Cisco UCS Central リリース 1.5 認証ガイド

初版：2016 年 07 月 29 日

最終更新：2016 年 08 月 11 日

最終更新：2017 年 04 月 05 日

最終更新：2017 年 04 月 17 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

対象読者

このガイドは、次の 1 つ以上に責任を持つ、専門知識を備えたデータセンター管理者を主な対象にしています。

- サーバ管理
- ストレージ管理
- ネットワーク管理
- ネットワーク セキュリティ

表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールドラベルなどのGUI要素は、イタリック体（italic）で示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[Main titles] のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*italic*）で示しています。

テキストのタイプ	説明
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、courier フォントで示しています。
システム出力	システムが表示するターミナル セッションおよび情報は、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、ボールド体（**this font**）で示しています。 CLI コマンド内の変数は、イタリック体（*italic*）で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒント 「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

ワンポイント アドバイス 「時間の節約に役立つ操作」です。ここに紹介している方法で作業を行うと、時間を短縮できます。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

Cisco UCS の関連ドキュメント

ドキュメント ロードマップ

すべての B シリーズ マニュアルの完全なリストについては、http://www.cisco.com/go/unifiedcomputing/b-series-doc で入手可能な『*Cisco UCS B-Series Servers Documentation Roadmap*』を参照してください。

すべての C シリーズ マニュアルの一覧については、http://www.cisco.com/go/unifiedcomputing/c-series-doc で入手できる『*Cisco UCS C-Series Servers Documentation Roadmap*』を参照してください。

管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、『Release Bundle Contents for Cisco UCS Software』を参照してください。

その他のマニュアル リソース

ドキュメントの更新通知を受け取るには、Cisco UCS Docs on Twitter をフォローしてください。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、ucs-docfeedback@cisco.com までご連絡ください。ご協力をよろしくお願いいたします。

第 1 章

概要

概要

Cisco UCS Central 認証ガイドでは、リモートまたはローカルで認証されたユーザ アカウントの管理と保守に関連したガイドラインとタスクについて説明します。

Cisco UCS Central ユーザ マニュアルのリファレンス

Cisco UCS Central を理解および設定するには、Cisco UCS Central の使用例ベースのドキュメントに従います。

ガイド	説明
Cisco UCS Central Getting Started Guide	Cisco UCS インフラストラクチャ、Cisco UCS Manager、および Cisco UCS Central について簡単に説明します。HTML5 UI の概要、Cisco UCS Central に Cisco UCS ドメインを登録する方法、およびライセンスをアクティブにする方法を説明します。
Cisco UCS Central Administration Guide	ユーザ管理、通信、ファームウェア管理、バックアップ管理、Smart Call Home などの管理タスクについて説明します。
Cisco UCS Central Authentication Guide	パスワード、ユーザ、ロール、RBAC、TACACS+、RADIUS、LDAP、SNMP などの認証タスクについて説明します。

ガイド	説明
Cisco UCS Central Server Management Guide	機器ポリシー、物理インベントリ、サービス プロファイルとテンプレート、サーバ プール、サーバのブート、サーバ ポリシーなどのサーバ管理について説明します。
Cisco UCS Central Storage Management Guide	ポートとポート チャネル、VSAN と vHBA の管理、ストレージ プール、ストレージ ポリシー、ストレージ プロファイル、ディスク グループ、ディスク グループ設定などのストレージ管理について説明します。
Cisco UCS Central Network Management Guide	ポートとポート チャネル、VLAN と vNIC の管理、ネットワーク プール、ネットワーク ポリシーなどのネットワーク管理について説明します。
Cisco UCS Central Operations Guide	小規模、中規模、および大規模な展開でのドメイン グループのセットアップ、設定、管理に関するベスト プラクティス。
Cisco UCS Central Troubleshooting Guide	Cisco UCS Central で共通する問題に関するヘルプを提供します。

第 2 章

ユーザとロール

ロールベース アクセス コントロールの概要

ロールベース アクセス コントロール（RBAC）は、ユーザのロールとロケールに基づいてユーザのシステム アクセスを制限または許可する方法です。ロールによってシステム内でのユーザの権限が定義され、ロケールによってユーザがアクセス可能な組織（ドメイン）が定義されます。権限がユーザに直接割り当てられることはないため、適切なロールとロケールを割り当てることによって個々のユーザ権限を管理できます。

必要なシステム リソースへの書き込みアクセス権限がユーザに与えられるのは、割り当てられたロールによりアクセス権限が与えられ、割り当てられたロケールによりアクセスが許可されている場合に限ります。たとえば、エンジニアリング組織の管理者ロールを与えられたユーザは、エンジニアリング組織のサーバ設定を更新できます。ただし、そのユーザに割り当てられたロケールに財務部門が含まれている場合を除いて、財務部門内のサーバ設定を更新することはできません。

Cisco UCS Central ユーザ アカウント

システムにはユーザ アカウントを使ってアクセスします。各 Cisco UCS Central ドメインで最大 128 のユーザ アカウントを設定できます。各ユーザ アカウントには、一意のユーザ名とパスワードが必要です。

OpenSSH または SECSH のいずれかの形式の SSH 公開キーで、ユーザ アカウントを設定できます。

管理者アカウント

Cisco UCS Central 管理者アカウントはデフォルトのユーザ アカウントです。変更または削除することはできません。このアカウントは、システム管理者つまりスーパーユーザ アカウントであり、すべての権限が与えられています。管理者アカウントにはデフォルトのパスワードは割り当てられていません。システムの初期設定時にパスワードを選択する必要があります。

管理者アカウントは常にアクティブで、有効期限がありません。管理者アカウントを非アクティブに設定することはできません。

ローカルの管理者ユーザは、認証がリモートに設定されている場合でも、フェールオーバーのためにログインできます。

ローカル認証されたユーザ アカウント

ローカル認証されたユーザ アカウントは、Cisco UCS Central ユーザ データベースを介して認証されます。管理者または aaa 権限を持つユーザであれば、誰でもそれを有効または無効にすることができます。ローカルユーザアカウントを無効にすると、そのユーザはログインできなくなります。

（注） Cisco UCS Central では、ローカル ユーザ アカウントを無効にしても、その設定の詳細がデータベースから削除されることがありません。無効ローカル ユーザ アカウントを再度有効にすると、アカウントはユーザ名とパスワードを含め、既存のコンフィギュレーションで再びアクティブになります。

リモート認証されたユーザ アカウント

リモート認証されたユーザ アカウントは、LDAP を介して認証される Cisco UCS Central ユーザ アカウントです。Cisco UCS ドメイン は、LDAP、RADIUS および TACACS+ をサポートしています。

ユーザがローカル ユーザ アカウントとリモート ユーザ アカウントを同時に保持する場合、ローカル ユーザ アカウントで定義されたロールがリモート ユーザ アカウントに保持された値を上書きします。

ユーザ アカウントの有効期限

ユーザアカウントは、事前に定義した時間に有効期限が切れるように設定できます。ユーザアカウントの有効期限が来ると、そのアカウントは無効になります。

デフォルトでは、ユーザ アカウントの有効期限はありません。

（注） ユーザ アカウントに有効期限日付を設定した後は、アカウントの有効期限をなくすよう再設定できません。ただし、アカウントの有効期限を可能な限り最も遅い日付に設定することは可能です。

ユーザ名の作成に関するガイドライン

ユーザ名は、Cisco UCS Central のログイン ID としても使用されます。Cisco UCS Central ユーザ アカウントにログイン ID を割り当てるときは、次のガイドラインおよび制約事項を考慮してください。

- ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。
  - 任意の英字
  - 任意の数字
  - _（アンダースコア）
  - -（ダッシュ）
  - .（ドット）
- ログイン ID は、Cisco UCS Central 内で一意である必要があります。
- ログイン ID は、英文字で開始する必要があります。数字やアンダースコアなどの特殊文字からは開始できません。
- ログイン ID では、大文字と小文字が区別されます。
- すべて数字のログイン ID は作成できません。
- ユーザ アカウントの作成後は、ログイン ID を変更できません。ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

予約語：ローカル認証されたユーザ アカウント

次の語は Cisco UCS でローカル ユーザ アカウントを作成するときに使用できません。

- root
- bin
- daemon

- adm
- lp
- sync
- shutdown
- halt
- news
- uucp
- operator
- games
- gopher
- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- ftp
- man
- sys
- samdme
- debug

ユーザ ロール

ユーザ ロールには、ユーザに許可される操作を定義する 1 つ以上の権限が含まれます。ユーザごとに 1 つ以上のロールを割り当てることができます。複数のロールを持つユーザは、割り当てられたすべてのロールを組み合わせた権限を持ちます。たとえば、Role1 にストレージ関連の権限が含まれ、Role2 にサーバ関連の権限が含まれている場合、Role1 と Role2 の両方を持つユーザは、ストレージ関連の権限とサーバ関連の権限を持つことになります。

Cisco UCS ドメインは、デフォルトのユーザ ロールを含めて、最大 48 個のユーザ ロールを持つことができます。最初の 48 のユーザ ロールが許可された後に設定されたユーザ ロールは、障害が発生して無効になります。Cisco UCS Central の各ドメイン グループも、親ドメイン グループから継承されたユーザ ロールを含めて、48 個のユーザ ロールを持つことができます。Cisco UCS Central から Cisco UCS Manager にユーザ ロールがプッシュされると、最初の 48 個のロールだけ

がアクティブになります。最初の 48 個より後のユーザ ロールは、非アクティブなために、障害が発生します。

すべてのロールには、Cisco UCS ドメイン内のすべての設定に対する読み取りアクセス権限が含まれています。読み取り専用ロールを持つユーザは、システム状態を変更できません。

権限を作成したり、既存の権限を変更または削除したり、ロールを削除したりできます。ロールを変更すると、そのロールを持つすべてのユーザに新しい権限が適用されます。権限の割り当ては、デフォルト ロールに定義されている権限に限定されません。つまり、権限を自由に組み合わせて独自のロールを作成できます。たとえば、デフォルトのサーバ管理者ロールとストレージ管理者ロールには、異なる組み合わせの権限が付与されています。しかし、両方のロールの権限を持つサーバおよびストレージ管理者ロールを作成することができます。

（注） ロールをユーザに割り当てた後で削除すると、そのロールはそれらのユーザ アカウントからも削除されます。

AAA サーバ（RADIUS または TACACS+）上のユーザ プロファイルを、そのユーザに付与される権限に対応したロールを追加するように変更します。属性にロール情報が保存されます。AAA サーバでは、要求とともにこの属性が返され、それを解析することでロールが得られます。LDAP サーバでは、ユーザ プロファイル属性内のロールが返されます。

デフォルト ユーザ ロール

システムには、次のデフォルトのユーザ ロールが用意されています。

AAA アドミニストレータ

ユーザ、ロール、および AAA 設定に対する読み取りと書き込みのアクセス権。その他のシステムに対する読み取りアクセス。

アドミニストレータ

システム全体に対する完全な読み取りと書き込みのアクセス権。このロールは、デフォルトで管理者アカウントに割り当てられます。変更することはできません。

ファシリティ マネージャ

power management 権限による、電源管理操作に対する読み取りと書き込みのアクセス。その他のシステムに対する読み取りアクセス。

ネットワーク管理者

ファブリック インターコネクト インフラストラクチャとネットワーク セキュリティ操作に対する読み取りと書き込みのアクセス権。その他のシステムに対する読み取りアクセス。

オペレーション

システムのログ（syslogサーバを含む）と障害に対する読み取りと書き込みのアクセス権。その他のシステムに対する読み取りアクセス。

Read-Only

システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。

サーバ計算

サービス プロファイルのほとんどの側面に対する読み取りと書き込みのアクセス権。ただし、ユーザは vNIC または vHBA を作成、変更、または削除できません。

サーバ機器アドミニストレータ

物理サーバ関連の操作に対する読み取りと書き込みのアクセス。その他のシステムに対する読み取りアクセス。

サーバ プロファイル アドミニストレータ

論理サーバ関連の操作に対する読み取りと書き込みのアクセス。その他のシステムに対する読み取りアクセス。

サーバ セキュリティ アドミニストレータ

サーバ セキュリティ関連の操作に対する読み取りと書き込みのアクセス。その他のシステムに対する読み取りアクセス。

ストレージ アドミニストレータ

ストレージ操作に対する読み取りと書き込みのアクセス権。その他のシステムに対する読み取りアクセス。

予約語：ユーザ ロール

Cisco UCS でカスタム ロールを作成するときは次の語を使用できません。

- network-admin
- network-operator
- vdc-admin
- vdc-operator
- server-admin

権限

ユーザ ロールを割り当てられたユーザは、権限により、特定のシステム リソースへアクセスしたり、特定のタスクを実行したりできるようになります。次の表に、各権限と、その権限がデフォルトで与えられるユーザ ロールのリストを示します。

ヒント　これらの権限および権限によってユーザが実行できるようになるタスクの詳細情報は、『*Privileges in Cisco UCS*』は、次の URL で入手可能です。 http://www.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html で利用可能です。

表 *1*：システム定義ロール

ロール	権限	LDAP/RADIUS/TACACS サーバに設定するロール
AAA アドミニストレータ	aaa	aaa
管理者	admin	admin
ファシリティ マネージャ	facility-manager	power-mgmt
KVM 管理者	kvm	kvm
ネットワーク	pod-qos,pod-config,pod-policy,ext-lan-qos,pod-security,	network
オペレーション	fault, operations	fault, operations
Read-Only	read-only	read-only
サーバ計算アドミニストレータ		server-compute
サーバ機器アドミニストレータ	server-policy,server-equipment,server-maintenance	server-equipment
サーバ プロファイル アドミニストレータ		server-profile
サーバ セキュリティ アドミニストレータ		server-security
統計情報の管理者	stats	stats-management

ロール	権限	LDAP/RADIUS/TACACS サーバに設定するロール
ストレージアドミニストレータ	[illegible]	storage

表 *2* : ユーザの権限

特権	説明	デフォルトのロール割り当て
aaa	システム セキュリティおよび AAA	AAA アドミニストレータ
admin	システム管理	アドミニストレータ
domain-group-management	ドメイン グループ管理	ドメイン グループ管理者
ext-lan-config	外部 LAN 設定	ネットワーク管理者
ext-lan-policy	外部 LAN ポリシー	ネットワーク管理者
ext-lan-qos	外部 LAN QoS	ネットワーク管理者
ext-lan-security	外部 LAN セキュリティ	ネットワーク管理者
ext-san-config	外部 SAN 設定	ストレージアドミニストレータ
ext-san-policy	外部 SAN ポリシー	ストレージアドミニストレータ
ext-san-qos	外部 SAN QoS	ストレージアドミニストレータ
ext-san-security	外部 SAN セキュリティ	ストレージアドミニストレータ
fault	アラームおよびアラーム ポリシー	オペレーション
kvm	KVM の起動	オペレーション
operations	ログおよび Smart Call Home	オペレーション
org-management	組織管理	オペレーション
pod-config	ポッド設定	ネットワーク管理者
pod-policy	ポッド ポリシー	ネットワーク管理者

特権	説明	デフォルトのロール割り当て
pod-qos	ポッド QoS	ネットワーク管理者
pod-security	ポッド セキュリティ	ネットワーク管理者
power-mgmt	電源管理操作に対する読み取りと書き込みのアクセス	ファシリティ マネージャ
read-only	読み取り専用アクセス権 読み取り専用は、権限として選択できません。この権限は、すべてのユーザ ロールに割り当てられます。	Read-Only
server-equipment	サーバ ハードウェア管理	サーバ機器アドミニストレータ
server-maintenance	サーバ メンテナンス	サーバ機器アドミニストレータ
server-policy	サーバ ポリシー	サーバ機器アドミニストレータ
server-security	サーバ セキュリティ	サーバセキュリティアドミニストレータ
service-profile-compute	サービス プロファイルの計算	サーバ計算アドミニストレータ
service-profile-config	サービス プロファイル設定	サーバプロファイルアドミニストレータ
service-profile-config-policy	サービスプロファイル設定ポリシー	サーバプロファイルアドミニストレータ
service-profile-ext-access	サービス プロファイル エンドポイント アクセス	サーバプロファイルアドミニストレータ
service-profile-network	サービス プロファイル ネットワーク	ネットワーク管理者
service-profile-network-policy	サービス プロファイル ネットワーク ポリシー	ネットワーク管理者
service-profile-qos	サービス プロファイル QoS	ネットワーク管理者
service-profile-qos-policy	サービス プロファイル QoS ポリシー	ネットワーク管理者

特権	説明	デフォルトのロール割り当て
service-profile-security	サービス プロファイル セキュリティ	サーバセキュリティアドミニストレータ
service-profile-security-policy	サービス プロファイル セキュリティ ポリシー	サーバセキュリティアドミニストレータ
service-profile-server	サービス プロファイル サーバ管理	サーバプロファイルアドミニストレータ
service-profile-server-oper	サービス プロファイル コンシューマ	サーバプロファイルアドミニストレータ
service-profile-server-policy	サービス プロファイル プール ポリシー	サーバセキュリティアドミニストレータ
service-profile-storage	サービスプロファイルストレージ	ストレージアドミニストレータ
service-profile-storage-policy	サービスプロファイルストレージ ポリシー	ストレージアドミニストレータ
stats	統計情報管理	統計情報の管理者

UCS Central ロールの管理

手順

ステップ 1 アクション バーで、「Manage UCS Central Roles」と入力して、Enter キーを押します。
これにより、[UCS Central Roles Manage] ダイアログボックスが開きます。

ステップ 2 [Roles] で、[Add] をクリックして新しいロールを作成するか、既存のロールを選択します。

ステップ 3 [Network] タブで、[Add] をクリックして権限を更新および追加します。

ステップ 4 ロールの関連する権限を選択します。

ステップ 5 [Apply] をクリックして新しい権限を適用します。

ステップ 6 ロールの [Storage]、[Server]、および [Operations] の各権限を同じように更新します。

ステップ 7 [Save] をクリックします。

UCS Central ローカル ユーザの管理

手順

ステップ 1 アクション バーで、「Manage UCS Central Local Users」と入力して、Enter キーを押します。これにより、[UCS Central Local Users Manage] ダイアログボックスが開きます。

ステップ 2 [Local Users] で、[Add] をクリックして新しいローカルユーザを作成するか、既存のユーザを選択します。

ステップ 3 [Basic] タブで、ユーザに関する必要な情報を入力します。

ステップ 4 [Roles] タブで、ユーザに割り当てるロールを追加または削除します。

a) [Add] をクリックしてロールを表示します。
b) 1 つまたは複数のロールを選択します。
c) [Apply] をクリックして新しい権限を適用します。

ステップ 5 [Locales] タブで、ユーザに割り当てるロケールを追加または削除します。

a) [Add] をクリックしてロールを表示します。
b) 1 つまたは複数のロールを選択します。
c) [Apply] をクリックして新しい権限を適用します。

ステップ 6 [SSH] タブで、[Authentication Type] を選択します。

ステップ 7 [Save] をクリックします。

UCS Central リモート ユーザの管理

手順

ステップ 1 アクション バーで、「Manage UCS Central Remote Users」と入力して、Enter キーを押します。これにより、[UCS Central Remote Users Manage] ダイアログボックスが開きます。

ステップ 2 [Remote Users] で、リモート LDAP ユーザ、ロール、およびロケールを確認します。

（注） このセクションは読み取り専用です。

ステップ 3 ウィンドウを閉じる場合は [Cancel] をクリックし、他のセクションで行った変更を保存する場合は [Save] をクリックします。

ユーザ ロケール

ユーザは 1 つ以上のロケールに割り当てることができます。各ロケールでは、ユーザがアクセスできる 1 つ以上の組織（ドメイン）を定義します。通常、アクセスできるのは、ロケールで指定された部門のみに限定されます。ただし、部門をまったく含まないロケールは例外です。このようなロケールは、全部門のシステム リソースへの無制限のアクセスを提供します。

Cisco UCS ドメインは、最大 48 個のユーザ ロケールを持つことができます。最初の 48 個のユーザ ロケールが許可された後に設定されたユーザ ロケールは、障害が発生して無効になります。Cisco UCS Central の各ドメイン グループも、親ドメイン グループから継承されたユーザ ロケールを含めて、48 個のユーザ ロケールを持つことができます。Cisco UCS Central から Cisco UCS Manager にユーザ ロケールがプッシュされると、最初の 48 個のロケールだけがアクティブになります。最初の 48 個より後のユーザ ロケールは非アクティブなため、障害が発生します。

admin または aaaadmin、aaa、または domain-group-management の権限を持つユーザは、組織をその他のユーザのロケールに割り当てることができます。組織の割り当ては、それを行うユーザのロケール内の組織だけに制限されます。たとえば、ロケールにエンジニアリング組織しか含まれていない場合、そのロケールを割り当てられたユーザは、他のユーザにエンジニアリング組織のみを割り当てることできます。

（注） admin 権限を持つユーザにロケールを割り当てることはできません。

（注） ロケールを次の権限の 1 つ以上を持つユーザに割り当てることはできません。

- aaa
- admin
- fault
- operations

組織は階層的に管理できます。トップ レベルの組織に割り当てられたユーザは、自動的にその下にあるすべての組織にアクセスできます。たとえば、エンジニアリング組織が、ソフトウェア エンジニアリング組織とハードウェア エンジニアリング組織で構成されているとします。ソフトウェアエンジニアリング部門のみを含むロケールでは、その部門内のシステムリソースにのみアクセスできます。しかし、エンジニアリング部門を含むロケールでは、ソフトウェア エンジニアリング部門とハードウェア エンジニアリング部門の両方のリソースにアクセスできます。

ユーザ組織

ユーザは、1つ以上の組織を作成できます。各組織では、サブ組織、障害、イベント、UUID接尾辞プール、および UUID のブロックが定義されます。

Cisco UCS 組織は、ユーザによって階層的に管理されます。ルート レベルの組織に割り当てられたユーザは、自動的にすべての組織およびその下にあるドメイン グループにアクセスできます。

UCS Central ロケールの管理

手順

ステップ 1 アクション バーで、「Manage UCS Central Locales」と入力して、Enter キーを押します。
これにより、[UCS Central Locales Manage] ダイアログボックスが開きます。

ステップ 2 [Locales] で、[Add] をクリックして新しいロケールを追加するか、既存のロケールを選択します。

ステップ 3 [Organizations] および [Domain Groups] をロケールに割り当てます。

a) [Add] をクリックして、組織またはドメイン グループを表示します。
b) 組織またはドメイン グループを選択します。
c) [Apply] をクリックして新しい権限を適用します。

ステップ 4 [Save] をクリックします。

ドメイン グループ ユーザの管理

手順

ステップ 1 [Domain Group] アイコンをクリックして、[root] を選択します。

ステップ 2 [Settings] アイコンをクリックして、[Users] を選択します。

ステップ 3 [Roles] で、ドメイン グループに関連付けるロールを選択します。ドメイン グループから関連付けを解除するロールのチェックを外します。

ステップ 4 [Network] タブで、[Add] をクリックして権限を更新および追加します。

a) [Add] をクリックして、組織を表示します。
b) ロールの関連する権限を選択します。
c) [Apply] をクリックして新しい権限を適用します。

ステップ 5 ロールの [Storage]、[Server]、および [Operations] の各権限を同じように更新します。

ステップ 6 [Locales] で、ドメイン グループに関連付けるロケールを選択します。ドメイン グループから関連付けを解除するロールのチェックを外します。

ステップ 7 [Organizations] をロケールに割り当てます。

a) [Add] をクリックして、組織を表示します。
b) 組織またはドメイン グループを選択します。

c) [Apply] をクリックして新しい権限を適用します。

ステップ 8 [Save] をクリックします。

第 3 章

認証サービス

認証サービス

Cisco UCS Central は、ユーザ ログインを認証するための次の方法をサポートします。

- Cisco UCS Central でのローカルに存在するユーザ アカウントのローカル ユーザ認証
- 次のプロトコルのいずれかを使用した登録済み UCS ドメインのリモート ユーザ認証
  - LDAP
  - RADIUS
  - TACACS+

パスワードの作成に関するガイドライン

それぞれのローカル認証されたユーザ アカウントにはパスワードが必要です。シスコでは、各ユーザに強力なパスワードを設定することを推奨します。admin、aaa、または domain-group-management 権限を持つユーザは、ユーザ パスワードに対してパスワード強度チェックを実行するように Cisco UCS Central を設定できます。パスワード強度チェックを有効にした場合、それぞれのユーザは強力なパスワードを使用する必要があります。

Cisco UCS Central では、次の要件を満たさないパスワードは拒否されます。

- 8 ～ 80 文字を含む。
- 次の少なくとも 3 種類を含む。
  - 小文字
  - 大文字
  - 数字
  - 特殊文字
- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。つまり、辞書に記載されている標準的な単語に基づくパスワードを指定することはできません。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。
- ローカル ユーザ アカウントおよび admin アカウントのパスワードは空白にしない。

ローカル認証されたユーザのパスワード プロファイル

パスワードプロファイルには、Cisco UCS Central のローカル認証されたすべてのユーザのパスワード履歴やパスワード変更間隔プロパティが含まれます。ローカル認証されたユーザに異なるパスワード プロファイルを指定することはできません。

（注） パスワード プロファイル プロパティを変更するには、admin、aaa、または domain-group-management 権限を持っている必要があります。パスワード履歴を除き、これらのプロパティはこれらの管理権限を持つユーザには適用されません。

パスワード履歴カウント

パスワード履歴のカウントにより、ローカル認証されたユーザが同じパスワードを再利用しないようにすることができます。パスワード履歴カウントを設定すると、Cisco UCS Central で以前に使用されたパスワードが最大15個保存されます。パスワード履歴カウントには最新のパスワードが先頭で、パスワードが新しい順に保存されます。そのため、履歴カウントがしきい値に達したときには、最も古いパスワードを再利用できます。

パスワード履歴カウントで設定された数のパスワードを作成して使用すると、ユーザはパスワードを再使用できます。たとえば、パスワード履歴カウントを 8 に設定した場合、ユーザは最初のパスワードを 9 番目のパスワードが期限切れになる後まで再使用できません。

デフォルトでは、パスワード履歴は 0 に設定されます。この値は、履歴のカウントをディセーブルにし、ユーザはいつでも前のパスワードを使用できます。

ローカル認証されたユーザのパスワード履歴カウントをクリアして、以前のパスワードを再使用可能にすることができます。

パスワード変更間隔

パスワード変更間隔は、ローカル認証されたユーザが特定の時間内に行えるパスワード変更の回数を制限します。次の表で、パスワード変更間隔の 2 つの間隔設定オプションについて説明します。

間隔の設定	説明	例
パスワード変更不許可	パスワードの変更後、指定された時間の間は、ローカル認証されたユーザのパスワードを変更することはできません。 1 ～ 745 時間の変更禁止間隔を指定できます。デフォルトでは、変更禁止間隔は 24 時間です。	パスワード変更後 48 時間以内にユーザがパスワードを変更するのを防ぐため： • [Change During Interval] を無効に設定 • [No Change Interval] を 48 に設定
変更間隔内のパスワード変更許可	ローカル認証されたユーザのパスワードを事前に定義された時間内に変更できる最大回数を指定します。 変更間隔を 1 ～ 745 時間で、パスワード変更の最大回数を 0 ～ 10 で指定できます。デフォルトでは、ローカル認証されたユーザに対して、48 時間間隔内で最大 2 回のパスワード変更が許可されます。	パスワード変更後 24 時間以内に最大 1 回のパスワード変更を許可するには、次のような設定を行います。 • [Change during interval] を有効に設定 • [Change count] を 1 に設定 • [Change interval] を 24 に設定

UCS Central 認証の管理

手順

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

ステップ 2 [LDAP]で、以下のタブで要求される情報を入力します。

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

b) [Providers] タブで、[+] 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。
SSL セクションの [Enabled] または [Disabled] を選択します。[Enabled] を選択すると、LDAP データベースとの通信に暗号化が必要になります。SSL LDAP を有効にするには STARTTLS を使用します。これにより、ポート 389 を使用した暗号化通信が可能になります。[Disabled] を選択すると、認証情報はクリア テキストで送信されます。

c) [Groups] タブで、[+] 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。

- Cisco UCS Central に対してサポートされる LDAP プロバイダー グループの最大数は 16 です。
- 1 つのプロバイダー グループに対して Cisco UCS Central でサポートされる最大プロバイダー数は 8 です。

d) [Group Maps] タブで、[Provider Group Map DN] を入力してから、オプションで、[Roles] と [Locales] を追加します。
最大グループ マップ長は、Cisco UCS Central 内で 240 文字を超えることはできません。次に例を示します。

```
maximum group-map length:
---------------------------------
CN=jeewan2,\
OU=1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-\
23-24-1,\
OU=1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-\
23-24-0,\
OU=ou-01-11-1,\
DC=ucsm,DC=qasam-lab,DC=in
```

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 Connection Timeout] と [Retry Count] の値を入力します。
b) [Providers] タブで、[+] 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、[+] 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 Connection Timeout] と [Retry Count] の値を入力します。
b) [Providers] タブで、[+] 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、[+] 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、ネイティブまたはコンソール デフォルト ドメインを設定、追加、または削除します。
Cisco UCS Central でサポートされる認証ドメインの最大数は 8 です。

ステップ 6 [Native (Default)] をクリックします。

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

- 読み取り専用アクセス ロールを割り当てる
- ログインを拒否する

b) [Web Session Refresh Period (Seconds)] に、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。
セッションが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に変更しますが、そのセッションを終了することはありません。

60 ～ 172800 秒の間で指定します。デフォルトは 600 秒です。

c) [Web Session Timeout (Seconds)] に、最後の更新要求後の最大経過時間を入力します。Web セッションが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 秒の間で指定します。デフォルト値は 7200 秒です。

d) [Enable] または [Disable] を、[Authentication] に選択します。

e) [Enable] を選択した場合は、[Authentication Realm] を選択します。

- [LDAP]：ユーザを Cisco UCS Central で指定された LDAP サーバ上で定義します。
- [Local]：ユーザを Cisco UCS Central または Cisco UCS ドメインでローカルに定義します。
- [RADIUS]：ユーザを Cisco UCS Central で指定された RADIUS サーバ上で定義します。
- [TACACS+]：ユーザを Cisco UCS Central で指定された TACACS+ サーバ上で定義します。

f) [LDAP]、[RADIUS] または [TACACS+] を選択した場合は、[Provider Group] 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 [Console (Default)] をクリックします。

a) [Authentication] の有効化または無効化を選択します。

b) [Enable] を選択した場合は、[Authentication Realm] を選択します。

c) [LDAP]、[RADIUS] または [TACACS+] を選択した場合は、[Provider Group] 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 8 [+] をクリックして、新しい認証ドメインを追加します。

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。スペースおよび次を除く特殊文字は使用できません：-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）が使用できます。この名前は、いったん保存した後では変更できません。

RADIUS を使用するシステムの場合、認証ドメイン名については、ローカルに作成されたユーザ名に対して 32 文字の制限が適用されます。Cisco UCS ではフォーマット用として 5 文字が予約されているため、ドメイン名とユーザ名を合わせて合計 27 文字を超えることができません。

b) [Web Session Refresh Period (Seconds)] を入力します。

c) [Web Session Timeout (Seconds)] を入力します。

d) [Authentication Realm] が [LDAP]、[RADIUS] または [TACACS+] に設定されている場合は、[Provider Group] を選択します。

ステップ 9 [Save] をクリックします。
認証ドメイン作成後、設定の編集や削除が可能になります。

Windows パススルー認証

Cisco UCS Central リリース 2.0 では、リモート ユーザのログインに Windows パススルー認証を使用して、アカウントのログインのセキュリティ レベルを高めています。Windows パススルー認証には、ドメインに存在するコンピュータにログオンした後で、もう一度ユーザ クレデンシャルを入力しないで Cisco UCS Central にサインインできるように合理化されています。

Windows パススルー認証は、ログイン プロンプトのチェックボックスから有効にできます。ただし、このチェックボックスを最初にクリックし、Windows のクレデンシャル使用してサインオンすることはできません。Cisco UCS Central から外部プラグインをダウンロードするように求められます。プラグインをダウンロード、インストールして、有効にした後に、Windows パススルー認証を使用してサインオンできます。

（注）

Cisco UCS Central 2.0 の Windows パススルー認証には次の前提条件があります。

- Windows クライアント システムを Active Directory ドメインに接続する必要があります。Active Directory のクレデンシャルを使用してログインする必要もあります。
- Active Directory の導入では、Active Directory フェデレーション サービスをサポートしている必要があります。
- 環境は、少なくとも .NET Framework バージョン 4.0.30319 にする必要があります。

Windows パススルー認証には、次の制限事項があります。

- Cisco UCS Central では、Microsoft Internet Explorer バージョン 11 でのみ Windows パススルー認証をサポートします。
- シスコのプラグインをダウンロードしてインストールする必要があります。
- 現在、Windows パススルー認証は、認証レルムを LDAP に設定し、RADIUS または TACACS+ には設定していない場合にのみサポートされます。LDAP のレルム名はドメイン名と一致させる必要があります。たとえば、LDAP レルム名が CISCO/ユーザ名の場合、LDAP レルムは CISCO になります。

ドメイン グループ認証の管理

手順

ステップ 1 [Domain Group Navigation] アイコンをクリックして、ルートを選択します。
これにより、[root Domain Group] ページが表示されます。

ステップ 2 [Settings] アイコンをクリックして、[Authentication] ページを起動します。
[Root Manage] ダイアログが開きます。

ステップ 3 [LDAP] で、次の情報を入力します。

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

b) [Providers] タブで、[+] 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。
SSL セクションの [Enabled] または [Disabled] を選択します。[Enabled] を選択すると、LDAP データベースとの通信に暗号化が必要になります。LDAP を有効にするには STARTTLS を使用します。これにより、ポート 389 を使用した暗号化通信が可能になります。[Disabled] を選択すると、認証情報はクリア テキストで送信されます。

c) [Groups] タブで、[+] 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。

- Cisco UCS Central に対してサポートされる LDAP プロバイダー グループの最大数は 16 です。
- 1 つのプロバイダー グループに対して Cisco UCS Central でサポートされる最大プロバイダー数は 8 です。

d) [Group Maps] タブで、[+] をクリックして [Provider Group Map DN] を入力してから、オプションで、[Roles] と [Locales] を追加します。
Cisco UCS Central でサポートされる最大グループ マップ長は 240 です。

```
maximum group-map length:
---------------------------------
CN=jeewan2,OU=1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-\
17-18-19-20-21-22-23-24-1,OU=1-2-3-4-5-6-7-8-9-10-11-\
12-13-14-15-16-17-18-19-20-21-22-23-24-0,OU=ou-01-11-1,\
DC=ucsm,DC=qasam-lab,DC=in
```

ステップ 4 [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 Connection Timeout] と [Retry Count] の値を入力します。

b) [Providers] タブで、[+] 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、[+] 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 [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 Connection Timeout] と [Retry Count] の値を入力します。

b) [Providers] タブで、[+] 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、[+] 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 6 [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) [+] をクリックして、ドメイン グループの認証ポリシーを作成します。
ポリシーは、親グループから継承した設定を上書きします。Cisco UCS Central でサポートされる認証ドメインの最大数は 8 です。

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。RADIUS を使用したシステムでは、認証ドメイン名はユーザ名の一部と見なされます。これについては、ローカルに作成されたユーザ名に対して 32 文字の制限が適用されます。Cisco UCS はフォーマット用に 5 文字を挿入するため、ドメイン名とユーザ名を合わせた合計が 27 文字を超えると、認証は失敗します。

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 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 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、Cisco UCS Central が Web セッションを終了するまでの最大経過時間を入力します。Web セッションが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 秒の整数を指定します。デフォルト値は 7200 秒です。

e) [Authentication Realm] を選択します。

- [LDAP]：ユーザを Cisco UCS Central で指定された LDAP サーバ上で定義します。
- [Local]：ユーザを Cisco UCS Central または Cisco UCS ドメインでローカルに定義します。
- [RADIUS]：ユーザを Cisco UCS Central で指定された RADIUS サーバ上で定義します。
- [TACACS+]：ユーザを Cisco UCS Central で指定された TACACS+ サーバ上で定義します。

ステップ 7 [Save] をクリックします。

第 4 章

リモート認証

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、ユーザ認可に関係する次のガイドラインに留意してください。

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には、次のことを確認してください。

- ユーザが Cisco UCS Central で作業するために必要なロールが、アカウントに含まれている。
- これらのロールの名前が、Cisco UCS Central で使用される名前と一致する。

ロール ポリシーによっては、ユーザがログイン許可を付与され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、LDAP、RADIUS、および TACACS+ を使用してリモート認証を行います。

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 は次のことを実行します。

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 そのユーザに割り当てたロールとロケールをチェックします（ユーザが検証にパスした場合）。

次の表は、Cisco UCS Central でサポートしているリモート認証プロバイダーのユーザ属性要件を比較したものです。

表 *3*：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	次のいずれかを実行します。 • 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 次のセクションで、OID（オブジェクト識別子）のサンプルを示します。
RADIUS	任意	次のいずれかを実行します。 • RADIUS スキーマを拡張せず、要件を満たす既存の未使用属性を使用する。 • RADIUS スキーマを拡張して、cisco-avpair などの一意の名前でカスタム属性を作成する。	シスコによる RADIUS の実装のベンダー ID は 009 であり、属性のベンダー ID は 001 です。 次の構文例は、cisco-avpair 属性を作成する場合に複数のユーザロールとロケールを指定します。`shell:roles="admin,aaa" shell:locales="L1,abc"`複数の値を区切るには、区切り文字としてカンマ「,」を使用します。

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
TACACS+	必須	スキーマを拡張し、cisco-av-pair という名前のカスタム属性を作成する必要があります。	cisco-av-pair 名は、TACACS+ プロバイダーの属性 ID を提供する文字列です。 次の構文例は、cisco-av-pair 属性を作成するときに複数のユーザロールとロケールを指定します。 `cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`cisco-av-pair 属性構文でアスタリスク（*）を使用すると、ロケールがオプションとして指定され、同じ認可プロファイルを使用する他のシスコデバイスで認証の失敗を防ぐことができます。複数の値を区切るには、区切り文字としてスペースを使用します。

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
```

第 5 章

LDAP 認証

LDAP プロバイダー

LDAP リモート ユーザを作成および設定し、Cisco UCS Central からロールとロケールを、Cisco UCS Manager と同じ要領で割り当てます。LDAP プロバイダーの作成は、常に Cisco UCS Central ドメイン グループ ルートから行ってください。

LDAP グループ マップ

複数の LDAP グループ マップを定義して、Cisco UCS Central のネストに対して Windows Active Directory がサポートするレベルまでネストできます。ネスト グループにプロバイダーを割り当てると、プロバイダーが異なる 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。認証の際に、Cisco UCS Central は、プロバイダー グループ内のすべてのプロバイダーを順番に試行します。Cisco UCS Central は、設定されたサーバのいずれにもアクセスできない場合、ローカル ユーザ名とパスワードを使用して自動的にローカル認証方式にフォールバックします。

LDAP グループ マップの数は Cisco UCS Manager のバージョンに応じて定義できます。サポートされる LDAP グループ マップ，（31 ページ）を参照してください。

プロバイダー グループ

プロバイダー グループは、認証プロセス中に Cisco UCS が使用するプロバイダーのセットです。Cisco UCS Central では、最大 16 のプロバイダー グループを作成でき、グループごとに最大 8 つのプロバイダーを含めることができます。

認証の際には、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サーバが使用できない場合、または到達不能な場合、Cisco UCS Central は、ローカル ユーザ名とパスワードを使用して自動的に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

LDAP データベースへのアクセス制限のために LDAP グループを使用している組織では、Cisco UCS ドメインで、グループ メンバーシップ情報を使用してログイン時に LDAP ユーザにロールや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 を導入するときに、LDAP ユーザ オブジェクトでロールや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はユーザのロールとロケールに関する情報を LDAP グループ マップから取得します。ロールとロケールの条件がポリシーの情報に一致すると、Cisco UCS Centralはそのユーザにアクセス権を提供します。

LDAP グループ マップの数は Cisco UCS Manager のバージョンに応じて定義できます。

Cisco UCS Central のネストに対して Windows Active Directory がサポートするレベルまで LDAP グループマップをネストできます。ネストグループにプロバイダーを割り当てると、プロバイダーが異なる 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。認証の際に、Cisco UCS Central は、プロバイダー グループ内のすべてのプロバイダーを順番に試行します。Cisco UCS Central は、設定されたサーバのいずれにもアクセスできない場合、ローカル ユーザ名とパスワードを使用して自動的にローカル認証方式にフォールバックします。

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更新されることはありません。LDAP ディレクトリで LDAP グループを削除または名前変更する場合、Cisco UCS Centralで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いずれかの組み合わせ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

たとえば、特定のロケーションのサーバ管理者グループを表す LDAP グループの認証を設定する場合は、その LDAP グループに対する server-profile や server-equipment などのユーザ ロールを含めることができます。特定のロケーションのサーバ管理者に対しアクセスを制限する場合は、特定のサイト名をロケールに指定できます。

（注） Cisco UCS Central にはすぐに使用できる多数のユーザ ロールが含まれていますが、ロケールは含まれていません。カスタム ロケールを作成して LDAP プロバイダー グループをロケールにマップする必要があります。

サポートされる LDAP グループ マップ

サポートされる LDAP グループ マップの数は Cisco UCS Manager バージョンによって異なります。

Cisco UCS Manager バージョン	サポートされる LDAP グループ マップ
Cisco UCS Manager リリース 3.1(2) 以降	160
Cisco UCS Manager リリース 3.1(1)	128
Cisco UCS Manager リリース 2.2(8) 以降	160
Cisco UCS Manager リリース 2.2(7) 以前	28

ネストされた LDAP グループ

LDAP グループを他のグループのメンバーとしてネストすることにより、アカウントを統合して複製を減らすことができます。

デフォルトでは、LDAP グループを別のグループ内にネストすると、ユーザ権限が継承されます。たとえば、Group_2 のメンバーとして Group_1 を作成する場合、Group_1 のユーザは Group_2 のメンバーと同じ権限が与えられます。その結果、Group_1 のメンバーであるユーザを検索するときは、LDAP グループ マップで Group_2 だけを選択します。Group_1 と Group_2 を別々に検索する必要はありません。

LDAP グループ マップで定義されたネストしたグループを検索できます。グループをネストすることによって、サブグループを作成する必要がなくなります。

（注） ネストした LDAP グループの検索は、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。

ネストしたグループ名に特殊文字を含めた場合は、次の例に示す構文を使用してそれらをエスケープする必要があります。

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

UCS Central LDAP 設定の管理

手順

ステップ 1 [Actions] バーから、「Managing UCS Central LDAP Configuration」と入力します。
これにより、[UCS Central LDAP Configuration Manage] ダイアログ ボックスが開きます。

ステップ 2 [LDAP]で、以下のタブで要求される情報を入力します。

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

b) [Providers] タブで、[+] 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。
SSL セクションの [Enabled] または [Disabled] を選択します。[Enabled] を選択すると、LDAP データベースとの通信に暗号化が必要になります。SSL LDAP を有効にするには STARTTLS を使用します。これにより、ポート 389 を使用した暗号化通信が可能になります。[Disabled] を選択すると、認証情報はクリア テキストで送信されます。

c) [Groups] タブで、[+] 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] を入力します。オプションで、[Roles] と [Locales] を追加します。
（注） プロバイダー グループ マップの識別名に特殊文字を使用しないでください。

ステップ 3 [Authentication Domains] で、ネイティブまたはコンソール デフォルト ドメインを設定、追加、または削除します。

ステップ 4 [Native(Default)] をクリックして、次の手順を実行します。

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

b) [Web Session Refresh Period (Seconds)] に、更新要求間の最大許容時間を入力します。
Web セッションが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 秒の間で指定します。デフォルトは 600 秒です。

c) [Web Session Timeout (Seconds)] に、最後の更新要求後の最大経過時間を入力します。Web セッションが時間制限を超えると、Cisco UCS Central は、Web セッションが終了したと見なし、自動的に Web セッションを終了します。
60 ～ 172800 秒の間で指定します。デフォルト値は 7200 秒です。

d) [Enabled] または [Disabled] を、[Authentication] に選択します。

e) [Enabled] を選択した場合は、[Authentication Realm] を選択します。

- [LDAP]：ユーザを Cisco UCS Central で指定された LDAP サーバ上で定義します。
- [Local]：ユーザを Cisco UCS Central または Cisco UCS ドメインでローカルに定義します。

- [RADIUS]：ユーザを Cisco UCS Central で指定された RADIUS サーバ上で定義します。
- [TACACS+]：ユーザを Cisco UCS Central で指定された TACACS+ サーバ上で定義します。

f) [LDAP]、[RADIUS] または [TACACS+] を選択した場合は、[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 5 [Console (Default)] をクリックします。

a) [Enabled] または [Disabled] を、[Authentication] に選択します。

b) [Enabled] を選択した場合は、[Authentication Realm] を選択します。

- [LDAP]：ユーザを Cisco UCS Central で指定された LDAP サーバ上で定義します。
- [Local]：ユーザを Cisco UCS Central または Cisco UCS ドメインでローカルに定義します。
- [RADIUS]：ユーザを Cisco UCS Central で指定された RADIUS サーバ上で定義します。
- [TACACS+]：ユーザを Cisco UCS Central で指定された TACACS+ サーバ上で定義します。

c) [LDAP]、[RADIUS] または [TACACS+] を選択した場合は、[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 6 [+] をクリックして、新しい認証ドメインを追加します。

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。スペースは使用できません。特殊文字では、-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）が使用できます。この名前は、いったん保存した後では変更できません。

RADIUS を使用したシステムでは、認証ドメイン名はユーザ名の一部と見なされます。したがって、ローカルに作成されたユーザ名に対して 32 文字の制限が適用されます。Cisco UCS ではフォーマット用として 5 文字が予約されているため、ドメイン名とユーザ名を合わせて合計 27 文字を超える名前は使用できません。

b) [Web Session Refresh Period (Seconds)] を入力します。

c) [Web Session Timeout (Seconds)] を入力します。

d) [LDAP]、[RADIUS] または [TACACS+] を選択した場合は、[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] をクリックします。
認証ドメインを作成したら、必要に応じて、設定を編集できます。また、ごみ箱をクリックして、選択した認証ドメインを削除することもできます。

第 6 章

SNMP 認証

SNMP ポリシー

Cisco UCS Central では、以下がサポートされます。

- グローバル SNMP ポリシー
- SNMP のトラップとインフォームの定義
- SNMP ユーザの定義

これらの定義には、通常のパスワードとプライバシーパスワード、認証タイプ MD5 または SHA、および暗号化タイプ DES と AES-128 を使用できます。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の SNMP ポリシーをグローバルに定義する選択をしている場合、SNMP ポリシーはすべて、Cisco UCS Central への登録に従います。

SNMP エージェント機能は、Cisco UCS Central をリモートで監視します。また、Cisco UCS Central ホスト IP を変更し、新しい IP で SNMP エージェントを再起動することもできます。SNMP は、アクティブまたはスタンバイのどちらの状態の Cisco UCS Central サーバ上でも稼働します。設定は、どちらの場合も存続します。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 を使用して、SNMP v1、v2c のコミュニティ ストリングを設定し、SNMPv3 ユーザを作成および削除することができます。

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およびモニタリングするシステム。

SNMP エージェント

Cisco UCS Central 内のソフトウェア コンポーネント。Cisco UCS Central 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する管理対象デバイス。Cisco UCS Central 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、SNMP をイネーブルにして、その設定を行います。

管理情報ベース（MIB）

SNMP エージェント内の管理対象オブジェクトのコレクション。Cisco UCS Central では OS MIB モードだけがサポートされます。

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 サーバの場合は MIB Reference for Cisco UCS Manager を、C シリーズ サーバの場合は MIB Reference for Cisco UCS Standalone C-Series Servers を、それぞれ参照してください。

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。これらの通知を使えば、SNMP マネージャが要求を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 では SNMP 通知がトラップとして生成されます。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。したがって、Cisco UCS Central ではトラップを受信したかどうかを判断できません。

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 UCS Central は、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。

メッセージ整合性

不正な方法でのメッセージの変更や破棄が行われないことを確認します。また、悪意のないレベルを超えたデータ シーケンスの変更が行われていないことも確認します。

メッセージ発信元の認証

データを受信したユーザが提示する ID を確認します

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、またはプロセスに情報が使用または開示されないことを保証します

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、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 モデルは、選択したセキュリティ レベルと結合され、Cisco UCS Central による SNMP メッセージの処理時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。セキュリティ レベルは、Cisco UCS Central でメッセージを保護して開示されないようにする必要があるかどうか、またはメッセージを認証する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。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 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。

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 *4* : ***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。

モデル	レベル	認証	暗号化	結果
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	No	次のコードまたはアルゴリズムに基づいて認証を提供します。 • ハッシュ ベースの メッセージ 認証コード（HMAC） • メッセージ ダイジェスト 5（MD5）アルゴリズム • HMAC セキュア ハッシュ アルゴリズム（SHA）

モデル	レベル	認証	暗号化	結果
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	次のコードまたはアルゴリズムに基づいて認証を提供します。 • ハッシュ ベースのメッセージ認証コード（HMAC） • メッセージ ダイジェスト 5（MD5）アルゴリズム • HMAC セキュア ハッシュ アルゴリズム（SHA） • データ暗号化標準（DES）56 ビット暗号化を提供します。 • 暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいて認証を提供します。

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 に対して set 操作は使用できません。Cisco UCS Centralでサポートされている MIB を次に示します。

- SNMP MIB-2 システム
- HOST-RESOURCES-MIB
  - hrSystem
  - hrStorage
  - hrDevice
  - hrSWRun
  - hrSWRunPerf
- UCD-SNMP-MIB
  - Memory
  - 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 および Cisco UCS Central MIB をサポートしません。

SNMPv3 ユーザの認証プロトコル

Cisco UCS Central は、SNMPv3 ユーザ向け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 設定を有効にし、SNMPv3 ユーザのプライバシー パスワードをインクルードした場合、Cisco UCS Central はプライバシー 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

手順

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

ステップ 2 [Basic] タブで、[Enabled] または [Disabled] をクリックします。[Enabled] を選択した場合、次のフィールドに値を入力します。

a) [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。

b) [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。

c) [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 3 [Save] 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 トラップあるいはインフォームの作成と編集

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。

手順

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

ステップ 2 [SNMP Traps] タブで、[Add] をクリックします。

ステップ 3 [Trap Host Name/IP Address] で、トラップの送信先とする SNMP ホストの IP アドレスを入力します。

ステップ 4 [SNMP Trap Properties] で、次の操作を行います。

a) [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。

b) [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。

c) [Version] には、[V1]、[V2C]、または [V3] を選択します。

d) [V2C] または [V3] を選択した場合は、[Type] に [Traps] または [Informs] を選択します。

e) [V3] を選択した場合は、さらに [V3Privilege] を選択します。

- [Auth]：認証あり、暗号化なし
- [NoAuth]：認証または暗号化なし
- [Priv]：認証あり、暗号化あり

ステップ 5 [Save] をクリックします。

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。

手順

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

ステップ 2 [SNMP Users] タブで、[Add] をクリックします。

ステップ 3 [SNMP User Name] で、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）、-（ハイフン）も指定できます。

ステップ 4 [SNMP User Properties] で、次の操作を行います。

a) [Authentication Type] で、承認タイプとして [MD5] または [SHA] を選択します。
b) [AES-128 Encryption] に対して、[Enabled] または [Disabled] をクリックします。
c) [Password] と [Privacy Password] を入力して確認します。

ステップ 5 [Save] をクリックします。