Cisco UCS Central リリース 1.5 管理ガイド

初版：2016 年 07 月 29 日

最終更新：2017 年 01 月 03 日

最終更新：2017 年 04 月 05 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)

© 2016-2017 Cisco Systems, Inc. All rights reserved.

目 次

はじめに

対象読者

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

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

表記法

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

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

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

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

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

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

警告 安全上の重要事項

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

第 1 章

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
- イメージ ライブラリ
- 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

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

ガイド	説明
Cisco UCS Central Getting Started Guide	Cisco UCS インフラストラクチャ、Cisco UCS Manager、および Cisco UCS Central について簡単に説明します。HTML5 UI の概要、Cisco UCS Central に Cisco UCS ドメインを登録する方法、およびライセンスをアクティブにする方法を説明します。
Cisco UCS Central Administration Guide	ユーザ管理、通信、ファームウェア管理、バックアップ管理、Smart Call Home などの管理タスクについて説明します。
Cisco UCS Central Authentication Guide	パスワード、ユーザ、ロール、RBAC、TACACS+、RADIUS、LDAP、SNMP などの認証タスクについて説明します。
Cisco UCS Central Server Management Guide	機器ポリシー、物理インベントリ、サービス プロファイルとテンプレート、サーバ プール、サーバのブート、サーバ ポリシーなどのサーバ管理について説明します。
Cisco UCS Central Storage Management Guide	ポートとポート チャネル、VSAN と vHBA の管理、ストレージ プール、ストレージ ポリシー、ストレージ プロファイル、ディスク グループ、ディスク グループ設定などのストレージ管理について説明します。
Cisco UCS Central Network Management Guide	ポートとポート チャネル、VLAN と vNIC の管理、ネットワーク プール、ネットワーク ポリシーなどのネットワーク管理について説明します。
Cisco UCS Central Operations Guide	小規模、中規模、および大規模な展開でのドメイン グループのセットアップ、設定、管理に関するベスト プラクティス。
Cisco UCS Central Troubleshooting Guide	Cisco UCS Central で共通する問題に関するヘルプを提供します。

第 2 章

ユーザ管理

この章は、次の項で構成されています。

UCS Central ユーザの管理

[UCS Central Users Administration Manage] 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

手順

ステップ 1 [System Configuration] アイコンをクリックし、[Users] を選択します。
これにより、[UCS Central Users Administration Manage] 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]：[UCS Central Password Profile Manage] ダイアログ ボックスと同じタスクを実行します。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]：[UCS Central Roles Manage] ダイアログ ボックスと同じタスクを実行します。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]：[UCS Central Locales Manage] ダイアログ ボックスと同じタスクを実行します。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]：[UCS Central Local Users Manage] ダイアログ ボックスと同じタスクを実行します。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]：[UCS Central Remote Users Manage] ダイアログ ボックスと同じタスクを実行します。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] をクリックします。

UCS Central パスワード プロファイルの管理

手順

ステップ 1 アクション 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、[UCS Central Password Profile Manage] 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 ユーザが以前のパスワードを再利用できるようには、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] 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

手順

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

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

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

手順

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

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

手順

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

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

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

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

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

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

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

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

ステップ 7 [Save] をクリックします。

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

手順

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

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

（注） このセクションは読み取り専用です。

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

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

手順

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

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

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

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

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

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

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

ステップ 7 [Organizations] をロケールに割り当てます。

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

ステップ 8 [Save] をクリックします。

第 3 章

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，（20 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]：障害がクリアされると、フラッピング間隔と保持期間を決定します。

  Flapping Interval

  Cisco UCS Central で障害が発生してその状態がクリアされるまでの時間の長さ。

Retention Interval

Cisco UCS Central がシステムの障害を保持する時間の長さ。

- [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します。
- [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

[UCS Central System Policies Manage] 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。

手順

ステップ 1 [System Configuration] アイコンをクリックし、[System Policies] を選択します。

ステップ 2 [UCS Central System Policies] ダイアログ ボックスで、設定するセクションのアイコンをクリックします。

- [Fault]：[UCS Central Fault Policy Manage] ダイアログ ボックスと同じタスクを実行します。詳細については、UCS Central 障害ポリシーの管理, （13 ページ）を参照してください。
- [Syslog]：[UCS Central Syslog Manage] ダイアログ ボックスと同じタスクを実行します。詳細については、UCS Central Syslog の管理, （14 ページ）を参照してください。
- [Core Dump Export]：[UCS Central Core Dump Export Manage] ダイアログ ボックスと同じタスクを実行します。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 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] 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, （13 ページ）
UCS Central Syslog の管理, （14 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

手順

ステップ 1 [Domain Group Navigation] アイコンをクリックして、ドメイン グループを選択します。

ステップ 2 [Configuration] アイコンをクリックし、[System Policies] 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。

- [Auto Acknowledged]：Cisco UCS は、使用可能なサーバ接続に基づいてドメインによるサーバ管理を自動的に設定します。
- [User Acknowledged]：Cisco UCS は、サーバ管理を自動的に設定しません。ユーザによる承認を待機します。

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。

- [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]：Cisco UCS は、テーブルから MAC アドレスを削除しません。
- [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、Cisco UCS が 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。

- [User Acknowledged]：Cisco UCS は、管理者がアップグレードを承認するまでファームウェアを同期しません。
- [No Actions]：Cisco UCS は、サーバのファームウェア アップグレードを実行しません。

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、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、システムの IO コントローラ、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。

c) [Multicast Hardware Hash] で、[Enable] をクリックして、Cisco UCS がマルチキャスト トラフィック用に IOM または FEX からファブリック インターコネクトへのすべてのリンクを使用できるかどうかを指定します。

d) [Backplane Speed Preference] で、使用する速度を選択します。

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。

- [N+1]：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。シャーシの電力負荷が均等に分担されます。さらに電源装置を取り付けた場合、それらは Cisco UCS によって「オフ」状態に設定されます。
- [Grid]：2 つの電源がオンにされます。そうでなければ、シャーシに N+1 よりも高い冗長性が要求されます。1 台の電源装置が故障した場合、残っている電源モジュールがシャーシに電力を提供し続けます。
- [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。1 つの電源による電力の小さい構成（2500W 未満である必要があります）のみです。

b) [Power Allocation] 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。

- [Policy Driven Chassis Group Cap]：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 レベルの電源割り当てを設定します。
- [Manual Blade Level Cap]：すべてのシャーシの個々のブレード サーバの電力割り当てを設定します。

c) [ID Soaking Interval] で、Cisco UCS が解放したプール エンティティを再割り当てするまでの Cisco UCS Central の待機時間（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] をクリックします。

ラック ディスカバリ ポリシーの管理

手順

ステップ 1 [Domain Group Navigation] アイコンをクリックして、ドメイン グループを選択します。

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

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

ステップ 4 [Discovery Policy Action] の、[Basic] 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。

- [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。

- [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。

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] をクリックします。

UCS Central 障害ポリシーの管理

手順

ステップ 1 [Actions] バーで次のように入力します。[Manage UCS Central Fault Policy] で、Enter を押します。

ステップ 2 [UCS Central Fault Policy] ダイアログボックスで、[Fault] をクリックし、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です。そ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。

   Cisco UCS Central が数回立て続けに障害を発生およびクリアす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ユーザ定義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。動作は、[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、Cisco UCS Central が自動的に障害をクリアします。[Custom Interval] を選択した場合は、Cisco UCS Central 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クリアします。

4. [Action on Clear] で、障害がクリアされたときの Cisco UCS Central の動作を選択します。

   [Retain Cleared Faults] を選択した場合は、Cisco UCS Central はクリアした障害を [Retention Interval] で指定された時間だけ保存します。[Delete Cleared Faults] を選択すると、Cisco UCS Central はすぐにエラーをクリアします。

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

[Forever] を選択すると、Cisco UCS Central は、すべてのクリアされた障害メッセージを期限なしで保存します。[Custom Interval] を選択すると、Cisco UCS Central は、クリアされた障害メッセージを関連する間隔フィールドで指定された時間保存します。

ステップ 3 [Save] 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, （14 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

手順

ステップ 1 [Actions] バーで次のように入力します。[Manage UCS Central Syslog] で、Enter を押します。

ステップ 2 [UCS Central Syslog] ダイアログボックスで、[Syslog Sources] をクリックして、ログ ファイルを収集する各ソースの [Enabled] を選択します。

- Faults
- Audits
- Events

ステップ 3 [Local Destination] で、Cisco UCS Central が syslog メッセージを追加および表示できる場所を指定します。

- [Console]：コンソールに syslog メッセージが表示され、それらが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]：モニタに syslog メッセージが表示され、それらが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]：ログ ファイルに syslog メッセージを保存します。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。

[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。システムはそのログ レベル以上のメッセージを保存します。

- Alert
- Critical (UCSM Critical)
- Error (UCSM Major)
- Emergency

- 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。
  - Alert
  - Critical (UCSM Critical)
  - Error (UCSM Major)
  - Emergency
  - 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 サーバを設定します。

ステップ 5 [Save] 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, （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 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。これは tar 形式のコア ファイルをエクスポートします。

手順

ステップ 1 [Actions] バーで次のように入力します。[Manage UCS Central Core Dump Export] で、Enter を押します。

ステップ 2 [UCS Central Core Dump Export] ダイアログボックスで、[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] 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, （13 ページ）
UCS Central Syslog の管理, （14 ページ）

システム イベント ログの設定

手順

ステップ 1 [Description] に、システム イベントの説明を入力します。

ステップ 2 [SEL Backup] で、バックアップを [Enable] にするか、または [Disable] にするかを選択します。

ステップ 3 [SEL Backup Format] で、バックアップ ファイルの形式として [ASCII] または [Binary] を選択します。

ステップ 4 [SEL Backup Frequency] で、次のいずれかのオプションを選択して、自動バックアップ間の待機時間を設定します。

- Hourly
- Every 2 Hours
- Every 4 Hours
- Every 8 Hours

- Daily
- Weekly
- Monthly

ステップ 5 [Protocol] で、リモート サーバと通信するためのプロトコルとして次のいずれかのオプションを選択します。

- FTP
- SFTP
- TFTP
- SCP

ステップ 6 [Absolute Remote Path *] で、リモート サーバ上のファイルへの絶対パスを入力します。
SCP を使用する場合、絶対パスは常に必要です。他のプロトコルを使用する場合は、ファイルがデフォルトのダウンロードフォルダにあれば、リモートパスを指定する必要はありません。ファイル サーバの設定方法の詳細については、システム管理者に問い合わせてください。

ステップ 7 [Remote Server Host Name/IP Address] で、バックアップ設定が存在するサーバのホスト名または IP アドレスを入力します。IP アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。

ステップ 8 [User Name] で、リモート サーバへのログインに使用するユーザ名を入力します。TFTP プロトコルを選択する場合、このフィールドは該当しません。

ステップ 9 [Password] で、リモート サーバへのログインに使用するパスワードを入力します。TFTP プロトコルを選択する場合、このフィールドは該当しません。

ステップ 10 [SEL Backup on Log Full] で、ログがサイズの上限に達したときに SEL のバックアップを作成するオプションを選択します。

ステップ 11 [SEL Backup on Service Profile Association] で、サーバとサービス プロファイルの間の関連付けが変更されたときに SEL のバックアップを作成するオプションを選択します。

ステップ 12 [SEL Backup on Manual Log Clear] で、システム ログを手動でクリアするときに SEL のバックアップを作成するオプションを選択します。

ステップ 13 [SEL Backup on Backup Clear Interval] で、[SEL Backup Frequency] ドロップダウンで指定された時間間隔に達したときに SEL バックアップを作成するオプションを選択します。

ステップ 14 [Clear Log on Backup] で、バックアップ後にすべてのシステム イベント ログを消去するオプションを選択します。

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，（22 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

手順

ステップ 1 [System Configuration] アイコンをクリックし、[System Profile] を選択します。

ステップ 2 [UCS Central] セクションで、Cisco UCS Central システム名、モード、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。システム名および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] をクリックします。

関連トピック

UCS Central NTP サーバの管理，（19 ページ）
UCS Central 管理ノードの管理，（19 ページ）
UCS Central DNS サーバの管理，（20 ページ）

UCS Central 管理ノードの管理

手順

ステップ 1 アクション 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、[UCS Central Management Node Manage] 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] 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, （18 ページ）
UCS Central NTP サーバの管理, （19 ページ）
UCS Central DNS サーバの管理, （20 ページ）

UCS Central NTP サーバの管理

手順

ステップ 1 アクション 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、[UCS Central NTP Servers Manage] 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] 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, （18 ページ）
UCS Central 管理ノードの管理, （19 ページ）
UCS Central DNS サーバの管理, （20 ページ）

UCS Central DNS サーバの管理

手順

ステップ 1 アクション 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、[UCS Central DNS Servers Manage] 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] 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, （18 ページ）
UCS Central NTP サーバの管理, （19 ページ）
UCS Central 管理ノードの管理, （19 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します。
- [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ます。
- [Faults]：障害がクリアされると、フラッピング間隔と保持期間を決定します。

  Flapping Interval

  Cisco UCS Central で障害が発生してその状態がクリアされるまでの時間の長さ。

  Retention Interval

  Cisco UCS Central がシステムの障害を保持する時間の長さ。

- [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します。
- [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監視するための基準を設定します。
- [System Events]：ドメイン グループ システム イベント ログの基準を設定します。

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します。

手順

ステップ 1 [Domain Group Navigation] アイコンをクリックして、ドメイン グループを選択します。

ステップ 2 [Settings] アイコンをクリックします。

ステップ 3 システム ポリシーの [Launch] をクリックします。

ステップ 4 [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, （11 ページ）を参照してください。

ステップ 5 [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 6 [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, （13 ページ）を参照してください。

ステップ 7 [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, （14 ページ）を参照してください。

ステップ 8 [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 9 [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 10 [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 11 [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。
詳細については、システム イベント ログの設定, （16 ページ）を参照してください。

ステップ 12 [Save] 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。

ドメイン グループ システム プロファイルの管理

手順

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

ステップ 2 [Settings] アイコンをクリックします。

ステップ 3 システム ポリシーの [Launch] をクリックします。

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、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、HTTPS、HTTPS ポートを入力し、必要に応じて Web およびシェル セッションのデフォルト値を変更します。

（注） SSH フィールドは読み取り専用です。

ステップ 7 [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 8 [Save] をクリックします。

スケジュール

特定のアクティビティを行う日時を決定するためにスケジュールを使用します。Cisco UCS Central にスケジュールを作成した後、そのスケジュールを以下で使用できます。

- バックアップ操作
- 設定のエクスポート
- メンテナンス ポリシー

（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。

スケジュールの作成または編集

（注） 繰り返しまたは1回のみ実行するシンプルなスケジュールです。ユーザの承認は必要ありません。ユーザの承認を求める場合は、高度なスケジュールを選択します。

手順

ステップ 1 [Actions] バーで次のように入力します。[Create Schedule] で Enter を押します。

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 スケジュールの [Recurring]、[One Time] または [Advanced] を選択します。
[Advanced] の場合、ユーザの承認の [enable] または [disable] を選択します。

ステップ 4 [Schedules] をクリックします。

ステップ 5 [Add] をクリックして、スケジュールを追加します。

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 6 [Create] をクリックします。

サーバ 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。

さ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への変更が発生したとき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。

- [On Save]：サービス プロファイルを変更すると、Cisco UCS Central はすぐに変更を適用します。
- [User Acknowledgment]：管理者が変更を確認した後に、その変更を適用します。
- [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

サーバ 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。

手順

ステップ 1 [Actions] バーで次のように入力します。[Create Maintenance Policy] で、Enter を押します。

ステップ 2 [Maintenance Policy Create] ダイアログ ボックスで、[Server] を選択します。
シャーシ メンテナンス ポリシーの作成の詳細については、『Cisco UCS Central Storage Management Guide』を参照してください。

ステップ 3 ポリシーを作成する [Organization] を選択し、[Name] とオプションで [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 サーバ メンテナンス ポリシーについて、次の項目を入力します。

a) ハード シャットダウン OS オプションの選択：

- [Enabled] を選択すると、Cisco UCS Manager は、シャットダウンと再起動をトリガーする前に Cisco UCS Central で指定した [Hard Shutdown Timer] の値の間待機します。
  （注） [Hard Shutdown Timer] は、シャットダウンと再起動をトリガーする前に Cisco UCS Manager が待機する時間を秒単位（150、300、または 600）で指定します。このタイマー値は、グローバル メンテナンス ポリシーで指定されます。
- [Disable] を選択すると、Cisco UCS Manager はサーバ シャットダウンを実行しません。

b) 再起動が必要な変更を適用するタイミングを選択します。

- [User Acknowledgment]：ユーザが設定の変更を承認して再起動を確認する必要があります。
- [Schedule]：Cisco UCS Central は選択したスケジュールに応じて設定の変更を適用します。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，（23 ページ）を参照してください。
- [On Save]：Cisco UCS Central は設定変更の即時の保存と再起動を適用します。

c) Cisco UCS Central で次の再起動時に変更を適用し、[Apply Changes On] フィールドの選択を無視する場合は、[Apply on Next Reboot] を有効にします。

ステップ 5 [Evaluate] をクリックし、ポリシーの影響を表示します。

ステップ 6 [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。キーで暗号化されたメッセージを他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 ～ 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 リングを再生成した後、Cisco UCS Central へのログインは数分かかることがあります。

クラスタ名が変更されたり証明書の期限が切れたら、手動でデフォルトのキー リングの証明書を再生成します。

（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 企業証明機関のサーバを使用すると、証明書を生成するために**コンピュータ**のテンプレートを使用します。キー用途セットの両方が含まれている必要があります。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します。

キー リングの作成

手順

ステップ 1 [System Configuration] アイコンをクリックし、[System Profile] を選択します。
ステップ 2 [Certificates] をクリックします。
ステップ 3 キー リングを追加するには [Add] をクリックします。
ステップ 4 [Basic] タブで、[Modulus] をデフォルト値のままにするか、または必要に応じて変更します。
ステップ 5 トラスト ポイントを入力します。
ステップ 6 生成されたキー リングから証明書チェーンに貼り付けます。
ステップ 7 [Certificate Request] をクリックします。
ステップ 8 フィールドに組織の有効な情報を入力します。
ステップ 9 [Save] をクリックします。

トラスト ポイントの作成

Cisco UCS Central でトラスト ポイントを作成できます。トラスト ポイントには、ルート認証局（CA）および下位 CA のバンドル形式の証明書が含まれています。

（注） 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。

手順

ステップ 1 [System Configuration] アイコンをクリックし、[System Profile] を選択します。
ステップ 2 [Trusted Points] をクリックします。
ステップ 3 トラスト ポイントを追加するには、[Add] をクリックします。
ステップ 4 生成されたキー リングから証明書チェーンに貼り付けます。
ステップ 5 [Save] 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、[Refresh]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、[System Alerts] アイコンをクリックして、[System Faults] を選択します。障害のタイプと重大度レベルの情報が [Faults Logs] ページに表示されます。システム障害をモニタおよび確認して、表示された障害をフィルタ処理することもできます。

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]：障害に対して必要なアクション

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。

ドメイン障害

Cisco UCS Central では、[Domain Faults] ページに登録済みの Cisco UCS ドメイン からの障害が収集および表示されます。インベントリ障害も表示されます。Cisco UCS Central では、次のようなドメイン障害が分類および表示されます。

- [Fault Level]：プロファイルをトリガーする障害レベル。
  - [Critical]：1 つ以上のコンポーネントに重大な問題があります。これらの問題を迅速に調査し、修正します。
  - [Major]：1 つ以上のコンポーネントに深刻な問題があります。これらの問題を迅速に調査し、修正します。
  - [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。メジャーまたは重大な問題となる前に、これらの問題をできるだけ早く調査し、修正します。
  - [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。メジャーまたは重大な問題となる前に、これらの問題をできるだけ早く調査し、修正します。
  - [Cleared]：障害の原因となった状態が解決されて、障害がクリアされます。
  - [Info]：通知または情報メッセージ。
  - [Condition]：状態に関する情報メッセージ。
- [Filter]：テーブルのデータをフィルタ処理します。
- [Code]：障害に関連付けられた 固有識別子。
- [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の名前と場所、およびそれが見つかった場所のドメイン名。
- [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。
- [Action]：ユーザの確認が必要かどうか。

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。これらのイベント ログを表示するには、[System Alerts] アイコンをクリックし、[Events] を選択します。イベント ログには次の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
- [Event Details]：イベントの詳細。

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、[System Alerts] アイコンをクリックし、[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]：作成日。

- [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、[System Alerts] アイコンをクリックし、[Active Sessions] を選択します。ログ テーブルで、次の情報を確認できます。

- [ID]：ユーザのログイン元であるターミナルのタイプ。
- [Timestamp]：ユーザがログインした日付と時刻。
- [User]：ユーザ名。
- [Type]：ユーザのログイン元であるターミナルのタイプ。
- [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、[System Alerts] アイコンをクリックし、[Internal Services] を選択します。

[Services] セクションで、次の情報を確認できます。

- [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。

[Lost Domains] セクションで、次の情報を確認できます。

- [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。

Tomcat ロギングのイネーブル化

ターミナル エミュレータを使用して CLI にアクセスします。

手順

	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。
ステップ 5	UCSC /monitoring/sysdebug/mgmt-logging # **commit-buffer**	変更を確定します。

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 # commit-buffer
```

Cisco UCS Central からの重要なオブジェクト削除の防止

リリース 2.0 から、Cisco UCS Central は、Cisco UCS Central GUI とコマンド ラインから重要なオブジェクトが削除されるのを防止します。Cisco UCS Central からこれらの項目を削除しようとすると、潜在的な影響があるエラー メッセージが表示されます。以下の表は、削除する前に実行する項目と手順です。

Cisco UCS Central 内のオブジェクト	Cisco UCS Central からオブジェクトを削除する前に必要なアクション
サーバに関連付けられているサービス プロファイル	サーバとの関連付けを解除します
関連付けられたサービス プロファイルがある組織	その組織内のサービス プロファイルすべてとサブ組織のすべての関連付けを解除します

Cisco UCS Central 内のオブジェクト	Cisco UCS Central からオブジェクトを削除する前に必要なアクション
バインドされている関連付けられたサービスプロファイルのあるサービスプロファイルのテンプレート	すべての関連付けされたサービスプロファイルのバインドを解除するか、すべての関連付けを解除します
登録済み Cisco UCS ドメインを持つドメイン グループと機能 VLAN	• ドメイン グループ、またはそのサブドメイン グループ内の登録されたドメインは削除してください • 関連付けられたサービス プロファイルまたはサブドメイン グループによって参照されている VLAN は削除してください

API 通信レポート

Cisco UCS Central 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

手順

ステップ 1 メニュー バーで、[System Tools] 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、[System Tools] アイコンをクリックして、[Stop Logging Session] を選択します。API レポートのテキスト ファイルがシステムに保存されます。

テクニカル サポート ファイル

Cisco Technical Assistance Center（Cisco TAC）によるトラブルシューティングやサポートが必要な問題が発生した場合は、Cisco UCS Central または影響を受ける Cisco UCS ドメインについてできるだけ多くの情報を収集します。Cisco UCS Central はこれらの情報をテクニカル サポート ファイルに出力します。このファイルを Cisco TAC に送信することができます。

Cisco UCS Central のすべてまたは Cisco UCS ドメインの次のコンポーネントのテクニカル サポート ファイルを作成できます。

- ドメイン全体：すべての Cisco UCS ドメインのテクニカル サポート データが含まれます。
- FEX：特定の FEX のテクニカル サポート データが含まれます。
- ドメイン管理サービス：ファブリック インターコネクトを除く、Cisco UCS Central 管理サービスのテクニカル サポート データが含まれます。
- ラック サーバ：特定のラック サーバおよびアダプタのテクニカル サポート データが含まれます。
- シャーシ：特定のシャーシのブレード サーバ上の I/O モジュールまたは CIMC のテクニカル サポート データが含まれます。
- サーバ メモリ：特定のラックマウント サーバとブレード サーバに関するサーバ メモリのテクニカル サポート データが含まれます。

Cisco TAC に連絡する前に、次を参照してください。

1 テクニカル サポート ファイルの生成, （33 ページ）

2 テクニカル サポート ファイルのダウンロード, （34 ページ）

テクニカル サポート ファイルの生成

Cisco UCS Central のテクニカル サポート ファイルまたは Cisco UCS ドメインのサポートされているコンポーネントのテクニカル サポート ファイルを生成できます。

手順

ステップ 1 [System Tools] アイコンをクリックし、[Tech Support] を選択します。

ステップ 2 [Domains] で、[UCS Central] またはテクニカル サポート ファイルを生成するドメインを選択します。

ステップ 3 [Generate Tech Support] アイコンをクリックします。

ステップ 4 [UCS Central] を選択した場合は、次の手順を実行します。

a) レポートにシステム データを含めるかどうかを選択します。

b) [Yes] をクリックしてファイルを生成します。

収集の進行中に、リスト ページにテクニカル サポート ファイルの収集ステータスが表示されます。プロセスが完了すると、収集時間、ファイル名、および可用性ステータスが表示されます。

ステップ 5 ドメインを選択した場合は、次の手順を実行します。

a) テクニカル サポートを生成するデータのタイプを選択します。

b) CLI コマンドを除外するかどうかを選択します。

c) [Generate File] をクリックします。
収集の進行中に、リスト ページにテクニカル サポート ファイルの収集ステータスが表示されます。プロセスが完了すると、収集時間、ファイル名、および可用性ステータスが表示されます。

テクニカル サポート ファイルのダウンロード

手順

ステップ 1 [System Tools] アイコンをクリックし、[Tech Support] を選択します。

ステップ 2 [Domains] で、[UCS Central] またはテクニカル サポート ファイルを表示するドメインを選択します。
右ペインに、選択したシステムで利用可能なテクニカルサポートファイルのリストが表示されます。

ステップ 3 ダウンロードするファイルを選択します。

ステップ 4 [Download] をクリックします。

第 4 章

イメージ ライブラリ

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。[System Tools] アイコンを介してイメージ ライブラリにアクセスします。

- [Packages]：すべてのファームウェア パッケージを表示します。
- [Downloads]：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。

ファームウェア ポリシーの作成時にファームウェア イメージを使用します。

[Image Library] では、以下の操作を実行できます。

- イメージを選択し、[Delete] をクリックして、ダウンロードし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。

- 定期的なファームウェア イメージ同期をスケジュール設定する。
- Cisco.com のイメージとファームウェア イメージを同期する。
- ファームウェア バンドル（またはサービス パック）をインポートする。
- イメージのダウンロードの詳細については、Cisco.com からのファームウェアのダウンロード, （36 ページ）を参照してください。

Cisco.com からのファームウェアのダウンロード

指定された間隔でシスコの Web サイトと通信してファームウェア イメージのリストを取得するように、Cisco UCS Central を設定できます。イメージのダウンロード用にシスコのクレデンシャルを設定した後に、リフレッシュを行うと、Cisco UCS Central によって Cisco.com から使用可能なイメージ データが取得され、ファームウェア イメージ ライブラリにファームウェア イメージが表示されます。ファームウェア イメージのバージョンを使用してポリシーを作成する場合、または [Store Locally] オプションを使用してイメージをダウンロードする場合には、実際のファームウェア イメージをダウンロードできます。

Cisco.com からのファームウェア イメージをダウンロードするには、次の操作を実行する必要があります。

1. ユーザ クレデンシャルを使用して、Cisco.com のアカウントを設定します。
2. GUI を介して、EULA と K9 を承認します。
3. 同期の頻度を設定します（オンデマンド、毎日、毎週、隔週）。
4. メタデータをダウンロードします。

（注） このプロセスはバックグラウンドで動作し、完了するまで約 15 分かかります。ダウンロード時間は、イメージの数によって異なります。

5. イメージをメタデータから選択し、ダウンロードします。

重要 Cisco.com から Cisco UCS Central にファームウェアをダウンロードするには、Cisco.com アカウントを作成してください。

（注） Cisco.com アカウントのユーザを変更すると、イメージ ライブラリが完全に同期されます。同期中は、ダウンロード操作を実行できません。これは、ライブラリのサイズによって、最大 15 分かかることがあります。

Cisco.Com アカウントの設定

ファームウェア管理とハードウェア互換性リストのクレデンシャルはともにcisco.comアカウントを使用して管理されます。

手順

ステップ 1 [System Configuration] アイコンをクリックし、Cisco.com のアカウントを選択します。

ステップ 2 ユーザ名およびパスワードを入力します。

ステップ 3 HTTP を介して Cisco.com にアクセスする場合は、[HTTP Proxy To Access Cisco.com] フィールドで [Enabled] を選択します。適切なフィールドに、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 4 使用するシスコ サービスを選択します。

- [Firmware Image Downloads]：Cisco.com からインフラストラクチャ ファームウェアの更新およびファームウェア イメージのダウンロードをダウンロードする場合に選択します。
- [Hardware Compatibility Catalog]：ローカル リストを Cisco.com と同期させ、使用しているハードウェアに互換性があることを確認する場合に選択します。

ステップ 5 [Save] をクリックします。

シスコからのインフラストラクチャ ファームウェア イメージのダウンロード

手順

ステップ 1 [System Tools] アイコンをクリックし、[Image Library] を選択します。

ステップ 2 [Packages] をクリックして使用可能なパッケージを表示します。

ステップ 3 パッケージ（1 つまたは複数）を選択し、[Import Selected Image] アイコンをクリックします。

ステップ 4 [Download] をクリックします。
テーブルでダウンロードのステータスの情報を確認できます。

ステップ 5 [Transfer State] 列で、[Launch] をクリックしてステータスのダイアログを表示します。
このダイアログにダウンロード ステータスの詳細情報を表示します。

ファームウェア ライブラリからのイメージの削除

ライブラリからファームウェア イメージを削除するオプションを次に示します。

- **ファームウェア イメージの削除**：イメージを選択して削除をクリックすると、ファームウェア ライブラリ内のダウンロードされたイメージを削除できます。
- **ファームウェア イメージのメタデータのパージ**：パージ オプションを使用すると、イメージのメタデータを削除できます。ライブラリからファームウェア イメージを削除した後でも、メタデータは引き続き存在しています。このメタデータ情報を使用すると、イメージを削除した後でも Cisco.com から実際のファームウェア イメージをいつでもダウンロードすることができます。ファームウェア イメージ ライブラリからファームウェア イメージと関連するメタデータを完全に削除する場合は、実際のファームウェアイメージを削除し、ライブラリからメタデータをパージしてください。

重要 メタデータに対応するイメージがファームウェア イメージ ライブラリにすでにダウンロードされている場合は、イメージを削除しないでメタデータをパージすることはできません。

イメージ ライブラリ上のイメージのメタデータの削除

CLI を使用してメタデータの削除のみできます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCSC# **connect operation-mgr**	Operations Manager モードを開始します。
ステップ 2	UCSC(ops-mgr)# **scope firmware**	ファームウェア管理モードを開始します。
ステップ 3	UCSC(ops-mgr) /firmware# **scope download-source cisco**	Cisco Web サイトからダウンロードしたイメージのメタデータにアクセスします。
ステップ 4	UCSC(ops-mgr) /firmware/download-source# **purge list**	イメージ ライブラリからファームウェア イメージのメタデータを削除します。

次に、イメージ ライブラリからイメージのメタデータを削除する例を示します。

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
UCSC(ops-mgr) /firmware # scope download-source cisco
UCSC(ops-mgr) /firmware/download-source # purge list
```

機能カタログ

機能カタログは調整可能なパラメータ、文字列、およびルールのセットです。Cisco UCS はカタログを使用してサーバの新しく資格を持ったDIMMやディスク ドライブなどのコンポーネントの表示と設定可能性を更新します。

カタログは、シャーシ、CPU、ローカル ディスク、I/O モジュールなどのハードウェア コンポーネントによって分割されます。カタログを使用すると、該当するコンポーネントで利用可能なプロバイダーのリストを表示できます。1 つのハードウェア コンポーネントに対して 1 つのプロバイダーが存在します。各プロバイダーは、ベンダー、モデル（PID）、およびリビジョンによって識別されます。各プロバイダーに対して、装置の製造元とフォーム ファクタの詳細を表示することもできます。

特定のカタログのリリースに依存するハードウェア コンポーネントの詳細については、『Service Notes for the B- Series server』のコンポーネントのサポートの表を参照してください。特定のリリースで導入されたコンポーネントの情報については、『Cisco UCS Release Notes』を参照してください。

機能カタログの内容

機能カタログの内容は次のとおりです。

実装固有の調整可能なパラメータ

- 電力および熱に関する制約
- スロット範囲および番号
- アダプタ機能

ハードウェア固有のルール

- BIOS、CIMC、RAIDコントローラ、アダプタなどのコンポーネントのファームウェア互換性
- 診断
- ハードウェア固有のリブート

ユーザ表示文字列

- CPN や PID/VID などの部品番号
- コンポーネントの説明
- 物理レイアウト/寸法
- OEM 情報

機能カタログの更新

Cisco UCS インフラストラクチャ ソフトウェア バンドルには、機能カタログの更新が含まれています。Cisco Technical Assistance Center から特に指示された場合を除いて、Cisco UCS インフラストラクチャ ソフトウェアバンドルをダウンロード、更新、およびアクティブ化した後に、機能カタログの更新をアクティブ化する必要があるだけです。

機能カタログの更新をアクティブ化すると、Cisco UCSによってすぐに新しいベースライン カタログに更新されます。それ以外の作業は行う必要がありません。機能カタログの更新では、Cisco UCS ドメイン内のコンポーネントをリブートまたは再インストールする必要はありません。

各 Cisco UCS インフラストラクチャ ソフトウェア バンドルには、ベースライン カタログが含まれます。まれに、シスコが Cisco UCS リリースの間で機能カタログの更新をリリースし、ファームウェア イメージをダウンロードするのと同じサイトで更新を入手できるようにする場合があります。

（注） 機能カタログのバージョンは、使用している Cisco UCS のバージョンによって決まります。たとえば、Cisco UCS 3.x リリースは、機能カタログのあらゆる 3.x リリースと一緒に使用できますが、2.x リリースと一緒に使用することはできません。特定の Cisco UCS リリースでサポートされている機能カタログのリリースについては、http://www.cisco.com/go/unifiedcomputing/b-series-doc で入手可能な『*Cisco UCS B-Series Servers Documentation Roadmap*』にある『*Release Notes for Cisco UCS Software*』を参照してください。

定期的なファームウェアイメージの同期のスケジューリング

はじめる前に

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。「Cisco.Com アカウントの設定」を参照してください

手順

ステップ 1 [System Tools] アイコンをクリックし、[Image Library] を選択します。

ステップ 2 [Image Library] ページで、[Tools] をクリックし、[Schedule Periodic Firmware Image Syncs] を選択します。
これにより [Periodic Firmware Image Sync] ダイアログ ボックスが起動します。

ステップ 3 www.cisco.com からのインフラストラクチャ ファームウェアのダウンロードの頻度を選択します。

- [On Demand]：ユーザが [Schedule] をクリックすると、ファームウェア イメージ ライブラリのリストをダウンロードします。
- [Daily]：1 日に 1 回ファームウェア イメージ ライブラリのリストをダウンロードします。
- [Weekly]：1 週間に 1 回ファームウェア イメージ ライブラリのリストをダウンロードします。
- [Bi-weekly]：隔週で ファームウェア イメージ ライブラリのリストをダウンロードします。

ステップ 4 [Cisco End User License Agreement] をクリックし、手順に従って EULA を許可します。

ステップ 5 [K9 TM] をクリックし、手順に従って利用規約に同意します。

ステップ 6 [Schedule] をクリックします。

（注） UCS Central のインストール後、または UCS Central v1.4 から v1.5 へのアップグレード後、最初にファームウェア イメージの同期を実行すると、Cisco.com からのイメージ カタログのダウンロードに 15 分かかります。

ファームウェア バンドルのインポート

はじめる前に

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。Cisco.Com アカウントの設定

手順

ステップ 1 [System Tools] アイコンをクリックし、[Image Library] を選択します。

ステップ 2 [Image Library] ページで、[Tools] 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 [Firmware Bundle Import] 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、[Open] をクリックします。
d) [Firmware Bundle Import] ダイアログボックスで、[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) 転送プロトコルを選択します。
c) 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 バンドルを削除します。

（注） これを削除する前に関連付けられたすべてのポリシーからファームウェア バンドルを削除します。

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

手順

ステップ 1 [Actions] バーで次のように入力します。 [Create Host Firmware Package Policy] で Enter キーを押します。

ステップ 2 [Host Firmware Package Policy] ダイアログ ボックスで、[Basic] をクリックし、ポリシーを作成する [Organization] 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。
ポリシー名では、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] および [Rack Version] を選択します。

ステップ 5 ファームウェアに必要な [Service Pack Version] を選択します。
サービス パックはリリースの基本バージョンにのみ適用でき、そのバージョンと互換性がなければなりません。サービスパックが基本バージョンと互換性がない場合、次のエラーメッセージが表示されます。

パックのすべてのバンドルのパッケージ バージョンが一致する必要があります。

適切なサービス パックの詳細については、「サービス パックについて，（58 ページ）」を参照してください。サービス パックのバージョンは、ドロップダウンから選択を削除するときにデフォルト設定にロールバックします。イメージのダウンロードの詳細については、『*Cisco UCS Central Administration Guide*』の「Downloading Firmware from Cisco.com」を参照してください。

ステップ 6 [Components] タブで、[Add] をクリックしてファームウェア更新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。

ステップ 7 すべてのコンポーネントを除外するには、[Excluded Components] をクリックします。

ステップ 8 除外コンポーネントを削除するには、それを選択して [Delete] をクリックします。

ステップ 9 [Create] をクリックします。

（注） ポリシーの影響を確認するには、[Evaluate] をクリックします。

ホスト ファームウェア パッケージ ポリシーを作成して、それをサービス プロファイル テンプレートに関連付けた後は、サービスパック イメージが優先され、それが解決されるときにファームウェア イメージが適宜コンポーネントに適用されます。

第 5 章

ファームウェア管理

インフラストラクチャ ファームウェアの更新

以前に、ユーザはドメイン グループ 1 人あたりのインフラストラクチャ ファームウェアの更新をスケジュールしました。Cisco UCS Central の機能が変更されています。ここで、メンテナンス グループとタグを使用して、特定のドメインもしくはドメイン グループに割り当てられているドメインに対してインフラストラクチャ ファームウェアの更新をスケジュールします。

製品ファミリに基づいて、1 つのドメイン、複数のドメイン、またはドメイン グループに属するドメインでインフラストラクチャ ファームウェアの更新をトリガーできます。たとえば、Cisco UCS Mini システムすべてのインフラストラクチャ ファームウェアは更新できますが、ブレード サーバは更新できません。別の例を挙げると、西海岸のすべてのメンテナンス グループは更新できますが、東海岸のものはできません。以下は、必要な初期手順の概要です。

手順

ステップ 1 Cisco UCS Central に UCS ドメインを登録します。
詳細については、『*Cisco UCS Central Getting Started Guide*』を参照してください。

ステップ 2 登録時に、インフラストラクチャとカタログ ファームウェア ポリシーに同意し、それをグローバル ポリシーにします。
詳細については、『*Cisco UCS Central Getting Started Guide*』を参照してください。

ステップ 3 イメージ ライブラリから適切なインフラストラクチャ ファームウェア イメージをダウンロードします。
詳細については、「シスコからのインフラストラクチャ ファームウェア イメージのダウンロード」を参照してください。
（注） 更新はイメージ全体をダウンロードするまで開始することはできません。

ステップ 4 メンテナンス グループ タグの値を作成します。個々のドメインまたはドメイン グループのすべてのドメインにタグを適用して、メンテナンス グループにこれらを含めます。
詳細については、「メンテナンス グループを作成してメンテナンス グループにタグなしドメインを含める」を参照してください。

ステップ 5 メンテナンス グループ タグにインフラストラクチャ ファームウェアの更新をスケジュールします。
詳細については、「インフラストラクチャ ファームウェア更新スケジュールの設定」を参照してください。

ステップ 6 ユーザ確認応答を有効にした場合、保留中のアクティビティ セクションの更新を確認します。
詳細については、「インフラストラクチャ ファームウェア更新ポリシーの確認」を参照してください。

グローバルへのファームウェア ポリシーの設定

インフラストラクチャとカタログのファームウェア ポリシーは、破壊的な障害をもたらすため、デフォルトではローカルに設定されています。ドメイン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する前に、これを編集してグローバルに設定します。ファームウェア ポリシーがローカルに設定されると、実行時にドメインへの影響はありません。

登録時にポリシーをグローバル設定するか、または、登録後に Cisco UCS Central 内から設定できます。次のステップでは、登録後に設定する方法を説明します。

手順

ステップ 1 [Browse Tables] アイコンをクリックして、[Domains] を選択します。
ステップ 2 ドメインを選択します。
ステップ 3 [domain] ページで、[Tools] アイコンをクリックし、[Edit Policy Resolution Control] を選択します。
ステップ 4 [Infrastructure and Catalog Firmware] スロットで、[Global] をクリックします。
ステップ 5 [Save] をクリックします。

メンテナンス グループ

メンテナンス グループには、選択したドメインのコレクションか、ファームウェアを同時に更新するドメイン グループに割り当てられているドメインすべてが含まれています。ファームウェアは、すぐにアップグレードするか、スケジュールしてアップグレードできます。アップグレードは、確認するようにユーザに要求することも、自動的に開始することもできます。

メンテナンス グループのタグまたは値によってドメインのコレクションをグループ化することができます。地理的なロケーション、ジョブ機能、ハードウェア、その他のビジネス ーズに基づいてドメインをグループ化できます。また、ドメイン グループ内のドメインすべてにメンテナンス タグを適用することもできます。

重要 ドメインに対して、同時に割り当てられるメンテナンス グループ タグは 1 つのみです。

ファームウェア更新のカタログ バージョン

ジョブがスケジュールされたドメイン インフラストラクチャの更新ごとに 1 つのカタログを選択できます。各カタログのバージョンは 1 つの製品ファミリにのみ適用されます。したがって、ベスト プラクティスは、カタログを更新する際に、同一の製品ファミリを持つドメインのみを含むメンテナンス グループを作成することです。次に、メンテナンス グループに含まれる Cisco UCS ドメインは、その製品ファミリに定義された機能カタログで更新されます。そのメンテナンス グループに他の製品ファミリを含めると、カタログ バージョンは更新されません。

メンテナンス グループを作成してメンテナンス グループにタグなしドメインを含める

Cisco UCS Central に最初にアップグレードするときに、メンテナンス グループを作成し、ドメイン、またはアクション バーからドメイン グループに割り当てられているすべてのドメインにタグ付けします。

（注） メンテナンス グループ タグですでにタグ付けされていないドメインまたはドメイン グループにのみタグ付けできます。

手順

ステップ 1 アクション テーブルで、「Create Maintenance Group Tag」と入力して、Enter キーを押します。

ステップ 2 **メンテナンス グループ タグ**の名前を入力します。

ステップ 3 ドメインにタグを適用する方法を選択します。

- ドメイン グループごと
  メンテナンス グループ タグは、選択したドメイン グループ内のすべてのドメインに適用されます。これは、その後ドメイン グループに追加された新しいドメインには適用されません。サブドメイン グループを含めることを選択すると、メンテナンス グループ タグはサブドメイン グループ内のすべてのドメインにも適用されます。
- 手動で定義する
  手動でメンテナンス グループに含めるドメインを選択します。ドメインは、ドメイン グループに属すことも、グループに属さないことも可能です。

ステップ 4 選択に応じた手順を実行します。

選択した項目	選択方法
ドメイン グループごと	**1** ドロップダウン リストからドメイン グループを選択します。 **2** サブドメイン グループのすべてのドメインを含めるかどうかを選択します。 **3** [Create] をクリックします。
手動で定義する	**1** [Add] をクリックして、メンテナンス グループに含めるドメインを追加します。 **2** 下方向へスクロールして、[Select] をクリックします。 **3** [Create] をクリックします。

メンテナンス グループ タグの値の作成

複数のメンテナンス グループ タグを作成するには、[Tag type] ページで作成します。

手順

ステップ 1 [Browse Tables] アイコンをクリックして、[Tag Management] を選択します。
ステップ 2 [Tag Types] をクリックします。
ステップ 3 [Maintenance Group] をクリックして選択します。
ステップ 4 [Edit] をクリックします。
ステップ 5 [Maintenance Group] ダイアログボックスで、[Values] をクリックします。
ステップ 6 [Add] をクリックし、メンテナンス グループの名前を追加します。
ステップ 7 上記のステップを繰り返してメンテナンス グループに必要なすべて値を追加します。
ステップ 8 [Save] をクリックします。

メンテナンス グループに含めるドメインまたはドメイン グループのタグ付け

ドメインに適用できるメンテナンス グループ タグは 1 つだけです。現在 Cisco UCS Central では、ドメインへの複数のメンテナンス グループ タグの適用はサポートしていません。

手順

ステップ 1 [Browse Tables] アイコンをクリックして、[Domains] を選択します。
ステップ 2 ドメインを選択するか、ドメイン グループに基づいてドメインをフィルタ処理し、ドメイン グループに割り当てられているすべてのドメインを選択します。
（注） 個々のドメインについて、そのドメインがドメイン グループに含まれているか、含まれていないかは重要ではありません。これはドメイン インフラストラクチャ ファームウェアの更新には影響しません。
ステップ 3 [Tag] をクリックします。
ステップ 4 [Add Tag] ダイアログボックスの [Type] フィールドで、[Maintenance Group] を選択します。
ステップ 5 [Value] フィールドで、値を選択します。
ステップ 6 [Add] をクリックします。
ステップ 7 このメンテナンス グループに含めるすべてドメインでこれを繰り返します。
メンテナンスグループのリストにすべてのドメインを含めるには、見出しのドメインオプションを選択して [Tag] をクリックします。
ステップ 8 メンテナンス グループに複数のドメイン グループ含めるには、それらが親ドメイン グループのサブドメインである必要があります。ドメイン グループおよびサブドメイン グループに基づいてフィルタ処理し、その検索結果からすべてのドメインにタグを付けます。

インフラストラクチャファームウェア更新スケジュールの設定

[Infrastructure Firmware update] ページでは、新しいジョブのスケジュール設定や、すでに作成されたジョブの日付変更（将来の日付に変更）が行えます。

手順

ステップ 1 [System Tools] アイコンをクリックし、[Firmware Management] を選択します。

ステップ 2 [Firmware Management] ページで、[Tools] アイコンをクリックして、[Schedule Infrastructure Firmware Update] を選択します。

ステップ 3 [Infrastructure Firmware Update] ダイアログボックスで、[Maintenance Group] ドロップダウン リストからタグを選択します。

ステップ 4 更新に使用する UCS ファブリック インターコネクト 製品ファミリおよび適切なファームウェアのバージョンを [Infrastructure firmware version] ドロップダウンから選択します。
使用可能なすべてのシステム ハードウェアをアップデートする必要はありません。また、ファームウェア バージョンの異なる別のハードウェア タイプをアップデートできます。

ステップ 5 ファブリック インターコネクト製品ファミリのドロップ ダウンから互換性のある [Service Pack Version] を選択します。
サービス パックは Cisco UCS Manager 3.1(3) 以降でサポートされます。サービス パックを選択しない場合、ファームウェアのバージョンはリリースの基本の該当するバージョンにロールバックされます。サポートされる/該当するサービス パックのバージョンの詳細については、サービス パックについて，（58 ページ）を参照してください。

（注） サービス パック 3.1(3) 以前でインストールされた Cisco UCS ドメインのダウングレードはサポートされていません。

Cisco UCS Manager 3.1(2) 以前のバージョンから Cisco UCS Manager リリース 3.1(3) へのアップグレードの場合、サービス パックを使用したインフラストラクチャの更新はサポートされません。この場合、Cisco UCS Manager はサービス パックを認識せず、アップグレードは基本バージョンのみを考慮して続行されます。

ステップ 6 （任意） 製品ファミリの [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 7 （任意） 製品ファミリの [Force Deploy] オプションを選択します。[Enable] を選択すると、Cisco UCS は、選択したバージョンをインストールする試行が以前に失敗または中断された場合でもインストールを試行します。アップグレードの検証が失敗すると、アップグレードは失敗します。その場合、障害を解決し、[Force Deploy] オプションを再度選択して、アップグレードを続行する必要があります。
[Force Deploy] オプションと [Fabric Evacuation] オプションはデフォルトで無効になっています。これらのオプションは、Cisco UCS Manager、リリース 3.1(3) 以降でのみサポートされます。それ以前の Cisco UCS Manager バージョンでは、[Enable] オプションを選択しても機能しません。[Tools]

メニュー ドロップダウンから [Configuration Status] を選択するか、または [Domain Status] テーブルをクリックして、ファブリックエバキュエーションのステータスを表示します。

ステップ 8 （任意） 製品ファミリの [Fabric Evacuation] オプションを選択して、AutoInstall 中の IO モジュールまたはファブリック インターコネクト上のトラフィックを開始または停止します。

ステップ 9 ファームウェア更新をすぐにトリガーするには、[Trigger Firmware Update] フィールドの [Immediately] をクリックします。

ステップ 10 ファームウェア更新をスケジュールするには、[Schedule Infrastructure Firmware update] フィールドでアップデートの日時を選択します。

ステップ 11 [User acknowledgment required to install] フィールドで、アップデートにユーザの承認が必要かどうかを選択します。

- [Enabled]：（デフォルト値）ドメインをアップデートするには手動でアップデート要求を承認する必要があります。

  （注） ドメイン グループがメンテナンス グループに含まれていても、確認はドメインごとです。

- [Disabled]：ファームウェア更新はスケジュールどおりに動作します。

ステップ 12 [Schedule] をクリックします。
[Firmware Management] ページでファームウェア更新を監視できます。ジョブ リストには、設定済みのファームウェア更新スケジュールが表示されます。

デスクトップ ファームウェア管理ウィジェットには、設定済みのファームウェア更新スケジュールがすべて表示されます。ファームウェア更新のステータスは、[Configuration Settings] ウィンドウで確認できます。

スケジュールされたインフラストラクチャファームウェアの更新ジョブの編集

手順

ステップ 1 [System Tools] アイコンをクリックし、[Firmware Management] を選択します。

ステップ 2 ジョブ リストの特定のジョブを選択し、[Edit] をクリックします。

ステップ 3 適切な変更を行って、[Schedule] をクリックします。

（注） すでにトリガーされた状態または最後にトリガーされた状態のジョブは編集できません。

インフラストラクチャファームウェア更新ポリシーの確認

開始前にユーザの承認を必要とするようにインフラストラクチャ ファームウェア更新ジョブを設定すると、Cisco UCS Central はこの承認が発生するまで起動しません。

手順

ステップ 1 [Domains Impacted] テーブルで、[Firmware Status] 列が [Start Pending] に変わったら、[Alerts] アイコンをクリックして [Pending Activities] を選択します。

ステップ 2 [Acknowledge] をクリックしてメインのファームウェア更新を開始します。

ステップ 3 [Firmware Status] 列が [Pending User Acknowledgment] に変わる場合は、Cisco UCS Central がファブリック インターコネクトを再起動するためにユーザの承認が必要であることを示します。再起動を承認するには、ステップ 1 および 2 を繰り返します。

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。

- Maintenance group - メンテナンス グループ名。
- Scheduled for - スケジュールされたファームウェア更新、およびすでにトリガーされている場合はステータスの詳細。
- User Ack - ユーザ承認のステータス。ファームウェアを更新する前に、[User Ack] が [Enabled] の場合、[Alerts] > [Pending Activities] ページでユーザ承認が必要です。

[Maintenance Group] についてスケジュールされた [Infrastructure Firmware Management] の次の詳細が右パネルに表示されます。選択した [Service Pack Version] が右パネルに表示されます。

- Product family - 適切な FI 製品ファミリ
- Firmware Version - 選択したファームウェアのバージョン
- Service Pack Version - 製品ファミリの選択したサービス パックのバージョン互換性のないサービス パックのバージョンを選択して、アップグレードのスケジュールを設定することはできません。Cisco UCS Manager のリリース用にサポートされているサービス パックのバージョンの詳細については、サービス パックについて, （58 ページ）を参照してください。
- Catalog Version - 製品ファミリのカタログ バージョンの詳細。

- Force Deploy - 製品ファミリの [Force Deploy] オプション。[Enable] を選択すると、Cisco UCS は、ファームウェア更新の選択したバージョンをインストールする試行が以前に失敗または中断された場合でもインストールを試行します。
- Evacuation - 製品ファミリの [Evacuation] オプションを選択して、AutoInstall 中の IO モジュールまたはファブリック インターコネクト上のトラフィックを開始または停止します。
- Impacted Domain - 現在のバージョン、導入しているサービス パックのターゲット バージョン、ファームウェア ステータス、および影響を受けるドメインのドメイン ステータス。

（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有効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。

インフラストラクチャ ファームウェアの更新の防止

インフラストラクチャ ファームウェアの更新を防ぐにはさまざまな方法があります。

- インフラストラクチャ ファームウェアの更新ジョブのキャンセル
- メンテナンス グループからのドメインの削除または除外
- メンテナンス タグの値の削除

メンテナンス グループからのドメインの削除または除外

複数のドメインに影響があるメンテナンス グループからドメインを削除する場合、アップグレードを開始する前に、ドメインに割り当てられたメンテナンス タグを削除します。これによりポリ

シーがドメインに影響することを回避します。インフラストラクチャ ファームウェア更新の開始後、ドメインにタグが付けられていなければ、ドメインがアップデートされます。

手順

ステップ 1 [Browse Tables] アイコンをクリックして、[Domains] を選択します。

ステップ 2 ドメインを選択します。
IP アドレスの下に割り当てられたタグが表示されます。

ステップ 3 メンテナンス タグの名前ラベル内の [X] をクリックし、タグを解除してメンテナンス グループから削除します。
警告が表示されます。

ステップ 4 [Delete] をクリックします。

ファームウェア更新ジョブのキャンセル

これはドメインに含まれるすべてのジョブを取り消します。

手順

ステップ 1 [System Tools] アイコンをクリックし、[Firmware Management] を選択します。

ステップ 2 ジョブ リストからジョブを選択します。

ステップ 3 [Delete] をクリックします。

メンテナンス グループの値の削除

重要 メンテナンス グループの値、またはタグを削除する前に、それらに関連付けられているジョブがないことを確認します。

- アップグレードの開始**前**にメンテナンス タグを削除すると、ユーザへの通知後にアップグレード プロセスが削除します。
- アップグレードの開始**後**にメンテナンス タグを削除すると、アップグレードは継続されます。
- メンテナンス タグを削除してその後にジョブのスケジュールがある場合は、メンテナンス タグを再作成します。ジョブはドメインで実行されます。

- メンテナンスのタグを削除しても、ジョブは削除されません。これは、どのようなジョブがスケジュールされていたか、またどのドメインが影響を受けたかが分かるように、履歴の目的で保存されます。

手順

ステップ 1 [Browse Tables] アイコンをクリックして、[Tag Management] を選択します。
ステップ 2 [Tag Types] をクリックします。
ステップ 3 [Maintenance Group] をクリックして選択します。
ステップ 4 [Edit] をクリックします。
ステップ 5 [Maintenance Group] ダイアログボックスで、[Values] をクリックします。
ステップ 6 タグを選択して [Delete] 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更新とディザスタ リカバリ

Cisco UCS Central では、2 種類のバックアップを実行します。

[Backup for Cisco UCS Domain]：Cisco UCS Manager ドメイン全体のスナップショットを含むバイナリ ファイルを作成します。スケジュールされたインフラストラクチャ ファームウェアのアップグレード ジョブは UCS ドメインに含まれていません。そのため、ドメインの復元は、スケジュールされたインフラストラクチャ ファームウェアのアップグレード ジョブには影響しません。

[Backup for Cisco UCS Central]：Cisco UCS Central システム全体のスナップショットを含むバイナリ ファイルを作成します。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。このバックアップからの復元は、ジョブ スケジュールに影響する可能性があります。

重要 Cisco UCS Central のリリース 2.0 へのアップグレードの影響があるため、アップグレードする前に、すべてのドメイン グループの更新を行うことをお勧めします。ユーザ確認応答が保留中の更新ジョブがないことを確認します。すべてのジョブがアップグレード中に削除されるため、リリース 2.0 で作成しなおす必要があります。

シナリオ	影響
過去にジョブをスケジュールした Cisco UCS Central バックアップを復元します。	**影響なし**：更新は影響を受けません。バックアップ ファイルにはメンテナンス タグと登録済みドメイン情報が含まれます。それまでのジョブは含まれないので影響は受けません。それまでの日付でスケジュールされたジョブは実行されません。
将来にジョブをスケジュールした Cisco UCS Central バックアップを復元します。	**影響なし**：ジョブはスケジュールどおりに実行されます。
Cisco UCS Central システムは、インフラストラクチャ ファームウェアの更新を実行している間にクラッシュします。	**影響あり**：Cisco UCS Central システムの回復後はジョブは実行されません。スケジュールをしなおす必要があります。
構成のバックアップを復元します。	**影響なし**：構成のバックアップには、ジョブ情報は含まれませんが、メンテナンスのタグ情報が含まれます。交換オプションを使用して構成のバックアップから復元すると、復元されたシステムにはジョブ情報が含まれていません。統合オプションを使用して復元し、将来の日付でジョブをスケジュールしていた場合、バックアップからのタグ付けされたドメインは将来のジョブに含まれます（この情報は影響を受けたドメイン リストに表示されます）。
現在のシステムと完全な状態のバックアップをマージします。	**多少の影響あり**：現在スケジュールしているものはオーバーライドしませんが、ジョブの記述を復元しないため、そのジョブを再作成する必要があります。
Cisco UCS Manager ドメインは表示されなくなり、更新の前または最中に登録解除されるようになります。	**影響あり**：ドメインが再度表示されたときに更新は再度開始されません。手動で開始する必要があります（オンデマンドで）。
完全な状態のバックアップを作成します。ドメインのタグを外します。バックアップから復元します。	**影響あり**：ドメインがバックアップにタグ付けされているため、バックアップの復元時タグ付けされたままになっています。ジョブを将来にスケジュールしていた場合は、ドメインが含まれています。これを防ぐには、再度ドメインのタグを外します。

シナリオ	影響
ジョブの実行中、編集します。	**影響なし**：進行中はジョブを編集できません。ただし、ドメインからメンテナンス タグを削除したり、最初の保留中の確認応答要求を確認する前に、ジョブを削除することができます。
HA フェールオーバーが発生します。	**影響なし**：スケジュールされたジョブは通常どおり実行されます。
Cisco UCS Central の以前のリリースからアップグレードします。	**影響あり**：以前のバージョンはドメイン グループごとにファームウェアを更新しました。現在のバージョンではメンテナンス グループごとに更新します。ドメイン グループまたはスケジュールされたジョブの情報はアップグレード中は保存も転送もされません。メンテナンス グループを作成し、含めるドメインをタグ付けする必要があります。さらに、すべてのインフラストラクチャ ファームウェアの更新ジョブを再作成し、スケジュールしなおす必要があります。

Lightweight のアップグレードについて

Cisco UCS Central 2.0 には、ファームウェアのアップグレードを強化し、サービス パックによってセキュリティ更新を提供する Lightweight のアップグレードが導入されています。サービス パックは、固有のものであり、メンテナンス リリースに累積されます。Cisco UCS Central は、Cisco UCS Manager バージョン 3.1(3) 以降のサービス パックによってファームウェアのアップグレードをサポートしています。

- Lightweight のアップグレードでは、次の方法でファームウェアのアップグレードを強化しています。
  - コンポーネントのファームウェア バージョンは、変更された場合にのみ更新されます。
  - セキュリティ更新はサービス パックを通じて提供されます。
  - サービス パック内では、更新は特定のコンポーネントにのみ適用される場合があります。これらのコンポーネントは、エンドポイントの再起動なしでアップグレードされることがあります。
  - インフラストラクチャおよびサーバ コンポーネントの更新は、共通のサービス パック バンドルを通じて提供されます。サーバ コンポーネントについては、変更したファームウェア イメージのみがサービス パック バンドルの一部となります。

サービス パックについて

サービス パックは、Cisco UCS Manager インフラストラクチャとサーバ コンポーネントにセキュリティ更新を適用するために使用できるパッチです。サービス パックは、基本リリースに固有のものです。サービス パックは、インフラストラクチャ コンポーネントとサーバ コンポーネント用の単一バンドルとして提供されます。

サービス パックのバージョンには、次のガイドラインが適用されます。

- サービス パックは基本のバンドルにのみ適用できます。サービス パックは単独でインストールできません。たとえば、サービス パック 3.1(3)SP2 は 3.1(3) リリースにのみ適用できます。3.1(4) またはそれ以降のリリースと互換性がありません。
- サービス パックではこれまでの修正内容が累積されています。同じメンテナンス リリースであれば、どのパッチ バージョンでも最新のサービス パックを適用できます。たとえば、3.1(3)SP3 には、3.1(3)SP2 および 3.1(3)SP1 に行われたすべての修正が含まれます。任意の 3.1(3) リリースに 3.1(3)SP3 を適用できます。
- 個別のメインテナンス リリースのサービス パックのバージョンの番号付けに関連はありません。たとえば、サービス パック 3.1(3)SP2 と 3.1(4)SP2 は別個のもので関連はありません。
- 個別のサービスパックを使用して、メンテナンス リリースごとに同じ修正を適用できます。たとえば、3.1(3)SP2 および 3.1(4)SP3 で同じ修正を適用できます。
- メンテナンス リリースのサービス パックを、デフォルトのサービス パックのバージョンより下のバージョンにダウングレードすることはできません。次に例を示します。
  - 基本バンドルのバージョン：3.1(3b)
  - デフォルトのサービス パックのバージョン：3.1(3)SP2（デフォルト）
  - 実行中のサービス パックのバージョン：3.1(3)SP3
  - サービス パックは、3.1(3)SP2 より下にダウングレードできません
- サービス パックのアップグレードまたはダウングレードが失敗すると、そのメンテナンス リリースのデフォルトのサービスパックのバージョンが実行中のサービスパックのバージョンになります。
- サービス パックの選択を削除することにより、基本リリースに適用されたサービス パックをロールバックできます。

次の表は、Cisco UCS Manager のリリース バージョンおよびサービス パックが適用されるさまざまな状況で導入された実行中のバージョンを示しています。

更新のシナリオ	バンドルのバージョン	サービス パックのバージョン
同じメンテナンス リリースでのサービス パックの更新	バンドルのバージョンは変更されません	サービス パックは、指定したバージョンに更新されます

更新のシナリオ	バンドルのバージョン	サービス パックのバージョン
サービス パックの削除	バンドルのバージョンは変更されません	サービス パックは、バンドルに付属するデフォルトのバージョンです
別のメンテナンス リリースへの基本バンドルの更新	基本バンドルは、指定したメンテナンス リリースのバージョンに変更されます	現在のサービス パックが削除され、基本バンドルのデフォルトのバージョンに更新されます
別のメンテナンス リリース、およびサービス パックに更新されます	基本バンドルは、指定したメンテナンス リリースのバージョンに変更されます	サービス パックは、指定したバージョンに更新されます

ファームウェア アップグレード用の互換性のあるサービス パックの選択の詳細については、「ホスト ファームウェア パッケージ ポリシー」、「インフラストラクチャ ファームウェアの更新のスケジューリング」および「シャーシ ファームウェア パッケージ ポリシー」を参照してください。

第 6 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。バックアップをスケジュールしてポリシーを復元することができます。Cisco UCS Central の即時オンデマンド バックアップまたは選択したドメイン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。

スケジュール済みバックアップ ポリシーはデフォルトで無効になっています。Cisco UCS Central または登録済み UCS ドメインをバックアップするには、この両方のバックアップ状態を有効にします。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。

Cisco UCS Central は、バックアップの Cisco UCS Central リポジトリを使用して設定したポリシーをリモートで制限します。これは、Cisco UCS Manager によって内部的にマウントされます。

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、どちら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

バックアップ操作を前もって作成し、そのバックアップの実行準備が整うまで管理状態を無効のままにしておくことはできます。Cisco UCS 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 ファイルを保存したり、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。

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。Cisco UCS Central からポートを再設定します。

バックアップ タイプ

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

- [Full-state]：完全な状態のバックアップはインストール時にのみ指定できます。Full State バックアップは、システム全体のスナップショットを含むバイナリ ファイルです。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。

- [Config-all]：全設定バックアップは、すべてのシステムおよび論理構成設定を含むXMLファイルです。このファイルは、インストール時のシステム復元には使用できません。
- [Config-logical]：論理設定バックアップは、すべての論理構成設定を含むXMLファイルです。サービスプロファイル、VLAN、VSAN、プール、ポリシー、ユーザ、ロケール、LDAP、NTP、およびDNS認証と管理設定が含まれます。これらの構成設定をインポートするときに、このバックアップから生成されたファイルを使用できます。このファイルは、インストール時の完全な状態のシステム復元には使用できません。
- [Config-system]：システム構成バックアップは、統計情報設定とスケジューラ情報を含むXMLファイルです。これらの構成設定をインポートするときに、このバックアップから生成されたファイルを使用できます。このファイルは、インストール時の完全な状態のシステム復元には使用できません。

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 ロケーションを指定する場合は、そのロケーションが存在していることを確認します。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：*/home/user01/central*
- 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

手順

ステップ 1 [Actions] バーで次のように入力します。 [Schedule Central Backup] で、Enter キーを押します。

ステップ 2 （任意） [Central Backup] ダイアログボックスの [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。

- [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, （23 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。
（注） リモートの絶対パスは、*/home/user01/central* です。

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。

フィールド名	説明
Transfer Protocol	転送プロトコルを選択します。 • FTP • SFTP • TFTP • SCP
Absolute Remote Path	絶対リモート パス。
Remote Server Host Name/IP Address	リモート サーバの IP アドレス。
User Name	リモート サーバのユーザ名。
Password	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。
- 手動バックアップを設定するには、この形式で絶対リモート パスを指定します：*/path/filename.tgz*

- スケジュール済みバックアップを設定するには、ファイル名を含めずホーム フォルダのパス（/）を指定します。SFTP では、ホーム フォルダのパスを指定する前に、SFTP サーバでパスおよび必須のサブフォルダ/ディレクトリを作成する必要があります。フォルダが事前に設定されていないと、エクスポートは失敗します。たとえば、SFTP サーバのホーム フォルダのパスを *C:\sftp* に設定して、階層内に他のフォルダがなく、絶対リモート パスを *C:sftp\abc* と指定すると、このシステムにはそのようなディレクトリがないため、エクスポートは失敗します。

はじめる前に

リモート ロケーションを指定する場合は、そのロケーションが存在していることを確認します。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

手順

ステップ 1 [Actions] バーで次のように入力します。 [Schedule Domain Backup]。

ステップ 2 完全状態バックアップをスケジュールする [Domain Group] 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 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。

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。

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。

フィールド名	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	絶対リモート パス。

フィールド名	説明
Remote Server Host Name/IP Address	リモート サーバの IP アドレス。
User Name	リモート サーバのユーザ名。
Password	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：`/home/test/central/file.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

手順

ステップ 1 [System Tools] アイコンをクリックし、[Backup & Restore] を選択します。

ステップ 2 [UCS Central and Domains] のリストで、[UCS Central] をクリックするか、またはドメイン 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。

ステップ 4 [Backup] ダイアログで、[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。

Cisco UCS Central は、指定したリモート ロケーションに完全状態のバックアップ ファイルを作成して保存します。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 オンデマンドの完全状態バックアップに障害が発生すると、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、Cisco UCS Central はバックアップ リポジトリにバックアップ ファイルを作成します。

Cisco UCS ドメインの完全状態バックアップの削除

下記の手順に加えて、次のシナリオで完全状態のバックアップを無効化または削除できます。

- 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。

手順

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

ステップ 2 [Backup and Restore] ページで、[Tools] アイコンをクリックし、[Remove Domain Backup Schedule] を選択します。

ステップ 3 [Domain Backup Schedule] ダイアログボックスで、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

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

- 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。

手順

ステップ 1 [System Tools] アイコンをクリックし、[Backup & Restore] を選択します。

ステップ 2 [Backup and Restore] ページで、[Tools] アイコンをクリックし、[Remove Central Backup Schedule] を選択します。

ステップ 3 [Central Backup Schedule] ダイアログ ボックスで、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

手順

ステップ 1 System Tools アイコンをクリックし、[Backup & Restore] を選択します。

ステップ 2 [UCS Central and Domains] のリストで、[UCS Central] またはドメインを選択します。

ステップ 3 右側のペインに、バックアップ ファイルのリストを表示します。バックアップ ファイルごとに、ステータス、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。

スケジュール済みバックアップ ポリシーはデフォルトで無効になっています。Cisco UCS Central または登録済み Cisco UCS ドメインをバックアップするには、この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。

Cisco UCS Central は、バックアップの Cisco UCS Central リポジトリを使用して設定したポリシーをリモートで制限します。これは、Cisco UCS Manager によって内部的にマウントされます。

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, （69 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。
- Cisco UCS ドメインから登録が解除された後にのみバックアップを削除できます。

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**：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 ドメインに Cisco UCS Manager リリース 2.2(2x) がない場合、リモート バックアップを使用するグローバル バックアップ ポリシーは機能しません。

バックアップのスケジュール時に、どちら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。

コンフィギュレーション ファイルのインポート

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 ロケーションを指定する場合は、そのロケーションが存在していることを確認します。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

手順

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

ステップ 2 [UCS Central and Domains] のリストで、[UCS Central] をクリックします。

ステップ 3 [Tools] 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 ロケーションを指定する場合は、そのロケーションが存在していることを確認します。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

手順

ステップ 1 [System Tools] アイコンをクリックし、[Export and Import] を選択します。

ステップ 2 [UCS Central and Domains] のリストで、[Tools] アイコンをクリックして [Schedule Domain Export] を選択します。

ステップ 3 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。

ステップ 4 [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 5 [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 6 （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、リモートの場所と関連情報を入力します。

ステップ 7 [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 ロケーションを指定する場合は、そのロケーションが存在していることを確認します。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

手順

ステップ 1 [System Tools] アイコンをクリックし、[Export and Import] を選択します。
ステップ 2 [UCS Central and Domains] のリストで、[UCS Central] をクリックします。
ステップ 3 エクスポートする構成のバックアップ ファイルを選択します。
ステップ 4 [Config Export] アイコンをクリックします。
ステップ 5 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 6 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 7 [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

手順

ステップ 1 [System Tools] アイコンをクリックし、[Export and Import] を選択します。
ステップ 2 UCS セントラルとドメイン リストで、ドメインを選択します。
ステップ 3 エクスポートするドメインのバックアップ ファイルを選択します。
ステップ 4 [Config Export] アイコンをクリックします。
ステップ 5 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 6 [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 7 [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。

手順

ステップ 1 [System Tools] アイコンをクリックし、[Export and Import] を選択します。

ステップ 2 UCS セントラルとドメイン リストで、UCS セントラルを選択します。

ステップ 3 [Config Import] アイコンをクリックします。

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、設定を Cisco UCS Central にインポートする場所を選択します。

- [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]：ローカル ファイルの場所を参照して、ファイルを選択します。
- [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。

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 ドメインが一時停止状態にある、表示されない、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。

手順

ステップ 1 [System Tools] アイコンをクリックし、[Export and Import] を選択します。

ステップ 2 [UCS Central and Domains] リストで、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。

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。

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

手順

ステップ 1 [System Tools] アイコンをクリックし、[Export and Import] を選択します。

ステップ 2 [Config Export & Import] ページで、[Tools] アイコンをクリックし、[Remove Central Export Schedule] 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。

手順

ステップ 1 [System Tools] アイコンをクリックし、[Export and Import] を選択します。

ステップ 2 [Config Export & Import] ページで、[Tools] アイコンをクリックし、[Remove Domain Export Schedule] 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

手順

ステップ 1 System Tools アイコンをクリックし、[Backup & Restore] を選択します。

ステップ 2 [UCS Central and Domains] のリストで、[UCS Central] またはドメインを選択します。

ステップ 3 右側のペインに、バックアップファイルのリストを表示します。バックアップファイルごとに、ステータス、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 7 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、「Smart Call Home の障害」に一覧表示される Cisco UCS Central の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、「UCS Manager の Call Home の設定」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、「Smart Call Home の障害」に一覧表示される Cisco UCS Central の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、「UCS Manager の Call Home の設定」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。

手順

ステップ 1 [System Configuration] アイコンをクリックし、[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。
Cisco UCS Central はこのメール アドレスの最初の登録とアラート通知を送信します。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 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。無効イベントが発生した場合は通知を受信しません。

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] をクリックします。

Smart Call Home の登録

最初に Cisco UCS Central Smart Call Home を無効にすると、Cisco UCS Central によってシステム 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。

障害名	障害コード	説明
fltSysdebugCoreCoreFile	F10000005	障害はプロセスのいずれかが応答を停止したときに発生します。Cisco UCS Central によりコア ファイルが生成されます。
fltExtpolProviderProviderLostConnectivity	F10000190	プロバイダーに Cisco UCS Central の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	コントローラに、Cisco UCS Central の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	登録された UCS ドメインに Cisco UCS Central の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	複数のサービス プロファイルが同じ ID を所有しています。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	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	障害は、TrustPoint 証明書のステータスが無効になっている場合に発生します。
ltPkiKeyRingStatus	F10000592	障害は、変調証明書のステータスが無効になっている場合に発生します。
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	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	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 機能を使用してドメイン グループの Cisco UCS Manager アラートを表示します。

手順

ステップ 1 [Domain Group Navigation] アイコンをクリックして、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 [Settings] をクリックして Call Home を起動します。

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]：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]：受信するアラートのタイプを選択します。
c) [Alert Recipients]：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] をクリックします。