Cisco UCS Central 管理ガイド リリース 1.4

初版：2015 年 12 月 17 日

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

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

目 次

はじめに

対象読者

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

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

表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールドのラベルのような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。

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。

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。

警告

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger.You are in a situation that could cause bodily injury.Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Cisco UCS の関連ドキュメント

ドキュメント ロードマップ

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

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

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

その他のマニュアル リソース

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

マニュアルに関するフィードバック

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

第 1 章

概要

概要

このガイドでは、Cisco UCS Central 管理設定に固有の次のコンポーネントに関する概念情報と手順情報を提供します。

- ユーザ管理
- システム管理
- ファームウェア管理
- バックアップ管理
- Smart Call Home

Cisco UCS Central ユーザ マニュアルのリファレンス

リリース 1.4 から、Cisco UCS Central のユーザ ガイドは、複数の使用事例ベースのドキュメントに分けられました。Cisco UCS Central を理解および設定するのに適切なガイドを使用できます。

ガイド	説明
Cisco UCS Central Getting Started Guide	Cisco UCS インフラストラクチャ、Cisco UCS Manager、および Cisco UCS Central について簡単に説明します。HTML5 UI の概要、Cisco UCS Central に Cisco UCS ドメインを登録する方法、およびライセンスをアクティブにする方法を説明します。

ガイド	説明
Cisco UCS Central Administration Guide	ユーザ管理、通信、ファームウェア管理、バックアップ管理、Smart Call Home などの管理タスクについて説明します。
Cisco UCS Central Authentication Guide	パスワード、ユーザ、ロール、RBAC、TACACS+、RADIUS、LDAP、SNMP などの認証タスクについて説明します。
Cisco UCS Central Server Management Guide	機器ポリシー、物理インベントリ、サービス プロファイルとテンプレート、サーバ プール、サーバのブート、サーバ ポリシーなどのサーバ管理について説明します。
Cisco UCS Central Storage Management Guide	ポートとポート チャネル、VSAN と vHBA の管理、ストレージ プール、ストレージ ポリシー、ストレージ プロファイル、ディスク グループ、ディスク グループ設定などのストレージ管理について説明します。
Cisco UCS Central Network Management Guide	ポートとポート チャネル、VLAN と vNIC の管理、ネットワーク プール、ネットワーク ポリシーなどのネットワーク管理について説明します。

第 2 章

ユーザ管理

この章は、次の項で構成されています。

UCS Central ユーザの管理

[Manage UCS Central Users Administration] ダイアログボックスでは、ユーザ、ロール、ロケール、およびパスワード プロファイルを設定できます

ステップ 1 [System Settings] アイコンから、[Users] を選択します。
これにより、[Manage UCS Central Users Administration] ダイアログボックスが開きます。

ステップ 2 設定するセクションのアイコンをクリックします。

- [Password Profile] セクションでは、[Manage UCS Central Password Profile] ダイアログボックスと同じタスクを実行できます。詳細については、 UCS Central パスワード プロファイルの管理，（4 ページ）を参照してください。
- [Roles] セクションでは、[Manage UCS Central Roles] ダイアログボックスと同じタスクを実行できます。詳細については、 UCS Central ロールの管理，（4 ページ）を参照してください。
- [Locales] セクションでは、[Manage UCS Central Locales] ダイアログボックスと同じタスクを実行できます。詳細については、UCS Central ロケールの管理，（5 ページ）を参照してください。
- [Local Users] セクションでは、[Manage UCS Central Local Users] ダイアログボックスと同じタスクを実行できます。詳細については、UCS Central ローカル ユーザの管理，（6 ページ）を参照してください。

- [Remote Users] セクションでは、[Manage UCS Central Remote Users] ダイアログボックスと同じタスクを実行できます。詳細については、UCS Central リモート ユーザの管理, （6 ページ）を参照してください。

ステップ 3 セクションごとに必要なフィールドに値を入力します。

ステップ 4 [Save（保存）] をクリックします。

UCS Central パスワード プロファイルの管理

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

ステップ 2 [Password Profile] で、[Password Strength Check] を有効にするかどうかを選択します。

ステップ 3 以前のパスワードが再利用できるようになるまでのパスワードの最小数を選択します。

ステップ 4 [Password Change During Interval] を有効にするかどうかを選択します。

ステップ 5 [Password Change Interval] を選択します。

ステップ 6 変更間隔期間のパスワードの最大数を選択します。
このフィールドは、[Password Change During Interval] が [Enabled] に設定されている場合にのみ表示されます。

ステップ 7 [Save（保存）] をクリックします。

関連トピック

UCS Central ロールの管理, （4 ページ）
UCS Central ロケールの管理, （5 ページ）
UCS Central ローカル ユーザの管理, （6 ページ）
UCS Central リモート ユーザの管理, （6 ページ）

UCS Central ロールの管理

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

ステップ 2 [Roles] で、[+] をクリックして新しいロールを作成するか、既存のロールを選択します。
ステップ 3 [Network] タブで、[+] をクリックして権限を更新および追加します。
ステップ 4 ロールの関連する権限を選択します。
ステップ 5 □ をクリックして新しい権限を適用します。
ステップ 6 ロールの [Storage]、[Server]、および [Operations] の各権限を同じように更新します。
ステップ 7 [Save（保存）] をクリックします。

関連トピック

UCS Central パスワード プロファイルの管理, （4 ページ）
UCS Central ロケールの管理, （5 ページ）
UCS Central ローカル ユーザの管理, （6 ページ）
UCS Central リモート ユーザの管理, （6 ページ）

UCS Central ロケールの管理

ステップ 1 タスク バーで、「Manage UCS Central Locales」と入力して、Enter キーを押します。
これにより、[UCS Central Locales Manage] ダイアログボックスが開きます。
ステップ 2 [Locales] で、[+] をクリックして新しいロケールを追加するか、既存のロケールを選択します。
ステップ 3 [Organizations] または [Domain Groups] をロケールに割り当てます。
a) [+] をクリックして、組織またはドメイン グループを表示します。
b) 組織またはドメイン グループを選択します。
c) □ をクリックして新しい権限を適用します。
ステップ 4 [Save（保存）] をクリックします。

関連トピック

UCS Central パスワード プロファイルの管理, （4 ページ）
UCS Central ロールの管理, （4 ページ）
UCS Central ローカル ユーザの管理, （6 ページ）
UCS Central リモート ユーザの管理, （6 ページ）

UCS Central ローカル ユーザの管理

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

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

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

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

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

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

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

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

ステップ 7 [Save（保存）] をクリックします。

関連トピック

UCS Central パスワード プロファイルの管理, （4 ページ）
UCS Central ロールの管理, （4 ページ）
UCS Central ロケールの管理, （5 ページ）
UCS Central リモート ユーザの管理, （6 ページ）

UCS Central リモート ユーザの管理

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

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

（注） このセクションは読み取り専用です。

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

関連トピック

UCS Central パスワード プロファイルの管理, （4 ページ）
UCS Central ロールの管理, （4 ページ）
UCS Central ロケールの管理, （5 ページ）
UCS Central ローカル ユーザの管理, （6 ページ）

ドメイン グループ ユーザの管理

ステップ 1 [Domain Group] > [root] をクリックします。

ステップ 2 [Settings] > [Users] をクリックします。

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

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

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

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

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

ステップ 7 [Organizations] をロケールに割り当てます。

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

ステップ 8 [Save（保存）] をクリックします。

第 3 章

システム管理

システム ポリシー

システム ポリシーは、すべての Cisco UCS Central に対して、または、ドメイン グループ レベルで設定することができます。システム ポリシーをドメイン グループ レベルで設定するには、ドメイン グループ システム ポリシー，（18 ページ）を参照してください。

UCS Central システム ポリシーには以下が含まれます。

- [Faults]：障害がクリアされたタイミング、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）を特定できます。
- [Syslog]：収集するログ ファイルのタイプとそれらを表示または保存する場所を決定できます。
- [Core Dump]：Core File Exporter を使用して、生成されたコア ファイルをエクスポートします。

UCS Central システム ポリシーの設定

[Manage UCS Central System Policies] ダイアログボックスで、障害、syslog、およびコア ダンプ エクスポートのプロパティと設定値を指定できます。

ステップ 1 [System Settings] アイコンから、[System Policies] を選択します。
これにより、[Manage UCS Central System Policies] ダイアログボックスが開きます。

ステップ 2 設定するセクションのアイコンをクリックします。

- [Fault] セクションでは、[Manage UCS Central Fault Policy] ダイアログボックスと同じタスクを実行できます。詳細については、UCS Central 障害ポリシーの管理, （12 ページ）を参照してください。
- [Syslog] セクションでは、[Manage UCS Central Syslog] ダイアログボックスと同じタスクを実行できます。詳細については、UCS Central Syslog の管理, （13 ページ）を参照してください。
- [Core Dump Export] セクションでは、[Manage UCS Central Core Dump Export] ダイアログボックスと同じタスクを実行できます。詳細については、UCS Central コア ダンプ エクスポートの管理, （15 ページ）を参照してください。

ステップ 3 セクションごとに必要なフィールドに値を入力します。

ステップ 4 [Save（保存）] をクリックします。

関連トピック

UCS Central 障害ポリシーの管理, （12 ページ）
UCS Central Syslog の管理, （13 ページ）
UCS Central コア ダンプ エクスポートの管理, （15 ページ）

機器ポリシーの管理

ステップ 1 ルートの [Domain Group] ページに移動します。

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

ステップ 3 [Equipment] で、[Basic] をクリックして、次のフィールドに値を入力します。

a) [Rack Management Action] で、新しいラック サーバが検出されたときのサーバ管理の設定方法を選択します。次のいずれかになります。

- [Auto Acknowledged]：Cisco UCS ドメインによるサーバ管理が、使用可能なサーバ接続に基づいて自動的に設定されます。

- [User Acknowledged]：Cisco UCS ドメインによるサーバ管理が、ユーザが確認するまで設定されません。

b) [MAC Address Table Aging Time] で、アイドル状態の MAC アドレスが MAC アドレス テーブルから削除されるまでの時間を選択します。次のいずれかになります。

- [Mode Default]：システムのデフォルト値が使用されます。エンド ホスト モードでは、デフォルトが 14,500 秒です。スイッチング モードでは、デフォルトが 300 秒です。
- [Never]：MAC アドレスがテーブルから削除されません。
- [Other]：[dd:hh:mm:ss] フィールドにカスタム値を入力します。

c) [VLAN Port Count Optimization] で、FI 上の CPU 負荷を軽減するために、VLAN を論理的にグループ分けしてポートの使用を最適化するかどうかを選択します。

d) [Firmware Auto Server Sync State]で、最近検出されたブレード サーバまたはラック サーバのファームウェア同期ポリシーを選択します。次のいずれかになります。

- [Auto Acknowledge]：サーバ上のファームウェアは検出後に自動的に同期されます。
- [User Acknowledged]：サーバ上のファームウェアは管理者がアップグレードを確認するまで同期されません。
- [No Action]：ファームウェアのアップグレードがサーバで開始されません。

e) [Info Action] で、情報ポリシーに Cisco UCS ドメインに接続されたアップリンク スイッチを表示するかどうかを選択します。

ステップ 4 [Discovery] をクリックして、次のフィールドに値を入力し、新しいシャーシまたは FEX を追加したときのシステムの動作を指定します。

a) [Chassis/FEX Link Action] で、シャーシまたは FEX とファブリック インターコネクト間のリンク数の最小しきい値を選択します。

b) [Chassis/FEX Link Grouping Preference] で、IOM または FEX からファブリック インターコネクトへのリンクを 1 つのポート チャネルにグループ化するかどうかを選択します。

ステップ 5 [Power] をクリックして、次のフィールドに値を入力します。

a) [Power Redundancy] で、使用する冗長電源ポリシーを選択します。次のいずれかになります。

- [N+1]：非冗長性を満たす電源装置の合計数に、冗長性を与える追加の電源装置を 1 つ加えたものです。これらすべての電源装置がオンになり、シャーシの電力負荷が均等に分担されます。追加の電源装置を設置すると、Cisco UCS によってそれらが「オフ」状態に設定されます。
- [Grid]：2 つの電源がオンになります。オンにならない場合は、シャーシに N+1 よりも高い冗長性が必要です。電源の 1 つに障害が発生しても（それにより、1 つまたは 2 つの電源装置への電力供給が失われる）、別の電力回路に接続されている残りの電源装置により、シャーシへの電力供給は継続されます。
- [Non-Redundant]：設置されたすべての電源装置がオンになり、負荷が均等に分散されます。小規模の構成（必要な電力が 2500 W 未満）に限り、1 つの電源装置でも電力を供給できます。

b) [Power Allocation Method] で、Cisco UCS ドメインで使用される電力割り当て管理モードを選択します。次のいずれかになります。

- [Policy Driven Chassis Group Cap]：電源割り当ては、関連付けられたサービス プロファイルに含まれる電力制御ポリシーによって、シャーシ レベルで設定されます。
- [Manual Blade Level Cap]：電力割り当ては、すべてのシャーシの個々のブレード サーバに設定されます。

c) [ID Soaking Interval] で、Cisco UCS Central が、割り当てられた Cisco UCS ドメインから解放されたプールエンティティが再割り当てされるまで待機する秒数を指定します。0 ～ 86400 の整数を入力します。

ステップ 6 [Save（保存）] をクリックします。

ラック ディスカバリ ポリシーの管理

ステップ 1 ルートの [Domain Group] ページに移動します。

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

ステップ 3 [Rack Discovery] で、[Basic] をクリックします。

ステップ 4 [Discovery Policy Action] で、新しいラック サーバを追加したときのシステムの動作を選択します。

- [User Acknowledged]：Cisco UCS ドメインは、ユーザから新しいサーバを検索するように指示されるまで待機します。
- [Immediate]：Cisco UCS ドメインは、自動的に新しいサーバの検出を試みます。

ステップ 5 [Policies] をクリックして、新しく検出されたサーバで実行するスクラブ ポリシーを選択します。
サーバは、選択されたサーバ プール ポリシー資格の基準を満たしている必要があります。

ステップ 6 [Save（保存）] をクリックします。

UCS Central 障害ポリシーの管理

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

ステップ 2 [Fault] で、次のフィールドに値を入力します。

（注） [Initial Severity] フィールドと [Action on Acknowledgment] フィールドは読み取り専用のため、変更できません。

1 [Flapping Interval (Seconds)] フィールドに時間を秒単位で入力します。

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。これを防止するため、Cisco UCS Central 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。その時点でどうなるかは、[Action on Clear] フィールドの設定によって異なります。

2 [Soaking Interval] で、[None] を選択するか、カスタム ソーキング間隔を選択します。

3 [Clear Interval] で、Cisco UCS Central が障害をその経過時間に基づいて自動的にクリア済みとしてマークするかどうかを選択します。

[None] を選択した場合は、障害が自動的にクリアされません。[Custom Interval] を選択した場合は、Cisco UCS が自動的に関連する間隔フィールドで指定された時間後に障害メッセージを消去します。

4 [Action on Clear] で、障害がクリアされたときのシステムの動作を選択します。

[Retain Cleared Faults] を選択した場合は、クリアされた障害が [Retention Interval] で指定された時間だけ保存されます。[Delete Cleared Faults] を選択した場合は、クリアされた障害が即座に削除されます。

5 [Action on Clear] が [Retain Cleared Faults] に設定されている場合は、[Retention Interval] で、クリア済みとしてマークされた障害を Cisco UCS で保存する時間の長さを指定します。

[Forever] を選択した場合は、Cisco UCS が経過時間に関係なくすべてのクリア済みの障害メッセージを保存します。[Custom Interval] を選択した場合は、Cisco UCS が関連する間隔フィールドで指定された時間だけクリア済みの障害メッセージを保存します。

ステップ 3 [Save（保存）] をクリックします。

関連トピック

UCS Central システム ポリシーの設定, （10 ページ）
UCS Central Syslog の管理, （13 ページ）
UCS Central コア ダンプ エクスポートの管理, （15 ページ）

UCS Central Syslog の管理

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

ステップ 2 [Syslog Sources] で、ログ ファイルを収集するソースごとに [Enabled] を選択します。
次のいずれかになります。

- 障害
- 監査
- イベント

ステップ 3 [Local Destination] で、syslog メッセージを追加して表示可能な場所を指定します。次のいずれかになります。

- [Console]：有効にした場合は、syslog メッセージがコンソールに表示されるだけでなく、ログに追加されます。表示するメッセージのログ レベルを選択します。
- [Monitor]：有効にした場合は、syslog メッセージがモニタに表示されるだけでなく、ログに追加されます。表示するメッセージのログ レベルを選択します。
- [Log File]：有効にした場合は、syslog メッセージがログ ファイルに保存されます。無効にした場合は、syslog メッセージが保存されません。ログ レベル、ファイル名、および最大ファイル サイズを選択します。

システムに保存するメッセージの最も低いレベルを選択します。システムはそのレベル以上のメッセージを保存します。ログ レベルは次のいずれかになります。

- Critical (UCSM Critical)
- Alert
- Emergency
- Error (UCSM Major)
- Warning (UCSM Minor)
- Notification (UCSM Warning)
- Information
- Debug

ステップ 4 [Remote Destination] で、プライマリ、セカンダリ、またはターシャリのどのサーバに syslog メッセージを保存するかを指定します。
リモート宛先ごとに次の情報を指定します。

- [Logging Level]：システムに保存する最も低いメッセージ レベルを選択します。リモート ファイルにそのレベル以上のメッセージが保存されます。次のいずれかになります。
  - Critical (UCSM Critical)
  - Alert
  - Emergency
  - Error (UCSM Major)

- Warning (UCSM Minor)
- Notification (UCSM Warning)
- Information
- Debug

- [Facility]：リモート宛先に関連付けられた機能。
- [Host Name/IPAddress]：リモート ログ ファイルが存在するホスト名または IP アドレス。IPv4 または IPv6 アドレス以外のホスト名を使用している場合は、Cisco UCS Central で DNS サーバを設定する必要があります。

ステップ 5 [Save（保存）] をクリックします。

関連トピック

UCS Central システム ポリシーの設定, （10 ページ）
UCS Central 障害ポリシーの管理, （12 ページ）
UCS Central コア ダンプ エクスポートの管理, （15 ページ）

UCS Central コア ダンプ エクスポートの管理

Cisco UCS は、Core File Exporter を使用して、コア ファイルが生成されるとすぐにそれらを TFTP 経由でネットワーク上の指定された場所にエクスポートします。この機能を使用すれば、コア ファイルを tar 形式でエクスポートすることができます。

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

ステップ 2 [Enable] をクリックして、コア ファイルをエクスポートします。

ステップ 3 （任意） コア ファイルを保存するために使用するリモート サーバに関する説明を入力します。

ステップ 4 [Frequency]、[Maximum No. of Files]、[Remote Copy]、および [Protocol] の各フィールドはデフォルトで設定されています。

ステップ 5 （任意） [Absolute Remote Path] に、コア ファイルをリモート サーバにエクスポートするときに使用するパスを入力します。

ステップ 6 [Remote Server Host Name/IP Address] に、TFTP 経由で接続するホスト名または IP アドレスを入力します。

ステップ 7 （任意） [TFTP Port] に、TFTP 経由でコア ファイルをエクスポートするときに使用するポート番号を入力します。デフォルト ポート番号は、69 です。

ステップ 8 [Save（保存）] をクリックします。

関連トピック

UCS Central システム ポリシーの設定, （10 ページ）
UCS Central 障害ポリシーの管理, （12 ページ）
UCS Central Syslog の管理, （13 ページ）

システム プロファイル

システム プロファイルを使用すれば、すべての Cisco UCS Central に関するインターフェイス、日付と時刻、DNS、リモートアクセス、トラストポイント、証明書情報などのシステム情報を設定することができます。

ドメイン グループ システム プロファイルを設定するには、ドメイン グループ システム プロファイル, （19 ページ）を参照してください。

UCS Central システム プロファイルの管理

ステップ 1 [System Settings] アイコンから、[System Profile] を選択します。
これにより、[Manage UCS Central System Profile] ダイアログボックスが開きます。

ステップ 2 [UCS Central] セクションで、[UCS Central System Name]、[Mode]、および仮想 IPv4 アドレスと仮想 IPv6 アドレスを表示できます。
これらの値は、最初に Cisco UCS Central を設定したときに生成されます。システム名とモードは変更できません。

ステップ 3 [Interfaces] で、次の管理ノードを確認または変更します。

- プライマリ ノード（IPv4）
- プライマリ ノード（IPv6）
- セカンダリ ノード（IPv4）
- セカンダリ ノード（IPv6）

ステップ 4 [Date & Time] で、タイム ゾーンを選択して、NTP サーバを追加します。

ステップ 5 [DNS] で、Cisco UCS Central ドメイン名を入力して、DNS サーバを追加します。

ステップ 6 [Remote Access] で、キー リングを選択します。

ステップ 7 [Trusted Points] で、[Add] をクリックして、新しいトラスト ポイントと証明書チェーンを追加します。

ステップ 8 [Certificates] では、既存のキー リングを表示したり、新しいキー リングと証明書要求を作成したりできます。

ステップ 9 [Save（保存）] をクリックします。

関連トピック

UCS Central NTP サーバの管理, （17 ページ）
UCS Central 管理ノードの管理, （17 ページ）
UCS Central DNS サーバの管理, （18 ページ）

UCS Central 管理ノードの管理

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

ステップ 2 [Management Node] で、設定するノードの名前をクリックします。

ステップ 3 [IP Address]、[Subnet Mask]、および [Default Gateway] の値を入力します。

ステップ 4 [Save（保存）] をクリックします。

関連トピック

UCS Central システム プロファイルの管理, （16 ページ）
UCS Central NTP サーバの管理, （17 ページ）
UCS Central DNS サーバの管理, （18 ページ）

UCS Central NTP サーバの管理

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

ステップ 2 [Time Zone] で、ドメインのタイム ゾーンを選択します。

ステップ 3 [NTP Servers] で、[Add] をクリックして新しい NTP サーバを追加するか、[Delete] をクリックして既存のサーバを削除します。

ステップ 4 [Save（保存）] をクリックします。

関連トピック

UCS Central システム プロファイルの管理, （16 ページ）
UCS Central 管理ノードの管理, （17 ページ）
UCS Central DNS サーバの管理, （18 ページ）

UCS Central DNS サーバの管理

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

ステップ 2 [UCS Central Domain Name] に、Cisco UCS Central ドメインの名前を入力します。

ステップ 3 [DNS Servers] で、[Add] をクリックして新しい DNS サーバを追加するか、[Delete] をクリックして既存のサーバを削除します。

ステップ 4 [Save（保存）] をクリックします。

関連トピック

UCS Central システム プロファイルの管理, （16 ページ）
UCS Central NTP サーバの管理, （17 ページ）
UCS Central 管理ノードの管理, （17 ページ）

ドメイン グループ システム ポリシー

システム ポリシーは、ドメイン グループ レベルで、または、すべての Cisco UCS Central に対して設定することができます。UCS Central のシステム ポリシーを設定するには、システム ポリシー, （9 ページ）を参照してください。

ドメイン グループ システム ポリシーには以下が含まれます。

- [Equipment]：検出ポリシーや電力ポリシーなどのドメイングループ内の機器に関するポリシーを設定できます。
- [Rack Discovery]：ラックマウント サーバが検出されたときに実行するアクションを決定し、スクラブ ポリシーを割り当てることができます。
- [Fault]：障害がクリアされたタイミング、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）を特定できます。
- [Syslog]：収集するログ ファイルのタイプとそれらを表示または保存する場所を決定できます。
- [Core Dump]：Core File Exporter を使用して、生成されたコア ファイルをエクスポートします。
- [Interfaces]：ドメイン グループ インターフェイスをモニタリングする基準を設定できます。
- [System Events]：ドメイン グループ システム イベント ログの基準を設定できます。

ドメイン グループ システム ポリシーの管理

（注） サブドメイン用のシステム ポリシーを設定する場合は、先にそれぞれのポリシーをイネーブルにする必要があります。

ステップ 1 ルートの [Domain Group] ページに移動します。

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

ステップ 3 [Equipment] で、必要なフィールドに値を入力します。
詳細については、機器ポリシーの管理, （10 ページ）を参照してください。

ステップ 4 [Rack Discovery] で、必要なフィールドに値を入力します。
詳細については、ラック ディスカバリ ポリシーの管理, （12 ページ）を参照してください。

ステップ 5 [Fault] で、必要なフィールドに値を入力します。
詳細については、UCS Central 障害ポリシーの管理, （12 ページ）を参照してください。

ステップ 6 [Syslog] で、必要なフィールドに値を入力します。
詳細については、UCS Central Syslog の管理, （13 ページ）を参照してください。

ステップ 7 [Core Dump] で、必要なフィールドに値を入力します。
詳細については、UCS Central コア ダンプ エクスポートの管理, （15 ページ）を参照してください。

ステップ 8 [Interfaces] で、[Interface Monitoring Policy] を有効にするかどうかを選択します。

ステップ 9 [Enabled] を選択した場合は、必要に応じてインターフェイス モニタリング情報を入力します。

ステップ 10 [System Events] で、必要なフィールドに値を入力して、システム イベント ログの収集方法を決定します。

ステップ 11 [Save（保存）] をクリックします。

ドメイン グループ システム プロファイル

ドメイン グループ システム プロファイルを使用すれば、ドメイン グループごとの日付と時刻、DNS 設定、リモート アクセス、およびトラスト ポイントを設定することができます。

Cisco UCS Central のシステム プロファイルを設定するには、システム プロファイル, （16 ページ）を参照してください。

ドメイン グループ システム プロファイルの管理

ステップ 1 ルートの [Domain Group] ページに移動します。
ステップ 2 [Settings] アイコンをクリックして、[System Profile] を選択します。
ステップ 3 [Date & Time] で、タイム ゾーンを選択して、NTP サーバを追加します。
ステップ 4 [DNS] で、UCS Central ドメイン名を入力して、DNS サーバを追加します。
ステップ 5 [Remote Access] で、HTTPS と HTTPS ポートを入力して、キー リングを選択します。
ステップ 6 [Trusted Points] で、[Add] をクリックして、トラスト ポイントを作成し、証明書チェーンを追加します。
ステップ 7 [Save（保存）] をクリックします。

メンテナンス ポリシー

登録されたドメイン内のサーバに関連付けられたサービス プロファイルを変更したら、サーバをリブートする必要があります。メンテナンス ポリシーによって Cisco UCS Central がリブート要求にどのように対処するかが決定されます。

メンテナンスポリシーを作成して、リブート要件を指定することによって、サービスプロファイルを変更せずに自動的にサーバがリブートされないことを確認できます。メンテナンス ポリシーに関する次のオプションのいずれかを指定できます。

- [Immediately]：サービス プロファイルを変更すると、その変更が即座に適用されます。
- [User Acknowledgment]：管理者特権を持っているユーザがシステム内の変更を承認後に変更が適用されます。
- [Schedule]：スケジュール内で指定された日付と時刻に基づいて変更が適用されます。

スケジュールを指定した場合は、メンテナンス ポリシーを作成すると、スケジュールによって最初の利用可能なメンテナンス時間中に変更が適用されます。

（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 ポリシーの作成または編集

メンテナンスポリシーの作成とそのサービスプロファイルへの関連付けに関するビデオを観るには、『Video: Creating a Global Maintenance Policy and Associating the Policy with a Service Profile』を参照してください。

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

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 リブートが必要な変更を適用するタイミングを選択します。
次のいずれかになります。

- [User Acknowledgement]：設定の変更をユーザが承認する必要があり、リブートを確認する必要があります。
- [Schedule]：設定の変更が選択されたスケジュールに基づいて適用されます。 新しいスケジュールを値のリストに追加するには、スケジュールの作成または編集, （22 ページ）を参照してください。
- [Save]：設定の変更が保存直後に適用され、リブートが実行されます。

ステップ 5 次回のリブート時に変更を適用するかどうかを選択して、[Apply Changes On] フィールド内の値を無視します。

ステップ 6 [Create] をクリックします。

スケジュールの作成または編集

（注） 繰り返し実行か、ワンタイム実行かに関係なく、単純なスケジュールには、ユーザの承認を必要とするオプションはありません。ユーザの承認が必要な場合は、高度なスケジュールを選択する必要があります。

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

ステップ 2 [Basic] で、[Name] とオプションの [Description] を入力します。

ステップ 3 スケジュールを [Recurring]、[One Time]、または [Advanced] のどれにするのかを選択します。
[Advanced] の場合は、ユーザの承認が必要かどうかを選択します。

ステップ 4 [Schedule] で、次の手順を実行します。

a) [Recurring] スケジュールの場合は、開始日、頻度、時刻、およびその他のプロパティを選択します。
b) [One Time] スケジュールの場合は、開始日、時刻、およびその他のプロパティを選択します。
c) [Advanced] スケジュールの場合は、スケジュールの名前を入力して、ワンタイム スケジュールを使用するのか、繰り返しスケジュールを使用するのかを選択し、その他のプロパティの値を選択します。

ステップ 5 [Create] をクリックします。

キー リング

Cisco UCS Central では、より強力な認証のためにキー リングをサードパーティの証明書として作成できます。HTTPS は 2 つのデバイス間でセキュアな通信を確立するために Public Key Infrastructure（PKI）コンポーネントを使用します。

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 2048 ビット ～ 4096 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 Central では、最初に 2048 ビットのキー ペアを含むデフォルトのキー リングが提供されます。そして、追加のキー リングを作成できます。

（注） デフォルトのキー リングを作り直した場合は、その後の Cisco UCS Central へのログインに数分かかります。

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。

（注） キー リングおよび証明書要求を作成すると、Cisco UCS Central によって必要なキー用途セットを含む証明書要求が生成されます。CA サーバから署名された証明書に対するキー用途には、**SSL クライアント認証**と **SSL サーバ認証**を含める必要があります。内部 CA として Microsoft Windows Enterprise Certificate Authority Server を使用する場合は、**コンピュータ** テンプレートを使用して、これらのキー用途セットの両方を含む証明書を生成する必要があります。このテンプレートがセットアップで使用できない場合は、**SSL クライアント認証**と **SSL サーバ認証**の両方のキー用途セットを含む適切なテンプレートを使用する必要があります。

キー リングの作成

ステップ 1 メニュー バーで、[System Profile] をクリックします。
ステップ 2 [Certificates] をクリックして、すべてのフィールドに値を入力します。
ステップ 3 [OK] をクリックします。
ステップ 4 [Save（保存）] をクリックします。

トラスト ポイントの作成

Cisco UCS Central では、ルート認証局（CA）および従属 CA の証明書がバンドル形式で含まれているトラスト ポイントを作成できます。ルート CA にはプライマリ証明書と自己署名証明書が含まれている必要があります。

ステップ 1 メニュー バーで、[System Profile] をクリックします。
ステップ 2 [Trusted Points] をクリックします。
ステップ 3 [Trusted Points] で、+ アイコンをクリックして、すべてのフィールドに値を入力します。
ステップ 4 [OK] をクリックします。
ステップ 5 [Save（保存）] をクリックします。

障害とログのモニタリング

Cisco UCS Central を使用すれば、障害ログ、監査ログ、セッション、およびその他のイベントを表示できます。

（注） 表示している画面やウィジェットが最新でない場合は、更新アイコンをクリックして最新のデータを表示します。

システム障害

Cisco UCS Central は、Cisco UCS Central のシステム障害を収集して、そのすべてを [Fault Logs] ページに表示します。これらのシステム障害ログを表示するには、[Alerts] アイコンをクリックして、[System Faults] を選択します。[Faults Logs] ページでは、障害のタイプと重大度レベルに関する情報が表示され、システム障害を監視して認識したり、表示する障害を絞り込んだりすることができます。

障害テーブルには、障害ごとに次の情報が表示されます。

- [Code]：障害に関連付けられた ID
- [Timestamp]：障害が発生した日付と時刻
- [Type]：障害の発生元
- [Cause]：障害の原因
- [Affected Object]：この障害の影響を受けるコンポーネント
- [Fault Details]：障害の詳細
- [Severity]：障害の重大度
- [Action]：障害に必要なアクション

収集された情報を管理するには、UCS Central システム ポリシーの設定, （10 ページ）を参照してください。

UCS ドメインの障害

Cisco UCS Central は、UCS ドメインの [Faults Log] ページに、登録された Cisco UCS ドメインからの障害を収集して表示します。障害はタイプと重大度レベル別に表示されます。障害タイプをク

リックすると、その障害が発生した具体的なCisco UCS ドメインが展開され、確認できます。UCS ドメイン障害ログは次のようにカテゴリ別に表示されます。

- [Fault Level]：プロファイルをトリガーする障害レベル。次のいずれかになります。
  - [Critical]：1 つ以上のコンポーネントに重大な問題があります。これらの問題を調査し、すぐに修正する必要があります。
  - [Major]：1 つ以上のコンポーネントに深刻な問題があります。これらの問題を調査し、すぐに修正する必要があります。
  - [Minor]：1 つ以上のコンポーネントにシステム パフォーマンスに悪影響を及ぼす可能性のある問題があります。これらの問題を調査し、重大な問題や緊急の問題に発展する前にできるだけ早く修正する必要があります。
  - [Warning]：1 つ以上のコンポーネントに問題が解消されなければシステム パフォーマンスに悪影響を及ぼす可能性のある潜在的な問題があります。これらの問題を調査し、問題が悪化する前にできるだけ早く修正する必要があります。
  - [Healthy]：ドメイン内のどのコンポーネントにも障害がありません。
  - [Unknown]：ドメイン内のどのコンポーネントにも障害がありません。
- [No Of Domains]：それぞれの重大度レベルで障害が発生したドメインの数。
- [Domain]：障害が発生したドメイン。 タイプをクリックすると、そのタイプの障害が 1 つ以上発生している Cisco UCS ドメインと障害の詳細が表示されます。
- [Critical]：Cisco UCS ドメイン内の選択したタイプの重大障害の件数。
- [Major]：Cisco UCS ドメイン内の選択したタイプのメジャー障害の件数。
- [Minor]：Cisco UCS ドメイン内の選択したタイプのマイナー障害の件数。
- [Warning]：Cisco UCS ドメイン内の選択したタイプの警告障害の件数。

このテーブルは、[UCS Domain Faults] ページでドメインを選択したときにだけ表示されます。

- [Filter]：テーブル内のデータをフィルタ処理できます。
- [ID]：障害に関連付けられた一意の識別子。
- [Timestamp]：障害が発生した日付と時刻。
- [Type]：障害の発生場所に関する情報。
- [Cause]：障害の原因の簡単な説明。
- [Affected Object]：この問題の影響を受けるコンポーネント。
- [Fault Details]：ログ メッセージに関する詳細情報。
- [Severity]：障害の重大度を示すアイコンが表示されます。 テーブルの下にアイコン キーが表示されます。

イベント ログ

Cisco UCS Central は、ユーザがログインしたときやシステムでエラーが発生したときなど、システムで発生したイベントを収集して表示します。このようなイベントが発生すると、システムがそのイベントを**イベント ログ**に記録して表示します。このイベントログを確認するには、メニューバーで [Alerts] アイコンをクリックして、[Events] を選択します。イベントログには以下に関する情報が記録されます。

- [ID]：障害を引き起こしたイベントに関連付けられた一意の識別子
- [Timestamp]：イベントが発生した日付と時刻
- [Trig. By]：イベントに関連付けられたユーザのタイプ
- [Affected Object]：イベントの影響を受けるコンポーネント

監査ログ

Cisco UCS Centralの**監査ログ**では、設定変更の包括的なリストを表示できます。Cisco UCS Central GUI または Cisco UCS Central CLI で作成、編集、または削除タスクに関する設定変更を実施したときに、Cisco UCS Central が監査ログを生成します。設定に関連した情報に加えて、以下に関する情報が監査ログに記録されます。

- アクセスされたリソース。
- イベントが発生した日付と時刻。
- ログ メッセージに関連付けられた一意の識別子。
- 監査ログが生成されるアクションをトリガーしたユーザ。これは、内部セッションの場合と Cisco UCS Central GUI または Cisco UCS Central CLI を使用して変更を加えた外部ユーザの場合があります。
- アクションをトリガーしたソース。
- 影響を受けるコンポーネント。

コア ダンプ

システムがクラッシュするエラーが発生した場合に、コア ダンプ ファイルが作成されます。このコア ダンプ ファイルには、エラーが発生する前のシステムの状態やシステムがクラッシュした時刻などに関する情報が含まれています。コア ダンプ ファイルを表示するには、メニュー バーで [Alerts] アイコンをクリックして、[Core Dumps] を選択します。[Core Dumps] ログ テーブルで、次の情報を確認できます。

- [Timestamp]：コア ダンプ ファイルが作成された日時。
- [Name]：コア ダンプ ファイルの完全名。

- [Description]：コア ダンプ ファイルのタイプ。

アクティブ セッション

Cisco UCS Central でリモート ユーザとローカル ユーザのアクティブ セッションを表示して、サーバからそれらのセッションを終了することができます。アクティブ セッションを表示するには、メニュー バーで [Alerts] アイコンをクリックして、[Sessions] を選択します。[Active Sessions] ログ テーブルで、次の情報を確認することができます。

- [ID]：ユーザがログインした端末のタイプ。
- [Timestamp]：ユーザがログインした日付と時刻。
- [User]：ユーザ名。
- [Type]：ユーザがログインした端末のタイプ。
- [Host]：ユーザがログインした IP アドレス。
- [Status]：セッションが現在アクティブかどうか。
- [Actions]：[Terminate] をクリックすると、選択したセッションが終了します。

内部サービス

内部サービス ログは、さまざまなプロバイダーとそれらのプロバイダーに関連付けられた Cisco UCS Central のバージョンに関する情報を提供します。内部サービスを表示するには、メニュー バーで [Alerts] アイコンをクリックして、[Sessions] を選択します。

[Internal Services] ページの [Services] セクションで、次の情報を表示できます。

- [Name]：プロバイダーのタイプ。
- [Last Poll]：Cisco UCS Central がプロバイダーを最後にポーリングした日付と時刻。
- [IP Address]：プロバイダーに関連付けられた IP アドレス。
- [Version]：プロバイダーに関連付けられた Cisco UCS Central のバージョン。
- [Status]：プロバイダーの稼働状態。

[Internal Services] ページの [Clean Up] セクションで、次の情報を表示できます。

- [Domain]：ドメイン名。
- [Last Poll]：Cisco UCS Central がプロバイダーを最後にポーリングした日付と時刻。
- [Lost Visibility]：Cisco UCS Central がプロバイダーを認識できなくなった時点。
- [Clean Up]：[Clean Up] をクリックすると、Cisco UCS Central からこの Cisco UCS ドメインのすべての参照が削除されます。

（注） ドメインは、Cisco UCS Central に再登録しないかぎり、Cisco UCS Central で再び管理することはできません。

Tomcat ロギングのイネーブル化

手順の概要

1. UCSC # **scope monitoring**
2. UCSC /monitoring # **scope sysdebug**
3. UCSC /monitoring/sysdebug # **scope mgmt-logging**
4. UCSC /monitoring/sysdebug/mgmt-logging # **set module tomcat_config** [**crit** | **debug0** | **debug1** | **debug2** | **debug3** | **debug4** | **info** | **major** | **minor** | **warn**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	UCSC # **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCSC /monitoring # **scope sysdebug**	sysdebug モードを開始します。
ステップ 3	UCSC /monitoring/sysdebug # **scope mgmt-logging**	管理ロギング モードを開始します。
ステップ 4	UCSC /monitoring/sysdebug/mgmt-logging # **set module tomcat_config** [**crit**	**debug0**	**debug1**	**debug2**	**debug3**	**debug4**	**info**	**major**	**minor**	**warn**]	ロギング レベルを設定します。

次に、tomcat ロギングをレベル デバッグ 4 に設定する例を示します。

```
UCSC # scope monitoring
UCSC /monitoring # scope sysdebug
UCSC /monitoring/sysdebug # scope mgmt-logging
UCSC /monitoring/sysdebug/mgmt-logging # set module tomcat_config debug4
UCSC /monitoring/sysdebug/mgmt-logging #
```

API 通信レポート

Cisco UCS Central 1.4 を使用すれば、Cisco UCS Central GUI から GUI とバックエンド間のアクティブな API 通信に関するレポートを生成できます。このような通信を収集してサードパーティの自動化に使用することができます。このレポートはアクティブな通信中にいつでも収集を開始または停止することができます。

- セッションのロギングを停止したら、レポートを GUI からテキスト ファイルとして使用できます。このファイルを後で使用する場合は、ローカルデスクトップに保存してください。
- 記録中にログアウトした場合やセッションが期限切れになった場合は、テキストファイルが生成されません。

API 通信レポートの生成

ステップ 1 メニュー バーで、操作アイコンをクリックして、[Start Logging Session] を選択します。
システムが Cisco UCS Central GUI とバックエンド間のアクティブな API 通信のロギングを開始します。

ステップ 2 メニュー バーで、操作アイコンをクリックして、[Stop Logging Session] を選択します。
ポップアップ ダイアログボックスに、API レポートのテキスト ファイルを開いたり保存したりするためのオプションが表示されます。

ステップ 3 オプションを選択して、[OK] をクリックし、ファイルを開いたり保存したりします。

第 4 章

ファームウェア管理

ファームウェア管理

Cisco UCS Central では、登録されているすべての Cisco UCS ドメインのすべてのファームウェア コンポーネントを管理することができます。すべてのファームウェア更新のステータスが、[Domains] セクションに表示されます。

- [Firmware Ready]：ファームウェアは正常に更新されています。
- [In Progress]：ファームウェア更新が現在進行中です。
- [Pending User Ack]：ファームウェアを更新する前に、[Alerts] > [Pending Activities] ページでユーザ承認が必要です。

（注） Cisco UCS Central から Cisco UCS ドメインのファームウェアを管理するには、Cisco UCS Manager でグローバル ファームウェア管理オプションをイネーブルにする必要があります。グローバル ファームウェア管理オプションは、Cisco UCS Manager を Cisco UCS Central に登録するときにイネーブルにできます。また、管理要件に基づいてグローバル管理オプションのオン/オフを切り替えることもできます。

Cisco UCS ドメインは、Cisco UCS Central のドメイン グループに管理目的で分類されます。ファームウェアは、ドメイン グループ レベルで各ドメイン グループごとに別個に管理することも、ドメイン グループのルートからドメイン グループ全体に対して管理することもできます。Cisco UCS Central には、次の Cisco UCS ドメインのファームウェア パッケージを管理するオプションがあります。

- **機能カタログ**：ドメイン グループごとに機能カタログを 1 つ使用します。特定のドメイン グループに登録されたすべての Cisco UCS ドメインによって、ドメイン グループで定義された機能カタログが使用されます。

- **インフラストラクチャ ファームウェア**：ドメイン グループごとにインフラストラクチャ ファームウェア ポリシーを 1 つ使用します。特定のドメイン グループに登録されたすべての Cisco UCS ドメインによって、ドメイン グループで定義された同じインフラストラクチャ ファームウェア バージョンが使用されます。

イメージ ライブラリ

Cisco UCS Central のイメージ ライブラリには、Cisco.com から Cisco UCS Central のローカル ファイル システムとリモート ファイル システムにダウンロードされたすべてのファームウェア イメージのリストが表示されます。

- [Packages] タブに、すべてのファームウェア パッケージが表示されます。
- [Downloads] タブで、ダウンロードのステータスをモニタすることができます。

これらのファームウェア イメージは、ファームウェア ポリシーの作成に使用できます。

グローバル設定に関して実行できることは次のとおりです。

- イメージを選択して、[Delete] アイコンをクリックすることによって、イメージ ライブラリからダウンロードされたイメージを削除する。

（注） 削除しようとしているファームウェア イメージがスケジュールされたポリシーから参照されている場合は、削除操作が失敗します。このポリシーはイメージ ライブラリから削除できません。

- [Flash] アイコンをクリックすることによって、ファームウェア イメージと Cisco.com 上のイメージを同期させます。

ファームウェア バンドルのインポート

Cisco.comからファームウェア バンドルをダウンロードして、ローカルデスクトップまたはサポートされているリモート ファイル システムに保存されていることを確認してください。

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

ステップ 2 [Firmware] ページで、[Operations] アイコンをクリックして、[Import Firmware Bundle] を選択します。これにより、[Import Firmware Bundle] ダイアログボックスが開きます。

ステップ 3 ローカル システムにファームウェア バンドルを含む BIN ファイルが存在する場合は、

a) [FW Bundle Location] で、[Local] をクリックします。
b) [File Name] フィールドで、ファイル アイコンをクリックしてローカル ブラウザを開きます。

c) ファイルの場所から、BIN ファイルを選択して、[Import] をクリックします。

ステップ 4 リモート ファイル システムにファームウェア バンドルが存在する場合は、

（注） リモート ファイル システムのホスト名、ユーザ名、およびパスワードがわかっていることを確認してください。

a) [FW Bundle Location] で、[Remote] をクリックします。
これにより、サポートされているファイル転送プロトコルが表示されます。

b) ファイルをインポートするオプションのいずれかを選択して、フィールドに必要な情報を入力し、[Import] をクリックします。
たとえば、リモート サーバ上の BIN ファイル `ucs-k9-bundle-infra.2.2.3a.A.bin` を使用する場合は、絶対パス /home/cisco-ucs-central/firmware/ucs-k9-bundle-infra.2.2.3a.A.bin を入力します。

次の作業

ファームウェア バンドルを適切なポリシーに追加して、アップグレードを実行します。

アップグレードが完了したら、Cisco UCS Central からファームウェア バンドルを削除できますが、先に、関連するすべてのポリシーから削除する必要があります。

Cisco.com からの自動ファームウェア更新同期起動の有効化

Cisco.com 上の最新のファームウェア バンドルにアクセスするには、有効な Cisco.com ユーザ名とパスワードを持っている必要があります。

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

ステップ 2 該当するフィールドに Cisco.com ユーザ名とパスワードを入力します。

ステップ 3 Cisco UCS Central で新しいファームウェアのアップデートを自動的にダウンロードする場合：

a) [Sync FW Updates Periodically] フィールドで、[Enable] をクリックします。

b) [Frequency] フィールドで、必要な頻度を選択します。

（注） このフィールドで [On Demand] を選択した場合は、Cisco UCS Central が自動的に新しいファームウェアのアップデートをダウンロードしません。代わりに、このダイアログボックスの [Sync] ボタンを使用して手動でダウンロードする必要があります。

ステップ 4 システムから HTTP 経由で Cisco.com にアクセスできるようにする場合は、[HTTP Proxy To Access Cisco.com] フィールドで [Enabled] を選択して、該当するフィールドに HTTP 接続情報を入力します。

（注） この機能には、Cisco UCS Central が Cisco.com へのネットワーク アクセスを備えている必要があります。必要に応じて、プロキシ サーバ設定を有効にして適用してください。

ステップ 5 [Sync] をクリックします。

インフラストラクチャファームウェアのアップデートのスケジューリング

ドメイン グループ内のすべてのサーバのインフラストラクチャ ファームウェア更新をスケジュールできます。

ステップ 1 タスク バーで、「Schedule Infra Firmware Update」と入力して、Enter キーを押します。
これにより、[Schedule Infra Firmware Update] ダイアログボックスが表示されます。

ステップ 2 [Domain Group for UCS Infra Update] ドロップダウン リストで、ドメイン グループを選択します。
Cisco UCS Central に、ファームウェア アップグレードの影響を受けるドメインの数と、それらのドメインの Cisco UCS Manager バージョンが表示されます。

ステップ 3 ファブリック インターコネクト用のドロップダウン リストで使用するファームウェア バージョンを選択します。

ステップ 4 （任意） [Catalog Version] ドロップダウン リストで、カタログ バージョンを選択します。

ステップ 5 [FW Update Maintenance Window] フィールドで、メンテナンス ウィンドウの日付と時刻を選択します。

ステップ 6 [User Acknowledgement Required To Install] フィールドで、サーバのリブートにユーザの承認が必要かどうかを選択します。

- [Enabled]：選択したドメイン グループ内のサーバがリブートする前に、ユーザがリブート要求を手動で承認する必要があります。
- [Disabled]：選択されたドメイン グループ内のサーバは、必要に応じて更新中に自動的にリブートされます。

ステップ 7 [Schedule] をクリックします。
[Firmware] ページでファームウェア更新を監視できます。ファームウェア管理, （31 ページ）を参照してください。

ホスト ファームウェア パッケージ ポリシーの作成または編集

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

ステップ 2 [Basic] タブで、[Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 環境の要件に応じて、ファームウェアの [Blade Version]、[Rack Version]、または [Modular Version] を選択します。

ステップ 5 [Components] タブで、プラス アイコンをクリックしてファームウェアのアップデートから除外するコンポーネントを選択します。
含まれるコンポーネントと除外されたコンポーネントが表示されます。

（注） 除外されたコンポーネントは、Cisco UCS Manager リリース 2.2.6 以前で登録されたドメインではサポートされません。

ステップ 6 除外されたコンポーネントを削除するには、コンポーネントのチェックボックスを選択し、ごみ箱アイコンをクリックします。

ステップ 7 [Create] をクリックします。

第 5 章

バックアップ管理

バックアップと復元

Cisco UCS Central を使用すれば、Cisco UCS Central と登録された UCS ドメインをバックアップして復元することができます。バックアップおよび復元ポリシーをスケジュールすることも、Cisco UCS Central または選択したドメインの即時オンデマンド バックアップを実行することもできます。

[Backup & Restore] ページから、Cisco UCS Central と登録された Cisco UCS ドメインの完全状態バックアップをスケジュールできます。Cisco UCS ドメインの場合は、完全状態バックアップ ポリシーをローカルに作成することもできます。

スケジュールされたバックアップ ポリシーはデフォルトで無効にされます。Cisco UCS Central または登録された UCS ドメインをバックアップする場合は、両方のバックアップ状態を有効にする必要があります。バックアップ プロセスが、サーバまたはネットワーク トラフィックを中断または変更することはありません。バックアップは、ドメイン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が保存されます。

リモートで設定されたポリシーは、バックアップに関して、Cisco UCS Managerによって内部的にマウントされた Cisco UCS Central リポジトリを使用するように制限されます。

定期バックアップをスケジュールすると、バックアップ リポジトリがデータの収集を開始できます。バックアップ アーカイブを管理するために、保存されているバックアップ バージョンの最大数を指定できます。ポリシー仕様を使用して、各 Cisco UCS ドメインで維持するバックアップの数を指定します。

（注） この最大数は、リモート ロケーションに保存できるバックアップ イメージ ファイルの数には影響しません。

また、Cisco UCS Central GUI から各 Cisco UCS ドメインのバックアップのリストを表示し、保存済みまたは未使用のバックアップ ディレクトリおよび設定を削除できます。

重要

- 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。
- バックアップは、Cisco UCS ドメイン（バックアップが取得された）の登録が解除されてからしか削除できません。

バックアップ イメージ ファイル

データベースまたは設定のバックアップ ファイルは次の場所に保存できます。

- **ローカル ファイル システム**：ローカル ファイル システム内。
- **リモートの場所**：TFTP、FTP、SCP、SFTP などのプロトコルを使用したリモートの場所。

重要 イメージ ファイルをリモートの場所に保存するためのオプションを使ってグローバル バックアップ ポリシーを指定するには、Cisco UCS Manager リリース 2.2(2x) 以降を Cisco UCS Central に登録する必要があります。

バックアップのスケジュール時に、いずれかのシステムに保存するバックアップ ファイルの最大数を指定できます。

設定の復元

Cisco UCS Central の完全状態バックアップを復元できるのはセットアップ中だけです。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。

Cisco UCS Manager では、初期設定中にファブリック インターコネクトのコンソールから完全状態バックアップ設定を復元できます。

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 Central 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 Central 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 タイプを変更する必要があります。バックアップ タイプの識別を容易にし、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 Central 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

Cisco UCS Manager または Cisco UCS Central の増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。

Cisco UCS Manager からのバックアップ

Cisco UCS Manager で all-config バックアップを実行すると、グローバル VLAN および VSAN を含むポート設定は復元されません。このポートは、Cisco UCS Central から再設定する必要があります。

Cisco UCS Central の完全状態バックアップのスケジューリング

バックアップのスケジューリングに関するビデオを観るには、『Video: Creating Scheduled Backup for UCS Central』を参照してください。

はじめる前に

リモートの場所を指定する場合は、その場所が存在することを確認してください。バックアップ ファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。たとえば、転送プロトコルが SCP の場合：`scp://user@<ip>/x/y/z`
- リモート サーバのホスト名または IP アドレス

- リモート サーバのユーザ名とパスワード

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

ステップ 2 （任意） [Description] フィールドに、このバックアップ ポリシーの説明を入力します。

ステップ 3 [Schedule] ドロップダウンから、このバックアップのスケジュールを選択します。次のいずれかになります。

- [One Time Schedules]：バックアップはスケジュールされた日付と時刻にのみ行われます。
- [Recurring Schedules]：バックアップはスケジュールされた頻度で行われます。

（注） この完全状態バックアップと事前定義されたスケジュールを関連付ける必要があります。スケジュールを作成するには、スケジュールの作成または編集, （22 ページ）を参照してください。

ステップ 4 [Maximum No of Backup Files] フィールドで、システムに保存するバックアップ ファイルの数を指定します。
バックアップ ファイルの最大数に達すると、最も古いバックアップ ファイルが最も新しいバックアップ ファイルで上書きされます。

ステップ 5 （任意） バックアップ ファイルをリモートの場所に保存する場合は、[Remote Copy] フィールドで、[Enabled] をクリックします。
次のフィールドに値を入力して、リモートの場所に関する情報を追加します。

名前	説明
[Transfer Protocol]	転送プロトコルを選択します。次のいずれかにすることができます。 • FTP • SFTP • TFTP • SCP
[Absolute Remote Path] フィールド	絶対リモート パス。
[Remote Server Host Name/IP Address] フィールド	リモート サーバの IP アドレス。
[User Name] フィールド	リモート サーバのユーザ名。
[Password] フィールド	リモート サーバのパスワード。

Cisco UCS ドメインの完全状態バックアップのスケジューリング

登録された Cisco UCS ドメインの完全状態バックアップはドメイン グループ レベルでしか作成できません。

バックアップのスケジューリングに関するビデオを観るには、『Video: Creating Scheduled Backup for a UCS Domain』を参照してください。

はじめる前に

リモートの場所を指定する場合は、その場所が存在することを確認してください。バックアップ ファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。たとえば、転送プロトコルが SCP の場合：`scp://user@<ip>/x/y/z`
- リモート サーバのホスト名または IP アドレス
- リモート サーバのユーザ名とパスワード

ステップ 1 [Domain Group] ドロップダウン オプションをクリックして、完全状態バックアップをスケジュールするドメイン グループを選択します。
この選択によって、[Schedule] オプションと [No of Backup Files] オプションが表示されます。

ステップ 2 [Schedule] ドロップダウンから、このバックアップのスケジュールを選択します。次のいずれかを指定できます。

- [Simple]：1 つのワンタイム実行または繰り返し実行を作成します。
- [Advanced]：複数のワンタイム実行または繰り返し実行を作成します。

（注） この完全状態バックアップと事前定義されたスケジュールを関連付ける必要があります。

ステップ 3 [Maximum No of Backup Files] フィールドで、システムに保存するバックアップ ファイルの数を指定します。

ステップ 4 （任意） バックアップ ファイルをリモートの場所に保存する場合は、[Remote Copy] フィールドで、[Enabled] をクリックします。
次のフィールドに値を入力して、リモートの場所に関する情報を追加します。

名前	説明
[Transfer Protocol]	転送プロトコルを選択します。次のいずれかにすることができます。 • FTP • SFTP • TFTP • SCP
[Absolute Remote Path] フィールド	絶対リモート パス。
[Remote Server Host Name/IP Address] フィールド	リモート サーバの IP アドレス。
[User Name] フィールド	リモート サーバのユーザ名。
[Password] フィールド	リモート サーバのパスワード。

オンデマンド完全状態バックアップの作成

いつでも Cisco UCS Central の完全状態バックアップを作成して、ファイルをローカルの場所とリモートの場所の両方に保存できます。ただし、登録済みの Cisco UCS ドメインでは、バックアップをリモートの場所でしか作成することができません。

オンデマンドバックアップの作成に関するビデオを観るには、『Video: Creating On-Demand Backup for UCS Central』または『Video: Creating On-Demand Backup for a UCS Domain』を参照してください。

はじめる前に

オンデマンドバックアップファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。たとえば、転送プロトコルが SCP の場合：
  `scp://user@ipaddress/x/y/backup_filename.tgz`
- リモート サーバのホスト名または IP アドレス

- リモート サーバのユーザ名とパスワード

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

ステップ 2 [UCS Central] をクリックするか、ドメイン グループを選択します。

ステップ 3 [Backup] アイコンをクリックします。
これにより、[Create Backup] ダイアログボックスが開きます。

ステップ 4 Cisco UCS Central の完全状態バックアップの場合は、[Remote Copy] を有効にするか、無効にするかを選択します。
[Disabled] を選択した場合は、ローカル バックアップ コピーが作成され、ステップ 6 に進むことができます。

ステップ 5 [Transfer Protocol] を選択して、必要なリモートの場所に関する情報を入力します。

ステップ 6 [Create] をクリックします。

完全状態バックアップ ファイルが、指定されたリモートの場所に作成され、保存されます。Cisco UCS ドメインのバックアップ状態を確認するには、ドメイン グループ名をクリックします。

（注） Cisco UCS Central または Cisco UCS Manager のオンデマンド完全状態バックアップが失敗すると、次のエラー メッセージが表示されます。
End point timed out.Check for IP, password, space or access related issues.
このエラーを修正するには、設定を再送信します。再送信が成功すると、バックアップ ファイルがバックアップ リポジトリ内に作成されます。

Cisco UCS ドメインの完全状態バックアップの削除

後述する手順に加えて、次のシナリオで完全状態バックアップを無効化/削除することができます。

- ルート ドメイン グループ ポリシーを削除すると、バックアップ/エクスポート ポリシーが無効になります。
- サブドメイン グループ ポリシーを削除すると、バックアップ/エクスポート ポリシーが削除されます。

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

ステップ 2 [Schedule] アイコンをクリックして、[Remove Domain Backup Schedule] を選択します。
これにより、[Remove Domain Backup Schedule] ダイアログボックスが開きます。

ステップ 3 バックアップを削除する [Domain Group] を選択します。

ステップ 4 選択後に表示されるフィールド内の情報を調べて、これが削除するバックアップ スケジュールであることを確認します。

ステップ 5 [Remove] をクリックします。

Cisco UCS Central の完全状態バックアップの削除

後述する手順に加えて、次のシナリオでは、Cisco UCS Central の完全状態バックアップを無効化または削除することができます。

- Cisco UCS Central ポリシーを削除すると、バックアップ/エクスポート ポリシーが無効になります。

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

ステップ 2 [Schedule] アイコンをクリックして、[Remove Central Backup Schedule] を選択します。
これにより、[Remove Central Backup Schedule] ダイアログボックスが開きます。

ステップ 3 表示されたフィールド内の情報を調べ、それが削除するバックアップ スケジュールであることを確認します。

ステップ 4 [Remove] をクリックします。

Cisco UCS Central のバックアップ ファイルの表示

ステップ 1 メニュー バーで、[Backup & Restore] を選択します。

ステップ 2 [Domains] で、Cisco UCS Central ドメインを選択して、Cisco UCS Central スコープを入力します。

ステップ 3 右側のペインで、すべての Cisco UCS Central バックアップ ファイルのリストを確認します。バックアップ ファイルごとに、ステータス、最終バックアップ日付、スケジュール、最大ファイル数、およびリモート コピーの場所を表示できます。

設定のエクスポートとインポート

[Export & Import] から、Cisco UCS Central と登録済みの Cisco UCS ドメインの設定バックアップをスケジュールすることができます。エクスポートまたはインポート ポリシーをスケジュールすることも、Cisco UCS Central または選択したドメインの即時オンデマンド設定エクスポートを実行することもできます。Cisco UCS ドメインの場合は、オンデマンド バックアップがすべてリモートに保存されます。バックアップをスケジュールする場合は、ローカルまたはリモートに保存できます。

（注） HTML5 GUI では、全設定バックアップと完全状態バックアップのみがサポートされます。論理設定バックアップとシステム設定バックアップを使用する場合は、Java ベースの GUI を使用してください。

スケジュールされたバックアップ ポリシーはデフォルトで無効にされます。Cisco UCS Central または登録された Cisco UCS ドメインをバックアップする場合は、両方のバックアップ状態を有効にする必要があります。バックアップ プロセスは、サーバ トラフィックまたはネットワーク トラフィックを中断せず、またこれらのトラフィックに影響しません。バックアップは、ドメイン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が保存されます。

リモートで設定されたポリシーは、バックアップに関して、Cisco UCS Managerによって内部的にマウントされた Cisco UCS Central リポジトリを使用するように制限されます。

定期的なバックアップをスケジュールすると、バックアップ リポジトリはデータの蓄積を開始できます。バックアップ アーカイブを管理するために、保存されているバックアップ バージョンの最大数を指定できます。ポリシー指定を使用して、Cisco UCS ドメインごとに保持するバックアップ数を指定します。

（注） この最大数は、リモート ロケーションに保存できるバックアップ イメージ ファイルの数には影響しません。

Cisco UCS Central GUI から各 Cisco UCS ドメインのバックアップのリストを表示できます（Cisco UCS Central のバックアップ ファイルの表示, （44 ページ）を参照してください。また、保存されたまたは未使用のバックアップ ディレクトリと設定を削除することもできます）。

重要

- 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。
- バックアップは、Cisco UCS ドメイン（バックアップが取得された）の登録が解除されてからしか削除できません。

バックアップ イメージ ファイル

データベースまたは設定のバックアップ ファイルは次の場所に保存できます。

- **ローカル ファイル システム**：ローカル ファイル システム。
- **リモート ロケーション**：TFTP、FTP、SCP、SFTP などのプロトコルを使用するリモート ロケーション。

重要 イメージ ファイルをリモートの場所に保存するためのオプションを使ってグローバル バックアップ ポリシーを指定するには、登録された Cisco UCS ドメイン内に Cisco UCS Manager リリース 2.2(2x) が存在する必要があります。Cisco UCS ドメイン内に Cisco UCS Manager リリース 2.2(2x) が存在しない場合は、リモート バックアップを使用したグローバル バックアップ ポリシーが機能しません。

バックアップをスケジュールするときに、システムに保存するバックアップ ファイルの最大数を指定することもできます。

設定のインポート

バックアップ リポジトリに保存された設定を使用して、管理対象の Cisco UCS ドメインのいずれかをインポートして設定できます。TFTP プロトコルを使用して、バックアップ設定にアクセスします。

Cisco UCS Central の設定エクスポートのスケジューリング

設定エクスポートの使い方に関するビデオを観るには、『Video: Creating UCS Central Configuration Export』を参照してください。

はじめる前に

リモートの場所を指定する場合は、その場所が存在することを確認してください。バックアップ ファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。たとえば、転送プロトコルが SCP の場合：`scp://user@<ip>/x/y/z`
- リモート サーバのホスト名または IP アドレス
- リモート サーバのユーザ名とパスワード

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

ステップ 2 [Config Export & Import] ページで、[UCS Central] をクリックします。

ステップ 3 [Schedule] アイコンをクリックして、[Schedule Central Export] を選択します。
これにより、[Schedule Central Configuration Export] ダイアログボックスが開きます。

ステップ 4 （任意） [Description] フィールドに、このバックアップ ポリシーの説明を入力します。

ステップ 5 [Schedule] ドロップダウンをクリックして、このバックアップのスケジュールを選択します。
（注） この設定バックアップと事前定義のスケジュールを関連付ける必要があります。

ステップ 6 [Maximum No of Backup Files] フィールドで、システムに保存するバックアップ ファイルの数を指定します。

ステップ 7 （任意） バックアップ ファイルをリモートの場所に保存する場合は、[Remote Copy] フィールドで、[Enabled] をクリックして、必要なリモートの場所に関する情報を入力します。

Cisco UCS ドメインの設定エクスポートのスケジューリング

登録された Cisco UCS ドメインの設定バックアップは、ドメイン グループ レベルでのみ作成できます。

設定エクスポートの使い方に関するビデオを観るには、『Video: Creating UCS Domain On-Demand Configuration Export』を参照してください。

はじめる前に

リモートの場所を指定する場合は、その場所が存在することを確認してください。バックアップ ファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。たとえば、転送プロトコルが SCP の場合：`scp://user@<ip>/x/y/z`
- リモート サーバのホスト名または IP アドレス
- リモート サーバのユーザ名とパスワード

ステップ 1 [Domain Group] ドロップダウン オプションをクリックして、設定バックアップをスケジュールするドメイン グループを選択します。
この選択により、[Schedule] オプションと [No. of Backup Files] オプションが表示されます。

ステップ 2 [Schedule] ドロップダウンをクリックして、このバックアップのスケジュールを選択します。
（注） この設定バックアップと事前定義のスケジュールを関連付ける必要があります。

ステップ 3 [Maximum No of Backup Files] フィールドで、システムに保存するバックアップ ファイルの数を指定します。

ステップ 4 （任意） バックアップ ファイルをリモートの場所に保存する場合は、[Remote Copy] フィールドで、[Enabled] をクリックします。
表示されたフィールドに、必要なリモートの場所の関連情報を入力します。

ステップ 5 [Schedule] をクリックします。

UCS Central の設定バックアップのエクスポート

はじめる前に

リモートの場所を指定する場合は、その場所が存在することを確認してください。バックアップファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。たとえば、転送プロトコルが SCP の場合：`scp://user@<ip>/x/y/z`
- リモート サーバのホスト名または IP アドレス
- リモート サーバのユーザ名とパスワード

ステップ 1 [Config Export & Import] ページで、[UCS Central] をクリックします。

ステップ 2 エクスポートするバックアップ ファイルを選択します。

ステップ 3 [Config Export] アイコンをクリックします。

ステップ 4 バックアップ ファイルをリモートの場所に保存する場合は、[Remote Copy] フィールドで、[Enabled] をクリックします。
[Disabled] が選択された場合は、ファイルがローカルに保存されます。

ステップ 5 リモートの場所については、[Transfer Protocol] を選択して、表示されたフィールドに必要なリモートの場所に関する情報を入力します。

ステップ 6 [Export] をクリックします。

ドメインの設定オンデマンド バックアップのエクスポート

登録された Cisco UCS ドメインの設定バックアップは、ドメイン グループ レベルでのみ作成できます。

はじめる前に

オンデマンド バックアップが使用できるのはリモートの場所だけです。ローカル Cisco UCS ドメインでは、オンデマンドバックアップがサポートされません。バックアップファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。たとえば、転送プロトコルが SCP の場合：`scp://user@<ip>/x/y/z`
- リモート サーバのホスト名または IP アドレス

- リモート サーバのユーザ名とパスワード

ステップ 1 [Config Export & Import] ページで、ドメインを選択します。
ステップ 2 エクスポートするバックアップ ファイルを選択します。
ステップ 3 [Config Export] アイコンをクリックします。
ステップ 4 [Transfer Protocol] を選択して、表示されたフィールドに必要なリモートの場所に関する情報を入力します。
ステップ 5 [Export] をクリックします。

Cisco UCS Central の設定のインポート

別の Cisco UCS Central から設定をインポートすることも、ローカルまたはリモートの場所にエクスポートした xml ファイルをインポートすることもできます。

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[Export & Import] を選択します。
ステップ 2 [Config Export & Import] ページで、[UCS Central] をクリックします。
ステップ 3 [Config Import] アイコンをクリックします。
これにより、[Import Central Backup] ダイアログボックスが開きます。
ステップ 4 [Behavior on Configuration Import] で、要件に基づいて次のオプションのいずれかを選択します。

オプション	説明
Replace	インポートしたファイル内のオブジェクトごとに、現在の設定内の対応するオブジェクトを置き換えます。
Merge	インポートしたファイル内の設定情報と既存の設定情報をマージします。競合が存在する場合は、現在の設定内の情報がインポートした設定ファイル内の情報に置き換えられます。

ステップ 5 [Config File Location] で、すべての設定を Cisco UCS Central にインポートする場所を選択します。
以下を選択した場合：

- [UCS Central]：[Config File] ドロップダウンから設定バックアップを選択します。
- [Local]：ファイルの場所を参照して、ファイルを選択します。

（注） このバックアップ XML ファイルはローカルに存在します。

- [Remote]：リモート サーバ関連情報とファイル パスを入力します。

（注） このバックアップ XML ファイルはリモート サーバ上に存在します。

ステップ 6 [Import] をクリックします。
Cisco UCS Central のインポートが失敗した場合は、次のエラー メッセージが表示されます。
End point timed out.Check for IP, password, space or access related issues.
このエラーを修正するには、設定を再送信します。再送信が成功すると、インポート プロセスが開始されます。

Cisco UCS ドメインの設定のインポート

（注） Cisco UCS ドメインが中断状態にある場合、表示されない場合、または切断されている場合は、インポート設定機能が無効になります。

はじめる前に

バックアップポリシーを使用して、全設定バックアップファイルが作成されていることを確認します。

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

ステップ 2 [Config Export & Import] ページで、バックアップをインポートするドメインをクリックします。

ステップ 3 [Config Import] アイコンをクリックします。
これにより、[Import Domain Config Backup] ダイアログボックスが開きます。

ステップ 4 [Behavior on Configuration Import] で、要件に基づいて [Replace] または [Merge] を選択します。

オプション	説明
Replace	インポートしたファイル内のオブジェクトごとに、現在の設定内の対応するオブジェクトを置き換えます。
Merge	インポートしたファイル内の設定情報と既存の設定情報をマージします。競合が存在する場合は、現在の設定内の情報がインポートした設定ファイル内の情報に置き換えられます。

ステップ 5 [Import From] ドロップダウンで、すべての設定をこのドメインにインポートするドメインを選択します。ここでの選択肢は、[Config File] ドロップダウンに表示されます。

ステップ 6 [Config File] ドロップダウンをクリックして、設定ファイルを選択します。

ステップ 7 [Import] をクリックします。

Cisco UCS Central の設定エクスポート スケジュールの削除

ステップ 1 [Config Export & Import] ページで、[Schedule] アイコンをクリックします。

ステップ 2 [Remove Central Export Schedule] アイコンを選択します。

ステップ 3 スケジュール内のエントリを確認します。

（注） Cisco UCS Central のスケジュールは 1 つだけです。

ステップ 4 [Remove] をクリックします。

Cisco UCS ドメインの設定エクスポート スケジュールの削除

後述の手順に加えて、次のシナリオでは、Cisco UCS Central の完全状態バックアップを無効化または削除できます。

- サブドメイン グループ ポリシーを削除すると、バックアップ/エクスポート ポリシーが削除されます。
- 中央またはルート ドメイン グループ ポリシーを削除すると、バックアップ/エクスポート ポリシーが無効になります。

ステップ 1 [Config Export & Import] ページで、[Schedule] アイコンをクリックします。

ステップ 2 [Remove Domain Export Schedule] アイコンを選択します。

ステップ 3 設定バックアップを削除するドメイン グループを選択します。

ステップ 4 削除するスケジュールを選択します。

ステップ 5 [Remove] をクリックします。

Cisco UCS Central のバックアップ ファイルの表示

ステップ 1 メニュー バーで、[Backup & Restore] を選択します。

ステップ 2 [Domains] で、Cisco UCS Central ドメインを選択して、Cisco UCS Central スコープを入力します。

ステップ 3 右側のペインで、すべての Cisco UCS Central バックアップ ファイルのリストを確認します。バックアップ ファイルごとに、ステータス、最終バックアップ日付、スケジュール、最大ファイル数、およびリモート コピーの場所を表示できます。

第 6 章

Smart Call Home

Smart Call Home は、Cisco UCS Central で予防的診断を実行することによってダウンタイムを最小限に抑える自動サポート機能です。Cisco UCS Central は、システムによって生成されるリアルタイムのアラートを、Call Home の設定で指定された電子メールアドレスに送信します。Cisco Smart Call Home のサポート ページで、既知の問題の詳細と考えられる対策に関する推奨事項を確認できます。

詳細については、『Smart Call Home User Guide』の「Smart Call Home Web Application」の章を参照してください。

Smart Call Home は、「Cisco UCS CentralSmart Call Home の障害」に一覧表示される障害に関するアラートを提供します。

Cisco UCS Manager の障害に関するアラートを受信する場合は、「Configuring Call Home for UCS Manager」を参照してください。

Smart Call Home

Smart Call Home は、Cisco UCS Central で予防的診断を実行することによってダウンタイムを最小限に抑える自動サポート機能です。Cisco UCS Central は、システムによって生成されるリアルタイムのアラートを、Call Home の設定で指定された電子メールアドレスに送信します。Cisco Smart Call Home のサポート ページで、既知の問題の詳細と考えられる対策に関する推奨事項を確認できます。

詳細については、『Smart Call Home User Guide』の「Smart Call Home Web Application」の章を参照してください。

Smart Call Home は、「Cisco UCS CentralSmart Call Home の障害」に一覧表示される障害に関するアラートを提供します。

Cisco UCS Manager の障害に関するアラートを受信する場合は、「Configuring Call Home for UCS Manager」を参照してください。

Smart Call Home の設定

はじめる前に

Smart Call Home を設定する前に、DNS サーバを設定する必要があります。

ステップ 1 システム設定アイコンから、[Smart Call Home] を選択します。
これにより、[UCS Central Smart Call Home] ダイアログボックスが表示されます。

ステップ 2 [Basic] タブで、[Enabled] をクリックします。

ステップ 3 主要な連絡先の必須電子メール アドレスを入力します。
初期登録とアラート通知がこの電子メール アドレスに送信されます。Smart Call Home をイネーブルにするために必要なものは電子メール アドレスのみです。

重要 正しい電子メールアドレスが入力されていることを確認します。間違った電子メールアドレスを入力した場合は、Cisco TAC にお問い合わせください。

ステップ 4 [Advanced] で、[Throttling] と [Send System Inventory Periodically] をイネーブルにするか、ディセーブルにするかを選択します。
[Send System Inventory Periodically] がイネーブルになっている場合は、システム インベントリを Call Home データベースに送信する間隔を指定します。または、[Basic] タブで、ツール アイコンをクリックして、[Send System Inventory Now] を選択し、その場で送信することもできます。

（注） 初めて Smart Call Home をイネーブルにした場合は、[Save] をクリックしたときにシステム インベントリが自動的に送信されます

ステップ 5 オプションの連絡先情報を入力します。

ステップ 6 [Transport Gateway] で、[Enabled] をクリックして、トランスポート ゲートウェイを使用して Cisco Smart Call Home ポータルと通信します。
トランスポート ゲートウェイは、Cisco UCS Central と Cisco.com の Smart Call Home サーバ間のプロキシとして機能します。

HTTP の場合は、トランスポート ゲートウェイの URL を入力します。HTTPS を使用する場合は、トランスポート ゲートウェイの証明書も入力する必要があります。

（注） 自己署名証明書のみがサポートされます。トランスポート ゲートウェイのセットアップ方法については、『Transport Gateway Communication over HTTPS』を参照してください。

ステップ 7 [Profiles] で、[Basic] をクリックして、デフォルトの CiscoTAC-1 プロファイルを表示します。

（注） CiscoTAC-1 プロファイルは、Cisco UCS Central リリース 1.4(1a) でサポートされる唯一のプロファイルです。このプロファイルは削除できませんが、受信するメッセージのデバッグ レベルを変更することができます。

ステップ 8 [Alerts] で、プラス アイコンをクリックして、ディセーブルにするアラートを選択します。
ディセーブルのイベントが発生しても通知は送られてきません。

ステップ 9 [Configuration Status] で、Smart Call Home 設定の現在のステータスを表示できます。

ステップ 10 [Save（保存）] をクリックします。

Smart Call Home の登録

最初に Cisco UCS Central Smart Call Home をイネーブルにすると、システム インベントリが Cisco Smart Call Home サーバに自動的に送信されます。自動電子メール メッセージが、入力された電子メール アドレスに送信されます。これには、Smart Call Home ポータルへのリンクが含まれます。登録の確認まで 3 ヵ月（90 日）の猶予が与えられます。

登録後に、契約 ID を入力しなかった場合は、4 ヵ月（120 日）の試用期間がアクティブになります。有効な契約 ID を入力した場合は、登録が完了します。登録を再度アクティブにするには、120 日の試用期間の前か後に、契約 ID を入力してインベントリを送信したことを確認します。

Smart Call Home の障害

この項で説明する障害によって、ファブリック インターコネクトから Smart Call Home アラートが発行されます。Cisco UCS Central 障害の詳細については、該当する『Cisco UCS Central Faults Reference』を参照してください。

（注） リリース 1.4(1a) では、どの Cisco UCS Central 障害においてもサービス要求が発行されません。

障害名	障害コード	説明
fltSysdebugCoreCoreFile	F10000005	この障害は、プロセスの 1 つが応答を停止し、コア ファイルが生成された場合に発生します。
fltExtpolProviderProviderLostConnectivity	F10000190	このプロバイダーに Cisco UCS Central レジストリから到達できません。この障害は、通常、プロバイダー プロセスが応答を停止した場合や過剰なビジー状態でレジストリから送信されたハートビート メッセージに応答できない場合に発生します。
fltExtpolControllerControllerLostConnectivity	F10000191	このコントローラに Cisco UCS Central レジストリから到達できません。この障害は、通常、コントローラ プロセスが応答を停止した場合や過剰なビジー状態でレジストリから送信されたハートビート メッセージに応答できない場合に発生します。

障害名	障害コード	説明
fltExtpolClientClientLostConnectivity	F10000192	この登録済みの UCS ドメインに Cisco UCS Central レジストリから到達できません。この障害は、通常、UCS ドメインがネットワーク アクセスを失ったり、UCS ドメイン DME プロセスが応答を停止したりした場合や、過剰なビジー状態でレジストリから送信されたハートビート メッセージに応答できない場合に発生します。
fltIdentpoolElementDuplicatedAssigned	F10000208	同じ ID が複数のサービス プロファイルに割り当てられています。この障害は、Cisco UCS Central が、ローカル プールからの 1 つの ID が複数のサービス プロファイルに割り当てられている可能性があることを検出した場合に発生します。
fltConfigDbConfigStats-DB-Error	F10000536	この障害は、統計情報データベースの設定が間違っている場合やそのデータベースがダウンしているか、ディスク領域が不足している場合に発生します。
fltPkiTPStatus	F10000591	この障害は、トラストポイントの証明書ステータスが無効になった場合に発生します。
ltPkiKeyRingStatus	F10000592	この障害は、キーリングの証明書ステータスが無効になった場合に発生します。
fltConfigBackupUngrouped-domain	F10000616	リモート スケジュール バックアップが失敗しました。この障害は、通常、管理者がリモート マシンに誤ったパスワード、ホスト、ユーザ名、またはパスを指定した場合に発生します。
fltStorageItemCapacityExceeded	F10000034	この障害は、パーティションのディスク使用率が 70% を超えているが 90% 未満である場合に発生します。
fltStorageItemCapacityWarning	F10000035	この障害は、パーティションのディスク使用率が 90% を超えている場合に発生します。
fltSmartlicenseEntitlementEnforcementModeFault	F10000750	ライセンスの権限付与が不適切です。

UCS Manager の Call Home の設定

Cisco UCS Central の Call Home 機能は、ドメイン グループの Cisco UCS Manager アラートを表示するために使用します。

ステップ 1　ドメイン アイコンから、Call Home を設定するドメイン グループを選択します。

すべての登録済みドメインのアラートを表示するには、ルートを選択します。

ステップ 2 システム設定アイコンから、[Call Home] を選択します。

ステップ 3 [Basic] で、[Enabled] をクリックして Call Home をイネーブルにします。

ステップ 4 必要な連絡先情報を入力します。

ステップ 5 [Advanced] で、[Throttling] と [Send System Inventory Periodically] をイネーブルにするか、ディセーブルにするかを選択します。
[Send System Inventory Periodically] がイネーブルになっている場合は、システム インベントリを Call Home データベースに送信する間隔を指定します。または、[Basic] タブで、ツール アイコンをクリックして、[Send System Inventory Now] を選択し、その場で送信することもできます。

（注） 初めて Call Home をイネーブルにした場合は、システム インベントリが自動的に送信されます。

ステップ 6 [Profiles] で、新しいプロファイルを追加したり、既存のプロファイルを削除したりできます。

a) [Basic] で、説明と最大電子メール サイズを入力して、デバッグ レベルと電子メール形式を選択します。
b) [Alert Groups] で、受信するアラートのタイプを選択します。
c) [Alert Recipients] で、アラートを送信する追加の電子メール アドレスを入力します。

ステップ 7 [Alerts] で、プラス アイコンをクリックして、ディセーブルにするアラートを選択します。
ディセーブルのイベントが発生しても通知は送られてきません。

ステップ 8 [Save（保存）] をクリックします。