を展開します。
ステップ 3 [Communication Services] タブで、ディセーブルにする各サービスの [disable] オプション ボタンをクリックします。
ステップ 4 [Save Changes] をクリックします。