Cisco UCS Manager リリース 4.1 アドミニストレーション管理ガイド

初版：2020 年 2 月 20 日

最終更新：2020 年 7 月 30 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 つ以上に責任を持つ、専門知識を備えたデータセンター管理者を主な対象にしています。

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

表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールド ラベルなどの GUI 要素は、イタリック体（**italic**）で示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルなどのメイン 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。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

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

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

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

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

警告 安全上の重要な注意事項

This warning symbol means danger. 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

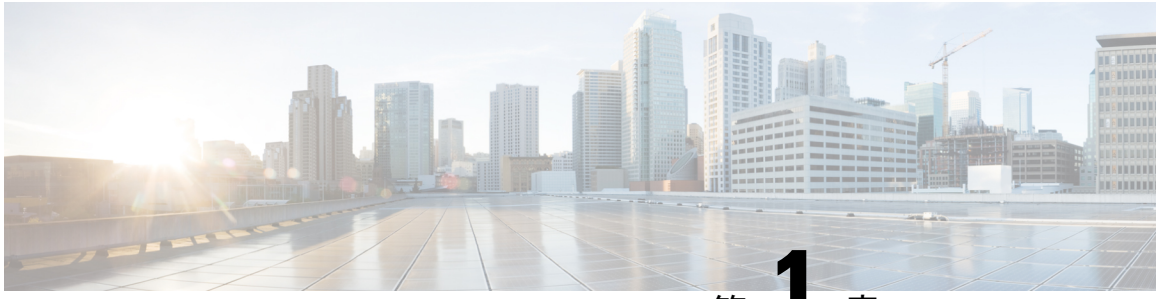
管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、「Release Bundle Contents for Cisco UCS Software」を参照してください。

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

このリリースの新規情報および変更情報

新機能および変更された機能に関する情報

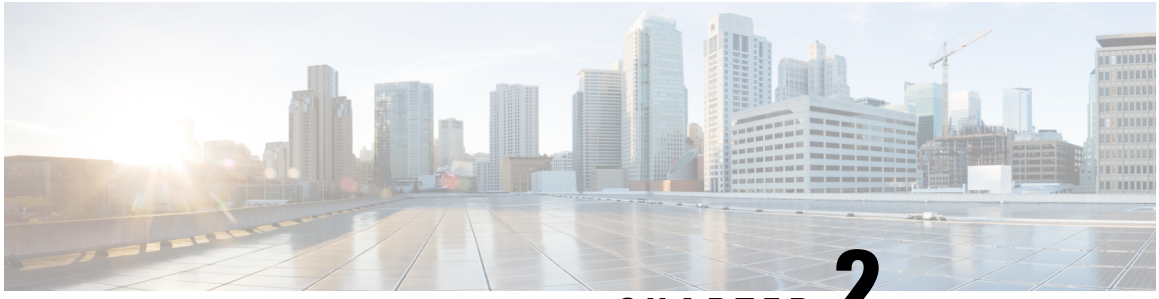
ここでは、Cisco UCS Manager リリース 4.1 (x) の新機能および変更された動作について説明します。

表 *1 : Cisco UCS Manager* リリース *4.1(2)* の新機能と変更された動作

機能	説明	参照先
Intersight 管理モード (IMM)	IMM は、Cisco UCS Manager で最初に導入されたコンセプトを新しく実装しており、ポリシー モデルのオーナーシップを Cisco Intersight に移行しています。	Intersight 管理モード （195 ページ）

表 *2 : Cisco UCS Manager* リリース *4.1(1)* の新機能と変更された動作

機能	説明	参照先
Cisco UCS 64108 ファブリックインターコネクトのパスワード回復	Cisco UCS 6400 ファブリックインターコネクトで管理者パスワードを回復する方法を説明します。	amin アカウントのパスワードの復旧 （12 ページ）



CHAPTER 2

管理の概要

この章は、次の項で構成されています。

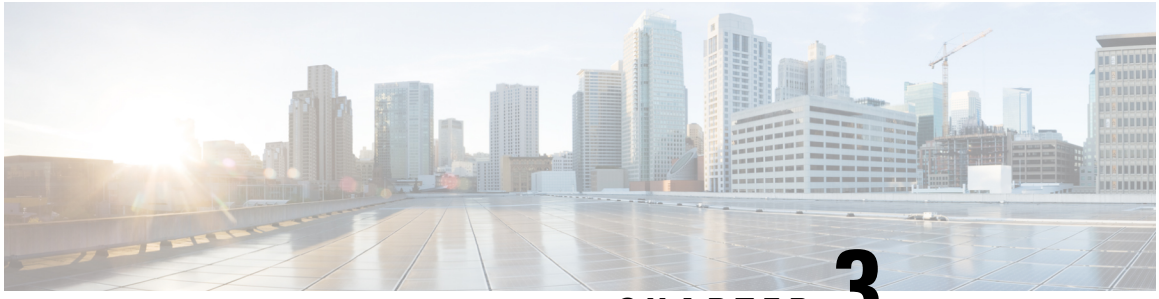
管理の概要

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 6400 シリーズ ファブリック インターコネクト、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。



CHAPTER 3

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 3 : UCS パスワードに使用可能な ASCII 文字の表 （5 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 *3 : 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

出力可能な ASCII 文字	説明
'	アポストロフィ
(	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

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]の順に展開します。**

ステップ 3 [Locally Authenticated Users] ノードをクリックします。

ステップ 4 [Password Profile] 領域で、次の手順を実行します。

a) [Change During Interval] フィールド で、**[Enable]** をクリックします。

b) [Change Count] フィールド で、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 を入力します。

この値は、0 ～ 10 から自由に設定できます。

c) [Change Interval] フィールド で、[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 を入力します。

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。

ステップ 5 [Save Changes] をクリックします。

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

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]の順に展開します。**

ステップ 3 [Locally Authenticated Users] ノードをクリックします。

ステップ 4 [Password Profile] 領域で、次の手順を実行します。

a) [Change During Interval] フィールド で、**[Enable]** をクリックします。

b) [No Change Interval] フィールド で、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。 を入力します。

この値は、1 ～ 745 時間の範囲で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 [Save Changes] をクリックします。

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

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]の順に展開します。**

ステップ 3 [Locally Authenticated Users] ノードをクリックします。

ステップ 4 [Password Profile] 領域で、ローカル認証されたユーザが、以前 [History Count] フィールド で使用したパスワードを再使用できるようになる前に、作成する必要がある一意のパスワードの数を入力します。

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 5 [Save Changes] をクリックします。

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

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]** > **[Locally Authenticated Users]**の順に展開します。

ステップ 3 パスワード履歴をクリアするユーザをクリックします。

ステップ 4 [Actions] 領域で、[Clear Password History] をクリックします。

ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

失われたパスワードの復旧

amin アカウントのパスワードの復旧

admin アカウントは、システム アドミニストレータまたはスーパーユーザのアカウントです。アドミニストレータが admin アカウントのパスワードを失うと、重大なセキュリティ上の問題が発生する可能性があります。admin アカウントのパスワードを回復させる手順では、すべてのファブリック インターコネクトに電源を再投入する必要があり、データ伝送が一時的に停止します。

admin アカウントのパスワードを復旧する場合、実際にはそのアカウントのパスワードを変更します。admin アカウントに対応する元のパスワードを取得することはできません。

admin 以外のすべてのローカル アカウントのパスワードは、Cisco UCS Manager からリセットできます。ただし、aaa または admin 権限を持つアカウントを使用して Cisco UCS Manager にログインする必要があります。

注意 Cisco UCS Mini の場合、この手順で Cisco UCS ドメインに含まれるすべてのファブリック インターコネクトをシャーシ スロットから取り出す必要があります。したがって、ファブリック インターコネクトがそれぞれのシャーシ スロットに戻されるまでは、Cisco UCS ドメインでのデータ送信が全面的に停止します。

他の Cisco UCSについては、この手順ですべてのファブリック インターコネクトの電源を切る必要があります。したがって、ファブリック インターコネクトが再起動されるまでは、Cisco UCS ドメイン内のデータ送信が全面的に停止します。

（注） Cisco UCS 6400 シリーズ ファブリック インターコネクト 別のカーネルとシステム イメージを持っていません。1 つの統一されたイメージがあります。

ファブリック インターコネクトのリーダーシップ ロールの決定

重要 管理者パスワードがわからなくなった場合にクラスタ内のファブリック インターコネクトの権限を判別するには、両方のファブリック インターコネクトの IP アドレスから Cisco UCS Manager GUI を開きます。従属ファブリック インターコネクトは失敗し、次のメッセージが表示されます。

```
UCSM GUI is not available on secondary node.
```

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] を展開します。

ステップ 3 ロールを識別するファブリック インターコネクトをクリックします。

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

ステップ 5 [General] タブで、[High Availability Details] バーの下矢印をクリックしてこの領域を展開します。

ステップ 6 [Leadership] フィールドを表示して、このファブリック インターコネクトがプライマリ ファブリック インターコネクトか、従属ファブリック インターコネクトかを決定します。

ファブリック インターコネクトのファームウェア バージョンの確認

次の手順を使用して、Cisco UCS ドメイン のすべてのファブリック インターコネクトのファームウェア バージョンを確認できます。ファブリック インターコネクトの [Installed Firmware] タブを使用すると、単一のファブリック インターコネクトのファームウェアを確認できます。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブで [Equipment] ノードをクリックします。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Installed Firmware] タブで、次に示す各ファブリック インターコネクトのファームウェア バージョンが、アップデートしたファームウェアのバージョンと一致していることを確認します。

- カーネル バージョン
- システム バージョン

6200 および 6300 FI シリーズのスタンドアロン構成での admin アカウント パスワードの復旧

この手順により、ファブリック インターコネクトで初期システム セットアップの実行時に admin アカウントに設定したパスワードを復旧できます。admin アカウントは、システム アドミニストレータまたはスーパーユーザのアカウントです。

始める前に

1. ファブリック インターコネクトのコンソール ポートを、コンピュータ ターミナルまたはコンソール サーバに物理的に接続します。
2. 次のファームウェアの実行中のバージョンを確認します。
   - ファブリック インターコネクトのファームウェア カーネル バージョン
   - ファームウェア システム バージョン

ヒント　この情報を検索するには、Cisco UCS ドメインに設定されている任意のユーザ アカウントを使用してログインします。

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 インターコネクトの電源を次のように再投入します。

a) Cisco UCS Mini の場合、ファブリック インターコネクトをシャーシ スロットから引き抜きます。それ以外の構成の場合は、ファブリック インターコネクトの電源をオフにします。

b) Cisco UCS Mini の場合、ファブリック インターコネクトをシャーシ スロット内に戻します。それ以外の構成の場合は、ファブリック インターコネクトの電源をオンにします。

ステップ 3　コンソールで次のいずれかのキーの組み合わせを押して、起動時に `loader` プロンプトを表示させます。

- **`Ctrl+l`**
- **`Ctrl+Shift+r`**

`loader` プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

ステップ 4　ファブリック インターコネクトのカーネル ファームウェア バージョンをブートします。

```
loader >
boot /installables/switch/
kernel_firmware_version
```

例：

```
loader > boot
/installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin

loader > boot
/installables/switch/ucs-mini-k9-kickstart.5.0.3.N2.3.01a.bin
```

ステップ 5　config ターミナル モードを入力します。

```
Fabric(boot)#
config terminal
```

ステップ 6 admin パスワードをリセットします。

```
Fabric(boot)(config)#
admin-password
password
```

大文字と数字がそれぞれ1つ以上含まれる強力なパスワードを選択します。このパスワードは空にできません。

新しいパスワードはクリア テキスト モードで表示されます。

ステップ 7 config ターミナル モードを終了し、ブート プロンプトに戻ります。

ステップ 8 ファブリック インターコネクトのシステム ファームウェア バージョンをブートします。

```
Fabric(boot)#
load /installables/switch/
system_firmware_version
```

例：

```
Fabric(boot)# load
/installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin
```

```
Fabric(boot)# load
/installables/switch/ucs-mini-k9-system.5.0.3.N2.3.01a.bin
```

ステップ 9 システム イメージがロードされたら、Cisco UCS Manager にログインします。

ステップ 10 Cisco UCS Manager で新しいパスワードを同期します。

```
UCS-B # scope security
UCS-B/security  # set password
Enter new password: New_password
Confirm new password: New_password
UCS-B/security* # commit-buffer
```

スタンドアロン構成の Admin アカウント パスワードの復旧 Cisco UCS 6400 シリーズ ファブリック インターコネクト

この手順により、ファブリック インターコネクトで初期システム セットアップの実行時に admin アカウントに設定したパスワードを復旧できます。admin アカウントは、システム アドミニストレータまたはスーパーユーザのアカウントです。

始める前に

1. ファブリック インターコネクトのコンソール ポートを、コンピュータ ターミナルまたはコンソール サーバに物理的に接続します。

2. 実行中の Cisco UCS 6400 シリーズ ファブリック インターコネクト イメージのバージョンを確認します。

（注） Cisco UCS 6400 シリーズ ファブリック インターコネクト 別のカーネルとシステム イメージを持っていません。1 つの統一されたイメージがあります。

ヒント この情報を検索するには、Cisco UCS ドメインに設定されている任意のユーザ アカウントを使用してログインします。

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 UCS-A(local-mgmt)# **reboot**

これにより、ファブリック インターコネクトがリブートします。

ファブリック インターコネクトの電源再投入を行うこともできます。

ステップ 3 リブートしたら、コンソールで **Ctrl+c** キーを押して loader プロンプトを表示させます。

Ctrl+c

loader プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

ステップ 4 loader プロンプトで、次のコマンドを実行します。

loader > **cmdline recoverymode=1**

ステップ 5 ファブリック インターコネクトでCisco UCS 6400 シリーズ ファブリック インターコネクトイメージをブートします。

loader > **boot /installables/switch/***Cisco UCS 6400 FI Image*

例：

loader > **boot /installables/switch/ucs-6400-k9-system.7.0.3.N2.3.40.173.gbin**

ステップ 6 config ターミナル モードを開始します。

switch(boot)# **config terminal**

ステップ 7 admin パスワードをリセットします。

switch(boot)(config)# **admin-password** *New_password*

大文字と数字がそれぞれ 1 つ以上含まれる強力なパスワードを選択します。このパスワードは空にできません。

新しいパスワードはクリア テキスト モードで表示されます。

ステップ 8 config ターミナル モードを終了して FI をリブートします。

```
switch(boot)(config)# exit
switch(boot)# exit
```

ステップ 9 ログインプロンプトが表示されるまで待ってから、新しいパスワードを使用してログインします。

```
Cisco UCS 6400 Series Fabric Interconnect
login: admin
Password:New_password
```

ステップ 10 Cisco UCS Manager で新しいパスワードを同期します。

```
UCS-A # scope security
UCS-A/security  # set password
Enter new password: New_password
Confirm new password: New_password
UCS-A/security* # commit-buffer
```

6200 および 6300 FI シリーズのクラスタ構成での Admin アカウント パスワードの復旧

この手順により、ファブリック インターコネクトで初期システム セットアップの実行時に admin アカウントに設定したパスワードを復旧できます。admin アカウントは、システム アドミニストレータまたはスーパーユーザのアカウントです。

始める前に

1. ファブリック インターコネクトのコンソール ポートのいずれか1つを、コンピュータ ターミナルまたはコンソール サーバに物理的に接続します。
2. 次の情報を入手します。
   - ファブリック インターコネクトのファームウェア カーネル バージョン
   - ファームウェア システム バージョン
   - プライマリ リーダーシップ ロールを持つファブリック インターコネクトと、従属ファブリック インターコネクト

ヒント この情報を検索するには、Cisco UCS ドメインに設定されている任意のユーザ アカウントを使用してログインします。

手順

ステップ 1 下位のファブリック インターコネクトのコンソール ポートに接続します。

ステップ 2 従属ファブリック インターコネクトの場合は、次の手順を実行します。

a) Cisco UCS Mini の場合、ファブリック インターコネクトをシャーシ スロットから引き抜きます。それ以外の構成の場合は、ファブリック インターコネクトの電源をオフにします。

b) Cisco UCS Mini の場合、ファブリック インターコネクトをシャーシ スロット内に戻します。それ以外の構成の場合は、ファブリック インターコネクトの電源をオンにします。

c) コンソールで次のいずれかのキーの組み合わせを押して、起動時に `loader` プロンプトを表示させます。

- **`Ctrl+l`**
- **`Ctrl+Shift+r`**

`loader` プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

ステップ 3 プライマリ ファブリック インターコネクトの電源を次のように再投入します。

a) Cisco UCS Mini の場合、ファブリック インターコネクトをシャーシ スロットから引き抜きます。それ以外の構成の場合は、ファブリック インターコネクトの電源をオフにします。

b) Cisco UCS Mini の場合、ファブリック インターコネクトをシャーシ スロット内に戻します。それ以外の構成の場合は、ファブリック インターコネクトの電源をオンにします。

ステップ 4 コンソールで次のいずれかのキーの組み合わせを押して、起動時に `loader` プロンプトを表示させます。

- **`Ctrl+l`**
- **`Ctrl+Shift+r`**

`loader` プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

ステップ 5 プライマリ ファブリック インターコネクトのカーネル ファームウェア バージョンをブートします。

```
loader > boot /installables/switch/
kernel_firmware_version
```

例：

```
loader > boot
/installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin

loader > boot
/installables/switch/ucs-mini-k9-kickstart.5.0.3.N2.3.01a.bin
```

ステップ 6 config ターミナル モードを入力します。

```
Fabric(boot)# config terminal
```

ステップ 7 admin パスワードをリセットします。

```
Fabric(boot)(config)# admin-password password
```

大文字と数字がそれぞれ 1 つ以上含まれる強力なパスワードを選択します。このパスワードは空にできません。

新しいパスワードはクリア テキスト モードで表示されます。

ステップ 8 config ターミナル モードを終了し、ブート プロンプトに戻ります。

ステップ 9 プライマリ ファブリック インターコネクトのシステム ファームウェア バージョンをブートします。

```
Fabric(boot)# load /installables/switch/
system_firmware_version
```

例：

```
Fabric(boot)# load
/installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin

Fabric(boot)# load
/installables/switch/ucs-mini-k9-system.5.0.3.N2.3.01a.bin
```

ステップ 10 システム イメージがロードされたら、Cisco UCS Manager にログインします。

ステップ 11 従属ファブリック インターコネクトのコンソールで、次の手順を実行してシステムを起動します。

a) 従属ファブリック インターコネクトのカーネル ファームウェア バージョンをブートします。

```
loader > boot /installables/switch/
kernel_firmware_version
```

b) 従属ファブリック インターコネクトのシステム ファームウェア バージョンをブートします。

```
Fabric(boot)# load /installables/switch/
system_firmware_version
```

ステップ 12 Cisco UCS Manager と他の FI で新しいパスワードを同期します。

```
UCS-B # scope security
UCS-B/security  # set password
Enter new password: New_password
Confirm new password: New_password
UCS-B/security* # commit-buffer
```

クラスタ構成での Admin アカウント パスワードの復旧 Cisco UCS 6400 シリーズ ファブリック インターコネクト

この手順により、ファブリック インターコネクトで初期システム セットアップの実行時に admin アカウントに設定したパスワードを復旧できます。admin アカウントは、システム アドミニストレータまたはスーパーユーザのアカウントです。

始める前に

1. ファブリック インターコネクトのコンソール ポートのいずれか1つを、コンピュータ ターミナルまたはコンソール サーバに物理的に接続します。
2. 次の情報を入手します。
   - Cisco UCS 6400 シリーズ ファブリック インターコネクト のイメージ

     （注） Cisco UCS 6400 シリーズ ファブリック インターコネクト 別のカーネルとシステム イメージを持っていません。1 つの統一されたイメージがあります。

   - プライマリ リーダーシップ ロールを持つファブリック インターコネクトと、従属ファブリック インターコネクト

ヒント この情報を検索するには、Cisco UCS ドメインに設定されている任意のユーザ アカウントを使用してログインします。

手順

ステップ 1 下位のファブリック インターコネクトのコンソール ポートに接続します。

ステップ 2 UCS-B(local-mgmt) # **reboot**

これにより、従属ファブリック インターコネクトがリブートします。

従属ファブリック インターコネクトの電源再投入を行うこともできます。

ステップ 3 リブートしたら、コンソールで **Ctrl+c** キーを押して `loader` プロンプトを表示させます。

Ctrl+c

`loader` プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

ステップ 4 loader プロンプトで、次のコマンドを実行します。

```
loader > cmdline recoverymode=1
```

ステップ 5 ファブリック インターコネクトでCisco UCS 6400 シリーズ ファブリック インターコネクトイメージをブートします。

```
loader > boot /installables/switch/Cisco UCS 6400 Series FI Image
```

例：

```
loader > boot
/installables/switch/ucs-6400-k9-system.7.0.3.N2.3.40.173.gbin
```

ステップ 6 config ターミナル モードを開始します。

```
switch(boot)# config terminal
```

ステップ 7 admin パスワードをリセットします。

```
switch(boot)(config)# admin-password New_password
```

大文字と数字がそれぞれ1つ以上含まれる強力なパスワードを選択します。このパスワードは空にできません。

新しいパスワードはクリア テキスト モードで表示されます。

ステップ 8 config ターミナル モードを終了して FI をリブートします。

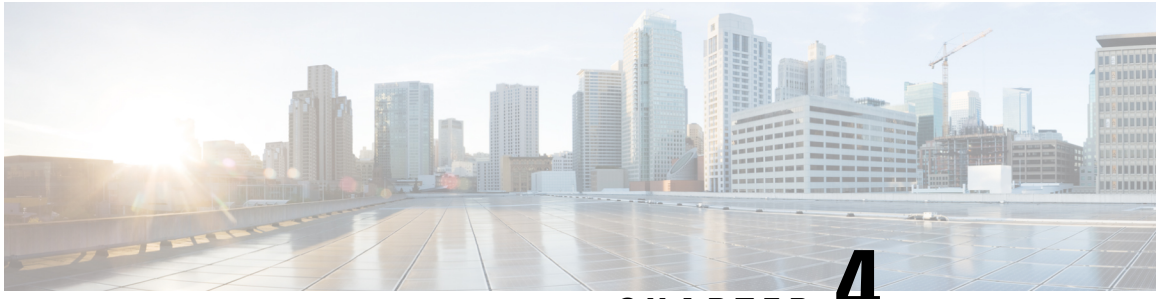
```
switch(boot)(config)# exit
switch(boot)# exit
```

ステップ 9 ログインプロンプトが表示されるまで待ってから、新しいパスワードを使用してログインします。

```
Cisco UCS 6400 Series Fabric Interconnect
login: admin
Password:New_password
```

ステップ 10 Cisco UCS Manager と他の FI で新しいパスワードを同期します。

```
UCS-B # scope security
UCS-B/security  # set password
Enter new password: New_password
Confirm new password: New_password
UCS-B/security* # commit-buffer
```



CHAPTER 4

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。

Note 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。

Note 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。

Note 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。

Tip 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

Table 4: 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
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

権限	説明	デフォルトのロール割り当て
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
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

権限	説明	デフォルトのロール割り当て
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
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

Procedure

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]**の順に展開します。

ステップ 3 [User Services] を右クリックし、[Create Role] を選択します。

また、[Roles] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 4 [Create Role] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	このユーザ ロールのユーザ定義名。 この名前には、1～16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Privileges] リスト ボックス	システムに定義されている権限のリスト。 その権限の説明を表示するには、権限をクリックします。チェックボックスをオンにすると、選択したユーザにその権限が割り当てられます。
[Help] セクション	
[Description] フィールド	[Privileges] リスト ボックス内で最後にクリックした権限の説明。

ステップ 5 [OK] をクリックします。

ユーザ ロールへの権限の追加

Procedure

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]**の順に展開します。

ステップ 3 [Roles] ノードを展開します。

ステップ 4 権限を追加するロールを選択します。

ステップ 5 [General] タブで、ロールに追加する権限に対応するチェックボックスをオンにします。

ステップ 6 [Save Changes] をクリックします。

ユーザ ロールからの権限の削除

Procedure

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]**の順に展開します。

ステップ 3 [Roles] ノードを展開します。

ステップ 4 権限を削除するロールを選択します。

ステップ 5 [General] タブで、ロールから削除する権限に対応するボックスをオフにします。

ステップ 6 [Save Changes] をクリックします。

ユーザ ロールの削除

あるユーザー ロールを削除すると、Cisco UCS Managerにより、このロールは割り当て先のすべてのユーザー アカウントから削除されます。

Procedure

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]の順に展開します。**

ステップ 3 [Roles] ノードを展開します。

ステップ 4 削除するロールを右クリックし、[Delete] を選択します。

ステップ 5 [Delete] ダイアログボックスで、[Yes] をクリックします。

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。

Note 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。

ロケールへの組織の割り当て

手順

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]の順に展開します。**

ステップ 3 [Locales] ノードを展開し、組織を追加するロケールをクリックします。

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

ステップ 5 [Organizations] 領域のテーブル アイコン バーで [+] をクリックします。

ステップ 6 [Assign Organizations] ダイアログボックスで、次の手順を実行します。

a) **[Organizations]**領域を展開して、 Cisco UCS ドメイン内の組織を表示します。
b) [root] ノードを展開して、サブ組織を表示します。
c) ロケールを割り当てる組織をクリックします。
d) [Organizations] 領域の組織を右側のペインの設計領域にドラッグ アンド ドロップします。
e) すべての適切な組織をロケールに割り当てるまで、ステップ b および c を繰り返します。

ステップ 7 [OK] をクリックします。

ロケールの作成

始める前に

ロケールを作成するには、1 つ以上の組織が存在する必要があります。

手順

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]の順に展開します。**

ステップ 3 [Locales] を右クリックし、[Create a Locale] を選択します。

ステップ 4 [Create Locale] ページで、次の手順を実行します。

a) [Name] フィールドに、ロケールの一意の名前を入力します。

この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。

b) [Next] をクリックします。

ステップ 5 [Assign Organizations] ダイアログボックスで、次の手順を実行します。

a) **[Organizations]**領域を展開して、 Cisco UCS ドメイン内の組織を表示します。

b) [root] ノードを展開して、サブ組織を表示します。

c) ロケールを割り当てる組織をクリックします。

d) [Organizations] 領域の組織を右側のペインの設計領域にドラッグ アンド ドロップします。

e) すべての適切な組織をロケールに割り当てるまで、ステップ b および c を繰り返します。

ステップ 6 [Finish] をクリックします。

次のタスク

ロケールを 1 つまたは複数のユーザ アカウントに追加します。詳細については、ローカル認証されたユーザ アカウントに割り当てられたロケールの変更 （40 ページ）を参照してください。

ロケールからの組織の削除

手順

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]の順に展開します。**

ステップ 3 [Locales] ノードを展開し、組織を削除するロケールをクリックします。

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

ステップ 5 [Organizations] 領域で、ロケールから削除する組織を右クリックし、[Delete] を選択します。

ステップ 6 [Save Changes] をクリックします。

ロケールの削除

手順

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]**の順に展開します。

ステップ 3 [Locales] ノードを展開します。

ステップ 4 削除するロケールを右クリックし、[Delete] を選択します。

ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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

Note ユーザ アカウントの作成後、Cisco UCS Manager GUIからユーザ アカウントのフィールドのいずれかを変更する場合は、パスワードをもう一度入力する必要があります。

Before you begin

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。

Procedure

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]の順に展開します。**

ステップ 3 [User Services] を右クリックし、[Create User] を選択して [User Properties] ダイアログボックスを開きます。

[Locally Authenticated Users] の右クリックでもそのオプションにアクセスできます。

ステップ 4 ユーザに関して要求される情報を使用して、次のフィールドに値を入力します。

名前	説明

[Login ID] フィールド	このアカウントにログインするときに使用されるアカウント名。このアカウントは固有である必要があり、しかも Cisco UCS Manager ユーザ アカウントに関する次のガイドラインと制約事項を満たしている必要があります。
	• 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。
	ユーザを保存した後は、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。

名前	説明
[First Name] フィールド	ユーザの名。このフィールドには、32 文字までの値を入力できます。
[Last Name] フィールド	ユーザの姓。このフィールドには、32 文字までの値を入力できます。
[Email] フィールド	ユーザの電子メール アドレス。
[Phone] フィールド	ユーザの電話番号。

[Password] フィールド	このアカウントに関連付けられているパスワード。パスワード強度チェックが有効にされている場合は、ユーザ パスワードを強固なものにする必要があります。Cisco UCS Manager は次の要件を満たしていないパスワードを拒否します。
	• 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。
	Note 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。

[Confirm Password] フィールド	確認のためのパスワードの再入力。

名前	説明
[Account Status] フィールド	ステータスが **[Active]**に設定されている場合、ユーザはこのログイン ID とパスワードを使用して Cisco UCS Manager にログインできます。
[Account Expires] チェックボックス	オンにすると、このアカウントは期限切れになり、[Expiration Date] フィールドに指定した日付以降に使用できなくなります。 **Note** 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。
[Expiration Date] フィールド	アカウントが期限切れになる日付。日付の形式は yyyy-mm-dd です。 このフィールドの終端にある下矢印をクリックするとカレンダーが表示されるので、それを使用して期限日を選択できます。 **Note** **[Account Expires]** チェックボックスをオンにすると、Cisco UCS Manager GUI が表示されます。

ステップ 5 [Roles] 領域で 1 つ以上のボックスをオンにして、ユーザ アカウントにロールと権限を割り当てます。

Note 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。

ステップ 6 (Optional) システムに組織が含まれる場合、[Locales] 領域の 1 つ以上のチェックボックスをオンにして、適切なロケールをユーザに割り当てます。

ステップ 7 [SSH] 領域で、次のフィールドに値を入力します。

a) [Type] フィールドで、次をクリックします。

- [Password Required]：ユーザはログインするときにパスワードを入力する必要があります。
- [Key]：このユーザがログインするときに、SSH 暗号化が使用されます。

b) [Key] を選択する場合、[SSH data] フィールドに SSH キーを入力します。

ステップ 8 [OK] をクリックします。

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

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]**の順に展開します。

ステップ 3 [Locally Authenticated Users] ノードをクリックします。

ステップ 4 [Work] ペインで、[Properties] 領域の [Password Strength Check] チェックボックスをオンにします。

ステップ 5 [Save Changes] をクリックします。

Web セッション制限の設定

手順

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

ステップ 2 **[All]** > **[Communication Management]** > **[Communication Services]** の順に展開します。

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

ステップ 4 [Web Session Limits] 領域で、次のフィールドに入力します。

（注） HTML-5 インターフェイスではブラウザごとにユーザ セッションを 1 つサポートします。

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。

名前	説明
[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 [Save Changes] をクリックします。

ローカル認証されたユーザアカウントに割り当てられたロケールの変更

（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

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

ステップ 2 [Admin] タブの **[All]** > **[User Management]** > **[User Services]** > **[Locally Authenticated Users]** を展開します。

ステップ 3 修正するユーザ アカウントをクリックします。

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

ステップ 5 [Locales] 領域で、次の手順を実行します。

- ユーザアカウントに新しいロケールを割り当てるには、適切なチェックボックスをオンにします。
- ユーザ アカウントからロケールを削除するには、適切なチェックボックスをオフにします。

ステップ 6 [Save Changes] をクリックします。

ローカル認証されたユーザアカウントに割り当てられたロールの変更

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 アカウントへの新しいロールの割り当てや既存のロールの削除を行うときにユーザがログインしている場合、アクティブなセッションは以前のロールや権限を引き続き使用します。

手順

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

ステップ 2 [Admin] タブの **[All]** > **[User Management]** > **[User Services]** > **[Locally Authenticated Users]** を展開します。

ステップ 3 修正するユーザ アカウントをクリックします。

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

ステップ 5 [Roles] 領域で、次の手順を実行します。

- ユーザアカウントに新しいロールを割り当てるには、適切なチェックボックスをオンにします。
- ユーザアカウントからロールを削除するには、適切なチェックボックスをオフにします。

ステップ 6 [Save Changes] をクリックします。

ユーザ アカウントの有効化

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

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

ステップ 2 **[All]** > **[User Management]** > **[User Services]** > **[Locally Authenticated Users]の順に展開します。**

ステップ 3 有効にするユーザをクリックします。

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

ステップ 5 [Account Status] フィールドで、[active] オプション ボタンをクリックします。

ステップ 6 [Save Changes] をクリックします。

ユーザ アカウントの無効化

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。

（注） Cisco UCS Manager GUI を介して無効化されたアカウントのパスワードを変更した場合、アカウントを有効化してアクティブ化した後、ユーザはこの変更されたパスワードを使用できません。アカウントを有効化してアクティブ化した後に、必要なパスワードを再び入力する必要があります。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[User Services]** > **[Locally Authenticated Users]**の順に展開します。
ステップ 3 無効にするユーザをクリックします。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Account Status] フィールドで、[inactive] オプション ボタンをクリックします。

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。

ステップ 6 [Save Changes] をクリックします。

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

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[User Services]** > **[Locally Authenticated Users]**の順に展開します。
ステップ 3 パスワード履歴をクリアするユーザをクリックします。
ステップ 4 [Actions] 領域で、[Clear Password History] をクリックします。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ローカルに認証されたユーザ アカウントの削除

Procedure

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[User Services]**の順に展開します。
ステップ 3 [Locally Authenticated Users] ノードを展開します。

ステップ 4 削除するユーザ アカウントを右クリックし、[Delete] を選択します。

ステップ 5 [Delete] ダイアログボックスで、[Yes] をクリックします。

ログイン プロファイル

ログイン プロファイルでは、ログインの試行が失敗した後、特定の期間、Cisco UCS Manager へのログイン要求をブロックする機能を提供します。

この機能は現在、Cisco UCS 6400 シリーズ ファブリック インターコネクト および Cisco UCS Manager リリース 4.0 (1) 以降のリリースでのみサポートされています。

ログイン プロファイルの設定

手順

ステップ 1 [Navigation (ナビゲーション)] ペインで **[Admin (管理)]** をクリックします。

ステップ 2 **[All (すべて)]** > **[User Management (ユーザー管理)]** > **[User Services (ユーザー サービス)]** > **[Login Profile (ログイン プロファイル)]** の順に展開します。

ステップ 3 [Work (作業)] ペインで、**[Admin State (管理状態)]** フィールドの **[Enable (有効化)]** オプション ボタンをクリックして、ログイン試行が失敗した後、特定の期間中 Cisco UCS Manager に対するログイン要求をブロックできるようにします。

この機能を有効にすると、ログイン試行の失敗が *z* 秒で *y* 回発生した場合に、Cisco UCS Manager へのログイン要求が *x* 秒間ブロックされます。ここで、各変数は次のように定義されます。

- *x* は、**[Block Login (ブロックログイン)]** フィールドで指定します。
- *y* は、**[Failed Attempts (失敗試行回数)]** フィールドで指定します。
- *z*は、**[Attempted Within (試行中)]** フィールドで指定されます。

ステップ 4 **[Block Login (ログインのブロック)]** フィー[ルドで、指定した回数ログイン試行が失敗した後に、Cisco UCS Manager へのログイン要求がブロックされる秒数を指定します。

ログイン要求がブロックされるデフォルトの秒数は 60 秒です。

ステップ 5 **[Failed attempts (失敗した試行回数)]** フィールドで、Cisco UCS Manager へのログイン要求がブロックされるまでの試行失敗回数を指定します。

指定した期間内で、ログイン要求がブロックされるデフォルトの試行回数は5です。

ステップ 6 **[Attempted Within (試行中)]** フィールドで、特定の回数を失敗した際に、Cisco UCS Manager へのログイン要求をブロックする秒数を指定します。

ログインに失敗するデフォルト秒数は、30秒です。

ユーザ セッションのモニタリング

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] を展開します。

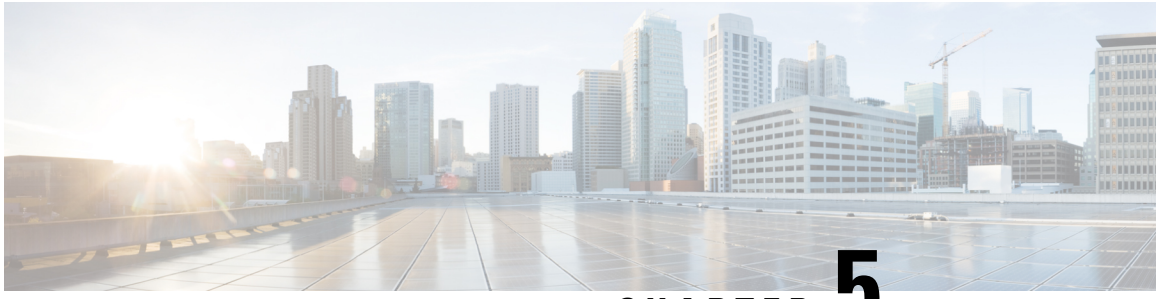
ステップ 3 [User Services] ノードをクリックします。

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

このタブには、ユーザ セッションに関する次の詳細情報が表示されます。

名前	説明
[Name] カラム	セッションの名前。
[User] カラム	セッションに参加しているユーザ名。
[Fabric ID] カラム	このセッションのためにユーザがログインしているファブリック インターコネクト。
[Login Time] カラム	セッションが開始された日時。
[Refresh Period] カラム	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。
[Session Timeout] カラム	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。
[Terminal Type] カラム	ユーザがログインするときに使用する端末の種類。
[Host] カラム	ユーザのログイン元である IP アドレス。

名前	説明
[Current Session] カラム	このカラムに [Y] が表示された場合は、関連するユーザ セッションが現在アクティブです。



CHAPTER 5

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 *5:* 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+ プロバイダーの属性 ID を提供する文字列です。 次の構文例は、cisco-av-pair 属性を作成するときに複数のユーザ ロールとロケールを指定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ー接続のデフォルト設定です。個々のプロバイダー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。

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。

手順

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

ステップ 2 **[All]** > **[User Management]** > **[LDAP] の順に展開します。**

ステップ 3 [Properties] 領域で、すべてのフィールドに入力します。

（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。

ステップ 4 [Save Changes] をクリックします。

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 プロバイダーをサポートします。

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 つめのファブリック インターコネクトで障害が発生し、システムが 2 つめのファブリック 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 プロバイダーを変更したり、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、プロバイダーに変更を加えた後、ドメイン認証レルムを LDAP に戻します。

注目 特殊文字が含まれる LDAP リモート ユーザ名では、バージョン 2.2(3a) 以降を実行しているシステムにログインできません。ユーザがログインできない理由は、Nexus OS では特殊文字 !、%、^ をユーザ名に対してサポートしていないという制限があるためです。

手順

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

ステップ 2 **[All]** > **[User Management]** > **[LDAP]** の順に展開します。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Actions] エリアで、[Create LDAP Provider] をクリックします。

ステップ 5 ウィザードの [Create LDAP Provider] ページで、すべてのフィールドに適切な LDAP サービス情報を入力します。

a) 使用する LDAP サービスに関する情報を使用して、次のフィールドに値を入力します。

名前	説明
[Hostname/FDQN (or IP Address)] フィールド	LDAP プロバイダが存在するホスト名または IP アドレス（IPv4 または IPv6）。SSL が有効の場合、このフィールドは、LDAP データベースのセキュリティ証明書内の通常名（CN）と正確に一致している必要があります。 （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、または DNS 管理が**ローカル**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 [グローバル（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。
[Order] フィールド	Cisco UCS でユーザーの認証にこのプロバイダーを使用する順序。 1 ～ 16 の範囲の整数を入力します。または、このCisco UCS ドメインで定義されている他のプロバイダーに基づいて、次に使用できる順序をCisco UCSで自動的に割り当てる場合には、**[lowest-available]** または **[0]**（ゼロ）を入力します。
[Bind DN] フィールド	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。
[Base DN] フィールド	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。 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。

名前	説明
[Port] フィールド	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。
[Enable SSL] チェックボックス	このチェックボックスをオンにすると、LDAP データベースとの通信に暗号化が必要になります。このチェックボックスをオフにすると、認証情報はクリアテキストで送信されます。 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。 オンにした場合、ポートを 636 に変更せずに、389 のままにしてください。Cisco UCS は SSL 用のポート 636 で TLS セッションのネゴシエーションを行いますが、最初の接続は暗号化されずに 389 で開始されます。
[Filter] フィールド	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。
[Attribute] フィールド	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。
[Password] フィールド	[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。
[Confirm Password] フィールド	確認のための LDAP データベース パスワードの再入力。

名前	説明
[Timeout] フィールド	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。
[Vendor] オプション ボタン	ユーザが使用する LDAP ベンダー。次のいずれかになります。 • [Open Ldap]：LDAP プロトコルのオープン ソース実装。 • [MS AD]：Microsoft Active Directory。

b) [Next] をクリックします。

ステップ 6 ウィザードの [LDAP Group Rule] ページで、すべてのフィールドに適切な LDAP グループ ルール情報を入力します。

（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。

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、LDAP プロバイダー 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

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

ステップ 2 **[All]** > **[User Management]** > **[LDAP]** の順に展開します。

ステップ 3 [LDAP Providers] を展開し、グループ ルールを変更する LDAP プロバイダーを選択します。

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

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

名前	説明
[Group Authorization] フィールド	リモートユーザを認証し、ユーザロールとロケールを割り当てる際に、Cisco UCS が LDAP グループも検索するかどうか。次のいずれかになります。 • [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 内でマッピングされたすべての LDAP 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。 （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。
[Group Recursion] フィールド	マッピングされたグループとその親グループの両方を Cisco UCS が検索するかどうか。次のいずれかになります。 • [Non Recursive]：Cisco UCS はこの Cisco UCS ドメイン でマッピングされたグループだけを検索します。どのグループにもユーザの認証プロパティを明示的に設定するユーザが含まれない場合、Cisco UCS はデフォルト設定を使用します。 • [Recursive]：Cisco UCS はマッピングされた各グループとその親グループでユーザの認証プロパティを検索します。これらのプロパティは累積的です。したがって、Cisco UCS は明示的な認証プロパティ設定を検出した各グループについて、それらの設定を現在のユーザに適用します。それ以外の場合は、デフォルト設定が使用されます。
[Target Attribute] フィールド	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。

名前	説明
[Use Primary Group] フィールド	メンバーシップの確認のための LDAP グループ マップとしてプライマリ グループを設定できるかどうかを判断するために、Cisco UCS で使用される属性。このオプションを使用すると、Cisco UCS Manager は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できます。

ステップ 6 [Save Changes] をクリックします。

LDAP プロバイダの削除

Procedure

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

ステップ 2 **[All]** > **[User Management]** > **[LDAP] の順に展開します。**

ステップ 3 [LDAP Providers] を展開します。

ステップ 4 削除する LDAP プロバイダーを右クリックし、[Delete] を選択します。

ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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

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

ステップ 2 **[All]** > **[User Management]** > **[LDAP]** の順に展開します。

ステップ 3 [LDAP Group Maps] を右クリックし、[Create LDAP Group Map] を選択します。

ステップ 4 [Create LDAP Group Map] ダイアログボックスで、必要に応じてすべての LDAP グループ マップ情報を指定します。

重要 **[LDAP Group DN] フィールド** で指定する名前は、LDAP データベース内の名前と一致する必要があります。

（注） [LDAP Group DN] フィールドに特殊文字を使用する場合は、特殊文字の前にエスケープ文字 \（シングル バックスラッシュ）を付ける必要があります。

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

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

ステップ 2 **[All]** > **[User Management]** > **[LDAP]** の順に展開します。

ステップ 3 [LDAP Group Maps] を展開します。

ステップ 4 削除する LDAP グループ マップを右クリックし、[Delete] を選択します。

ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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ー接続のデフォルト設定です。個々のプロバイダー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。

（注） RADIUS 認証では、Password Authentication Protocol（PAP）を使用します。

手順

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

ステップ 2 **[User Management]** > **[RADIUS]** の順に選択します。

ステップ 3 [Properties] 領域で、すべてのフィールドに入力します。

ステップ 4 [Save Changes] をクリックします。

次のタスク

RADIUS プロバイダーを作成します。

RADIUS プロバイダの作成

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

Before you begin

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 つめのファブリック インターコネクトで障害が発生し、システムが 2 つめのファブリック 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。

Procedure

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

ステップ 2 **[All]** > **[User Management]** > **[RADIUS]の順に展開します。**

ステップ 3 [Create RADIUS Provider] ダイアログボックスで、該当するすべての RADIUS サービス情報を指定します。

Note IPv4 または IPv6 のアドレスの代わりにホスト名を使用する場合、DNS サーバにはホスト名が必ず設定されているようにする必要があります。

ステップ 4 [Save Changes] をクリックします。

What to do next

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、RADIUS プロバイダー グループを設定します。

RADIUS プロバイダの削除

Procedure

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

ステップ 2 **[User Management]** > **[RADIUS]** の順に選択します。

ステップ 3 削除する RADIUS プロバイダーを右クリックし、[Delete] を選択します。

ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

TACACS+ プロバイダ

TACACS+ プロバイダのプロパティの設定

（注） 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ー接続のデフォルト設定です。個々のプロバイダー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

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

ステップ 2 **[User Management]** > **[TACACS+]** の順に選択します。

ステップ 3 [Properties] 領域で、**[Timeout]** フィールド に値を入力します。

ステップ 4 [Save Changes] をクリックします。

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+ プロバイダーをサポートします。

Before you begin

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+ プロバイダーの属性 ID を提供する文字列です。

  次の構文例は、cisco-av-pair 属性を作成するときに複数のユーザ ロールとロケールを指定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 つめのファブリック インターコネクトで障害が発生し、システムが 2 つめのファブリック 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。

Procedure

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

ステップ 2 **[All]** > **[User Management]** > **[TACACS+]の順に展開します。**

ステップ 3 [General] タブの [Actions] 領域で、[Create TACACS+ Provider] をクリックします。

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

a) 必要に応じてすべてのフィールドに TACACS+ サービス情報を入力します。

Note IPv4 または IPv6 のアドレスの代わりにホスト名を使用する場合、DNS サーバにはホスト名が必ず設定されているようにする必要があります。

b) [OK] をクリックします。

ステップ 5 [Save Changes] をクリックします。

What to do next

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、TACACS+ プロバイダー グループを設定します。

TACACS+ プロバイダの削除

Procedure

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

ステップ 2 **[User Management]** > **[TACACS+]** の順に選択します。

ステップ 3 削除する TACACS+ プロバイダーを右クリックし、[Delete] を選択します。

ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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

Before you begin

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ーを作成します。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。

Procedure

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

ステップ 2 **[All]** > **[User Management]** > **[Authentication]の順に展開します。**

ステップ 3 [Native Authentication] をクリックします。

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

ステップ 5 [Console Authentication] 領域で、次のフィールドに入力します。

名前	説明
[Realm] フィールド	コンソールにログインするユーザが認証される方法。次のいずれかになります。 • [Local]：ユーザ アカウントをこの Cisco UCS ドメイン 内でローカルに定義する必要があります。 • [Radius]：この Cisco UCS ドメイン に対して指定された Radius サーバでユーザを定義する必要があります。 • [Tacacs]：この Cisco UCS ドメイン に対して指定された Tacacs サーバでユーザを定義する必要があります。 • [Ldap]：この Cisco UCS ドメイン に対して指定された LDAP サーバでユーザを定義する必要があります。 • **[None]**：ユーザ アカウントがこの Cisco UCS ドメインにローカルである場合、ユーザがコンソールにログインするときにパスワードは必要ありません。
[Provider Group]	ユーザがコンソールにログインするときに認証に使用するプロバイダー グループ。 **Note** **[Provider Group]** は、ユーザを認証する方法として [Ldap]、[Radius]、または [Tacacs] を選択した場合に表示されます。
Two Factor Authentication	二要素認証は、[Realm] が [Radius] または [Tacacs] に設定されている場合にのみ使用できます。このチェックボックスをオンにすると、コンソールは、アカウントが RADIUS または TACACS サーバによって認証されるユーザにトークンとパスワードを入力してログインするように求めます。

ステップ 6 [Save Changes] をクリックします。

デフォルト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ーを作成します。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

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

ステップ 2 **[All]** > **[User Management]** > **[Authentication]の順に展開します。**

ステップ 3 [Native Authentication] をクリックします。

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

ステップ 5 [Default Authentication] 領域で、次のフィールドに入力します。

名前	説明
[Realm] ドロップダウン リストt	リモート ログイン中にユーザが認証されるデフォルトの方法。次のいずれかになります。 • [Local]：ユーザ アカウントをこの Cisco UCS ドメイン 内でローカルに定義する必要があります。 • **[Radius]**：この Cisco UCS ドメイン に関して指定された Radius サーバでユーザ アカウントを定義する必要があります。 • **[Tacacs]**—この Cisco UCS ドメインに関して指定された TACACS サーバでユーザ アカウントを定義する必要があります。 • **[Ldap]**—この Cisco UCS ドメイン に関して指定された LDAP サーバでユーザ アカウントを定義する必要があります。 • **[None]**—ユーザ アカウントがこの Cisco UCS ドメイン にローカルである場合、ユーザがリモートでログインするときにパスワードは必要ありません。
[Provider Group]	リモート ログイン中にユーザを認証するために使用するデフォルト プロバイダー グループ。 （注） [Provider Group] ドロップダウンは、ユーザを認証する方法として [Ldap]、[Radius]、または [Tacacs] を選択した場合に表示されます。

名前	説明
Web Session Refresh Period (sec)	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。
Web Session Timeout (sec)	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。
[Two Factor Authentication] チェックボックス	二要素認証は、[Realm] が [Radius] または [Tacacs] に設定されている場合にのみ使用できます。このチェックボックスを選択すると、Cisco UCS Manager と KVM Launch Manager では、アカウントが RADIUS または TACACS サーバによって認証されるユーザにトークンとパスワードを入力してログインするよう求めます。[Web セッションの更新期間（Web Session Refresh Period）] が期限切れになるまでに 60 秒ある場合は、新しいトークンを生成し、そのトークンとパスワードを入力してセッションを続行する必要があります。 （注） 二要素要素認証を有効にして、デフォルト設定を保存すると、デフォルトの **Web Session Refresh Period (sec)**が 7200 に、デフォルトの **Web Session Timeout (sec)** が 8000 に変更されます。

ステップ 6 [Save Changes] をクリックします。

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

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

ステップ 2 **[All]** > **[User Management]** > **[Authentication]の順に展開します。**

ステップ 3 [Native Authentication] をクリックします。

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

ステップ 5 **[Role Policy for Remote Users]** フィールド では、ユーザがログインを試行した際に、リモート認証プロバイダーが認証情報を伴うユーザ ロールを提供しない場合にどのように処理するかを決定するために、次のオプション ボタンのいずれかをクリックします。

- [No Login]：ユーザ名とパスワードが正しい場合でも、ユーザはシステムにログインできません。
- [Assign Default Role]：ユーザは、読み取り専用ユーザ ロールでログインできます。

ステップ 6 [Save Changes] をクリックします。

マルチ認証サービスの設定

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

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 プロバイダー 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 プロバイダーを作成します。

手順

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

ステップ 2 **[All]** > **[User Management]** > **[LDAP] の順に展開します。**

ステップ 3 [LDAP Provider Groups] を右クリックし、[Create LDAP Provider Group] を選択します。

（注） IPv4 または IPv6 のアドレスの代わりにホスト名を使用する場合、DNS サーバにはホスト名が必ず設定されているようにする必要があります。

ステップ 4 [Create LDAP Provider Group] ダイアログボックスで、適切なすべての LDAP プロバイダー グループ情報を指定します。

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ー グループを削除します。

手順

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

ステップ 2 **[All]** > **[User Management]** > **[LDAP] の順に展開します。**

ステップ 3 [LDAP Provider Groups] を展開します。

ステップ 4 削除する LDAP プロバイダー グループを右クリックし、[Delete] を選択します。

ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

RADIUS プロバイダ グループの作成

RADIUS プロバイダー 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 プロバイダーを作成します。

手順

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

ステップ 2 **[All]** > **[User Management]** > **[RADIUS]の順に展開します。**

ステップ 3 [RADIUS Provider Groups] を右クリックし、[Create RADIUS Provider Group] を選択します。

ステップ 4 [Create RADIUS Provider Group] ダイアログボックスで、次を実行します。

a) [Name] フィールドに、グループの一意の名前を入力します。

この名前には、1 ～ 127 の ASCII 文字を使用できます。

b) **[RADIUS プロバイダー]** テーブル で、グループに含める 1 つ以上のプロバイダーを選択します。

c) **[>>]** ボタン をクリックして、[Included Providers] テーブル にプロバイダーを追加します。

[<<] ボタン を使用して、グループからプロバイダーを排除できます。

d) （任意）RADIUS プロバイダーがプロバイダーを認証する順序を変更するには、[Included Providers] リストの [Move Up] または [Move Down] の矢印を使用します。
e) 必要なすべてのプロバイダーをプロバイダー グループに追加した後、[OK] をクリックします。

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

別の認証設定がプロバイダー グループを使用している場合、そのプロバイダー グループを削除することはできません。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[RADIUS]の順に展開します。**
ステップ 3 [RADIUS Provider Groups] を展開します。
ステップ 4 削除する RADIUS プロバイダー グループを右クリックし、[Delete] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

TACACS+ プロバイダー グループの作成

TACACS+ プロバイダー 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

1 つ以上の TACACS+ プロバイダーを作成します。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。
ステップ 2 **[All]** > **[User Management]** > **[TACACS+]の順に展開します。**
ステップ 3 [TACACS+ Provider Groups] を右クリックし、[Create TACACS+ Provider Group] を選択します。
ステップ 4 [Create TACACS+ Provider Group] ダイアログボックスで、必要に応じてすべての TACACS+ プロバイダーのグループ情報を指定します。

TACACS+ プロバイダー グループの削除

別の認証設定がプロバイダー グループを使用している場合、そのプロバイダー グループを削除することはできません。

手順

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

ステップ 2 **[All]** > **[User Management]** > **[TACACS+]の順に展開します。**

ステップ 3 [TACACS+ Provider Groups] を展開します。

ステップ 4 削除する TACACS+ プロバイダー グループを右クリックし、[Delete] を選択します。

ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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

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

ステップ 2 **[All]** > **[User Management]** > **[Authentication]の順に展開します。**

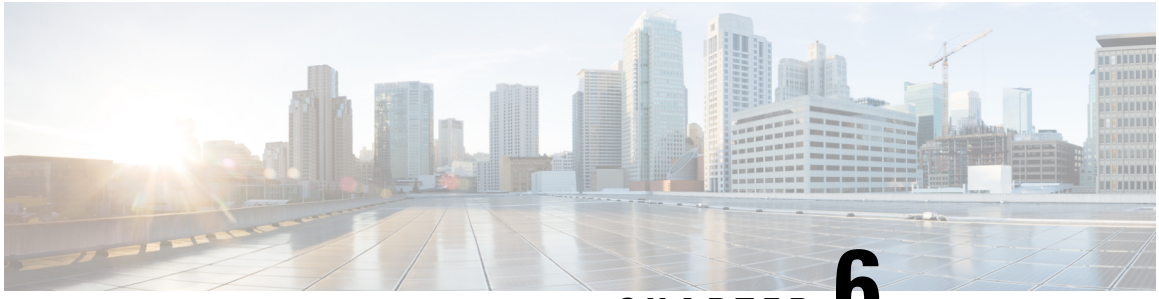
ステップ 3 [Authentication Domains] を右クリックし、[Create a Domain] を選択します。

ステップ 4 [Create a Domain] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name]	ドメインの名前。 この名前には、1～16文字の英数字を使用できます。スペースや (ハイフン)、_(アンダースコア) 以外の特殊文字は使用できません。（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。 （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。
Web Session Refresh Period (sec)	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。

名前	説明
Web Session Timeout (sec)	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。
Realm	このドメインのユーザに適用される認証プロトコル。次のいずれかになります。 • [Local]：ユーザ アカウントをこの Cisco UCS ドメイン内でローカルに定義する必要があります。 • [Radius]：この Cisco UCS ドメイン に対して指定された Radius サーバでユーザを定義する必要があります。 • [Tacacs]：この Cisco UCS ドメイン に対して指定された Tacacs サーバでユーザを定義する必要があります。 • [Ldap]：この Cisco UCS ドメイン に対して指定された LDAP サーバでユーザを定義する必要があります。
Provider Group	リモート ログイン中にユーザを認証するために使用するデフォルト プロバイダ グループ。 （注） [Provider Group] ドロップダウン リストは、ユーザを認証する方法として [Ldap]、[Radius]、または [Tacacs] を選択した場合に表示されます。
Two Factor Authentication	二要素認証は、[Realm] が [Radius] または [Tacacs] に設定されている場合にのみ使用できます。このチェックボックスを選択すると、Cisco UCS Manager と KVM Launch Manager では、アカウントが RADIUS または TACACS サーバによって認証されるユーザにトークンとパスワードを入力してログインするよう求めます。[Web セッションの更新期間（Web Session Refresh Period）] が期限切れになるまでに 60 秒ある場合は、新しいトークンを生成し、そのトークンとパスワードを入力してセッションを続行する必要があります。

ステップ 5 [OK] をクリックします。



CHAPTER 6

Call Home 機能を有効または無効にする方法

UCS の Call Home の概要

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 によって適切な CLI **show** コマンドが実行され、コマンド出力がメッセージに添付されます。

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。

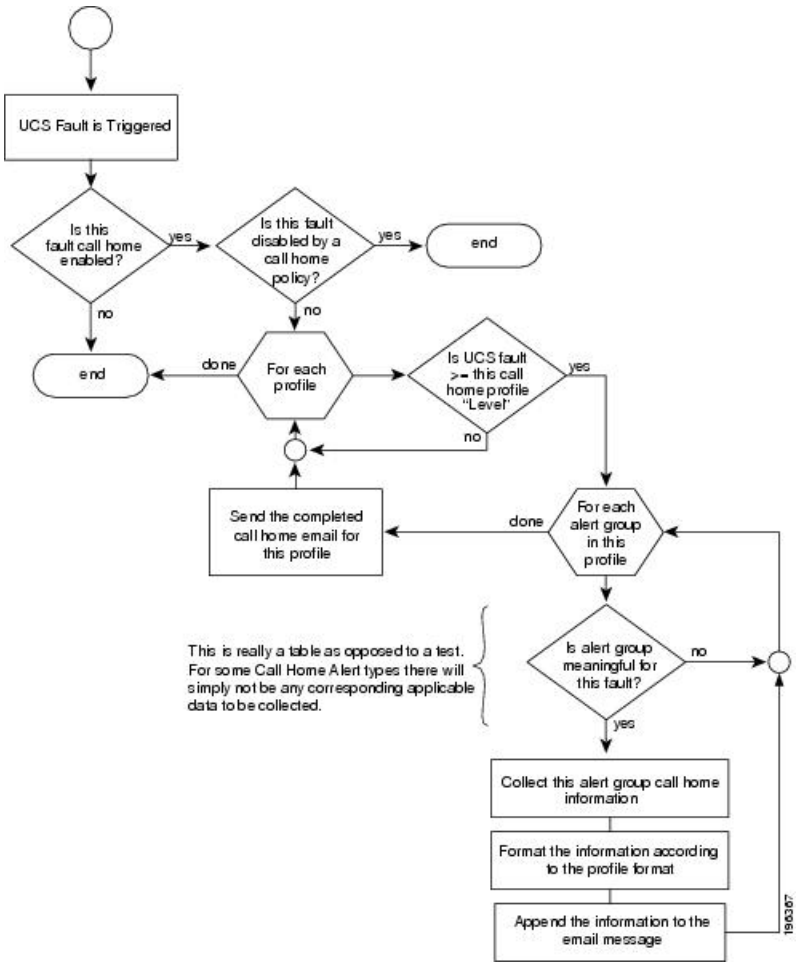
- 1 または 2 行で障害を説明する、ポケットベルや印刷レポートに適したショート テキスト フォーマット。

- 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

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

ステップ 2 **[All]** > **[Communication Management]** > **[Call Home]** の順に展開します。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Admin] 領域で、次のフィールドに入力して [Call Home] をイネーブルにします。

名前	説明
[State] フィールド	次のいずれかになります。 • **[Off]**：Call Home はこのCisco UCS ドメインには使用されません。 • **[On]**：Cisco UCSは、システムで定義された Call Home ポリシーおよびプロファイルに基づいて Call Home アラートを生成します。 （注） Cisco UCS Manager GUIでは、このフィールドを **[on]** に設定すると、このタブに残りのフィールドが表示されます。
[Switch Priority] ドロップダウン リスト	次のいずれかになります。 • **[アラート（Alerts）]** • **[Critical]** • デバッグ • 緊急（**Emergencies**） • **Errors** • **Information** • 通知 • 警告

名前	説明
[Throttling] フィールド	同じイベントについて受信する重複メッセージの数を制限するかどうかを示します。次のいずれかになります。 • On：送信される重複メッセージの数が 2 時間以内に 30 件を越えると、そのアラートタイプに関するそれ以降のメッセージは破棄されます。 • [Off]：検出された数に関係なく、すべての重複メッセージが送信されます。

ステップ 5 [Save Changes] をクリックします。

Call Home の無効化

手順

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

ステップ 2 **[All]** > **[Communication Management]** > **[Call Home] の順に展開します。**

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Admin] 領域の **[State]** フィールドで、[off] をクリックします。

（注） このフィールドが [off] に設定されている場合、Cisco UCS Manager ではこのタブの残りのフィールドが表示されません。

ステップ 5 [Save Changes] をクリックします。

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 プロファイルの作成

デフォルトでは、Cisco TAC-1 プロファイルを設定する必要があります。しかし、プロファイルを追加作成することにより、指定したレベルでイベントが発生したときに、指定された 1 つ以上のグループにアラート メールを送信することもできます。

手順

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

ステップ 2 **[All]** > **[Communication Management]** > **[Call Home]** の順に展開します。

ステップ 3 [Work] ペインで、[Profiles] タブをクリックします。

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。

[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 5 [Create Call Home Profile] ダイアログボックスで、次の情報フィールドに値を入力します。

名前	説明
[Name] フィールド	このプロファイルのユーザ定義名。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Level] フィールド	Cisco UCS の障害がこのレベル以上の場合は、プロファイルがトリガーされます。次のいずれかになります。 • **[Critical]** • **Debug** • **Disaster** • **Fatal** • **[Major]** • **[Minor]** • 標準 • 通知 • 警告
[Alert Groups] フィールド	この Call Home プロファイルに基づいて警告されるグループ。これは次のいずれか、または複数の値になります。 • [Cisco Tac]：Cisco TAC の受信者 • [Diagnostic]：POST 完了サーバ障害通知の受信者 • [Environmental]：PSU やファンなどの問題に関する通知の受信者

ステップ 6 [Email Configuration] 領域で、次のフィールドに値を入力して電子メール アラートを設定します。

名前	説明
[Format] フィールド	次のいずれかになります。 • [Xml]：Extensible Markup Language（XML）と Adaptive Messaging Language（AML）XML Schema Definition（XSD）を使用するマシンが読み取り可能な形式。この形式により、Cisco Systems Technical Assistance Center との通信が可能になります。 • [Full Txt]：人間が判読するのに適している完全にフォーマットされたメッセージ（詳細な情報付き）。 • [Short Txt]：ポケットベルまたは印刷されたレポートに適している 1 ～ 2 行の障害の説明。
[Max Message Size] フィールド	指定された Call Home 受信者に送信される最大メッセージ サイズ。 1 ～ 5000000 の整数を入力します。デフォルト値は 5000000 です。 フルテキスト メッセージおよび xml メッセージの推奨最大サイズは 5,000,000 です。ショート テキスト メッセージの推奨最大サイズは 100,000 です。Cisco TAC アラート グループの場合、最大メッセージ サイズは 5,000,000 である必要があります。

ステップ 7 [Recipients] 領域で次の手順を実行して電子メール アラートの 1 つ以上の電子メール受信者を追加します。

a) テーブルの右側のアイコン バーの [+] をクリックします。

b) [Add Email Recipients] ダイアログボックスで、[Email] フィールド に Call Home アラートの送信先の電子メール アドレスを入力します。

この電子メールアドレスに Call Home のアラートと障害が送信されます。

保存した電子メール アドレスは削除できますが、変更はできません。

c) [OK] をクリックします。

ステップ 8 [OK] をクリックします。

Call Home プロファイルの削除

手順

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

ステップ 2 **[All]** > **[Communication Management]** > **[Call Home]** の順に展開します。

ステップ 3 [Work] ペインで、[Profiles] タブをクリックします。

ステップ 4 削除するプロファイルを右クリックし、[Delete] を選択します。

ステップ 5 [Save Changes] をクリックします。

Call Home ポリシー

ヒント デフォルトでは、すべての Call Home ポリシーがイネーブルになっており、重要なシステム イベントすべてについてアラートが電子メールで送信されます。

手順

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

ステップ 2 **[All]** > **[Communication Management]** > **[Call Home]** の順に展開します。

ステップ 3 [Work] ペインの [Policies] タブをクリックします。

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。

[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

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

名前	説明
[State] フィールド	このフィールドが [Enabled] の場合、関連付けられた原因と一致するエラーが発生した際にシステムはこのポリシーを使用します。それ以外の場合、一致するエラーが発生しても、システムはこのポリシーを無視します。デフォルトでは、すべてのポリシーがイネーブルになります。

名前	説明
[Cause] フィールド	このアラートをトリガーするイベント。各ポリシーは、アラートがいずれかのタイプのイベントに送信されるかどうかを定義します。

ステップ 6 [OK] をクリックします。

ステップ 7 異なる種類の障害またはイベントに Call Home ポリシーを設定する場合は、ステップ 4 および 5 を繰り返します。

Call Home ポリシーの削除

手順

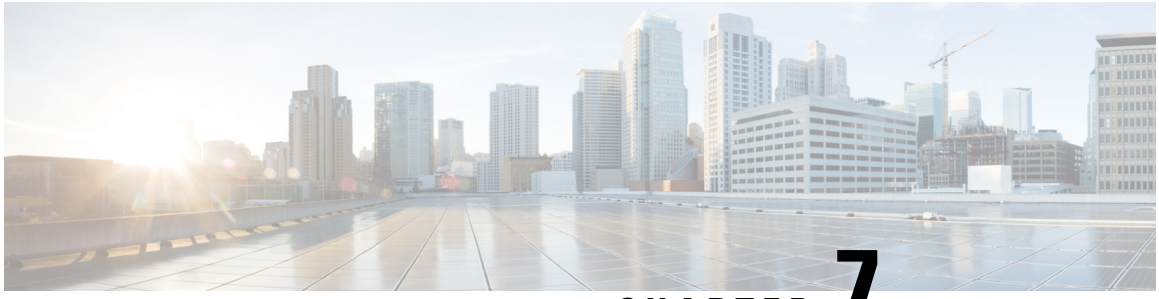
ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[All]** > **[Communication Management]** > **[Call Home]** の順に展開します。

ステップ 3 [Work] ペインの [Policies] タブをクリックします。

ステップ 4 ディセーブルにするポリシーを右クリックし、[Delete] を選択します。

ステップ 5 [Save Changes] をクリックします。



CHAPTER 7

UCS Manager コミュニケーション サービス

コミュニケーション プロトコル

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。 **Note** 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。 **Note** 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。

セキュアでないコミュニケーション サービス

ユーザ アカウントの Web セッション制限

Cisco UCS Manager では、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 セッションはユーザ 1 人あたり 32 に設定されます。ただし、この値は最大でシステム上限である 256 まで設定できます。

Web セッション制限の設定

手順

ステップ 1 **[Admin]** > **[Communication Management]** > **[Communication Services]** に移動します。

ステップ 2 [Web Session Limits] で次のフィールドに入力します。

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 3 [Save Changes] をクリックします。

シェル セッション制限の設定

手順

ステップ 1 **[Admin]** > **[Communication Management]** > **[Communication Services]** に移動します。

ステップ 2 [Shell Session Limits] で次のフィールドに入力します。

名前	説明
Maximum Sessions Per User	ユーザごと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。
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 3 [Save Changes] をクリックします。

CIM-XML の設定

Procedure

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

ステップ 2 **[All]** > **[Communication Management]** > **[Communication Services]** の順に展開します。

ステップ 3 [CIM-XML] 領域で、[Enabled] オプション ボタンをクリックします。

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

ステップ 4 [Save Changes] をクリックします。

HTTP の設定

Procedure

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

ステップ 2 **[All]** > **[Communication Management]** > **[Communication Services]** の順に展開します。

ステップ 3 [HTTP] 領域で、[Enabled] オプション ボタンをクリックします。

[HTTP] 領域が展開され、利用可能な設定オプションが表示されます。

ステップ 4 (Optional) [Port] フィールドで、 Cisco UCS Manager GUI が HTTP に使用するデフォルトのポートを変更します。

デフォルトのポートは 80 です。

ステップ 5 (Optional) [Redirect HTTP to HTTPS] フィールドで、[Enabled] オプション ボタンをクリックします。

HTTP ログインの HTTPS ログインへのリダイレクションをイネーブルにするには、HTTPS も設定して有効にする必要があります。いったんイネーブルにすると、HTTPS をディセーブルにするまではリダイレクションをディセーブルにできません。

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

ステップ 6 [Save Changes] をクリックします。

セキュアなコミュニケーション サービス

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、M4、および M3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。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。

キー リングの作成

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

手順

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

ステップ 2 **[All]** > **[Key Management] の順に展開します。**

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

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

a) **[Name]** フィールド で、キー リングの一意の名前を入力します。

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

- **[Mod2048]**
- **[Mod2560]**
- **[Mod3072]**
- **[Mod3584]**
- **[Mod4096]**

c) [OK] をクリックします。

次のタスク

このキー リングの証明書要求を作成します。

キー リングの証明書要求の作成

手順

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

ステップ 2 **[All]** > **[Key Management]** の順に展開します。

ステップ 3 証明書要求を作成するキー リングをクリックします。

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

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

ステップ 6 [Create Certificate Request] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[DNS] フィールド	ネットワークに割り当てられたドメイン名（すべてのホストに共通）。
[Locality] フィールド	証明書を要求している会社の本社が存在する市または町。 最大 64 文字まで入力できます。任意の文字、数字、スペース、および次の特殊文字を使用できます : ,（カンマ）、.（ピリオド）、@（アット マーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。
[State] フィールド	証明書を要求している会社の本社が存在する州または行政区分。 最大 64 文字まで入力できます。任意の文字、数字、スペース、および次の特殊文字を使用できます : ,（カンマ）、.（ピリオド）、@（アット マーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。
[Country] フィールド	会社所在国の国コード。 2 文字のアルファベットを入力します。
[Organization Name] フィールド	証明書を要求している組織。 最大 64 文字まで入力できます。任意の文字、数字、スペース、および次の特殊文字を使用できます : ,（カンマ）、.（ピリオド）、@（アット マーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。

名前	説明
[Organization Unit Name] フィールド	組織ユニット 最大 64 文字まで入力できます。任意の文字、数字、スペース、および次の特殊文字を使用できます : ,（カンマ）、.（ピリオド）、@（アット マーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。
[Email] フィールド	要求に関連付けられている電子メール アドレス。
[Password] フィールド	この要求に対するオプションのパスワード。
[Confirm Password] フィールド	パスワードを指定した場合は、確認のためにそのパスワードを再入力します。
[Subject] フィールド	ファブリック インターコネクトの完全修飾ドメイン名。

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

- [IPv4] タブをクリックし、次のフィールドに値を入力します。

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

- [IPv6] タブをクリックし、次のフィールドに値を入力します。

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

ステップ 8 [OK] をクリックします。

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

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

次のタスク

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 証明書の変更

この手順を使用して、KVM 証明書をユーザ生成のパブリック証明書に変更できます。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 **[Equipment]** > **[Chassis]** > ***[Chassis Number]*** > **[Servers]** の順に展開します。

ステップ 3 KVM 証明書を変更するサーバをクリックします。

ステップ 4 [Work] ペインの [Inventory] タブをクリックします。

ステップ 5 [CIMC] サブタブをクリックします。

ステップ 6 [Actions] 領域で、[Change KVM Certificate] をクリックします。

ステップ 7 [Change KVM Certificate] ダイアログボックスで、次のフィールドに入力します。

フィールド	説明
[Certificate] フィールド	ユーザ生成公開証明書。
[Key] フィールド	対応するユーザ生成秘密キー。 （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 8 [OK] をクリックします。

ステップ 9 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

この操作により、CIMC がリブートします。

KVM 証明書のクリア

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 **[Equipment]** > **[Chassis]** > ***[Chassis Number]*** > **[Servers]** の順に展開します。

ステップ 3 KVM 証明書をクリアするサーバをクリックします。

ステップ 4 [Work] ペインの [Inventory] タブをクリックします。

ステップ 5 [CIMC] サブタブをクリックします。

ステップ 6 [Actions] 領域で、[Clear KVM Certificate] をクリックします。

ステップ 7 [Clear KVM Certificate] ダイアログボックスで、[Yes] をクリックします。

この操作により、CIMC がリブートします。

トラスト ポイントの作成

手順

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

ステップ 2 **[All]** > **[Key Management] の順に展開します。**

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

ステップ 4 [Create Trusted Point] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	トラスト ポイントの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。

名前	説明
[Certificate Chain] フィールド	このトラスト ポイントの証明書情報。 **重要** 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。 Windows 2012 サーバの場合は、RSASSA-PSS を使用すると次のエラーが発生します。トラストポイントの証明書チェーンが無効、理由は不明。UCS Manager では、このアルゴリズムはサポートされていません。

ステップ 5 [OK] をクリックします。

次のタスク

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

キー リングへの証明書のインポート

手順

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

ステップ 2 **[All]** > **[Key Management]** の順に展開します。

ステップ 3 証明書のインポート先となるキー リングをクリックします。

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

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

a) **[Trusted Point]** ドロップダウン リストから、この証明書を付与したトラスト アンカーのトラスト ポイントを選択します。

b) [Certificate] フィールドに、トラスト アンカーまたは認証局から受け取った証明書のテキストを貼り付けます。

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

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

ステップ 6 [Save Changes] をクリックします。

次のタスク

キー リングを使用して HTTPS サービスを設定します。

HTTPS の設定

Caution 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。

Procedure

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

ステップ 2 **[All]** > **[Communication Management]** > **[Communication Services]** の順に展開します。

ステップ 3 [HTTPS] 領域で、[Enabled] オプション ボタンをクリックします。

[HTTPS] 領域が展開され、利用可能な設定オプションが表示されます。

ステップ 4 次のフィールドに入力します。

名前	説明
[Admin State] フィールド	次のいずれかになります。 • イネーブル • **Disabled** **[Admin State]** が有効になっている場合は、 Cisco UCS Manager GUI にこのセクションの残りのフィールドが表示されます。
[Port] フィールド	HTTPS 接続に使用するポート。 1 ～ 65535 の整数を指定します。 デフォルトでは、HTTPS はポートで有効になっています。
[Operational Port] フィールド	Cisco UCS Manager がシステム レベルの HTTPS 通信を行うために必要なポート。 このポートは変更できません。
[Key Ring] ドロップダウン リスト	HTTPS 接続のキー リング。

名前	説明
[Cipher Suite Mode] フィールド	Cisco UCS ドメイン で使用される暗号スイート セキュリティのレベル。次のいずれかになります。 • **[High Strength]** • **[Medium Strength]** • **[Low Strength]** • [Custom]：ユーザ定義の暗号スイート仕様の文字列を指定できます。
[Cipher Suite] フィールド	[Cipher Suite Mode] フィールドで [Custom] を選択した場合は、このフィールドでユーザ定義の暗号スイート仕様の文字列を指定します。 暗号スイート仕様の文字列は最大 256 文字まで使用できますが、OpenSSL 暗号スイート仕様に準拠する必要があります。次を除き、スペースや特殊文字は使用できません。！（感嘆符）、+（プラス記号）、-（ハイフン）、および:（コロン）。詳細については、http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuiteを参照してください。 たとえば、Cisco UCS Manager がデフォルトとして使用する中強度仕様の文字列は次のようになります。 **ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL**
Allowed SSL Protocols	使用可能な 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 TSLV1.2] を選択すると、安全性が低い TLS バージョンの使用を試みている Web クライアントの接続がすべてブロックされます。

ステップ 5 [Save Changes] をクリックします。

キーリングの削除

手順

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

ステップ 2 **[All]** > **[Key Management]** の順に展開します。

ステップ 3 削除するキー リングを右クリックし、[Delete] を選択します。

ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

トラスト ポイントの削除

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

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

ステップ 2 **[All]** > **[Key Management]** の順に展開します。

ステップ 3 削除するトラスト ポイントを右クリックし、[Delete] を選択します。

ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 5 [OK] をクリックします。

ネットワーク関連のコミュニケーション サービス

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。

Procedure

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

ステップ 2 **[All]** > **[Communication Management]** > **[Communication Services]** の順に展開します。

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

ステップ 4 [SNMP] 領域で、次のフィールドに入力します。

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

ステップ 5 [Save Changes] をクリックします。

What to do next

SNMP トラップおよびユーザを作成します。

CIMC Web サービスの有効化

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

手順

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

ステップ 2 **[All]** > **[Communication Management]** > **[Communication Services]** の順に展開します。

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

ステップ 4 [CIMC Web Service] 領域で、[Enabled] オプション ボタンをクリックします。

ステップ 5 [Save Changes] をクリックします。

通信サービスの無効化

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

Procedure

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

ステップ 2 **[All]** > **[Communication Management]** > **[Communication Services]** の順に展開します。

ステップ 3 [Communication Services] タブで、ディセーブルにする各サービスの [disable] オプション ボタンをクリックします。

ステップ 4 [Save Changes] をクリックします。

Telnet の有効化

Procedure

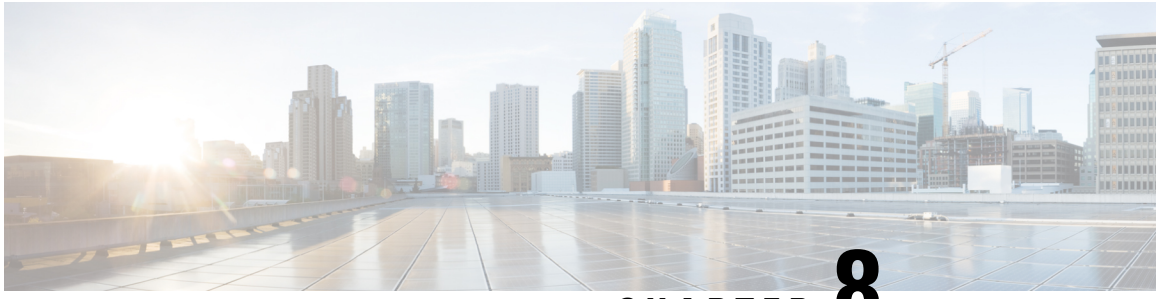
ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 **[All]** > **[Communication Management]** > **[Communication Services]** の順に展開します。

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

ステップ 4 [Telnet] 領域で、[Enabled] オプション ボタンをクリックします。

ステップ 5 [Save Changes] をクリックします。



CHAPTER 8

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。

すべての CIMC セッションの表示

ここでは、Cisco UCS Manager でグローバルに開かれている CIMC セッションの表示方法を 1 つ説明します。ローカル ユーザ、リモート ユーザ、IPMI ユーザによって開かれたすべてのサーバの CIMC セッションを表示できます。

手順

ステップ 1 [Navigation] ペインで、**[Admin]** > **[User Management]** > **[User Services]** の順にクリックします。

ステップ 2 [Work] ペインの [CIMC Sessions] タブをクリックします。

サーバの CIMC セッションの表示

ここでは、特定のサーバの CIMC セッションの表示方法について説明します。サーバおよびサービス プロファイルで開かれている CIMC セッションを表示できます。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 **[Chassis]** > **[Chassis Number]** > **[Servers]** > ***[Server Number]*** の順に展開します。

ステップ 3 [Work] ペインの [CIMC Sessions] タブをクリックします。

サービス プロファイルの CIMC セッションの表示

ここでは、特定のサービスプロファイルのCIMCセッションの表示方法について説明します。

（注） サービス プロファイルの下に CIMC セッションが表示されるのは、そのサービス プロファイルで指定された IP アドレスで CIMC セッションが開かれた場合だけです。

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 **[Servers]** > **[Service Profiles]** > **[Root]** > ***[Service Profile Name]*** の順に展開します。

ステップ 3 [Work] ペインの [CIMC Sessions] タブをクリックします。

ローカル ユーザによって開かれた CIMC セッションの表示

ここでは、ローカル ユーザによって開かれた CIMC セッションの表示方法について説明します。

手順

ステップ 1 [Navigation] ペインで、**[Admin]** > **[User Management]** > **[User Services]** > **[Locally Authenticated Users]** > ***[User Name]*** の順にクリックします。

ステップ 2 [Work] ペインの [CIMC Sessions] タブをクリックします。

リモート ユーザによって開かれた CIMC セッションの表示

ここでは、リモート ユーザによって開かれた CIMC セッションの表示方法について説明します。

手順

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

ステップ 2 [Admin] で、**[User Management]** > **[User Services]** > **[Remotely Authenticated Users]** > ***[User Name]*** の順に展開します。

ステップ 3 [Work] ペインの [CIMC Sessions] タブをクリックします。

開いているすべての CIMC セッションのクリア

このタスクでは、開いているすべてのCIMCセッションをクリアする方法を示します。ローカル、リモート、および IPMI ユーザが開いているすべてのサーバとサービスプロファイルの CIMC セッションをクリアできます。

手順

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

ステップ 2 [Admin] タブの [User Management] をクリックします。

ステップ 3 [Work] ペインの [CIMC Sessions] タブをクリックします。

ステップ 4 クリアする CIMC セッションを選択して右クリックし [Clear CIMC Session] を選択します。

ステップ 5 Cisco UCS Manager GUI に確認ダイアログ ボックスが表示されたら、[Yes] をクリックします。

サーバの CIMC セッションのクリア

このタスクでは、サーバのCIMCセッションをクリアする方法について説明します。サーバ上で開いている 1 つ以上の CIMC セッションをクリアできます。

手順

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

ステップ 2 [Equipment] タブで、**[Servers]** > ***[Server Name]*** を展開します。

ステップ 3 [Work] ペインの [CIMC Sessions] タブをクリックします。

ステップ 4 クリアする CIMC セッションを選択して右クリックし、[Clear CIMC Session] を選択します。

ステップ 5 Cisco UCS Manager GUI に確認ダイアログ ボックスが表示されたら、[Yes] をクリックします。

サービス プロファイルの CIMC セッションのクリア

このタスクは、サービス プロファイルの CIMC セッションをクリアする方法について説明します。サービスプロファイルで提供されている IP アドレスで開いている 1 つ以上の CIMC セッションをクリアできます。

手順

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

ステップ 2 [Servers] タブで、**[Servers]** > **[Service Profiles]** > **[root]** > ***[Service Profile Name]*** を展開します。

ステップ 3 [Work] ペインの [CIMC Sessions] タブをクリックします。

ステップ 4 クリアする CIMC セッションを選択して右クリックし、[Clear CIMC Session] を選択します。

ステップ 5 Cisco UCS Manager GUI に確認ダイアログ ボックスが表示されたら、[Yes] をクリックします。

ローカル ユーザの CIMC セッションのクリア

このタスクは、ローカル ユーザの CIMC セッションをクリアする方法について説明します。ローカル ユーザが開いている、1 つ以上の CIMC セッションをクリアすることができます。

手順

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

ステップ 2 [Admin] タブで、**[User Services]** > **[Locally Authenticated Users]** > ***[User Name]*** を展開します。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [General] タブ下で、[CIMC Sessions] セクションを展開します。

ステップ 5 クリアする CIMC セッションを選択して右クリックし [Clear CIMC Session] を選択します。

ステップ 6 Cisco UCS Manager GUI に確認ダイアログ ボックスが表示されたら、[Yes] をクリックします。

リモート ユーザの CIMC セッションのクリア

このタスクでは、リモートユーザのCIMCセッションをクリアする方法について説明します。リモート ユーザによって開かれている、1 つ以上の CIMC セッションをクリアできます。

手順

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

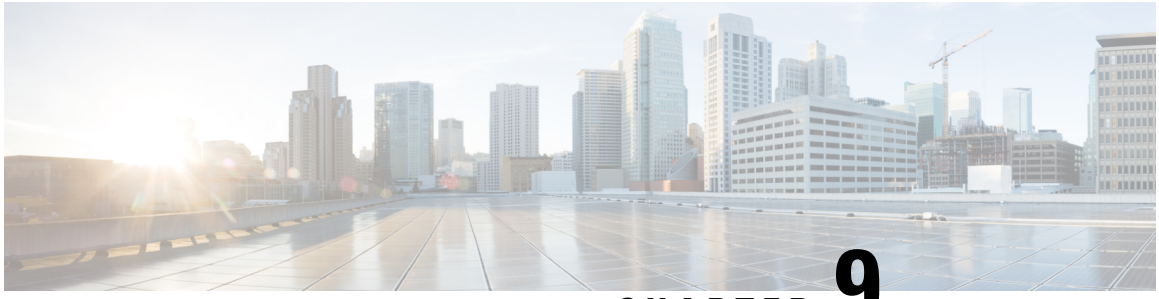
ステップ 2 **[User Management]** > **[User Services]** > **[Remotely Authenticated Users]** > ***[User Name]*** の順に展開します。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [General] タブ下で、[CIMC Sessions] セクションを展開します。

ステップ 5 クリアする CIMC セッションを選択して右クリックし、[Clear CIMC Session] を選択します。

ステップ 6 Cisco UCS Manager GUI に確認ダイアログ ボックスが表示されたら、[Yes] をクリックします。



CHAPTER 9

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。この要求は、現在のファブリック インターコネクト（FI）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 FI 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。デフォルトのポーリング間隔は 1 秒で、ポーリング間隔は最大 5 秒に設定できます。3 回ポーリングに失敗すると、CIMC は他の FI にフェールオーバーします。フェールオーバー中に、CIMCは新しく選択されたアップリンクでGratuitous Address Resolution Protocol（GARP）を発行し、MACが新しい場所に移動されたことをネットワークに通知します。

サーバの管理 IP アドレスの設定

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

このアクションがグレー表示されている場合、サーバにはすでにスタティック IP アドレスが割り当てられています。

サーバ 1 台あたり合計 3 つのスタティック管理アドレスを設定できます。

- アウトバンド IPv4
- インバンド IPv4
- インバンド IPv6

（注） 3 つをすべて設定する必要はありません。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 **[Equipment]** > **[Chassis]** > **[Chassis *Number*]** > **[Cartridges]** > **[Cartridge *Number*]** > **[Servers]** の順に展開します

ステップ 3 IP アドレスを設定するサーバをクリックします。

ステップ 4 [Work] ペインの [Inventory] タブをクリックします。

ステップ 5 [CIMC] サブタブをクリックします。

[Actions] 領域では、管理 IP アドレスに関して 2 つの選択肢があります。

- **[Modify Outband Static Management IP]**
- **[Change Inband Management IP]**

ステップ 6 アウトバンド スタティック管理 IP アドレスを変更するには、[Actions] 領域で [Modify Outband Static Management IP] をクリックします。

ステップ 7 [Modify Outband Static Management IP] ダイアログ ボックスで、次のフィールドに入力します。

フィールド	説明
IP Address	サーバに割り当てられるスタティック IPv4 アドレス。
[サブネット マスク（Subnet Mask）]	IP アドレスのサブネット マスク。
デフォルト ゲートウェイ	IP アドレスで使用するデフォルト ゲートウェイ。

ステップ 8 [**OK**] をクリックします。

ステップ 9 インバンド管理 IP アドレスを変更するには、[Change Inband Management IP] をクリックします。

[Change Management IP Address] ダイアログ ボックスには、2 つのタブがあります。

- **Inband IPv4**
- **[Inband IPv6]**

a) スタティック インバンド管理 IPv4 アドレスを変更するには、[In-Band IPv4] サブタブをクリックします。

b) [Change Management IP Address] ダイアログ ボックスで、次のフィールドに入力します。

フィールド	説明
[Management IP Address Policy] ドロップダウン	[Static] をクリックします。
IP Address	サーバに割り当てられるスタティック IPv4 アドレス。
[サブネット マスク（Subnet Mask）]	IP アドレスのサブネット マスク。
デフォルト ゲートウェイ	IP アドレスで使用するデフォルト ゲートウェイ。

c) [**OK**] をクリックします。

d) スタティック インバンド管理 IPv6 アドレスを変更するには、[In-Band IPv6] サブタブをクリックします。

e) [Change Management IP Address] ダイアログ ボックスで、次のフィールドに入力します。

フィールド	説明
[Management IP Address Policy] ドロップダウン	[Static] をクリックします。
IP Address	サーバに割り当てられるスタティック IPv6 アドレス。
[Prefix]	IP アドレスのネットワーク プレフィックス。
デフォルト ゲートウェイ	IP アドレスで使用するデフォルト ゲートウェイ。

ステップ 10 [OK] をクリックします。

ステップ 11 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバで管理 IP プールを使用するための設定

この手順のなかのどれかのアクションがグレー表示されている場合、設定がすでに完了していることを示します。サーバ 1 台あたりに合計 3 つの管理 IP プールを設定できます。

- アウトバンド IPv4
- インバンド IPv4
- インバンド IPv6

（注） 3 つをすべて設定する必要はありません。

始める前に

サーバで管理 IP プールを使用するように設定する前に、管理 IP プールを設定します。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 **[Equipment]** > **[Chassis]** > **[Chassis *Number*]** > **[Cartridges]** > **[Cartridge *Number*]** > **[Servers]** の順に展開します

ステップ 3 管理 IP プールを使用するように設定するサーバをクリックします。

ステップ 4 [Work] ペインの [Inventory] タブをクリックします。

ステップ 5 [CIMC] サブタブをクリックします。

- アウトバンド IP プール管理 IP アドレス ポリシーを設定するには、ステップ 6 に進みます。
- インバンド IPv4、IPv6 管理 IP アドレス ポリシーを設定するには、ステップ 8 に進みます。

ステップ 6 [Actions] 領域で、[Use Outband Pooled Management IP] をクリックします。

ステップ 7 [Use Outband Pooled Management IP] の確認ダイアログ ボックスで [Yes] をクリックし、[OK] をクリックします。
これで管理 IP アドレス ポリシーが、アウトバンド管理 IP プールの OOB IP アドレスを使用するように設定されます。

ステップ 8 [Actions] 領域で、[Change Inband Management IP] をクリックします。

ステップ 9 [Change Management IP] ダイアログ ボックスには、2 つのタブがあります。

- **Inband IPv4**
- **[Inband IPv6]**

a) インバンド IPv4 管理 IP プールを変更するには、[Inband IPv4] タブをクリックし、次のフィールドに入力します。

フィールド	説明
[Network] ドロップダウン リスト	関連付けられている VLAN グループから選択された VLAN。

フィールド	説明
[Management IP Address Policy] ドロップダウン リスト	サーバに割り当てる管理 IP プール。使用可能なプールが 2 種類あります。 • **[Domain Pools]** • **[Global Pools]** [Domain Pools] のエントリ、または [Global Pools] のエントリから使用可能なプールを 1 つ選択します。

b) インバンド IPv6 管理 IP プールを変更するには、[Inband IPv6] タブをクリックし、次のフィールドに入力します。

フィールド	説明
[Network] ドロップダウン リスト	関連付けられている VLAN グループから選択された VLAN。
[Management IP Address Policy] ドロップダウン リスト	サーバに割り当てる管理 IP プール。使用可能なプールが 2 種類あります。 • **[Domain Pools]** • **[Global Pools]** [Domain Pools] のエントリ、または [Global Pools] のエントリから使用可能なプールを 1 つ選択します。

ステップ 10 [OK] をクリックします。

ステップ 11 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバからのインバンド設定の削除

この手順では、サーバからインバンド管理 IP アドレスの設定を削除します。このアクションがグレー表示されている場合、インバンド設定は完了していません。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 **[Equipment]** > **[Chassis]** > **[Chassis *Number*]** > **[Cartridges]** > **[Cartridge *Number*]** > **[Servers]** の順に展開します

ステップ 3 インバンド管理 IP 設定を削除するサーバを選択します。

ステップ 4 [Work] 領域の [Inventory] タブをクリックします。

ステップ 5 [CIMC] サブタブをクリックします。

ステップ 6 [**Actions**] 領域で、[Delete Inband Configuration] をクリックします。

ステップ 7 [Delete] の確認ダイアログボックスで [Yes] をクリックします。

サーバのインバンド設定が削除されます。

（注） Cisco UCS Manager でインバンド サービス プロファイルがデフォルト VLAN とプール名で設定されている場合、ここでインバンド設定を削除した約1分後、サーバCIMCが自動的にインバンド プロファイルからインバンド設定を取得します。

サービス プロファイル テンプレートの管理 IP アドレスの設定

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 **[Servers]** > **[Service Profile Templates] の順に展開します。**

ステップ 3 管理 IP アドレスを設定するサービス プロファイル テンプレートを含む組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 管理 IP アドレスを設定するサービス プロファイル テンプレートをクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Management IP Address] 領域を展開します。

ステップ 7 [Actions] 領域で、[Change Management IP Address] をクリックします。

ステップ 8 [Change Management IP Address] ダイアログボックスのフィールドに入力します。

ステップ 9 [Save Changes] をクリックします。

サービス プロファイル テンプレートの管理 IP アドレスの設定

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 **[Servers]** > **[Service Profile Templates]** の順に展開します。

ステップ 3 管理 IP アドレスを設定するサービス プロファイル テンプレートを含む組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 管理 IP アドレスを設定するサービス プロファイル テンプレートをクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Management IP Address] 領域を展開します。

ステップ 7 [Actions] 領域で、[Change Management IP Address] をクリックします。

ステップ 8 [Change Management IP Address] ダイアログボックスのフィールドに入力します。

ステップ 9 [Save Changes] をクリックします。

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 アドレスが、管理 IP プールに含まれていてはなりません。

管理 IP プールでの IPv6 アドレス ブロックの作成

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 アドレスが、管理 IP プールに含まれていてはなりません。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] タブで、**[LAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。

ステップ 3 [IP Pools] ノードを展開します。

ステップ 4 [IP Pool ext-mgmt] を右クリックし、[Create Block of IP Addresses] を選択します。

ステップ 5 [Create a Block of IPv6 Addresses] ダイアログボックスで、必要な情報を指定します。

ステップ 6 [OK] をクリックします。

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

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] タブで、**[LAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。

ステップ 3 [IP Pools] ノードを展開します。

ステップ 4 [IP Pool ext-mgmt] を選択します。

ステップ 5 削除する IP アドレス ブロックを右クリックし、[Delete] を選択します。

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

管理 IP プールでの IPv4 アドレス ブロックの作成

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 アドレスが、管理 IP プールに含まれていてはなりません。

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。

ステップ 2 [LAN] タブで、**[LAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。

ステップ 3 [IP Pools] ノードを展開します。

ステップ 4 [IP Pool ext-mgmt] を右クリックし、[Create Block of IP Addresses] を選択します。

ステップ 5 [Create a Block of IPv4 Addresses] ダイアログ ボックスで、次のフィールドに入力します。

名前	説明
[Name] カラム	ブロックに割り当てられた IPv4 アドレスの範囲。
[From] カラム	ブロック内の最初の IPv4 アドレス。
[To] カラム	ブロック内の最後の IPv4 アドレス。
[Subnet] カラム	ブロック内の IPv4 アドレスと関連付けられたサブネットマスク。
[Default Gateway] カラム	ブロック内の IPv4 アドレスと関連付けられたデフォルト ゲートウェイ。
[Primary DNS] カラム	IPv4 アドレスのこのブロックがアクセスする必要のあるプライマリ DNS サーバ。
[Secondary DNS] カラム	IPv4 アドレスのこのブロックがアクセスする必要のあるセカンダリ DNS サーバ。

ステップ 6 [OK] をクリックします。

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。

CHAPTER 10

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作成

手順

ステップ 1 ツールバーで、[New] > [Create Organization] を選択します。

ステップ 2 [Create Organization] ダイアログボックスの [Name] フィールドに、組織の一意の名前を入力します。

この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。

ステップ 3 [Description] フィールドに、組織の説明を入力します。

ステップ 4 [OK] をクリックします。

サブ組織下の組織の作成

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 **[Service Profiles]** > **[root]** の順に展開します。

[Policies] ノードまたは [Pools] ノードの下の [Sub-Organizations] ノードにもアクセスできます。

ステップ 3 [Sub-Organizations] ノードを展開し、次のいずれかの手順を実行します。

- ルート直下に組織を作成するには、[Sub-Organizations] を右クリックし、[Create Organization] を選択します。
- より低いレベルのサブ組織の下に組織を作成するには、階層内のサブ組織ノードを展開してから、新しい組織を作成するサブ組織を右クリックし、[Create Organization] を選択します。

ステップ 4 [Create Organization] ダイアログボックスの [Name] フィールドに、組織の一意の名前を入力します。

この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。

ステップ 5 [Description] フィールドに、組織の説明を入力します。

ステップ 6 [OK] をクリックします。

組織の削除

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 削除する組織に移動します。

ステップ 3 組織を右クリックし、[Delete] を選択します。

ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

CHAPTER 11

バックアップと復元

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

Before you begin

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。

Procedure

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

ステップ 2 [All] ノードをクリックします。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Actions] 領域の [Backup Configuration] をクリックします。

ステップ 5 [Backup Configuration] ダイアログボックスで、[Create Backup Operation] をクリックします。

ステップ 6 [Create Backup Operation] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Admin State] フィールド	次のいずれかになります。 • **[enabled]**： **[OK]** をクリックするとすぐに、Cisco UCS Manager によってバックアップ操作が実行されます。 • **[disabled]**：**[OK]** をクリックしても、Cisco UCS Manager によってバックアップ操作は実行されません。このオプションを選択すると、ダイアログボックスのすべてのフィールドが表示されたままになります。ただし、[Backup Configuration] ダイアログボックスからバックアップを手動で実行する必要があります。

名前	説明
[Type] フィールド	バックアップ設定ファイルに保存された情報。次のいずれかになります。 • [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。 **Note** 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。

名前	説明
[Preserve Identities] チェックボックス	[All Configuration] および [System Configuration] タイプのバックアップ操作では、このチェックボックスは常に選択されており、次の機能を提供します。 • All Configuration - バックアップ ファイルは、プールから取得したすべてのアイデンティティ (vHBA、WWPN、WWNN、vNIC、MAC、UUID を含む) を保存します。また、シャーシ、FEX、ラック サーバのアイデンティティ、ならびにシャーシ、FEX、ラック サーバ、IOM、ブレード サーバのユーザ ラベルも保存されます。 **Note** このチェックボックスが選択されていない状態で復元を行うと、アイデンティティが再割り当てされ、ユーザ ラベルが失われます。 • System Configuration - バックアップ ファイルはシャーシ、FEX、ラック サーバのアイデンティティ、ならびにシャーシ、FEX、ラック サーバ、IOM、ブレード サーバのユーザ ラベルを保存します。 **Note** このチェックボックスが選択されていない状態で復元を行うと、アイデンティティが再割り当てされ、ユーザ ラベルが失われます。 [Logical Configuration] タイプのバックアップ操作でこのチェックボックスが選択されている場合、バックアップ ファイルはプールから取得したすべてのアイデンティティ (vHBA、WWPN、WWNN、vNIC、MAC、UUID を含む) を保存します。 **Note** このチェックボックスが選択されていない状態で復元を行うと、アイデンティティが再割り当てされ、ユーザ ラベルが失われます。

名前	説明
[Location of the Backup File] フィールド	バックアップ ファイルの保存場所。次のいずれかになります。 • **[Remote File System]**：バックアップ XML ファイルはリモート サーバに保存されます。Cisco UCS Manager GUI によって次に示すフィールドが表示され、リモート システムのプロトコル、ホスト、ファイル名、ユーザ名、パスワードを指定できます。 • [ローカル ファイル システム（Local File System）]：バックアップ XML ファイルはローカルに保存されます。 HTML ベースの Cisco UCS Manager GUI に **[Filename]** フィールドが表示されます。バックアップ ファイルの名前を ***<filename>*.xml** 形式で入力します。ファイルがダウンロードされ、ブラウザの設定に応じた場所に保存されます。
[Protocol] フィールド	リモート サーバとの通信時に使用するプロトコル。次のいずれかになります。 • **FTP** • **TFTP** • **SCP** • **SFTP** • [USB A]：ファブリック インターコネクト A に挿入された USB ドライブ。 このオプションを使用できるのは、特定のシステム設定の場合のみです。 • USB B：ファブリック インターコネクト B に挿入された USB ドライブ。 このオプションを使用できるのは、特定のシステム設定の場合のみです。

名前	説明
[Hostname] フィールド	バックアップ ファイルが格納されている場所のホスト名または IP アドレス（IPv4 または IPv6）。これは、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。 **Note** 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、または DNS 管理が**ローカル**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 [グローバル（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。
[Remote File] フィールド	バックアップ設定ファイルのフル パス。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。
[User] フィールド	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。このフィールドは、プロトコルが TFTP または USB の場合は適用されません。
[Password] フィールド	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または USB の場合は適用されません。 Cisco UCS Manager ではこのパスワードは保存されません。そのため、バックアップ操作をすぐに有効にして、実行する予定がない限り、このパスワードを入力する必要はありません。

ステップ 7 [OK] をクリックします。

ステップ 8 Cisco UCS Manager に確認ダイアログボックスが表示されたら、[OK] をクリックします。

[Admin State] フィールド をイネーブルに設定すると、Cisco UCS Manager によって、選択した設定タイプのスナップショットが取得され、ファイルがネットワークの場所にエクスポートされます。[Backup Configuration] ダイアログボックスの [Backup Operations] テーブルに、バックアップ操作が表示されます。

ステップ 9 (Optional) バックアップ操作の進行状況を表示するには、次の操作を実行します。

a) [Properties] 領域に操作が表示されない場合、[Backup Operations] テーブルの操作をクリックします。

b) [Properties] 領域で、[FSM Details] バーの下矢印をクリックします。

[FSM Details] 領域が展開され、操作のステータスが表示されます。

ステップ 10 [OK] をクリックし、[Backup Configuration] ダイアログボックスを閉じます。

バックアップ操作は完了するまで実行し続けます。進捗を表示するには、[Backup Configuration] ダイアログボックスを再度開きます。

バックアップ操作の実行

Procedure

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

ステップ 2 [All] ノードをクリックします。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Actions] 領域の [Backup Configuration] をクリックします。

ステップ 5 [Backup Configuration] ダイアログボックスの [Backup Operations] テーブルで、実行するバックアップ操作をクリックします。

選択されたバックアップ操作の詳細が [Properties] 領域に表示されます。

ステップ 6 [Properties] 領域で、次のフィールドに値を入力します。

a) [Admin State] フィールドで、[Enabled] オプション ボタンをクリックします。

b) TFTP を除くすべてのプロトコルについて、ユーザ名に対応するパスワードを [Password] フィールドに入力します。

c) (Optional) その他の使用可能なフィールドでコンテンツを変更します。

Note スケジュールバックアップを毎週から毎日にリセットするなど、他のフィールドを変更する場合は、ユーザ名とパスワードを再入力する必要があります。これを行わないと、FI のバックアップは失敗します。

ステップ 7 [Apply] をクリックします。

Cisco UCS Manager は、選択された設定タイプのスナップショットを作成し、ファイルをネットワークの場所にエクスポートします。[Backup Configuration] ダイアログボックスの [Backup Operations] テーブルに、バックアップ操作が表示されます。

ステップ 8 (Optional) バックアップ操作の進捗状況を確認するには、[FSM Details] バーの下矢印をクリックします。

[FSM Details] 領域が展開され、操作のステータスが表示されます。

ステップ 9 [OK] をクリックし、[Backup Configuration] ダイアログボックスを閉じます。

バックアップ操作は完了するまで実行し続けます。進捗を表示するには、[Backup Configuration] ダイアログボックスを再度開きます。

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。

（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。

手順

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

ステップ 2 [All] ノードをクリックします。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Actions] 領域の [Backup Configuration] をクリックします。

ステップ 5 [Backup Configuration] ダイアログボックスの [Backup Operations] 領域で、変更するバックアップ操作をクリックします。

選択されたバックアップ操作の詳細が [Properties] 領域に表示されます。バックアップ操作がディセーブル状態の場合、このフィールドはグレー表示されています。

ステップ 6 [Admin State] フィールドで、[enabled] オプション ボタンをクリックします。

ステップ 7 該当するフィールドを変更します。

バックアップ操作をただちに実行する場合を除き、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） バックアップ操作を今すぐに実行しない場合は、[Admin State] フィールドの [disabled] オプション ボタンをクリックします。

ステップ 9 [OK] をクリックします。

1 つまたは複数のバックアップ操作の削除

Procedure

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

ステップ 2 [All] ノードをクリックします。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Actions] 領域の [Backup Configuration] をクリックします。

ステップ 5 [Backup Configuration] ダイアログボックスの [Backup Operations] テーブルで、削除するバックアップ操作をクリックします。

Tip 操作の管理状態が [Enabled] に設定されている場合、テーブルでバックアップ操作をクリックすることはできません。

ステップ 6 [Backup Operations] テーブルのアイコン バーの [Delete] アイコンをクリックします。

ステップ 7 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 [Backup Configuration] ダイアログボックスで、次のいずれかをクリックします。

オプション	説明
適用	ダイアログボックスを閉じずに、選択したバックアップ操作を削除します。
OK	選択したバックアップ操作を削除し、ダイアログボックスを閉じます。

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。

Note 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

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

ステップ 2 [All] ノードをクリックします。

ステップ 3 [Work] ペインで、[Backup and Export Policy] タブをクリックします。

ステップ 4 [Full State Backup Policy] 領域で、次のフィールドに入力します。

名前	説明
[Hostname] フィールド	ポリシーのバックアップ ファイルが格納されている場所のホスト名またはIPアドレス（IPv4またはIPv6）。これは、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、または DNS 管理が**ローカル**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 [グローバル（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。
[Protocol] フィールド	リモート サーバとの通信時に使用するプロトコル。次のいずれかになります。 • **FTP** • **TFTP** • **SCP** • **SFTP** • [USB A]：ファブリック インターコネクト A に挿入された USB ドライブ。 このオプションを使用できるのは、特定のシステム設定の場合のみです。 • USB B：ファブリック インターコネクト B に挿入された USB ドライブ。 このオプションを使用できるのは、特定のシステム設定の場合のみです。
[User] フィールド	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。このフィールドは、プロトコルが TFTP または USB の場合は適用されません。
[Password] フィールド	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または USB の場合は適用されません。

名前	説明
[Remote File] フィールド	ポリシーのバックアップ ファイルのフルパス。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。
[Admin State] フィールド	次のいずれかになります。 • **[Enabled]**：**[Schedule]** フィールドで指定されたスケジュールに従って、Cisco UCS Manager はすべてのポリシー情報をバックアップします。 • **[Disabled]**—Cisco UCS Manager はポリシー情報をバックアップしません。
[Schedule] フィールド	Cisco UCS Manager がポリシー情報をバックアップする頻度。
[Max Files] フィールド	Cisco UCS Manager が保持するバックアップ ファイルの最大数。 この値は変更できません。
[Description] フィールド	バックアップ ポリシーの説明。デフォルトの説明は [Database Backup Policy] です。 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 5 （任意） [Backup/Export Config Reminder] 領域で、次のフィールドに入力します。

名前	説明
[Admin State] カラム	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
[Remind Me After (days)] 列	バックアップの実行に関するリマインダ通知を受け取るまでの日数。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 [Save Changes] をクリックします。

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

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

ステップ 2 [All] ノードをクリックします。

ステップ 3 [Work] ペインで、[Policy Backup & Export] タブをクリックします。

ステップ 4 [Config Export Policy] 領域で、次のフィールドに入力します。

名前	説明
[Hostname] フィールド	設定のバックアップ ファイルが格納されている場所のホスト名または IP アドレス（IPv4 または IPv6）。これは、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、または DNS 管理が**ローカル**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 [グローバル（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。

名前	説明
[Protocol] フィールド	リモート サーバとの通信時に使用するプロトコル。次のいずれかになります。 • **FTP** • **TFTP** • **SCP** • **SFTP** • [USB A]：ファブリック インターコネクト A に挿入された USB ドライブ。 このオプションを使用できるのは、特定のシステム設定の場合のみです。 • USB B：ファブリック インターコネクト B に挿入された USB ドライブ。 このオプションを使用できるのは、特定のシステム設定の場合のみです。
[User] フィールド	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。このフィールドは、プロトコルが TFTP または USB の場合は適用されません。
[Password] フィールド	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または USB の場合は適用されません。
[Remote File] フィールド	バックアップ設定ファイルのフル パス。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。
[Admin State] フィールド	次のいずれかになります。 • **[Enabled]**：**[Schedule]** フィールドで指定されたスケジュールに従って、Cisco UCS Manager はすべてのポリシー情報をバックアップします。 • **[Disabled]**—Cisco UCS Manager はポリシー情報をバックアップしません。
[Schedule] フィールド	Cisco UCS Manager がポリシー情報をバックアップする頻度。

名前	説明
[Max Files] フィールド	Cisco UCS Manager が保持する設定バックアップ ファイルの最大数。 この値は変更できません。
[Description] フィールド	設定のエクスポート ポリシーの説明。デフォルトの説明は [Configuration Export Policy] です。 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 5 （任意） [Backup/Export Config Reminder] 領域で、次のフィールドに入力します。

名前	説明
[Admin State] カラム	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
[Remind Me After (days)] 列	バックアップの実行に関するリマインダ通知を受け取るまでの日数。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 [Save Changes] をクリックします。

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。

Note 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

フル ステート 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 コンフィギュレーション

Before you begin

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

Procedure

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

ステップ 2 [All] ノードをクリックします。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Actions] 領域で、[Import Configuration] をクリックします。

ステップ 5 [Import Configuration] ダイアログボックスで、[Create Import Operation] をクリックします。

ステップ 6 [Create Import Operation] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Admin State] フィールド	次のいずれかになります。 • **[Enabled]**—Cisco UCS Managerでは、**[OK]** をクリックするとただちに、インポート操作が実行されます。 • **[Disabled]**—Cisco UCS Manager では、**[OK]** をクリックするとインポート操作が実行されません。このオプションを選択すると、ダイアログボックスのすべてのフィールドが表示されたままになります。ただし、インポートは [Import Configuration] ダイアログボックスから手動で実行する必要があります。
[Action] フィールド	次のいずれかになります。 • [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。
[Location of the Import File] フィールド	インポートするバックアップ ファイルが置かれている場所。次のいずれかになります。 • **[Remote File System]**—バックアップ XML ファイルはリモート サーバに保存されます。Cisco UCS Manager GUI に次に示すフィールドが表示され、リモート システムのプロトコル、ホスト、ファイル名、ユーザ名、パスワードを指定できます。 • **[Local File System]**：—バックアップ XML ファイルはローカルに保存されます。 Cisco UCS Manager GUI に **[Filename]** フィールドが関連付けられた **[Browse]** ボタンと共に表示されて、インポートするバックアップ ファイルの名前と場所を指定できます。

名前	説明
[Protocol] フィールド	リモート サーバとの通信時に使用するプロトコル。次のいずれかになります。 • **FTP** • **TFTP** • **SCP** • **SFTP** • [USB A]：ファブリック インターコネクト A に挿入された USB ドライブ。 このオプションを使用できるのは、特定のシステム設定の場合のみです。 • USB B：ファブリック インターコネクト B に挿入された USB ドライブ。 このオプションを使用できるのは、特定のシステム設定の場合のみです。
[Hostname] フィールド	コンフィギュレーション ファイルのインポート元のホスト名、IPv4 または IPv6 アドレス。 **Note** 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、または DNS 管理が**ローカル**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 [グローバル（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。
[リモートファイル（Remote File）] フィールド	XML コンフィギュレーション ファイルの名前。
[User] フィールド	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。このフィールドは、プロトコルが TFTP または USB の場合は適用されません。

名前	説明
[Password] フィールド	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または USB の場合は適用されません。 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、インポート操作をイネーブル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 7 [OK] をクリックします。

ステップ 8 確認ダイアログボックスで、[OK] をクリックします。

[Admin State] をイネーブルに設定した場合、Cisco UCS Manager は、ネットワークの場所から設定ファイルをインポートします。選択した処理に応じて、ファイル内の情報が既存の設定と結合されるか、既存の設定と置き換えられます。インポート操作は、[Import Configuration] ダイアログボックスの [Import Operations] テーブルに表示されます。

ステップ 9 (Optional) インポート操作の進捗状況を表示するには、次の手順を実行します。

a) [Properties] 領域にインポート操作が自動的に表示されない場合は、[Import Operations] テーブルでインポート操作をクリックします。

b) [Properties] 領域で、[FSM Details] バーの下矢印をクリックします。

[FSM Details] 領域が展開され、操作のステータスが表示されます。

ステップ 10 [OK] をクリックして、[Import Configuration] ダイアログボックスを閉じます。

インポート操作は、終了するまで実行されます。進捗状況を表示するには、[Import Configuration] を再度開きます。

インポート操作の実行

フル ステート 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 コンフィギュレーション

Procedure

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

ステップ 2 [All] ノードをクリックします。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Actions] 領域で、[Import Configuration] をクリックします。

ステップ 5 [Import Configuration] ダイアログボックスの [Import Operations] テーブルで、実行する操作をクリックします。

選択されたインポート操作の詳細が [Properties] 領域に表示されます。

ステップ 6 [Properties] 領域で、次のフィールドに値を入力します。

a) [Admin State] フィールドで、[Enabled] オプション ボタンをクリックします。

b) TFTP を除くすべてのプロトコルについて、ユーザ名に対応するパスワードを [Password] フィールドに入力します。

c) (Optional) その他の使用可能なフィールドでコンテンツを変更します。

ステップ 7 [Apply] をクリックします。

Cisco UCS Manager によって、ネットワークの場所からコンフィギュレーション ファイルがインポートされます。選択した処理に応じて、ファイル内の情報が既存の設定と結合されるか、既存の設定と置き換えられます。インポート操作は、[Import Configuration] ダイアログボックスの [Import Operations] テーブルに表示されます。

ステップ 8 (Optional) インポート操作の進捗状況を確認するには、[FSM Details] バーの下矢印をクリックします。

[FSM Details] 領域が展開され、操作のステータスが表示されます。

ステップ 9 [OK] をクリックして、[Import Configuration] ダイアログボックスを閉じます。

インポート操作は、終了するまで実行されます。進捗状況を表示するには、[Import Configuration] を再度開きます。

インポート操作の変更

手順

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

ステップ 2 [All] ノードをクリックします。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Actions] 領域で、[Import Configuration] をクリックします。

ステップ 5 [Import Configuration] ダイアログボックスの [Import Operations] 領域で、変更するインポート操作をクリックします。

選択されたインポート操作の詳細が [Properties] 領域に表示されます。インポート操作がディセーブル状態の場合、このフィールドはグレー表示されています。

ステップ 6 [Admin State] フィールドで、[enabled] オプション ボタンをクリックします。

ステップ 7 該当するフィールドを変更します。

インポート操作をただちに実行する場合を除き、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） インポート操作を今すぐに実行しない場合は、[Admin State] フィールドの [disabled] オプション ボタンをクリックします。

ステップ 9 [OK] をクリックします。

1 つまたは複数のインポート操作の削除

Procedure

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

ステップ 2 [All] ノードをクリックします。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Actions] 領域で、[Import Configuration] をクリックします。

ステップ 5 [Backup Configuration] ダイアログボックスの [Import Operations] テーブルで、削除するインポート操作をクリックします。

Tip 操作の管理状態が [Enabled] に設定されている場合、テーブルでインポート操作をクリックすることはできません。

ステップ 6 [Import Operations] テーブルのアイコン バーの [Delete] アイコンをクリックします。

ステップ 7 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 [Import Configuration] ダイアログボックスで、次のいずれかをクリックします。

オプション	説明
適用	ダイアログボックスを閉じずに、選択したインポート操作を削除します。
OK	選択したインポート操作を削除し、ダイアログボックスを閉じます。

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。

Cisco UCS Manager リリース 4.0(1) 以降のリリースでは、UCS 6200 シリーズ ファブリック インターコネクト上で次に示すサポート対象外の機能を使用して Full State バックアップが収集された場合、Full State 復元を使用してこのファイルを Cisco UCS 6400 シリーズ ファブリック インターコネクト上で復元することはできません。

- シャーシ ディスカバリ ポリシーおよびシャーシ接続ポリシーは非ポート チャネル モードで適用されます。
- 仮想マシン（VMware、Linux KVM または Microsoft ハイパーバイザ）の管理は有効にされます。

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。

Note 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
- デフォルトのゲートウェイの 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 **gui** と入力します。

ステップ 4 システムが DHCP サーバにアクセスできない場合、次の情報を入力するよう求められることがあります。

- ファブリック インターコネクトの管理ポートの IPv4 アドレスまたは IPv6 アドレス
- 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 マスクまたはプレフィックス
- ファブリック インターコネクトに割り当てられたデフォルト ゲートウェイの IPv4 アドレスまたは IPv6 アドレス

ステップ 5 プロンプトから、Web ブラウザに Web リンクをコピーし、Cisco UCS Manager GUI 起動ページに移動します。

ステップ 6 起動ページで [Express Setup] を選択します。

ステップ 7 [Express Setup] ページで [Restore From Backup] を選択し、[Submit] をクリックします。

ステップ 8 [Cisco UCS Manager Initial Setup] ページの [Protocol] 領域で、完全な状態のバックアップ ファイルをアップロードするために使用するプロトコルを選択します。

- **SCP**
- **TFTP**
- **[FTP]**
- **SFTP**

ステップ 9 [Server Information] 領域で、次のフィールドに値を入力します。

名前	説明
サーバ IP（サーバ IP）	完全な状態のバックアップ ファイルがあるコンピュータの IPv4 アドレスまたは IPv6 アドレス。これは、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。
Backup File Path	フォルダ名やファイル名など、完全な状態のバックアップファイルがあるファイルのパス。 （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。
ユーザ ID（User ID）	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。このフィールドは、プロトコルが TFTP または USB の場合は適用されません。
Password	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または USB の場合は適用されません。

ステップ 10 [Submit] をクリックします。`

コンソールに戻ってシステム復元の進捗状況を確認できます。

ファブリック インターコネクトはバックアップ サーバにログインし、指定された完全な状態のバックアップ 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 Manager 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。

CHAPTER 12

スケジュール オプション

スケジュールの作成

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 [Servers] タブで、[Schedules] をクリックし、[Create Schedule] を選択します。

ステップ 3 [Create Schedule] ウィザードの [Identify Schedule] ページで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	スケジュールの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。

名前	説明
[Description] フィールド	スケジュールの説明。スケジュールを使用すべき場所や条件に関する情報を含めることを推奨します。 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。
[Owner] フィールド	スケジュールのオーナー。次のいずれかになります。 • **[Local]**—Cisco UCS Manager がこの Cisco UCS ドメイン内に構成されているスケジュールを所有します。 • **[Pending Global]**—Cisco UCS Manager は現在、このスケジュールを Cisco UCS Central に転送しているところです。 • **[Global]**—リモート サーバ上に構成されている Cisco UCS Central がスケジュールを所有しています。

ステップ 4 [Next] をクリックします。

ステップ 5 [One Time Occurrences] ページで、次のいずれかをクリックします。

オプション	説明
[Next]	次のページに移動します。このスケジュールのワンタイム オカレンスを作成しない場合は、このオプションを選択します。 このオプションを選択した場合は、ステップ 8 に進みます。
[追加（Add）]	[Create a One Time Occurrence] ダイアログボックスを開き、このスケジュールを実行する単一の時間を指定できます。 このオプションを選択した場合は、ステップ 6 に進みます。

ステップ 6 （任意） [Create a One Time Occurrence] ダイアログボックスで、次の手順を実行します。

a) 次のフィールドに入力します。

名前	説明
[Name] フィールド	このスケジュールの 1 回のオカレンスの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。

名前	説明
[Start Time] フィールド	オカレンスが実行される日時。 フィールドの端にある下矢印をクリックして、カレンダーから日付を選択します。

b) 下矢印をクリックして [Options] 領域を展開します。

c) [Options] 領域で、次のフィールドに値を入力します。

名前	説明
[Max Duration] フィールド	スケジュールされたオカレンスを実行できる最大時間長。次のいずれかになります。 • [None]：オカレンスはすべてのタスクが完了するまで実行されます。 • **[other]**：Cisco UCS Manager GUI に **[dd:hh:mm:ss]** フィールドが表示されます。ここでは、オカレンスを実行できる最大時間長を指定できます。Cisco UCS は、指定された時間内に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。 デフォルトでは、最大時間は [none] に設定されます。この設定を変更せずに最大タスク数を設定しなければ、保留中のすべてのアクティビティが完了するまでメンテナンス期間は続きます。
[Max Number of Tasks] フィールド	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。次のいずれかになります。 • **[Unlimited]**：Cisco UCS は、**[Max Duration]** フィールドで指定された最大時間長を超えない限り、すべてのスケジュールされたタスクを実行します。[Max Duration] が [none] に設定されている場合にこのオプションを選択すると、保留中のすべてのアクティビティが完了するまでメンテナンス ウィンドウが続きます。 • **[other]**：Cisco UCS Manager GUI はテキスト フィールドを表示し、このオカレンス中に実行可能なタスクの最大数を指定できるようにします。1 ～ 65535 の整数を入力します。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。

名前	説明
[Max Number of Concurrent Tasks] フィールド	このオカレンス中に同時実行可能なタスクの最大数。次のいずれかになります。 • **[Unlimited]**：Cisco UCS はシステムが扱える最大数の同時実行タスクを実行します。 • **[other]**：Cisco UCS Manager GUI はテキスト フィールドを表示し、このオカレンス中に実行可能な同時実行タスクの最大数を指定できるようにします。1～65535 の整数を入力します。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。
[Minimum Interval Between Tasks] フィールド	システムが新しいタスクを開始するまで待機する最小時間長。この設定は、同時実行タスクの最大数が [None] 以外の値に設定されている場合にのみ有効です。次のいずれかになります。 • **[None]**：Cisco UCS は次のタスクをできるだけ早く実行します。 • **[other]**：Cisco UCS Manager GUI は、Cisco UCS のタスク間の待機時間の最小長を指定できるよう、**[dd:hh:mm:ss]** フィールドを表示します。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。

d) [**OK**] をクリックします。

ステップ 7 もう 1 つワン タイム オカレンスを追加するには、[Add] をクリックし、ステップ 6 を繰り返します。それ以外の場合は、[Next] をクリックします。

ステップ 8 （任意） このスケジュールの繰り返しオカレンスを定義する場合は、[Recurring Occurrences] ページで [Add] をクリックします。

a) [Create a Recurring Occurrence] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	このスケジュールの繰り返しオカレンスの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Day] フィールド	Cisco UCS がこのスケジュールのオカレンスを実行する日。次のいずれかになります。 • **[every day]** • **[Monday]** • **[Tuesday]** • **[Wednesday]** • **[Thursday]** • **[Friday]** • **[Saturday]** • **[Sunday]** • **[odd days]** • **[even days]**
[Hour] フィールド	スケジュールのこのオカレンスが開始される指定した曜日の時刻。0 ～ 24 の整数で指定します。0 と 24 は両方とも深夜を指します。 （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。 午後 11:59 までに繰り返しオカレンスが完了するよう、開始時刻として早めの時刻を設定してください。
[Minute] フィールド	スケジュール オカレンスを開始する時刻（分単位）。0 ～ 60 の整数を指定できます。

b) 下矢印をクリックして [Options] 領域を展開します。

c) [Options] 領域で、次のフィールドに値を入力します。

名前	説明
[Max Duration] フィールド	このスケジュールの各オカレンスを実行できる最大時間長。次のいずれかになります。 • [None]：オカレンスはすべてのタスクが完了するまで実行されます。 • **[other]**：Cisco UCS Manager GUI に **[dd:hh:mm:ss]** フィールドが表示されます。ここでは、オカレンスを実行できる最大時間長を指定できます。Cisco UCS は、指定された時間内に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。
[Max Number of Tasks] フィールド	各オカレンス中に実行可能な、スケジュール設定されたタスクの最大数。次のいずれかになります。 • **[Unlimited]**：Cisco UCS は、**[Max Duration]** フィールドで指定された最大時間長を超えない限り、すべてのスケジュールされたタスクを実行します。[Max Duration] が [none] に設定されている場合にこのオプションを選択すると、保留中のすべてのアクティビティが完了するまでメンテナンス ウィンドウが続きます。 • **[other]**：Cisco UCS Manager GUI はテキスト フィールドを表示し、このオカレンス中に実行可能なタスクの最大数を指定できるようにします。1 ～ 65535 の整数を入力します。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。
[Max Number of Concurrent Tasks] フィールド	このオカレンス中に同時実行可能なタスクの最大数。次のいずれかになります。 • **[Unlimited]**：Cisco UCS はシステムが扱える最大数の同時実行タスクを実行します。 • **[other]**：Cisco UCS Manager GUI はテキスト フィールドを表示し、このオカレンス中に実行可能な同時実行タスクの最大数を指定できるようにします。1～65535 の整数を入力します。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。

名前	説明
[Minimum Interval Between Tasks] フィールド	システムが新しいタスクを開始するまで待機する最小時間長。この設定は、同時実行タスクの最大数が [None] 以外の値に設定されている場合にのみ有効です。次のいずれかになります。 • **[None]**：Cisco UCS は次のタスクをできるだけ早く実行します。 • **[other]**：Cisco UCS Manager GUI は、Cisco UCS のタスク間の待機時間の最小長を指定できるよう、**[dd:hh:mm:ss]** フィールドを表示します。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。

d) [**OK**] をクリックします。
e) 別の繰り返しオカレンスを追加するには、[Add] をクリックし、このステップを繰り返します。

ステップ 9 [完了（Finish）] をクリックします。

スケジュールのワンタイム オカレンスの作成

（注） デフォルトでは、タスクの最大期間と最大数は [none] に設定されています。これらのデフォルトをどちらも変更しない場合、Cisco UCS Managerは、メンテナンス ウィンドウの存続期間に対する制限を課しません。保留中のすべてのアクティビティは、スケジュールされたメンテナンス ウィンドウが開始されるとすぐに適用され、Cisco UCS Manager は、これらすべてのタスクが完了するまで、保留中のアクティビティによる影響を受けるサーバのリブートを続行します。

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 [Schedules] を展開します。

ステップ 3 オカレンスを追加するスケジュールを右クリックし、[Create a One Time Occurrence] を選択します。

ステップ 4 [Create a One Time Occurrence] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	このスケジュールの 1 回のオカレンスの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Start Time] フィールド	オカレンスが実行される日時。 フィールドの端にある下矢印をクリックして、カレンダーから日付を選択します。

ステップ 5 下矢印をクリックして [Options] 領域を展開します。

ステップ 6 [Options] 領域で、次のフィールドに値を入力します。

名前	説明
[Max Duration] フィールド	スケジュールされたオカレンスを実行できる最大時間長。次のいずれかになります。 • [None]：オカレンスはすべてのタスクが完了するまで実行されます。 • **[other]**：Cisco UCS Manager GUI に **[dd:hh:mm:ss]** フィールドが表示されます。ここでは、オカレンスを実行できる最大時間長を指定できます。Cisco UCS は、指定された時間内に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。 デフォルトでは、最大時間は [none] に設定されます。この設定を変更せずに最大タスク数を設定しなければ、保留中のすべてのアクティビティが完了するまでメンテナンス期間は続きます。

名前	説明
[Max Number of Tasks] フィールド	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。次のいずれかになります。 • **[Unlimited]**：Cisco UCS は、**[Max Duration]** フィールドで指定された最大時間長を超えない限り、すべてのスケジュールされたタスクを実行します。[Max Duration] が [none] に設定されている場合にこのオプションを選択すると、保留中のすべてのアクティビティが完了するまでメンテナンス ウィンドウが続きます。 • **[other]**：Cisco UCS Manager GUI はテキスト フィールドを表示し、このオカレンス中に実行可能なタスクの最大数を指定できるようにします。1 ～ 65535 の整数を入力します。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。
[Max Number of Concurrent Tasks] フィールド	このオカレンス中に同時実行可能なタスクの最大数。次のいずれかになります。 • **[Unlimited]**：Cisco UCS はシステムが扱える最大数の同時実行タスクを実行します。 • **[other]**：Cisco UCS Manager GUI はテキスト フィールドを表示し、このオカレンス中に実行可能な同時実行タスクの最大数を指定できるようにします。1 ～ 65535 の整数を入力します。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。
[Minimum Interval Between Tasks] フィールド	システムが新しいタスクを開始するまで待機する最小時間長。この設定は、同時実行タスクの最大数が [None] 以外の値に設定されている場合にのみ有効です。次のいずれかになります。 • **[None]**：Cisco UCS は次のタスクをできるだけ早く実行します。 • **[other]**：Cisco UCS Manager GUI は、Cisco UCS のタスク間の待機時間の最小長を指定できるよう、**[dd:hh:mm:ss]** フィールドを表示します。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。

ステップ 7 [OK] をクリックします。

スケジュールへの繰り返しオカレンスの作成

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 [Schedules] を展開します。

ステップ 3 オカレンスを追加するスケジュールを右クリックし、[Create a Recurring Occurrence] を選択します。

ステップ 4 [Create a Recurring Occurrence] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	このスケジュールの繰り返しオカレンスの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Day] フィールド	Cisco UCS がこのスケジュールのオカレンスを実行する日。次のいずれかになります。 • **[every day]** • **[Monday]** • **[Tuesday]** • **[Wednesday]** • **[Thursday]** • **[Friday]** • **[Saturday]** • **[Sunday]** • **[odd days]** • **[even days]**

名前	説明
[Hour] フィールド	スケジュールのこのオカレンスが開始される指定した曜日の時刻。0 ～ 24 の整数で指定します。0 と 24 は両方とも深夜を指します。 （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。 午後 11:59 までに繰り返しオカレンスが完了するよう、開始時刻として早めの時刻を設定してください。
[Minute] フィールド	スケジュール オカレンスを開始する時刻（分単位）。0 ～ 60 の整数を指定できます。

ステップ 5 下矢印をクリックして [Options] 領域を展開します。

ステップ 6 [Options] 領域で、次のフィールドに値を入力します。

名前	説明
[Max Duration] フィールド	このスケジュールの各オカレンスを実行できる最大時間長。次のいずれかになります。 • [None]：オカレンスはすべてのタスクが完了するまで実行されます。 • **[other]**：Cisco UCS Manager GUI に **[dd:hh:mm:ss]** フィールドが表示されます。ここでは、オカレンスを実行できる最大時間長を指定できます。Cisco UCS は、指定された時間内に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。

名前	説明
[Max Number of Tasks] フィールド	各オカレンス中に実行可能な、スケジュール設定されたタスクの最大数。次のいずれかになります。 • **[Unlimited]**：Cisco UCS は、**[Max Duration]** フィールドで指定された最大時間長を超えない限り、すべてのスケジュールされたタスクを実行します。[Max Duration] が [none] に設定されている場合にこのオプションを選択すると、保留中のすべてのアクティビティが完了するまでメンテナンス ウィンドウが続きます。 • **[other]**：Cisco UCS Manager GUI はテキスト フィールドを表示し、このオカレンス中に実行可能なタスクの最大数を指定できるようにします。1 ～ 65535 の整数を入力します。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。
[Max Number of Concurrent Tasks] フィールド	このオカレンス中に同時実行可能なタスクの最大数。次のいずれかになります。 • **[Unlimited]**：Cisco UCS はシステムが扱える最大数の同時実行タスクを実行します。 • **[other]**：Cisco UCS Manager GUI はテキスト フィールドを表示し、このオカレンス中に実行可能な同時実行タスクの最大数を指定できるようにします。1 ～ 65535 の整数を入力します。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。
[Minimum Interval Between Tasks] フィールド	システムが新しいタスクを開始するまで待機する最小時間長。この設定は、同時実行タスクの最大数が [None] 以外の値に設定されている場合にのみ有効です。次のいずれかになります。 • **[None]**：Cisco UCS は次のタスクをできるだけ早く実行します。 • **[other]**：Cisco UCS Manager GUI は、Cisco UCS のタスク間の待機時間の最小長を指定できるよう、**[dd:hh:mm:ss]** フィールドを表示します。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。

ステップ 7 [OK] をクリックします。

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、1 回限りの実行か繰り返し実行をスケジュールに追加する必要があります。

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 **[Schedules]** > ***[Schedule_Name]*** の順に展開します。

ステップ 3 [One Time Occurrences] を展開します。

ステップ 4 削除するオカレンスを右クリックし、[Delete] を選択します。

ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ス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、1 回限りの実行か繰り返し実行をスケジュールに追加する必要があります。

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 **[Schedules]** > ***[Schedule_Name]*** の順に展開します。

ステップ 3 [Recurring Occurrences] を展開します。

ステップ 4 削除するオカレンスを右クリックし、[Delete] を選択します。

ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

スケジュールの削除

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

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 [Schedules] を展開します。

ステップ 3 削除するスケジュールを右クリックし、[Delete] を選択します。

ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

CHAPTER 13

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

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
- 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 ポリシーを自動遅延展開用に設定する予定の場合は、スケジュールを作成します。

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 **[Servers]** > **[Policies]** の順に展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Maintenance Policies] を右クリックし、[Create Maintenance Policy] を選択します。

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

名前	説明
[Name] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Description] フィールド	ポリシーの説明。ポリシーを使用する場所とタイミングについての情報を含めることを推奨します。 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。

名前	説明
[Soft Shutdown Timer] ドロップダウン リスト	このタイマーを使用して、Cisco UCS Manager がサーバをシャット ダウンして再起動を実行するまでの時間（秒数）を指定できます。Cisco UCS Manager は、メンテナンス ポリシーで指定されたこの待機時間が経過した後でハード シャットダウンを実行します。次のいずれかになります。 • **[150 Secs]**： Cisco UCS Manager は 150 秒の待機時間が経過して時点でハード シャットダウンを実行してサーバを再起動します。 • **[300 Secs]**： Cisco UCS Manager は 300 秒の待機時間が経過して時点でハード シャットダウンを実行してサーバを再起動します。 • **[600 Secs]**：Cisco UCS Manager は 600 秒待機してからサーバのハード シャットダウンとリブートを実行します。 • **[Never]**：Cisco UCS Manager はサーバのシャットダウンを実行しません。

名前	説明
[Reboot Policy] フィールド	サービス プロファイルがサーバに関連付けられたとき、またはサーバにすでに関連付けられているサービス プロファイルに変更を加えたときは、プロセスを完了するためにサーバをリブートする必要があります。[Reboot Policy] フィールドは、このメンテナンス ポリシーを含むサービス プロファイルのいずれかに関連付けられたサーバをリブートする時期を決定します。次のいずれかになります。 • [Immediate]：サービス プロファイルの関連付けが完了するか、サービス プロファイルの変更を保存するとすぐに、サーバが自動的にリブートされます。 • [User Ack]：サービスプロファイルに行われた変更は、保留中のアクティビティを明示的に確認するまで関連サーバに適用されません。 • **[Timer Automatic]**：Cisco UCS は、すべてのサービス プロファイルの関連付けを **[Schedule]** フィールドに表示されているスケジュールによって定義されているメンテナンス時間まで延期します。 • [On Next Boot]：このオプションは、[User Ack] または [Timer Automatic] のいずれかと組み合わせて使用します。[On Next Boot] オプションが有効な場合、ホスト OS のリブート、シャットダウン、リセット、またはサーバ リセットとシャットダウンにより、[User Ack] を待っている変更を適用する関連 FSM または [Timer Automatic] メンテナンス ウィンドウもトリガーされます。 （注） [On Next Boot] オプションを選択解除すると、BMC のメンテナンス ポリシーは無効になります。

名前	説明
[Schedule] ドロップダウン リスト	**[Reboot Policy]** が **[Timer Automatic]** に設定されている場合、メンテナンス操作がサーバに適用されるタイミングはスケジュールによって指定されます。Cisco UCS は、スケジュールされた時刻にサーバをリブートし、サービス プロファイルの変更を完了します。
[Create Schedule] リンク	この Cisco UCS ドメイン内のすべてのオブジェクトで使用できる新しいスケジュールを作成します。

ステップ 6 [OK] をクリックします。

次のタスク

ポリシーはサービス プロファイルまたはサービス プロファイル テンプレートにインクルードします。

メンテナンス ポリシーの削除

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 **[Servers]** > **[Policies]** > ***[Organization_Name]*** の順に展開します。

ステップ 3 [Maintenance Policies] を展開します。

ステップ 4 削除するメンテナンス ポリシーを右クリックし、[Delete] を選択します。

ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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

ステップ 1 ツールバーの [Pending Activities] をクリックします。

ステップ 2 次のいずれかのタブをクリックします。

- [User Acknowledged Activities]：完了する前にユーザ確認が必要なタスクを表示する [Service Profiles] タブと [Fabric Interconnects] タブが含まれています。
- [Scheduled Activities]：関連するメンテナンス スケジュールに基づいて実行されるタスクを表示します。

ステップ 3 表の行をクリックし、保留アクティビティの詳細を表示します。

[Server] 列のリンクをクリックすると、Cisco UCS Manager によってサーバのプロパティが表示されます。

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

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止められません。

手順

ステップ 1 ツールバーの [Pending Activities] をクリックします。

ステップ 2 [Pending Activities] ダイアログボックスで、[User Acknowledged Activities] タブをクリックしてから [Service Profiles] タブをクリックします。

ステップ 3 即時展開する保留中の各アクティビティの [Reboot Now] 列のチェックボックスをオンにします。

ステップ 4 [OK] をクリックします。

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。

ユーザの確認応答待ちのすべてのサービス プロファイル変更の展開

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止められません。

手順

ステップ 1 ツールバーの [Pending Activities] をクリックします。

ステップ 2 [Pending Activities] ダイアログボックスで、[User Acknowledged Activities] タブをクリックしてから [Service Profiles] タブをクリックします。

ステップ 3 ツールバーの [Acknowledge All] チェックボックスをオンにします。

Cisco UCS Manager GUI が、テーブル内のすべての保留中のアクティビティに対して [Reboot Now] チェックボックスをオンにします。

ステップ 4 [OK] をクリックします。

Cisco UCS Manager によって、テーブル内にリストされている保留中のアクティビティに影響されるすべてのサーバがただちに再起動されます。

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

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止められません。

手順

ステップ 1 ツールバーの [Pending Activities] をクリックします。

ステップ 2 [Pending Activities] ダイアログボックスの [Scheduled Activities] タブをクリックします。

ステップ 3 即時展開する保留中の各アクティビティの [Reboot Now] 列のチェックボックスをオンにします。

ステップ 4 [OK] をクリックします。

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。

スケジュールされたすべてのサービス プロファイル変更の即時展開

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止められません。

手順

ステップ 1 ツールバーの [Pending Activities] をクリックします。

ステップ 2 [Pending Activities] ダイアログボックスの [Scheduled Activities] タブをクリックします。

ステップ 3 ツールバーの [Acknowledge All] チェックボックスをオンにします。

Cisco UCS Manager GUI が、テーブル内のすべての保留中のアクティビティに対して [Reboot Now] チェックボックスをオンにします。

ステップ 4 [OK] をクリックします。

Cisco UCS Manager によって、テーブル内にリストされている保留中のアクティビティに影響されるすべてのサーバがただちに再起動されます。

CHAPTER 14

UCS の障害抑制

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。

グローバル障害ポリシーの設定

手順

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

ステップ 2 **[All]** > **[Faults, Events, and Audit Log]** の順に展開します。

ステップ 3 [Settings] をクリックします。

ステップ 4 [Work] ペインの [Global Fault Policy] タブをクリックします。

ステップ 5 [Global Fault Policy] タブで、次のフィールドに入力します。

名前	説明
[Flapping Interval] フィールド	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。これを防止するため、 Cisco UCS Manager では、最後に状態が変更されてからこの時間が経過するまで、障害が発生しても状態は変更されません。 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。その時点で何が発生するかは、[Clear Action] フィールドの設定によって異なります。 5 ～ 3,600 の範囲の整数を入力します。デフォルトは 10 です。
[Initial Severity] フィールド	次のいずれかになります。 • **Info** • 条件 • 警告
[Action on Acknowledgment] フィールド	認識されたアクションはログがクリアされると必ず削除されます。このオプションは変更できません。
[Clear Action] フィールド	エラーがクリアされるときに Cisco UCS Managerが実行するアクション。次のいずれかになります。 • **[Retain]**：Cisco UCS Manager GUI によって **[Length of time to retain cleared faults]** セクションが表示されます。 • **[Delete]**：障害メッセージにクリアのマークが付いた時点で、Cisco UCS Managerはすぐに障害メッセージを削除します。

名前	説明
[Clear Interval] フィールド	Cisco UCS Manager によって特定の間隔で自動的に障害をクリアするかどうかを指定します。次のいずれかになります。 • **[Never]**：Cisco UCS Manager は自動的に障害をクリアしません。 • **[other]**：Cisco UCS Manager GUI によって **[dd:hh:mm:ss]** フィールドが表示されます。
[dd:hh:mm:ss] フィールド	Cisco UCS Manager が障害にクリア済みのマークを付けるまでの経過時間（日、時、分、および秒）。その時点で何が発生するかは、[Clear Action] フィールドの設定によって異なります。

ステップ 6 [Save Changes] をクリックします。

次のタスク

障害抑制の詳細については、『*Cisco UCS* システム モニタリング ガイド』を参照してください。

第 15 章

KVM コンソール

KVM コンソール

KVM コンソールは、Cisco UCS Manager GUI または KVM の直接接続をエミュレートする KVM Launch Manager からアクセスできるインターフェイスです。サーバに物理的に接続する必要がある KVM ドングルとは異なり、KVM コンソールを使用すると、ネットワーク上のリモートロケーションからサーバに接続できます。Cisco UCS Manager リリース 4.1 (1) 以降では、KVM コンソール GUI は HTML5 ベースのアプリケーションとしてのみ使用できます。Java ベースのアプリケーションとしては使用できなくなりました。

KVM コンソールを使用してサーバにアクセスする場合は、サーバまたはサーバに関連付けられているサービス プロファイルのいずれかに CIMC IP アドレスが設定されていることを確認する必要があります。KVM コンソールは、サーバまたはサービス プロファイルに割り当てられた CIMC IP アドレスを使用して、Cisco UCS ドメイン内の正しいサーバを識別し、そのサーバに接続します。

CD、DVD、またはフロッピー ドライブを使用してサーバに直接接続する代わりに、KVM コンソールでは仮想メディアを使用します。仮想メディアは、仮想 CD、DVD、またはフロッピー ドライブにマップされた実際のディスク ドライブまたはディスク イメージ ファイルです。次に示す任意の仮想ドライブをマップできます。

- お使いのコンピュータ上の CD/DVD またはフロッピー ドライブ
- コンピュータ上のディスク イメージ ファイル

- ネットワーク上の CD/DVD またはフロッピー ドライブ
- ネットワーク上のディスク イメージ ファイル

（注） 物理サーバから KVM コンソールを起動すると、そのサーバがサービス プロファイルに関連付けられているか否かがチェックされます。関連付けられている管理 IP アドレスによってサーバがサービス プロファイルに関連付けられている場合は、その管理 IP アドレスを使用して KVM コンソールが起動されます。管理 IP アドレスがサービス プロファイルで関連付けられていない場合は、物理サーバを使用して KVM コンソールが起動されます。

サーバ OS のインストールに KVM コンソールを使用する場合の推奨事項

仮想 CD/DVD またはフロッピー ドライブから OS をインストールするには、その仮想 CD/DVD またはフロッピー ドライブがサービス プロファイルで最初のブート デバイスとして設定されている必要があります。

KVM コンソールを使用した OS のインストールは、KVM ドングルを使用する場合よりも時間がかかることがあります。これは、ネットワークを介してインストール ファイルをサーバにダウンロードする必要があるためです。ディスク ドライブまたはディスク イメージ ファイルをネットワーク共有から仮想ドライブにマップする場合は、インストールにさらに時間がかかることがあります。これは、インストール ファイルをネットワークから KVM コンソール（お使いのコンピュータ）にダウンロードした後、KVM コンソールからサーバにダウンロードする必要があるからです。このインストール方式を使用する場合は、KVM コンソールを搭載したシステムのできる限り近くにインストール メディアを配置することを推奨します。

仮想 KVM コンソール

KVM コンソールは Cisco IMC からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス（KVM）の直接接続をエミュレートします。コンソール上では、遠隔地のサーバを制御し、KVM セッション中にアクセスできる仮想ドライブに物理ロケーションをマッピングできます。

HTML5 KVM は、Cisco UCS Manager リリース 3.1(3) が稼働する M3 以降のサーバのみを対象としています。HTML5 KVM の Web ブラウザの最小要件は、Chrome 45、Firefox 45、IE 11、Opera 35、および Safari 9 です。最良の結果を得るため、最新バージョンのブラウザを使用してください。単一のブラウザでサポートされる同時セッションの数は、ブラウザの設定とメモリ使用量によって異なります。

[KVM Console] タブ

このタブは、サーバへのコマンドラインアクセスを提供します。このタブで使用可能なメニューオプションは以下のとおりです。

[Server Actions] メニュー

システムで実行するリモート サーバ操作を選択します。

メニュー項目	説明
Boot Server	仮想コンソール セッションからシステムの電源をオンにします。
Shutdown Server	仮想コンソール セッションからシステムの電源をオフにします。
Reset	仮想コンソール セッションからシステムをリセットします。

[ファイル（File）] メニュー

メニュー項目	説明
[ファイルにキャプチャ（Capture to File）] ボタン	JPG イメージとして現在の画面を保存できる [保存（Save）] ダイアログボックスが開きます。 （注） このオプションは、[KVM] タブ上でのみ利用できます。
[終了（Exit）] ボタン	KVM コンソールを閉じます。

[View] メニュー

メニュー項目	説明
[更新（Refresh）]	サーバの現在のビデオ出力を使用してコンソール表示を更新します。
Full Screen	画面全体になるように KVM コンソールを拡大します。

[Macros] メニュー

リモート システムで実行するキーボード ショートカットを選択します。

メニュー項目	説明
[静的マクロ（Static Macros）] メニュー	マクロの定義済みのセットを表示します。
[ユーザ定義マクロ（User Defined Macros）] メニュー	作成済みのユーザ定義マクロを表示します。
[Server Defined Macros] メニュー	作成済みのサーバ定義マクロを表示します。

メニュー項目	説明
[Manage] ボタン	マクロの作成および管理ができる [Configure User Defined Macros] ダイアログ ボックスを開きます。システム定義されたマクロは削除できません。

[Tools] メニュー

メニュー項目	説明
[Session Options]	以下の項目が指定できる [Session Settings] ダイアログを開きます。 • [Scaling] では、KVM 画面の表示縦横比を選択できます。 • これにより、ターゲット システムで使用するマウス アクセラレーションが定義されます。デフォルトは [Absolute Positioning] です。
[セッション ユーザ リスト（Session User List）]	アクティブ KVM セッションを持つすべてのユーザ ID を表示する [セッション ユーザ リスト（Session User List）] ダイアログ ボックスを開きます。
[Chat]	現在の KVM セッションにログインしているすべての管理者に対してグループ チャット ウィンドウを開きます。
[Virtual Keyboard]	現在の KVM セッションの画面キーボードを開きます。
[Playback Controls]	Java KVM が作成したを選択するためのダイアログボックスが開きます。

[Virtual Media] メニュー

名前	説明
Activate Virtual Devices	vMedia セッションをアクティブにし、ユーザがローカル コンピュータまたはネットワークから、ドライブまたはイメージ ファイルをアタッチできるようにします。 （注） セキュアでない接続を許可していない場合は、セッションを受け入れるためのプロンプトが表示されます。セッションを拒否すると、その仮想メディア セッションは終了します。

名前	説明
[CD/DVD]	ユーザがアクセスする CD/DVD を選択し、[Map Drive] ボタンをクリックしてそれをホスト サーバのデバイスにマップします。 （注） [Read Only] チェックボックスがオンの場合、デバイスに書き込み機能があってもサーバはその vMedia デバイスに書き込むことができません。
[Removable Disk]	ユーザがアクセスするリムーバブル ディスクを選択し、[Map Drive] ボタンをクリックしてそれをホスト サーバのデバイスにマップします。 （注） [Read Only] チェックボックスがオンの場合、デバイスに書き込み機能があってもサーバはその vMedia デバイスに書き込むことができません。
[Floppy Disk]	ユーザがアクセスするフロッピーを選択し、[Map Drive] ボタンをクリックしてそれをホスト サーバのデバイスにマップします。 （注） [Read Only] チェックボックスがオンの場合、デバイスに書き込み機能があってもサーバはその vMedia デバイスに書き込むことができません。

[Online Help] メニュー

名前	説明
[Contents and Index]	オンライン ヘルプを開きます。
[About KVM Viewer]	HTML5 KVM Viewer のビルド バージョン情報を表示します。

KVM ダイレクト アクセス

KVM ダイレクト アクセスにより、ユーザの Cisco UCS Manager ドメイン内のブレードおよびラック サーバを管理する管理者は、Web ブラウザを使用してサーバの KVM に直接アクセスすることができます。この機能により、管理者に彼らが管理するサーバの KVM コンソールへの

アクセスを許可する一方で、ファブリック インターコネクトの IP アドレスへのアクセスを制限することができます。

Cisco UCS Manager リリース 4.0 までは、アウトオブバンド IPv4 管理インターフェイス アドレスのみが KVM ダイレクト アクセス用にサポートされていました。Cisco UCS Manager リリース 4.0 は、インバンド IPv4 または IPv6 管理インターフェイス アドレスについても、 KVM ダイレクト アクセスのサポートを導入しています。

（注） KVM ダイレクト アクセスは、Cisco UCS M5 サーバでのみサポートされます。

アウトバンドでの KVM ダイレクト アクセスでは、Cisco UCS Manager GUIインターフェイスや KVM Launch Manager を使用せずに、ユーザがサーバ管理 IP アドレスに移動できるようにするためのカスタム アプリケーションもサポートされます。

KVM ダイレクト アクセスは、サーバに直接割り当てられた管理 IP アドレス、またはサーバの管理者がサービス プロファイルでサーバに関連付けた管理 IP アドレスを指定することでサポートされます。サーバ管理者は、割り当てられたインバンドまたはアウトバンド IP アドレスをブラウザに入力し、[Cisco UCS KVM Direct] ログイン ページに移動します。ログイン ページでは、ユーザがユーザ名とパスワードを入力します。アウトバンドアドレスの場合は、認証ドメインを選択することもできます。Cisco UCS KVM ダイレクトが起動すると、Cisco UCS Manager GUIからサーバにアクセスする場合と同じように、サーバ用のコンソールが表示されます。**[Launch]** ボタンの横で、このサーバに関連付けられている使用可能なアウトバンド アドレスおよびインバンド アドレスのリストを選択できます。Cisco UCS Manager リリース 4.1 (1) 以降では、KVM コンソール GUI は HTML5 ベースのアプリケーションとしてのみ使用できます。Java ベースのアプリケーションとしては使用できなくなりました。

インバウンドの KVM ダイレクト アクセスは、認証に自己署名証明書を使用します。ユーザがサーバの管理 IP アドレスまたはサービス プロファイルの IP アドレスに初めてアクセスしたときに、警告ダイアログボックスが表示され、ブラウザのキャッシュに証明書の例外を追加する必要があることが告げられます。

Cisco UCS KVM ダイレクト アクセスをサポートするデフォルトの通信サービスは HTTPS です。これは無効化できません。ユーザがアドレスの一部として HTTP を使用してブラウザで管理 IP を入力すると、HTTPS サービスに自動的にリダイレクトされます。

KVM ダイレクト アクセスに対応するには、Cisco UCS Manager で CIMC Web サービス（通信サービス）が有効になっていることを確認してください。

（注） Cisco UCS Manager では、CIMC Web サービスがデフォルトで有効化されます。

KVM 直接ユーザ

Cisco UCS Manager 適切な権限を持つユーザは、インバンド経由で直接 KVM でシャーシの任意のブレード サーバにログインできます。ブレード サーバに固有のログイン クレデンシャル

を使用するには、そのブレード サーバに関連付けられている IPMI プロファイルに基づくログイン権限を使用できます。これらのログイン権限は次のとおりです。

- 読み取り専用：ユーザはホストのキーボード入力またはマウス入力、vMedia、電源制御、マクロにアクセスできません。
- 管理者：ユーザにはすべての権限が与えられます。

サーバからの KVM コンソールの起動

サーバに割り当てられたアドレスを使用して複数の KVM コンソール セッションを起動できます。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 **[Equipment]** > **[Chassis]** > ***[Chassis Number]*** > **[Servers]** の順に展開します。

ステップ 3 **KVM コンソール** を通じてアクセスするサーバを選択します。

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

ステップ 5 [Actions] 領域を下にスクロールし、[KVM Console] の右にある [>>] ボタンをクリックします。

KVM コンソール が別のウィンドウで開き、サーバに関連付けられている使用可能なアウトバンドとインバンドのアドレスのリストが表示されます。

（注） [>>] ボタンではなく [KVM Console] をクリックすると、セッションは、最初がインバンド IPv6、2 番目がインバンド IPv4、3 番目がアウトオブバンド IPv4 の優先順序でサーバ アドレスを使用して自動的に起動します。

ステップ 6 [Select IP Address] リストからアドレスを選択します。

[(Inband)] と表示されるアドレスは、アップリンク ポート経由でサーバにアクセスし、[(Outband)] と表示されるアドレスは、管理インターフェイスのポート経由でサーバにアクセスします。

ステップ 7 [OK] をクリックします。

KVM コンソールは、選択したアドレスを使用して起動します。

ヒント キーボードの **`Caps Lock`** キーがオンになっている状態で KVM セッションを開き、その後に **`Caps Lock`** キーをオフにすると、**KVM コンソール**は Caps Lock キーがオンのときのように動作する場合があります。KVM コンソールとキーボードを同期させるには、**KVM コンソール**にフォーカスがない状態で **`Caps Lock`** キーを 1 度押し、次に **KVM コンソール**にフォーカスを置いて **`Caps Lock`** キーをもう一度押します。

ステップ 8 同じサーバの別の KVM セッションを開始するには、ステップ 5 ～ 7 を繰り返します。

別の KVM セッションが開始されます。設定されているアドレスの数に応じて、サーバに対して最大 6 つのセッションを開始できます。

サービス プロファイルからの KVM コンソールの起動

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 **[Servers]** > **[Service Profiles] の順に展開します。**

ステップ 3 KVM コンソールを起動するサービス プロファイルを含む組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 関連付けられているサーバへの KVM のアクセスが必要なサービス プロファイルを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Actions] 領域を下にスクロールし、[KVM Console] の右にある [>>] ボタンをクリックします。

KVM コンソールが別のウィンドウで開き、サーバに関連付けられている使用可能なアウトオブバンドとインバンドのアドレスのリストが表示されます。

（注） [>>] ボタンではなく [KVM Console] をクリックすると、セッションは、最初がインバンド IPv6、2 番目がインバンド IPv4、3 番目がアウトバンド IPv4 の優先順序でサーバアドレスを使用して自動的に起動します。

ステップ 7 [Select IP Address] リストからアドレスを選択します。

[(Inband)] と表示されるアドレスは、アップリンク ポート経由でサーバにアクセスし、[(Outband)] と表示されるアドレスは、管理インターフェイスのポート経由でサーバにアクセスします。

ステップ 8 [OK] をクリックします。

KVM コンソールは、選択したアドレスを使用して起動します。

ヒント キーボードの **`Caps Lock`** キーがオンになっている状態で KVM セッションを開き、その後に **`Caps Lock`** キーをオフにすると、**KVM コンソール**は Caps Lock キーがオンのときのように動作する場合があります。KVM コンソールとキーボードを同期させるには、**KVM コンソール**にフォーカスがない状態で **`Caps Lock`** キーを 1 度押し、次に **KVM コンソール**にフォーカスを置いて **`Caps Lock`** キーをもう一度押します。

ステップ 9 同じサーバの別のセッションを開始するには、ステップ 6 ～ 8 を繰り返します。

別の KVM セッションが開始されます。設定されているアドレスの数に応じて、サーバに対して最大 6 つのセッションを開始できます。

[Cisco UCS KVM Direct] Web ページからの KVM コンソールの起動

Cisco UCS KVM ダイレクト ログイン ページでは、Cisco UCS Managerにログインせずに Web ブラウザからサーバに直接アクセスできます。

始める前に

[Cisco UCS KVM Direct] ログイン ページを使用してサーバの KVM コンソールにアクセスするには、次の情報が必要です。

- Cisco UCS のユーザ名とパスワード。
- アクセスするサーバに関するサーバ CIMC またはサービス プロファイルの IPv4 アウトバンドまたは IPv4/IPv6 インバンド管理アドレス。

手順

ステップ 1 Web ブラウザで、アクセスするサーバの管理 IP アドレスの Web リンクを入力または選択します。

ステップ 2 [Security Alert] ダイアログボックスが表示されたら、[Yes] をクリックしてセキュリティ例外を作成します。
セキュリティ例外はブラウザのキャッシュに永続的に保存されます。

ステップ 3 Cisco UCS [KVM Direct] ダイアログボックスで、名前、パスワード、およびドメインを指定します。

ステップ 4 [Lauch KVM] ボタンをクリックして HTML5 KVM を開始します。[Launch] ボタンの横で、このサーバに関連付けられている使用可能なアウトバンド アドレスおよびインバンド アドレスのリストを選択できます。

KVM Launch Manager からの KVM コンソールの起動

KVM Launch Manager からサーバの KVM コンソールにアクセスするには、次の情報が必要です。

- Cisco UCS ユーザ名とパスワード

- アクセスする KVM のサーバに関連付けられたサーバ プロファイル名。

KVM Launch Manager では、Cisco UCS Manager にログインせずに KVM コンソールからサーバにアクセスできます。

手順

ステップ 1 Web ブラウザで、Cisco UCS Manager GUI への Web リンクを入力または選択します。

例：

HTTP アクセスのデフォルトの Web リンクは、IPv4 アドレスの場合は `http://UCSManager_IP`、IPv6 アドレスの場合は `http://UCSManager_IP6` です。HTTPS アクセスのデフォルトの Web リンクは、IPv4 アドレスの場合は `https://UCSManager_IP`、IPv6 アドレスの場合は `https://UCSManager_IP6` です。スタンドアロン設定では、*UCSManager_IP* または *UCSManager_IP6* はそれぞれ、ファブリック インターコネクトの管理ポートの IPv4 アドレスまたは IPv6 アドレスです。クラスタ設定では、*UCSManager_IP* または *UCSManager_IP6* はそれぞれ、Cisco UCS Managerに割り当てられた IPv4 アドレスまたは IPv6 アドレスです。

ステップ 2 Cisco UCS Manager の起動ページ で、**[Launch KVM Manager]** をクリックします。

ステップ 3 [Security Alert] ダイアログボックスが表示された場合は、[Yes] をクリックしてセキュリティ証明書を受け入れ、続行します。

ステップ 4 [UCS - KVM Launch Manager Login] ページで、次の手順を実行します。

a) Cisco UCS のユーザ名およびパスワードを入力します。

b) （任意） Cisco UCS の実装に複数のドメインが含まれる場合、**[Domain]** ドロップダウンリストから適切なドメインを選択します。

c) [OK] をクリックします。

ステップ 5 KVM Launch Manager の [Service Profiles] テーブルで、次の手順を実行します。

a) サービス プロファイルと、KVM アクセスが必要な関連するサーバを含む行を探します。

b) そのサーバの [Launch KVM] 列の [Launch] をクリックします。[Launch] ボタンの横で、このサーバに関連付けられている使用可能なアウトバンド アドレスおよびインバンド アドレスのリストを選択できます。

別ウィンドウに KVM コンソールが表示されます。

ヒント キーボードの **`Caps Lock`** キーがオンになっている状態で KVM セッションを開き、その後に **`Caps Lock`** キーをオフにすると、**KVM コンソール**は Caps Lock キーがオンのときのように動作する場合があります。KVM コンソールとキーボードを同期させるには、**KVM コンソール**にフォーカスがない状態で **`Caps Lock`** キーを 1 度押し、次に **KVM コンソール**にフォーカスを置いて **`Caps Lock`** キーをもう一度押します。

KVM のフォルダ マッピング

KVM のフォルダ マッピングは、UCS Manager 3.2(1) でサポートされています。フォルダ マッピングは、リモート システムの更新のために HTML5 KVM インターフェイスを使用して、KVM コンソールへの外部ファイル アクセスを提供します。この機能は、Google Chrome バージョン 57 以降を実行しているシステムを搭載した B シリーズ サーバと C シリーズ サーバで使用できます。

手順

ステップ 1 KVM コンソールを起動します。

ステップ 2 [Create Image] ボタンをクリックします。

ステップ 3 任意のファイルをドラッグし、[Create Image] ダイアログボックスにドロップします。

ステップ 4 [Download ISO Image File] をクリックして ISO イメージを作成します。HTML5 KVM インターフェイスを通じて使用できるのは ISO イメージのみです。

ステップ 5 [Virtual Media] ボタンをクリックし、[Activate Virtual Devices] を選択します。仮想デバイスがロードされるまで数秒間待機します。

ステップ 6 [Virtual Media] ボタンをクリックし、[CD/DVD] を選択します。

ステップ 7 新しい ISO ファイルまたはフォルダをドラッグして [Virtual Disk Management] ダイアログボックスにドロップし、[Map Drive] をクリックします。読み取り専用アクセス用に、この KVM セッションに新しいファイルがマップされました。

KVM 証明書

KVM 証明書の変更

この手順を使用して、KVM 証明書をユーザ生成のパブリック証明書に変更できます。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 **[Equipment]** > **[Chassis]** > ***[Chassis Number]*** > **[Servers]** の順に展開します。

ステップ 3 KVM 証明書を変更するサーバをクリックします。

ステップ 4 [Work] ペインの [Inventory] タブをクリックします。

ステップ 5 [CIMC] サブタブをクリックします。

ステップ 6 [Actions] 領域で、[Change KVM Certificate] をクリックします。

ステップ 7 [Change KVM Certificate] ダイアログボックスで、次のフィールドに入力します。

フィールド	説明
[Certificate] フィールド	ユーザ生成公開証明書。
[Key] フィールド	対応するユーザ生成秘密キー。 （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 8 [OK] をクリックします。

ステップ 9 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

この操作により、CIMC がリブートします。

KVM 証明書のクリア

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 **[Equipment]** > **[Chassis]** > ***[Chassis Number]*** > **[Servers]** の順に展開します。

ステップ 3 KVM 証明書をクリアするサーバをクリックします。

ステップ 4 [Work] ペインの [Inventory] タブをクリックします。

ステップ 5 [CIMC] サブタブをクリックします。

ステップ 6 [Actions] 領域で、[Clear KVM Certificate] をクリックします。

ステップ 7 [Clear KVM Certificate] ダイアログボックスで、[Yes] をクリックします。

この操作により、CIMC がリブートします。

第 16 章

デバイス コネクタ

Intersight 管理モード

Intersight 管理モード (IMM)は、Cisco Intersight で導入された新しい機能セットで、B シリーズブレードおよび FI の管理対象 C シリーズのサーバのサーバ プロファイルを設定、展開、管理することができます。IMM は、Cisco UCS Manager で最初に導入されたコンセプトを新しく実装しており、ポリシー モデルのオーナーシップを Cisco Intersight に移行しています。それで、ポリシー、VLAN、VSAN を前もって作成し、サーバ プロファイルに組み込むことができます。その後、サーバプロファイルは、B シリーズのブレードまたは管理対象 C シリーズのサーバで検出された Cisco Intersight に割り当てられ、展開されます。

第 4 世代のファブリック インターコネクト (FI) で IMM を有効にするには、Cisco UCS インフラストラクチャとサーバ ファームウェア (FW)(4.1(2)) で通常どおりのアップグレードを実行し、アップグレードが正常に完了してから、FI をリセットします。FI のリセット後に、セットアップ プロンプトで、Intersight を管理ノードとして選択します。FI のうちの一方を IMM モードでセットアップし、もう一方はクラスタに参加させることができます。それから、IMM ドメインを Cisco Intersight に対して要求します。IMM では、UCS のためのすべての設定と処理は、 Cisco Intersight から行われます。IMM では、FI をユニファイド ポート (イーサネットと FC) およびポート ロール)(アップリンクとサーバ) によって FI-A と FI-B にプログラムできるように、UCS のドメイン プロファイルを設定し、展開します。新しい UCS ドメイン プロファイルは、新しい UCS ドメインが Cisco Intersight ですばやくオンボードされるようにします。

（注） Cisco UCS インフラストラクチャおよびサーバ FW バージョン 4.1(2) では、IMM のテクニカル プレビューをオプトインできます (FI および接続されたサーバ用のポリシー駆動型設定プラットフォーム)。IMM を有効にすると、UCS ドメイン全体が工場出荷時のデフォルトにリセットされ、ドメイン内のサーバで実行されているワークロードが中断されます。この機能はテクニカル プレビューであり、実稼働ワークロードやアプリケーションには推奨されません。

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。

Cisco Intersight 管理の有効化または無効化

Cisco Intersight 管理を有効にすると、Intersight クラウド アプリケーションとデバイス間の双方向通信が確立されます。

始める前に

デバイス コネクタを設定するには、管理者である必要があります。

手順

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

ステップ 2 **[すべて (All)]** > **[デバイス コネクタ (Device Connector)]** の順に展開します。

[デバイス コネクタ (Device Connector)] タブに、接続ステータスと、セット アクセス モードが表示されます。**[デバイス コネクタ (Device Connector)]** タブに表示されるデバイス ID と要求コードは、Cisco Intersight で Cisco UCS Manager を要求するために使用されているものです。

ステップ 3 [設定（Settings）] をクリックします。

ステップ 4 **[設定 (Settings)]** ウィザードで、**[全般 (General)]** をクリックします。

ステップ 5 Intersight 管理を有効にするには **[デバイス コネクタ (Device Connector)]** スライダを有効にし、Intersight 管理を無効にするには **[デバイス コネクタ(Device Connector)]** スライダを無効にします。

デフォルトで、Cisco Intersight び管理状態が**有効**なっています。

ステップ 6 [アクセス モード（Access Mode）] で [読み取り専用（Read-only）] または [制御を許可（Allow Control）] を選択します。

[Read-only (読み取り専用)] アクセス モードを選択すると、Cisco Intersight を使用してデバイスを構成できなくなります。したがって、クラウドからデバイス コネクタに送信される構成は、エラー コードを伴って拒否されます。

[Allow Control (制御を許可)] モードを選択すると、Cisco Intersight を使用したデバイスの構成を完全に制御できます。

ステップ 7 Intersight 管理を無効にするには、**[デバイスコネクタ (Device Connector)]** スライダを無効にします。

Intersight 管理を無効にすると、[接続（Connection）] 領域に接続状態が [管理上無効（Administratively Disabled）] として表示されます。

ステップ 8 **[Save]** をクリックします。

Intersight デバイス コネクタのプロパティの表示

手順

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

ステップ 2 **[すべて (All)]** > **[デバイス コネクタ (Device Connector)]** の順に展開します。

[デバイス コネクタ (Device Connector)] タブに、接続ステータスと、セット アクセス モードが表示されます。**[デバイス コネクタ (Device Connector)]** タブに表示されるデバイス ID と要求コードは、Cisco Intersight で Cisco UCS Manager を要求するために使用されているものです。

ステップ 3 [設定（Settings）] をクリックします。

ステップ 4 **[設定 (Settings)]** ウィザードで、次の情報を確認します。

名前	説明
[General] タブ	Cisco UCS Manager と Cisco Intersight 間の接続の状態。 **[デバイス コネクタ (Device Connector)]** スライダ：Cisco Intersight の管理を有効または無効にできます。次のいずれかを実行できます。 • **[デバイス コネクタ (Device Connector)]** スライダをオンにする： Cisco Intersight 管理を有効にします。このシステムを要求（請求）して、Cisco Intersightの機能を活用できます。 （これがデフォルトの接続ステータスです）。 • **[デバイス コネクタ (Device Connector)]** スライダをオフにする：Cisco Intersight 管理を無効にします。Cisco Intersight との通信は許可されません。 **[Access Mode]**：**[Read-only]** または **[Allow Control]** としてアクセスを構成します。 • **[Read-only]**：**[Read-only]** アクセス モードを選択すると、Intersight を使用してデバイスを設定できなくなります。 • **[Allow Control]** — **[Allow Control]** アクセス モードを選択すると、Intersight を使用したデバイスの構成を完全に制御できます。
[DNS の構成 (DNS Configuration)] タブ	DNS 設定を行います。 • **[ドメイン名 (Domain name)]** フィールド：ドメイン名を追加します。 • **[DNS サーバ (DNS Server)]** フィールド：DNS 名前解決を有効にするように少なくとも 1 つの DNS サーバを設定します。Intersight Device Connector は、DNS レコードを正常に解決できる必要があります。 （注） DNS 設定が Cisco UCS Central のグローバル ポリシーで管理されている場合、DNS 設定はグレー表示されます。このような場合は、Cisco UCS Central から DNS 設定を更新します。

名前	説明
[NTP の設定（NTP Configuration）] タブ	NTP 設定を行います。時刻同期用に少なくとも 1 つの NTP サーバを設定することを強く推奨します。システム クロックの時刻がインターネットの時刻と同期していない場合でも、Intersight デバイス コネクタは、時間オフセットが大きすぎない限り、Intersight サービスと通信できます。タイムオフセットが Intersight X.509 証明書の有効期間外の場合、デバイスコネクタは Intersight サービスと通信できません。 • **[NTPサーバ (NTP Server)]** フィールド：少なくとも 1 つの NTP サーバを設定します。 （注） NTP 設定が Cisco UCS Central のグローバルポリシーで管理されている場合、NTP 設定はグレー表示されます。このような場合は、Cisco UCS Central から NTP 設定を更新します。

[Proxy Configuration (プロキシ設定)] タブ	HTTPS プロキシ設定が無効か、または手動で設定されているかどうかを示します。次のいずれかになります。
	• **[プロキシの有効化 (Enable Proxy)]** をオフにする：HTTPS プロキシ構成を無効にします。
	• **[プロキシの有効化 (Enable Proxy)]** をオンにする：HTTPS プロキシ構成を有効にします。
	  • [Proxy Hostname/IP]：プロキシのホスト名または IP アドレスを入力します。
	  • [Proxy Port]：プロキシ ポート番号を入力します。
	  • [Authentication]：プロキシ サーバへのアクセスを認証するには、このオプションを有効にします。
	  アクセスを認証する**ユーザ名**と**パスワード**を入力します。
	  （注） デバイス コネクタで必須となるログインクレデンシャルのフォーマットはなく、入力したクレデンシャルがそのまま構成済み HTTP プロキシ サーバに渡されます。ドメイン名でユーザ名を限定する必要があるかどうかは、HTTPプロキシサーバの設定によって異なります。

名前	説明
[Certificate Manager (証明書マネージャ)] タブ	信頼できる証明書のリストを表示し、有効な信頼できる証明書をインポートできます。 • **[Import]**：CA 署名付き証明書をインポートすることができます。 重要　インポートされた証明書が *.pem (base64 エンコード) 形式である必要があります。 • 次の情報と証明書のリストを表示することができます。 　• **[Name]**：CA 証明書の共通名。 　• **[In Use]**：信頼ストアで証明書を正常にリモートサーバの確認に使用されたかどうか。 　• **[Issued By]**: 証明書の発行認証局。 　• **[Expires]**—証明書の有効期限。 （注）　バンドルされた証明書は削除できません。

ステップ 5 [閉じる（**Close**）] をクリックします。

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。
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。

	コマンドまたはアクション	目的
		• *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。 • **volatile:** • **workspace:** • *dest-filename*：コピー先のファイルの新しいファイル名。dest-filename

	コマンドまたはアクション	目的
		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)#
```