認証

この章は、次の内容で構成されています。

- 認証，1 ページ
- LDAP プロバイダー，3 ページ
- UCS Central 認証の管理，5 ページ
- UCS Central LDAP 設定の管理，7 ページ
- ドメイン グループ認証の管理，7 ページ
- SNMP ポリシー，9 ページ

認証

Cisco UCS Central から、登録された UCS ドメインの認証用に LDAP、RADIUS、および TACACS+ を設定できます。

（注） リモート認証に使用できるのは、LDAP だけです。

リモート認証プロバイダーに関する注意事項および推奨事項

システムを、サポートされているリモート認証サービスのいずれかに設定する場合は、そのサービス用のプロバイダーを作成して、Cisco UCS Central がそのサービスと通信できるようにする必要があります。 また、ユーザ許可に影響する次のガイドラインに留意する必要があります。

リモート認証サービスのユーザ アカウント

ユーザ アカウントは、Cisco UCS Central にローカルに存在するか、またはリモート認証サーバに存在することができます。 リモート認証サービスを介してログインしているユーザの一時的なセッションは、Cisco UCS Central GUI または Cisco UCS Central CLI で表示できます。

リモート認証サービスのユーザ ロール

リモート認証サーバでユーザ アカウントを作成する場合は、ユーザが Cisco UCS Central で作業するために必要なロールをそれらのアカウントに含めること、およびそれらのロールの名前を Cisco UCS Central で使用される名前と一致させることが必要です。 ロール ポリシーによっては、ユーザがログインできない場合や読み取り専用権限しか付与されない場合があります。

ローカルおよびリモート ユーザ認証のサポート

Cisco UCS Central はリモート認証のために LDAP を使用しますが、このリリースでは RADIUS および TACACS+ 認証を除外します。 ただし、RADIUS、TACACS+、および LDAP 認証は、ローカルに管理される Cisco UCS ドメイン でサポートされています。

リモート認証プロバイダーのユーザ属性

ユーザがログインすると、Cisco UCS Central は次を実行します。

1. リモート認証サービスに問い合わせます。
2. ユーザを検証します。
3. ユーザが検証されると、そのユーザに割り当てられているロールとロケールをチェックします。

次の表に、Cisco UCS Central によってサポートされるリモート認証プロバイダーのユーザ属性要件の比較を示します。

表 *1*：リモート認証プロバイダーによるユーザ属性の比較

認証プロバイダー	カスタム属性	スキーマの拡張	属性 ID 要件
LDAP	任意	オプション。 次のいずれかを選択して実行できます。 • LDAP スキーマを拡張せず、要件を満たす既存の未使用の属性を設定します。 • LDAP スキーマを拡張して、CiscoAVPair などの一意の名前でカスタム属性を作成します。	シスコの LDAP の実装では、Unicode タイプの属性が必要です。 CiscoAVPair カスタム属性を作成する場合は、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します 次の項で、サンプル OID を示します。

LDAP ユーザ属性のサンプル OID

カスタム CiscoAVPair 属性のサンプル OID は、次のとおりです。

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

LDAP プロバイダー

Cisco UCS Manager から LDAP ユーザを作成するのと同じ方法で、リモート ユーザを設定して、Cisco UCS Central からロールとロケールを割り当てることができます。 必ず、Cisco UCS Central Domain Group ルートから LDAP プロバイダーを作成する必要があります。

LDAP プロバイダー グループ マップ

最大 28 の LDAP プロバイダー グループ マップを定義して、Active Directory で Cisco UCS Central 内のネスティングがサポートされるレベルまでそれらのマップをネストすることができます。 プロバイダーをネスト グループに割り当てると、そのプロバイダーが別の LDAP グループのメン

バーであっても、親ネスト グループの認証メンバーになります。 認証中、プロバイダー グループ内のすべてのプロバイダーが順番に試行されます。 設定されたすべての LDAP サーバが使用または到達できない場合は、Cisco UCS Central が自動的にローカル ユーザ名とパスワードを使用するローカル認証方式にフォールバックします。

LDAP グループ マップ

すでに LDAP グループを使用して LDAP データベースへのアクセスを制限している組織では、Cisco UCS ドメインでグループ メンバーシップ情報を使用することによって、ログイン中の LDAP ユーザにロールまたはロケールを割り当てることができます。 これにより、Cisco UCS Central の展開時に LDAP ユーザ オブジェクトでロールまたはロケール情報を定義する必要がなくなります。

Cisco UCS Central は、ユーザ ロールとロケールをリモート ユーザに割り当てるときに LDAP グループ ルールを使用して LDAP グループを決定します。 ユーザがログインすると、Cisco UCS Central が LDAP グループ マップからそのユーザのロールとロケールに関する情報を取得します。ロールとロケールの条件がポリシー内の情報と一致すると、Cisco UCS Central がアクセス権をユーザに付与します。

ロールとロケールの定義は Cisco UCS Central でローカルに設定され、LDAP ディレクトリに対する変更に基づいて自動的には更新されません。 LDAP ディレクトリ内の LDAP グループを削除または名前を変更した場合は、Cisco UCS Central でその変更を更新してください。

LDAP グループ マップは、次のロールとロケールの組み合わせのいずれかを含むように設定できます。

- ロールのみ
- ロケールのみ
- ロールとロケール

例：特定の場所にいるサーバ管理者のグループを表す LDAP グループに対する認証を設定する場合は、server-profile や server-equipment などのユーザ ロールをその LDAP グループに含めることができます。 特定の場所にいるサーバ管理者にアクセスを制限する場合は、特定のサイト名を含むロケールを指定できます。

（注） Cisco UCS Central には、すぐに使用可能なユーザ ロールが複数付属していますが、ロケールは付属していません。 そのため、LDAP プロバイダー グループをロケールにマッピングするカスタム ロケールを作成する必要があります。

ネストされた LDAP グループ

LDAP グループ マップで定義された別のグループ内でネストされた LDAP グループを検索できます。 この機能を使用する場合は、Cisco UCS Central でグループ マップ内にサブグループを作成する必要がありません。

（注） ネストされた LDAP の検索サポートは Microsoft Active Directory サーバに対してのみサポートされます。 サポートされているバージョンは Microsoft Windows 2003 SP3、Microsoft Windows 2008 R2、および Microsoft Windows 2012 です。

（注） MS-AD 内でネストされた LDAP グループを作成するときに、名前に特殊文字を使用する場合は、必ず、\\(と \\) を使用して文字を設定してください。 Cisco UCS Central CLI を使用して、ネストされた LDAP グループを作成する例を以下に示します。

create ldap-group CN=test1\\(\\),CN=Users,DC=ucsm,DC=qasam-lab,DC=in

LDAP ネスティング機能を使用して、LDAP グループを他のグループおよびネスト グループのメンバとして追加し、メンバ アカウントを統合してトラフィックの重複を減らすことができます。

LDAP グループが別のグループ内でネストされている場合は、デフォルトで、ユーザの権限が継承されます。 たとえば、Group_2 のメンバとして Group_1 を作成する場合、Group_1 のユーザは Group_2 のメンバと同じ権限が与えられます。 その結果、Group_1 のメンバになっているユーザを検索する場合は、Group_1 と Group_2 を別々に検索しなくても、LDAP グループ マップ内の Group_2 を選択するだけで済みます。

UCS Central 認証の管理

Cisco UCS Central は、ネイティブ認証に LDAP を使用しますが、RADIUS 認証と TACACS+ 認証は除きます。 ただし、Cisco UCS Central ドメイン グループ ルートからの RADIUS、TACACS+、または LDAP リモート認証が Cisco UCS ドメインに対してサポートされます。

認証ドメインを作成したら、必要に応じて、認証情報を編集できます。

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[Authentication] を選択します。
これにより、[Manage Cisco UCS Central Authentication] ダイアログボックスが開きます。

ステップ 2 [LDAP] で、[Basic]、[Providers]、[Groups]、および [Group Maps] タブの該当するフィールドに値を入力します。

ステップ 3 [Authentication Domains] で、次の手順を実行します。

ステップ 4 [Native(Default)] をクリックして、次の情報を入力します。

a) [Default Behavior for Remote Users] を選択します。

b) [Web Session Refresh Period(Seconds)] と [Web Session Timeout(Seconds)] の値を入力します。
c) [Authentication] を [Enabled] にするか、[Disabled] にするかを選択します。
d) [Enabled] を選択した場合は、[Authentication Realm] を [Local] にするか、[LDAP] にするかを選択します。
e) [LDAP] を選択した場合は、[Provider Group] を選択します。

ステップ 5 [Console(Default)] をクリックして、次の情報を入力します。

a) [Authentication] を [Enabled] にするか、[Disabled] にするかを選択します。
b) [Enabled] を選択した場合は、[Authentication Realm] を [Local] にするか、[LDAP] にするかを選択します。
c) [LDAP] を選択した場合は、[Provider Group] を選択します。

ステップ 6 [Add] をクリックして、新しい認証ドメインを作成します。

a) 認証ドメインの名前を入力します。
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）以外の特殊文字またはスペースを使用できません。

優先認証プロトコルとして RADIUS を使用しているシステムでは、認証ドメイン名がユーザ名の一部と見なされ、ローカルに作成されたユーザ名の 32 文字の制限が考慮されます。 Cisco UCS では書式設定用として 5 文字が予約されているため、ドメイン名とユーザー名で 27 文字を超えることができません。

b) [Web Session Refresh Period(Seconds)] に、選択した Cisco UCS Central ドメイン グループに含まれる Cisco UCS ドメインにアクセスしているユーザの更新要求間の最大許容時間を入力します。
この時間制限を超えると、Cisco UCS Central は Web セッションを非アクティブと見なしますが、そのセッションを終了することはありません。

60 ～ 172800 を指定します。 デフォルトは 600 秒です。

c) [Web Session Timeout(Seconds)] に、最後の更新要求後から CiscoCisco UCS Central で Web セッションが終了したと見なされるまでの最大経過時間を入力します。 この時間制限を超えると、Cisco UCS Central は自動的に Web セッションを終了します。
60 ～ 172800 を指定します。 デフォルトは 7200 秒です。

d) ドメイン内のユーザに適用される [Authentication Realm] を選択します。 次のいずれかになります。

- [LDAP]：ユーザを Cisco UCS Central で指定された LDAP サーバ上で定義する必要があります。
- [Local]：ユーザ アカウントを Cisco UCS Central または Cisco UCS ドメイン内でローカルに定義する必要があります。

e) [Realm] が LDAP に設定されている場合は、[Provider Group] ドロップダウン リストから関連するプロバイダー グループを選択できます。

ステップ 7 [Save（保存）] をクリックします。

UCS Central LDAP 設定の管理

ステップ 1 タスク バーで、「Create Domain Group」と入力して、Enter キーを押します。
これにより、[Create Domain Group] ダイアログボックスが開きます。

ステップ 2 [LDAP] で、必要に応じて次のセクションに値を入力します。

a) [Basic] タブで、[Database Conection Timeout]、[Filter]、[Attribute]、および [Base DN] の値を入力します。

b) [Providers] タブで、[Add] をクリックして、プロバイダーを追加し、[Basic] タブと [Group Rules] タブで必要な情報を入力します。

c) [Groups] タブで、[Add] をクリックして、プロバイダー グループを追加し、オプションで、それをプロバイダーに関連付けます。

d) [Group Maps] タブで、[Provider Group Map DN] を追加してから、オプションで、[Roles] と [Locales] を追加します。

ステップ 3 [Authentication Domains] で、新しいドメインを追加して、その値を更新します。

ステップ 4 [Save] をクリックします。

ドメイン グループ認証の管理

ステップ 1 タスク バーで、「Manage Domain Group Authentication」と入力して、Enter キーを押します。
これにより、[Manage Domain Group Authentication] ダイアログボックスが開きます。

ステップ 2 [LDAP] で、必要に応じて次のセクションに値を入力します。

a) [Basic] タブで、[Database Conection Timeout]、[Filter]、[Attribute]、および [Base DN] の値を入力します。

b) [Providers] タブで、[Add] をクリックして、プロバイダーを追加し、[Basic] タブと [Group Rules] タブで必要な情報を入力します。

c) [Groups] タブで、[Add] をクリックして、プロバイダー グループを追加し、オプションで、それをプロバイダーに関連付けます。

d) [Group Maps] タブで、[Provider Group Map DN] を追加してから、オプションで、[Roles] と [Locales] を追加します。

ステップ 3 [TACACS+] で、必要に応じて次のセクションに値を入力します。

a) [Basic] タブで、[Database Conection Timeout] と [Retry Count] の値を入力します。

b) [Providers] タブで、[Add] をクリックして、プロバイダーを追加し、必要な設定情報を入力します。
上矢印と下矢印を使用して、プロバイダーの順序を変更できます。

c) [Groups] タブで、[Add] をクリックして、プロバイダー グループを追加し、オプションで、それをプロバイダーに関連付けます。

ステップ 4 [RADIUS] で、必要に応じて次のセクションに値を入力します。

a) [Basic] タブで、[Database Conection Timeout] と [Retry Count] の値を入力します。

b) [Providers] タブで、[Add] をクリックして、プロバイダーを追加し、必要な設定情報を入力します。
上矢印と下矢印を使用して、プロバイダーの順序を変更できます。

c) [Groups] タブで、[Add] をクリックして、プロバイダー グループを追加し、オプションで、それをプロバイダーに関連付けます。

ステップ 5 [Authentication Domains] で、必要に応じて次のセクションに値を入力します。

a) [Add] をクリックして、親グループから継承された設定をオーバーライドする、選択したユーザ作成ドメイン グループの認証ポリシーを作成します。

b) 認証ドメインの名前を入力します。
この名前には、1 ～ 16 文字の英数字を使用できます。 優先する認証プロトコルとして RADIUS を使用するシステムの場合、認証ドメイン名はユーザ名の一部と見なされ、ローカルに作成されたユーザ名の 32 文字の制限に対して考慮されます。 Cisco UCS はフォーマット用に 5 文字を挿入するため、認証はユーザ名とドメイン名を組み合わせた合計が 27 文字を超えると失敗します。

c) [Web Session Refresh Period(Seconds)] に、選択した Cisco UCS Central ドメイン グループに含まれる Cisco UCS ドメインにアクセスしているユーザの更新要求間の最大許容時間を入力します。
この時間制限を超えると、Cisco UCS Manager は Web セッションを非アクティブと見なしますが、そのセッションを終了することはありません。

60 ～ 172800 の整数を指定します。 デフォルトは 600 秒です。

d) [Web Session Timeout(Seconds)] に、最後の更新要求後から Cisco UCS Manager で Web セッションが終了したと見なされるまでの最大経過時間を入力します。 この時間制限を超えると、Cisco UCS Manager は自動的に Web セッションを終了します。
60 ～ 172800 の整数を指定します。 デフォルトは 7200 秒です。

e) ドメイン内のユーザに適用される [Authentication Realm] を選択します。
次のいずれかになります。

- [LDAP]：ユーザを Cisco UCS Central で指定された LDAP サーバ上で定義する必要があります。
- [Local]：ユーザ アカウントを Cisco UCS Central または Cisco UCS ドメイン内でローカルに定義する必要があります。
- [RADIUS]：ユーザを Cisco UCS Central で指定された RADIUS サーバ上で定義する必要があります。
- [TACACS+]：ユーザを Cisco UCS Central で指定された TACACS+ サーバ上で定義する必要があります。

ステップ 6 [Save（保存）] をクリックします。

SNMP ポリシー

Cisco UCS Central は、SNMP トラップと SNMP ユーザの定義（通常のパスワードとプライバシーパスワード、md5 または sha の認証タイプ、および暗号化タイプの DES と AES-128 を使用）を有効または無効にするグローバル SNMP ポリシーをサポートします。 登録済み Cisco UCS ドメインでは、そのクライアントのポリシー解決コントロール内で SNMP ポリシーをグローバルに定義するようにしている場合、すべての SNMP ポリシーについて Cisco UCS Central への登録に従うことになります。

SNMP エージェント機能は、Cisco UCS Central をリモートで監視できる能力を提供します。 また、Cisco UCS Central のホスト IP を変更してから、新しい IP 上で SNMP エージェントを再起動することもできます。 SNMP は、アクティブとスタンバイの両方の Cisco UCS Central サーバ上で動作し、その両方で設定が保持されます。 Cisco UCS Central は、オペレーティング システム管理情報ベース（MIB）のみへの読み取り専用アクセスを提供します。Cisco UCS Central CLI 経由で、SNMP v1、v2c 用のコミュニティ ストリングを設定したり、SNMPv3 ユーザを作成または削除したりできます。

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：管理対象デバイスである Cisco UCS Central 内部のソフトウェア コンポーネントで、Cisco UCS Central に関するデータを保持し、必要に応じてそのデータを SNMP に報告します。 Cisco UCS Central には、エージェントと、MIB のコレクションが組み込まれています。 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構築するには、Cisco UCS Central で SNMP を有効にして設定します。
- 管理情報ベース（MIB）：SNMP エージェント上の管理対象オブジェクトのコレクション。 Cisco UCS Central は、OS MIB のみをサポートします。

Cisco UCS Central 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。 次の RFC で SNMP が規定されています。

- 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 Central は、SNMP 通知をトラップとして生成します。 SNMP マネージャはトラップの受信時に確認応答を送信せず、Cisco UCS Central はトラップが受信されたかどうかを確認できないため、トラップは信頼できません。

SNMP 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を保証します。また、データ シーケンスが、通常発生するものよりも高い頻度で変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- 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、またはプロセスからの情報の利用や開示を行えないようにします。

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。 権限レベルは、メッセージが開示されないよう保護または認証の必要があるかどうかを決定します。 サポートされるセキュリティ レベルは、セキュリティ モデルが設定されているか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 モデルおよびセキュリティ レベル

次の表に、Cisco UCS Central でサポートされる SNMP 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を示します。

表 *2*： ***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	No	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	No	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	No	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	No	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。

モデル	レベル	認証	暗号化	結果
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。

Cisco UCS Central での SNMP サポート

MIB のサポート

Cisco UCS Central は、OS MIB への読み取り専用アクセスをサポートします。 MIB に対する設定操作は使用できません。 次の MIB が Cisco UCS Central でサポートされます。

- SNMP MIB-2 システム
- HOST-RESOURCES-MIB
  - hrSystem
  - hrStorage
  - hrDevice
  - hrSWRun
  - hrSWRunPerf
- UCD-SNMP-MIB
  - メモリ
  - dskTable
  - systemStats
  - fileTable
- SNMP MIB-2 インターフェイス
  - ifTable
- IP-MIB

- SNMP-FRAMEWORK-MIB
  - snmpEngine
- IF-MIB
- DISMAN-EVENT-MIB
- SNMP MIB-2 snmp

（注） Cisco UCS Central は、IPV6 と Cisco UCS Central MIB に対するサポートを提供しません、

関連トピック

SNMP のイネーブル化, （13 ページ）
SNMP ユーザの作成と編集, （14 ページ）
SNMP トラップの作成と編集, （14 ページ）

SNMP のイネーブル化

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[SNMP] を選択します。

- タスク バーで「Manage UCS Central SNMP」と入力して Enter キーを押すことによって、SNMP を選択できます。

これにより、[Manage UCS Central SNMP] ダイアログボックスが開きます。

ステップ 2 [Basic] で、次のフィールドに値を入力します。

ステップ 3 [Community/User Name] に、デフォルトの SNMP v1 または v2c コミュニティ名または SNMPv3 ユーザ名を入力します。

ステップ 4 [System Contact] に、SNMP 実装のシステム担当者を入力します。
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。

ステップ 5 [System Location] に、SNMP エージェント（サーバ）が動作するホストの場所を入力します。
最大 510 文字の英数字文字列を入力します。

ステップ 6 [Save（保存）] 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 トラップの作成と編集

SNMP トラップを作成したら、必要に応じて、SNMP トラップ情報を編集できます。

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[SNMP] を選択します。
これにより、[Manage UCS Central SNMP] ダイアログボックスが開きます。

ステップ 2 [Trap Host Name/IP Address] で、トラップを受信する SNMP ホストの IP アドレスを入力します。

ステップ 3 [SNMP Trap Properties] 領域で、次の手順を実行します。

ステップ 4 [Community/User Name] に、システムがトラップを SNMP ホストに送信するときに追加される SNMP v1 または v2c コミュニティ名、あるいは、SNMPv3 ユーザ名を入力します。 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。

ステップ 5 [Port] に、システムがトラップ用に SNMP ホストと通信するポートを入力します。
1 ～ 65535 の整数を入力します。 デフォルト ポートは 162 です。

ステップ 6 [V1]、[V2C]、または [V3] をクリックして、SNMP のバージョンを選択します。

ステップ 7 [Trap] をクリックして、SNMP トラップの [Type] を選択します。

ステップ 8 [V3Privilege] を定義するために、次のいずれかを選択します。

ステップ 9 [Save（保存）] をクリックします。

- [auth]：認証されますが、暗号化されません
- [Noauth]：認証または暗号化なし
- [Priv]：認証あり、暗号化あり

次の作業

SNMP ユーザを作成する。

SNMP ユーザの作成と編集

SNMP ユーザを作成したら、必要に応じて、SNMP ユーザ情報を編集できます。

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[SNMP] を選択します。
これにより、[Manage UCS Central SNMP] ダイアログボックスが開きます。

ステップ 2 [Manage UCS Central SNMP] ページで、[SNMP User] をクリックします。

ステップ 3 プラス記号をクリックして、SNMP ユーザを作成します。

ステップ 4 SNMP ユーザに割り当てるユーザ名を入力します。
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）、および -（ハイフン）も指定できます。

ステップ 5 [SNMP User Properties] で、次の手順を実行します。

ステップ 6 [Authentication Type] で、認証タイプを選択します。 次のいずれかになります。

- MDS
- SHA

ステップ 7 [AES-128 Encryption] を有効にします。 有効にした場合は、このユーザが AES-128 暗号化を使用します。

ステップ 8 ユーザのパスワードを入力します。

ステップ 9 このユーザのプライバシー パスワードを入力します。

ステップ 10 [Save（保存）] をクリックします。