Cisco UCS Manager 管理ガイド 3.1

初版：2016 年 01 月 20 日

最終更新：2016 年 09 月 17 日

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

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2016 Cisco Systems, Inc. All rights reserved.

目 次

はじめに ix

対象読者 ix

表記法 ix

Cisco UCS の関連ドキュメント xi

マニュアルに関するフィードバック xi

このリリースの新規情報および変更情報 1

このリリースの新規情報および変更情報 1

管理の概要 3

管理の概要 3

Cisco UCS Manager ユーザ マニュアル 4

パスワード管理 7

Cisco UCS パスワードの注意事項 7

Cisco UCS ユーザ名に関する注意事項 8

変更間隔のパスワード変更の最大数の設定 8

パスワードの変更禁止間隔の設定 9

パスワード履歴カウントの設定 10

ローカル認証されたユーザのパスワード プロファイル 11

ローカル認証されたユーザのパスワード履歴のクリア 13

ロールベース アクセスの設定 15

ロールベース アクセス コントロールの概要 15

Cisco UCS のユーザ アカウント 15

予約語：ローカル認証されたユーザ アカウント 16

ユーザ アカウントの Web セッション制限 17

ユーザ ロール 18

デフォルト ユーザ ロール 18

予約語：ユーザ ロール 20

権限 20
ユーザ ロールの作成 23
ユーザ ロールへの権限の追加 24
ユーザ ロールからの権限の削除 24
ユーザ ロールの削除 24
ロケール 25
ユーザ ロケール 25
ロケールへの組織の割り当て 26
ロケールの作成 26
ロケールからの組織の削除 27
ロケールの削除 27
ローカル認証されたユーザ アカウント 28
ユーザ アカウントの作成 28
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イネーブル化 31
Web セッション制限の設定 32
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 33
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 33
ユーザ アカウントの有効化 34
ユーザ アカウントの無効化 34
ローカル認証されたユーザのパスワード履歴のクリア 35
ローカルに認証されたユーザ アカウントの削除 35
ユーザ セッションのモニタリング 36
リモート認証 39
認証サービス 39
リモート認証プロバイダーに関する注意事項および推奨事項 40
リモート認証プロバイダーのユーザ属性 40
二要素認証 42
LDAP プロバイダーとグループ 43
ネストされた LDAP グループ 43
LDAP グループ ルール 44
LDAP プロバイダーのプロパティの設定 44
LDAP プロバイダーの作成 44

LDAP プロバイダーの LDAP グループ ルールの変更 46
LDAP プロバイダーの削除 48
LDAP グループ マッピング 48
LDAP グループ マップの作成 49
LDAP グループ マップの削除 50
RADIUS プロバイダー 50
RADIUS プロバイダーのプロパティの設定 50
RADIUS プロバイダーの作成 51
RADIUS プロバイダーの削除 52
TACACS+ プロバイダー 52
TACACS+ プロバイダーのプロパティの設定 52
TACACS+ プロバイダーの作成 52
TACACS+ プロバイダーの削除 54
プライマリ認証サービス 54
コンソール認証サービスの選択 54
デフォルト認証サービスの選択 56
リモート ユーザのロール ポリシー 58
リモート ユーザのロール ポリシーの設定 58
マルチ認証サービスの設定 59
マルチ認証サービス 59
プロバイダー グループ 59
LDAP プロバイダー グループの作成 59
LDAP プロバイダー グループの削除 60
RADIUS プロバイダー グループの作成 60
RADIUS プロバイダー グループの削除 61
TACACS+ プロバイダー グループの作成 61
TACACS+ プロバイダー グループの削除 62
認証ドメイン 62
認証ドメインの作成 63
Call Home 機能をイネーブルまたはディセーブルにする方法 67
Call Home 67
Call Home のイネーブル化 69

Call Home のディセーブル化 69
UCS Manager コミュニケーション サービス 71
コミュニケーション プロトコル 71
コミュニケーション サービス 71
セキュアでないコミュニケーション サービス 73
CIM-XML の設定 73
HTTP の設定 74
セキュアなコミュニケーション サービス 74
証明書、キー リング、トラスト ポイント 74
キー リングの作成 75
キー リングの証明書要求の作成 76
トラスト ポイントの作成 78
キー リングへの証明書のインポート 79
HTTPS の設定 80
キーリングの削除 81
トラスト ポイントの削除 82
ネットワーク関連のコミュニケーション サービス 82
SNMP のイネーブル化および SNMP プロパティの設定 82
CIMC Web サービスのイネーブル化 83
通信サービスのディセーブル化 84
Telnet のイネーブル化 84
CIMC セッション管理 85
CIMC セッション管理 85
すべての CIMC セッションの表示 86
サーバの CIMC セッションの表示 86
サービス プロファイルの CIMC セッションの表示 87
ローカル ユーザによって開かれた CIMC セッションの表示 87
リモート ユーザによって開かれた CIMC セッションの表示 87
開いているすべての CIMC セッションのクリア 88
サーバの CIMC セッションのクリア 88
サービス プロファイルの CIMC セッションのクリア 88
ローカル ユーザの CIMC セッションのクリア 89

リモート ユーザの CIMC セッションのクリア 89
管理 IP アドレスの設定 91
管理 IP アドレス 91
サーバの管理 IP アドレスの設定 92
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 92
サーバで管理 IP プールを使用するための設定 95
サーバからのインバンド設定の削除 97
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 97
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 98
管理 IP プール 98
管理 IP プールでの IPv6 アドレス ブロックの作成 99
管理 IP プールからの IP アドレス ブロックの削除 100
管理 IP プールでの IPv4 アドレス ブロックの作成 100
UCS Manager の組織 103
マルチテナント環境の組織 103
マルチテナント環境における階層的な名前解決 104
ルート組織下の組織の作成 106
サブ組織下の組織の作成 106
組織の削除 107
バックアップと復元 109
UCS でのバックアップの操作 109
バックアップ操作の考慮事項と推奨事項 109
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 110
バックアップ操作の作成 111
バックアップ操作の実行 115
バックアップ操作の変更 116
1 つまたは複数のバックアップ操作の削除 117
バックアップ タイプ 118
Full State バックアップ ポリシーの設定 118
All Configuration エクスポート ポリシーの設定 121
インポート方法 123
インポートの設定 124

インポート操作の作成 124
インポート操作の実行 127
インポート操作の変更 128
1 つまたは複数のインポート操作の削除 129
システムの復元 129
ファブリック インターコネクトの設定の復元 130
スケジュール オプション 133
スケジュールの作成 133
スケジュールのワンタイム オカレンスの作成 140
スケジュールの繰り返しオカレンスの作成 142
スケジュールからのワンタイム オカレンスの削除 145
スケジュールからの繰り返しオカレンスの削除 146
スケジュールの削除 146
サービス プロファイル更新の遅延展開 147
サービス プロファイルの遅延展開 147
遅延展開のスケジュール 148
遅延展開に関するガイドラインおよび制限事項 148
メンテナンス ポリシー 149
メンテナンス ポリシーの作成 150
メンテナンス ポリシーの削除 154
遅延展開のための保留アクティビティ 154
保留アクティビティの表示 155
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 155
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 156
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 156
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 157
UCS の障害抑制 159
グローバル障害ポリシー 159
グローバル障害ポリシーの設定 160

はじめに

- 対象読者，ix ページ
- 表記法，ix ページ
- Cisco UCS の関連ドキュメント，xi ページ
- マニュアルに関するフィードバック，xi ページ

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、フィールドのラベルのようなGUI要素は、[GUI 要素] のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[メイン タイトル] のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*italic*）で示しています。

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

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

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

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

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

警告 安全上の重要事項

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

これらの注意事項を保管しておいてください。

Cisco UCS の関連ドキュメント

ドキュメント ロードマップ

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

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

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

その他のマニュアル リソース

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

マニュアルに関するフィードバック

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

第 1 章

このリリースの新規情報および変更情報

- このリリースの新規情報および変更情報，1 ページ

このリリースの新規情報および変更情報

次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。この表は、このマニュアルに加えられた変更やこのリリースの新しい機能をすべて網羅するものではありません。

表 *1*：*Cisco UCS Manager* リリース *3.1 (2)* の新機能と変更された動作

機能	説明	参照先
160 の LDAP グループ マップのサポート	Cisco UCS Manager は最大 160 の LDAP グループ マップをサポートできるようになりました。	LDAP グループ マッピング，（48 ページ）
グレースフル シャットダウン	グレースフル シャットダウンを使用したサーバの再起動、またはサーバの再起動を要求するサービス プロファイルの変更を承認すると、Cisco UCS Manager はメンテナンス ポリシーで指定された時間が経過するまで待機してから、ハード シャットダウンを実行します。	メンテナンス ポリシー，（149 ページ）
Cisco UCS のバックアップでは、デフォルトで ID が保存されます。	バックアップ操作を開始すると、GUI において [Preserve Identities] がデフォルトで選択されるようになりました。	バックアップ操作の作成，（111 ページ）

このリリースの新規情報および変更情報

第 2 章

管理の概要

この章は、次の項で構成されています。

- 管理の概要，3 ページ
- Cisco UCS Manager ユーザ マニュアル，4 ページ

管理の概要

Cisco UCS Manager から必須のユーザ アクセス機能を構成することで、同じドメインにある Cisco UCS 6332 40 GB ファイバ インターコネクト（FI）と UCS 6200 シリーズ 10 GB FI 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すると共に、各ユーザアカウントに対して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て、マルチテナントなどのテナントに定義されている組織境界内でユーザ 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 とのインターフェイスのために、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 テンプレートに対する中断を伴う設定変更の実装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。

Cisco UCS Manager ユーザ マニュアル

Cisco UCS Manager では、次の表に示す、使用例を基本とした従来よりもコンパクトな新しいマニュアルが用意されています。

ガイド	説明
『Cisco UCS Manager Getting Started Guide』	Cisco UCS アーキテクチャのほか、Cisco UCS Manager の初期設定や構成のベスト プラクティスなど、稼働前に必要な操作について説明しています。
『Cisco UCS Manager Administration Guide』	パスワード管理、ロール ベース アクセスの設定、リモート認証、通信サービス、CIMC セッション管理、組織、バックアップと復元、スケジューリング オプション、BIOS トークン、および遅延展開について説明しています。
『Cisco UCS Manager Infrastructure Management Guide』	Cisco UCS Manager によって使用および管理される物理/仮想インフラストラクチャ コンポーネントについて説明します。

ガイド	説明
『Cisco UCS Manager Firmware Management Guide』	ファームウェアのダウンロードと管理、自動インストール によるアップグレード、サービス プロファイルによるアップグレード、ファームウェアの自動同期によるエンドポイントでの直接アップグレード、機能カタログの管理、展開シナリオ、およびトラブルシューティングについて説明しています。
『Cisco UCS Manager Server Management Guide』	新しいライセンス、Cisco UCS Central へのCisco UCS ドメインの登録、パワー キャッピング、サーバのブート、サーバ プロファイルおよびサーバ関連ポリシーについて説明しています。
『Cisco UCS Manager Storage Management Guide』	Cisco UCS Manager の SAN や VSAN など、ストレージ管理のあらゆる側面について説明しています。
『Cisco UCS Manager Network Management Guide』	Cisco UCS Manager の LAN や VLAN 接続など、ネットワーク管理のあらゆる側面について説明しています。
『Cisco UCS Manager System Monitoring Guide』	Cisco UCS Manager における、システム統計を含むシステムおよびヘルス モニタリングのあらゆる側面について説明しています。

第 3 章

パスワード管理

- Cisco UCS パスワードの注意事項，7 ページ
- Cisco UCS ユーザ名に関する注意事項，8 ページ
- 変更間隔のパスワード変更の最大数の設定，8 ページ
- パスワードの変更禁止間隔の設定，9 ページ
- パスワード履歴カウントの設定，10 ページ
- ローカル認証されたユーザのパスワード プロファイル，11 ページ
- ローカル認証されたユーザのパスワード履歴のクリア，13 ページ

Cisco UCS パスワードの注意事項

それぞれのローカル認証されたユーザ アカウントにはパスワードが必要です。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の確認を実行できます。

強いパスワードを使用することをお勧めします。そうしないと、ローカル認証されたユーザに対してパスワード強度の確認をしたときに、Cisco UCS Manager は、次の要件を満たさ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が可変で、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 ユーザ名に関する注意事項

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、次の注意事項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、英文字で開始する必要があります。数字やアンダースコアなどの特殊文字からは開始できません。
- ログイン ID では、大文字と小文字が区別されます。
- すべて数字のログイン ID は作成できません。
- ユーザ アカウントの作成後は、ログイン ID を変更できません。ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

変更間隔のパスワード変更の最大数の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope password-profile**	パスワード プロファイル セキュリティ モードを開始します。
ステップ 3	UCS-A /security/password-profile # **set change-during-interval enable**	ローカル認証されたユーザが指定された時間の間に実行できるパスワード変更の回数を制限します。
ステップ 4	UCS-A /security/password-profile # **set change-count** *pass-change-num*	ローカル認証されたユーザが、[Change Interval] の間に自分のパスワードを変更できる最大回数を指定します この値は、0 ～ 10 から自由に設定できます。
ステップ 5	UCS-A /security/password-profile # **set change-interval** *num-of-hours*	[Change Count] フィールドで指定したパスワード変更回数が有効になる時間の最大数を指定します この値は、1～745時間から自由に設定できます。 たとえば、このフィールドが 48 に設定され、[Change Count] フィールドが 2 に設定されている場合、ローカル認証されたユーザは 48 時間以内に 2 回を超えるパスワード変更を実行することはできません。
ステップ 6	UCS-A /security/password-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

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

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

パスワードの変更禁止間隔の設定

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

手順

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

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

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

パスワード履歴カウントの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。

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

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

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

ローカル認証されたユーザのパスワード プロファイル

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

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

パスワード履歴カウント

パスワード履歴のカウントにより、ローカル認証されたユーザが同じパスワードを再利用しないようにすることができます。パスワード履歴カウントを設定すると、Cisco UCS Manager で以前に使用されたパスワードが最大 15 個保存されます。パスワード履歴カウントでは、最新のものを先頭に、逆時系列でパスワードを保存します。これにより、パスワードの再使用が可能になるのは、履歴カウントがしきい値に到達したときの最も古いパスワードのみに限定されます。

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

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

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

パスワード変更間隔

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

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

ローカル認証されたユーザのパスワード履歴のクリア

手順

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

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

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

第 4 章

ロールベース アクセスの設定

- ロールベース アクセス コントロールの概要，15 ページ
- Cisco UCS のユーザ アカウント，15 ページ
- ユーザ ロール，18 ページ
- ロケール，25 ページ
- ローカル認証されたユーザ アカウント，28 ページ
- ユーザ セッションのモニタリング，36 ページ

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、エンジニアリング部門のサーバ管理者ロールを持つユーザは、エンジニアリング部門内のサーバ設定を更新できます。ただし、そのユーザに割り当てられたロケールに財務部門が含まれている場合を除いて、財務部門内のサーバ設定を更新することはできません。

Cisco UCS のユーザ アカウント

ユーザ アカウントを使用してシステムにアクセスします。各 Cisco UCS Managerドメインに、48 のローカル ユーザ アカウントを設定できます。各ユーザ アカウントには、一意のユーザ名とパスワードが必要です。

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

管理者アカウントは、各 Cisco UCS ドメインに設定されています。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 アカウントをディセーブルにすると、そのユーザはログインできなくなります。しかしディセーブル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。ディセーブルにされたローカルユーザアカウントを再度イネーブルにすると、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している場合は、ローカル ユーザ アカウントで定義されたロールによってリモート ユーザ アカウントのロールが上書きされます。

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 アカウントはディセーブルになります。

デフォルトでは、ユーザ アカウントの有効期限はありません。

（注） ユーザ アカウントに有効期限日付を設定した後は、アカウントの有効期限をなくすよう再設定できません。ただし、使用できる最新の有効期限の日付でアカウントを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 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、Cisco UCS Manager の許容同時 Web セッション数はユーザ 1 人あたり 32 です。ただし、この値は最大でシステム上限の 256 まで設定できます。

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 ドメインは、デフォルトのユーザ ロールを含めて、最大 48 個のユーザ ロールを持つことができます。最初の 48 のユーザ ロールが許可された後に設定されたユーザ ロールは、障害が発生して無効になります。

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が含まれています。読み取り専用ロールを持つユーザは、システム状態を変更できません。

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

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

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

（注） ローカル ユーザ アカウントとリモート ユーザ アカウントに同じユーザ名がある場合、Cisco UCS Manager は、リモート ユーザに割り当てられたすべての役割を、ローカル ユーザに割り当てられた内容で上書きします。

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 アドミニストレータ

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。

動作

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

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

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

権限

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

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

表 *2*：ユーザの権限

特権	説明	デフォルトのロール割り当て
aaa	システム セキュリティおよび AAA	AAA アドミニストレータ
admin	システム管理	アドミニストレータ
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

特権	説明	デフォルトのロール割り当て
ext-san-policy	外部 SAN ポリシー	ストレージアドミニストレータ
ext-san-qos	外部 SAN QoS	ストレージアドミニストレータ
ext-san-security	外部 SAN セキュリティ	ストレージアドミニストレータ
fault	アラームおよびアラーム ポリシー	動作
operations	ログおよび Smart Call Home	動作
org-management	組織管理	動作
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と書き込みのアクセス	ファシリティ マネージャ
read-only	読み取り専用アクセス権 読み取り専用は、権限として選択できません。この権限は、すべてのユーザ ロールに割り当てられます。	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

特権	説明	デフォルトのロール割り当て
service-profile-config	サービス プロファイル設定	サーバプロファイルアドミニストレータ
service-profile-config-policy	サービスプロファイル設定ポリシー	サーバプロファイルアドミニストレータ
service-profile-ext-access	サービス プロファイル エンドポイント アクセス	サーバプロファイルアドミニストレータ
service-profile-network	サービス プロファイル ネットワーク	ネットワーク アドミニストレータ
service-profile-network-policy	サービス プロファイル ネットワーク ポリシー	ネットワーク アドミニストレータ
service-profile-qos	サービス プロファイル QoS	ネットワーク アドミニストレータ
service-profile-qos-policy	サービス プロファイル QoS ポリシー	ネットワーク アドミニストレータ
service-profile-security	サービス プロファイル セキュリティ	サーバセキュリティアドミニストレータ
service-profile-security-policy	サービス プロファイル セキュリティ ポリシー	サーバセキュリティアドミニストレータ
service-profile-server	サービス プロファイル サーバ管理	サーバプロファイルアドミニストレータ
service-profile-server-oper	サービス プロファイル コンシューマ	サーバプロファイルアドミニストレータ
service-profile-server-policy	サービス プロファイル プール ポリシー	サーバセキュリティアドミニストレータ
service-profile-storage	サービスプロファイルストレージ	ストレージアドミニストレータ
service-profile-storage-policy	サービスプロファイルストレージ ポリシー	ストレージアドミニストレータ

ユーザ ロールの作成

手順

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

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 [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

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 [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 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 アカウントから削除されます。

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] > [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。通常、アクセスできるのは、ロケールで指定された部門のみに限定されます。ただし、部門をまったく含まないロケールは例外です。このようなロケールは、全部門のシステム リソースへの無制限のアクセスを提供します。

Cisco UCS ドメインは、最大 48 個のユーザ ロケールを持つことができます。最初の 48 個の後に設定されたユーザ ロケールは受け入れられますが、非アクティブなために、障害が発生します。

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だけに制限されます。たとえば、ロケールにエンジニアリング組織しか含まれていない場合、そのロケールを割り当てられたユーザは、他のユーザにエンジニアリング組織のみを割り当てることできます。

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

- aaa
- admin
- fault
- operations

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

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

はじめる前に

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。

次の作業

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, （33 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

（注） 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。

はじめる前に

システムに次のいずれかがある場合は、該当するタスクを実行します。

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

手順

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。このアカウントは一意のものであるとともに、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、英文字で開始する必要があります。数字やアンダースコアなどの特殊文字からは開始できません。 • ログイン ID では、大文字と小文字が区別されます。 • すべて数字のログイン ID は作成できません。 • ユーザ アカウントの作成後は、ログイン ID を変更できません。ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。 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。
[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。

名前	説明
[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を有効にした場合は、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が可変で、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。
[Confirm Password] フィールド	確認のためのパスワードの再入力。
[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。

名前	説明
[Account Expires] チェックボックス	オンにすると、このアカウントは [Expiration Date] フィールドで指定した日付に期限切れになり、それ以降は使用できなくなります。 （注） ユーザ アカウントに有効期限日付を設定した後は、アカウントの有効期限をなくすよう再設定できません。ただし、使用できる最新の有効期限の日付でアカウントを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。 （注） [Account Expires] チェックボックスをオンにすると、Cisco UCS Manager GUI にこのフィールドが表示されます。

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。

（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。

ステップ 6 （任意） 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イネーブル化

パスワードの強度の確認を有効にするには、ユーザが admin または aaa 権限を持っている必要があります。 パスワードの強度の確認が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してい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] フィールド	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] フィールド	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。

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 ロールと権限の変更は、次回ユーザがログインするまで有効になりません。 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、ユーザが admin または aaa 権限を持っている必要があります。

はじめる前に

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、ユーザが admin または aaa 権限を持っている必要があります。

（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。アカウントをイネーブル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

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。

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	Cisco UCS Manager に接続している場合、Web クライアントは、Web セッションをアクティブに保つために、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、セッションの終了は行いません。
[Session Timeout] カラム	最後の更新要求から Cisco UCS Manager が Web セッションが非アクティブであると見なすまでの最大経過時間。この時間制限を超えると、Cisco UCS Manager は自動的に Web セッションを終了させます。
[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。
[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。

第 5 章

リモート認証

- 認証サービス，39 ページ
- リモート認証プロバイダーに関する注意事項および推奨事項，40 ページ
- リモート認証プロバイダーのユーザ属性，40 ページ
- 二要素認証，42 ページ
- LDAP プロバイダーとグループ，43 ページ
- RADIUS プロバイダー，50 ページ
- TACACS+ プロバイダー，52 ページ
- プライマリ認証サービス，54 ページ
- マルチ認証サービスの設定，59 ページ

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ーに関する注意事項および推奨事項

システムを、サポートされているリモート認証サービスのいずれかに設定する場合は、そのサービス用のプロバイダーを作成して、Cisco UCS 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 にローカルに存在するか、またはリモート認証サーバに存在することができます。

リモート認証サービスを介してログインしているユーザの一時的なセッションは、Cisco UCS 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ーのユーザ属性

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ーに 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. ユーザが検証されると、そのユーザに割り当てられているロールとロケールをチェックします。

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

表 *3*：リモート認証プロバイダーによるユーザ属性の比較

認証プロバイダー	カスタム属性	スキーマの拡張	属性 ID 要件
LDAP	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します。 • LDAP スキーマを拡張して、CiscoAVPair などの一意の名前でカスタム属性を作成します。	シスコの LDAP の実装では、Unicode タイプの属性が必要です。 CiscoAVPair カスタム属性を作成する場合は、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します 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。

認証プロバイダー	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
```

二要素認証

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ために、リクエストがトークン サーバに送信されます。Cisco UCS Manager は、トークン サーバがリクエストを AAA サーバに転送できるように、トークン サーバを AAA サーバと統合することを要求します。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+ プロバイダー 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、二要素認証がイネーブルの場合は 7200 秒、二要素認証がイネーブルでない場合は 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、二要素認証がイネーブルの場合は 8000 秒、二要素認証がイネーブルでない場合は 7200 秒です。

LDAP プロバイダーとグループ

ネストされた LDAP グループ

LDAP グループを他のグループおよびネスト グループのメンバーとして追加し、メンバー アカウントを統合してトラフィックの重複を減らすことができます。Cisco UCS Manager のリリース 2.1(2) 以降では、LDAP グループ マップで定義された他のグループ内にネストされた 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 だけを選択します。Group_1 と Group_2 を別々に検索する必要はありません。

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 プロバイダー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。

はじめる前に

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。

次の作業

LDAP プロバイダーを作成します。

LDAP プロバイダーの作成

Cisco UCS Manager では、最大 16 の LDAP プロバイダーがサポートされます。

はじめる前に

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をユーザに対して設定します。 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は、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 により使用されている仮想 IPv4 または IPv6 アドレスではありません。

- セキュアな通信を使用する場合は、LDAP サーバのルート認証局（CA）の証明書が格納されたトラスト ポイントを Cisco UCS Manager で作成します。

- 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。

（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 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属している場合や LDAP 属性で指定されたロールまたはロケールを持っている場合、Cisco UCS は、それらのグループまたは属性のいずれかにマップされているすべてのロールとロケールをそのユーザに割り当てます。

次の作業

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

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

LDAP プロバイダーの 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	Cisco UCS が、ユーザ ロールとロケールを認証してリモート ユーザに割り当てるときに、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 UCS は LDAP グループにアクセスしません。 • [Enable]：Cisco UCS は、この Cisco UCS ドメインに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 ユーザが検出されると、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属している場合やLDAP属性で指定されたロールまたはロケールを持っている場合、Cisco UCS は、それらのグループまたは属性のいずれかにマップされているすべてのロールとロケールをそのユーザに割り当てます。
[Group Recursion] フィールド	Cisco UCS が、マッピングされたグループとそれらの親グループの両方を検索するかどうか。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。ユーザが属するいずれのグループでもユーザの認証プロパティが明示的に設定されていない場合、Cisco UCS はデフォルトの設定を使用します。 • [Recursive]：Cisco UCS は、マップされた各グループおよびそのすべて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あるため、Cisco UCS は、明示的な認証プロパティ設定を備えたグループを検出すると、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 データベース内のグループ メンバーシップを判別するために使用する属性。 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] > [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 マッピングにより、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 にログインする際、LDAP グループ マップはユーザのロールとロケールに関する情報を取り出します。ロールとロケールの基準がポリシーの情報と一致する場合、アクセスが許可されます。Cisco UCS Manager は、リリース バージョンに応じて、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) は最大 128 の LDAP グループ マップをサポートし、リリース 3.1(2) 以降は最大 160 の LDAP グループ マップをサポートします。

Cisco UCS Manager でローカルに設定したロールとロケール定義に対しては、LDAP ディレクトリに対する変更に基づいた自動更新は行われません。LDAP ディレクトリ内の LDAP グループの削除や名前変更を行う場合は、その変更に合わせて 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いずれかの組み合わせを含むように設定できます。

- ロールのみ
- ロケールのみ
- ロールとロケールの両方

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 にはすぐに使用できるユーザ 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 プロバイダー 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

はじめる前に

- 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させる必要があります。

（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。

次の作業

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 プロバイダー

RADIUS プロバイダー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。

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。

次の作業

RADIUS プロバイダーを作成します。

RADIUS プロバイダーの作成

Cisco UCS Manager では、最大 16 の RADIUS プロバイダーがサポートされます。

はじめる前に

RADIUS サーバで、次の設定を行います。

- Cisco UCS Manager のユーザ ロールとロケール情報を保持する属性をユーザに対して設定します。 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 により使用されている仮想 IP アドレスではありません。

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] > [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。

（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 [Save Changes] をクリックします。

次の作業

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

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

RADIUS プロバイダーの削除

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 [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+ プロバイダー

TACACS+ プロバイダー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。

次の作業

TACACS+ プロバイダーを作成します。

TACACS+ プロバイダーの作成

Cisco UCS Manager では、最大 16 の TACACS+ プロバイダーがサポートされます。

はじめる前に

TACACS+ サーバで、次の設定を行います。

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

  cisco-av-pair 名は、TACACS+ プロバイダーの属性 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 により使用されている仮想 IP アドレスではありません。

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] > [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。

（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。

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。

次の作業

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

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

TACACS+ プロバイダーの削除

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 [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

はじめる前に

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、最初にプロバイダー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 [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 アカウントは、この Cisco UCS ドメインでローカルに定義する必要があります。 • [Radius]：ユーザは、この Cisco UCS ドメインに対して指定された RADIUS サーバで定義する必要があります。 • [Tacacs]：ユーザは、この Cisco UCS ドメインに対して指定された TACACS+ サーバで定義する必要があります。 • [Ldap]：ユーザは、この Cisco UCS ドメインに対して指定された LDAP サーバで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 ドメインに対してローカルである場合は、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] ドロップダウン リスト	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。 （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。
二要素認証	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

はじめる前に

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、最初にプロバイダー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	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 アカウントは、この Cisco UCS ドメインでローカルに定義する必要があります。 • [Radius]：ユーザ アカウントは、この Cisco UCS ドメインに対して指定された RADIUS サーバで定義する必要があります。 • [Tacacs]：ユーザ アカウントは、この Cisco UCS ドメインに対して指定された TACACS+ サーバで定義する必要があります。 • [Ldap]：ユーザ アカウントは、この Cisco UCS ドメインに対して指定された LDAP サーバで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 ドメインに対してローカルである場合は、ユーザがリモート ログインするときにパスワードは必要ありません。
[Provider Group] ドロップダウン リスト	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)	Cisco UCS Manager に接続している場合、Web クライアントは、Web セッションをアクティブに保つために、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、セッションの終了は行いません。 60 ～ 172800 の整数を指定します。デフォルト値は、二要素認証がイネーブルでない場合は 600 秒、二要素認証がイネーブルの場合は 7200 秒です。
Web Session Timeout (sec)	最後の更新要求から Cisco UCS Manager が Web セッションが非アクティブであると見なすまでの最大経過時間。この時間制限を超えると、Cisco UCS Manager は自動的に Web セッションを終了させます。 300 ～ 172800 の整数を指定します。デフォルト値は、二要素認証がイネーブルでない場合は 7200 秒、二要素認証がイネーブルの場合は 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 Session Refresh Period] が期限切れになるまでに 60 秒ある場合は、ユーザ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） 二要素認証をイネーブルにして設定を保存した後、デフォルトの Web Session Refresh Period (sec) は 7200 に、デフォルトの Web Session Timeout (sec)は 8000 に変わります。

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

次の機能を実装して、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。

- プロバイダー グループ
- 認証ドメイン

プロバイダー グループ

プロバイダー グループは、認証プロセス中に Cisco UCS がアクセスするプロバイダーのセットです。プロバイダー グループ内のすべてのプロバイダーが、ユーザの認証に Cisco UCS プロバイダー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、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 のプロバイダー グループを作成でき、グループごとに最大 8 つのプロバイダーを含めることができます。

LDAP プロバイダー 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。

（注） 単一の LDAP データベースを使用した認証では、LDAP プロバイダー グループを設定する必要はありません。

はじめる前に

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。

次の作業

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 プロバイダー グループの削除

はじめる前に

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 プロバイダー 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。

（注） 単一の RADIUS データベースを使用した認証では、RADIUS プロバイダー グループを設定する必要はありません。

はじめる前に

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 Providers] 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削除できます。

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。

次の作業

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 プロバイダー グループの削除

認証設定で使用されているプロバイダー グループは削除できません。

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。

（注） 単一の TACACS+ データベースを使用した認証では、TACACS+ プロバイダー グループを設定する必要はありません。

はじめる前に

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

認証設定で使用されているプロバイダー グループは削除できません。

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 内のプロバイダー グループと領域に関連付けられています。プロバイダー 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
名前	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。-（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。 （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 はフォーマットに 5 文字を挿入するため、ドメイン名とユーザ名を合わせた合計が 27 文字を超えると、認証は失敗します。

名前	説明
Web Session Refresh Period (sec)	Cisco UCS Manager に接続している場合、Web クライアントは、Web セッションをアクティブに保つために、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、セッションの終了は行いません。 60 ～ 172800 の整数を指定します。デフォルト値は、二要素認証がイネーブルでない場合は 600 秒、二要素認証がイネーブルの場合は 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。
Web Session Timeout (sec)	最後の更新要求から Cisco UCS Manager が Web セッションが非アクティブであると見なすまでの最大経過時間。この時間制限を超えると、Cisco UCS Manager は自動的に Web セッションを終了させます。 300 ～ 172800 の整数を指定します。デフォルト値は、二要素認証がイネーブルでない場合は 7200 秒、二要素認証がイネーブルの場合は 8000 秒です。
レルム	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 アカウントは、この Cisco UCS ドメインでローカルに定義する必要があります。 • [Radius]：ユーザは、この Cisco UCS ドメインに対して指定された RADIUS サーバで定義する必要があります。 • [Tacacs]：ユーザは、この Cisco UCS ドメインに対して指定された TACACS+ サーバで定義する必要があります。 • [Ldap]：ユーザは、この Cisco UCS ドメインに対して指定された LDAP サーバで定義する必要があります。

名前	説明
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 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。
二要素認証	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 Session Refresh Period] が期限切れになるまでに 60 秒ある場合は、ユーザ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。

第 6 章

Call Home 機能をイネーブルまたはディセーブルにする方法

- Call Home, 67 ページ
- Call Home のイネーブル化, 69 ページ
- Call Home のディセーブル化, 69 ページ

Call Home

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

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

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

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

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

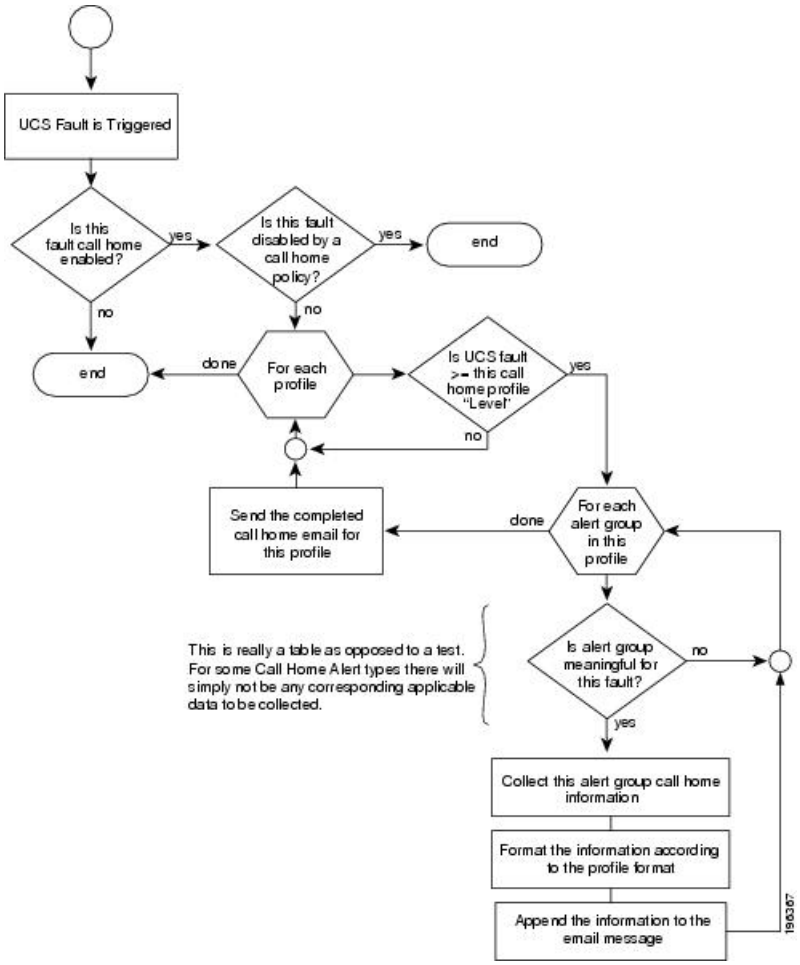
- 1 または 2 行で障害を説明する、ポケットベルや印刷レポートに適したショート テキスト フォーマット。
- 詳細な情報を十分に書式が整えられたメッセージで提供する、ユーザが読むのに適したフル テキスト フォーマット。

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

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

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

図 *1*：障害発生後のイベントの流れ



Call Home のイネーブル化

手順

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

次に、Call Home をイネーブルにし、トランザクションをコミットする例を示します。

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

次の作業

Call Home 機能の詳細については、『*Cisco UCS* システム モニタリング ガイド』を参照してください。

Call Home のディセーブル化

手順

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

次に、Call Home をディセーブルにし、トランザクションをコミットする例を示します。

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

次の作業

Call Home 機能の詳細については、『*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 7 章

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，71 ページ
- コミュニケーション サービス，71 ページ
- セキュアでないコミュニケーション サービス，73 ページ
- セキュアなコミュニケーション サービス，74 ページ
- ネットワーク関連のコミュニケーション サービス，82 ページ

コミュニケーション プロトコル

コミュニケーション サービス

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

Cisco UCS Manager 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、次のサービスをイネーブルにする必要があります。

- CIMC Web サービス

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

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イネーブルになり、**show** コマンドなど、プロトコルの一部のサブセットをサポートします。これをディセーブルにすることはできません。 このシェル サービスは、Distributed Management Task Force によって定義された標準の 1 つです。
SNMP	デフォルトでは、このサービスはディセーブルになっています。イネーブルの場合、デフォルトのポートは161です。コミュニティと少なくとも 1 つの SNMP トラップを設定する必要があります。 システムに SNMP サーバとの統合が含まれる場合にだけこのサービスをイネーブルにします。
SSH	このサービスは、ポート 22 でイネーブルになります。これはディセーブルにできず、デフォルトのポートを変更することもできません。 このサービスは Cisco UCS Manager CLI へのアクセスを提供します。
Telnet	デフォルトでは、このサービスはディセーブルになっています。 このサービスは Cisco UCS Manager CLI へのアクセスを提供します。

セキュアでないコミュニケーション サービス

CIM-XML 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 [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

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

ステップ 5 （任意） [Redirect HTTP to HTTPS] フィールドで、[Enabled] オプション ボタンをクリックします。
HTTP ログインの HTTPS ログインへのリダイレクションをイネーブルにするには、HTTPS も設定して有効にする必要があります。いったんイネーブルにすると、HTTPS をディセーブルにするまではリダイレクションをディセーブルにできません。

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

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

暗号キーとキー リング

各 PKI デバイスは、内部キー リングに非対称の Rivest-Shamir-Adleman（RSA）暗号キーのペア（1 つはプライベート、もう 1 つはパブリック）を保持します。いずれかのキーで暗号化されたメッセージは、もう一方のキーで復号化できます。暗号化されたメッセージを送信する場合、送信者は受信者の公開キーで暗号化し、受信者は独自の秘密キーを使用してメッセージを復号化します。送信者は、独自の秘密キーで既知のメッセージを暗号化（「署名」とも呼ばれます）して公開キーの所有者を証明することもできます。受信者が該当する公開キーを使用してメッセージを正常に復号化できる場合は、送信者が対応する秘密キーを所有していることが証明されます。暗号キー

の長さはさまざまであり、通常の長さは 512 ビット ～ 2048 ビットです。一般的に、短いキーよりも長いキーの方がセキュアになります。Cisco UCS Manager では、最初に 1024 ビットのキー ペアを含むデフォルトのキー リングが提供されます。その後、追加のキー リングを作成できるようになります。

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

この操作は、UCS Manager CLI のみで使用できます。

証明書

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

トラスト ポイント

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

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

キー リングの作成

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

手順

ステップ 1 [Navigation] ペインで [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。

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

c) [OK] をクリックします。

次の作業

このキー リングの証明書要求を作成します。

キー リングの証明書要求の作成

手順

ステップ 1 [Navigation] ペインで [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）。

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

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

- [IPv4] タブをクリックし、次のフィールドに値を入力します。

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

- [IPv6] タブをクリックし、次のフィールドに値を入力します。

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

ステップ 8 [OK] をクリックします。

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

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

次の作業

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

トラスト ポイントの作成

手順

ステップ 1 [Navigation] ペインで [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。
[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。

次の作業

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

キー リングへの証明書のインポート

手順

ステップ 1 [Navigation] ペインで [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。

次の作業

キー リングを使用して HTTPS サービスを設定します。

HTTPS の設定

⚠

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

手順

ステップ 1　[Navigation] ペインで [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。 • Enabled • Disabled [Admin State] がイネーブルの場合は、Cisco UCS Manager GUI に、このセクションの残りのフィールドが表示されます。
[Port] フィールド	HTTPS 接続に使用するポート。 1 ～ 65535 の整数を入力します。デフォルトでは、HTTPS はポートでイネーブルになっています。
[Operational Port] フィールド	Cisco UCS Manager がシステム レベルの HTTPS 通信を行うために必要なポート。 このポートは変更できません。

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

ステップ 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

はじめる前に

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

手順

ステップ 1 [Navigation] ペインで [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 のイネーブル化および SNMP プロパティの設定

Cisco UCS ドメインからの SNMP メッセージには、システム名ではなくファブリック インターコネクト名が表示されます。

手順

ステップ 1 [Navigation] ペインで [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。 • Enabled • Disabled システムに SNMP サーバとの統合が含まれる場合にだけこのサービスをイネーブルにします。 [Admin State] がイネーブルの場合は、Cisco UCS Manager GUI に、このセクションの残りのフィールドが表示されます。
[Port] フィールド	Cisco UCS Manager が SNMP ホストと通信するポート。デフォルト ポートは変更できません。
[Community/Username] フィールド	Cisco UCS Manager が SNMP ホストに送信するトラップ メッセージに含まれるデフォルトの SNMP v1 または v2c コミュニティ名あるいは SNMP v3 ユーザ名。 1～32 文字の英数字文字列を入力します。@（アットマーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペースは使用しないでください。デフォルトは public です。
[System Contact] フィールド	SNMP の実装を担当するシステムの連絡先。 電子メール アドレス、名前、電話番号など、255 文字までの文字列を入力します。
[System Location] フィールド	SNMP エージェント（サーバ）が実行するホストの場所。 最大 510 文字の英数字を入力します。

ステップ 5 [Save Changes] をクリックします。

次の作業

SNMP トラップおよびユーザを作成します。

CIMC Web サービスのイネーブル化

CIMC Web サービスはデフォルトでイネーブルとなっています。ディセーブルになっている場合は、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。

通信サービスのディセーブル化

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

手順

ステップ 1 [Navigation] ペインで [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 のイネーブル化

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] > [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。

第 8 章

CIMC セッション管理

- CIMC セッション管理，85 ページ

CIMC セッション管理

Cisco UCS Manager 内の 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。値は、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__ を用い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。

第 9 章

管理 IP アドレスの設定

- 管理 IP アドレス，91 ページ
- サーバの管理 IP アドレスの設定，92 ページ
- 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，97 ページ
- 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，98 ページ
- 管理 IP プール，98 ページ
- 管理 IP プールでの IPv6 アドレス ブロックの作成，99 ページ
- 管理 IP プールからの IP アドレス ブロックの削除，100 ページ
- 管理 IP プールでの IPv4 アドレス ブロックの作成，100 ページ

管理 IP アドレス

Cisco UCS ドメインの各サーバには 1 つ以上の管理 IP アドレスが必要です。これらの IP アドレスは、Cisco Integrated Management Controller（CIMC）や、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ます。Cisco UCS Manager は、これらの IP アドレスを CIMC で終端する外部アクセス用に使用します。この外部アクセスは、次のいずれかのサービスを経由することが可能です。

- 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の管理 IP アドレスとして、アウトオブバンド（OOB）アドレス（このアドレスから管理ポート経由で、トラフィックがファブリック インターコネクトを通過）、またはインバンドアドレス（このアドレスからファブリック アップリンク ポート経由で、トラフィックがファブリック インターコネクトを通過）を使用できます。サーバの CIMC にアクセスする最大 6 つの IP アドレスを設定できます（2 つはアウトオブバンド（OOB）アドレス、他の 4 つはインバンド アドレス）。

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。別のサーバにサービス プロファイルを移行するときに KVM または SoL セッションがアクティブな場合、Cisco UCS Manager はセッションを終了させ、移行完了後もその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） Cisco UCS ドメイン内のサーバまたはサービス プロファイルにすでにスタティック IP アドレスが割り当てられている場合、サーバまたはサービス プロファイルにそのスタティック 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みると、Cisco UCS Manager は IP アドレスがすでに使用中であることを警告し、設定を拒否します。

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

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

重要 Cisco UCS Manager リリース 3.1(2) 以降では、Cisco UCS M シリーズ サーバはサポートされていません。

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。
Subnet Mask	IP アドレスのサブネット マスク。
Default Gateway	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。
Subnet Mask	IP アドレスのサブネット マスク。
Default Gateway	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。
Default Gateway	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。

はじめる前に

重要 Cisco UCS Manager リリース 3.1(2) 以降では、Cisco UCS M シリーズ サーバはサポートされていません。

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。
[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

重要 Cisco UCS Manager リリース 3.1(2) 以降では、Cisco UCS M シリーズ サーバはサポートされていません。

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。静的 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。静的 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。

個別のアウトオブバンド 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 プールを設定できます。IPv4 と IPv6 アドレス ブロックの両方を含むインバンド プールを設定できます。

ヒント　サーバ CIMC に IPv4 アドレスのみを含む IP プールをインバンド IPv6 ポリシーとして割り当てたり、IPv6 アドレスのみを含む IP プールをインバンド IPv4 ポリシーとして割り当てることを回避するために、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。

次の作業

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。

名前	説明
[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。

次の作業

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。

第 10 章

UCS Manager の組織

- マルチテナント環境の組織，103 ページ
- マルチテナント環境における階層的な名前解決，104 ページ
- ルート組織下の組織の作成，106 ページ
- サブ組織下の組織の作成，106 ページ
- 組織の削除，107 ページ

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することができます。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が使用できるのは、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. ポリシーを検出したか、使用可能なリソースがプール内にある場合、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. ルート組織まで検索し、使用可能なリソースまたはポリシーを検出できない場合、Cisco UCS Manager はローカル組織に戻り、デフォルト プール内でデフォルト ポリシーまたは使用可能なリソースの検出を開始します。
4. デフォルト プール内で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を検出した場合、Cisco UCS Manager はこのポリシーまたはリソースを使用します。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 プロバイダーは、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だけにアクセスできます。

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 プールを調べます。

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 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 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 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 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。

第 11 章

バックアップと復元

- UCS でのバックアップの操作，109 ページ
- バックアップ操作の考慮事項と推奨事項，109 ページ
- 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，110 ページ
- バックアップ操作の作成，111 ページ
- バックアップ操作の実行，115 ページ
- バックアップ操作の変更，116 ページ
- 1 つまたは複数のバックアップ操作の削除，117 ページ
- バックアップ タイプ，118 ページ
- システムの復元，129 ページ

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 つしか保持できません。

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。識別を容易にし、また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ために、ファイル名を変更することを推奨します。

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て、バックアップを実行できるようになるまで管理状態をディセーブル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イネーブルに設定されるまで、バックアップ操作を実行したり、コンフィギュレーション ファイルを保存またはエクスポートしたりしません。

増分バックアップ

差分バックアップは実行できません。

完全な状態の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、完全な状態のバックアップは暗号化されます。

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

はじめる前に

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、[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] をクリックするとただちに、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 コンフィギュレーション 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。 （注） Full State バックアップ ファイルを使用した場合にのみ、バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元できます。 • [All configuration]：すべてのシステム設定と論理設定が含まれる XML ファイル。このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。このファイルは、システムの復元には使用できません。このファイルには、ローカル認証されたユーザのパスワードは含まれません。 • [System configuration]：ユーザ名、ロール、ロケールなどのすべてのシステム設定が含まれる XML ファイル。このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。このファイルは、システムの復元には使用できません。 • [Logical configuration]：サービス プロファイル、VLAN、VSAN、プール、ポリシーなどのすべての論理設定が含まれる XML ファイル。このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。このファイルは、システムの復元には使用できません。

名前	説明
[Preserve Identities] チェックボックス	このチェックボックスは、バックアップ操作の [All Configuration] および [System Configuration] タイプで選択されたままになり、次の機能が提供されます。 • [All Configuration]：vHBA、WWPN、WWNN、vNIC、MAC、UUID などのプールから取得したすべての ID がバックアップファイルに保持されます。また、シャーシ、FEX、ラック サーバの ID と、シャーシ、FEX、ラック サーバ、IOM、ブレード サーバのユーザ ラベルも保持されます。 （注） このチェックボックスが選択されていない場合、ID は再び割り当てられ、ユーザ ラベルは復旧後に失われます。 • [System Configuration]：シャーシ、FEX、ラック サーバの ID と、シャーシ、FEX、ラック サーバ、IOM、ブレード サーバのユーザ ラベルがバックアップ ファイルに保持されます。 （注） このチェックボックスが選択されていない場合、ID は再び割り当てられ、ユーザ ラベルは復旧後に失われます。 このチェックボックスがバックアップ操作の [Logical Configuration] で選択されている場合は、vHBA、WWPN、WWNN、vNIC、MAC、UUID などのプールから取得したすべての ID がバックアップ ファイルに保持されます。 （注） このチェックボックスが選択されていない場合、ID は再び割り当てられ、ユーザ ラベルは復旧後に失われます。
[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。 • [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] フィールドとそれに関連付けられている [Browse] ボタンが表示され、バックアップ ファイルの名前と場所を指定できます。 （注） [OK] をクリックした後、場所は変更できません。

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。 このオプションは特定のシステム設定でしか使用できません。 • 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。 このオプションは特定のシステム設定でしか使用できません。
[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。 （注） IPv4 または IPv6 アドレスではなくホスト名を使用する場合、 で DNS サーバを設定する必要があります。Cisco UCS ドメインが Cisco UCS Central に登録されていないか、DNS 管理が [Local] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [Global] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
[Remote File] フィールド	バックアップ コンフィギュレーション 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。

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。そのため、バックアップ操作をすぐにイネーブルにして、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 （任意） 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

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] 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) （任意） 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。

（注） 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 （任意） 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に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

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] 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。

ヒント 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
Apply	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、次のバックアップのタイプのうちの 1 つ以上を実行できます。

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

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

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

Full State バックアップ ポリシーの設定

はじめる前に

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 または IPv6 アドレスではなくホスト名を使用する場合、で DNS サーバを設定する必要があります。Cisco UCS ドメインが Cisco UCS Central に登録されていないか、DNS 管理が [Local] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [Global] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
[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。 このオプションは特定のシステム設定でしか使用できません。 • 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。 このオプションは特定のシステム設定でしか使用できません。
[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。
[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]：Cisco UCS Manager は [Schedule] フィールドで指定されたスケジュールを使用して、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。次を除く任意の文字またはスペースを使用できます。`（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。 • [Enabled]：指定時間内にバックアップが実行されない場合、Cisco UCS Manager はエラーを発生させます。 • [Disable]：指定時間内にバックアップが実行されない場合、Cisco UCS Manager はエラーを発生させません。

名前	説明
[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

はじめる前に

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 または IPv6 アドレスではなくホスト名を使用する場合、 で DNS サーバを設定する必要があります。Cisco UCS ドメインが Cisco UCS Central に登録されていないか、DNS 管理が [Local] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [Global] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。

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。 このオプションは特定のシステム設定でしか使用できません。 • 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。 このオプションは特定のシステム設定でしか使用できません。
[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 コンフィギュレーション 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]：Cisco UCS Manager は [Schedule] フィールドで指定されたスケジュールを使用して、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 が保持する設定のバックアップ 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。次を除く任意の文字またはスペースを使用できます。`（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。 • [Enabled]：指定時間内にバックアップが実行されない場合、Cisco UCS Manager はエラーを発生させます。 • [Disable]：指定時間内にバックアップが実行されない場合、Cisco UCS Manager はエラーを発生させません。
[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を使用して、Cisco UCS によるシステム設定のインポートおよびアップデートを実行できます。

- [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、インポートしたコンフィギュレーション ファイルの情報によって 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。

インポートの設定

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

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

インポート機能は、すべてのコンフィギュレーション ファイル、システム コンフィギュレーション ファイル、および論理コンフィギュレーション ファイルで使用できます。インポートは、システムがアップ状態で、稼働中に実行できます。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ディセーブルのままにしておくことはできます。Cisco UCS は、管理状態がイネーブルに設定されるまで、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 つしか保持できません。

インポート操作の作成

Full State コンフィギュレーション 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 コンフィギュレーション
- システム設定
- Logical コンフィギュレーション

はじめる前に

コンフィギュレーション ファイルのインポートに必要な次の情報を収集します。

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

手順

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]：[OK] をクリックするとただちに、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。

名前	説明
[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 ファイルをリモート サーバに保存します。Cisco UCS Manager GUI によって次の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、ユーザ名とパスワードを指定できます。 • [Local File System]：バックアップ XML ファイルをローカルの場所に保存します。Cisco UCS Manager GUI によって、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る [Filename] フィールドと [Browse] ボタンが表示されます。
[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。 このオプションは特定のシステム設定でしか使用できません。 • 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。 このオプションは特定のシステム設定でしか使用できません。
[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。 （注） IPv4 または IPv6 アドレスではなくホスト名を使用する場合、 で DNS サーバを設定する必要があります。Cisco UCS ドメインが Cisco UCS Central に登録されていないか、DNS 管理が [Local] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [Global] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。

名前	説明
[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。
[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 （任意） 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

Full State コンフィギュレーション 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 コンフィギュレーション
- システム設定
- Logical コンフィギュレーション

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] 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) （任意） 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 （任意） 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

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 [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。

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

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

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

ファブリック インターコネクトの設定の復元

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

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

はじめる前に

システム コンフィギュレーションを復元するために必要な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
Server 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。

名前	説明
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。
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再起動すると、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。

第 12 章

スケジュール オプション

- スケジュールの作成，133 ページ
- スケジュールのワンタイム オカレンスの作成，140 ページ
- スケジュールの繰り返しオカレンスの作成，142 ページ
- スケジュールからのワンタイム オカレンスの削除，145 ページ
- スケジュールからの繰り返しオカレンスの削除，146 ページ
- スケジュールの削除，146 ページ

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、[スケジュール] 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。次を除く任意の文字またはスペースを使用できます。`（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 ドメインで設定されたスケジュールを所有しています。 • [Pending Global]：Cisco UCS Manager は Cisco UCS Central にこのスケジュールを転送中です。 • [Global]：Cisco UCS Central がリモート サーバで設定された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。
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。
[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時間の最大長。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、オカレンスを実行できる最長時間を指定できます。Cisco UCS は、指定された時間内にできるだけ多くのスケジュール設定されたタスクを完了します。 デフォルトで、最長時間は [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 ウィンドウが続きます。

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 によって、[Max Duration] フィールドで指定された最長時間を超えない限り、スケジュールされたすべてのタスクが実行されます。 [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 にテキスト フィールドが表示され、このオカレンスのときに実行できるタスクの最大数を指定できます。1 ～ 65535 の整数を入力します。 （注） このスケジュールが障害抑制タスクと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	このオカレンスの間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 はシステムで処理が可能な限りの数の同時実行タスクを実行します。 • [other]：Cisco UCS Manager GUI にテキスト フィールドが表示され、このオカレンスの間に同時に実行できるタスクの最大数を指定できます。1 ～ 65535 の整数を入力します。 （注） このスケジュールが障害抑制タスクと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時間の最小長。この設定は、同時に実行できるタスクの最大数が [None] 以外の値に設定されている場合にだけ有効です。次のいずれかになります。 • [None]：Cisco UCS は次のタスクを可能な限り早く実行します。 • [other]：Cisco UCS Manager GUI に、[dd:hh:mm:ss] フィールドが表示され、Cisco UCS がタスク間で待機する最短時間を指定できます。 （注） このスケジュールが障害抑制タスクと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曜日。次のいずれかになります。 • 毎日 • 月曜日 • 火曜日 • 水曜日 • 木曜日 • 金曜日 • 土曜日 • 日曜日 • 奇数日 • 偶数日

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、最長期間に到達していない場合でも、すべての繰り返しオカレンスを開始されたその日のうちに終了します。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に、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、オカレンスを実行できる最長時間を指定できます。Cisco UCS は、指定された時間内にできるだけ多くのスケジュール設定された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 によって、[Max Duration] フィールドで指定された最長時間を超えない限り、スケジュールされたすべてのタスクが実行されます。 [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 にテキスト フィールドが表示され、このオカレンスのときに実行できるタスクの最大数を指定できます。1 ～ 65535 の整数を入力します。 （注） このスケジュールが障害抑制タスクと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	各オカレンス中に同時に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 はシステムで処理が可能な限りの数の同時実行タスクを実行します。 • [other]：Cisco UCS Manager GUI にテキスト フィールドが表示され、このオカレンスの間に同時に実行できるタスクの最大数を指定できます。1 ～ 65535 の整数を入力します。 （注） このスケジュールが障害抑制タスクと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時間の最小長。この設定は、同時に実行できるタスクの最大数が [None] 以外の値に設定されている場合にだけ有効です。次のいずれかになります。 • [None]：Cisco UCS は次のタスクを可能な限り早く実行します。 • [other]：Cisco UCS Manager GUI に、[dd:hh:mm:ss] フィールドが表示され、Cisco UCS がタスク間で待機する最短時間を指定できます。 （注） このスケジュールが障害抑制タスクと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 [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 ウィンドウが続く期間に対する制限は課せられません。 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時間の最大長。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、オカレンスを実行できる最長時間を指定できます。Cisco UCS は、指定された時間内にできるだけ多くのスケジュール設定されたタスクを完了します。 デフォルトで、最長時間は [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 ウィンドウが続きます。
[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 によって、[Max Duration] フィールドで指定された最長時間を超えない限り、スケジュールされたすべてのタスクが実行されます。 [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 にテキスト フィールドが表示され、このオカレンスのときに実行できるタスクの最大数を指定できます。1 ～ 65535 の整数を入力します。 （注） このスケジュールが障害抑制タスクと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	このオカレンスの間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 はシステムで処理が可能な限りの数の同時実行タスクを実行します。 • [other]：Cisco UCS Manager GUI にテキスト フィールドが表示され、このオカレンスの間に同時に実行できるタスクの最大数を指定できます。1～65535の整数を入力します。 （注） このスケジュールが障害抑制タスクと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時間の最小長。この設定は、同時に実行できるタスクの最大数が [None] 以外の値に設定されている場合にだけ有効です。次のいずれかになります。 • [None]：Cisco UCS は次のタスクを可能な限り早く実行します。 • [other]：Cisco UCS Manager GUI に、[dd:hh:mm:ss] フィールドが表示され、Cisco UCS がタスク間で待機する最短時間を指定できます。 （注） このスケジュールが障害抑制タスクと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。

名前	説明
[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曜日。次のいずれかになります。 • 毎日 • 月曜日 • 火曜日 • 水曜日 • 木曜日 • 金曜日 • 土曜日 • 日曜日 • 奇数日 • 偶数日
[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、最長期間に到達していない場合でも、すべての繰り返しオカレンスを開始されたその日のうちに終了します。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に、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、オカレンスを実行できる最長時間を指定できます。Cisco UCS は、指定された時間内にできるだけ多くのスケジュール設定された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 によって、[Max Duration] フィールドで指定された最長時間を超えない限り、スケジュールされたすべてのタスクが実行されます。 [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 にテキスト フィールドが表示され、このオカレンスのときに実行できるタスクの最大数を指定できます。1 ～ 65535 の整数を入力します。 （注） このスケジュールが障害抑制タスクと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	各オカレンス中に同時に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 はシステムで処理が可能な限りの数の同時実行タスクを実行します。 • [other]：Cisco UCS Manager GUI にテキスト フィールドが表示され、このオカレンスの間に同時に実行できるタスクの最大数を指定できます。1～65535の整数を入力します。 （注） このスケジュールが障害抑制タスクと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時間の最小長。この設定は、同時に実行できるタスクの最大数が [None] 以外の値に設定されている場合にだけ有効です。次のいずれかになります。 • [None]：Cisco UCS は次のタスクを可能な限り早く実行します。 • [other]：Cisco UCS Manager GUI に、[dd:hh:mm:ss] フィールドが表示され、Cisco UCS がタスク間で待機する最短時間を指定できます。 （注） このスケジュールが障害抑制タスクと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。

第 13 章

サービス プロファイル更新の遅延展開

- サービス プロファイルの遅延展開，147 ページ
- メンテナンス ポリシー，149 ページ
- 遅延展開のための保留アクティビティ，154 ページ

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、中断をともなうことや、サーバのリブートが必要になることがあります。ただし、これらの中断をともな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 は変更のロール バックのためサーバを 2 度目にリブートする必要がある場合があります。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、スケジューラとメンテナンス ポリシーには手順を制御する方法がありません。サービスプロファイルの関連付けが割り当てられたメンテナンス時間に完了しない場合、プロセスが完了するまで続行されます。たとえば、いくつかの段階の再試行やその他の問題のため、関連付けが完了しなかった場合に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、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、サーバに関連付けられたサービス プロファイル、または 1 つ以上のサービス プロファイルに関連付けられた更新中のサービス プロファイルに対して、サーバのリブートが必要になるような変更が加えられた場合の Cisco UCS Manager の対処方法を定義します。

メンテナンス ポリシーは、Cisco UCS Manager でのサービス 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する
- スケジュールで指定された時間に自動的に実行する
- 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

（注） メンテナンス ポリシーで [On Next Boot] オプションが有効で、Cisco UCS Manager リリース 3.1(1) 以降から Cisco UCS Manager リリース 2.2(8) よりも以前のリリースにダウングレードしている場合は、ファームウェアのダウングレードに失敗します。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

はじめる前に

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関する情報を含めることをお勧めします。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（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	このタイマーにより、Cisco UCS Managerがサーバをシャットダウンおよびリブートするときの時間を秒単位で指定できます。Cisco UCS Managerは、ハードシャットダウンを実行する前にメンテナンスポリシーで指定された時間が経過するまで待機します。次のいずれかになります。 • [150 Secs]：Cisco UCS Manager は、サーバのハード シャットダウンおよびリブートを実行するまで 150 秒間待機します。 • [300 Secs]：Cisco UCS Manager は、サーバのハード シャットダウンおよびリブートを実行するまで 300 秒間待機します。 • [600 Secs]：Cisco UCS Manager は、サーバのハード シャットダウンおよびリブートを実行するまで 600 秒間待機します。 • [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でリブートがいつ発生するかを決定します。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]：関連サーバに適用されるサービス プロファイルの変更に対する保留中の作業を明示的に確認します。 • [Timer Automatic]：Cisco UCS によって、すべてのサービス プロファイルの関連付けや変更は、[Schedule] フィールドに表示されるスケジュールで定義されているメンテナンス ウィンドウまで延期されます。 • [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。
[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、メンテナンス操作をいつサーバに適用できるかをスケジュールが指定します。Cisco UCS によって、スケジュールされた時間にサーバがリブートされ、サーバプロファイルの変更が完了します。

名前	説明
[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可能な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。

次の作業

ポリシーをサービス プロファイルまたはサービス プロファイル テンプレートに含めます。

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設定すると、Cisco UCS Manager ですべての保留アクティビティを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） 特定の保留中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。メンテナンス期間は、保留中の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たメンテナンス ポリシーに依存します。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禁止できません。

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禁止できません。

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禁止できません。

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禁止できません。

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。

第 14 章

UCS の障害抑制

- グローバル障害ポリシー，159 ページ
- グローバル障害ポリシーの設定，160 ページ

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うち、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] ペインで [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 • Condition • Warning
[Action on Acknowledgment] フィールド	ログがクリアされると、確認されたアクションは常に削除されます。このオプションは変更できません。
[Clear Action] フィールド	障害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 は [Length of time to retain cleared faults] セクションを表示します。 • [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 はこれらのメッセージをすべて削除します。

名前	説明
[Clear Interval] フィールド	特定の時間が経過した後に、Cisco UCS Manager が障害を自動的に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 はどの障害も自動的にクリアしません。 • [other]：Cisco UCS Manager GUI は [dd:hh:mm:ss] フィールドを表示します。
[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自動的に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。

次の作業

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。