Cisco UCS Manager リリース 3.2 アドミニストレーション管理（CLI 用）ガイド

初版：2017 年 8 月 18 日

最終更新：2018 年 11 月 14 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/

目 次

はじめに

対象読者

このガイドは、次の 1 つ以上を担当し、専門知識を持つ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などのメイン タイトルは、ボールド体（**bold**）で示しています。
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。
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。

テキストのタイプ	説明
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、**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（*this font*）で示しています。
[ ]	角かっこの中の要素は、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、波かっこで囲み、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、角かっこで囲み、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 と見なされます。
< >	パスワードのように出力されない文字は、山かっこ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、角かっこ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 安全上の重要な注意事項

この警告マークは「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。機器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、一般的な事故防止対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。

関連 Cisco UCS 資料

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、以下の URL で入手可能な「*Cisco UCS B-Series Servers Documentation Roadmap*」を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

すべての C-Series マニュアルの完全なリストについては、次の URL で入手可能な「『*Cisco UCS C-Series Servers Documentation Roadmap*』」を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html

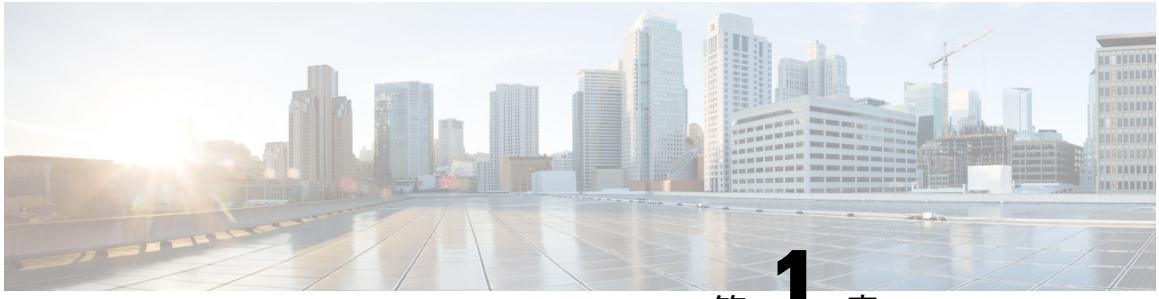
管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、「Release Bundle Contents for Cisco UCS Software」を参照してください。

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@external.cisco.com までコメントをお送りください。ご協力をよろしくお願いいたします。



第 1 章

管理の概要

この章は、次の項で構成されています。

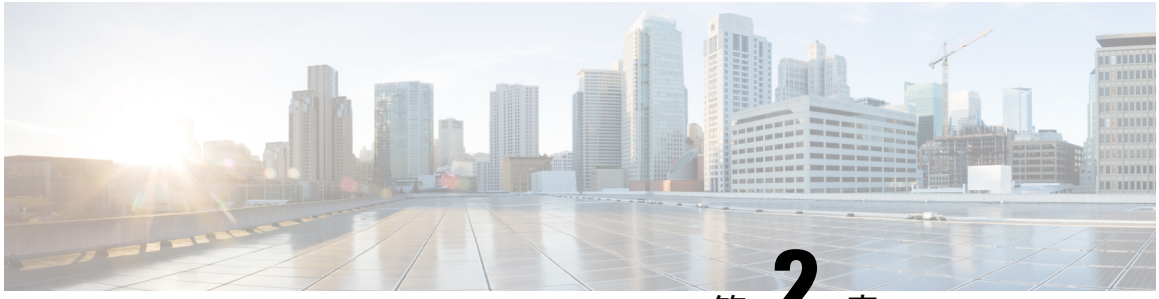
管理の概要

Cisco UCS Manager から規定のユーザ アクセス機能を設定することで、同じドメインにある Cisco UCS 6332 40 GB ファブリック インターコネクト、および UCS 6200 シリーズ 10 GB ファブリック インターコネクトを 1 つのコンソールから管理できるようになります。環境で UCS 6324 40 GB Mini を使用している場合は、同じ Cisco UCS Manager 機能を使用してユーザ アクセス機能を管理できます。

環境内のユーザ アクセスを管理するために、次の基本的な管理設定を構成できます。

- パスワード：デフォルトの管理ユーザアカウントを初期セットアップする際にパスワードを選択し、システムにアクセスするための一意のユーザ名とパスワードをユーザアカウントごとに作成します。
- RBAC：ロールに従ってユーザのアクセス権限を委譲および制御し、マルチテナントなどのテナント用に定義された組織境界内でのユーザ アクセスを制限します。
- 認証：UCS Manager のローカル ユーザ アカウント、または LDAP、RADIUS、TACACS+ プロトコルを使用してリモート ユーザ アカウントを作成します。
- コミュニケーション サービス：サードパーティ製アプリケーションと Cisco UCS のインターフェイス用途として、CIM XML、HTTP、HTTPS、SMASH CLP、SNMP、SSH、Telnet を設定します。
- 組織：ポリシー、プール、サービスプロファイルのための組織を作成します。デフォルトのルート組織の下に複数のサブ組織を作成し、各サブ組織の下にサブ組織をネストすることができます。
- CIMC：ユーザの KVM、vMedia、および SoL セッションを閉じます。UCS Manager が CIMC からイベントを受け取ると、そのセッションテーブルを更新し、すべてのユーザに情報を表示します。

- バックアップと復元：システム設定の全体またはその一部のスナップショットを作成し、そのファイルをネットワーク上の場所にエクスポートします。Full State、すべての設定、システム設定、および論理設定のバックアップを設定できます。
- Call Home：UCS のエラーや障害に関する電子メール アラート通知を設定します。Cisco TAC（事前定義済み）または他の受信者宛ての電子メール通知を設定できます。
- 遅延展開：サービスプロファイルの展開について、すぐに展開するか、または指定されたメンテナンス時間帯に展開するかを設定します。これを使用して、サービスプロファイルまたはサービス プロファイル テンプレートに中断を伴う設定変更を行うタイミングを制御します。
- スケジューリング：あるスケジュールのワンタイム オカレンスや繰り返しオカレンスをスケジュールしたり、スケジュール削除したりします。
- 障害抑制：予定されたメンテナンス時間帯に SNMP トラップおよび Call Home 通知を抑制する、障害抑制を有効にします。



第 2 章

パスワード管理

Cisco UCS パスワードに関するガイドライン

ローカル認証された各ユーザ アカウントには、パスワードが必要です。admin または aaa の権限を持つユーザは、Cisco UCS Managerを設定して、ユーザのパスワードの強度チェックを実行できます。表 1 : UCS パスワードに使用可能な ASCII 文字の表 （3 ページ） に、UCS パスワードに使用可能な ASCII 文字のリストを示します。

表 *1 : UCS* パスワードに使用可能な *ASCII* 文字の表

出力可能な ASCII 文字	説明
A ～ Z	大文字の A ～ Z
a ～ z	小文字の a ～ z
0 ～ 9	数字の 0 ～ 9
!	感嘆符
"	引用符
%	パーセント記号
&	アンパサンド
'	アポストロフィ

出力可能な ASCII 文字	説明
(	左カッコ
)	右カッコ
*	アスタリスク
+	プラス記号
,	カンマ
-	ハイフン
.	ピリオド
/	スラッシュ
:	コロン
;	セミコロン
<	小なり
>	大なり
@	アット マーク
[	開き大カッコ
\	バックスラッシュ
]	閉じ大カッコ
^	キャレット
_	アンダースコア
`	アクサングラーブ
{	開き中カッコ
|	縦棒
}	閉じ中カッコ
~	チルダ

シスコでは強力なパスワードを使用することを推奨しています。そうしなかった場合、ローカル認証されたユーザに対するパスワードの強度チェックで、Cisco UCS Manager によって次の要件を満たさないパスワードが拒否されます。

- 8 ～ 80 文字を含む。
- パスワードの強度の確認が有効になっている場合はパスワード長は可変で、6 ～ 80 文字の間で設定できます。

（注） デフォルトは 8 文字です。

- 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。たとえば、パスワードには辞書に記載されている標準的な単語に基づいたもの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。

Cisco UCS ユーザ名に関するガイドライン

ユーザ名は、Cisco UCS Manager のログイン ID としても使用されます。Cisco UCS 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 Manager 内で一意である必要があります。
- ログイン ID は、英文字から始まる必要があります。アンダースコアなどの特殊文字や数字から始めることはできません。

- ログイン ID では、大文字と小文字が区別されます。
- すべてが数字のログイン 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。

変更間隔のパスワード変更の最大回数の設定

パスワード プロファイル プロパティを変更するには、admin または aaa 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、admin または aaa 権限を持つユーザに適用されません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope password-profile**	パスワード プロファイル セキュリティ モードを開始します。
ステップ 3	UCS-A /security/password-profile # **set change-during-interval enable**	ローカル認証されたユーザが実行できる、指定時間内のパスワード変更回数を制限します。
ステップ 4	UCS-A /security/password-profile # **set change-count** *pass-change-num*	ローカル認証されたユーザが、[Change Interval] の間に自分のパスワードを変更できる最大回数 を指定します。 この値は、0 ～ 10 から自由に設定できます。
ステップ 5	UCS-A /security/password-profile # **set change-interval** *num-of-hours*	[Change Count] フィールドで指定したパスワード変更回数が有効になる時間の最大数 を指定します。 この値は、1 ～ 745 時間から自由に設定できます。 たとえば、このフィールドが 48 に設定され、[Change Count] フィールドが 2 に設定されている場合、ローカル認証されたユーザは 48 時間以内に 2 回を超えるパスワード変更を実行することはできません。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /security/password-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、change during interval オプションを有効にし、変更回数を 5 回、変更間隔を 72 時間に設定し、トランザクションをコミットします。

```
UCS-A # scope security
UCS-A /security # scope password-profile
UCS-A /security/password-profile # set change-during-interval enable
UCS-A /security/password-profile* # set change-count 5
UCS-A /security/password-profile* # set change-interval 72
UCS-A /security/password-profile* # commit-buffer
UCS-A /security/password-profile #
```

パスワードの変更禁止間隔の設定

パスワード プロファイル プロパティを変更するには、admin または aaa 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、admin または aaa 権限を持つユーザに適用されません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope password-profile**	パスワード プロファイル セキュリティ モードを開始します。
ステップ 3	UCS-A /security/password-profile # **set change-during-interval disable**	間隔中の変更機能を無効にします。
ステップ 4	UCS-A /security/password-profile # **set no-change-interval** *min-num-hours*	ローカル認証されたユーザが、新しく作成されたパスワードを変更する前に待機する時間の最小数。 を指定します。 この値は、1 ～ 745 時間から自由に設定できます。 この間隔は、[Change During Interval] プロパティが [Disable] に設定されている場合、無視されます。
ステップ 5	UCS-A /security/password-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、間隔中の変更オプションを無効にし、変更禁止間隔を72時間に設定し、トランザクションをコミットする例を示します。

```
UCS-A # scope security
UCS-A /security # scope password-profile
UCS-A /security/password-profile # set change-during-interval disable
UCS-A /security/password-profile* # set no-change-interval 72
UCS-A /security/password-profile* # commit-buffer
UCS-A /security/password-profile #
```

パスワード履歴カウントの設定

パスワードプロファイルプロパティを変更するには、adminまたはaaa権限を持っている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope password-profile**	パスワード プロファイル セキュリティ モードを開始します。
ステップ 3	UCS-A /security/password-profile # **set history-count** *num-of-passwords*	ローカル認証されたユーザが、以前に使用されたパスワードを再利用できるまでに、作成する必要がある一意のパスワードの数を指定します。 この値は、0 ～ 15 から自由に設定できます。 デフォルトでは、[History Count] フィールドは0に設定されます。これにより、履歴カウントが無効になるため、ユーザはいつでも以前に使用していたパスワードを再利用できます。
ステップ 4	UCS-A /security/password-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、パスワード履歴カウントを設定し、トランザクションをコミットします。

```
UCS-A # scope security
UCS-A /security # scope password-profile
UCS-A /security/password-profile # set history-count 5
UCS-A /security/password-profile* # commit-buffer
UCS-A /security/password-profile #
```

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 Manager 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 または aaa 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、admin または aaa 権限を持つユーザに適用されません。

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使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 Manager は過去に使用されたパスワードを最大 15 個まで保存します。パスワード履歴カウントには最新のパスワードを先頭に、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使用できます。

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 9 番目のパスワードが期限切れになるまで最初のパスワードを再使用できません。

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、履歴のカウントを無効にし、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
[No password change allowed]	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
[Password changes allowed within change interval]	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

ローカル認証されたユーザのパスワード履歴のクリア

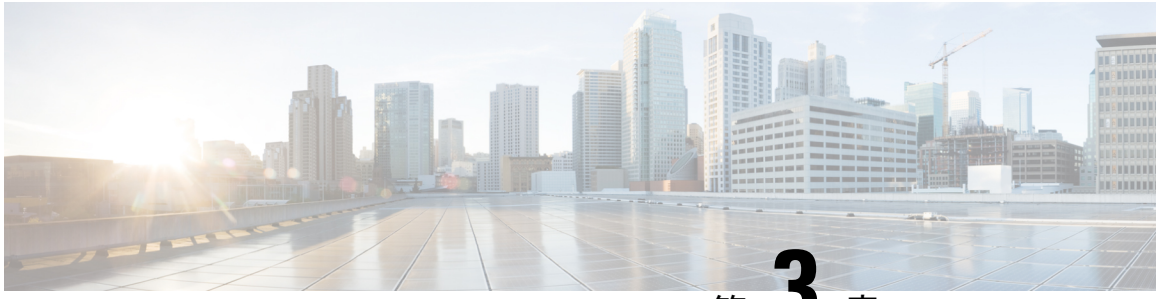
手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope local-user** *user-name*	指定されたユーザ アカウントに対するローカル ユーザ セキュリティ モードを開始します。
ステップ 3	UCS-A /security/local-user # **set clear password-history yes**	指定されたユーザアカウントのパスワード履歴をクリアします。
ステップ 4	UCS-A /security/local-user # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、パスワード履歴カウントを設定し、トランザクションをコミットします。

```
UCS-A # scope security
UCS-A /security # scope local-user admin
UCS-A /security/local-user # set clear password-history yes
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```



第 3 章

ロールベース アクセスの設定

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。

ユーザ アカウント Cisco UCS

ユーザ アカウントは、システムへのアクセスに使用します。Cisco UCS Manager ドメインごとに最大 48 個の ローカル ユーザ アカウントを構成できます。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。

ユーザ アカウントは、SSH 公開キーを付けて設定できます。公開キーは、OpenSSH と SECSH のいずれかの形式で設定できます。

管理者アカウント

Cisco UCS ドメイン にはそれぞれ、1 つの管理者アカウントが付随しています。管理者アカウントはデフォルト ユーザ アカウントであり、変更や削除はできません。このアカウントはシステム管理者またはスーパーユーザ アカウントであり、すべての権限が与えられています。admin 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ません。初期システムセットアップ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、ファブリック インターコネクトのを介して直接認証され、admin または aaa 権限の所有者によって有効または無効にできます。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。しかし無効になったローカル ユーザ アカウントの構成の詳細はデータベースから削除されません。無効にされた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、既存の構成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 アカウントとは、LDAP、RADIUS、または TACACS+ で認証されたユーザ アカウントです。

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により、リモート ユーザ アカウントに保持された値が上書きされます。

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。有効期限の時間になると、ユーザ 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を設定した後、「有効期限なし」に再設定することはできません。ただし、そのアカウントの有効期限切れになる日付を更新して設定することは可能です。

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 アカウントの Web セッション制限

Cisco UCS Manager は、Web セッション制限を使用して、あるユーザ アカウントに対してある時点で許容される Web セッション数（GUI と XML の両方）を制限します。

各 Cisco UCS Manager ドメインは、ユーザ 1 人につき同時 Web セッションを最大 32 件、合計 256 件のユーザ セッションをサポートします。デフォルトでは、Cisco UCS Managerが許容する同時 Web セッション数はユーザ 1 人あたり 32 に設定されます。ただし、この値を最大でシステム上限の 256 まで構成できます。

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 には、デフォルトのユーザ ロールを含めて最大 48 個のユーザ ロールを含めることができます。48 個目のユーザ 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。

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のユーザは、システム状態を変更することはできません。

ユーザは権限を作成したり、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。属性には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。

（注） ローカル ユーザ アカウントとリモート ユーザ アカウントが同じユーザ名である場合、Cisco UCS Manager は、リモート ユーザに割り当てられたロールをローカル ユーザに割り当てられたロールで上書きします。

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。

読み取り専用

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

次の語は、Cisco UCS でカスタム ロールを作成するときに使用できません。

- ネットワーク管理者
- 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 リソースにアクセスしたり、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、次の *URL* から入手可能な『 Privileges in Cisco UCS http://www.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html

表 *2:* ユーザの権限

権限	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

権限	説明	デフォルトのロール割り当て
ext-lan-config	外部 LAN 設定	ネットワークアドミニストレータ
ext-lan-policy	外部 LAN ポリシー	ネットワークアドミニストレータ
ext-lan-qos	外部 LAN QoS	ネットワークアドミニストレータ
ext-lan-security	外部 LAN セキュリティ	ネットワークアドミニストレータ
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
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	ネットワークアドミニストレータ
pod-policy	ポッド ポリシー	ネットワークアドミニストレータ
pod-qos	ポッド QoS	ネットワークアドミニストレータ
pod-security	ポッド セキュリティ	ネットワークアドミニストレータ
power-mgmt	電源管理操作に対する読み取りおよび書き込みアクセス権	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。	読み取り専用

権限	説明	デフォルトのロール割り当て
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	ネットワークアドミニストレータ
service-profile-network-policy	サービス プロファイル ネットワーク ポリシー	ネットワークアドミニストレータ
service-profile-qos	サービス プロファイル QoS	ネットワークアドミニストレータ
service-profile-qos-policy	サービス プロファイル QoS ポリシー	ネットワークアドミニストレータ
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

権限	説明	デフォルトのロール割り当て
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

ユーザ ロールの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **create role** *name*	ユーザ ロールを作成し、セキュリティ ロール モードを開始します。
ステップ 3	UCS-A /security/role # **add privilege** *privilege-name*	ロールに 1 つ以上の権限を追加します。 （注） 複数の *privilege-name* を同じコマンドラインに指定してロールに複数の権限を追加することも、複数の **add** コマンドを使用して同じロールに複数の権限を追加することもできます。
ステップ 4	UCS-A /security/role # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、service-profile-security-admin ロールを作成し、ロールにサービス プロファイル セキュリティおよびサービス プロファイル セキュリティ ポリシー権限を追加し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # create role ls-security-admin
UCS-A /security/role* # add privilege service-profile-security
service-profile-security-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

ユーザ ロールへの権限の追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope role** *name*	指定したロールに対するセキュリティ ロール モードを開始します。
ステップ 3	UCS-A /security/role # **add privilege** *privilege-name*	ユーザ ロールの既存の権限に 1 つ以上の権限を追加します。 （注） 複数の *privilege-name* を同じコマンドラインに指定してロールに複数の権限を追加することも、複数の **add privilege** コマンドを使用して同じロールに複数の権限を追加することもできます。
ステップ 4	UCS-A /security/role # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、service-profile-security-admin ロールにサーバ セキュリティ権限とサーバ ポリシー権限を追加し、トランザクションをコミットする方法を示します。

```
UCS-A# scope security
UCS-A /security # scope role service-profile-security-admin
UCS-A /security/role # add privilege server-security server-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

ユーザ ロールの権限の置換

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ 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	UCS-A /security # **scope role** *name*	指定したロールに対するセキュリティ ロール モードを開始します。
ステップ 3	UCS-A /security/role # **set privilege** *privilege-name*	ユーザ ロールの既存の権限を置き換えます。 （注） 同じコマンド ラインで複数の *privilege-name* を指定することで、既存の権限を複数の権限に置換できます。権限を置換した後、**add privilege** コマンドを使用して同じロールに権限を追加できます。
ステップ 4	UCS-A /security/role # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、service-profile-security-admin ロール用の既存の権限をサーバ セキュリティおよびサーバ ポリシー権限に置き換え、トランザクションをコミットする方法を示します。

```
UCS-A# scope security
UCS-A /security # scope role service-profile-security-admin
UCS-A /security/role # set privilege server-security server-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

ユーザ ロールからの権限の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope role** *name*	指定したロールに対するセキュリティ ロール モードを開始します。
ステップ 3	UCS-A /security/role # **remove privilege** *privilege-name*	既存のユーザ ロール権限から 1 つ以上の権限を削除します。

	コマンドまたはアクション	目的
		（注） 同じコマンド ラインで複数の *privilege-name* を指定することで、複数の権限をロールから削除できます。または、複数の **remove privilege** コマンドを使用することで、同じロールから権限を削除できます。
ステップ 4	UCS-A /security/role # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、service-profile-security-admin ロールからサーバ セキュリティ権限とサーバ ポリシー権限を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope role service-profile-security-admin
UCS-A /security/role # remove privilege server-security server-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

ユーザ ロールの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **delete role** *name*	ユーザ ロールを削除します。
ステップ 3	UCS-A /security # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、service-profile-security-admin ロールを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # delete role service-profile-security-admin
UCS-A /security* # commit-buffer
UCS-A /security #
```

ロケール

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。アクセスは通常、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。

1 つの Cisco UCS ドメイン には、最大 48 個のユーザ ロケールを含めることができます。48 個目のユーザ ロ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。

admin または aaa 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のみに制限されます。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） 次の権限の 1 つ以上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。

- 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。

ロケールの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ 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	UCS-A /security # **create locale** *locale-name*	ロケールを作成し、セキュリティ ロケール モードを開始します。
ステップ 3	UCS-A /security/locale # **create org-ref** *org-ref-name* **orgdn** *orgdn org-root/org-ref-name*	ロケールに組織を参照（バインド）します。*org-ref-name* 引数は組織参照の識別に使用される名前で、*orgdn-name* 引数は参照されている組織の識別名です。
ステップ 4	UCS-A /security/locale # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、western ロケールを作成し、そのロケールに財務組織を参照し、参照に finance-ref という名前を指定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # create locale western
UCS-A /security/locale* # create org-ref finance-ref orgdn org-root/org-finance
UCS-A /security/locale* # commit-buffer
UCS-A /security/locale #
```

ロケールへの組織の割り当て

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A# **scope locale** *locale-name*	セキュリティ ロケール モードを開始します。
ステップ 3	UCS-A /security/locale # **create org-ref** *org-ref-name* **orgdn** *org-root/org-ref-name*	ロケールに組織を参照（バインド）します。*org-ref-name* 引数は組織参照の識別に使用される名前で、*orgdn-name* 引数は参照されている組織の識別名です。
ステップ 4	UCS-A /security/locale # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、western ロケールに入り、そのロケールに marketing 組織を追加（参照）し、参照に marketing-ref という名前を指定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope locale western
UCS-A /security/locale* # create org-ref marketing-ref orgdn org-root/org-marketing
UCS-A /security/locale* # commit-buffer
UCS-A /security/locale #
```

ロケールからの組織の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope locale** *locale-name*	セキュリティ ロケール モードを開始します。
ステップ 3	UCS-A /security/locale # **delete org-ref** *org-ref-name*	ロケールから組織を削除します。
ステップ 4	UCS-A /security/locale # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、western ロケールから finance 組織を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope locale western
UCS-A /security/locale # delete org-ref finance-ref
UCS-A /security/locale* # commit-buffer
UCS-A /security/locale #
```

ロケールの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **delete locale** *locale-name*	ロケールを削除します。
ステップ 3	UCS-A /security # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、western ロケールを削除し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # delete locale western
UCS-A /security* # commit-buffer
UCS-A /security #
```

ローカル認証されたユーザ アカウント

ユーザ アカウントの作成

少なくとも、次のユーザを作成することを推奨します。

- サーバ アドミニストレータ アカウント
- ネットワーク アドミニストレータ アカウント
- ストレージ アドミニストレータ

始める前に

システムに次のいずれかがある場合は、該当するタスクを実行します。

- リモート認証サービス：ユーザがリモート認証サーバに存在すること、および適切なロールと権限を持っていることを確認します。
- 組織のマルチテナント機能：1 つ以上のロケールを作成します。ロケールが 1 つもない場合、すべてのユーザはルートに作成され、すべての組織のロールと権限が割り当てられます。
- SSH 認証：SSH キーを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **create local-user** *local-user-name*	指定したローカルユーザのユーザアカウントを作成し、セキュリティローカル ユーザ モードを開始します。
ステップ 3	UCS-A /security/local-user # **set account-status** {**active**| **inactive**}	ローカルユーザアカウントを有効にするか、無効にするかを指定します。

	コマンドまたはアクション	目的
		ローカルユーザアカウントのアカウントステータスが非アクティブに設定された場合、ユーザは既存のクレデンシャルを使用してシステムにログインできません。
ステップ 4	UCS-A /security/local-user # **set password** *password*	ユーザアカウントのパスワードを設定します
ステップ 5	（任意） UCS-A /security/local-user # **set firstname** *first-name*	ユーザの名前を指定します。
ステップ 6	（任意） UCS-A /security/local-user # **set lastname** *last-name*	ユーザの姓を指定します。
ステップ 7	（任意） UCS-A /security/local-user # **set expiration** *month day-of-month year*	ユーザアカウントが期限切れになる日付を指定します。*month* 引数は、月の英名の最初の 3 文字です。 （注） ユーザアカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。ただし、そのアカウントの有効期限切れになる日付を更新して設定することは可能です。
ステップ 8	（任意） UCS-A /security/local-user # **set email** *email-addr*	ユーザの電子メールアドレスを指定します。
ステップ 9	（任意） UCS-A /security/local-user # **set phone** *phone-num*	ユーザの電話番号を指定します。
ステップ 10	（任意） UCS-A /security/local-user # **set sshkey** *ssh-key*	パスワードレスアクセス用の SSH キーを指定します。
ステップ 11	UCS-A security/local-user # **commit-buffer**	トランザクションをコミットします。

例

次の例は、kikipopo という名前のユーザ アカウントを作成し、ユーザ アカウントを有効にし、foo12345 にパスワードを設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # create local-user kikipopo
UCS-A /security/local-user* # set account-status active
UCS-A /security/local-user* # set password
Enter a password:
```

```
Confirm the password:
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

次の例は、lincey という名前のユーザ アカウントを作成し、ユーザ アカウントを有効にし、パスワードレス アクセス用の OpenSSH キーを設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # create local-user lincey
UCS-A /security/local-user* # set account-status active
UCS-A /security/local-user* #  set sshkey "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4K
iaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpD
m8HPh2LOgyH7Ei1MI8="
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

次の例は、jforlenz という名前のユーザ アカウントを作成し、ユーザ アカウントを有効にし、パスワードレスアクセス用のセキュアSSHキーを設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # create local-user jforlenz
UCS-A /security/local-user* # set account-status active
UCS-A /security/local-user* #  set sshkey
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
User's SSH key:
> ---- BEGIN SSH2 PUBLIC KEY ----
>AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw8
>5lkdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VO
>IEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8=
> ---- END SSH2 PUBLIC KEY ----
> ENDOFBUF
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

ローカル認証されたユーザへのパスワード強度チェックの有効化

パスワードの強度確認を有効にするには、admin または aaa 権限が必要です。有効になっている場合、Cisco UCS Manager では、強力なパスワードのガイドラインを満たさないパスワードを選択できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **enforce-strong-password** {**yes** | **no**}	パスワードの強度確認を有効にするか、無効にするかを指定します。

例

次に、パスワード強度チェックを有効にする例を示します。

```
UCS-A# scope security
UCS-A /security # set enforce-strong-password yes
UCS-A /security #
```

ユーザ アカウントの Web セッション制限の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **scope web-session-limits**	システム サービス Web セッション制限モードを開始します。
ステップ 4	UCS-A /system/services/web-session-limits # **set peruser** *num-of-logins-per-user*	各ユーザに許可する同時 HTTP および HTTPS セッションの最大数を設定します。 1 ～ 256 の整数を入力します。デフォルトでは 32 に設定されます。
ステップ 5	UCS-A /system/services/web-session-limits # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、各ユーザ アカウントに許可する HTTP および HTTPS セッションの最大数を 60 に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # scope web-session-limits
UCS-A /system/services/web-session-limits* # set peruser 60
UCS-A /system/services/web-session-limits* # commit-buffer
UCS-A /system/services/web-session-limits #
```

ユーザ アカウントへのロールの割り当て

ユーザ ロールおよび権限の変更は次回のユーザ ログイン時に有効になります。ユーザがログインしているときにユーザアカウントに対して新しいロールを割り当てたり既存のロールを削

除したりする場合、アクティブなセッションでは以前のロールや権限が引き続き使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope local-user** *local-user-name*	指定したローカル ユーザ アカウントに対するセキュリティ ローカル ユーザ モードを開始します。
ステップ 3	UCS-A /security/local-user # **create role** *role-name*	指定したロールをユーザ アカウントに割り当てます。 （注） **create role** コマンドは、1 つのユーザ アカウントに複数のロールを割り当てるために複数回入力できます。
ステップ 4	UCS-A security/local-user # **commit-buffer**	トランザクションをコミットします。

例

次の例では、ローカル ユーザ アカウント kikipopo に operations ロールを割り当て、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # create role operations
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

ユーザ アカウントへのロケールの割り当て

（注） admin または aaa ロールを持つユーザにロケールを割り当てないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ 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	UCS-A /security # **scope local-user** *local-user-name*	指定したローカル ユーザ アカウントに対するセキュリティ ローカル ユーザ モードを開始します。
ステップ 3	UCS-A /security/local-user # **create locale** *locale-name*	指定したロケールをユーザ アカウントに割り当てます。 （注） **create locale** コマンドは、1 つのユーザ アカウントに複数のロケールを割り当てるために複数回入力できます。
ステップ 4	UCS-A security/local-user # **commit-buffer**	トランザクションをコミットします。

例

次の例では、ローカルユーザ アカウント kikipopo に西洋言語ロケールを割り当て、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # create locale western
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

ユーザ アカウントからのロールの削除

ユーザ ロールおよび権限の変更は次回のユーザ ログイン時に有効になります。ユーザがログインしているときにユーザアカウントに対して新しいロールを割り当てたり既存のロールを削除したりする場合、アクティブなセッションでは以前のロールや権限が引き続き使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope local-user** *local-user-name*	指定したローカル ユーザ アカウントに対するセキュリティ ローカル ユーザ モードを開始します。
ステップ 3	UCS-A /security/local-user # **delete role** *role-name*	指定したロールをユーザ アカウントから削除します。

	コマンドまたはアクション	目的
		（注） **delete role** コマンドは、あるユーザ アカウントから複数のロールを削除するために複数回入力できます。
ステップ 4	UCS-A security/local-user # **commit-buffer**	トランザクションをコミットします。

例

次に、kikipopo というローカル ユーザ アカウントから operations ロールを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # delete role operations
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

ユーザ アカウントからのロケールの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope local-user** *local-user-name*	指定したローカル ユーザ アカウントに対するセキュリティ ローカル ユーザ モードを開始します。
ステップ 3	UCS-A /security/local-user # **delete locale** *locale-name*	指定したロケールをユーザ アカウントから削除します。 （注） **delete locale** コマンドは、あるユーザ アカウントから複数のロケールを削除するために複数回入力できます。
ステップ 4	UCS-A security/local-user # **commit-buffer**	トランザクションをコミットします。

例

次に、kikipopo というローカル ユーザ アカウントから western ロケールを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # delete locale western
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

ユーザ アカウントの有効化または無効化

ローカル ユーザ アカウントを有効または無効にするには、admin または aaa 権限が必要です。

始める前に

ローカル ユーザ アカウントを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope local-user**	ローカル ユーザ セキュリティ モードを開始します。
ステップ 3	UCS-A /security/local-user # **set account-status** {**active** | **inactive**}	ローカル ユーザ アカウントを有効にするか、無効にするかを指定します。 admin ユーザ アカウントは常にアクティブに設定されます。変更はできません。 （注） アカウント ステータスを非アクティブに設定しても、データベースからコンフィギュレーションは削除されません。

例

次に、accounting というローカル ユーザ アカウントを有効にする例を示します。

```
UCS-A# scope security
UCS-A /security # scope local-user accounting
UCS-A /security/local-user # set account-status active
```

ユーザ アカウントの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **delete local-user** *local-user-name*	ローカル ユーザ アカウントを削除します。
ステップ 3	UCS-A /security # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、foo というユーザ アカウントを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # delete local-user foo
UCS-A /security* # commit-buffer
UCS-A /security #
```

CLI からのユーザ セッションのモニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **show user-session** {**local** | **remote**} [**detail**]	システムにログインしているすべてのユーザのセッション情報を表示します。セッション ID の横のアスタリスク（*）は、現在のログイン セッションを示します。

例

次に、システムにログインしているすべてのローカルユーザのリストを表示する例を示します。アスタリスクは、どのセッションが現在のログインセッションであるかを示します。

```
UCS-A# scope security
UCS-A /security # show user-session local
```

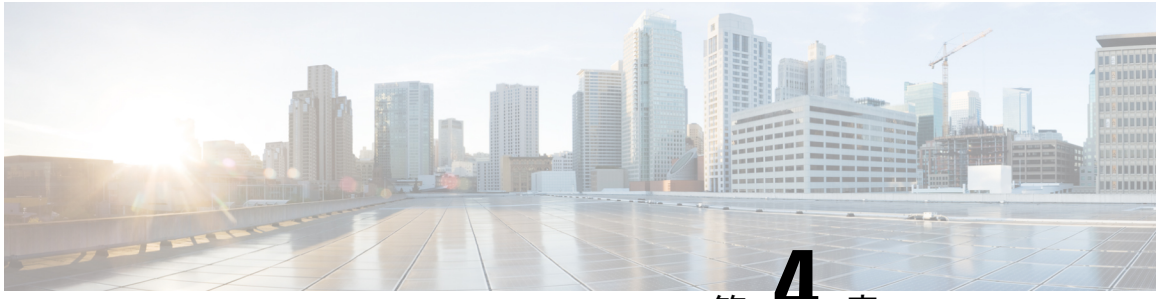
```
Session Id      User            Host                  Login Time
--------------- --------------- -------------------- ----------
pts_25_1_31264*  steve           192.168.100.111      2009-05-09T14:06:59
ttyS0_1_3532    jeff            console              2009-05-02T15:11:08
web_25277_A     faye            192.168.100.112      2009-05-15T22:11:25
```

次に、システムにログインしているすべてのローカル ユーザの詳細情報を表示する例を示します。

```
UCS-A# scope security
UCS-A /security # show user-session local detail
Session Id pts_25_1_31264:
    Fabric Id: A
    Term: pts/25
    User: steve
    Host: 64.101.53.93
    Pid: 31264
    Login Time: 2009-05-09T14:06:59

Session Id ttyS0_1_3532:
    Fabric Id: A
    Term: ttyS0
    User: jeff
    Host: console
    Pid: 3532
    Login Time: 2009-05-02T15:11:08

Session Id web_25277_A:
    Fabric Id: A
    Term: web_25277
    User: faye
    Host: 192.168.100.112
    Pid: 3518
    Login Time: 2009-05-15T22:11:25
```



第 4 章

リモート認証

認証サービス

Cisco UCS では、ユーザ ログインを認証するための次の 2 つの方法をサポートしています。

- ローカル ユーザ認証：ローカルの Cisco UCS Manager に存在するユーザ アカウントを使用します。
- リモート ユーザ認証：次のプロトコルのいずれかを使用します。
  - LDAP
  - RADIUS
  - TACACS+

リモート認証プロバイダ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を作成して、Cisco UCS Manager がそのシステムと通信できるようにする必要があります。ユーザ認証に影響する注意事項は次のとおりです。

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 Manager にローカルに設定したり、リモート認証サーバに設定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 Manager GUIと Cisco UCS Manager 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 Manager 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 Manager 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。

リモート認証プロバイダのユーザ属性

RADIUS および TACACS+ 構成では、ユーザが Cisco UCS Manager へのログインに使用する各リモート認証プロバイダに Cisco UCS 用のユーザ属性を設定する必要があります。このユーザ属性には、各ユーザに割り当てられたロールとロケールが含まれています。

（注） この手順は、LDAP グループ マッピングを使用してロールとロケールを割り当てる LDAP 設定では必要ありません。

ユーザがログインすると、Cisco UCS Manager 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. ユーザが有効である場合は、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。

次の表は、Cisco UCS でサポートしているリモート認証プロバイダ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によるユーザ属性の比較

認証プロバイダ	カスタム属性	スキーマの拡張	属性 ID 要件
LDAP	グループ マッピング使用時は不要 グループ マッピング不使用時は任意	オプション。次のいずれかを実行するよう選択できます。 • 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する。 • 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する。	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、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します サンプルの OID が次のセクションに示されています。
RADIUS	任意	オプション。次のいずれかを実行するよう選択できます。 • 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する方法を示しています。`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	カスタム属性	スキーマの拡張	属性 ID 要件
TACACS+	必須	必須です。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する方法を示しています。 `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
```

Two-Factor Authentication

Cisco UCS Manager では、リモート ユーザのログインに二要素認証を使用して、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。二要素認証のログインでは、パスワード

フィールドでユーザ名、トークン、パスワードの組み合わせが必要です。PIN、証明書、またはトークンを指定できます。

二要素認証では、認証アプリケーションを使用します。このアプリケーションはトークン サーバを保持して、ログイン プロセス中にユーザ用のワンタイム トークンを生成し、パスワードを AAA サーバに保存します。ベンダー固有の属性を取得する要求がトークン サーバに送信されます。Cisco UCS Manager は、トークン サーバが AAA サーバと統合されていることを想定するので、AAA サーバに要求を転送します。パスワードとトークンは、AAA サーバによって同時に検証されます。ユーザは、AAA サーバで設定されているのと同じ順序で、トークンとパスワードを入力する必要があります。

二要素認証は、RADIUS または TACACS+ プロバイダ グループを指定認証ドメインに関連付け、それらのドメインで二要素認証を有効にすることによってサポートされます。二要素認証では IPM をサポートしておらず、また認証レルムが LDAP、local、または none に設定されている場合はサポートされません。

Web セッションの更新および Web セッションのタイムアウト期限

[Web Session Refresh Period] は、Cisco UCS Manager GUI の Web セッションに対する更新要求間隔に許容される最大時間です。[Web Session Timeout] は、最後の更新要求後から Cisco UCS Manager GUI の Web セッションが非アクティブになるまでの最大経過時間です。

[Web Session Refresh Period] を 60 秒より長く、最大で 172800 秒まで長くすると、トークンとパスワードを繰り返し生成および再入力する必要があるセッション タイムアウトが頻繁に起きるのを避けることができます。デフォルト値は、二要素認証が有効の場合は 7200 秒、二要素認証が有効でない場合は 600 秒です。

[Web Session Timeout Period] には 300 から 172800 の間の値を指定できます。デフォルト値は、二要素認証が有効の場合は 8000 秒、二要素認証が有効でない場合は 7200 秒です。

LDAP プロバイダとグループ

ネストされた LDAP グループ

LDAP グループを別のグループのメンバーとして追加し、グループをネストすることで、グループ メンバーのアカウントを統合してレプリケーション トラフィックを削減できます。Cisco UCS Manager リリース 2.1(2) 以降では、LDAP グループ マップで定義されている別のグループに含まれるネストされた LDAP グループを検索できます。

（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。

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きに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 のみを選択します。Group_1 と Group_2 を別々に検索する必要はありません。

Cisco UCS Manager のグループ マップでサブグループを常に作成する必要がなくなります。

LDAP グループ ルール

LDAP グループ ルールによって、ユーザ ロールおよびロケールをリモート ユーザに割り当てるときに Cisco UCS が LDAP グループを使用するかどうかが決まります。

LDAP プロバイダのプロパティの設定

このタスクで設定するプロパティは、Cisco UCS Manager で定義されたこのタイプのすべてのプロバイダ接続のデフォルト設定です。個々のプロバイダにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS でその設定が使用され、デフォルト設定は無視されます。

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Cisco UCS にバインドするユーザ アカウントを作成します。このアカウントには、期限切れにならないパスワードを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **set attribute** *attribute*	指定された属性を含むレコードにデータベース検索を限定します。
ステップ 4	UCS-A /security/ldap # **set basedn** *distinguished-name*	指定された識別名を含むレコードにデータベース検索を限定します。
ステップ 5	UCS-A /security/ldap # **set filter** *filter*	指定されたフィルタを含むレコードにデータベース検索を限定します。
ステップ 6	（任意） UCS-A /security/ldap # **set timeout** *seconds*	システムがサーバをダウン状態として通知する前に、LDAP サーバからの応答を待つ時間間隔を設定します。
ステップ 7	UCS-A /security/ldap # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、LDAP 属性を CiscoAvPair に、ベース識別名を「DC=cisco-ucsm-aaa3,DC=qalab,DC=com」に、フィルタを sAMAccountName=$userid、タイムアウト間隔を 5 秒に設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # set attribute CiscoAvPair
UCS-A /security/ldap* # set basedn "DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap* # set filter sAMAccountName=$userid
UCS-A /security/ldap* # set timeout 5
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

（注） ユーザ ログインは、LDAP ユーザの userdn が 255 文字を超えると失敗します。

次のタスク

LDAP プロバイダを作成します。

LDAP プロバイダの作成

Cisco UCS Manager は最大 16 の LDAP プロバイダをサポートします。

始める前に

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Cisco UCS にバインドするユーザ アカウントを作成します。このアカウントには、期限切れにならないパスワードを設定します。

- LDAP サーバで、次のいずれかの設定を行います。
  - LDAP グループを設定します。LDAP グループには、ユーザのロールとロケール情報が含まれています。
  - Cisco UCS Manager のユーザ ロールとロケール情報を保持する属性でユーザを設定します。この属性について LDAP スキーマを拡張するかどうかを選択できます。スキーマを拡張しない場合は、既存の LDAP 属性を使用して Cisco UCS ユーザ ロールとロケールを保持します。スキーマを拡張する場合は、CiscoAVPair 属性などの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、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します
  - クラスタ設定では、両方のファブリック インターコネクトに対する管理ポートの IPv4 または IPv6 アドレスを追加します。この設定では、1 つ目のファブリック インター

コネクトで障害が発生し、システムが2つ目のファブリックインターコネクトにフェールオーバーしても、リモートユーザは引き続きログインできることが保証されます。ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager で使用される仮想 IPv4 または IPv6 アドレスからではありません。

- セキュア通信を使用するには、Cisco UCS Manager で LDAP サーバのルート認証局（CA）の証明書を含むトラスト ポイントを作成します。
- LDAP プロバイダを変更したり、追加または削除したりする必要がある場合は、ドメイン認証レルムをローカルに変更し、プロバイダに変更を加えた後、ドメイン認証レルムを LDAP に戻す必要があります。
- Active Directory バインド識別名の属性を定義する際に次の表にある特殊文字を使用する場合、対応する文字の 16 進数値の後にバックスラッシュ（\）を使用して、特殊文字をエスケープ文字で置き換える必要があります。

特殊文字	説明	16 進数値
,	カンマ	0x2C
+	プラス記号	0x2B
"	二重引用符	0x22
\	バックスラッシュ	0x5C
<	左角ブラケット	0x3C
>	右角ブラケット	0x3E
;	セミコロン	0x3B
LF	改行	0×0A
CR	復帰	0x0D
=	等号	0x3D
/	スラッシュ	0x2F

https://msdn.microsoft.com/en-us/library/aa366101 に特殊文字をエスケープ文字と 16 進数値に置き換える方法についての説明があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ 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	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **create server** *server-name*	LDAP サーバインスタンスを作成し、セキュリティ LDAP サーバモードを開始します。SSL が有効の場合、*server-name* は、通常 IP アドレスまたは FQDN となり、LDAP サーバのセキュリティ証明書内の Common Name（CN）と正確に一致している必要があります。IP アドレスが指定されている場合を除き、DNS サーバは Cisco UCS Manager で設定する必要があります。
ステップ 4	（任意） UCS-A /security/ldap/server # **set attribute** *attr-name*	ユーザロールとロケールの値を保管する LDAP 属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザレコードで、この属性名と一致する値を検索します。 LDAP スキーマを拡張しない場合、既存の未使用 LDAP 属性を Cisco UCS ロールとロケールに設定できます。あるいは、属性 ID「`1.3.6.1.4.1.9.287247.1`」を持つ、CiscoAVPair という名前の属性をリモート認証サービスに作成できます。 デフォルトの属性が LDAP の [General] タブで設定されていない場合は、この値が必要です。
ステップ 5	（任意） UCS-A /security/ldap/server # **set basedn** *basedn-name*	リモートユーザがログインし、システムがそのユーザ名に基づいてユーザの DN の取得を試みるときに、サーバが検索を開始する LDAP 階層内の特定の識別名。ベース DN の長さは、最大 255 文字から CN= username の長さを差し引いた長さに設定することができます。ここで、username は、LDAP 認証を使用して Cisco UCS Manager へアクセスしようとしているリモートユーザの識別に使用されます。

	コマンドまたはアクション	目的
		デフォルトのベース DN が LDAP の [General] タブで設定されていない場合は、この値が必要です。
ステップ 6	（任意） UCS-A /security/ldap/server # **set binddn** *binddn-name*	ベース DN のすべてのオブジェクトに対する読み取り権限と検索権限を持つ、LDAP データベース アカウントの識別名（DN）。 サポートされるストリングの最大長は 255 文字（ASCII）です。
ステップ 7	（任意） UCS-A /security/ldap/server # **set filter** *filter-value*	LDAP 検索は、定義したフィルタと一致するユーザ名に限定されます。 デフォルトのフィルタが LDAP の [General] タブで設定されていない場合は、この値が必要です。
ステップ 8	必須: UCS-A /security/ldap/server # **set password**	[Bind DN] フィールドで指定した LDAP データベース アカウントのパスワード。標準 ASCII 文字を入力できます。ただし、「§」（セクション記号）、「?」（疑問符）、「=」（等号）は除きます。 パスワードを設定するには、 **set password** コマンドを入力してから **Enter** を押し、プロンプトでキー値を入力します。
ステップ 9	（任意） UCS-A /security/ldap/server # **set order** *order-num*	Cisco UCS でユーザーの認証にこのプロバイダを使用する順序。
ステップ 10	（任意） UCS-A /security/ldap/server # **set port** *port-num*	Cisco UCS が LDAP データベースと通信するために使用されるポート。標準ポート番号は 389 です。
ステップ 11	UCS-A /security/ldap/server # **set ssl** {**yes** **no**}	LDAP サーバと通信するときの暗号化の使用を有効または無効にします。オプションは次のとおりです。 • **yes** ：暗号化が必要です。暗号化をネゴシエートできない場合は、接続に失敗します。 有効にしている場合は、ポートを 636 に変更せず、389 のままにして

	コマンドまたはアクション	目的
		ください。Cisco UCS は、SSL 用のポート 636 で TLS セッションをネゴシエートしますが、初期接続は暗号化されない状態で 389 で開始されます。 • **no**：暗号化は無効です。認証情報はクリアテキストとして送信されます。 LDAP では STARTTLS が使用されます。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。
ステップ 12	UCS-A /security/ldap/server # **set timeout** *timeout-num*	LDAP データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力するか、0（ゼロ）を入力して LDAP の [General] で指定したタイムアウト値を使用します。デフォルトは 30 秒です。
ステップ 13	UCS-A /security/ldap/server # **set vendor** *{ms-ad | openldap}*	LDAP サーバのネストされた LDAP グループ検索機能の使用を有効または無効にします。オプションは次のとおりです。 • **ms-ad**：ネストされた LDAP グループ検索は、このオプションでサポートされます。ベンダーを *ms-ad*（Microsoft Active Directory）に設定し、*ldap-group-rule* を有効にして recursive に設定すると、Cisco UCS Manager はネストされた LDAP グループを検索できます。 • **openldap**：ネストされた LDAP グループ検索は、このオプションでサポートされません。ベンダーを *openldap* に設定し、*ldap-group-rule* を有効にして recursive に設定すると、Cisco UCS Manager はネストされた LDAP グループを検索しません。このオプションを選択すると、親グループがグループ マップにすでに設定されていても、Cisco

	コマンドまたはアクション	目的
		UCS Manager で LDAP グループマップとして各 LDAP サブグループを作成する必要があります。 （注） Cisco UCS Manager を旧バージョンからリリース 2.1(2) にアップグレードすると、LDAP プロバイダのベンダー属性は **openldap** にデフォルトで設定され、LDAP 認証が正常に機能し続けます。
ステップ 14	UCS-A /security/ldap/server # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、10.193.169.246 という名前の LDAP サーバインスタンスを作成し、binddn、パスワード、順序、ポート、SSL、ベンダー属性を設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap* # create server 10.193.169.246
UCS-A /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap/server* # set password
Enter the password:
Confirm the password:
UCS-A /security/ldap/server* # set order 2
UCS-A /security/ldap/server* # set port 389
UCS-A /security/ldap/server* # set ssl yes
UCS-A /security/ldap/server* # set timeout 30
UCS-A /security/ldap/server* # set vendor ms-ad
UCS-A /security/ldap/server* # commit-buffer
UCS-A /security/ldap/server #
```

次の例では、12:31:71:1231:45b1:0011:011:900 という名前の LDAP サーバインスタンスを作成し、binddn、パスワード、順序、ポート、SSL、ベンダー属性を設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap* # create server 12:31:71:1231:45b1:0011:011:900
UCS-A /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap/server* # set password
Enter the password:
Confirm the password:
UCS-A /security/ldap/server* # set order 1
UCS-A /security/ldap/server* # set port 389
UCS-A /security/ldap/server* # set ssl yes
```

```
UCS-A /security/ldap/server* # set timeout 45
UCS-A /security/ldap/server* # set vendor ms-ad
UCS-A /security/ldap/server* # commit-buffer
UCS-A /security/ldap/server #
```

次のタスク

単一のLDAPデータベースが関係する実装の場合、認証サービスとしてLDAPを選択します。

複数の LDAP データベースが関係する実装の場合は、LDAP プロバイダ グループを設定します。

LDAP プロバイダの LDAP グループ ルールの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **scope server** *ldap-provider*	セキュリティ LDAP プロバイダ モードを開始します。
ステップ 4	UCS-A /security/ldap/server # **scope ldap-group-rule**	LDAP グループ ルール モードを開始します。
ステップ 5	UCS-A /security/ldap/server/ldap-group-rule # **set authorization** {**enable** | **disable**}	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、Cisco UCS が LDAP グループを検索するかを指定します。 • **disable**：Cisco UCS はどの LDAP グループにもアクセスしません。 • **enable**：Cisco UCS はこの Cisco UCS ドメイン 内にマッピングされた LDAP プロバイダ グループを検索します。リモート ユーザが見つかると、Cisco UCS は関連する LDAP グループ マップでその LDAP グループに対して定義されているユーザ ロールとロケールを割り当てます。

	コマンドまたはアクション	目的
		（注） ロールとロケールの割り当ては累積されます。ユーザが複数のグループに含まれる、または LDAP 属性で指定されたロールやロケールがある場合、Cisco UCS はそのユーザに対し、それらのグループや属性のいずれかにマッピングされたすべてのロールとロケールを割り当てます。
ステップ 6	UCS-A /security/ldap/server/ldap-group-rule # **set member-of-attribute** *attr-name*	Cisco UCS が LDAP データベースのグループ メンバーシップを決定するのに使用する属性。 サポートされるストリングの長さは 63 文字です。デフォルトの文字列は「**memberOf**」です。
ステップ 7	UCS-A /security/ldap/server/ldap-group-rule # **set traversal** {**non-recursive** | **recursive**}	必要に応じて Cisco UCS がグループ メンバの親グループの設定を使用するかどうか指定します。ここに表示される値は次のとおりです。 • **non-recursive**：Cisco UCS はユーザが属するグループだけを検索します。 • **recursive**：Cisco UCS はユーザが属する継承元グループすべてを検索します。
ステップ 8	UCS-A /security/ldap/server/ldap-group-rule # **set use-primary-group** {**yes** | **no**}	プライマリ グループをメンバーシップの検証のために Cisco UCS ドメイン 内の LDAP グループ マップとして設定します。Cisco UCS Manager を有効にして、ユーザのプライマリ グループ メンバーシップをダウンロードして検証することができます。
ステップ 9	UCS-A /security/ldap/server/ldap-group-rule # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、権限を有効にするLDAPグループルールを設定し、属性のメンバをmemberOfに設定し、traversalをnon-recursiveに設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # scope server ldapprovider
UCS-A /security/ldap/server # scope ldap-group-rule
UCS-A /security/ldap/server/ldap-group-rule # set authorization enable
UCS-A /security/ldap/server/ldap-group-rule* # set member-of-attribute memberOf
UCS-A /security/ldap/server/ldap-group-rule* # set traversal non-recursive
UCS-A /security/ldap/server/ldap-group-rule* # set use-primary-group yes
UCS-A /security/ldap/server/ldap-group-rule* # commit-buffer
UCS-A /security/ldap/server/ldap-group-rule #
```

LDAP プロバイダの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **delete server** *serv-name*	指定したサーバを削除します。
ステップ 4	UCS-A /security/ldap # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、ldap1という名前のLDAPサーバを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # delete server ldap1
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

LDAP グループ マッピング

LDAPグループマッピングを使用すると、LDAPユーザオブジェクトの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。LDAPデータベースへのアクセスを制限するLDAPグ

ループを使用している組織にログインする際、UCSM はグループ メンバーシップ情報を使用してロールとロケールを LDAP ユーザに割り当てます。

ユーザが Cisco UCS Manager にログインすると、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が取得されます。ロールとロケールの条件がポリシー内の情報と一致すれば、アクセス権が付与されます。リリース バージョンに応じて、Cisco UCS Manager では最大 28 個、128 個、または 160 個の LDAP グループ マップをサポートしています。

（注） Cisco UCS Manager リリース 3.1 (1) では最大 128 個の LDAP グループ マップ、リリース 3.1 (2) 以降では最大 160 個の LDAP グループ マップがサポートされます。

Cisco UCS Manager でローカルに構成したロールとロケールの定義が、LDAP ディレクトリの変更に応じて自動的に更新されることはありません。LDAP ディレクトリ内の LDAP グループを削除または名前変更するときには、その変更が反映されるよう Cisco UCS Manager も更新する必要があります。

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
- ロールとロケールの両方

たとえば、特定の場所のサーバ管理者グループを表す LDAP グループがあるとします。LDAP グループ マップには、サーバ プロファイルやサーバ機器などのユーザ ロールが含まれていることもあります。特定の場所のサーバ管理者へのアクセスを制限するために、ロケールに特定のサイト名を設定することができます。

（注） Cisco UCS Manager には、すぐに使用可能な多くのユーザ 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。LDAP プロバイダ グループをロケールにマッピングするには、カスタム ロケールを作成する必要があります。

LDAP グループ マップの作成

始める前に

- LDAP サーバで LDAP グループを作成します。
- LDAP サーバで LDAP グループの識別名を設定します。
- Cisco UCS Manager でロケールを作成します（任意）。
- Cisco UCS Manager でカスタム ロールを作成します（任意）。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **create ldap-group** *group-dn*	指定した DN 用の LDAP グループ マップを作成します。 グループ DN の最大文字数は 240 です。 （注） このコマンドに特殊文字を入力する場合は、特殊文字の前にエスケープ文字 \\（バックスラッシュ 2 個）を付ける必要があります。
ステップ 4	UCS-A /security/ldap/ldap-group # **create locale** *locale-name*	指定されたロケールに LDAP グループをマッピングします。
ステップ 5	UCS-A /security/ldap/ldap-group # **create role** *role-name*	指定されたロールに LDAP グループをマッピングします。
ステップ 6	UCS-A /security/ldap/ldap-group # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、DN に LDAP グループをマッピングし、ロケールを pacific に設定し、ロールを admin に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # create ldap-group cn=security,cn=users,dc=lab,dc=com
UCS-A /security/ldap/ldap-group* # create locale pacific
UCS-A /security/ldap/ldap-group* # create role admin
UCS-A /security/ldap/ldap-group* # commit-buffer
UCS-A /security/ldap/ldap-group #
```

次のタスク

LDAP グループ ルールを設定します。

LDAP グループ マップの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **delete ldap-group** *group-dn*	指定した DN 用の LDAP グループ マップを削除します。
ステップ 4	UCS-A /security/ldap # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、LDAP グループ マップを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # delete ldap-group cn=security,cn=users,dc=lab,dc=com
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

RADIUS プロバイダ

RADIUS プロバイダのプロパティの設定

このタスクで設定するプロパティは、Cisco UCS Manager で定義されたこのタイプのすべてのプロバイダ接続のデフォルト設定です。個々のプロバイダにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS でその設定が使用され、デフォルト設定は無視されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope radius**	セキュリティ RADIUS 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 3	（任意） UCS-A /security/radius # **set retries** *retry-num*	サーバをダウンとして通知する前にRADIUSサーバとの通信を再試行する回数を設定します。
ステップ 4	（任意） UCS-A /security/radius # **set timeout** *seconds*	システムがサーバをダウン状態として通知する前に、RADIUSサーバからの応答を待つ時間間隔を設定します。
ステップ 5	UCS-A /security/radius # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、RADIUS リトライを 4 に設定し、タイムアウト間隔を 30 秒に設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # set retries 4
UCS-A /security/radius* # set timeout 30
UCS-A /security/radius* # commit-buffer
UCS-A /security/radius #
```

次のタスク

RADIUS プロバイダを作成します。

RADIUS プロバイダの作成

Cisco UCS Manager は最大 16 の RADIUS プロバイダをサポートします。

始める前に

RADIUS サーバで、次の設定を行います。

- Cisco UCS Manager のユーザ ロールとロケール情報を保持する属性でユーザを設定します。この属性について RADIUS スキーマを拡張するかどうかを選択できます。スキーマを拡張しない場合は、既存の RADIUS 属性を使用して Cisco UCS ユーザ ロールとロケールを保持します。スキーマを拡張する場合は、cisco-avpair 属性などのカスタム属性を作成します。

  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する方法を示しています。`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。

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポートの IPv4 または IPv6 アドレスを追加します。この設定では、1 つ目のファブリック インターコネクトで障害が発生し、システムが 2 つ目のファブリック インターコネクトにフェールオーバーしても、リモートユーザは引き続きログインできることが保証されます。ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager によって使用されている仮想 IP アドレスではありません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope radius**	セキュリティ RADIUS モードを開始します。
ステップ 3	UCS-A /security/radius # **create server** *server-name*	RADIUS サーバインスタンスを作成し、セキュリティ RADIUS サーバ モードを開始します。
ステップ 4	（任意） UCS-A /security/radius/server # **set authport** *authport-num*	RADIUS サーバとの通信に使用するポートを指定します。
ステップ 5	UCS-A /security/radius/server # **set key**	RADIUS サーバ キーを設定します。キー値を設定するには、 **set key** コマンドを入力してから **Enter** を押し、プロンプトでキー値を入力します。
ステップ 6	（任意） UCS-A /security/radius/server # **set order** *order-num*	このサーバが試行される順序を指定します。
ステップ 7	（任意） UCS-A /security/radius/server # **set retries** *retry-num*	サーバをダウンとして通知する前に RADIUS サーバとの通信を再試行する回数を設定します。
ステップ 8	（任意） UCS-A /security/radius/server # **set timeout** *seconds*	システムがサーバをダウン状態として通知する前に、RADIUS サーバからの応答を待つ時間間隔を設定します。 ヒント RADIUS プロバイダに二要素認証を選択する場合は、より高い**タイムアウト値**を設定することを推奨します。
ステップ 9	UCS-A /security/radius/server # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、radiusserv7 という名前のサーバインスタンスを作成し、認証ポートを 5858 に設定し、キーを radiuskey321 に設定し、順序を 2 に設定し、再試行回数を 4 回に設定し、タイムアウトを 30 に設定し、二要素認証を有効にし、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # create server radiusserv7
UCS-A /security/radius/server* # set authport 5858
UCS-A /security/radius/server* # set key
Enter the key: radiuskey321
Confirm the key: radiuskey321
UCS-A /security/radius/server* # set order 2
UCS-A /security/radius/server* # set retries 4
UCS-A /security/radius/server* # set timeout 30
UCS-A /security/radius/server* # commit-buffer
UCS-A /security/radius/server #
```

次のタスク

単一の RADIUS データベースが関係する実装の場合、RADIUS をプライマリ認証サービスとして選択します。

複数の RADIUS データベースが関係する実装の場合は、RADIUS プロバイダ グループを設定します。

RADIUS プロバイダの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope RADIUS**	セキュリティ RADIUS モードを開始します。
ステップ 3	UCS-A /security/radius # **delete server** *serv-name*	指定したサーバを削除します。
ステップ 4	UCS-A /security/radius # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、radius1 という RADIUS サーバを削除し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # delete server radius1
UCS-A /security/radius* # commit-buffer
UCS-A /security/radius #
```

TACACS+ プロバイダ

TACACS+ プロバイダのプロパティの設定

このタスクで設定するプロパティは、Cisco UCS Manager で定義されたこのタイプのすべてのプロバイダ接続のデフォルト設定です。個々のプロバイダにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS でその設定が使用され、デフォルト設定は無視されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS+ モードを開始します。
ステップ 3	（任意） UCS-A /security/tacacs # **set timeout** *seconds*	システムがサーバをダウン状態として通知する前に、TACACS+ サーバからの応答を待つ時間間隔を設定します。
ステップ 4	UCS-A /security/tacacs # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、TACACS+ タイムアウト間隔を 45 秒に設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # set timeout 45
UCS-A /security/tacacs* # commit-buffer
UCS-A /security/tacacs #
```

次のタスク

TACACS+ プロバイダを作成します。

TACACS+ プロバイダの作成

Cisco UCS Manager は最大 16 の TACACS+ プロバイダをサポートします。

始める前に

TACACS+ サーバで、次の設定を行います。

- cisco-av-pair 属性を作成します。既存の TACACS+ 属性は使用できません。

  cisco-av-pair 名は、TACACS+ プロバイダの属性 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する方法を示しています。`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。

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポートの IPv4 または IPv6 アドレスを追加します。この設定では、1 つ目のファブリック インターコネクトで障害が発生し、システムが 2 つ目のファブリック インターコネクトにフェールオーバーしても、リモートユーザは引き続きログインできることが保証されます。ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager によって使用されている仮想 IP アドレスではありません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS+ モードを開始します。
ステップ 3	UCS-A /security/tacacs # **create server** *server-name*	TACACS+ サーバ インスタンスを作成し、セキュリティ TACACS+ サーバモードを開始します
ステップ 4	（任意） UCS-A /security/tacacs/server # **set key**	TACACS+ サーバ キーを設定します。キー値を設定するには、 **set key** コマンドを入力してから **Enter** を押し、プロンプトでキー値を入力します。
ステップ 5	（任意） UCS-A /security/tacacs/server # **set order** *order-num*	このサーバが試行される順序を指定します。
ステップ 6	（任意） UCS-A /security/tacacs/server # **set timeout***seconds*	システムがサーバをダウン状態として通知する前に、TACACS+ サーバからの応答を待つ時間間隔を設定します。

	コマンドまたはアクション	目的
		ヒント　TACACS+ プロバイダに二要素認証を選択する場合は、より高いタイムアウト値を設定することを推奨します。
ステップ 7	UCS-A /security/tacacs/server # **set port** *port-num*	TACACS+ サーバとの通信に使用するポートを指定します。
ステップ 8	UCS-A /security/tacacs/server # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、tacacsserv680 という名前のサーバインスタンスを作成し、キーを tacacskey321 に設定してそのキーを確認し、順序を 4 に設定し、認証ポートを 5859 に設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # create server tacacsserv680
UCS-A /security/tacacs/server* # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
UCS-A /security/tacacs/server* # set order 4
UCS-A /security/tacacs/server* # set port 5859
UCS-A /security/tacacs/server* # commit-buffer
UCS-A /security/tacacs/server #
```

次のタスク

単一の TACACS+ データベースが関係する実装の場合、TACACS+ をプライマリ認証サービスとして選択します。

複数の TACACS+ データベースが関係する実装の場合は、TACACS+ プロバイダ グループを設定します。

TACACS+ プロバイダの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS 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 3	UCS-A /security/tacacs # **delete server** *serv-name*	指定したサーバを削除します。
ステップ 4	UCS-A /security/tacacs # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、tacacs1 という TACACS サーバを削除し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # delete server TACACS1
UCS-A /security/tacacs* # commit-buffer
UCS-A /security/tacacs #
```

マルチ認証システムの設定

マルチ認証サービス

次の機能の実装により、Cisco UCS が複数の認証サービスを使用するよう設定することができます。

- プロバイダ グループ
- 認証ドメイン

プロバイダ グループと認証ドメインを Cisco UCS Manager で構成した後、構文 **ucs:***auth-domain* \ *user-name* を使用すると、Cisco UCS Manager CLI を使ってシステムにログインできます。

リモート認証サービスで複数の認証ドメインとネイティブ認証が設定されている場合は、次のいずれかの構文例を使用して SSH、Telnet または Putty でログインします。

（注） SSH ログインでは大文字と小文字が区別されます。

Linux 端末からは以下の SSH を使用します。

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCMS-ipv6-address*}

  ssh ucs-example\\jsmith@192.0.20.11

  ssh ucs-example\\jsmith@2001::1

- **ssh -l ucs-***auth-domain**username* {*UCSM-ip-address*| *UCSM-ipv6-address*| *UCSM-host-name*}

  ssh -l ucs-example\\jsmith 192.0.20.11

```
ssh -l ucs-example\\jsmith 2001::1
```

- **ssh** {*UCSM-ip-address* | *UCSM-ipv6-address* | *UCSM-host-name*} **-l ucs-***auth-domain**username*

```
ssh 192.0.20.11 -l ucs-example\\jsmith
ssh 2001::1 -l ucs-example\\jsmith
```

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCSM-ipv6-address*}

```
ssh ucs-ldap23\\jsmith@192.0.20.11
ssh ucs-ldap23\\jsmith@2001::1
```

Linux 端末からは以下の Telnet を使用します。

- **telnet ucs-***UCSM-host-name* **ucs-***auth-domain**username*

```
telnet ucs-qa-10
login: ucs-ldap23\blradmin
```

- **telnet ucs-**{*UCSM-ip-address* | *UCSM-ipv6-address*}*ucs-auth-domain**username*

```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\blradmin
```

Putty クライアントから：

- **ucs-***auth-domain**username* でログインします。

```
Login as: ucs-example\jsmith
```

（注） デフォルトの認証がローカルに設定され、コンソール認証がLDAPに設定されている場合は、**ucs-local\admin**（admin はローカル アカウント名）を使用して Putty クライアントからファブリック インターコネクトにログインできます。

マルチ認証システムの設定

プロバイダ グループ

プロバイダ グループは、認証プロセス中に Cisco UCS がアクセスするプロバイダのセットです。プロバイダ グループ内のすべてのプロバイダが、ユーザの認証にCisco UCS プロバイダが使用する順にアクセスされます。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 Manager 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。

Cisco UCS Manager では、最大 16 のプロバイダ グループを作成でき、グループごとに最大 8 つのプロバイダを含めることができます。

LDAP プロバイダ グループの作成

LDAP プロバイダ グループを作成すると、複数の LDAP データベースを使用して認証できます。

始める前に

1 つ以上の LDAP プロバイダを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **create auth-server-group** *auth-server-group-name*	LDAP プロバイダ グループを作成し、認証サーバ グループの LDAP セキュリティ モードを開始します。
ステップ 4	UCS-A /security/ldap/auth-server-group # **create server-ref** *ldap-provider-name*	指定された LDAP プロバイダを LDAP プロバイダ グループに追加し、サーバ参照認証サーバ グループの LDAP セキュリティ モードを開始します。
ステップ 5	UCS-A /security/ldap/auth-server-group/server-ref # **set order** *order-num*	Cisco UCS がこのプロバイダをユーザの認証に使用する順序を指定します。 有効な値には no-value と 0 ～ 16 が含まれ、値が小さいほど優先度が高いことを示します。順序を no-value に指定することは、そのサーバ参照の優先度を最高にするのと同じです。
ステップ 6	UCS-A /security/ldap/auth-server-group/server-ref # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ldapgroup という名前の LDAP プロバイダ グループを作成し、プロバイダ グループに ldap1 および ldap2 という 2 種類の事前設定されたプロバイダを追加し、順序を設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # create auth-server-group ldapgroup
UCS-A /security/ldap/auth-server-group* # create server-ref ldap1
```

```
UCS-A /security/ldap/auth-server-group/server-ref* # set order 1
UCS-A /security/ldap/auth-server-group/server-ref* # up
UCS-A /security/ldap/auth-server-group* # create server-ref ldap2
UCS-A /security/ldap/auth-server-group/server-ref* # set order 2
UCS-A /security/ldap/auth-server-group/server-ref* # commit-buffer
UCS-A /security/ldap/auth-server-group/server-ref #
```

次のタスク

認証ドメインを設定するか、デフォルト認証サービスを選択します。

LDAP プロバイダ グループの削除

始める前に

認証設定からプロバイダ グループを削除します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **delete auth-server-group** *auth-server-group-name*	LDAP プロバイダ グループを削除します。
ステップ 4	UCS-A /security/ldap # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、ldapgroup という名前の LDAP プロバイダ グループを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # delete auth-server-group ldapgroup
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

RADIUS プロバイダ グループの作成

RADIUS プロバイダ グループを作成すると、複数の RADIUS データベースを使用して認証できます。

始める前に

1 つ以上の RADIUS プロバイダを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope radius**	セキュリティ RADIUS モードを開始します。
ステップ 3	UCS-A /security/radius # **create auth-server-group** *auth-server-group-name*	RADIUS プロバイダ グループを作成し、認証サーバ グループの RADIUS セキュリティ モードを開始します。
ステップ 4	UCS-A /security/RADIUS/auth-server-group # **create server-ref** *radius-provider-name*	指定された RADIUS プロバイダを RADIUS プロバイダ グループに追加し、サーバ参照認証サーバ グループの RADIUS セキュリティ モードを開始します。
ステップ 5	UCS-A /security/radius/auth-server-group/server-ref # **set order** *order-num*	Cisco UCS がこのプロバイダをユーザの認証に使用する順序を指定します。 有効な値には no-value と 0 ～ 16 が含まれ、値が小さいほど優先度が高いことを示します。順序を no-value に指定することは、そのサーバ参照の優先度を最高にするのと同じです。
ステップ 6	UCS-A /security/radius/auth-server-group/server-ref # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、radiusgroup という名前の RADIUS プロバイダ グループを作成し、プロバイダ グループに radius1 と radius2 という 2 種類の事前設定されたプロバイダを追加し、順序を設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # create auth-server-group radiusgroup
UCS-A /security/radius/auth-server-group* # create server-ref radius1
UCS-A /security/radius/auth-server-group/server-ref* # set order 1
UCS-A /security/radius/auth-server-group/server-ref* # up
UCS-A /security/radius/auth-server-group* # create server-ref radius2
UCS-A /security/radius/auth-server-group/server-ref* # set order 2
UCS-A /security/radius/auth-server-group/server-ref* # commit-buffer
UCS-A /security/radius/auth-server-group/server-ref #
```

次のタスク

認証ドメインを設定するか、デフォルト認証サービスを選択します。

RADIUS プロバイダ グループの削除

認証設定からプロバイダ グループを削除します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope radius**	セキュリティ RADIUS モードを開始します。
ステップ 3	UCS-A /security/radius # **delete auth-server-group** *auth-server-group-name*	RADIUS プロバイダ グループを削除します。
ステップ 4	UCS-A /security/radius # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、radiusgroup という RADIUS プロバイダ グループを削除し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # delete auth-server-group radiusgroup
UCS-A /security/radius* # commit-buffer
UCS-A /security/radius #
```

TACACS プロバイダ グループの作成

TACACS+ プロバイダ グループを作成すると、複数の TACACS+ データベースを使用して認証できます。

始める前に

TACACS プロバイダを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ 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	UCS-A /security # **scope tacacs**	セキュリティ TACACS モードを開始します。
ステップ 3	UCS-A /security/tacacs # **create auth-server-group** *auth-server-group-name*	TACACS プロバイダ グループを作成し、認証サーバグループのセキュリティ TACACS モードを開始します。
ステップ 4	UCS-A /security/tacacs/auth-server-group # **create server-ref** *tacacs-provider-name*	指定した TACACS プロバイダを TACACS プロバイダ グループに追加し、サーバ参照認証サーバ グループ セキュリティ TACACS モードを開始します。
ステップ 5	UCS-A /security/tacacs/auth-server-group/server-ref # **set order** *order-num*	Cisco UCS がこのプロバイダをユーザの認証に使用する順序を指定します。 有効な値には no-value と 0 ～ 16 が含まれ、値が小さいほど優先度が高いことを示します。順序を no-value に指定することは、そのサーバ参照の優先度を最高にするのと同じです。
ステップ 6	UCS-A /security/tacacs/auth-server-group/server-ref # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、tacacsgroup という名前の TACACS プロバイダ グループを作成し、プロバイダ グループに tacacs1 と tacacs2 という 2 種類の事前設定されたプロバイダを追加し、順序を設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # create auth-server-group tacacsgroup
UCS-A /security/tacacs/auth-server-group* # create server-ref tacacs1
UCS-A /security/tacacs/auth-server-group/server-ref* # set order 1
UCS-A /security/tacacs/auth-server-group/server-ref* # up
UCS-A /security/tacacs/auth-server-group* # create server-ref tacacs2
UCS-A /security/tacacs/auth-server-group/server-ref* # set order 2
UCS-A /security/tacacs/auth-server-group/server-ref* # commit-buffer
UCS-A /security/tacacs/auth-server-group/server-ref #
```

次のタスク

認証ドメインを設定するか、デフォルト認証サービスを選択します。

TACACS プロバイダ グループの削除

認証設定からプロバイダ グループを削除します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS モードを開始します。
ステップ 3	UCS-A /security/tacacs # **delete auth-server-group** *auth-server-group-name*	TACACS プロバイダ グループを削除します。
ステップ 4	UCS-A /security/tacacs # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、tacacsgroup という TACACS プロバイダ グループを削除し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # delete auth-server-group tacacsgroup
UCS-A /security/tacacs* # commit-buffer
UCS-A /security/tacacs #
```

認証ドメイン

Cisco UCS Manager では、複数の認証システムを活用するために認証ドメインを使用しています。各認証ドメインはログイン時に指定および設定できます。これを行わない場合、Cisco UCS Manager はデフォルトの認証サービス設定を使用します。

最大 8 個の認証ドメインを作成できます。各認証ドメインは、Cisco UCS Manager 内のプロバイダ グループと領域に関連付けられています。プロバイダ グループを指定しないと、Cisco UCS Manager では領域内のすべてのサーバを使用します。

認証ドメインの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ 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	UCS-A /security # **create auth-domain** *domain-name*	認証ドメインを作成し、認証ドメインモードを開始します。 （注） リモート認証プロトコル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に 5 文字が挿入されるため、ドメイン名とユーザ名の合計が27文字を超える場合には認証が失敗します。
ステップ 3	（任意） UCS-A /security/auth-domain # **set refresh-period** *seconds*	Web クライアントが Cisco UCS Manager に接続する際は、Web セッションをアクティブ状態に維持するために、クライアントは Cisco UCS Manager に更新要求を送信する必要があります。このオプションを使用して、このドメインのユーザに許可する更新要求間隔の最大時間数を指定します。 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であると見なしますが、セッションを強制終了することはしません。 60 ～ 172800 の整数を指定します。デフォルト値は、二要素認証が有効でない場合は600秒、二要素認証が有効の場合は 7200 秒です。 （注） [Web Session Refresh Period] に設定する秒数は、[Web Session Timeout] に設定する秒数未満である必要があります。[Web Session Refresh Period] に [Web Session Timeout] と同じ値を設定しないでください。
ステップ 4	（任意） UCS-A /security/auth-domain # **set session-timeout** *seconds*	最後の更新要求時から Cisco UCS Manager が Web セッションを非アクティブとして見なすまでの最大経過時間。こ

	コマンドまたはアクション	目的
		の時間制限を超えた場合、Cisco UCS Manager は自動的に Web セッションを終了します。 300 ～ 172800 の整数を指定します。デフォルト値は、二要素認証が有効でない場合は 7200 秒、二要素認証が有効の場合は 8000 秒です。 （注） RADIUS または TACACS+ レルムに対して二要素認証を設定する場合は、リモート ユーザが頻繁に再認証する必要がないよう、**セッションの更新**時間および**セッションのタイムアウト**時間を増やすことを検討してください。
ステップ 5	（任意） UCS-A /security/auth-domain # **create default-auth**	認証ドメインのデフォルト認証を作成します。
ステップ 6	（任意） UCS-A /security/auth-domain/default-auth # **set auth-server-group** *auth-serv-group-name*	認証ドメインのプロバイダ グループを設定します。
ステップ 7	UCS-A /security/auth-domain/default-auth # **set realm** {**ldap** | **local** | **radius** | **tacacs**}	認証ドメインのレルムを設定します。
ステップ 8	（任意） UCS-A /security/auth-domain/default-auth # **set use-2-factor yes**	レルムの二要素認証に認証方式を設定します。 （注） 二要素認証は、RADIUS および TACACS+ レルムにのみ適用されます。
ステップ 9	UCS-A /security/auth-domain/default-auth # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、Web の更新時間が 3600 秒（1 時間）およびセッションのタイムアウト時間が 14400 秒（4 時間）の domain1 と呼ばれる認証ドメインを作成します。次に、radius1 でプロバイダを使用するように domain1 を設定し、レルム タイプを radius に設定し、二要素認証を有効にし、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # create auth-domain domain1
```

```
UCS-A /security/auth-domain* # set refresh-period 3600
UCS-A /security/auth-domain* # set session-timeout 14400
UCS-A /security/auth-domain* # create default-auth
UCS-A /security/auth-domain/auth-domain* # set auth-server-group radius1
UCS-A /security/auth-domain/auth-domain* # set realm radius
UCS-A /security/auth-domain/auth-domain* # set user-2-factor yes
UCS-A /security/auth-domain/auth-domain* # commit-buffer
UCS-A /security/auth-domain/auth-domain #
```

プライマリ認証サービス

コンソール認証サービスの選択

始める前に

システムでリモート認証サービスが使用されている場合は、その認証サービスに対するプロバイダを作成します。Cisco UCS を通じたローカル認証のみを使用する場合は、最初にプロバイダを作成する必要はありません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope console-auth**	コンソール認証セキュリティ モードを開始します。
ステップ 3	UCS-A /security/console-auth # **set realm** *auth-type*	コンソール認証を指定します。*auth-type* 引数は次のいずれかのキーワードです。 • **ldap** ：LDAP 認証を指定します。 • **local** ：ローカル認証を指定します。 • **none** ：ローカル ユーザはパスワードを指定せずにログインできます。 • **radius** ：RADIUS 認証を指定します。 • **tacacs** ：TACACS+ 認証を指定します。
ステップ 4	（任意） UCS-A /security/console-auth # **set auth-server-group** *auth-serv-group-name*	関連付けられたプロバイダ グループ（存在する場合）。

	コマンドまたはアクション	目的
ステップ 5	（任意） UCS-A /security/default-auth # **set use-2-factor yes**	レルムの二要素認証に認証方式を設定します。 （注） 二要素認証は、RADIUS および TACACS+ レルムにのみ適用されます。
ステップ 6	UCS-A /security/console-auth # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、認証レルムを TACACS+ に設定し、コンソール認証プロバイダ グループを provider1 に設定し、二要素認証を有効にし、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope console-auth
UCS-A /security/console-auth # set realm tacacs
UCS-A /security/console-auth # set auth-server-group provider1
UCS-A /security/console-auth* # set use-2-factor yes
UCS-A /security/console-auth* # commit-buffer
UCS-A /security/console-auth #
```

デフォルト認証サービスの選択

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope default-auth**	デフォルト認証セキュリティ モードを開始します。
ステップ 3	UCS-A /security/default-auth # **set realm** *auth-type*	デフォルト認証を指定します。*auth-type* は次のキーワードのいずれかです。 • **ldap**：LDAP 認証を指定します。 • **local**：ローカル認証を指定します。 • **none**：ローカル ユーザはパスワードを指定せずにログインできます。 • **radius**：RADIUS 認証を指定します。

	コマンドまたはアクション	目的
		• **tacacs**：TACACS+ 認証を指定します。
ステップ 4	（任意） UCS-A /security/default-auth # **set auth-server-group** *auth-serv-group-name*	関連付けられたプロバイダグループ（存在する場合）。
ステップ 5	（任意） UCS-A /security/default-auth # **set refresh-period** *seconds*	Web クライアントが Cisco UCS Manager に接続する際は、Web セッションをアクティブ状態に維持するために、クライアントは Cisco UCS Manager に更新要求を送信する必要があります。このオプションを使用して、このドメインのユーザに許可する更新要求間隔の最大時間数を指定します。 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であると見なしますが、セッションを強制終了することはしません。 60 ～ 172800 の整数を指定します。デフォルト値は、二要素認証が有効でない場合は 600 秒、二要素認証が有効の場合は 7200 秒です。
ステップ 6	（任意） UCS-A /security/default-auth # **set session-timeout** *seconds*	最後の更新要求時から Cisco UCS Manager が Web セッションを非アクティブとして見なすまでの最大経過時間。この時間制限を超えた場合、Cisco UCS Manager は自動的に Web セッションを終了します。 300 ～ 172800 の整数を指定します。デフォルト値は、二要素認証が有効でない場合は 7200 秒、二要素認証が有効の場合は 8000 秒です。 （注） RADIUS または TACACS+ レルムに対して二要素認証を設定する場合は、リモート ユーザが頻繁に再認証する必要がないよう、**セッションの更新**時間および**セッションのタイムアウト**時間を増やすことを検討してください。

	コマンドまたはアクション	目的
ステップ 7	（任意） UCS-A /security/default-auth # **set use-2-factor yes**	レルムの二要素認証に認証方式を設定します。 （注） 二要素認証は、RADIUS および TACACS+ レルムにのみ適用されます。
ステップ 8	UCS-A /security/default-auth # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、デフォルトの認証を RADIUS に設定し、デフォルトの認証プロバイダ グループを provider1 に設定し、二要素認証を有効にし、更新間隔を 7200 秒（2 時間）に設定し、セッションのタイムアウト間隔を 28800 秒（8 時間）に設定し、二要素認証を有効にします。そして、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope default-auth
UCS-A /security/default-auth # set realm radius
UCS-A /security/default-auth* # set auth-server-group provider1
UCS-A /security/default-auth* # set use-2-factor yes
UCS-A /security/default-auth* # set refresh-period 7200
UCS-A /security/default-auth* # set session-timeout 28800
UCS-A /security/default-auth* # commit-buffer
UCS-A /security/default-auth #
```

リモート ユーザのロール ポリシー

デフォルトでは、Cisco UCS Manager でユーザ ロールが設定されていない場合は、LDAP、RADIUS、または TACACS プロトコルを使用してリモート サーバから Cisco UCS Manager にログインしているすべてのユーザに読み取り専用アクセス権が付与されます。セキュリティ上の理由から、Cisco UCS Manager で確立されたユーザ ロールに一致するユーザへのアクセスを制限するのが望ましい場合があります。

リモート ユーザのロール ポリシーは、次の方法で設定できます。

assign-default-role

ユーザ ロールに基づいて、Cisco UCS Manager へのユーザ アクセスを制限しません。その他のユーザ ロールが Cisco UCS Manager で定義されていない限り、読み取り専用アクセス権がすべてのユーザに付与されます。

これはデフォルトの動作です。

no-login

ユーザ ロールに基づいて、Cisco UCS Manager へのユーザ アクセスを制限します。リモート認証システムにユーザ ロールが割り当てられていない場合、アクセスは拒否されます。

リモート ユーザのロール ポリシーの設定

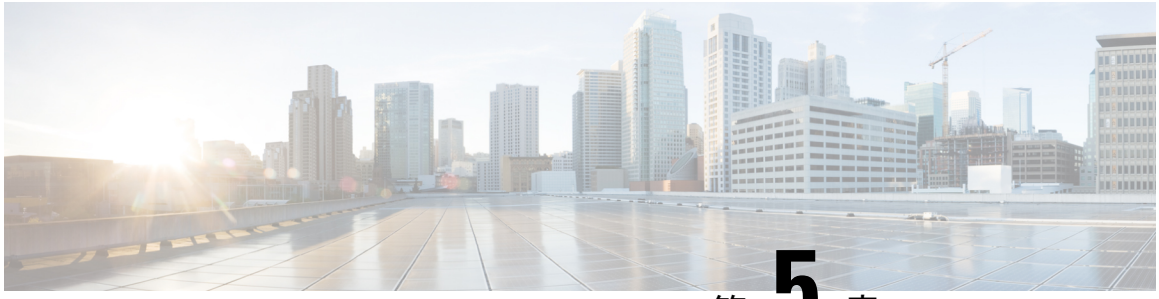
手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **set remote-user default-role** {**assign-default-role** | **no-login**}	ユーザ ロールに基づいて Cisco UCS Manager へのアクセスが制限されるかどうかを指定します。
ステップ 3	UCS-A /security # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、リモートユーザのロールポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # set remote-user default-role assign-default-role
UCS-A /security* # commit-buffer
UCS-A /security #
```



第 5 章

Call Home 機能を有効または無効にする方法

Call Home

Call Home では、重要なシステム ポリシーに対して電子メールベースの通知が提供されます。ポケットベル サービスや XML ベースの自動化された解析アプリケーションとの互換性のために、さまざまなメッセージ フォーマットが用意されています。 この機能を使用して、ネットワーク サポート エンジニアにポケットベルで連絡したり、ネットワーク オペレーション センターに電子メールを送信したりできます。また、Cisco Smart Call Home サービスを使用して TAC のケースを生成できます。

Call Home 機能では、診断情報および環境の障害とイベントに関する情報が含まれるアラートメッセージを配信できます。

Call Home 機能では、複数の受信者（Call Home 宛先プロファイルと呼びます）にアラートを配信できます。 各プロファイルには、設定可能なメッセージ フォーマットとコンテンツ カテゴリが含まれます。 Cisco TAC へアラートを送信するための宛先プロファイルが事前に定義されていますが、独自の宛先プロファイルを定義することもできます。

メッセージを送信するように Call Home を設定すると、Cisco UCS Manager は CLI の適切な **show** コマンドを実行し、そのコマンドの出力をメッセージに添付します。

Cisco UCS では、Call Home メッセージが次のフォーマットで配信されます。

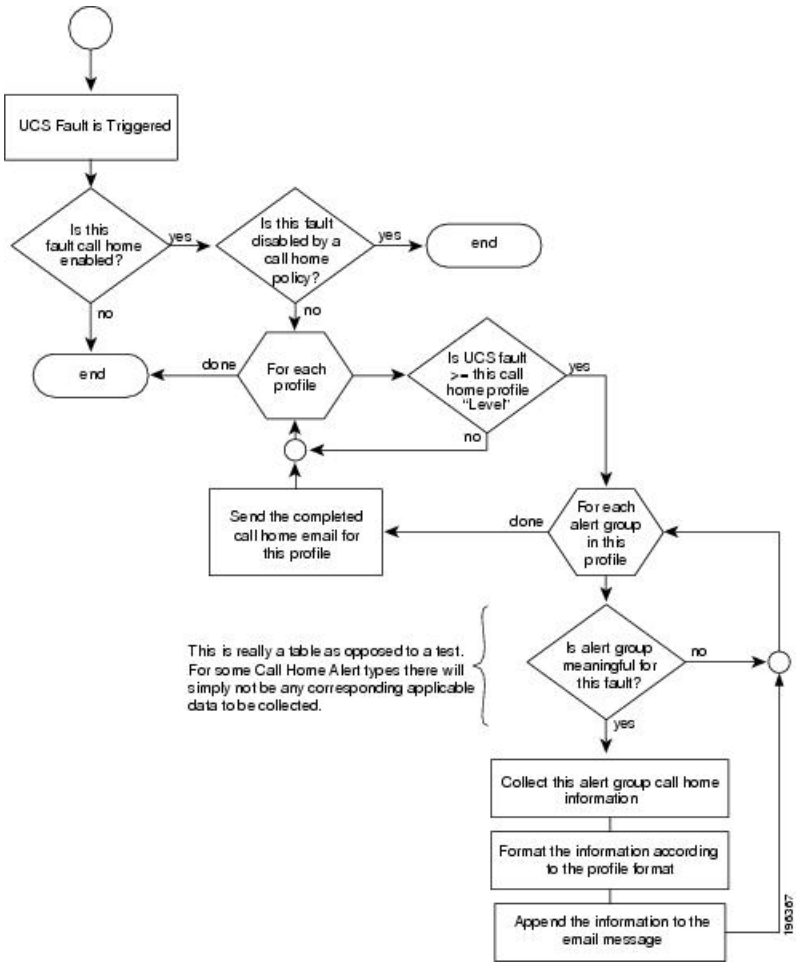
- 1 または 2 行で障害を説明する、ポケットベルや印刷レポートに適したショート テキスト フォーマット。
- 詳細な情報を十分に書式が整えられたメッセージで提供する、ユーザが読むのに適したフル テキスト フォーマット。

- Extensible Markup Language（XML）と Adaptive Messaging Language（AML）XML schema definition（XSD）を使用する、コンピュータで読み取り可能な XML フォーマット。 AML XSD は Cisco.com の Web サイトで公開されています。 XML フォーマットでは、シスコの TAC との通信が可能になります。

Call Home 電子メール アラートをトリガーする可能性がある障害についての情報は、『*Cisco UCS Faults and Error Messages Reference*』を参照してください。

次の図に、Call Home が設定されたシステムで Cisco UCS障害がトリガーされた後のイベントの流れを示します。

図 *1*：障害発生後のイベントの流れ



Call Home の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニタリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **enable**	Call Home を有効にします。
ステップ 4	UCS-A /monitoring/callhome # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、Call Home を有効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # enable
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

次のタスク

Call Home 機能の詳細については、『*Cisco UCS System Monitoring Guide*』を参照してください。

Call Home の無効化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニタリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **disable**	Call Home を有効にします。
ステップ 4	UCS-A /monitoring/callhome # **commit-buffer**	トランザクションをシステムの設定にコミットします。

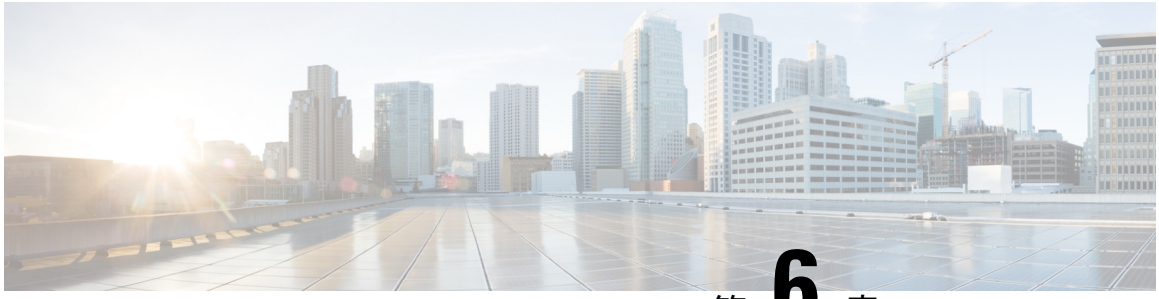
例

次に、Call Home を無効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # disable
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

次のタスク

Call Home 機能の詳細については、『*Cisco UCS System Monitoring Guide*』を参照してください。



第 6 章

UCS Manager コミュニケーションサービス

この章は、次の項で構成されています。

通信サービス

以下に定義する通信サービスは、サードパーティ アプリケーションと Cisco UCS のインターフェイス用途として使用できます。

Cisco UCS Manager では、次のサービスに対して IPv4 および IPv6 アドレス アクセスをサポートしています。

- 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、次のサービスを有効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では無効であり、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、デフォルトで無効になります。 このサービスを有効にすると、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 サービスは全体で有効または無効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 で有効になっています。 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。 ブラウザ セッションの安全性の理由により、HTTPS を有効にし、HTTP を無効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] を有効にします。
HTTPS	デフォルトでは、HTTPS はポートで有効になっています。 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。 ブラウザ セッションの安全性の理由により、HTTPS だけを使用し、HTTP 通信は無効にするかリダイレクトすることを推奨します。

通信サービス	説明
SMASH CLP	このサービスは読み取り専用アクセスに対して有効になり、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。これを無効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、このサービスは無効になっています。有効の場合、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有効にします。
SSH	このサービスは、ポート 22 で有効になります。これは無効にできず、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、このサービスは無効になっています。 このサービスは Cisco UCS Manager CLI へのアクセスを提供します。

非セキュアなコミュニケーション サービス

Web セッション制限の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system** .	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services** .	サービス モードを開始します。
ステップ 3	UCS-A /system/services # **scope web-session-limits** .	Web セッションの制限モードを開始します。
ステップ 4	UCS-A /system/services/web-session-limits # **set** {**maximum-event-interval** |**per-user** | **total**}*number* .	次の Web セッション制限を設定できます。

	コマンドまたはアクション	目的
		名前 / 説明 **[Maximum Sessions Per User]** / 各ユーザに許可される HTTP および HTTPS の同時セッションの最大数。1 ～ 256 の整数を入力します。 **[Maximum Sessions]** / システム内のすべてのユーザに許可される HTTP および HTTPS の同時セッションの最大数。1 ～ 256 の整数を入力します。 **[Maximum Event Interval (in seconds)]** / 2 つのイベント間の最大時間間隔。UI からのユーザ要求に対する応答など、さまざまなタイプのイベント変更通知を追跡します。時間間隔が経過すると、UI セッションは終了します。120 ～ 3600 の整数を入力します。
ステップ 5	UCS-A /system/services/web-session-limits # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、最大イベント間隔を設定する方法を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # scope web-session-limits
UCS-A /system/services/web-session-limits # set maximum-event-interval 300
UCS-A /system/services/web-session-limits # commit buffer
```

Web セッション制限の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	サービス モードを開始します。
ステップ 3	/system/services # **show web-session-limits**	Web セッションの設定を表示します。

例

次の例では、Web セッションの制限を表示する方法を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # show web-session-limits
Web Sessions:
    Maximum logins for single user Maximum Sessions Maximum Event Interval (sec)
    ------------------------------ ---------------- ----------------------------
    32                             256              600
UCS-A /system/services #
```

シェル セッション制限の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system** .	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services** .	サービス モードを開始します。
ステップ 3	UCS-A /system/services # **scope shell-session-limits**	
ステップ 4	UCS-A /system/services/shell-session-limits # **set** {**per-user** |**total**}*number*.	次のシェル セッション制限を設定できます。 名前: **[Maximum Sessions Per User]** 説明: 各ユーザに許可される同時シェル セッションの最大数。 1 ～ 32 の整数を入力します。

	コマンドまたはアクション	目的
		名前 / 説明 **[Maximum Sessions]** / システム内のすべてのユーザに許可される同時シェルセッションの最大数。 1 ～ 32 の整数を入力します。
ステップ 5	UCS-A /system/services/shell-session-limits # **commit-buffer** .	トランザクションをシステムの設定にコミットします。

例

次に、最大セッション数を設定する例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # scope shell-session-limits
UCS-A /system/services/shell-session-limits # set maximum-sessions 20
UCS-A /system/services/shell-session-limits # commit buffer
```

Viewing Shell Session Limits

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	サービス モードを開始します。
ステップ 3	/system/services # **show shell-session-limits**	シェルセッションの設定を表示します。

例

次の例では、シェル セッションの制限を表示する方法を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # show shell-session-limits
Shell Sessions:
    Maximum logins for single user Maximum Sessions
    ------------------------------ ----------------
    32                             32
UCS-A /system/services #
```

CIM XML の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **enable cimxml**	CIM XLM サービスを有効にします。
ステップ 4	UCS-A /system/services # **set cimxml port** *port-num*	CIM XML 接続のポートを指定します。
ステップ 5	UCS-A /system/services # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、CIM XML を有効にし、ポート番号を 5988 に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable cimxml
UCS-A /system/services* # set cimxml port 5988
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

HTTP の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **enable http**	HTTP サービスを有効にします。
ステップ 4	UCS-A /system/services # **set http port** *port-num*	HTTP 接続で使用されるポートを指定します。
ステップ 5	UCS-A /system/services # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、HTTP を有効にし、ポート番号を 80 に設定し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable http
UCS-A /system/services* # set http port 80
Warning: When committed, this closes all the web sessions.
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

HTTP の設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **disable http**	HTTP サービスを無効にします。
ステップ 4	UCS-A /system/services # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、HTTP を無効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # disable http
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

セキュアなコミュニケーション サービス

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **enable https**	HTTPS サービスを有効にします。
ステップ 4	（任意） UCS-A /system/services # **set https port** *port-num*	HTTPS 接続で使用されるポートを指定します。
ステップ 5	（任意） UCS-A /system/services # **set https keyring** *keyring-name*	HTTPS に対して作成したキー リングの名前を指定します。
ステップ 6	（任意） UCS-A /system/services # **set https cipher-suite-mode** *cipher-suite-mode*	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。 *cipher-suite-mode* には、以下のいずれかのキーワードを指定できます。 • **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。
ステップ 7	（任意） UCS-A /system/services # **set https cipher-suite** *cipher-suite-spec-string*	**cipher-suite-mode** が **custom** に設定されている場合、この Cisco UCS ドメインに対する暗号スイート セキュリティのカスタム レベルを指定します。

	コマンドまたはアクション	目的
		cipher-suite-spec-string 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** （注） **cipher-suite-mode** は **custom** 以外に設定されている場合、このオプションは無視されます。
ステップ 8	（任意） UCS-A /system/services # **set https ssl-protocol**	UCSM が許可する SSL プロトコルを選択できます。値は [Default (Allow all except SSLv2 and SSLv3)] と [Only TLSV1.2] です。[Only TLSv1.2] を選択すると、低いバージョンの TLS プロトコルを使用した Web クライアントからの接続は確立されません。
ステップ 9	UCS-A /system/services # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、HTTPS を有効にし、ポート番号を 443 に設定し、キーリング名を kring7984 に設定し、暗号スイートのセキュリティ レベルを high に設定し、Web サーバを TLSv1.2 を使用した接続のみを受け付けるように設定し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable https
UCS-A /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
UCS-A /system/services* # set https keyring kring7984
UCS-A /system/services* # set https cipher-suite-mode high
UCS-A /system/services* # set https ssl-protocol tls1-2
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

HTTPS の設定解除

始める前に

HTTP から HTTPS へのリダイレクションを無効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **disable https**	HTTPS サービスを無効にします。
ステップ 4	UCS-A /system/services # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、HTTPS を無効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # disable https
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

証明書、キー リング、トラスト ポイント

HTTPS は、公開キーインフラストラクチャ（PKI）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。通常、長いキーは短いキーよりもより安全です。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。そして、追加のキー リングを作成できます。

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、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の自己署名証明書が含まれます。

UCS M5サーバの CIMC の自己署名 KVM 証明書を、ユーザが生成したパブリック証明書に変更できます。ただし、パスワードで保護された X.509 証明書秘密キーはサポートされません。KVM 証明書の作成 （100 ページ）このプロセスに関する詳細情報を提供します。

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。

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。

信頼できない CA 署名付き証明書の作成

パブリック認証局（CA）を使用して証明書の生成と署名を行う代わりに、独自の CA を運用して独自の証明書に署名することができます。証明書とキーのペアを生成するには、2048 ビットの RSA鍵と x.509 PEM 証明書を生成する必要があります。このセクションでは、Linux で実行されている OpenSSL 証明書サーバを使用して CA を作成するコマンドおよび証明書を生成するコマンドについて説明します。OpenSSL の詳細については、http://www.openssl.org を参照してください。

（注）　これらのコマンドは、OpenSSL パッケージを使用している Linux サーバで入力します。

始める前に

組織内のサーバで、証明書サーバのソフトウェアパッケージを取得してインストールします。

手順

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out** *CA_keyfilename keysize* 例： `# openssl genrsa -out cert.private 2048`	このコマンドは、CA で使用される RSA 秘密キーを生成します。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。
ステップ 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* 例： `# openssl req -new -x509 -days 365 -key cert.private -out cert.pem`	このコマンドは、指定されたキーを使用して、CA の自己署名証明書を新規に作成します。証明書は指定された期間有効になります。このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 証明書サーバは、アクティブな CA です。
ステップ 3	（任意） **openssl x509 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf** 例： `# openssl x509 -req -days 365 -in csr.txt -CA cert.pem -set_serial 04 -CAkey cert.private -out myserver05.crt -extfile openssl.conf`	このコマンドは、CA が CSR ファイルを使用してサーバ証明書を生成するように指示します。 サーバ証明書は、出力ファイルに含まれています。

例

この例は、CA の作成方法、および新規に作成された CA が署名するサーバ証明書の生成方法を示します。これらのコマンドは、OpenSSL を実行している Linux サーバで入力します。

```
# /usr/bin/openssl genrsa -out cert.private 2048 Generating RSA private key,
2048 bit long modulus .............++++++ .....++++++ e is 65537 (0x10001) #
/usr/bin/openssl req -new -x509 -days 365 -key cert.private -out cert.pem You
 are about to be asked to enter information that will be incorporated into your
 certificate request. What you are about to enter is what is called a
Distinguished Name or a DN. There are quite a few fields but you can leave some
 blank For some fields there will be a default value, If you enter '.', the
field will be left blank. ----- Country Name (2 letter code) [GB]:US State or
 Province Name (full name) [Berkshire]:California Locality Name (eg, city)
[Newbury]:San Jose Organization Name (eg, company) [My Company Ltd]:Example
Incorporated Organizational Unit Name (eg, section) []:Unit A Common Name (eg,
```

```
 your name or your server's hostname) []:example.com Email Address
[]:admin@example.com # /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA
cert.pem -set_serial 01 -CAkey cert.private -out server.crt -extfile openssl.conf
 Signature ok subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit
A/CN=example.com/emailAddress=john@example.com Getting CA Private Key #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **create keyring** *keyring-name*	キー リングを作成し、名前を指定します。
ステップ 3	UCS-A /security/keyring # **set modulus** {**mod1024** | **mod1536** | **mod2048** | **mod512**}	SSL キーのビット長を設定します。
ステップ 4	UCS-A /security/keyring # **commit-buffer**	トランザクションをコミットします。

例

次の例は、1024 ビットのキー サイズのキー リングを作成します。

```
UCS-A# scope security
UCS-A /security # create keyring kr220
UCS-A /security/keyring* # set modulus mod1024
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring #
```

次のタスク

このキー リングの証明書要求を作成します。

デフォルト キー リングの再生成

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、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。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ 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	UCS-A /security # **scope keyring default**	デフォルト キー リングでキー リング セキュリティ モードを開始します。
ステップ 3	UCS-A /security/keyring # **set regenerate yes**	デフォルト キー リングを再生成します。
ステップ 4	UCS-A /security/keyring # **commit-buffer**	トランザクションをコミットします。

例

次に、デフォルト キー リングを再生成する例を示します。

```
UCS-A# scope security
UCS-A /security # scope keyring default
UCS-A /security/keyring* # set regenerate yes
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring #
```

基本オプション付きのキー リングの証明書要求の作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope keyring** *keyring-name*	キー リングのコンフィギュレーション モードを開始します。
ステップ 3	UCS-A /security/keyring # **create certreq** {**ip** [*ipv4-addr* | *ipv6-v6*] |**subject-name** *name*}	指定された IPv4 または IPv6 アドレス、またはファブリック インターコネクトの名前を使用して証明書要求を作成します。証明書要求のパスワードを入力するように求められます。
ステップ 4	UCS-A /security/keyring/certreq # **commit-buffer**	トランザクションをコミットします。
ステップ 5	UCS-A /security/keyring # **show certreq**	コピーしてトラスト アンカーまたは認証局に送信可能な証明書要求を表示します。

例

次の例では、基本オプション付きのキー リングについてIPv4アドレスで証明書要求を作成して表示します。

```
UCS-A# scope security
UCS-A /security # scope keyring kr220
UCS-A /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
Certificate request password:
Confirm certificate request password:
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

UCS-A /security/keyring #
```

詳細オプション付きのキー リングの証明書要求の作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope keyring** *keyring-name*	キー リングのコンフィギュレーション モードを開始します。
ステップ 3	UCS-A /security/keyring # **create certreq**	証明書要求を作成します。
ステップ 4	UCS-A /security/keyring/certreq* # **set country** *country name*	会社が存在している国の国コードを指定します。
ステップ 5	UCS-A /security/keyring/certreq* # **set dns** *DNS Name*	要求に関連付けられたドメイン ネーム サーバ（DNS）アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /security/keyring/certreq* # **set e-mail** *E-mail name*	証明書要求に関連付けられた電子メール アドレスを指定します。
ステップ 7	UCS-A /security/keyring/certreq* # **set ip** *certificate request ip-address* | **ipv6** *certificate request ipv6-address*	Cisco UCS ドメインの IPv4 または IPv6 アドレスを指定します。
ステップ 8	UCS-A /security/keyring/certreq* # **set fi-a-ip** *certificate request FI A ip-address* | **fi-a-ipv6** *certificate request FI A ipv6-address*	ファブリック インターコネクト A の IPv4 または IPv6 アドレスを指定します。
ステップ 9	UCS-A /security/keyring/certreq* # **set fi-b-ip** *certificate request FI B ip-address* | **fi-b-ipv6** *certificate request FI B ipv6-address*	ファブリック インターコネクト B の IPv4 または IPv6 アドレスを指定します。
ステップ 10	UCS-A /security/keyring/certreq* # **set locality** *locality name (eg, city)*	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を指定します。
ステップ 11	UCS-A /security/keyring/certreq* # **set org-name** *organization name*	証明書を要求している組織を指定します。
ステップ 12	UCS-A /security/keyring/certreq* # **set org-unit-name** *organizational unit name*	組織ユニットを指定します。
ステップ 13	UCS-A /security/keyring/certreq* # **set password** *certificate request password*	証明書要求に関するオプションのパスワードを指定します。
ステップ 14	UCS-A /security/keyring/certreq* # **set state** *state, province or county*	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を指定します。
ステップ 15	UCS-A /security/keyring/certreq* # **set subject-name** *certificate request name*	ファブリック インターコネクトの完全修飾ドメイン名を指定します。
ステップ 16	UCS-A /security/keyring/certreq* # **commit-buffer**	トランザクションをコミットします。
ステップ 17	UCS-A /security/keyring # **show certreq**	コピーしてトラストアンカーまたは認証局に送信可能な証明書要求を表示します。

例

次の例では、詳細オプション付きのキー リングについて IPv4 アドレスで証明書要求を作成して表示します。

```
UCS-A# scope security
UCS-A /security # scope keyring kr220
```

```
UCS-A /security/keyring # create certreq
UCS-A /security/keyring/certreq* # set ip 192.168.200.123
UCS-A /security/keyring/certreq* # set fi-a-ip 192.168.200.124
UCS-A /security/keyring/certreq* # set fi-b-ip 192.168.200.125
UCS-A /security/keyring/certreq* # set subject-name sjc04
UCS-A /security/keyring/certreq* # set country US
UCS-A /security/keyring/certreq* # set dns bgl-samc-15A
UCS-A /security/keyring/certreq* # set e-mail test@cisco.com
UCS-A /security/keyring/certreq* # set locality new york city
UCS-A /security/keyring/certreq* # set org-name "Cisco Systems"
UCS-A /security/keyring/certreq* # set org-unit-name Testing
UCS-A /security/keyring/certreq* # set state new york
UCS-A /security/keyring/certreq* # commit-buffer
UCS-A /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request FI A ip address: 192.168.200.124
Certificate request FI B ip address: 192.168.200.125
Certificate request e-mail name: test@cisco.com
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

UCS-A /security/keyring/certreq #
```

次のタスク

- 証明書要求のテキストを BEGIN および END 行を含めてコピーし、ファイルに保存します。キーリングの証明書を取得するため、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。
- 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。

KVM 証明書の作成

この手順を使用して、KVM 証明書を作成できます。この操作により、CIMC がリブートします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / blade-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope cimc**	シャーシ サーバ CIMC モードを開始します。
ステップ 3	UCS-A /chassis/server/cimc # **create kvm-certificate**	KVM 証明書を作成します。
ステップ 4	UCS-A /chassis/server/cimc/kvm-certificate* # set certificate	指定されたユーザ生成のパブリック証明書を設定します。
ステップ 5	UCS-A /chassis/server/cimc/kvm-certificate* # set key	対応するユーザ生成の秘密キーを設定します。 （注） パスワード保護された X.509 証明書の秘密キーはサポートされていません。
ステップ 6	UCS-A /chassis/server/cimc/kvm-certificate* # **commit-buffer**	トランザクションをシステムの設定にコミットします。 この操作により、CIMC がリブートします。

例

次に、KVM 証明書を作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope server 1/3
UCS-A /chassis/server # scope cimc
UCS-A /chassis/server/cimc # create kvm-certificate
UCS-A /chassis/server/cimc/kvm-certificate* # set certificate
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Prompt Certificate:
>
...

UCS-A /chassis/server/cimc/kvm-certificate* # set key
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Prompt Key:
>
...

UCS-A /chassis/server/cimc/kvm-certificate* # commit-buffer
UCS-A /chassis/server/cimc/kvm-certificate #
```

KVM 証明書のクリア

この操作により、CIMC がリブートします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id* / *blade-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope cimc**	シャーシ サーバ CIMC モードを開始します。
ステップ 3	UCS-A /chassis/server/cimc # **clear kvm-certificate**	KVM 証明書をクリアします。
ステップ 4	UCS-A /chassis/server/cimc* # **commit-buffer**	トランザクションをシステムの設定にコミットします。 この操作により、CIMC がリブートします。

例

次に、KVM 証明書をクリアし、トランザクションをコミットする例を示します。

```
UCS-A# scope server 1/3
UCS-A /chassis/server # scope cimc
UCS-A /chassis/server/cimc # clear kvm-certificate
Warning: When committed, this operation will result in CIMC reboot.
UCS-A /chassis/server/cimc* # commit-buffer
UCS-A /chassis/server/cimc #
```

トラスト ポイントの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **create trustpoint** *name*	トラスト ポイントを作成し、その名前を指定します。
ステップ 3	UCS-A /security/trustpoint # **set certchain** [*certchain*]	このトラスト ポイントの証明書情報を指定します。 コマンドで証明書情報を指定しない場合、ルート認証局（CA）への認証パス

	コマンドまたはアクション	目的
		を定義するトラスト ポイントのリストまたは証明書を入力するように求められます。入力内容の次の行に、ENDOFBUF と入力して終了します。 **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。
ステップ 4	UCS-A /security/trustpoint # **commit-buffer**	トランザクションをコミットします。

例

次の例は、トラスト ポイントを作成し、トラスト ポイントに証明書を提供します。

```
UCS-A# scope security
UCS-A /security # create trustpoint tPoint10
UCS-A /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
UCS-A /security/trustpoint* # commit-buffer
UCS-A /security/trustpoint #
```

次のタスク

トラスト アンカーまたは認証局からキー リング証明書を取得し、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

始める前に

- キー リング証明書の証明書チェーンを含むトラスト ポイントを設定します。
- トラスト アンカーまたは認証局からキー リング証明書を取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope keyring** *keyring-name*	証明書を受け取るキー リングでコンフィギュレーション モードを開始します。
ステップ 3	UCS-A /security/keyring # **set trustpoint** *name*	キー リング証明書の取得元のトラスト アンカーまたは認証局に対しトラスト ポイントを指定します。
ステップ 4	UCS-A /security/keyring # **set cert**	キー リング証明書を入力してアップロードするためのダイアログを起動します。 プロンプトで、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。証明書の後の行に ENDOFBUF と入力して、証明書の入力を完了します。 **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。
ステップ 5	UCS-A /security/keyring # **commit-buffer**	トランザクションをコミットします。

例

次に、トラストポイントを指定し、証明書をキー リングにインポートする例を示します。

```
UCS-A# scope security
UCS-A /security # scope keyring kr220
UCS-A /security/keyring # set trustpoint tPoint10
UCS-A /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
```

```
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring #
```

次のタスク

キー リングを使用して HTTPS サービスを設定します。

キーリングの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **delete keyring** *name*	名前付きのキー リングを削除します。
ステップ 3	UCS-A /security # **commit-buffer**	トランザクションをコミットします。

例

次の例では、キー リングを削除します。

```
UCS-A# scope security
UCS-A /security # delete keyring key10
UCS-A /security* # commit-buffer
UCS-A /security #
```

トラスト ポイントの削除

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ 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	UCS-A /security # **delete trustpoint** *name*	指定したトラスト ポイントを削除します。
ステップ 3	UCS-A /security # **commit-buffer**	トランザクションをコミットします。

例

次に、トラスト ポイントを削除する例を示します。

```
UCS-A# scope security
UCS-A /security # delete trustpoint tPoint10
UCS-A /security* # commit-buffer
UCS-A /security #
```

HTTPS への HTTP リダイレクションの有効化

始める前に

HTTP と HTTPS の両方を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **enable http-redirect**	HTTP リダイレクト サービスを有効にします。 有効の場合、HTTP 経由で試行される通信はすべて同等の HTTPS アドレスにリダイレクトされます。 このオプションは、この Cisco UCS ドメイン への HTTP アクセスを実質的に無効にします。
ステップ 4	UCS-A /system/services # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、HTTP から HTTPS へのリダイレクションを有効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable http-redirect
Warning: When committed, this closes all the web sessions.
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

ネットワーク関連のサービス

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。 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。
- 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 モデルは選択されたセキュリティ レベルと組み合わされ、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権限を決定します。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 *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	未対応	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	未対応	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	非対応	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のみを承認します。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、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）

Cisco UCS Manager リリース 3.2(3) および以降のリリースでは、SNMPv3 が連邦情報処理標準（FIPS） モードの場合、MD5 認証をサポートしていません。したがって、既存の、または新しく作成された MD5 認証の SNMPv3 ユーザは、これらのリリースでは展開されず、次のエラー メッセージが表示されます。

```
Major     F1036    2018-02-01T14:36:32.995     99095 SNMP User testuser can't be
deployed. Error: MD5 auth is not supported
```

このようなユーザを展開するには、認証タイプを [SHA] に変更します。

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。

Cisco UCS Managerリリース 3.2(3) および以降のリリースでは、SNMPv3 ユーザ AES 暗号化なしではサポートされません。したがって、既存の、または新しく作成された、AES暗号化されていない SNMPv3 ユーザは、これらのリリースでは展開されず、次のエラー メッセージが表示されます。

```
Major     F1036    2018-02-01T14:36:32.995     99095 SNMP User testuser can't be
deployed. Error: AES is not enabled
```

このようなユーザを展開するには、[AES-128] 暗号化を有効にします。

SNMP の有効化および 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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **enable snmp**	SNMP を有効にします。
ステップ 3	UCS-A /monitoring # **set snmp community**	snmp コミュニティ モードを開始します。
ステップ 4	UCS-A /monitoring # **Enter a snmp community:** *community-name*	SNMP コミュニティを指定します。パスワードとしてコミュニティ名を使用します。コミュニティ名は、最大 32 文字の英数字で指定できます。
ステップ 5	UCS-A /monitoring # **set snmp syscontact** *system-contact-name*	SNMP 担当者のシステムの連絡先を指定します。システムの連絡先名（電子メール アドレスや、名前と電話番号など）は、最大 255 文字の英数字で指定できます。
ステップ 6	UCS-A /monitoring # **set snmp syslocation** *system-location-name*	SNMP エージェント（サーバ）が実行されるホストの場所を指定します。システム ロケーション名は、最大 512 文字の英数字で指定できます。
ステップ 7	UCS-A /monitoring # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、SNMP を有効にし、SnmpCommSystem2 という名前の SNMP コミュニティを設定し、contactperson という名前のシステム連絡先を設定し、systemlocation という名前の連絡先ロケーションを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # set snmp community
UCS-A /monitoring* # Enter a snmp community: SnmpCommSystem2
UCS-A /monitoring* # set snmp syscontact contactperson1
UCS-A /monitoring* # set snmp syslocation systemlocation
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

次のタスク

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **enable snmp**	SNMP を有効にします。
ステップ 3	UCS-A /monitoring # **create snmp-trap** {*hostname* | *ip-addr* | *ip6-addr*}	指定したホスト名、IPv4 アドレス、または IPv6 アドレスで SNMP トラップ ホストを作成します。 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ができます。
ステップ 4	UCS-A /monitoring/snmp-trap # **set community** *community-name*	SNMP トラップに使用する SNMP コミュニティ名を指定します。
ステップ 5	UCS-A /monitoring/snmp-trap # **set port** *port-num*	SNMP トラップに使用するポートを指定します。
ステップ 6	UCS-A /monitoring/snmp-trap # **set version** {**v1** | **v2c** | **v3**}	トラップに使用する SNMP のバージョンとモデルを指定します。
ステップ 7	（任意） UCS-A /monitoring/snmp-trap # **set notification type** {**traps** | **informs**}	送信するトラップのタイプ。ここに表示される値は次のとおりです。 • バージョンで v2c または v3 を選択した場合は **traps**。 • バージョンに v2c を選択する場合は **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。
ステップ 8	（任意） UCS-A /monitoring/snmp-trap # **set v3 privilege** {**auth** | **noauth** | **priv**}	バージョンに v3 を選択した場合、トラップに関連付けられた権限。 ここに表示される値は次のとおりです。 • **auth**：認証あり、暗号化なし

	コマンドまたはアクション	目的
		• **noauth**：認証なし、暗号化なし • **priv**：認証あり、暗号化あり
ステップ 9	UCS-A /monitoring/snmp-trap # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、SNMP を有効にし、IPv4 アドレスを使用して SNMP トラップを作成し、トラップがポート 2 で SnmpCommSystem2 コミュニティを使用するよう指定し、バージョンを v3 に設定し、通知タイプを traps に設定し、v3 権限を priv に設定し、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-trap 192.168.100.112
UCS-A /monitoring/snmp-trap* # set community SnmpCommSystem2
UCS-A /monitoring/snmp-trap* # set port 2
UCS-A /monitoring/snmp-trap* # set version v3
UCS-A /monitoring/snmp-trap* # set notificationtype traps
UCS-A /monitoring/snmp-trap* # set v3 privilege priv
UCS-A /monitoring/snmp-trap* # commit-buffer
UCS-A /monitoring/snmp-trap #
```

次の例は、SNMP を有効にし、IPv6 アドレスを使用して SNMP トラップを作成し、トラップがポート 2 で SnmpCommSystem3 コミュニティを使用するよう指定し、バージョンを v3 に設定し、通知タイプを traps に設定し、v3 権限を priv に設定し、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-trap  2001::1
UCS-A /monitoring/snmp-trap* # set community SnmpCommSystem3
UCS-A /monitoring/snmp-trap* # set port 2
UCS-A /monitoring/snmp-trap* # set version v3
UCS-A /monitoring/snmp-trap* # set notificationtype traps
UCS-A /monitoring/snmp-trap* # set v3 privilege priv
UCS-A /monitoring/snmp-trap* # commit-buffer
UCS-A /monitoring/snmp-trap #
```

SNMP トラップの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング 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	UCS-A /monitoring # **delete snmp-trap** {*hostname* | *ip-addr*}	指定したホスト名または IP アドレスの指定した SNMP トラップ ホストを削除します。
ステップ 3	UCS-A /monitoring # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、IP アドレス 192.168.100.112 で SNMP トラップを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # delete snmp-trap 192.168.100.112
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

SNMPv3 ユーザの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **enable snmp**	SNMP を有効にします。
ステップ 3	UCS-A /monitoring # **create snmp-user** *user-name*	指定された SNMPv3 ユーザを作成します。 SNMP ユーザ名は、ローカル ユーザ名と同じにはできません。ローカル ユーザ名と一致しない SNMP ユーザ名を選択します。
ステップ 4	UCS-A /monitoring/snmp-user # **set aes-128** {**no** | **yes**}	AES-128 暗号化の使用を有効または無効にします。
ステップ 5	UCS-A /monitoring/snmp-user # **set auth** {**md5** | **sha**}	MD5 または DHA 認証の使用を指定します。
ステップ 6	UCS-A /monitoring/snmp-user # **set password**	ユーザ パスワードを指定します。 **set password** コマンドを入力すると、パスワードの入力と確認を促すプロンプトが表示されます。

	コマンドまたはアクション	目的
ステップ 7	UCS-A /monitoring/snmp-user # **set priv-password**	ユーザ プライバシー パスワードを指定します。 **set priv-password** コマンドを入力すると、プライバシー パスワードの入力と確認を促すプロンプトが表示されます。
ステップ 8	UCS-A /monitoring/snmp-user # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、SNMP を有効にし、snmp-user14 という名前の SNMPv3 ユーザを作成し、AES-128 暗号化を無効にし、MD5 認証の使用を指定し、パスワードおよびプライバシー パスワードを設定し、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-user snmp-user14
UCS-A /monitoring/snmp-user* # set aes-128 no
UCS-A /monitoring/snmp-user* # set auth md5
UCS-A /monitoring/snmp-user* # set password
Enter a password:
Confirm the password:
UCS-A /monitoring/snmp-user* # set priv-password
Enter a password:
Confirm the password:
UCS-A /monitoring/snmp-user* # commit-buffer
UCS-A /monitoring/snmp-user #
```

SNMPv3 ユーザの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **delete snmp-user** *user-name*	指定した SNMPv3 ユーザを削除します。
ステップ 3	UCS-A /monitoring # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、snmp user14 という名前の SNMPv3 ユーザを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # delete snmp-user snmp-user14
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

Telnet の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /services # **enable telnet-server**	Telnet サービスを有効にします。
ステップ 4	UCS-A /services # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、Telnet を有効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /services # enable telnet-server
UCS-A /services* # commit-buffer
UCS-A /services #
```

CIMC Web サービスの有効化

CIMC Web サービスを有効にするには：

- admin 権限でログインする必要があります。
- CIMC Web サービスは、デフォルトでは有効なので、無効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system** /	システム モードを開始します。
ステップ 2	UCS-A /system #**scope services**/	システムのサービス 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 3	UCS-A/system/services #**enable cimcwebsvc**/	CIMC Web サービスを有効にします。
ステップ 4	UCS-A/system/services *# **commit-buffer**/	トランザクションをシステムの設定にコミットします。

例

次に、CIMC Web サービスを有効にし、トランザクションを保存する例を示します。

```
UCS-A# scope system
UCS-A/system # scope services
UCS-A/system/services # enable cimcwebsvc
UCS-A/system/services *# commit-buffer
UCS-A/system/services # commit-buffer
UCS-A/system/services # show cimcwebsvc
Name: cimcwebservice
    Admin State: Enabled
```

CIMC Web サービスの無効化

CIMC Web サービスを無効にするには：

- admin 権限でログインする必要があります。
- CIMC Web サービスを有効にする必要があります。

（注） CIMC Web サービスはデフォルトで有効となっています。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system** /	システム モードを開始します。
ステップ 2	UCS-A /system #**scope services**/	システムのサービス モードを開始します。
ステップ 3	UCS-A/system/services #**disable cimcwebsvc**/	CIMC Web サービスを無効にします。
ステップ 4	UCS-A/system/services *# **commit-buffer**/	トランザクションをシステムの設定にコミットします。

例

次に、CIMC Web サービスを無効にし、トランザクションを保存する例を示します。

```
UCS-A# scope system
UCS-A/system # scope services
UCS-A/system/services # disable cimcwebsvc
UCS-A/system/services *# commit-buffer
UCS-A/system/services # commit-buffer
UCS-A/system/services # show cimcwebsvc
Name: cimcwebservice
    Admin State: Disabled
```

通信サービスの無効化

手順

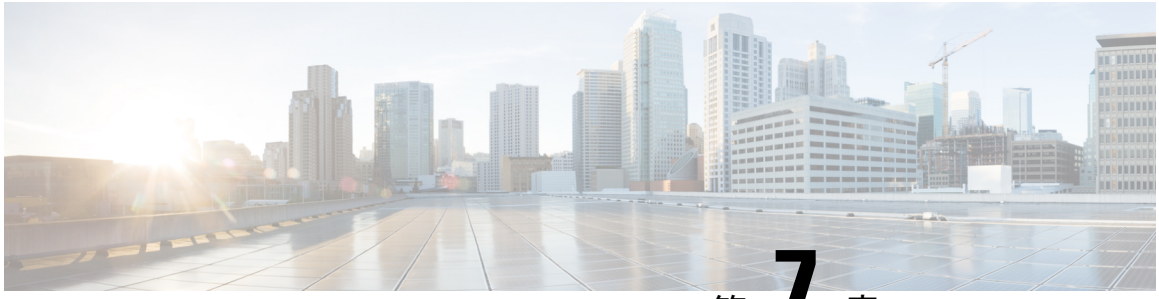
	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **disable** *service-name*	指定したサービスを無効にします。ここで *service-name* 引数は次のいずれかのキーワードです。 • *cimxml* ：CIM XML サービスを無効にします。 • **http** ：HTTP サービスを無効にします。 • **https** ：HTTPS サービスを無効にします。 • **telnet-server** ：Telnet サービスを無効にします。
ステップ 4	UCS-A /system/services # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、CIM XML を無効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A# scope services
UCS-A /system/services # disable cimxml
```

```
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```



第 7 章

CIMC セッション管理

CIMC セッション管理

Cisco UCS Manager では、KVM、vMedia、および SoL セッションを表示および終了できます。管理者権限を持つユーザは、任意のユーザの KVM、vMedia、および SoL セッションを切断できます。. Cisco Integrated Management Controller（CIMC）により、セッション情報が Cisco UCS Manager に提供されます。Cisco UCS Manager は CIMC からイベントを取得すると、そのセッション テーブルを更新し、すべてのユーザに情報を表示します。

セッション情報は次の情報で構成されます。

- 名前：セッションを開始したユーザの名前。
- セッション ID：セッションに関連付けられた ID。ブレードのセッション ID の形式は [unique identifier] _ [chassis id] _ [Blade id] です。ラックのセッション ID の形式は [unique identifier] _ 0 _ [Rack id] です。
- セッション タイプ：KVM、vMedia、または SoL。
- ユーザの権限レベル：読み取り/書き込み、読み取り専用、または付与。
- 管理状態：アクティブまたは非アクティブ。値は、セッションがアクティブの場合はアクティブです。セッション終了コマンドが発行されたがセッションが終了していない場合、値は非アクティブとなります。この状況は、サーバの FSM が別の操作で進行中である場合、または CIMC への接続が失われた場合に発生します。
- 送信元アドレス：セッションが開かれたコンピュータの IP アドレス。
- サービス プロファイル：セッションに関連付けられたサービス プロファイル。CIMC セッションのサービス プロファイルの属性値は、セッションがサービス プロファイルから提供された IP アドレスで開くときにだけ表示されます。
- サーバ：セッションに関連付けられたサーバの名前。
- ログイン時刻：セッションが開始された日時。

- 最終更新時刻：セッション情報が CIMC により更新された最終時刻。

新しいセッションは通常、ユーザが KVM、vMedia、または SOL に接続するときに追加されます。Pnuos vMedia セッションは、ユーザ名 __vmediausr__ を使用したサーバ検出時にセッション テーブルに表示されます。

CIMC セッション データは Cisco UCS Manager GUI の [CIMC Sessions] タブで使用できます。ユーザによって終了された CIMC セッションは、適切な詳細とともにログに記録された監査です。

（注） このガイドに記載されている GUI および CLI タスクを実行するには、2.1(2a) 以上の CIMC イメージ バージョンがブレード サーバのセッション管理サポートに必要です。1.5(1l) 以上の最新の CIMC イメージ バージョンが、ラック サーバに必要です。

ローカル ユーザにより開かれた CIMC セッションの表示

ローカル ユーザにより開かれたすべての CIMC セッション、または特定のローカル ユーザにより開かれた CIMC セッションを表示するには、このタスクを実行します。

（注） 特定のサーバまたはサービス プロファイル オプションの CIMC セッションの表示は CLI にありません。これは、GUI で可能です。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ 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	UCS-A /security # **show cimc-sessions local**	ローカル ユーザにより開かれたすべての CIMC セッションを表示します。
ステップ 3	UCS-A /security # **show cimc-sessions local** *user-name*	特定のローカル ユーザにより開かれたすべての CIMC セッションを表示します。

例

次に、以下を表示する例を示します。

- ローカル ユーザにより開かれたすべての CIMC セッション
- 特定のローカル ユーザにより開かれた CIMC セッション

- 特定のローカル ユーザにより開かれた CIMC セッションの詳細

```
All sessions opened by local users:
UCS-A # scope security
UCS-A /security # show cimc-sessions local

Session ID   Type     User      Source Addr     Admin State
----------   ------ --------- --------------- ------------
42_1_1       Kvm      admin     10.106.22.117     Active
4_1_5        Kvm      admin     10.106.22.117     Active
5_1_5        Vmedia   admin     10.106.22.117     Active

Session opened by a specific local user:
UCS-A /security # show cimc-sessions local admin
Session ID   Type     User      Source Addr     Admin State
----------   ------ --------- --------------- ------------
42_1_1       Kvm      admin     10.106.22.117     Active

Details of session opened by a specific local user:
UCS-A /security # show cimc-sessions local admin detail
Session ID 42_1_1
   Type: Kvm
   User: admin
   Source Addr: 10.106.22.117
   Login Time: 2013-06-28T06:09:53.000
   Last Updated Time: 2013-06-28T06:21:52.000
   Admin State: Active
   Priv: RW
   Server: sys/chassis-1/blade-1
   Service Profile:
```

リモート ユーザにより開かれた CIMC セッションの表示

リモート ユーザにより開かれたすべての CIMC セッション、または特定のリモート ユーザにより開かれた CIMC セッションを表示するには、このタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ 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	UCS-A /security # **show cimc-sessions remote**	リモート ユーザにより開かれたすべての CIMC セッションを表示します。
ステップ 3	UCS-A /security # **show cimc-sessions remote** *user-name*	特定のリモート ユーザにより開かれたすべての CIMC セッションを表示します。

例

次に、以下を表示する例を示します。

- リモート ユーザにより開かれたすべての CIMC セッション
- 特定のリモート ユーザにより開かれた CIMC セッション
- 特定のリモート ユーザにより開かれた CIMC セッションの詳細

```
All sessions opened by remote users:
UCS-A # scope security
UCS-A /security # show cimc-sessions remote

Session ID   Type     User            Source Addr      Admin State
----------   ------ ---------       ---------------   ------------
43_1_1       Kvm     administrator    10.106.22.117     Active
6_1_5        Kvm     test-remote      10.106.22.117     Active
7_1_5        Vmedia  test-remote      10.106.22.117     Active

Session opened by a specific remote user:
UCS-A /security # show cimc-sessions remote administrator

Session ID   Type     User            Source Addr      Admin State
----------   ------ ---------       ---------------   ------------
43_1_1       Kvm     administrator    10.106.22.117     Active

Details of session opened by a specific remote user:
UCS-A /security # show cimc-sessions remote administrator detail
Session ID 43_1_1
   Type: Kvm
   User: administrator
   Source Addr: 10.106.22.117
   Login Time: 2013-06-28T06:09:53.000
   Last Updated Time: 2013-06-28T06:21:52.000
   Admin State: Active
   Priv: RW
   Server: sys/chassis-1/blade-1
   Service Profile:
```

IPMI ユーザにより開かれた CIMC セッションの表示

IPMI ユーザにより開かれた CIMC セッションを表示するには、次の手順を完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org** *org-name*	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope ipmi-access-profile** *profile-name*	IPMI アクセス プロファイル名を入力します。
ステップ 3	UCS-A /org/ipmi-access-profile # **scope ipmi-user** *user-name*	IPMI ユーザ名を入力します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /org/ipmi-access-profile/ipmi-user # **show cimc-sessions**	指定された IPMI ユーザにより開かれたすべての CIMC セッションを表示します。

例

次の例では、IPMI ユーザにより開かれたすべての CIMC セッションを表示する方法を示します。

```
UCS-A # scope org Finance
UCS-A /org* # scope ipmi-access-profile ReadOnly
UCS-A /org/ipmi-access-profile* # scope ipmi-user alice
UCS-A /org/ipmi-access-profile/ipmi-user # show cimc-sessions

Session ID    Type    User        Source Addr       Admin State
----------   ------  ---------   ---------------   --------------
45_1_1        sol     alice       10.106.22.117     Active
```

サーバの CIMC セッションのクリア

このタスクでは、サーバ上に開かれたすべての CIMC セッションをクリアする方法を示します。セッション タイプとユーザ名に基づいて、サーバの CIMC セッションをクリアすることもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ 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	UCS-A /security # **terminate cimc-sessions server** *chassis-id/blade-id*	シャーシの特定のブレード サーバの CIMC セッションをクリアします。
ステップ 3	UCS-A /security # **terminate cimc-sessions server** *Rack-server-id*	特定のラック サーバの CIMC セッションをクリアします。
ステップ 4	UCS-A /security # **terminate cimc-sessions server** *server-id* **type** *session-type*	サーバの特定のタイプの CIMC セッションをクリアします。
ステップ 5	UCS-A /security # **terminate cimc-sessions server** *server-id* **user-name** *user-name*	サーバの特定のユーザの CIMC セッションをクリアします。

例

最初の例では、サーバのすべての CIMC セッションをクリアする方法を示します。2 番目の例では、サーバの特定のタイプの CIMC セッションをクリアする方法を示します。3 番目の例では、サーバの特定のユーザの CIMC セッションをクリアする方法を示します。

```
UCS-A /security # scope security
UCS-A /security # terminate cimc-sessions server 2/1
This will close KVM sessions. Are you sure? (yes/no):yes
UCS-A /security

UCS-A # scope security
UCS-A /security # terminate cimc-sessions server 2/1 type kvm
This will close KVM sessions. Are you sure? (yes/no):yes

UCS-A # scope security
UCS-A /security # terminate cimc-sessions server 2/1 user-name test-user
This will close KVM sessions. Are you sure? (yes/no):yes
```

モジュラ サーバの CIMC セッションのクリア

このタスクでは、サーバ上に開かれたすべての CIMC セッションをクリアする方法を示します。セッション タイプとユーザ名に基づいて、サーバの CIMC セッションをクリアすることもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ 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	UCS-A /security # **terminate cimc-sessions server** *chassis-id* / *cartridge-id* / *server-id*	シャーシ上の特定のモジュラ サーバ カートリッジの CIMC セッションをクリアします。
ステップ 3	UCS-A /security # **terminate cimc-sessions server** *chassis-id* / *cartridge-id* / *server-id* **type** *session-type*	サーバの特定のタイプの CIMC セッションをクリアします。
ステップ 4	UCS-A /security # **terminate cimc-sessions server** *chassis-id* / *cartridge-id* / *server-id* **user-name** *user-name*	サーバの特定のユーザの CIMC セッションをクリアします。

例

最初の例では、サーバのすべての CIMC セッションをクリアする方法を示します。2 番目の例では、サーバの特定のタイプの CIMC セッションをクリアする方法を示しま

す。3 番目の例では、サーバの特定のユーザの CIMC セッションをクリアする方法を示します。

```
UCS-A /security # scope security
UCS-A /security # terminate cimc-sessions server 1/2/1
This will close cimc sessions. Are you sure? (yes/no):yes
UCS-A /security

UCS-A # scope security
UCS-A /security # terminate cimc-sessions server 1/2/1 type kvm
This will close KVM sessions. Are you sure? (yes/no):yes

UCS-A # scope security
UCS-A /security # terminate cimc-sessions server 1/2/1 user-name test-user
This will close cimc sessions. Are you sure? (yes/no):yes
```

ローカル ユーザにより開かれたすべての CIMC セッションのクリア

このタスクでは、ローカル ユーザにより開かれたセッションをクリアする方法を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ 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	UCS-A /security # **terminate cimc-sessions local-user** *user-name*	ローカル ユーザにより開かれたすべての CIMC セッションをクリアします。
ステップ 3	UCS-A /security # **terminate cimc-sessions local-user** *user-name* **type** {**kvm** | **vmedia** **sol** | **all**}	ローカル ユーザにより開かれた特定のセッションタイプのすべての CIMC セッションをクリアします。

例

次の例では、ローカル ユーザにより開かれた CIMC セッションをクリアする方法を示します。

```
UCS-A /security# scope security
UCS-A /security# terminate cimc-sessions local-user testuser
This will close cimc sessions. Are you sure? (yes/no):yes
UCS-A /security#
```

リモート ユーザにより開かれたすべての CIMC セッションのクリア

このタスクでは、リモート ユーザにより開かれた CIMC セッションをクリアする方法を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ 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	UCS-A /security # **terminate cimc-sessions remote-user** *user-name*	リモート ユーザにより開かれたすべての CIMC セッションをクリアします。
ステップ 3	UCS-A /security # **terminate cimc-sessions remote-user** *user-name* **type** {**kvm** | **vmedia** **sol** | **all**}	リモート ユーザにより開かれた特定のセッション タイプのすべての CIMC セッションをクリアします。

例

次の例では、リモート ユーザにより開かれたすべての CIMC セッションをクリアする方法を示します。

```
UCS-A /security# scope security
UCS-A /security# terminate cimc-sessions remote-user testuser
This will close cimc sessions. Are you sure? (yes/no):yes
UCS-A /security#
```

ローカル ユーザにより開かれた特定の CIMC セッションのクリア

このタスクでは、ローカル ユーザにより開かれた特定の CIMC セッションをクリアする方法を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ 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	UCS-A /security # **scope local-user** *user-name*	ローカル ユーザ モードを開始します。
ステップ 3	UCS-A /security/local user # **terminate cimc-session** *session-id*	選択した CIMC セッションをクリアします。
ステップ 4	UCS-A /security/local user* # **commit-buffer**	トランザクションをコミットします。

例

次の例では、ローカル ユーザにより開かれた特定の CIMC セッションをクリアし、トランザクションをコミットする方法を示します。

```
UCS-A /security# scope security
UCS-A /security# scope local-user admin
UCS-A /security/local user # terminate cimc-session 6_1_2
UCS-A /security/local user*# commit-buffer
UCS-A /security/local user#
```

リモート ユーザにより開かれた特定の CIMC セッションのクリア

このタスクでは、リモート ユーザにより開かれた特定の CIMC セッションをクリアする方法を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ 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	UCS-A /security # **scope remote -user** *user-name*	リモート ユーザ モードを開始します。
ステップ 3	UCS-A /security/remote user # **terminate cimc-session** *session-id*	選択した CIMC セッションをクリアします。
ステップ 4	UCS-A /security/remote user* # **commit-buffer**	トランザクションをコミットします。

例

次の例では、リモート ユーザにより開かれた特定の CIMC セッションをクリアし、トランザクションをコミットする方法を示します。

```
UCS-A /security# scope security
UCS-A /security# scope remote-user admin
UCS-A /security/remote user # terminate cimc-session 6_1_3
UCS-A /security/remote user*# commit-buffer
UCS-A /security/remote user#
```

IPMI ユーザにより開かれた CIMC セッションのクリア

IPMI ユーザにより開かれた CIMC セッションをクリアするには、次の手順を完了します。

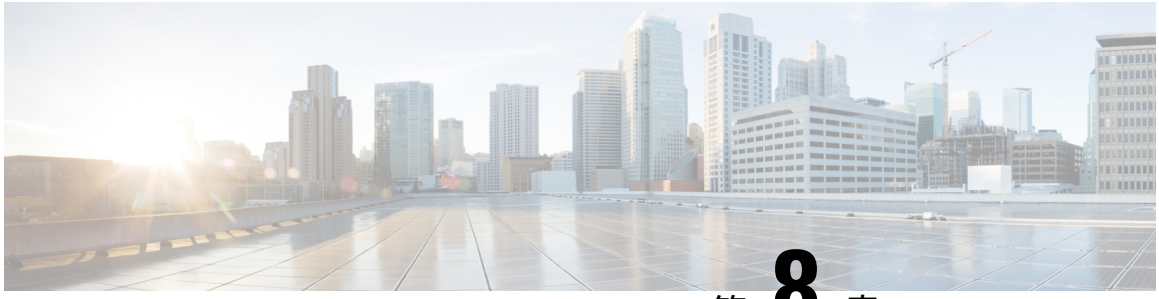
手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org** *org-name*	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope ipmi-access-profile** *profile-name*	IPMI アクセス プロファイル名を入力します。
ステップ 3	UCS-A /org/ipmi-access-profile # **scope ipmi-user** *user-name*	IPMI ユーザを入力します。
ステップ 4	UCS-A /org/ipmi-access-profile/ipmi-user # **terminate cimc-sessions** *session-id*	IPMI ユーザにより開かれた特定の CIMC セッションを終了します。
ステップ 5	UCS-A /org/ipmi-access-profile/ipmi-user * **commit-buffer**	変更をコミットします。

例

次の例では、IPMI ユーザにより開かれた特定の CIMC セッションをクリアし、変更をコミットする方法を示します。

```
UCS-A # scope org Finance
UCS-A /org* # scope ipmi-access-profile ReadOnly
UCS-A /org/ipmi-access-profile* # scope ipmi-user alice
UCS-A /org/ipmi-access-profile/ipmi-user # terminate cimc-sessions 5_1_2
UCS-A /org/ipmi-access-profile/ipmi-user* # commit-buffer
```



第 8 章

管理 IP アドレスの設定

管理 IP アドレス

Cisco UCS ドメイン 内の各サーバでは、1 つ以上の管理 IP アドレスが、Cisco Integrated Management Controller（CIMC）に割り当てられているか、またはサーバに関連付けられたサービス プロファイルに割り当てられている必要があります。Cisco UCS Manager は、CIMC で終端する外部アクセスにこれらの IP アドレスを使用します。この外部アクセスは、次のいずれかのサービスを経由できます。

- KVM コンソール
- Serial over LAN
- IPMI ツール

サーバの CIMC にアクセスするために使用される管理 IP アドレスには、アウトオブバンド（OOB）アドレス（そのアドレスからトラフィックが管理ポート経由でファブリック インターコネクトを通過する）、またはインバンドアドレス（そのアドレスからトラフィックがファブリック アップリンク ポート経由でファブリック インターコネクトを通過する）を使用できます。最大 6 つの IP アドレス（2 つはアウトオブバンド（OOB）アドレス、他 4 つはインバンドアドレス）がサーバの CIMC にアクセスするように設定できます。

以下の管理 IP アドレスを設定できます。

- サーバに直接割り当てられるスタティック OOB IPv4 アドレス

- グローバル ext-mgmt プールからサーバに割り当てられる OOB IPv4 アドレス
- サーバに関連付けられたサービス プロファイルから取得するインバンド IPv4 アドレス
- 管理 IP プールから取り込まれ、サービス プロファイルまたはサービス プロファイル テンプレートに割り当てられるインバンド IPv4 アドレス
- サーバに直接割り当てられるスタティック インバンド IPv6 アドレス
- サーバに関連付けられたサービス プロファイルから取得するインバンド IPv6 アドレス

サーバの各 CIMC およびサーバに関連付けられたサービス プロファイルに、複数の管理 IP アドレスを割り当てることができます。その場合は、それぞれ異なる IP アドレスを使用する必要があります。

サービス プロファイルに関連付けられた管理 IP アドレスは、そのサービス プロファイルとともに移動します。サービス プロファイルを別のサーバに移行するときに KVM または SoL セッションがアクティブな場合、Cisco UCS Manager はそのセッションを強制終了しますが、移行完了後にはセッションを再開しません。管理 IP アドレスは、サービス プロファイルを作成または変更するときに設定します。

（注） IP アドレスが Cisco UCS ドメイン のサーバまたはサービス プロファイルにすでに割り当てられている場合、サーバまたはサービス プロファイルにスタティック IP アドレスを割り当てることはできません。そのような設定を試行すると、Cisco UCS Manager は IP アドレスがすでに使用中であると警告し、設定を拒否します。

ARP 要求は、インバンド IP アドレスが設定された各サーバからゲートウェイ IP アドレスに毎秒送信されます。これは、現在のファブリック インターコネクトを使用したインバンド トラフィック用の接続が動作しているかを確認し、動作していない場合は他のファブリック インターコネクトに対してフェールオーバーを開始するためです。インバンド用に選択されたパスとフェールオーバー処理は、サーバのデータ トラフィックから完全に独立しています。

モジュラ サーバの管理 IP アドレスの設定

モジュラ サーバでスタティック IP アドレスを使用するための設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / cartridge-id / server-id*	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /chassis/cartridge/server # **scope cimc**	サーバ CIMC モードに入ります。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /chassis/cartridge/server/cimc # **create ext-static-ip**	指定されたサーバのスタティック管理 IP アドレスを作成します。
ステップ 4	UCS-A /chassis/cartridge/server/cimc/ext-static-ip # **set addr** *ip-addr*	サーバに割り当てられるスタティック IPv4 アドレスを指定します。
ステップ 5	UCS-A /chassis/cartridge/server/cimc/ext-static-ip # **set default-gw** *ip-addr*	IP アドレスが使用するデフォルト ゲートウェイを指定します。
ステップ 6	UCS-A /chassis/cartridge/server/cimc/ext-static-ip # **set subnet** *ip-addr*	IP アドレスのサブネット マスクを指定します。
ステップ 7	UCS-A /chassis/cartridge/server/cimc/ext-static-ip # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、シャーシ 1 カートリッジ 1 のサーバ 1 にスタティック管理 IP アドレスを設定し、スタティック IPv4 アドレス、デフォルト ゲートウェイ、サブネット マスクを設定して、トランザクションをコミットします。

```
UCS-A# scope server 1/1/1
UCS-A /chassis/cartridge/server # scope cimc
UCS-A /chassis/cartridge/server/cimc # create ext-static-ip
UCS-A /chassis/cartridge/server/cimc/ext-static-ip* # set addr 192.168.10.10
UCS-A /chassis/cartridge/server/cimc/ext-static-ip* # set default-gw 192.168.10.1
UCS-A /chassis/cartridge/server/cimc/ext-static-ip* # set subnet 255.255.255.0
UCS-A /chassis/cartridge/server/cimc/ext-static-ip* # commit-buffer
UCS-A /chassis/cartridge/server/cimc/ext-static-ip #
```

モジュラ サーバでスタティック IPv6 アドレスを使用するための設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id* / *cartridge-id* / *server-id*	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /chassis/cartridge/server # **scope cimc**	サーバ CIMC モードに入ります。
ステップ 3	UCS-A /chassis/cartridge/server/cimc # **create ext-static-ip6**	指定されたサーバのスタティック管理 IPv6 アドレスを作成します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /chassis/cartridge/server/cimc/ext-static-ip6 # **set addr ipv6-addr**	サーバに割り当てられるスタティック IPv6 アドレスを指定します。
ステップ 5	UCS-A /chassis/cartridge/server/cimc/ext-static-ip6 # **set default-gw ip6-addr**	IPv6アドレスが使用するデフォルトゲートウェイを指定します。
ステップ 6	UCS-A /chassis/cartridge/server/cimc/ext-static-ip6 # **set prefix ip6-addr**	IPv6アドレスのネットワークプレフィックスを指定します。
ステップ 7	UCS-A /chassis/cartridge/server/cimc/ext-static-ip6 # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、シャーシ 1 カートリッジ 1 のサーバ 1 にスタティック管理 IPv6 アドレスを設定し、スタティック IPv6 アドレス、デフォルト ゲートウェイ、ネットワーク プレフィックスを設定して、トランザクションをコミットします。

```
UCS-A# scope server 1/1/1
UCS-A /chassis/cartridge/server # scope cimc
UCS-A /chassis/cartridge/server/cimc # create ext-static-ip6
UCS-A /chassis/cartridge/server/cimc/ext-static-ip* # set addr 2001:888::10
UCS-A /chassis/cartridge/server/cimc/ext-static-ip* # set default-gw 2001:888::100
UCS-A /chassis/cartridge/server/cimc/ext-static-ip* # set prefix 64
UCS-A /chassis/cartridge/server/cimc/ext-static-ip* # commit-buffer
UCS-A /chassis/cartridge/server/cimc/ext-static-ip #
```

サーバで管理 IP プールを使用するための設定

スタティック管理 IP アドレスを削除すると、指定サーバを管理 IP プールに戻します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id* / *cartridge-id* / *server-id*	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /chassis/cartridge/server # **scope cimc**	サーバ CIMC モードに入ります。
ステップ 3	UCS-A /chassis/cartridge/server/cimc # **delete** {*ext-static-ip* | *ext-static-ip6*}	外部スタティック IPv4 または IPv6 アドレスを削除し、管理 IP プールにサーバを戻します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /chassis/cartridge/server/cimc/ # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、シャーシ 1 カートリッジ 1 のサーバ 1 のスタティック管理 IP アドレスを削除して、トランザクションをコミットします。

```
UCS-A# scope server 1/1/1
UCS-A /chassis/cartridge/server # scope cimc
UCS-A /chassis/cartridge/server/cimc # delete ext-static-ip
UCS-A /chassis/cartridge/server/cimc* # commit-buffer
UCS-A /chassis/cartridge/server/cimc/ #
```

次の例では、シャーシ 1 カートリッジ 1 のサーバ 1 のスタティック管理 IPv6 アドレスを削除して、トランザクションをコミットします。

```
UCS-A# scope server 1/1/1
UCS-A /chassis/cartridge/server # scope cimc
UCS-A /chassis/cartridge/server/cimc # delete ext-static-ip6
UCS-A /chassis/cartridge/server/cimc* # commit-buffer
UCS-A /chassis/cartridge/server/cimc/ #
```

サービス プロファイルまたはサービス プロファイル テンプレートでの管理 IP アドレスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。 ルート組織モードを開始するには、org-name に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **set ext-mgmt-ip-state** {*none* | *ext-pooled-ip* | *ext-pooled-ip6* | *ext-static-ip* | *ext-static-ip6*}	管理 IPv4 または IPv6 アドレスをサービス プロファイルに割り当てる方法を指定します。 次のオプションを使用して管理 IP アドレス ポリシーを設定できます。

	コマンドまたはアクション	目的
		• none：サービス プロファイルに IP アドレスは割り当てられません。 • pooled：サービスプロファイルに管理 IPv4 または IPv6 プールから IP アドレスが割り当てられます。 • static：サービス プロファイルに設定済みのスタティック IPv4 または IPv6アドレスが割り当てられます。 （注） サービスプロファイルテンプレートでは ext-management-ip-state を static に設定することはサポートされておらず、設定するとエラーが発生します。
ステップ 4	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、accounting というサービスプロファイルの管理 IP アドレス ポリシーを static IPv4 に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # set ext-mgmt-ip-state ext-static-ip
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

次のタスク

管理 IP アドレスを static に設定する場合、スタティック IP アドレスを使用するようにサーバを設定します。

管理 IP プールの設定

管理 IP プール

デフォルトの管理 IP プールである IP Pool ext-mgmt は、外部 IPv4 および IPv6 アドレスの集まりです。Cisco UCS Manager は、サーバの CIMC で終端する外部アクセスのために、管理 IP プールに IP アドレスの各ブロックを予約しています。

デフォルトでは、IP Pool ext-mgmt を使用して CIMC アウトバウンド管理 IP アドレスを設定します。スタティック IP アドレスがこのプールからサーバに割り当てられてしまうと、この IP プールを変更できません。スタティック IP アドレスから CIMC のアウトバウンド管理 IP アドレスを設定する場合は、デフォルトの管理 IP プールから IP アドレスを削除できます。

アウトオブバンド IPv4 アドレス プール、およびインバンド IPv4 または IPv6 アドレス プールは個別に設定できます。IPv4 と IPv6 アドレス ブロックの両方を含むインバンド プールも設定できます。

ヒント サーバ CIMC に IPv4 アドレスのみを含む IP プールがインバンド IPv6 ポリシーとして割り当てられたり、IPv6 アドレスのみを含む IP プールがインバンド IPv4 ポリシーとして割り当てられたりされないように、それぞれが IPv4 または IPv6 アドレスのみを持つ個別のインバンド アドレス プールを設定することを推奨します。

管理 IP プールの IP アドレスを使用するようにサービス プロファイルとサービス プロファイル テンプレートを設定できます。管理 IP プールを使用するようサーバを設定することはできません。

管理 IP プール内のすべての IP アドレスは、同じ IPv4 サブネットに含まれるか、ファブリック インターコネクトの IP アドレスと同じ IPv6 ネットワーク プレフィックスが付けられている必要があります。

（注） サーバまたはサービス プロファイルのスタティック IP アドレスとして割り当てられている IP アドレスは、管理 IP プールに含まれていてはなりません。

管理 IP プールの IP アドレス ブロックの設定

サーバまたはサービス プロファイルのスタティック IP アドレスとして割り当てられている IP アドレスは、管理 IP プールに含まれていてはなりません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope ip-pool ext-mgmt**	組織 IP プール モードを開始します。 （注） 管理 IP プールの作成（または削除）はできません。既存のデフォルト プールに入る（スコープを設定する）ことだけが可能です。
ステップ 3	（任意） UCS-A /org/ip-pool # **set descr** *description*	管理IPプールに説明を記入します。この説明は管理IPプールのすべてのアドレス ブロックに適用されます。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明の前後に引用符を付ける必要があります。引用符は、 **show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/ip-pool # **set assignmentorder** {**default** | **sequential**}	次のいずれかになります。 • **default**：Cisco UCS Manager はプールからランダム ID を選択します。 • **sequential**：Cisco UCS Manager はプールから最も小さい使用可能な ID を選択します。
ステップ 5	UCS-A /org/ip-pool # **create block** *first-ip-addr last-ip-addr gateway-ip-addr subnet-mask*	IP アドレス ブロック（範囲）を作成し、組織 IP プール ブロック モードを開始します。アドレス範囲の最初と最後の IP アドレス、ゲートウェイ IP アドレス、およびサブネットマスクを指定します。 （注） IP プールには、複数の IP ブロックを含めることができます。複数のブロックを作成するには、組織 IP プール モードから複数の **create block** コマンドを入力します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /org/ip-pool/block # **set primary-dns** *ip-addrress* |**secondary-dns** *ip-address*	プライマリ DNS とセカンダリ DNS の IP アドレスを指定します。
ステップ 7	UCS-A /org/ip-pool/ ipv6-block # **commit-buffer**	トランザクションをシステムの設定にコミットします。
ステップ 8	UCS-A /org/ip-pool/block # **exit**	IPv4 ブロック コンフィギュレーション モードを終了します。
ステップ 9	UCS-A /org/ip-pool # **create ipv6-block** *first-ip6-addr last-ip6-addr gateway-ip6-addr prefix*	IPv6 アドレスのブロック（範囲）を作成し、組織 IP プール IPv6 ブロック モードを開始します。アドレス範囲の最初と最後の IPv6 アドレス、ゲートウェイ IPv6 アドレス、およびネットワーク プレフィックスを指定する必要があります。 （注） IPv6 プールには、複数の IP ブロックを含めることができます。複数の IPv6 ブロックを作成するには、組織IPプール モードから複数の **create ipv6-block** コマンドを入力します。
ステップ 10	UCS-A /org/ip-pool/ipv6-block # **set primary-dns** *ip6-address* **secondary-dns** *ip6-address*	プライマリ DNS とセカンダリ DNS の IPv6 アドレスを指定します。
ステップ 11	UCS-A /org/ip-pool/ipv6-block # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、管理 IP プールの IPv4 アドレス ブロックを設定し、プライマリおよびセカンダリ IPv4 アドレスを指定し、IPv6 ブロックを作成し、プライマリおよびセカンダリ IPv6 アドレスを指定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope ip-pool ext-mgmt-ip
UCS-A /org/ip-pool* # set descr "This is a management ip pool example."
UCS-A /org/ip-pool* # create block 192.168.100.1 192.168.100.200 192.168.100.10
255.255.255.0
UCS-A /org/ip-pool/block* # set primary-dns 192.168.100.1 secondary-dns 192.168.100.20
UCS-A /org/ip-pool/block* commit-buffer
UCS-A /org/ip-pool/block exit
UCS-A /org/ip-pool* # create ipv6-block 2001:888::10 2001:888::100 2001:888::1 64
UCS-A /org/ip-pool/ipv6- block* set primary-dns 2001:888::11 secondary-dns 2001:888::12
```

```
UCS-A /org/ip-pool/ipv6- block* commit-buffer
UCS-A /org/ip-pool/ipv6- block #UCS-A /org/ip-pool/block* # commit-buffer
UCS-A /org/ip-pool/block #
```

次の例では、管理 IP プールの IPv6 アドレス ブロックを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org #scope ip-pool ext-mgmt-ip
UCS-A /org/ip-pool* # set descr "This is a management IPv6 pool example."
UCS-A /org/ip-pool* # create ipv6-block 2001:888::10 2001:888::100 2001:888::1 64
UCS-A /org/ip-pool/ipv6-block* # commit-buffer
UCS-A /org/ip-pool/ipv6-block* #
```

次のタスク

1 つ以上のサービス プロファイルまたはサービス プロファイル テンプレートを設定し、管理 IP プールから CIMC IP アドレスを取得します。

管理 IP プールからの IP アドレス ブロックの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope ip-pool ext-mgmt**	管理 IP プールを入力します。
ステップ 3	UCS-A /org/ip-pool # **delete** {*ip-block*|*ipv6-block*} {*first-ip-addr*|*first-ip6-addr*} {*last-ip-addr* | *last-ip6-addr*}	IPv4 または IPv6 アドレスの指定されたブロック（範囲）を削除します。
ステップ 4	UCS-A /org/ip-pool # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、管理 IP プールから IP アドレス ブロックを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope ip-pool ext-mgmt
UCS-A /org/ip-pool # delete block 192.168.100.1 192.168.100.200
UCS-A /org/ip-pool* # commit-buffer
UCS-A /org/ip-pool #
```

次に、管理 IP プールから IPv6 アドレス ブロックを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope ip-pool pool4
UCS-A /org/ip-pool # delete ipv6-block 2001::1 2001::10
UCS-A /org/ip-pool* # commit-buffer
UCS-A /org/ip-pool #
```

システム名の変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **set name** *name*	システム名を設定します。
ステップ 3	UCS-A /system # **commit-buffer**	トランザクションをシステムの設定にコミットします。

名前は、トランザクションがコミットされた後、30秒ほどの間に両方のファブリック インターコネクトで更新されます。

例

次の例は、システム名を変更し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system* # set name SanJose5
UCS-A /system* # commit-buffer
UCS-A /system #
```

クラスタの管理サブネットの変更

クラスタ設定の IPv4 管理サブネットを変更する場合は、次の 3 つの IPv4 アドレスを同時に変更する必要があり、3 つのアドレスは同じサブネットに設定する必要があります。

- ファブリック インターコネクト A の管理ポートの IP アドレス
- ファブリック インターコネクト B の管理ポートの IP アドレス
- クラスタ IP（仮想 IP）アドレス

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect a**	ファブリック A のファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **set out-of-band ip** *ip-address* **netmask** *netmask* **gw** *gateway-ip-address*	ファブリック インターコネクトの IP アドレス、ネットワーク マスク、およびゲートウェイ IPアドレスを設定します。
ステップ 3	UCS-A /fabric-interconnect # **scope fabric-interconnect b**	ファブリック B のファブリック インターコネクト モードを開始します。
ステップ 4	UCS-A /fabric-interconnect # **set out-of-band ip** *ip-address* **netmask** *netmask* **gw** *gateway-ip-address*	ファブリック インターコネクトの IP アドレス、ネット マスク、およびゲートウェイ IP アドレスを設定します。
ステップ 5	UCS-A /fabric-interconnect # **scope system**	システム モードを開始します。
ステップ 6	UCS-A /system # **set virtual-ip** *vip-address*	クラスタの仮想 IP アドレスを設定します。
ステップ 7	UCS-A /system # **commit-buffer**	トランザクションをシステムの設定にコミットします。

トランザクションをコミットすると、管理セッションから切断されます。新しい管理 IP アドレスに再接続します。

例

この例は、両方のファブリック インターコネクトの IP アドレスを変更し、仮想 IP アドレスを変更し、トランザクションをコミットして、セッションを切断します。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0 gw
192.0.2.1
UCS-A /fabric-interconnect* # scope fabric-interconnect b
UCS-A /fabric-interconnect* # set out-of-band ip 192.0.2.112 netmask 255.255.255.0 gw
192.0.2.1
UCS-A /fabric-interconnect* # scope system
UCS-A /system* # set virtual-ip 192.0.2.113
UCS-A /system* # commit-buffer
```

クラスタの管理プレフィックスの変更

クラスタ設定の IPv6 管理プレフィックスを変更する場合は、次の 3 つの IPv6 アドレスを同時に変更する必要があります。3 つのアドレスは同一ネットワーク プレフィックス内に設定する必要があります。

- ファブリック インターコネクト A の管理ポートの IPv6 アドレス
- ファブリック インターコネクト B の管理ポートの IPv6 アドレス
- クラスタ IPv6（仮想 IPv6）アドレス

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect a**	ファブリック A のファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A fabric-interconnect # **scope ipv6-config**	ファブリック A の IPv6 コンフィギュレーション モードを開始します。
ステップ 3	UCS-A fabric-interconnect/ ipv6-config # **set out-of-band ipv6** *ipv6 addr* **ipv6-gw** *ipv6-gw-addr* **ipv6-prefix** *prefix*	ファブリック A の管理 IPv6 アドレス、ゲートウェイ IPv6 アドレスおよびネットワークプレフィックスを設定します。
ステップ 4	UCS-A fabric-interconnect/ipv6-config # **scope fabric-interconnect b**	ファブリック B のファブリック インターコネクト モードを開始します。
ステップ 5	UCS-A fabric-interconnect/ # **scope ipv6-config**	ファブリック B の IPv6 コンフィギュレーション モードを開始します。
ステップ 6	UCS-A/fabric-interconnect/ipv6-config # **set out-of-band ipv6** *ipv6 addr* **ipv6-gw** *ipv6-gw-addr* **ipv6-prefix** *prefix*	ファブリック B の管理 IPv6 アドレス、ゲートウェイ IPv6 アドレスおよびネットワークプレフィックスを設定します。
ステップ 7	UCS-A/fabric-interconnect/ipv6-config # **scope system**	システム モードを開始します。
ステップ 8	UCS-A/system # **set virtual-ip ipv6** *virtual-ip6-addr*	クラスタの仮想 IPv6 アドレスを設定します。
ステップ 9	UCS-A/system # **commit-buffer**	トランザクションをシステムの設定にコミットします。

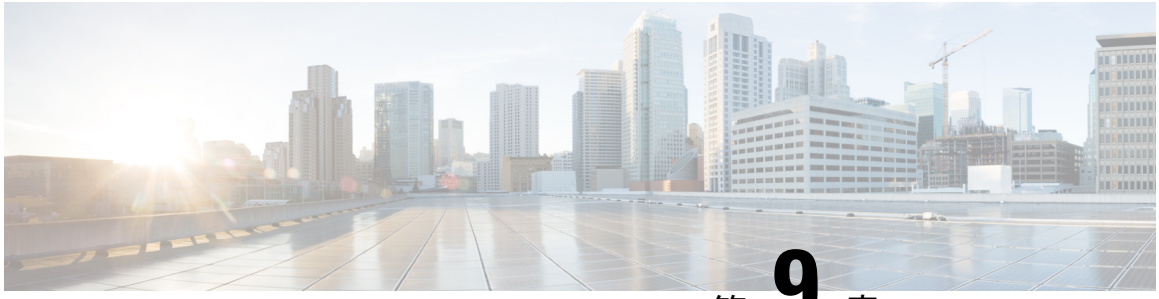
トランザクションをコミットすると、管理セッションから切断されます。新しい管理 IPv6 アドレスに再接続します。

例

次の例では、両方の管理 IPv6 アドレスを変更し、仮想 IPv6 アドレスを変更し、トランザクションをコミットします。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # scope ipv6-config
UCS-A /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001:10::157
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-gw 2001:10::1
```

```
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-prefix 64
UCS-A /fabric-interconnect/ipv6-config* # scope fabric-interconnect b
UCS-A /fabric-interconnect* # scope ipv6-config
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6 2001:10::158
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-gw 2001:10::1
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-prefix 64
UCS-A /fabric-interconnect/ipv6-config* # scope system
UCS-A /system* # set virtual-ip ipv6 2001:10::156
UCS-A /system* # commit-buffer
UCS-A /system #
```



第 9 章

UCS Manager の組織

マルチテナント環境の組織

マルチテナント機能を使用すると、Cisco UCS ドメイン の大きな物理的インフラストラクチャを組織と呼ばれる論理的なエンティティに分割できます。その結果、各組織に専用の物理インフラストラクチャを設けなくても各組織を論理的に分離できます。

マルチテナント環境では、関連する組織を通じて、各テナントに一意のリソースを割り当てられます。これらのリソースには、各種のポリシー、プール、および Quality of Service 定義などがあります。また、すべてのユーザがすべての組織にアクセスできるようにする必要がない場合は、ロケールを実装して、組織ごとにユーザ権限やロールを割り当てたり、制限したりすることもできます。

マルチテナント環境をセットアップする場合、すべての組織は階層的になります。最上位の組織は常にルートです。ルートに作成したポリシーおよびプールはシステム全体にわたるもので、このシステムに含まれるすべての組織で使用できます。しかし、他の組織で作成されたポリシーやプールを使用できるのは、同じ階層でそれより上にある組織だけです。たとえば、あるシステムに Finance と HR という組織があり、これらは同じ階層に存在しないとします。この場合、Finance は HR 組織にあるポリシーは一切使用できず、また、HR は Finance 組織にあるポリシーには一切アクセスできません。しかし、Finance と HR は両方とも、ルート組織にあるポリシーやプールを使用できます。

マルチテナント環境に組織を作成する場合、各組織、または同じ階層のサブ組織に次のうち 1 つ以上をセットアップすることもできます。

- リソース プール
- ポリシー

- サービス プロファイル
- サービス プロファイル テンプレート

ルート組織は、常にトップ レベルの組織です。

マルチテナント環境における階層的な名前解決

マルチテナント環境では、Cisco UCS は組織の階層を使用して、ポリシーおよびリソース プールの名前を解決します。Cisco UCS Manager は、プールに割り当てられているポリシーまたはリソースの詳細を検索する際に、以下の操作を実行します。

1. Cisco UCS Manager は、サービス プロファイルまたはポリシーに割り当てられている組織内で、指定された名前のポリシーとプールの有無を調べます。
2. ポリシーが検出されるか、使用可能なリソースがプール内に存在する場合、Cisco UCS Manager はこのポリシーまたはリソースを使用します。ローカル レベルで使用可能なリソースがプール内に存在しない場合、Cisco UCS Manager は上位階層の親組織に移動し、同じ名前のプールを検索します。Cisco UCS Manager では検索がルート組織に到達するまでこの手順を繰り返します。
3. 検索がルート組織まで到達し、使用可能なリソースまたはポリシーが検出されない場合、Cisco UCS Manager はローカル組織に戻り、デフォルト ポリシーまたはデフォルト プール内で使用可能なリソースの検出を開始します。
4. 適用可能なデフォルト ポリシーまたは使用可能なリソースがデフォルト プール内で検出されると、Cisco UCS Manager はこのポリシーまたはリソースを使用します。使用可能なリソースがプール内に存在しない場合、Cisco UCS Manager は上位階層の親組織に移動し、デフォルトのプールを検索します。Cisco UCS Manager は検索がルート組織に到達するまでこの手順を繰り返します。
5. Cisco UCS Manager は、適用可能なポリシーまたは使用可能なリソースを階層内で検出できない場合、割り当てエラーを返します。

例：単一階層でのサーバ プール名の解決

この例では、すべての組織がルート組織下の同一レベルにあります。たとえば、サービス プロバイダは、各顧客に対して個別の組織を作成します。この構成では、組織は、自身の組織およびルート組織に割り当てられたポリシーおよびリソースにのみアクセスできます。

この例では、XYZcustomer 組織のサービス プロファイルは、XYZcustomer サーバ プールのサーバを使用するように設定されています。リソース プールとポリシーがサービス プロファイルに割り当てられると、以下の動作が発生します。

1. Cisco UCS Manager は、XYZcustomer サーバ プール内で使用可能なサーバを調べます。

2. 使用可能なサーバが XYZcustomer サーバ プールに存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。プール内に使用可能なサーバが存在しない場合、Cisco UCS Manager はルート組織で同じ名前のサーバの有無を調べます。

3. ルート組織に XYZcustomer サーバ プールが含まれており、そのプールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。プール内に使用可能なサーバが存在しない場合、Cisco UCS Manager は XYZcustomer 組織に戻り、デフォルトのサーバ プールを調べます。

4. XYZcustomer 組織内のデフォルト プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager はルート組織内でデフォルトのサーバ プールを調べます。

5. ルート組織内のデフォルト サーバ プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は割り当てエラーを返します。

例：多階層でのサーバ プール名の解決

この例では、各組織に少なくとも 1 つのサブ組織が含まれています。たとえば、企業は、企業内の各主要部門に対しておよびこれらの部門のサブ部門に対して組織を作成できます。この構成では、各組織が、自身のローカル ポリシーとリソース プール、および親階層内のリソース プールにアクセスできます。

この例では、Finance 組織に 2 つのサブ組織（AccountsPayable および AccountsReceivable）が含まれています。AccountsPayable（AP）組織のサービス プロファイルは、AP サーバ プールのサーバを使用するように設定されています。リソース プールとポリシーがサービス プロファイルに割り当てられると、以下の動作が発生します。

1. Cisco UCS Manager は、サービス プロファイルに定義されている AP サーバ プールで使用可能なサーバを調べます。

2. 使用可能なサーバが AP サーバ プールに存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は 1 階層上位に移動し、Finance 組織で同じ名前のプールの有無を調べます。

3. Finance 組織に同じ名前のプールが含まれており、このプールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は 1 階層上位に移動し、ルート組織で同じ名前のプールの有無を調べます。

4. ルート組織に同じ名前のプールが含まれており、このプールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は AccountsPayable 組織に戻り、デフォルトのサーバ プールを調べます。
5. AccountsPayable 組織内のデフォルト プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は 1 階層上位に移動し、Finance 組織のデフォルトのサーバ プールを調べます。
6. Finance 組織内のデフォルト プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は 1 階層上位に移動し、ルート組織のデフォルトのサーバ プールを調べます。
7. ルート組織内のデフォルト サーバ プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は割り当てエラーを返します。

ルート組織下の組織の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **create org** *org-name*	ルート組織下に選択された組織を作成し、指定した組織で組織モードを開始します。 （注） ある組織モードから別の組織モードに移るとき、コマンド プロンプトは変更されません。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、root組織の下にFinanceという名前の組織を作成し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # create org Finance
UCS-A /org* # commit-buffer
UCS-A /org #
```

非ルートの組織下の組織の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope org** *org-name*	指定した組織の組織モードを開始します。 （注） ある組織モードから別の組織モードに移るとき、コマンドプロンプトは変更されません。
ステップ 3	UCS-A /org # **create org** *org-name*	事前設定された非ルート組織下に選択された組織を作成し、指定した組織で組織モードを開始します。
ステップ 4	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、NorthAmerica組織の下にFinanceという名前の組織を作成し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope org NorthAmerica
UCS-A /org # create org Finance
UCS-A /org* # commit-buffer
UCS-A /org #
```

組織の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **delete org** *org-name*	指定した組織を削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、Finance という名前のルート組織下の組織を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete org Finance
UCS-A /org* # commit-buffer
UCS-A /org #
```

第 10 章

バックアップと復元

バックアップと復元の操作

UCS でのバックアップの操作

Cisco UCS Manager からバックアップを実行する場合は、システム設定全体またはその一部のスナップショットを作成し、そのファイルをネットワーク上の場所にエクスポートします。Cisco UCS Manager を使用してサーバにデータをバックアップすることはできません。

バックアップは、システムが起動されて動作している間に実行できます。バックアップ操作では、管理プレーンからの情報だけが保存されます。バックアップは、サーバまたはネットワーク トラフィックには影響しません。

バックアップ操作の考慮事項と推奨事項

バックアップ操作を作成する前に、次のことを考慮してください。

バックアップの場所

バックアップ場所とは、Cisco UCS Manager でバックアップ ファイルをエクスポートするネットワーク上の宛先またはフォルダのことです。バックアップ操作は、バックアップ ファイルを保存する場所ごとに 1 つしか維持できません。

バックアップ ファイル上書きの可能性

ファイル名を変更しないでバックアップ操作を再実行すると、サーバ上にすでに存在するファイルが Cisco UCS Manager によって上書きされます。既存のバックアップ ファイルが上書きされるのを回避するには、バックアップ操作内のファイル名を変更するか、既存のファイルを別の場所にコピーします。

バックアップの複数のタイプ

同じ場所に対して複数種類のバックアップを実行し、エクスポートできます。バックアップ操作を再実行する前に、バックアップ タイプを変更します。識別が容易になるように、あるいは既存のバックアップ ファイルが上書きされないように、ファイル名の変更を推奨します。

スケジュール バックアップ

事前にバックアップ操作を作成し、バックアップを実行する準備が整うまで管理状態を無効のままにしておくことができます。Cisco UCS Manager は、バックアップ操作の管理状態が有効化されるまで、バックアップ操作、保存、設定ファイルのエクスポートを実行しません。

増分バックアップ

差分バックアップは実行できません。

Full State バックアップの暗号化

パスワードなどの機密情報がクリア テキストでエクスポートされることがないように、Full State バックアップは暗号化されます。

バックアップ ポリシーと設定エクスポート ポリシーの FSM タスク

[Policy Backup & Export] タブで [Backup Policy] と [Config Export Policy] の両方を設定し、両方のポリシーに同じホスト名を使用すると、Cisco UCS Managerは [Backup Configuration] ページで1つの**バックアップ操作**のみを作成して両方のタスクを実行します。それぞれのポリシー実行で、個別の FSM タスクは発生しません。

各ポリシーが個別の FSM タスクとなるようにするには、使用する DNS サーバに同じ FTP/TFTP/SCP/SFTP サーバを指すようにホスト名エイリアスを作成し、次に、**バックアップ ポリシー**に 1 つのホスト名を使用し、**設定エクスポート ポリシー**に別のホスト名を使用します。

バックアップ操作とインポート操作に必要なユーザロール

バックアップ操作とインポート操作を作成し、実行するには、管理ロールを持つユーザアカウントが必要です。

バックアップ操作の作成

始める前に

バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスおよび認証クレデンシャルを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **create backup** *URL backup-type*{**disabled** | **enabled**}	バックアップ操作を作成します。次のいずれかの構文を使用してバックアップするファイルの *URL* を指定します。 • **ftp:**// *username@hostname* / *path* • **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path* *backup-type* 引数には、次のいずれかの値を指定できます。 • **all-configuration** ：サーバ関連、ファブリック関連、システム関連の設定をバックアップします。 • **logical-configuration** ：ファブリックおよびサービス プロファイルの関連の設定をバックアップします。 • **system-configuration** ：システム関連の設定をバックアップします。 • **full-state** ：ディザスタ リカバリのために Full State バックアップをします。

	コマンドまたはアクション	目的
		（注） • Full State バックアップ ファイルはインポート操作を使用してインポートできません。これらは、ファブリック インターコネクトの設定を復元するためにのみ使用されます。 • Full State バックアップ ファイルを使用した場合にのみ、バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元できます。 複数のバックアップ操作を保存できますが、各ホスト名につき 1 種類の操作だけが保存されます。 **enable** キーワードを使用した場合、バックアップ操作は **commit-buffer** コマンドを入力するとすぐに自動実行されます。 **disable** キーワードを使用すると、バックアップ操作は有効にされるまで実行されません。バックアップ操作を有効にする場合、バックアップ操作を作成するときに使用したホスト名を指定する必要があります。
ステップ 3	UCS-A /system # **commit-buffer**	トランザクションをコミットします。

例

次の例では、ホスト名 host35 に対する disabled all-configuration バックアップ操作を作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope system
UCS-A /system* # create backup scp://user@host35/backups/all-config9.bak all-configuration
 disabled
Password:
```

```
UCS-A /system* # commit-buffer
UCS-A /system #
```

バックアップ操作の実行

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope backup** *hostname*	指定したホスト名でシステムバックアップ モードを開始します。
ステップ 3	UCS-A /system/backup # **enable**	バックアップ操作を有効にします。 （注） FTP、SCP、SFTP を使用するバックアップ操作では、パスワードの入力を求められます。トランザクションをコミットする前にパスワードを入力します。
ステップ 4	UCS-A /system/backup # **commit-buffer**	トランザクションをコミットします。

例

次に、host35 というバックアップ操作を有効にし、SCP プロトコルのパスワードを入力し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope backup host35
UCS-A /system/backup # enable
Password:
UCS-A /system/backup* # commit-buffer
UCS-A /system/backup #
```

バックアップ操作の変更

バックアップ操作を修正して、別のバックアップタイプのファイルをその場所に保存したり、前のバックアップ ファイルが上書きされないようファイル名を変更したりすることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope backup** *hostname*	指定したホスト名でシステム バックアップ モードを開始します。
ステップ 3	（任意） UCS-A /system/backup # **disable**	トランザクションのコミット時にバックアップ操作が自動的に実行されないようにするために、有効になっているバックアップ操作を無効にします。
ステップ 4	（任意） UCS-A /system/backup # **enable**	トランザクションをコミットすると、ただちにバックアップ操作が実行されるようにします。
ステップ 5	（任意） UCS-A /system/backup # **set descr** *description*	バックアップ操作の説明を指定します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明の前後に引用符を付ける必要があります。引用符は、show コマンド出力の説明フィールドには表示されません。
ステップ 6	（任意） UCS-A /system/backup # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	リモートサーバとの通信時に使用するプロトコルを指定します。
ステップ 7	（任意） UCS-A /system/backup # **set remote-file** *filename*	バックアップする設定ファイルの名前を指定します。
ステップ 8	（任意） UCS-A /system/backup # **set type** *backup-type*	作成するバックアップファイルのタイプを指定します。*backup-type* 引数には、次のいずれかの値を指定できます。 • **all-configuration** ：サーバ関連、ファブリック関連、システム関連の設定をバックアップします。 • **logical-configuration** ：ファブリックおよびサービスプロファイルの関連の設定をバックアップします。

	コマンドまたはアクション	目的
		• **system-configuration** ：システム関連の設定をバックアップします。 • **full-state** ：ディザスタ リカバリのために Full State バックアップをします。 （注） • Full State バックアップ ファイルはインポート操作を使用してインポートできません。これらは、ファブリック インターコネクトの設定を復元するためにのみ使用されます。 • Full State バックアップファイルを使用した場合にのみ、バックアップファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元できます。
ステップ 9	（任意） UCS-A /system/backup # **set preserve-pooled-values** {**no** | **yes**}	vHBA WWPN、vNIC MAC、WWNN、UUID など、プールから抽出された ID 値をバックアップで保存するかどうかを指定します。
ステップ 10	（任意） UCS-A /system/backup # **set user** *username*	システムがリモートサーバへのログインに使用する必要のあるユーザ名を指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 11	（任意） UCS-A /system/backup # **set password**	**Enter** キーを押すと、パスワードを入力するように促されます。 リモートサーバのユーザ名のパスワードを指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。

	コマンドまたはアクション	目的
ステップ 12	UCS-A /system/backup # **commit-buffer**	トランザクションをコミットします。

例

次に、説明を追加し、host35 バックアップ操作のプロトコル、ユーザ名、およびパスワードを変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope backup host35
UCS-A /system/backup # set descr "This is a backup operation for host35."
UCS-A /system/backup* # set protocol sftp
UCS-A /system/backup* # set user UserName32
UCS-A /system/backup* # set password
Password:
UCS-A /system/backup* # set preserve-pooled-values no
UCS-A /system/backup* # commit-buffer
UCS-A /system #
```

バックアップ操作の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **delete backup** *hostname*	指定したホスト名のバックアップ操作を削除します。
ステップ 3	UCS-A /system # **commit-buffer**	トランザクションをコミットします。

例

次に、host35 というホスト名のバックアップ操作を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # delete backup host35
UCS-A /system* # commit-buffer
UCS-A /system #
```

スケジュール バックアップ

次のタイプのバックアップをスケジュールするように Cisco UCS にポリシーを設定できます。

- Full State
- All Configuration

他のタイプのバックアップはスケジュールできません。

バックアップ タイプ

Cisco UCS Manager および Cisco UCS Central では、次のタイプのバックアップを 1 つ以上実行できます。

- [Full state]：システム全体のスナップショットが含まれるバイナリ ファイル。このバックアップにより生成されたファイルを使用して、ディザスタ リカバリ時にシステムを復元できます。このファイルにより、元のファブリック インターコネクト上で設定を復元または再構築できます。また、別のファブリック インターコネクト上で設定を再現することもできます。このファイルは、インポートには使用できません。

（注） Full State バックアップ ファイルを使用した場合にのみ、バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元できます。

- [All configuration]：すべてのシステム設定と論理設定が含まれる XML ファイル。このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。このファイルは、システムの復元には使用できません。このファイルには、ローカル認証されたユーザのパスワードは含まれません。
- [System configuration]：ユーザ名、ロール、ロケールなどのすべてのシステム設定が含まれる XML ファイル。このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。このファイルは、システムの復元には使用できません。
- [Logical configuration]：サービス プロファイル、VLAN、VSAN、プール、ポリシーなどのすべての論理設定が含まれる XML ファイル。このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。このファイルは、システムの復元には使用できません。

Full State バックアップ ポリシー

Full State バックアップ ポリシーを使用すると、システム全体のスナップショットの定期的な Full State バックアップをスケジュールすることができます。Full State バックアップを行う間隔は、日単位、週単位、または隔週単位で設定できます。

Cisco UCS Manager は、リモート サーバ上のバックアップ ファイルの最大数を維持します。maxfiles パラメータは、Cisco UCS Manager を Cisco UCS Central に登録するときに使用されます。maxfiles パラメータは Cisco UCS Central でユーザが設定できるパラメータで、Cisco UCS Central に保存するバックアップ ファイルの数を制御します。

Cisco UCS Manager が Cisco UCS Central に登録されておらず、ユーザがリモート バックアップ サーバにバックアップ ファイルを保存している場合、バックアップ ファイルは Cisco UCS Managerによって管理されません。リモートマシンのサーバ管理者は、ディスク使用率を監視してバックアップ ファイルのローテンションを行い、新しいバックアップ ファイル用の領域を確保する必要があります。

Full State バックアップ ポリシーの設定

始める前に

バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスおよび認証クレデンシャルを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードに入ります。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope backup-policy default**	All Configuration エクスポート ポリシーモードを開始します。
ステップ 3	UCS-A /org/backup-policy # **set hostname** {*hostname* | *ip-addr* | *ip6-addr*}	バックアップポリシーが格納されている場所のホスト名、IPv4 または IPv6 アドレスを指定します。これには、サーバ、ストレージアレイ、ローカル ドライブ、またはファブリック インターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。

	コマンドまたはアクション	目的
		（注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメイン が Cisco UCS Central に登録されていないか、または DNS 管理が [local] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメインが Cisco UCS Central に登録されていて、DNS 管理が [global] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
ステップ 4	UCS-A /org/backup-policy # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	リモートサーバとの通信時に使用するプロトコルを指定します。
ステップ 5	UCS-A /org/backup-policy # **set user** *username*	システムがリモートサーバへのログインに使用する必要のあるユーザ名を指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 6	UCS-A /system/backup-policy # **set password**	**Enter** キーを押すと、パスワードを入力するように促されます。 リモートサーバのユーザ名のパスワードを指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 7	UCS-A /system/backup-policy # **set remote-file** *filename*	バックアップファイルのフルパスを指定します。このフィールドには、ファイル名とパスを含めることができます。ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。
ステップ 8	UCS-A /system/backup-policy # **set adminstate** {**disabled** | **enabled**}	ポリシーの管理状態を指定します。次のいずれかになります。 • **enabled**：Cisco UCS Manager は、[Schedule] フィールドで指定されたスケジュールを使用してバック

	コマンドまたはアクション	目的
		アップ ファイルをエクスポートします。 • **disabled**：Cisco UCS Manager はファイルをエクスポートしません。
ステップ 9	UCS-A /system/backup-policy # **set schedule** {**daily** | **weekly** | **bi-weekly**}	Cisco UCS Manager がバックアップ ファイルをエクスポートする頻度を指定します。
ステップ 10	UCS-A /system/backup-policy # **set descr** *description*	バックアップ ポリシーの説明を指定します。 256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または '（一重引用符）は使用できません。
ステップ 11	UCS-A /backup-policy # **commit-buffer**	トランザクションをコミットします。

例

次の例では、週単位のバックアップのための Full State バックアップ ポリシーを設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope backup-policy default
UCS-A /org/backup-policy # set hostname host35
UCS-A /org/backup-policy* # set protocol scp
UCS-A /org/backup-policy* # set user UserName32
UCS-A /backup-policy* # set password
Password:
UCS-A /backup-policy* # set remote-file /backups/full-state1.bak
UCS-A /backup-policy* # set adminstate enabled
UCS-A /backup-policy* # set schedule weekly
UCS-A /backup-policy* # set descr "This is a full state weekly backup."
UCS-A /backup-policy* # commit-buffer
UCS-A /backup-policy #
```

All Configuration エクスポート ポリシーの設定

始める前に

バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスおよび認証クレデンシャルを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードに入ります。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope cfg-export-policy default**	All Configuration エクスポート ポリシーモードを開始します。
ステップ 3	UCS-A /org/cfg-export-policy # **set hostname** {*hostname* | *ip-addr* | *ip6-addr*}	コンフィギュレーションファイルが格納されている場所のホスト名、IPv4 または IPv6 アドレスを指定します。これには、サーバ、ストレージ アレイ、ローカル ドライブ、またはファブリック インターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。 （注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメイン が Cisco UCS Central に登録されていないか、または DNS 管理が [local] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメインが Cisco UCS Central に登録されていて、DNS 管理が [global] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
ステップ 4	UCS A/org/cfg-export-policy # **set protocol** {**ftp** |**scp** |**sftp** |**tftp**\\	リモート サーバとの通信時に使用するプロトコルを指定します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /org/cfg-export-policy # **set user** *username*	システムがリモートサーバへのログインに使用する必要のあるユーザ名を指定します。この手順は、TFTPプロトコルを使用する場合には適用されません。
ステップ 6	UCS-A /system/cfg-export-policy # **set password**	**Enter** キーを押すと、パスワードを入力するように促されます。 リモートサーバのユーザ名のパスワードを指定します。この手順は、TFTPプロトコルを使用する場合には適用されません。
ステップ 7	UCS-A /system/cfg-export-policy # **set remote-file** *filename*	エクスポートされたコンフィギュレーションファイルのフルパスを指定します。このフィールドには、ファイル名とパスを含めることができます。ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。
ステップ 8	UCS-A /system/cfg-export-policy # **set adminstate** {**disabled** | **enabled**}	ポリシーの管理状態を指定します。次のいずれかになります。 • **enabled**：Cisco UCS Manager は、[Schedule] フィールドで指定されたスケジュールを使用して設定情報をエクスポートします。 • **disabled**：Cisco UCS Manager は情報をエクスポートしません。
ステップ 9	UCS-A /system/cfg-export-policy # **set schedule** {**daily** | **weekly** | **bi-weekly**}	Cisco UCS Manager が設定情報をエクスポートする頻度を指定します。
ステップ 10	UCS-A /system/cfg-export-policy # **set descr** *description*	コンフィギュレーションエクスポートポリシーの説明を指定します。 256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または '（一重引用符）は使用できません。

	コマンドまたはアクション	目的
ステップ 11	UCS-A /cfg-export-policy # **commit-buffer**	トランザクションをコミットします。

例

次の例では、週単位のバックアップのための All Configuration エクスポート ポリシーを設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope cfg-export-policy default
UCS-A /org/cfg-export-policy # set hostname host35
UCS-A /org/cfg-export-policy* # set protocol scp
UCS-A /org/cfg-export-policy* # set user UserName32
UCS-A /cfg-export-policy* # set password
Password:
UCS-A /cfg-export-policy* # set remote-file /backups/all-config9.bak
UCS-A /cfg-export-policy* # set adminstate enabled
UCS-A /cfg-export-policy* # set schedule weekly
UCS-A /cfg-export-policy* # set descr "This is an all configuration backup."
UCS-A /cfg-export-policy* # commit-buffer
UCS-A /cfg-export-policy #
```

All Configuration エクスポート ポリシー

All Configuration バックアップ ポリシーでは、定期的なバックアップをスケジュールし、すべてのシステム設定と論理設定をエクスポートできます。このバックアップには、ローカル認証されたユーザのパスワードは含まれません。All Configuration バックアップを行う間隔は、日単位、週単位、または隔週単位で設定できます。

Cisco UCS は、リモート サーバ上のバックアップ ファイルの最大数を維持します。この数を超えると、Cisco UCS は最も古いバックアップ ファイルを上書きします。

バックアップ/エクスポートの設定リマインダの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードに入ります。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope backup-exp-policy**	バックアップ/エクスポート設定ポリシーモードを開始します。
ステップ 3	UCS-A /org/backup-exp-policy # **show**	既存のバックアップ/エクスポートの設定ポリシーを表示します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /org/backup-exp-policy # **set adminstate** {**disable** | **enable**}	ポリシーの管理状態を指定します。次のいずれかになります。 • **enable**：Cisco UCS Manager は、指定された期間内にバックアップが実行されない場合にエラーを起動します。 • **disable**：Cisco UCS Manager は、指定された期間内にバックアップが実行されなくてもエラーを起動しません。
ステップ 5	UCS-A /org/backup-exp-policy # **set frequency** *Number_of_Days*	バックアップを行うよう通知されるまでの日数を指定します。1 ～ 365 の整数を入力します。デフォルト値は 30 日間です。
ステップ 6	UCS-A /org/backup-exp-policy # **commit-buffer**	トランザクションをコミットします。

例

次に、現在のバックアップ/エクスポートの設定ポリシーを確認し、リマインダの頻度を変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope backup-exp-policy
UCS-A /org/backup-exp-policy # set frequency 5
UCS-A /org/backup-exp-policy* # commit-buffer
UCS-A /org/backup-exp-policy #
```

インポート操作

インポート方法

次のいずれかの方法により、Cisco UCS を介してシステム設定をインポートしてアップデートできます。

- **merge**：インポートされたコンフィギュレーションファイルの情報は、既存の設定情報と比較されます。情報が一致しない場合は、インポートされたコンフィギュレーションファイルの情報で Cisco UCS ドメインの情報が上書きされます。
- **replace**：現在の設定情報が、インポートされたコンフィギュレーション ファイルの情報で一度に 1 つのオブジェクトについて置き換えられます。

インポート設定

Cisco UCS からエクスポートされたコンフィギュレーション ファイルをインポートできます。ファイルは、同じ Cisco UCS からエクスポートされたものである必要はありません。

（注） 上位のリリースから下位のリリースに設定をインポートすることはできません。

インポート機能は、すべてのコンフィギュレーション ファイル、システム コンフィギュレーション ファイル、および論理コンフィギュレーション ファイルで使用できます。インポートは、システムがアップ状態で、稼働中の場合に実行できます。インポート操作によって情報が変更されるのは、管理プレーンだけです。インポート操作によって行われる一部の変更（サーバに割り当てられた vNIC に対する変更など）により、サーバのリブートまたはトラフィックを中断する他の動作が行われることがあります。

インポート操作はスケジュールできません。ただし、インポート操作を前もって作成し、そのインポートの実行準備が整うまで管理状態を無効のままにしておくことはできます。Cisco UCS は、管理状態が有効に設定されるまで、コンフィギュレーション ファイルに対してインポート操作を実行しません。

インポート操作は、コンフィギュレーション バックアップ ファイルを保存する場所ごとに 1 つしか維持できません。

インポート操作の作成

Full State バックアップ ファイルはインポートできません次のコンフィギュレーション ファイルのいずれもインポートできます。

- All Configuration
- System Configuration
- Logical Configuration

始める前に

コンフィギュレーション ファイルをインポートするには、次の情報を収集します。

- バックアップ サーバの IP アドレスおよび認証クレデンシャル
- バックアップ ファイルの完全修飾名

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム 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	UCS-A /system # **create import-config** *URL* {**disabled** | **enabled**} {**merge** | **replace**}	インポート操作を作成します。次のいずれかの構文を使用してインポートされるファイルの URL を指定します。 • **ftp:**// *username***@***hostname* / *path* • **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path* 複数のインポート操作を保存できますが、各ホスト名につき 1 種類の操作だけが保存されます。 **enable** キーワードを使用した場合、インポート操作は **commit-buffer** コマンドを入力するとすぐに自動実行されます。 **disable** キーワードを使用すると、インポート操作は有効にされるまで実行されません。インポート操作を有効にする場合、インポート操作を作成するときに使用したホスト名を指定する必要があります。 **merge** キーワードを使用すると、設定情報が既存の情報とマージされます。競合する場合、現在のシステム上の情報が、インポート設定ファイル内の情報に置き換えられます。 **replace** キーワードを使用すると、システムはインポート設定ファイル内の各オブジェクトを取得し、現在のコンフィギュレーション内の対応するオブジェクトを上書きします。
ステップ 3	（任意） UCS-A /system/import-config# **set descr** *description*	インポート操作の説明を記入します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明の前後に引用符を付ける必要があります。引用符は、show コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /system/import-config # **commit-buffer**	トランザクションをコミットします。

例

次の例は、現在のコンフィギュレーションを置き換える無効状態のホスト名 host35 のインポート操作を作成し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system* # create import-config scp://user@host35/backups/all-config9.bak disabled
 replace
Password:
UCS-A /system/import-config* # commit-buffer
UCS-A /system/import-config #
```

インポート操作の実行

Full State バックアップ ファイルはインポートできません次のコンフィギュレーション ファイルのいずれもインポートできます。

- All Configuration
- System Configuration
- Logical Configuration

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope import-config** *hostname*	指定したホスト名でシステムバックアップ モードを開始します。
ステップ 3	UCS-A /system/import-config # **enable**	インポート操作を有効にします。
ステップ 4	UCS-A /system/import-config # **commit-buffer**	トランザクションをコミットします。

例

次に、host35 というホスト名に対しインポート操作を有効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope import-config host35
UCS-A /system/import-config # enable
UCS-A /system/import-config* # commit-buffer
UCS-A /system/import-config #
```

インポート操作の変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope import-config** *hostname*	指定したホスト名でシステムインポートコンフィギュレーションモードを開始します。
ステップ 3	（任意） UCS-A /system/import-config # **disable**	トランザクションのコミット時にインポート操作が自動的に実行されないようにするために、有効になっているインポート操作を無効にします。
ステップ 4	（任意） UCS-A /system/import-config # **enable**	トランザクションをコミットすると、ただちにインポート操作が実行されるようにします。
ステップ 5	（任意） UCS-A /system/import-config # **set action** {**merge** | **replace**}	インポート操作に使用する次のいずれかのアクションタイプを指定します。 • **Merge** ：設定情報が既存の情報とマージされます。競合する場合、現在のシステム上の情報が、インポート設定ファイル内の情報に置き換えられます。 • **Replace** ：インポート設定ファイル内の各オブジェクトが採用され、現在の設定内の対応するオブジェクトは上書きされます。
ステップ 6	（任意） UCS-A /system/import-config # **set descr** *description*	インポート操作の説明を記入します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明の前後に引用符を付ける必要があります。引用符は、show コマンド出力の説明フィールドには表示されません。
ステップ 7	（任意） UCS-A /system/import-config # **set password**	**Enter** キーを押すと、パスワードを入力するように促されます。

	コマンドまたはアクション	目的
		リモートサーバのユーザ名のパスワードを指定します。この手順は、TFTPプロトコルを使用する場合には適用されません。 （注） Cisco UCS Manager では、このパスワードは保存されません。したがって、インポート操作を有効にしてただちに実行する場合を除き、このパスワードを入力する必要はありません。
ステップ 8	（任意） UCS-A /system/import-config # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	リモートサーバとの通信時に使用するプロトコルを指定します。
ステップ 9	（任意） UCS-A /system/import-config # **set remote-file** *filename*	インポートする設定ファイルの名前を指定します。
ステップ 10	（任意） UCS-A /system/import-config # **set user** *username*	システムがリモートサーバへのログインに使用する必要のあるユーザ名を指定します。この手順は、TFTPプロトコルを使用する場合には適用されません。
ステップ 11	UCS-A /system/import-config # **commit-buffer**	トランザクションをコミットします。

例

次に、説明を追加し、host35 インポート操作のパスワード、プロトコル、およびユーザ名を変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope import-config host35
UCS-A /system/import-config # set descr "This is an import operation for host35."
UCS-A /system/import-config* # set password
Password:
UCS-A /system/import-config* # set protocol sftp
UCS-A /system/import-config* # set user jforlenz32
UCS-A /system/import-config* # commit-buffer
UCS-A /system/import-config #
```

インポート操作の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **delete import-config** *hostname*	指定したホスト名のインポート操作を削除します。
ステップ 3	UCS-A /system # **commit-buffer**	トランザクションをコミットします。

例

次に、host35 というホスト名のインポート操作を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # delete import-config host35
UCS-A /system* # commit-buffer
UCS-A /system #
```

システムの復元

この復元機能は、ディザスタ リカバリに使用できます。

Cisco UCS からエクスポートされた任意の Full State バックアップ ファイルからシステム設定を復元できます。このファイルは、復元するシステム上の Cisco UCS からエクスポートされたものでなくてもかまいません。別のシステムからエクスポートされたバックアップ ファイルを使用して復元する場合、ファブリック インターコネクト、サーバ、アダプタ、および I/O モジュールまたは FEX 接続を含めて、同じまたは同様のシステム設定およびハードウェアを持つシステムを使用することを推奨します。ハードウェアまたはシステム設定が一致しない場合、復元されたシステムが完全には機能しないことがあります。2 つのシステムの I/O モジュール リンク間またはサーバ間に不一致がある場合、復元操作後にシャーシまたはサーバまたはその両方を承認します。

この復元機能は、Full State バックアップ ファイルにだけ使用できます。Full State バックアップ ファイルはインポートできません。復元は、初期システム セットアップで実行します。詳細については、該当する『*Cisco UCS Central Installation and Upgrade Guide*』を参照してください。

（注） Full State バックアップ ファイルを使用した場合にのみ、バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元できます。

ファブリック インターコネクトの設定の復元

バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元するには、Full State バックアップ ファイルを使用することを推奨します。同じリリース トレインの場合でも、Full State バックアップを使用してシステムを復元できます。たとえば、リリース 2.1(3a) を実行しているシステムから作成した Full State バックアップを使用して、リリース 2.1(3f) を実行するシステムを復元できます。

VSAN または VLAN 設定の問題を回避するには、バックアップ時にプライマリ ファブリック インターコネクトであったファブリック インターコネクトでバックアップを復元する必要があります。

始める前に

システム設定を復元するには、次の情報を収集します。

- ファブリック インターコネクト管理ポートの IPv4 アドレスとサブネット マスク、または IPv6 アドレスとプレフィックス
- デフォルト ゲートウェイの IPv4 アドレスまたは IPv6 アドレス
- バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスと認証クレデンシャル
- Full State バックアップ ファイルの完全修飾名

（注） システムを復元するには、Full State コンフィギュレーション ファイルへのアクセスが必要です。その他のタイプのコンフィギュレーション ファイルやバックアップ ファイルでは、システムを復元できません。

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトがオフの場合はオンにします。

ファブリック インターコネクトがブートする際、Power On Self-Test のメッセージが表示されます。

ステップ 3 インストール方式プロンプトに **console** と入力します。

ステップ 4 **restore** と入力して、Full State バックアップから設定を復元します。

ステップ 5 **y** と入力して、Full State バックアップから復元することを確定します。

ステップ 6 ファブリック インターコネクトの管理ポートの IP アドレスを入力します。

ステップ 7 ファブリック インターコネクトの管理ポートのサブネット マスクを入力します。

ステップ 8 デフォルト ゲートウェイの IP アドレスを入力します。

ステップ 9 バックアップ コンフィギュレーション ファイルを取得する際に使用する、次のいずれかのプロトコルを入力します。

- **scp**
- **ftp**
- **tftp**
- **sftp**

ステップ 10 バックアップ サーバの IP アドレスを入力します。

ステップ 11 Full State バックアップ ファイルのフル パスおよびファイル名を入力します。

（注） Full State バックアップ ファイルを使用した場合にのみ、バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元できます。

ステップ 12 バックアップ サーバにアクセスするためのユーザ名とパスワードを入力します。

ファブリック インターコネクトがバックアップ サーバにログインし、指定された Full State バックアップファイルのコピーを取得し、システム設定を復元します。クラスタ設定の場合、セカンダリ ファブリック インターコネクトを復元する必要はありません。セカンダリ ファブリック インターコネクトがリブートすると、Cisco UCS はただちにその設定をプライマリ ファブリック インターコネクトと同期させます。

例

次に、FTP を使用して 20.10.20.10 のバックアップ サーバから取得された Backup.bak ファイルからシステム設定を復元する例を示します。

```
Enter the configuration method. (console/gui) ? console

Enter the setup mode; setup newly or restore from backup. (setup/restore) ? restore

NOTE:
  To configure Fabric interconnect using a backup file on a remote server,
  you will need to setup management interface.
  The management interface will be re-configured (if necessary),
  based on information stored in the backup file.


Continue to restore this Fabric interconnect from a backup file (yes/no) ? yes

Physical Switch Mgmt0 IPv4 address : 192.168.10.10

Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 192.168.10.1

Enter the protocol to get backup file (scp/ftp/tftp/sftp) ?  scp
Enter the IP address of backup server: 20.10.20.10
Enter fully qualified backup file name: Backup.bak
Enter user ID: user
Enter password:
```

```
    Retrieved backup configuration file.
  Configuration file - Ok


Cisco UCS 6100 Series Fabric Interconnect
UCS-A login:
```

設定の削除

注意 必要な場合に限り設定を削除してください。設定を削除すると、設定が完全に削除され、システムが未設定の状態でリブートします。その後、バックアップファイルから設定を復元する必要、または初期システム セットアップを実行する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **connect local-mgmt**	ローカル管理 CLI を開始します。
ステップ 2	UCS-A(local-mgmt)# **erase configuration**	設定を削除します。 設定の削除を確認するプロンプトが表示されます。 **yes** と入力すると、設定は削除され、システムが未設定の状態でリブートします。

例

次に、設定を削除する例を示します。

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# erase configuration
All UCS configurations will be erased and system will reboot. Are you sure? (yes/no):
yes
```

第 11 章

スケジュール オプション

導入スケジュール オプション

スケジュールの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **create scheduler** *sched-name*	スケジューラを作成し、スケジューラ モードを開始します。
ステップ 3	UCS-A /system/scheduler # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、maintenancesched という名前のスケジューラを作成し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # create scheduler maintenancesched
UCS-A /system/scheduler* # commit-buffer
UCS-A /system/scheduler #
```

次のタスク

スケジュールのワンタイム オカレンスまたは繰り返しオカレンスを作成します。

スケジュールのワンタイム オカレンスの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope schedule** *sched-name*	スケジューラ システム モードを開始します。
ステップ 3	UCS-A /system/scheduler # **create occurrence one-time** *occurrence-name*	ワンタイム オカレンスを作成します。
ステップ 4	UCS-A /system/scheduler/one-time # **set date** *month day-of-month year hour minute*	このオカレンスを実行する日時を設定します。
ステップ 5	（任意） UCS-A /system/scheduler/one-time # **set concur-tasks** {**unlimited** | *max-num-concur-tasks*	このオカレンスの間に同時実行可能なタスクの最大数を設定します。 タスクの最大数に達すると、スケジューラは新しいタスクをスケジュールする前に、[minimum interval] プロパティで設定された時間だけ待機します。
ステップ 6	（任意） UCS-A /system/scheduler/one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	このスケジュール オカレンスを実行できる最長時間を設定します。ここで指定された時間内に、Cisco UCS は可能な限り多くのスケジュール済みタスクを完了します。
ステップ 7	（任意） UCS-A /system/scheduler/one-time # **set min-interval** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	システムが新しいタスクを開始するまで待機する時間の最小長を設定します。
ステップ 8	（任意） UCS-A /system/scheduler/one-time # **set proc-cap** {**unlimited** | *max-num-of-tasks*}	このオカレンスの間に実行可能な、スケジュール設定されたタスクの最大数を設定します。
ステップ 9	UCS-A /system/scheduler/one-time # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、onetimemaint という名前のワンタイム オカレンスを maintsched という名前のスケジューラに作成します。また、同時実行タスクの最大数を 5 に設定し、開始日時を 2011 年 4 月 1 日 11：00 に設定して、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope scheduler maintsched
UCS-A /system/scheduler # create occurrence one-time onetimemaint
UCS-A /system/scheduler/one-time* # set date apr 1 2011 11 00
UCS-A /system/scheduler/one-time* # set concur-tasks 5
UCS-A /system/scheduler/one-time* # commit-buffer
UCS-A /system/scheduler/one-time #
```

スケジュールへの繰り返しオカレンスの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope schedule** *sched-name*	スケジューラ システム モードを開始します。
ステップ 3	UCS-A /system/scheduler # **create occurrence recurring** *occurrence-name*	繰り返しオカレンスを作成します。
ステップ 4	（任意） UCS-A /system/scheduler/recurring # **set day** {**even-day** | **every-day** | **friday** | **monday** | **never** | **odd-day** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday**}	Cisco UCS でこのスケジュールのオカレンスを実行する曜日を選択します。 デフォルトでは、このプロパティは never に設定されています。
ステップ 5	（任意） UCS-A /system/scheduler/recurring # **set hour** *hour*	このオカレンスが開始する時間（時）を指定します。 （注） Cisco UCS は、最大長に達していない場合でも、すべての繰り返しオカレンスをそれが開始したのと同じ日に終了させます。たとえば、開始時刻を午後 11 時、最長継続時間を 3 時間に指定すると、Cisco UCS はこのオカレンスを午後 11 時に開始しますが、59 分しか経過していない午後 11 時 59 分に終了します。

	コマンドまたはアクション	目的
ステップ 6	（任意） UCS-A /system/scheduler/recurring # **set minute** *minute*	このオカレンスが開始する時間（分）を指定します。
ステップ 7	（任意） UCS-A /system/scheduler/recurring # **set concur-tasks** {**unlimited** | *max-num-concur-tasks*	このオカレンスの間に同時実行可能なタスクの最大数を設定します。 タスクの最大数に達すると、スケジューラは新しいタスクをスケジュールする前に、[minimum interval] プロパティで設定された時間だけ待機します。
ステップ 8	（任意） UCS-A /system/scheduler/recurring # **set max-duration** {**none** | *num-of-hours num-of-minutes num-of-seconds*}	このスケジュールオカレンスを実行できる最長時間を設定します。ここで指定された時間内に、Cisco UCS は可能な限り多くのスケジュール済みタスクを完了します。
ステップ 9	（任意） UCS-A /system/scheduler/recurring # **set min-interval** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	システムが新しいタスクを開始するまで待機する時間の最小長を設定します。
ステップ 10	（任意） UCS-A /system/scheduler/recurring # **set proc-cap** {**unlimited** | *max-num-of-tasks*}	このオカレンスの間に実行可能な、スケジュール設定されたタスクの最大数を設定します。
ステップ 11	UCS-A /system/scheduler/recurring # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、maintsched というスケジューラに recurringmaint という繰り返しオカレンスを作成し、同時実行タスクの最大数を 5 に設定し、このオカレンスの実行日を偶数日に設定し、11:05 から開始するように時間を設定してトランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope scheduler maintsched
UCS-A /system/scheduler # create occurrence recurring recurringmaint
UCS-A /system/scheduler/recurring* # set day even-day
UCS-A /system/scheduler/recurring* # set hour 11
UCS-A /system/scheduler/recurring* # set minute 5
UCS-A /system/scheduler/recurring* # set concur-tasks 5
UCS-A /system/scheduler/recurring* # commit-buffer
UCS-A /system/scheduler/recurring #
```

スケジュールからのワンタイム オカレンスの削除

これがスケジュールにおける唯一の実行である場合には、そのスケジュールは実行なしで再設定されます。スケジュールがメンテナンス ポリシーに含まれており、そのポリシーがサービス プロファイルに割り当てられている場合、サービス プロファイルに関連付けられているサーバに関連する保留中のアクティビティは展開できません。保留中のアクティビティを展開するには、ワンタイム オカレンスまたは繰り返しオカレンスをスケジュールに追加する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope scheduler** *sched-name*	スケジューラ システム モードを開始します。
ステップ 3	UCS-A /system/scheduler # **delete occurrence one-time** *occurrence-name*	指定されたワンタイム オカレンスを削除します。
ステップ 4	UCS-A /system/scheduler # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、maintsched スケジューラから onetimemaint というワンタイム オカレンスを削除し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope scheduler maintsched
UCS-A /system/scheduler # delete occurrence one-time onetimemaint
UCS-A /system/scheduler* # commit-buffer
UCS-A /system/scheduler #
```

スケジュールからの繰り返しオカレンスの削除

これがスケジュールにおける唯一の実行である場合には、そのスケジュールは実行なしで再設定されます。スケジュールがメンテナンス ポリシーに含まれており、そのポリシーがサービス プロファイルに割り当てられている場合、サービス プロファイルに関連付けられているサーバに関連する保留中のアクティビティは展開できません。保留中のアクティビティを展開するには、ワンタイム オカレンスまたは繰り返しオカレンスをスケジュールに追加する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope scheduler** *sched-name*	スケジューラ システム モードを開始します。
ステップ 3	UCS-A /system/scheduler # **delete occurrence recurring** *occurrence-name*	指定された繰り返しオカレンスを削除します。
ステップ 4	UCS-A /system/scheduler # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、maintsched スケジューラから onetimemaint という名前の繰り返しオカレンスを削除し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope scheduler maintsched
UCS-A /system/scheduler # delete occurrence recurring onetimemaint
UCS-A /system/scheduler* # commit-buffer
UCS-A /system/scheduler #
```

スケジュールの削除

このスケジュールがメンテナンス ポリシーに含まれている場合、ポリシーはスケジュールなしで再設定されます。そのポリシーがサービスプロファイルに割り当てられている場合、サービスプロファイルに関連付けられているサーバに関連する保留中のアクティビティは展開できません。保留中のアクティビティを展開するには、スケジュールをメンテナンス ポリシーに追加する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **delete scheduler** *sched-name*	スケジューラを削除し、スケジューラ モードを開始します。
ステップ 3	UCS-A /system # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、maintenancesched という名前のスケジューラを削除し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # delete scheduler maintenancesched
UCS-A /system* # commit-buffer
UCS-A /system #
```

第 12 章

サービス プロファイル更新の遅延展開

サービス プロファイルの遅延展開

サービス プロファイルの変更の一部、またはサービス プロファイル テンプレートの更新は、中断を伴うことや、サーバのリブートが必要になることがあります。ただし、これらの中断を伴う設定変更をいつ実行するかを、遅延展開によって制御できます。たとえば、サービスプロファイルの変更をすぐに展開するか、指定されたメンテナンス時間帯に展開するかを選択できます。また、サービスプロファイルの展開にユーザの明示的な確認応答が必要かどうかを選択できます。

遅延展開は、サーバとサービスプロファイルとの関連付けによって発生するすべての設定変更に使用できます。これらの設定変更は、サービス プロファイルへの変更、サービス プロファイルに含まれるポリシーへの変更、更新サービス プロファイル テンプレートへの変更によってプロンプト表示される場合があります。たとえば、サーバ BIOS、RAID コントローラ、ホスト HBA、ネットワーク アダプタなどのホスト ファームウェア パッケージや管理ファームウェア パッケージによって、ファームウェアのアップグレードおよびアクティブ化を延期することもできます。ただし、Cisco UCS Manager、ファブリック インターコネクト、I/O モジュールなど、ファームウェア パッケージを使用しないコンポーネントのファームウェア イメージの直接展開を遅延させることはできません。

遅延展開は、サーバのリブートを必要とする次のアクションに使用できません。

- サーバのサービス プロファイルの最初の関連付け
- サービス プロファイルと別のサーバを関連付けない、サービス プロファイルのサーバからの関連付けの最終解除
- サーバの解放
- サーバの再認識
- サーバのリセット

サービスプロファイル変更の展開を遅延させる場合、1つ以上のメンテナンス ポリシーを設定し、各サービス プロファイルにメンテナンス ポリシーを設定する必要があります。展開が発生する時間帯を指定する場合、1つ以上の繰り返しオカレンスまたはワンタイム オカレンスを持つスケジュールを少なくとも1つ作成し、そのスケジュールをメンテナンス ポリシーに含める必要があります。

遅延展開のスケジュール

スケジュールには、一連のオカレンスが含まれます。これらのオカレンスは、1回だけ発生させるか、または毎週指定した日時に繰り返し発生させることができます。オカレンスの時間長や実行されるタスクの最大数といった、オカレンスで定義されるオプションにより、あるサービスプロファイルの変更が展開されるかどうかが決まります。たとえば、最大時間長またはタスク数に達したため特定のメンテナンス時間帯に変更を展開できない場合、この展開は次のメンテナンス時間に持ち越されます。

各スケジュールは、Cisco UCS ドメイン が1つまたは複数のメンテナンス時間帯に入っているかどうか、定期的に確認します。入っている場合、スケジュールはメンテナンス ポリシーで指定された制限に対し適切な展開を実行します。

スケジュールには、スケジュールに関連付けられたメンテナンス時間を決定する1つ以上のオカレンスが含まれています。オカレンスは次のいずれかになります。

ワンタイム オカレンス

ワンタイム オカレンスは、単一のメンテナンス時間を定義します。これらの時間帯は、その時間帯の最大時間長まで、または時間帯の中で実行可能なタスクの最大数に達するまで継続されます。

繰り返しオカレンス

繰り返しオカレンスは、一連のメンテナンス時間を定義します。これらの時間帯は、タスクの最大数に達するまで、またはオカレンスに指定された日の終わりに達するまで継続します。

遅延展開のための保留アクティビティ

Cisco UCS ドメイン で遅延展開を構成すると、保留中のすべてのアクティビティを Cisco UCS Manager で表示することができます。ユーザの確認応答を待っているアクティビティと、スケジュールされたアクティビティを表示できます。

Cisco UCS ドメイン に保留中のアクティビティがある場合、Cisco UCS Manager GUI は、管理者権限を持つユーザがログインしたときにそれを通知します。

Cisco UCS Manager は、すべての保留アクティビティについて次のような情報を表示します。

- 展開され、サーバと関連付けられるサービス プロファイルの名前
- 展開の影響を受けるサーバ
- 展開により発生する中断

- 展開によって実行される変更

（注） 特定の保留アクティビティがサーバに適用されるメンテナンス時間を指定することはできません。メンテナンス時間帯は、保留アクティビティの数およびサービスプロファイルに割り当てられているメンテナンス ポリシーに応じて変化します。ただし、保留アクティビティがユーザの確認応答またはメンテナンス時間帯のいずれを待っているかにかかわらず、管理者権限を持つユーザは、手動で保留アクティビティを開始して、ただちにサーバをリブートできます。

遅延展開に関するガイドラインおよび制限事項

サービス プロファイルの関連付けの変更とメンテナンス ポリシーのオプション

サービス プロファイルの関連付けを変更する場合、次のメンテナンス ポリシーのオプションが変更の適用方法に影響する可能性があります。

- メンテナンス ポリシーで [On Next Boot] および [User Ack] オプションが有効になっている場合、サービスプロファイルの関連付けの変更では、確認が必要であるという警告が表示されます。ただし、関連付けはすぐに行われます。
- メンテナンス ポリシーで [On Next Boot] および [User Ack] オプションが有効になっていない場合、サービスプロファイルの関連付けの変更では、確認が必要であるという警告が表示され、確認されるまで保留されます。

サービス プロファイルまたはサービス プロファイル テンプレートへのすべての変更を元に戻すことはできない

保留中の変更をキャンセルする場合、Cisco UCS Manager はサーバを再起動せずに変更のロール バックを試みます。ただし、複雑な変更を行った場合、Cisco UCS Manager では変更をロール バックするために 2 回目のサーバ リブートが必要になることがあります。たとえば、vNIC を削除すると、Cisco UCS Manager はサービス プロファイルに含まれているメンテナンス ポリシーに従ってサーバをリブートします。サービス プロファイルで元の vNIC を復元しても、この再起動および変更はキャンセルできません。代わりに、Cisco UCS Manager は 2 回目の展開とサーバのリブートをスケジュールします。

サービス プロファイルの関連付けはメンテナンス時間の境界を超えてもよい

Cisco UCS Manager がサービス プロファイルの関連付けを開始した後は、スケジューラとメンテナンス ポリシーによって手順を制御する方法がなくなります。割り当てられたメンテナンス時間内にサービスプロファイルの関連付けが完了しない場合、プロセスは完了するまで続行されます。たとえば、段階の再試行やその他の問題のために時間内に関連付けが完了しなかった場合に、このような状況が発生することがあります。

保留中のアクティビティの順序を指定できない

スケジュールされた展開は、独立して並行実行されます。展開が発生する順序は指定できません。また、あるサービスプロファイルの変更を他のものの完了を条件として実行することもできません。

保留中のアクティビティの部分的な展開を実行できない

Cisco UCS Manager は、サーバ プロファイルに加えられたすべての変更をスケジュールされたメンテナンス時間に適用します。サービスプロファイルに複数の変更を加えた後にそれらの変更を別々のメンテナンス時間に振り分けることはできません。サービスプロファイルの変更を展開するとき、Cisco UCS Manager はデータベース内の最新の設定に一致するようにサービスプロファイルを更新します。

メンテナンス ポリシーの設定

メンテナンス ポリシー

メンテナンス ポリシーは、サービス プロファイルの変更の展開方法を指定します。展開は、次のいずれかの方法で実行されます。

- 即時実行
- ユーザが管理者権限で承認したときに実行
- スケジュールで指定された時間に自動的に実行
- ユーザによる確認応答の待機またはタイマー スケジュール オプションを伴わない次回のリブートまたはシャットダウン時に実行

[On Next Boot] が機能するには、ブレードまたはラック サーバの UCSM と CIMC バージョンで、3.1.x バンドルのファームウェアが実行されている必要があります。

メンテナンス ポリシーで [On Next Boot] オプションが有効にされている場合、Cisco UCS Manager リリース 3.1(1) 以降を Cisco UCS Manager リリース 2.2(8) より前のリリースにダウングレードすると、ファームウェア ダウングレードが失敗します。ダウングレードを継続するには、メンテナンス ポリシーから [On Next Boot] を無効にします。

メンテナンス ポリシーでソフト シャットダウン タイマーを使用すると、ハード シャットダウンを実行するまでの待機時間を設定できます。ソフト シャットダウン タイマーは、次のようにサーバを再起動するときに適用されます。

- [Gracefully Restart OS] オプションを使用してサーバをリセットします。
- [In case of graceful shutdown failure, a hard shutdown will be issued after X seconds] オプションを使用してサーバをシャットダウンします。
- サーバの再起動が必要なサービス プロファイルを変更します。

スケジュール済みのメンテナンス ウィンドウ中に変更を展開するように設定されているメンテナンスポリシーでは、ポリシーに有効なスケジュールが含まれていることが必要です。この場合、最初に使用可能なメンテナンス ウィンドウ中に変更が展開されます。

（注） メンテナンス ポリシーでは、関連付けられたサービス プロファイルに設定変更が加えられた場合に、サーバの即時リブートは回避できますが、次のアクションの即時実行は回避されません。

- 関連付けられたサービス プロファイルのシステムからの削除
- サーバ プロファイルのサーバからの関連付けの解除
- サービス ポリシーを使用しないファームウェア アップグレードの直接インストール
- サーバのリセット

メンテナンス ポリシーの作成

始める前に

このメンテナンスポリシーを遅延展開のために設定する場合は、スケジュールを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create maint-policy** *policy-name*	指定されたメンテナンス ポリシーを作成し、メンテナンス ポリシー モードを開始します。
ステップ 3	UCS-A /org/maint-policy # **set reboot-policy** {**immediate** | **timer-automatic** | **user-ack**} | **on next boot**	サービス プロファイルがサーバに関連付けられている場合、関連付けを完了するにはサーバをリブートする必要があります。reboot-policy コマンドを指定すると、このメンテナンス ポリシーを含むすべてのサービス プロファイルについて発生するタイミングを決定できます。有効な値は次のとおりです。 • **immediate**：サービス プロファイルが変更されると、すぐにサーバがリブートします。

	コマンドまたはアクション	目的
		• **timer-automatic** ：**`set scheduler`** コマンドを使用して、メンテナンス操作が適用されるタイミングを指定するスケジュールを選択できます。Cisco UCS はスケジュールされた時刻にサーバをリブートしてサービス プロファイルの変更を完了します。 • **user-ack** ：ユーザは、変更が適用される前に **apply pending-changes** コマンドを使用して変更を明示的に確認する必要があります。
ステップ 4	UCS-A /org/maint-policy # {**enable** | **disable**} **on-next-boot**	このオプションを有効にすると、サービス プロファイルの関連付けが完了した後の次のリブート時またはシャットダウン時にサーバが自動的にリブートされます。したがって、ユーザの確認やタイマーによる自動メンテナンス期間のスケジュール オプションを待機する必要はありません。 （注） [On Next Boot] オプションを選択しない場合、BMC のメンテナンス ポリシーは無効になります。 **reboot-policy** を **timer-automatic** または **user-ack** に設定してこのオプションを有効にすると、スケジュールされたメンテナンス期間外にサーバがリブートする場合や、ユーザによる確認がない場合でも、サーバがリブートするたびに変更が適用されることになります。
ステップ 5	（任意） UCS-A /org/maint-policy # **set scheduler** *scheduler-name*	reboot-policy プロパティが timer-automatic に設定された場合、メンテナンス操作がサーバに適用されるタイミングを指定するスケジュールを選択する必要があります。Cisco UCS はスケジュールされた時刻にサーバをリブートしてサービス プロファイルの変更を完了します。
ステップ 6	UCS-A /org/maint-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、maintenance というメンテナンス ポリシーを作成し、サービス プロファイルがサーバに関連付けられるとすぐにリブートするようシステムを設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # create maint-policy maintenance
UCS-A /org/maint-policy* # set reboot-policy immediate
UCS-A /org/maint-policy* # commit-buffer
UCS-A /org/maint-policy #
```

メンテナンス ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **delete maint-policy** *policy-name*	指定されたメンテナンス ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、maintenance という名前のメンテナンス ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete maint-policy maintenance
UCS-A /org/maint-policy* # commit-buffer
UCS-A /org/maint-policy #
```

保留アクティビティ

遅延展開のための保留アクティビティ

Cisco UCS ドメイン で遅延展開を構成すると、保留中のすべてのアクティビティを Cisco UCS Manager で表示することができます。ユーザの確認応答を待っているアクティビティと、スケジュールされたアクティビティを表示できます。

Cisco UCS ドメイン に保留中のアクティビティがある場合、Cisco UCS Manager GUI は、管理者権限を持つユーザがログインしたときにそれを通知します。

Cisco UCS Manager は、すべての保留アクティビティについて次のような情報を表示します。

- 展開され、サーバと関連付けられるサービス プロファイルの名前
- 展開の影響を受けるサーバ
- 展開により発生する中断
- 展開によって実行される変更

（注） 特定の保留アクティビティがサーバに適用されるメンテナンス時間を指定することはできません。メンテナンス時間帯は、保留アクティビティの数およびサービスプロファイルに割り当てられているメンテナンスポリシーに応じて変化します。ただし、保留アクティビティがユーザの確認応答またはメンテナンス時間帯のいずれを待っているかにかかわらず、管理者権限を持つユーザは、手動で保留アクティビティを開始して、ただちにサーバをリブートできます。

保留アクティビティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	組織モードを開始します。 ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **show pending-changes** [**detail** | **expand**]	保留中の変更に関する詳細を表示します。

例

次に、accounting というサービス プロファイルの保留中の変更を表示する例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # show pending-changes detail

Pending Changes:
    Scheduler:
    Changed by: admin
```

```
    Acked by:
    Mod. date: 2010-09-20T20:36:09.254
    State: Untriggered
    Admin State: Untriggered
    Pend. Changes: 0
    Pend. Disr.: 0
UCS-A /org/service-profile #
```

ユーザの確認応答待ちサービス プロファイル変更の展開

Cisco UCS Manager CLI は、ユーザの確認応答を待機中の複数のサービス プロファイルに関する、保留中のすべての変更を展開することはできません。複数のサービスプロファイルの保留中のすべての変更を同時に展開するには、Cisco UCS Manager GUIを使用します。

重要 保留中のアクティビティを確認した後、Cisco UCS Manager が影響のあるサーバをリブートすることは抑止できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	組織モードを開始します。 ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **apply pending-changes immediate**	保留中の変更をただちに適用します。 Cisco UCS Manager によって保留中のアクティビティの影響を受けるサーバがただちに再起動されます。

例

次に、accounting という名前のサービス プロファイルの保留中の変更を適用する例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # apply pending-changes immediate
UCS-A /org/service-profile #
```

スケジュールされたサービス プロファイル変更の即時展開

Cisco UCS Manager CLI は、複数のサービス プロファイルの、スケジュールされているすべての変更を同時に展開することはできません。複数のサービスプロファイルの、スケジュールされているすべての変更を同時に展開するには、Cisco UCS Manager GUIを使用します。

重要 保留中のアクティビティを確認した後、Cisco UCS Manager が影響のあるサーバをリブートすることは抑止できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	組織モードを開始します。 ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **apply pending-changes immediate**	保留中の変更をただちに適用します。 Cisco UCS Manager によって保留中のアクティビティの影響を受けるサーバがただちに再起動されます。

例

次に、accounting というサービス プロファイルの保留中の変更を適用する例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # apply pending-changes immediate
UCS-A /org/service-profile #
```

第 13 章

UCS の障害抑制

システム メンテナンスに対する障害抑制

グローバル障害ポリシー

グローバル障害ポリシーは、障害がクリアされた日時、フラッピング間隔（障害発生とクリア状態の間の時間）、および保持間隔（システムで障害が発生していた時間）など、Cisco UCS ドメイン 内の障害のライフサイクルを制御します。

Cisco UCS の障害には次のライフサイクルがあります。

1. ある状況がシステムで発生し、Cisco UCS Manager で障害が発生します。これはアクティブな状態です。
2. 障害が軽減されると、フラッピングまたはフラッピングを防ぐことを目的としたソーキング間隔になります。障害が発生し、すぐに何度かクリアされると、フラッピングが発生します。フラッピング間隔の間、グローバル障害ポリシーに指定されている期間は、障害の重要度が保持されます。
3. フラッピング間隔中に同じ条件が再発生した場合は、障害がアクティブ状態に戻ります。フラッピング間隔中に同じ条件が再発生しない場合は、障害がクリアされます。
4. クリアされた障害は保持期間になります。この期間があるため、障害が発生した状態が改善され、さらに障害が早々に削除されていない場合でも管理者が障害に気付くことができます。保持期間のうち、グローバル障害ポリシーに指定された期間はクリアされた障害が保持されます。
5. この状況が保持間隔中に再発生する場合は、障害がアクティブ状態に戻ります。この状況が再発生しない場合は、障害が削除されます。

障害収集ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope fault policy**	モニタリング障害ポリシー モードを開始します。
ステップ 3	UCS-A /monitoring/fault-policy # **set clear-action** {**delete** | **retain**}	クリアしたすべてのメッセージを保持するか、削除するかを指定します。 **retain** オプションが指定された場合、メッセージを保持する時間の長さは、 **set retention-interval** コマンドによって決まります。
ステップ 4	UCS-A /monitoring/fault-policy # **set flap-interval** *seconds*	障害状態を変更する前にシステムが待機する間隔を指定します（秒単位）。障害が発生し、すぐに何度かクリアされると、フラッピングが発生します。これを回避するために、最後の状態変更後からフラッピング間隔が経過するまで、システムは障害の状態の変更を許可しません。フラッピング間隔中に障害が再発生した場合は、障害がアクティブ状態に戻ります。それ以外の場合は、障害がクリアされます。
ステップ 5	UCS-A /monitoring/fault-policy # **set retention-interval** {*days hours minutes seconds* | **forever**}	システムが、削除する前にクリアしたすべての障害メッセージを保持する時間間隔を指定します。システムは、クリアされた障害メッセージを永続的に保持することも、指定された日数、時間数、分数、秒数保持することもできます。
ステップ 6	UCS-A /monitoring/fault-policy # **commit-buffer**	トランザクションをコミットします。

例

この例では、クリアされた障害メッセージを30日間保持するよう障害収集ポリシーを設定し、フラッピング間隔を 10 秒に設定し、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope fault policy
UCS-A /monitoring/fault-policy # set clear-action retain
```

```
UCS-A /monitoring/fault-policy* # set flap-interval 10
UCS-A /monitoring/fault-policy* # set retention-interval 30 0 0 0
UCS-A /monitoring/fault-policy* # commit-buffer
UCS-A /monitoring/fault-policy #
```

第 14 章

デバイス コネクタ

デバイス コネクタ

デバイス コネクタは、Cisco UCS Manager をクラウドホスト型のサーバ管理システムである Cisco Intersight に接続します。これにより、Cisco UCS Manager を Cisco Intersight を使用して管理およびモニタできるようになります。

クラウド内の Cisco Intersight にデバイスを登録するには、次の手順を実行します。

1. 必要に応じて、デバイス コネクタのプロキシ設定を行って、Cisco UCS Manager を Cisco Intersight と接続します。
2. デバイスのシリアル番号とセキュリティ コードを使用して、Cisco Intersight からデバイスへのアクセスを検証し、デバイスを要求します。

デバイス コネクタの更新

Cisco UCS Manager をアップグレードすると、デバイス コネクタは Cisco UCS Manager バージョンと統合されたイメージに自動的に更新されます。Cisco UCS Manager バージョンをダウングレードしても、デバイス コネクタはダウングレードされません。

Cisco Intersight GUI を使用して、デバイス コネクタを更新できます。Cisco UCS Manager CLI でローカル管理シェルを使用して、デバイス コネクタを更新することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **connect local-mgmt**	ローカル管理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	UCS-A(local-mgmt)# **copy** [*from-filesystem*:] [*from-path*] *filename to-path* [*dest-filename*]	指定されたファイル転送プロトコルを使用して、デバイス コネクタのイメージ ファイルをリモート サーバからローカルの宛先にコピーします。ファイルは、1 つのファブリック インターコネクトにのみコピーする必要があります。 • *from-filesystem*：コピー元のファイルを含んでいるリモート ファイル システム。 このファイルは、次のオプションのいずれかを使用して指定できます。 • **ftp:** [// [*username@*] *server*] • **scp:** [// [*username@*] *server*] • **sftp:** [// [*username@*] *server*] • **tftp:** [//*server* [:*port*]] ファイル システムを指定しない場合、現在の作業ファイル システムが表示されます。 サーバ名を指定せずに、リモート プロトコルを指定した場合、サーバ名の入力が求められます。 • *from-path*：コピー元のファイルの絶対パスまたは相対パス。パスを指定しない場合、現在の作業ディレクトリが前提とされます。 • *filename*：コピー元のファイルの名前。 • *to-path*：コピー先のファイルの絶対パスまたは相対パス。パスを指定しない場合、現在の作業ディレクトリが前提とされます。このパスにはローカル ファイル システムが組み込まれており、コピー先のファイルが含まれています。 このファイル システムは、次のオプションのいずれかから指定できます。

	コマンドまたはアクション	目的
		• **volatile:** • **workspace:** • *dest-filename*：コピー先のファイルの新しいファイル名。dest-filenameを指定すると、コピー元のファイルはコピー先で名前変更されます。 （注） Cisco UCS Manager GUIを使用してデバイス コネクタのイメージ ファイルをダウンロードすることはできません。
ステップ 3	UCS-A(local-mgmt)# **update-device-connector workspace:** | **volatile:**/*filename* [**skip-upgrade-on-peer**]	ピアのファブリック インターコネクトでデバイス コネクタ イメージを更新してから、ローカルのファブリック インターコネクトを更新します。 **skip-upgrade-on-peer** オプションを使用すると、ピアのファブリック インターコネクトの更新がスキップされます。

例

次に、両方のファブリック インターコネクトでデバイス コネクタを更新する例を示します。

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# copy scp://username@10.100.100.100/filepath/filename.bin workspace:/
UCS-A(local-mgmt)# update-device-connector workspace:/filename.bin
Update Started
Updating Device Connector on peer Fabric interconnect
Successfully updated device connector on peer Fabric interconnect
Updating Device Connector on local Fabric interconnect
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```

次に、ローカルのファブリック インターコネクトのみでデバイス コネクタが更新される例を示します。

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# copy scp://username@10.100.100.100/filepath/filename.bin workspace:/
UCS-A(local-mgmt)# update-device-connector workspace:/filename.bin skip-upgrade-on-peer
Update Started
Updating Device Connector on local Fabric interconnect
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```