Microsoft Azure Stack 向けシスコ統合システム 『Operations Guide』

初版：2018 年 9 月 17 日

最終更新：2021 年 3 月 10 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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2018–2021 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章 **概要** 1

ガイドの概要 1

第 2 章 **サポート ガイダンス** 3

サポート ケースの作成 3

サポート ケース マネージャ 3

Support Case Manager にログインする 4

Support Case Manager からケースを開く 4

関連 Microsoft Azure Stack 向けシスコ統合システム 資料 5

第 3 章 **Azure Stack Hub の開始および停止** 7

Azure Stack Hub の開始および停止 7

Azure Stack Hub の停止 7

Azure Stack Hub の開始 8

Azure Stack Hub の起動ステータスの取得 10

Azure Stack Hub 起動とシャットダウンのトラブルシューティング 10

第 4 章 **Secret Rotation** 13

Secret Rotation 13

Cisco Nexus Top of Rack Switch の Rotating Secrets 14

Rotating Secrets of Cisco UCS Manager の Rotating Secrets 14

第 5 章 **Upgrade Firmware** 19

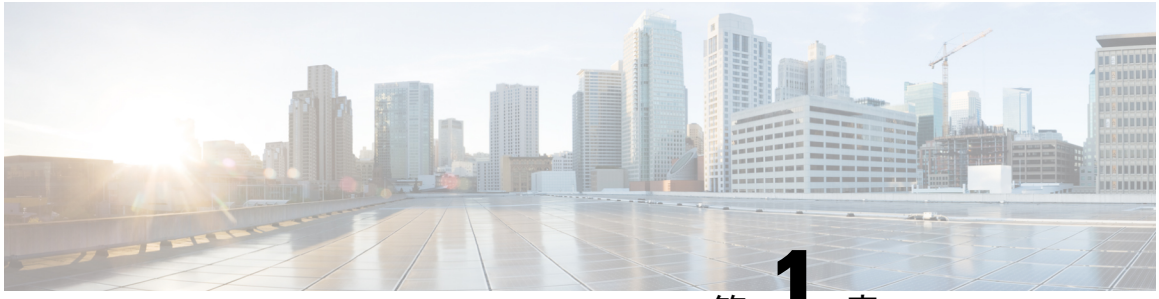
ファームウェア アップグレードの概要 19

インストールされているファームウェアの識別 20
UCS インフラストラクチャおよびサーバ ファームウェア 21
Top-of-Rack Nexus スイッチ ファームウェア 21
ファームウェア アップグレード中の既知の動作 22
Cisco Azure Stack Hub Platform アップグレード自動化 23
Cisco Azure Stack Hub Platform アップグレード 自動化の設定 25

第 6 章 容量の管理 29
物理メモリ容量の管理 29
スケール ユニット ノードの追加 30
管理 IP プールの拡張 31
スケール ユニット ノードの追加 33

第 7 章 ハードウェアの交換 39
ハードウェアの交換 39
ディスクの交換 39

第 8 章 システムの管理 41
UCS の Call Home の概要 41
Call Home の考慮事項とガイドライン 43
Cisco UCSの障害と Call Home の重大度 44
Call Home の設定 44
Call Home の有効化 48
Call Home の無効化 48



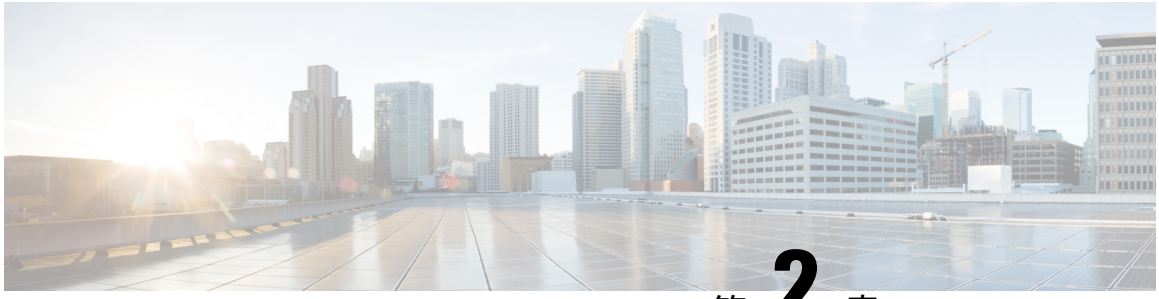
第 1 章

概要

- ガイドの概要 （1 ページ）

ガイドの概要

このガイドは、Azure Stack Hub ハードウェアのライフサイクルを所有し、維持する Azure Stack Hub オペレータを対象としています。このガイドは、https://docs.microsoft.com/en-us/azure-stack/operator/ の Azure Stack Hub operator ドキュメンテーションの「**ハウツーガイド > Azure Stack Hub の管理**」セクションを補足しています。



第 2 章

サポート ガイダンス

- サポート ケースの作成 （3 ページ）
- サポート ケース マネージャ （3 ページ）
- 関連 Microsoft Azure Stack 向けシスコ統合システム 資料 （5 ページ）

サポート ケースの作成

インストールが完了したら、ハンドオーバープロセスの一環として、プロフェッショナルサービス エンジニアとともにデジタル オンボーディング プロセスを実行する必要があります。このプロセスを実行することで、お使いのシステムが Cisco Service Contract の保証対象となり、契約番号と連絡先情報が Cisco Service Contract System（CSCC）内で更新されます。

シスコ サポート ケースは、次の 3 つの方法で開くことができます。

- 電話で TAC に連絡する：シスコのワールドワイドな連絡先
- 電子メールで TAC に連絡する：tac@cisco.com（ワールドワイドな連絡先リンクの追加の言語サポート）
- サポート ケース マネージャからケースを開く

サポート ケース マネージャ

Support Case Manager（SCM）は、エンドツーエンドのケース管理機能を提供します。SCM を使用するには、シスコ プロファイルのユーザ ID とパスワード、有効なサービス契約番号、サポートが必要な製品のシリアル番号または仮想ライセンス番号、対応インターネットブラウザが必要です。対応ブラウザには、Mozilla Firefox バージョン 10 以降、Google Chrome バージョン 20 以降、Safari バージョン 5 以降、および最新バージョンの Microsoft Internet Explorer などがあります。

- SCM 用のシスコ ユーザ ID を登録するには、ブラウザで次の URL を開きます。
  https://idreg.cloudapps.cisco.com/idreg/register.do

- SCM へのアクセスを要求するには、シスコ ユーザ ID と契約番号を web-help-sr@cisco.com に入力します。

このプロセスのスクリーン ショットについては、SCM の概要を参照してください。

Support Case Manager にログインする

手順

ステップ 1 ブラウザで次の URL にアクセスします。https://mycase.cloudapps.cisco.com

ステップ 2 シスコ プロファイルのユーザ ID とパスワードを入力し、[ログイン（Log In）] をクリックします。

Support Case Manager からケースを開く

始める前に

Support Case Manager にログインします。

手順

ステップ 1 ホーム ページで [新しいケースを開く（Open New Case）] をクリックして、[権限付与（Entitlement）] ページに進みます。

ステップ 2 [シリアル番号による製品の検索（Find Product by Serial Number）] フィールドに、サーバまたはスイッチのシリアル番号を入力します。

この情報はサービス契約で提供されています。

ステップ 3 [検索（Search）] をクリックします。

ステップ 4 検索結果の一覧から、このケースに必要な製品をクリックします。

ステップ 5 [次へ（Next）] をクリックします。

[問題の説明（Describe Problem）] ページが表示されます。製品タイプ、契約、ユーザ権限に基づいて重大度が割り当てられます。

ステップ 6 要求されたケースの詳細（[タイトル（ Title）] および要求を要約した [説明（Description）] など）を入力します。[タイトル（Title）] には最大 80 文字、[説明（Description）] には最大 32,000 文字を入力できます。

ステップ 7 [テクノロジー（Technology）] フィールドで [参照（Browse）] をクリックして、[テクノロジーの選択（Select Technology）] ウィンドウを開き、[Azure Stack] を検索します。

ステップ 8 [Azure Stack：（ソリューションサポート契約が必要）（Azure Stack - (Solution Support Contract Required)）] を選択し、[選択（Select）] をクリックします。

ステップ 9 [問題領域（Problem Area）] ドロップダウン リストから該当する障害を選択します。

ステップ 10 [コンタクト情報（Contact Preference）] 領域を確認します。ここで入力したコンタクト情報は、デフォルトの情報をオーバーライドし、このケースにのみ適用されます。

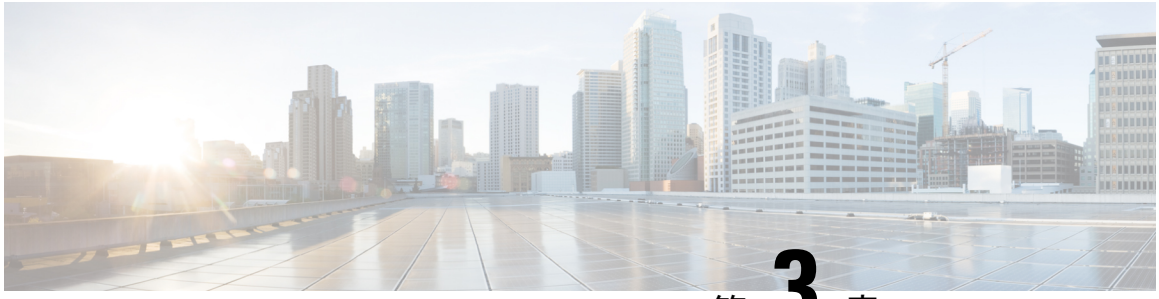
ステップ 11 [提出 (Submit)] をクリックします。

権限付与レベルに基づき、Cisco Solution Support エンジニアがご連絡いたします。Cisco Solution Support は、シスコ製品の問題を管理し、Microsoft Azure Stack サポート チームとの調整を行う単一の窓口です。

関連 Microsoft Azure Stack 向けシスコ統合システム 資料

Microsoft Azure Stack 向けシスコ統合システム の資料の詳細なリストについては、次の URL を参照してください。

Microsoft Azure Stack 向けシスコ統合システム



第 3 章

Azure Stack Hub の開始および停止

- Azure Stack Hub の開始および停止 （7 ページ）
- Azure Stack Hub の停止 （7 ページ）
- Azure Stack Hub の開始 （8 ページ）
- Azure Stack Hub の起動ステータスの取得 （10 ページ）
- Azure Stack Hub 起動とシャットダウンのトラブルシューティング （10 ページ）

Azure Stack Hub の開始および停止

Microsoft Azure Stack 向けシスコ統合システム で Azure Stack Hub サービスをシャットダウンして再起動することができます。Azure Stack Hub 環境全体をシャットダウンすると、物理的に電源がオフになります。すべてのインフラストラクチャの電源をオンにし、テナント リソースをシャットダウン前の電源状態に戻します。次の手順は、Azure Stack Hub サービスを適切にシャットダウンして再起動する方法を示しています。

Microsoft 固有の手順の最新バージョンについては、Microsoft のマニュアルを参照してください。

Azure Stack Hub の停止

Azure Stack Hub をシャットダウンするには、次の手順を実行します。

手順

ステップ 1 今後のシャットダウンのために、Azure Stack Hub 環境のテナント リソースで実行されているすべてのワークロードを準備します。

ステップ 2 Privileged Endpoint (PEP) セッションを、Azure Stack Hub ERCS VM へのネットワーク アクセスを有するマシンから開きます。

詳細については、『Azure Stack Hub の権限エンドポイントを使用する』を参照してください。

ステップ 3 PEP から、**Stop-AzureStack** を実行します。

ステップ 4 すべての物理 Azure Stack Hub ノードの電源がオフになるまで待ちます。

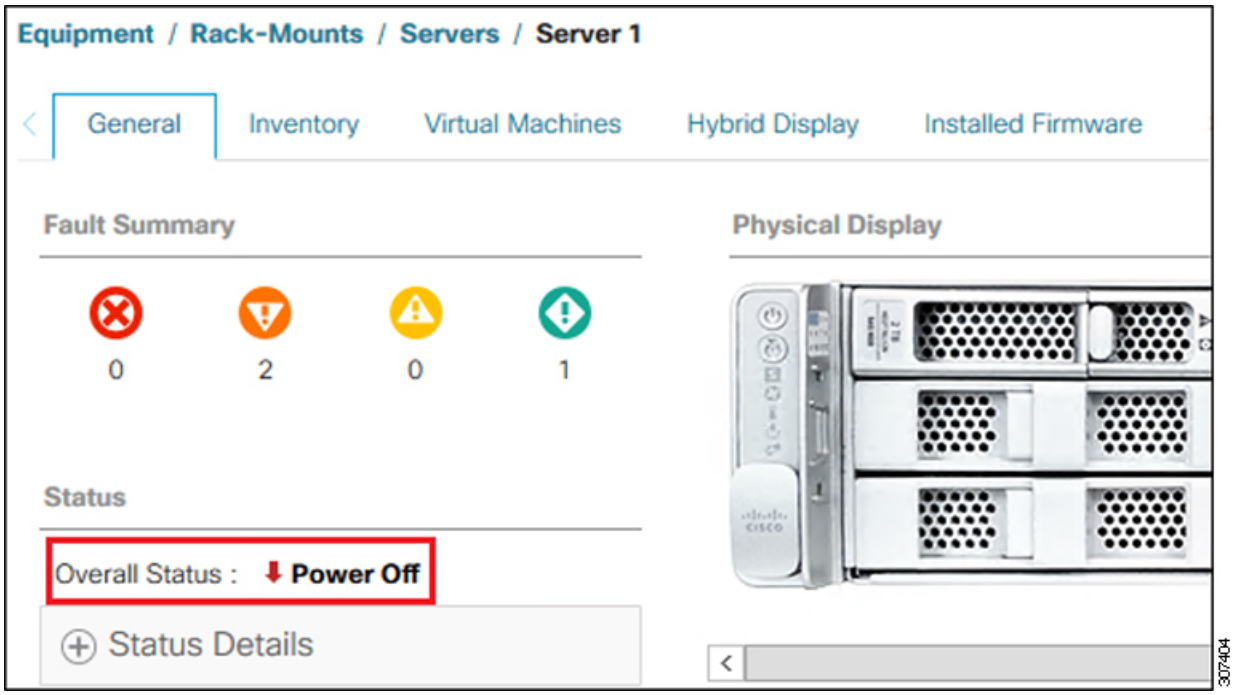
ステップ 5 管理者クレデンシャルを使用して、Cisco UCS Manager (https://< *UCS_Manager_IP* >) にログインします。

（注） Cisco UCS Manager の IP アドレスは、展開時に提供される Cisco 展開ワークシート補足ドキュメントで入手できます。

ステップ 6 Cisco UCS Manager GUI から **[Navigation (ナビゲーション)]** ペインで、**[Equipment (機器)]** をクリックします。

ステップ 7 **[Equipment (機器)]** > **[Rack Mounts (ラック マウント)]** > **[Servers (サーバ)]** を展開し、すべてのサーバが**電源オフ**状態になっていることを確認します。

ステップ 8 すべての物理サーバが**電源オフ**状態になったら、Azure Stack Hub ラックから電源を取り外すことができます。



Azure Stack Hub の開始

Azure Stack Hub を開始するには、Azure Stack Hub の停止方法に関係なく、次の手順を実行します。

手順

ステップ 1 管理者クレデンシャルを使用して、Cisco UCS Manager (https://< *UCS_Manager_IP* >) にログインします。

（注） Cisco UCS Manager の IP アドレスは、展開時に提供される Cisco 展開ワークシート補足ドキュメントで入手できます。

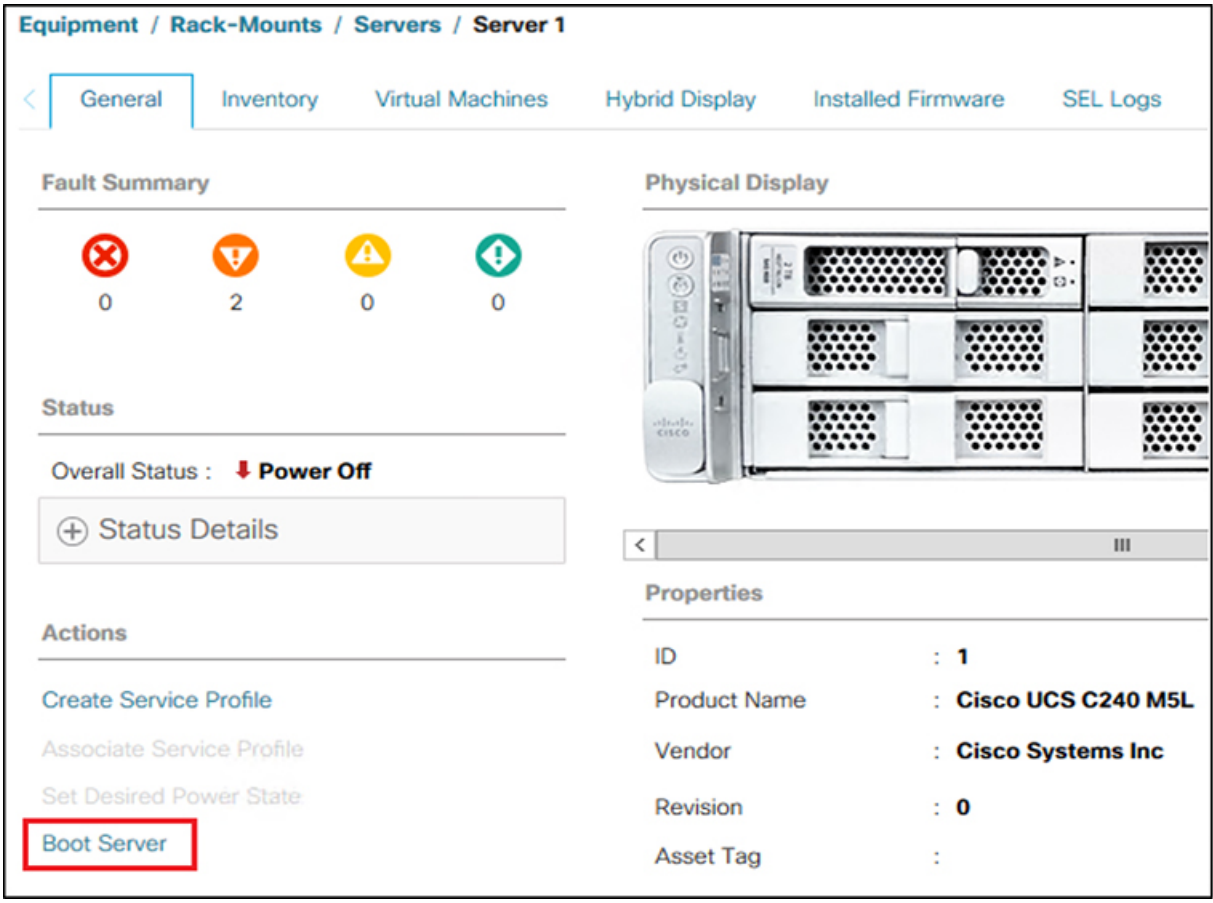
ステップ 2 [Navigation] ペインで [Equipment] をクリックします。

ステップ 3 **[Equipment]** > **[Rack Mounts]** > **[Servers] の順に展開します。**

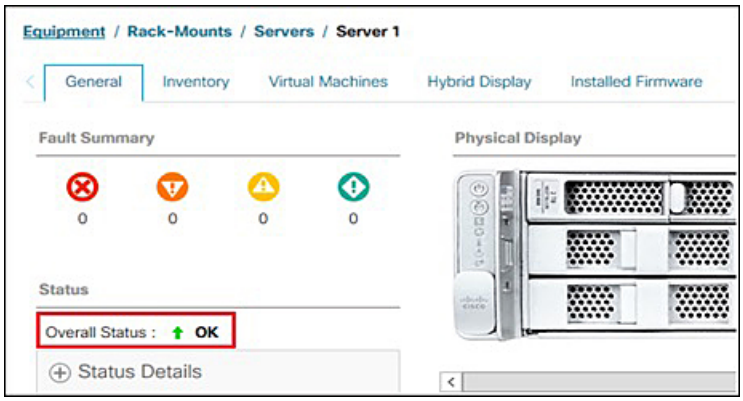
ステップ 4 ブートするサーバを選択します。

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

ステップ 6 [Actions] 領域の [Boot Server] をクリックします。



サーバが起動した後は、**[General (全般)]** タブの **[Overall Status (全体ステータス)]** フィールドに数分で **[OK]** ステータスが表示されます。



ステップ 7 Azure Stack Hub インフラストラクチャ サービスが開始されるまで待機します。

Azure Stack Hub インフラストラクチャ サービスは、開始プロセスを完了するのに 2 時間かかることがあります。Get actionstatus コマンドレットを使用して、Azure Stack Hub の開始ステータスを確認できます。

ステップ 8 すべてのテナント リソースが、シャットダウン前の状態に戻っていることを確認します。テナント リソースで実行されているワークロードは、ワークロード マネージャによる起動後に再設定する必要がある場合があります。

Azure Stack Hub の起動ステータスの取得

次の手順を使用して、Azure Stack Hub 起動ルーチンのステータスを取得します。

手順

ステップ 1 Privileged Endpoint (PEP) セッションを、Azure Stack Hub ERCS VM へのネットワーク アクセスを有するマシンから開きます。

詳細については、『Azure Stack Hub の権限エンドポイントを使用する』を参照してください。

ステップ 2 PEP から、**Get-ActionStatus Start-AzureStack** を実行します。

Azure Stack Hub 起動とシャットダウンのトラブルシューティング

Azure Stack Hub 環境の電源をオンにした 2 時間後、インフラストラクチャとテナント サービスが正常に開始しない場合は、次の手順を実行します。

手順

ステップ 1 Privileged Endpoint (PEP) セッションを、Azure Stack Hub ERCS VM へのネットワーク アクセスを有するマシンから開きます。

詳細については、『Azure Stack Hub の権限エンドポイントを使用する』を参照してください。

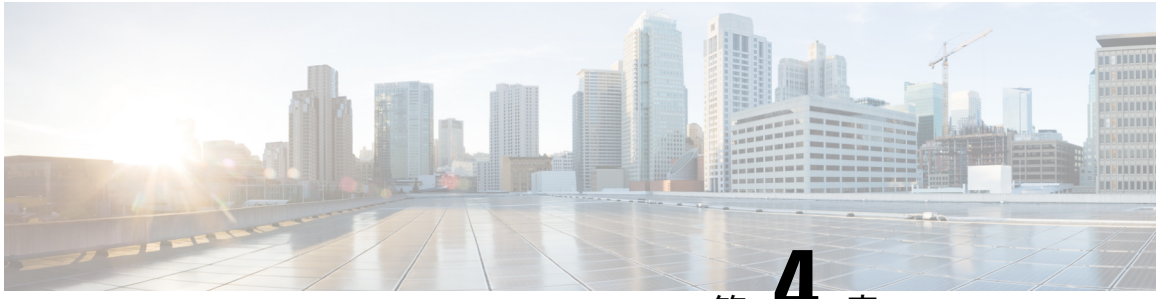
ステップ 2 PEP から、**Test-AzureStack** を実行します。

ステップ 3 出力を確認し、健全性エラーを解決します。

詳細については、『Run a validation test of Azure Stack Hub』を参照してください。

ステップ 4 PEP から、**Start-AzureStack** を実行します。

ステップ 5 Start-AzureStack を実行して失敗した場合は、Microsoft カスタマー サービス サポートにお問い合わせください。



第 4 章

Secret Rotation

- Secret Rotation （13 ページ）
- Cisco Nexus Top of Rack Switch の Rotating Secrets （14 ページ）
- Rotating Secrets of Cisco UCS Manager の Rotating Secrets （14 ページ）

Secret Rotation

Azure Stack Hub は、内部および外部の Secret を使用して、Azure Stack Hub インフラストラクチャ リソースとサービス間のセキュアな通信を維持します。Azure Stack Hub 固有の Secret Rotation の詳細については、https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-rotate-secrets?view=azs-2002 を参照してください。

すべてのユーザーアカウントに強力なパスワードを使用することを推奨します。この章では、ハードウェア管理ユーザー アカウントの Secret をローテーションする手順について説明します。

Cisco Azure Stack Hub には、インストール時に次のデフォルトのユーザー アカウントが作成されます。ユーザー アカウントは、インストール時に顧客が指定したパスワードで設定されます。

デバイス	アカウント	目的
Cisco UCS	admin	Cisco UCS Manager の管理者ロールを持つデフォルトの管理者アカウント
	UCSAzSAdmin	UCS Manager の管理者ロールを持つ追加の管理者アカウント
	IpmiUser	ベースボード管理コントローラ（BMC）ユーザーアカウント。

デバイス	アカウント	目的
Nexus	admin	ネットワーク管理者ロールを持つデフォルトの管理者アカウント
	azsadmin-<5 character random string>	network-administrator ロールを持つ追加の管理者アカウント

Cisco Nexus Top of Rack Switch の Rotating Secrets

Cisco Nexus Top of Rack スイッチの各ユーザー アカウントのパスワードを変更するには、次のコマンドを実行します。

```
n9k-1# conf t
n9k-1(config)# username <username> password <new password>
```

（注） Cisco Nexus Top of Rack スイッチは、強力なパスワードのみを許可するように設定されています。既存のパスワードを、『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』の「パスワード強度のチェックを有効化」の項に記載されている要件を満たす強力なパスワードに置き換えてください。

Rotating Secrets of Cisco UCS Manager の Rotating Secrets

Cisco UCS Manager は、UCS サーバインフラストラクチャのコントロールセンターです。Cisco UCS Manager は、Azure Stack Hub アウトオブバンド管理ネットワークにアクセスできる任意のコンピュータ上のサポートされているブラウザを使用してアクセスできます。

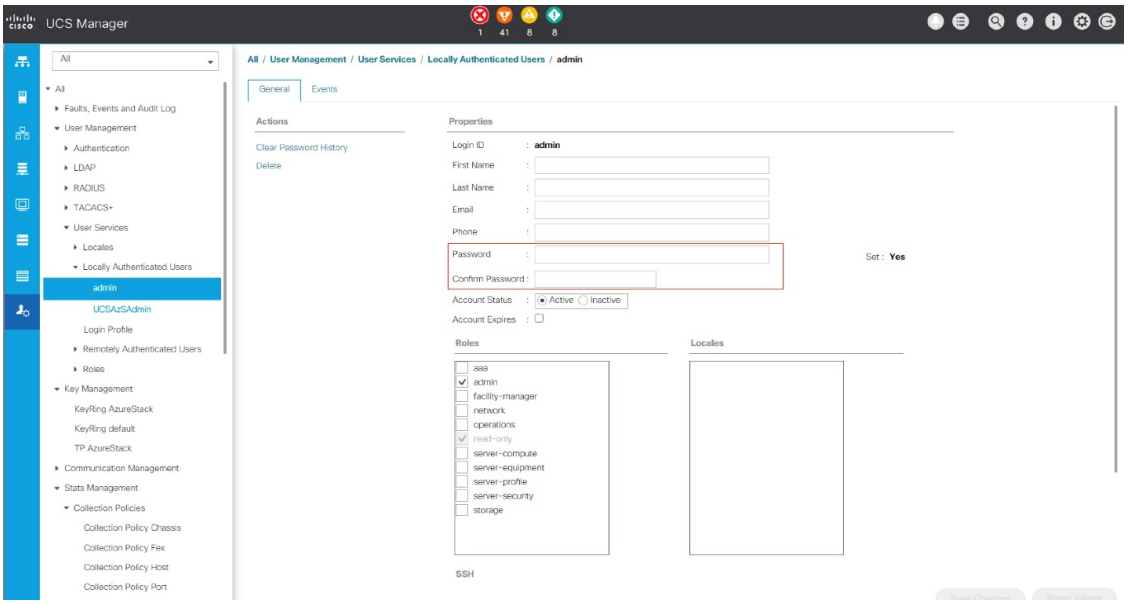
（注） シスコのサポート技術者から要求された場合を除き、Cisco UCS Manager を使用してサーバやその他のコンポーネントを再起動しないでください。Cisco UCS Manager からの再起動操作によって、一時的または永続的なデータが失われる可能性があります。

表に示すように、Cisco UCS Manager には 3 つのユーザー アカウントがあります。ユーザー アカウントのパスワードを変更するには、次のタスクを実行します。

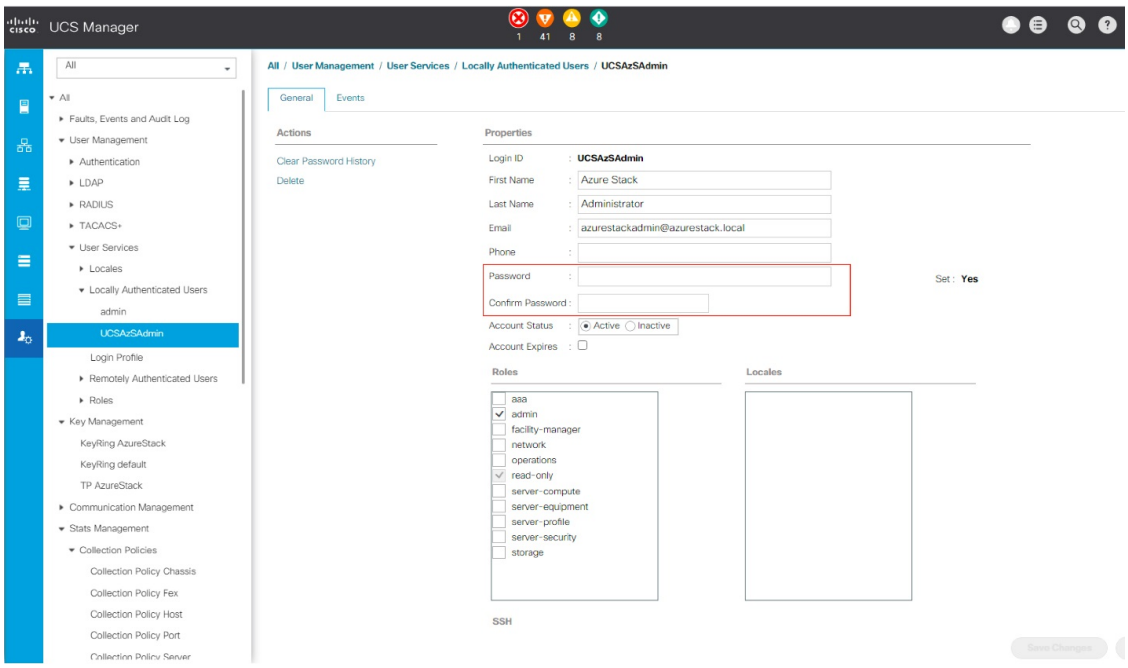
手順

ステップ 1 サポートされているブラウザで、`https://<UCS Manager IP>` と入力し、管理者クレデンシャルを使用して Cisco UCS Manager にログインします。

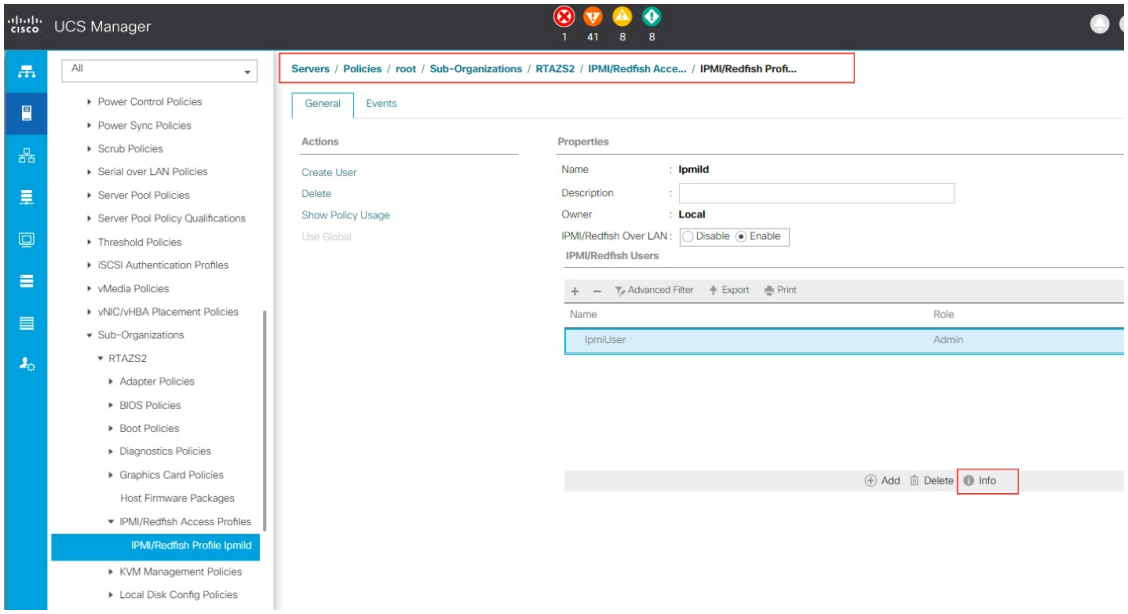
ステップ 2 [Navigation] ペインで [Admin] をクリックします。**[すべて（All）]** > **[ユーザー管理（User Management）]** > **[ユーザー サービス（User Services）]** > **[ローカル認証ユーザー（Locally Authenticated Users）]** の順に展開し、**[管理（Admin）]** ユーザーを選択します。右の **[プロパティ（Properties）]** 領域で、**[パスワード（Password）]** フィールドと **[パスワードの確認（Confirm Password）]** フィールドに、パスワードを入力します。変更を保存するには、**[パスワードの保存（Save Changes）]** をクリックします。



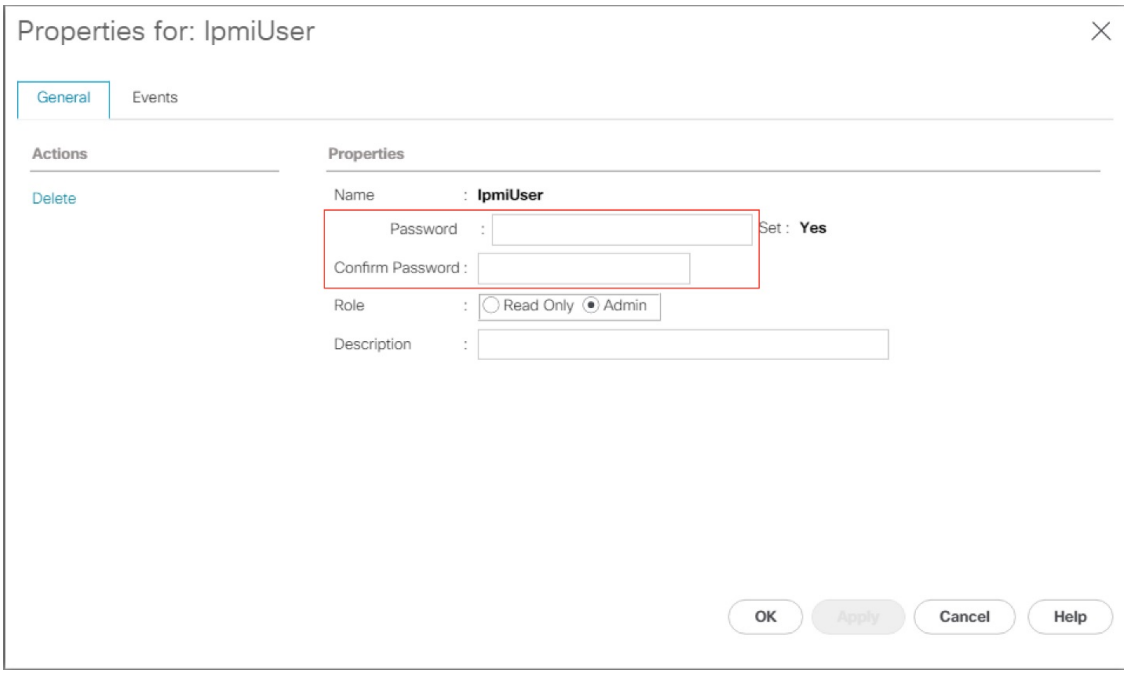
ステップ 3 **[すべて（All）]** > **[ユーザー管理（User Management）]** > **[ユーザー サービス（User Services）]** > **[ローカル認証ユーザー（Locally Authenticated Users）]** の下にある **[UCSAzSadmin]** ユーザーを選択します。右の **[プロパティ（Properties）]** 領域で、**[パスワード（Password）]** フィールドと **[パスワードの確認（Confirm Password）]** フィールドに、パスワードを入力します。変更を保存するには、**[パスワードの保存（Save Changes）]** をクリックします。



ステップ 4 [Navigation] ペインで [Servers] をクリックします。**[サーバ** > **ポリシー** > **ルート** > **サブ組織** > **[展開中に提供された組織名（IPMI / Redfish Access Profiles）]** > **[IPMI/Redfish アクセス プロファイル（IPMI/Redfish Access Profiles）]** を展開し、**[IPMI / Redfish profile IpmiId]** を選択します。右側の **[プロパティ（Properties）]** 領域の **[IPMI / Redfish ユーザー（IPMI / Redfish Users）]** サブ領域で、**[IpmiUser]** を選択し、**[情報（info)]** をクリックします。



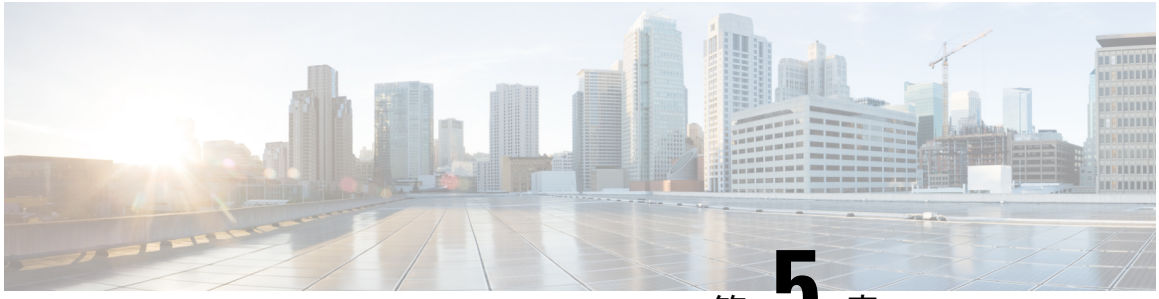
ステップ 5 **[パスワード（Password）]** フィールドと **[パスワードの確認（Confirm Password）]** フィールドに新しいパスワードを入力します。変更を保存するには、**[パスワードの保存（Save Changes）]** をクリックします。



ステップ 6 Elevated PowerShell ウィンドウを開き、「Cloudadmin」アカウントを使用して Azure Stack Hub Emergency Recovery コンソールに接続します。`-BypassBMCUpdate` フラグを指定して `set-bmccredential` コマンドを実行し、ベースボード管理コントローラ（BMC）クレデンシャルを更新します。

（注） 順序は、まず Cisco UCS Manager から各サーバの BMC クレデンシャルを更新し（ステップ 4 と 5）、次に `set-bmccredential` コマンドを実行します（ステップ 6）。詳細については、Microsoft 社のドキュメントを参照してください。

汎用 Azure Stack Hub では、`set-bmccredential` コマンドを使用して、各サーバの BMC コントローラの BMC クレデンシャルを内部クレデンシャルストアの更新とともに更新できます。ただし、Cisco Azure Stack Hub では、サーバ BMC コントローラは Cisco UCS Manager を使用して制御されるため、各サーバでのクレデンシャルの更新はできません。したがって、Cisco UCS Manager を使用して BMC コントローラで新しいクレデンシャルを設定し、`set-bmccredential` コマンドを使用して Azure Stack Hub の内部クレデンシャル ストアを更新します。



第 5 章

Upgrade Firmware

- ファームウェア アップグレードの概要 （19 ページ）
- インストールされているファームウェアの識別 （20 ページ）
- ファームウェア アップグレード中の既知の動作 （22 ページ）
- Cisco Azure Stack Hub Platform アップグレード自動化 （23 ページ）
- Cisco Azure Stack Hub Platform アップグレード 自動化の設定 （25 ページ）

ファームウェア アップグレードの概要

ここでは、Microsoft Azure Stack 向けシスコ統合システム のファームウェアとドライバの更新手順について説明します。シスコは、Azure Stack Hub プラットフォームのシステム アップデートを定期的にリリースしています。これらのシステム アップデートには、プラットフォームのライフサイクルを改善し、既知の不具合を解決する更新されたファームウェアとドライバが含まれています。お客様は、システム アップデートのリリース日から 60 日以内にシステムを最新のシステム アップデートに更新する必要があります。

Cisco アプライアンスの次のコンポーネントでは、既知の機能およびセキュリティの問題を解決するために、定期的なファームウェアの更新が必要です。

- Top-of-Rack スイッチ
- Cisco UCS
  - Cisco UCS Manager
  - UCS ファブリック インターコネクト
  - UCS ファブリック エクステンダ
  - UCS C シリーズ ラック サーバ コンポーネント (BIOS、SAS HBA、NIC、HDD、および SSD を含む)
  - サーバ デバイス ドライバ

ファームウェア アップグレードの問題やエラーに関してサポートが必要な場合は、「サポートガイダンス」の項を参照して、Azure Stack Hub サポートの Cisco TAC ケースを開始してください。

（注） Cisco では、メンテナンス時間枠内にファームウェア アップグレードを行うことをお勧めします。

Microsoft Azure Stack Hub 向け Cisco Integrated System のファームウェア ダウンロード ポータルには、[UCS C シリーズ ラックマウント UCS 管理対象サーバー ソフトウェア ダウンロード] ページで [Integrated System Azure Stack-System Updates] を選択してアクセスできます。また、新しいファームウェアの可用性について通知するように設定することもできます。Cisco では、これらの通知にサインアップすることを強く推奨しています。

Microsoft Azure Stack Hub ファームウェア ダウンロードにホストされている次のソフトウェア コンポーネントは、ファームウェア アップグレード手順に必要です。

コンポーネント	説明
ucs-6300-k9-bundle-infra.<*version number*>.A.bin	UCS インフラストラクチャ ファームウェア
ucs-k9-bundle-c-series<*version number*>.C.bin	UCS サーバ ファームウェア
nxos. <version number>.bin	ToR スイッチ ファームウェア
<*OEM extension version number*>.zip	OEM 拡張パッケージを含む Zip ファイル。OEM 拡張パッケージは 2 つのファイルで構成されています。1 つの zip ファイルと 1 つの xml ファイル。
Cisco_UCS_AzureStack_FwUpdate_<*version number*>.zip	ファームウェアおよびドライバ更新の自動化 (CASPU)

インストールされているファームウェアの識別

システムのインストールおよび更新のタイミングに基づいて、Micorsoft Azure Stack Hub ハードウェアの一部またはすべてのコンポーネントのファームウェアをアップグレードする必要があります。ここでは、インストールされているファームウェアを特定する手順について説明します。

UCS インフラストラクチャおよびサーバ ファームウェア

手順

ステップ 1 Putty など SSH クライアントで管理者クレデンシャルを使用して、Cisco UCS Manager（https://<UCS_Manager_IP>）にログインします。

ステップ 2 `show version` コマンドを使用してバージョンを確認します。

```
UCS-B# show  version
System version: 4.0(4b)
```

ステップ 3 Microsoft Azure Stack Hub のファームウェア ダウンロード ポータルで、ポストされた Cisco UCS ファームウェア ファイル（`ucs-6300-k9-bundle-infra.4.0.4g.A.bin` または `ucs-k9-bundle-c-series.4.0.4g.C.bin`）から最新のファームウェア バージョンを確認します。

バンドル イメージ ファイルのファームウェア バージョンが同じである。ポストされたファームウェア バージョンがインストールされているファームウェア バージョンよりも大きい場合、システムは UCS ファームウェアのアップグレードを必要とします。たとえば、インストールされている UCS ファームウェア バージョンが 4.0（4b）で、ポストされたファームウェア バージョンが 4.0（4g）である場合、システムでは 4.0（4b）から 4.0（4g）への UCS ファームウェアのアップグレードが必要です。

（注） UCS ファームウェアのアップグレードを完了するには、OEM 拡張パッケージのインストールが必要です。

Top-of-Rack Nexus スイッチ ファームウェア

手順

ステップ 1 PuTTY などの SSH クライアントを介して管理者クレデンシャルを使用して、Top-of-Rack Nexus スイッチ A にログインします。

ステップ 2 `show version | inc NXOS` コマンドを使用してバージョンを確認します。

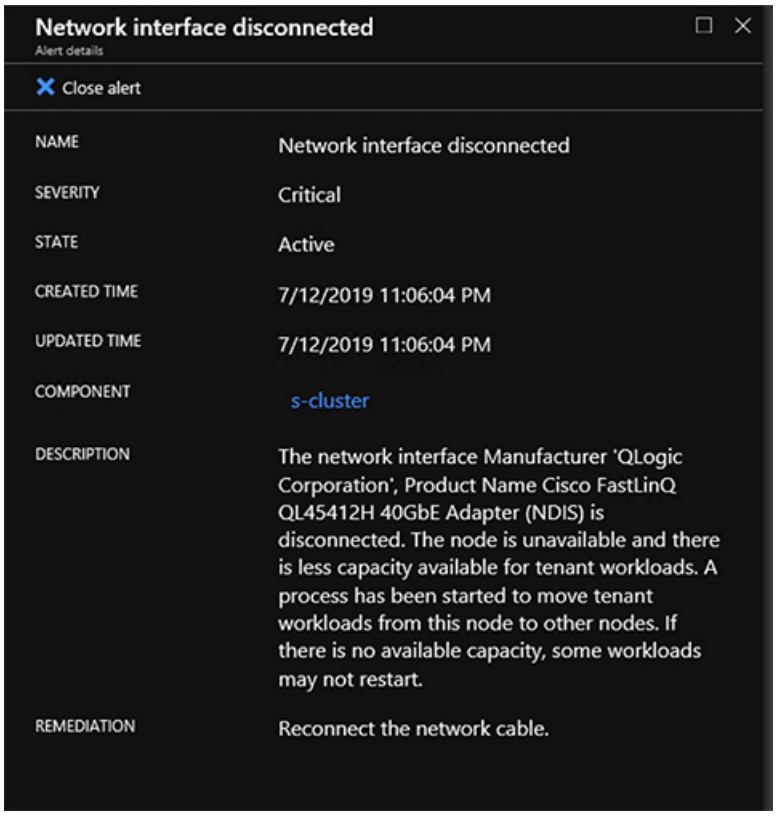
```
ToR-1# show version | inc NXOS
NXOS: version 7.0(3)I7(4)
NXOS image file is: bootflash:///nxos.7.0.3.I7.4.bin
NXOS compile time:  6/14/2018 2:00:00 [06/14/2018 10:49:04]
```

ステップ 3 Microsoft Azure Stack Hub のファームウェア ダウンロード ポータルで、Nexus スイッチ ファーム ウェア ファイル（`nxos.7.0.3.I7.8.bin`）から最新の Nexus スイッチ ファームウェア バージョンを確認します。ポストされたファームウェア バージョンがインストールされている

ファームウェア バージョンよりも大きい場合、システムは Nexus スイッチ ファームウェアのアップグレードを必要とします。

ファームウェア アップグレード中の既知の動作

- ToR スイッチのアップグレード中に、管理者ポータルにルート パブリケーション障害のアラートが表示される場合があります。この動作は予期されており、無視しても問題ありません。このアラートは、ファームウェアのアップグレード後に自動的にクリアされます。
- UCS 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中に、Cisco UCS Manager はサーバの再起動を確認するアラート メッセージを表示します。Cisco UCS Manager からサーバを再起動すると、Azure Stack Hub のダウンタイムが発生し、データが失われる可能性があるため、このアラート メッセージは無視する必要があります。サーバの安全な再起動は、OEM 拡張パッケージのインストール中に自動的にトリガーされます。
- UCS 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中に、Azure Stack Hub 管理者ポータルが次の図に示すようなアラートを生成する場合があります。この動作は予期されており、無視しても問題ありません。このアラートは、ファームウェアのアップグレード後に自動的にクリアされます。



Cisco Azure Stack Hub Platform アップグレード自動化

Microsoft Azure Stack 向けシスコ統合システム のファームウェア アップグレードは、Cisco Azure Stack Hub Platform UPGRADE (caspu) 自動化ソフトウェアを使用して完全に自動化された中断のない操作です。CASPU を使用すると、シスコのお客様はすべて Azure Stack Hub のすべてのコンポーネントを一度に、または 3 つの部分でアップグレードできます。

- Top-of-Rack Nexus スイッチのアップグレード（フラグ：**UpdateNexus**）
- UCS インフラストラクチャのアップグレード（フラグ：**UpdateUCSManager**）
- サーバ ファームウェアのアップグレードとドライバのインストール（フラグ：**UpdateOEMExtension**）

CASPU を実行しているホストが管理者ポータルにアクセスできず、UCS と ToR の管理 IP がすべて同時にスイッチされている場合は、その部分で CASPU を実行することが特に役立ちます。CASPU コンフィギュレーションファイル `FirmwareUpdateInputs` は、フラグ **Updatenexus**、**UpdateUCSManager**、および **UPDATEOEMEXTENSION**で構成され、CASPU の 3 つの部分の実行を設定します。デフォルトでは、すべてのフラグが true とマークされ、CASPU はすべてのコンポーネントを同時にアップグレードしようとします。

重要 Azure Stack Hub ファームウェアのアップグレードには実行順序が重要です。すべてのフラグが true とマークされている場合、CASPU は自動的に正しい順序を選択します。CASPU を部品で実行しているときには、**サーバファームウェアのアップグレードと、OEM 拡張パッケージを使用したドライバのインストール**前に、 **UCS インフラストラクチャのアップグレードとサーバファームウェアアップグレードのステージング**を実行していることを確認してください。

CASPU を部分的に実行する場合は、各手順の前後に Azure Stack Hub 検証ツール（Test-AzureStack）を手動で呼び出し（https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-diagnostic-test?view=azs-2005）、Azure Stack Hub が正常であることを確認します。CASPU がデフォルト モードで実行されると（すべてのフラグが true）、CASPU は各操作の前後に Azure Stack Hub が正常であることを確認します。

Azure Stack Hub システムは、CASPU ユーティリティを使用してファームウェアおよび OEM 拡張パッケージを更新する前に、Azure Stack Hub バージョン 1.1907.17.54 以降を実行している必要があります。

CASPU は PowerShell で記述され、次の要件を満たす任意の Microsoft Windows 環境から実行できます。

- MS Windows 10、2016 または 2019 オペレーティング システム

（注） オペレーティングシステムに最新のパッチがすべて設定されていることを確認します。

- Nexus ToR スイッチおよび UCS の管理 IP へのネットワーク接続
- Azure Stack Hub 管理者ポータルおよび権限エンドポイントへのネットワーク接続
- すべての Azure Stack Hub PKI 証明書がインストールされている
- PowerShell バージョン 5.1 以降がインストールされている
- Azure Stack Hub がインストールされている PowerShell の最新バージョン (https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-powershell-install)

（注） CASPU を実行しているホストは、顧客が指定した権限エンドポイント VM の IP アドレスを信頼できるホストに追加します。

CASPU を実行しているホストに、Azure Stack Hub への確実な有線ネットワーク接続があることを確認します。VPN または信頼できないネットワークを介して Azure Stack Hub に接続しているコンピュータから CASPU を実行することはサポートされていません。

ファームウェアのアップグレードに加えて、CASPU では Azure Stack Hub に対して次の設定変更が行われます。

- 両方の ToR スイッチ上のすべての SVI およびピア リンク ポート チャネル (po10) に 9216 MTU を設定します。この更新は、ToR スイッチ設定の新しい要件に対応します。
- ACL を Microsoft に必要な最新の ToR スイッチ セキュリティ設定を実装するために変更します。
- ToR スイッチおよびファブリック インターコネクトのクラスタ通信トラフィックの QoS クラスを設定します。
- UCS サーバのブート ポリシー設定をローカルディスクから組み込み LUN に変更します。

Cisco Azure Stack Hub Platform アップグレード 自動化の設定

手順

ステップ 1 前述の要件を満たしている Microsoft Windows 環境では、次のファームウェア アップグレードコンポーネントをフォルダ（例：c:\azsfirmwareupgrade）の下にダウンロードします。

- ucs-6300-k9-bundle-infra.<*version number*>.A.bin
- ucs-k9-bundle-c-series.<*version number*>.C.bin
- nxos. <version number>.bin
- <*OEM extension version number*>.zip
- Cisco_UCS_AzureStack_FwUpdate_<*version number*>.zip

ステップ 2 **gci -path**c:\azsfirmwareupgrade **-recurse** の実行 |**unblock-file**すべてのコンポーネントのブロックを解除します。

ステップ 3 `Cisco_UCS_AzureStack_FwUpdate_<version>.zip` パッケージを抽出します。

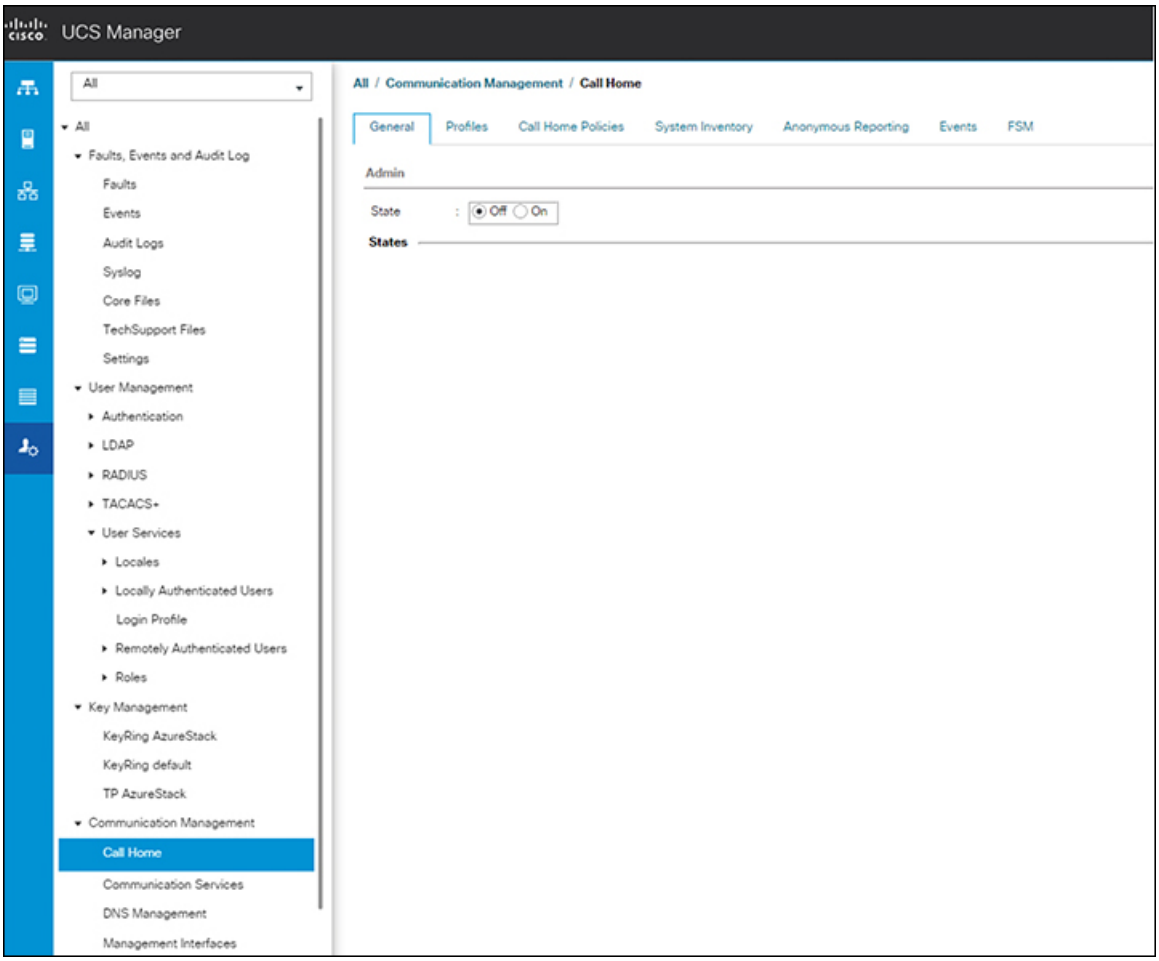
ステップ 4 OEM 拡張パッケージを `<OEM extension version number>.zip` から `C:\azsfirmwareupgrade\OEM` フォルダに抽出します。

ステップ 5 `C:\ azsfirmwareupgrade \Cisco_UCS_AzureStack_FwUpdate_<version>\FirmwareUpdate`フォルダ内部にある `FirmwareUpdateInputs.xml` を更新します。

フィールド名	説明
Updatenexus (True/False)	Nexus ファームウェア アップグレードを実行するためのフラグ
UpdateUCSManager (True/False)	UCS インフラストラクチャ ファームウェア アップグレードとサーバファームウェア アップグレード ステージングを実行するためのフラグ
Updateoem (True/False)	ローリング サーバファームウェアとドライバ更新を実行するためのフラグ

フィールド名	説明
RunAzureStackHubHealthCheck (True/False)	Nexus および UCS 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前に Test-AzureStack を実行するためのフラグ CASPU を実行しているホストが ERCS VM にアクセスできない場合は、このフラグを **False** に設定します。
ToRSwitch1IP	Nexus Top-of-Rack スイッチ 1 の IP アドレス
ToRSwitch1UserName	Nexus スイッチ 1 管理者ユーザー名
ToRSwitch2IP	Nexus Top-of-Rack スイッチ 2 の IP アドレス
ToRSwitch2UserName	Nexus スイッチ 2 管理者ユーザー名
ToRImageFilePath	Top-of-Rack スイッチ ファームウェア イメージのファイル パス
UCSMIP	Cisco UCS Manager の IP アドレス。
UCSMUserName	Cisco UCS Manager 管理者ユーザー名
ImagePathInfraBundle	UCSインフラストラクチャ ファームウェア バンドルのファイル パス
ImagePathHostBundle	UCSサーバ ファームウェア バンドルのファイル パス
AdminResourceManagerURI	Azure Stack Hub 管理リソース マネージャの URI。通常は、展開後に提供される AzureStackStampInformation にあります。たとえば、https://adminmanagement.usw.m4l.rtazslab.net/
OEMExtensionFolderPath	OEM 拡張パッケージのフォルダ パス `C:\azsfirmwareupgrade\OEM`
AzureRMUserName	Azure Stack Hub グローバル管理者のユーザー名
ERCSIPAddress	ERCS VM の IP アドレス
ERCSUserName	ERCS クラウド管理者のユーザー名。たとえば、< local domain > \ cloudadmin

ステップ 6 （任意） ファームウェア アップグレード期間が設定されている場合は、不要なアラートを回避するために UCS Call Home を無効にします。



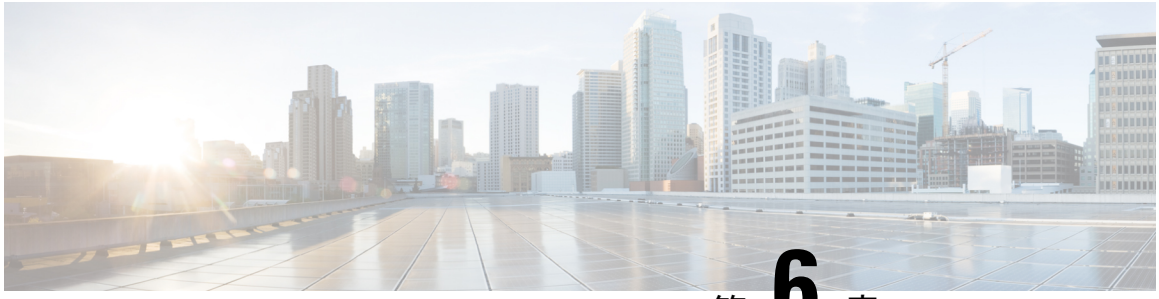
ステップ 7 昇格 PowerShell ウィンドウから、`C:\ azsfirmwareupgrade \Cisco_UCS_AzureStack_FwUpdate_<version>\FirmwareUpdate \RunFirmwareUpdate.ps1` を実行します。必要なクレデンシャルを入力します。

モジュール	クレデンシャルの詳細
UpdateUCSManager	Cisco UCS Manager の管理者クレデンシャル
Updatu	Nexus ToR スイッチごとの管理者クレデンシャル
UpdateOEMExtension	Azure Stack Hub グローバル管理者
	権限エンドポイントアクセスの Cloudadmin アカウント クレデンシャル

（注） **RunFirmwareUpdate** は、必要な PowerShell モジュールを自動インストールできます。デフォルトでは、スクリプトはインストール前にユーザーの確認を待機します。スクリプトでユーザーの確認なしに必要なすべてのモジュールをインストールする場合は、スクリプトの実行中に「force」パラメータを使用できます。たとえば、**RunFirmwareUpdate.ps1 -force**。

Updateoemextension モジュールは、Azure Stack Hub の OEM 拡張へのインストールのみを開始します。OEM 拡張の更新が完了するまで待機しません。管理者ポータルからの OEM 拡張更新のステータスをモニタする必要があります。

OEM 拡張が正常に更新されるまで、サーバ ファームウェアのアップグレードは完了しません。



第 6 章

容量の管理

- 物理メモリ容量の管理 （29 ページ）
- スケール ユニット ノードの追加 （30 ページ）
- 管理 IP プールの拡張 （31 ページ）
- スケール ユニット ノードの追加 （33 ページ）

物理メモリ容量の管理

Cisco では、Azure Stack Hub サーバでのメモリ拡張をサポートしています。メモリの拡張は破壊的な操作であり、Azure Stack Hub システムのシャットダウンが伴います。次に、メモリの拡張またはアップグレードのガイドラインを示します。

- Azure Stack Hub 内のすべてのサーバは、同種のハードウェア構成を備えています。このため、単一サーバでのみメモリ アップグレードを実行することはできません。すべてのサーバのメモリを同時にアップグレードする必要があります。
- M5 (32 GB DIMM を使用した 384 GB、512 GB、768 GB、または 64 GB DIMMS を使用した 1024 GB Dimm または 1536 GB) に対してサポートされている増分にのみアップグレードします。
- 32 GB および 64 GB の DIMM を混在させることはできません。

次のリンクから、Cisco のメモリ拡張のベスト プラクティスを確認してください。

https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/memory-guide-c220-c240-b200-m5.pdf

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C240M4/install/C240M4/replace.html

サポートされているメモリが調達されたら、次の Microsoft ガイドの手順に従ってメモリ拡張を実行します。

https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-manage-storage-physical-memory-capacity

スケール ユニット ノードの追加

Azure Stack Hub 更新 1807 Microsoft では、既存の Azure Stack Hub への物理サーバの追加がサポートされています。Azure Stack Hub バージョン 1807 以降を実行している Cisco のお客様は、既存の Azure Stack Hub にノードを発注して追加できるようになりました。[Add Node (ノードの追加)] 機能の現在のバージョンでは、Microsoft によって、既存のクラスタをスケールユニットごとに最大 16 台のサーバまで拡張できます。このセクションでは、既存の Azure Stack Hub システムへの新しいノードの追加に関する詳細な手順について説明します。

ノードの追加に関する前提条件

ノードを追加する前に、次の前提条件が完了している必要があります。

- Azure Stack Hub 管理者ポータルで、Azure Stack Hub がエラーまたは警告なしで 1807 以降の更新を実行していることを確認します。
- ノードパッケージの追加の一部として卯木のコンポーネントが受信されていることを確認します。
  - 既存の Azure Stack Hub の他のサーバとまったく同じコンポーネントを持つサーバ
  - QSFP-H40G-CU3M ケーブル x 2
  - 2 個のポートの UCS ポート ライセンス
- 2 本の CAT 6 ケーブルを入手します。
- Cisco UCS Manager にエラーまたは警告が表示されていないことを確認します。Cisco UCS Manager には、Azure Stack Hub アウトオブバンド管理ネットワークにアクセスできる任意のコンピュータを使用してアクセスできます。Web ブラウザを使用して Cisco UCS Manager にアクセスするには、https://<*Cisco_UCS_Manager_IP*> を開きます。Cisco UCS Manager の IP および管理者のログインクレデンシャルは、お客様への引き渡し情報で確認できます。
- UCS サービスプロファイルテンプレートに、新しく追加されたノードに十分な Cisco IMC (Integrated Management Controller)/BMC Ip があることを確認します。2018 年 9 月以降の新しい展開の大部分では、16 台のサーバをサポートするのに十分な Cisco IMC IP プールが用意されています。ただし、古い展開では、Cisco IMC IP プールで手動展開が必要です。各 Cisco Azure Stack Hub サーバには、次の 2 つの Cisco IMC IP が必要です。
  - アウトオブバンド管理 IP
  - インバンド管理 IP

管理 IP プールの拡張

Cisco IMC IP のタイプごとに 1 個の IP プールを設定できます。Cisco IMC IP プールは、すべての Cisco Azure Stack Hubアプライアンスにすでに存在している必要があります。

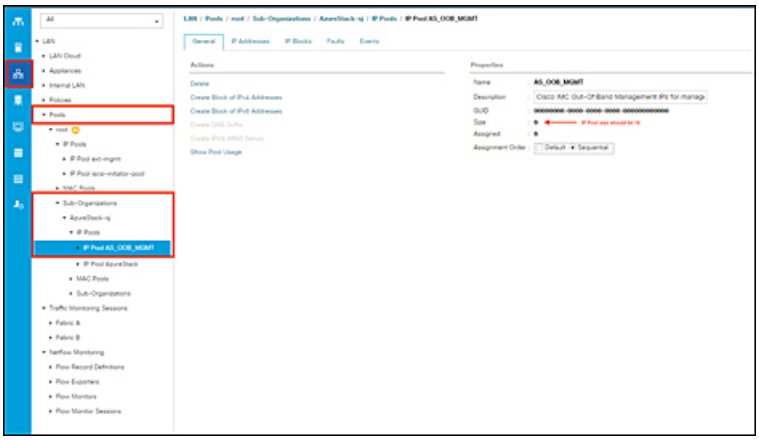
アウトオブバンド管理 IP プールを拡張するには、Cisco 展開ワークシート補遺で提供されているアウトオブバンド管理 IP サブネットを確認し、そのサブネット内の未使用の IP ブロックを検索します。プールの合計サイズを 16 IP に設定することをお勧めします。

Cisco UCS Manager から、**[LAN]** > **{Pools (プール)]** > **[Sub-Organizations (サブ組織)** > ***[AzureStack Org]*** > **[IP Pools (IP プール)]** に移動します。アウトオブバンド管理 IP プールを検索し、プールサイズが 16 であることを確認します。

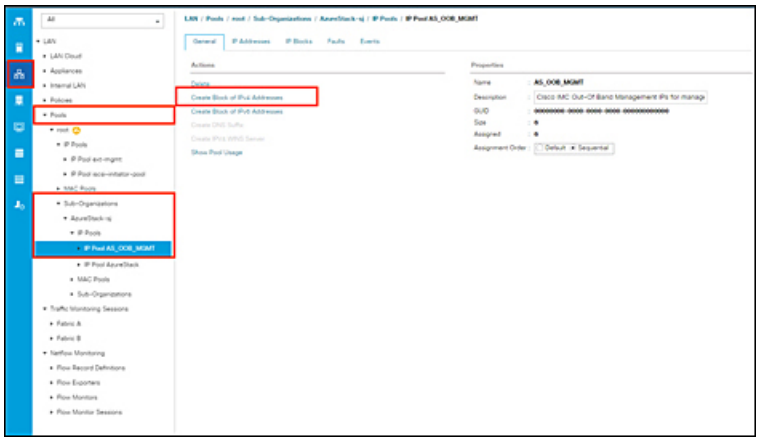
手順

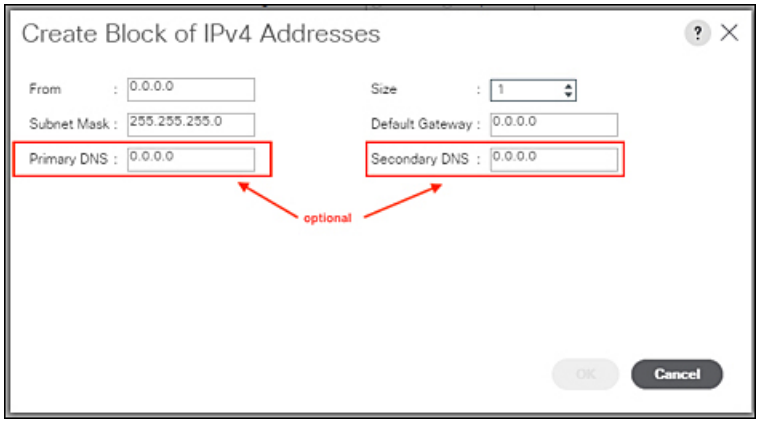
ステップ 1 Cisco UCS Manager から、**[LAN]** > **{Pools (プール)]** > **[Sub-Organizations (サブ組織)** > ***[AzureStack Org]*** > **[IP Pools (IP プール)]** に移動します。

ステップ 2 アウトオブバンド管理 IP プールを検索し、プール サイズが 16 であることを確認します。



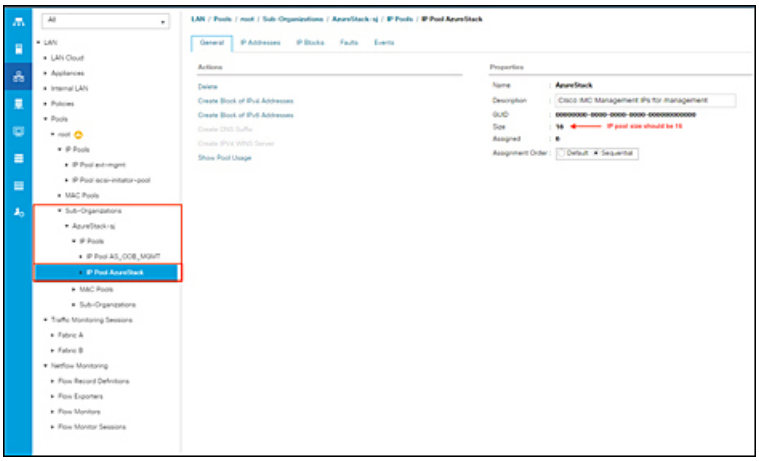
ステップ 3 プール サイズが 16 でない場合は、UI の **[Create Block Of IPv4 addresses (IPv4 アドレスのブロックの作成)]** オプションを使用して IP アドレスを追加します。プール サイズを 16 にするには、十分な IP アドレスを追加してください。DNS 値はデフォルトの「0.0.0.0」のままにします。





ステップ 4 インバンド管理 IP プールを拡張するには、これらの手順を繰り返します。

プール拡張のインバンド管理 IP を確認するには、展開前に展開ワークシートが完了していることを確認します。これには、[IP usage (IP 使用状況)] セクションの各サーバの BMC IP アドレスが含まれています。16 個すべてのサーバの IP アドレスがワークシートにリストされていない場合は、プールを拡張するために最後に使用された BMC IP の後に、次に連続して使用されていない IP アドレスを選択します。たとえば、4 ノード システムがあり、現在 4 個の IP アドレス (192.168.26.3 – 192.168.26.6) の IP プールが完全に消費されている場合は、IP アドレス 192.168.26.7 –192.168.26.18 を使用してインバンド IP プールを拡張します。



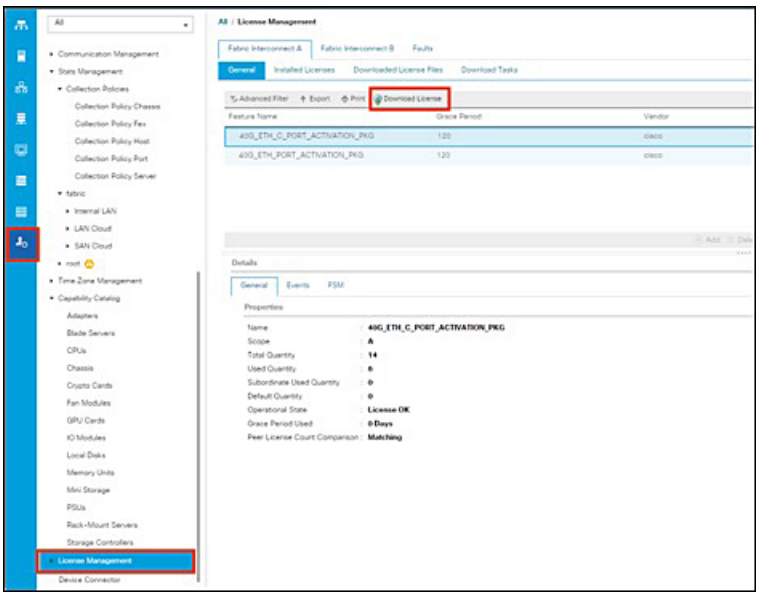
スケール ユニット ノードの追加

始める前に

「スケール ユニット ノードの追加」にリストされている前提条件のリストを入力します。

手順

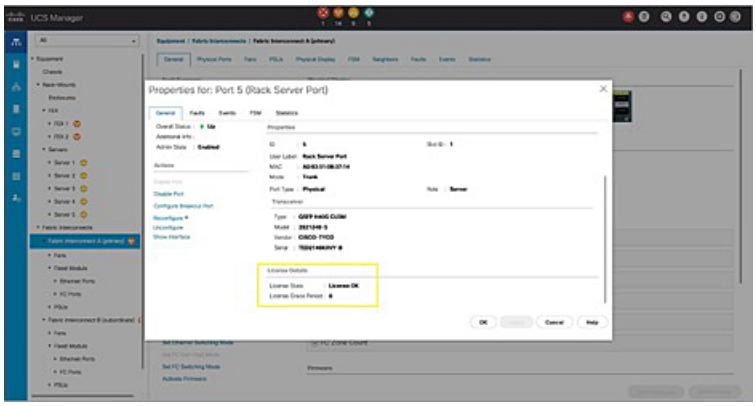
ステップ 1 Cisco UCS Manager にログインし、 **[Admin (管理)]** > **[License Management (ライセンス管理)]** > **[Fabric Interconnect A (ファブリック インターコネクト A)]** > **[General (全般)]** タブに移動します。



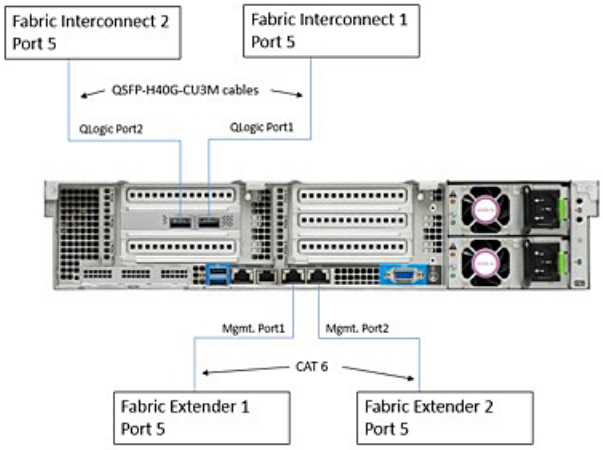
ステップ 2 **[Download License (ライセンスのダウンロード)]** をクリックし、ファブリック インターコネクト A に UCS ポート ライセンスをインストールします。

ステップ 3 ファブリック インターコネクト B に対して手順 1 と 2 を繰り返します。

各ファブリック インターコネクトにライセンスをインストールした後、ポートのプロパティを確認して、新しく追加されたサーバ ポートのライセンス ステータスを確認します。



ステップ 4 既存の Azure Stack Hub ラックにサーバを設置しますが、電源は接続しないでください。サーバの配置とケーブル配線の詳細については、Cisco Azure Stack Hub 配線ガイドを参照してください。QLogic および管理ポートをファブリック インターコネクトとファブリック エクステンダに接続します。新しいサーバは、ファブリック インターコネクトとファブリック エクステンダ上で次に連続するポートを取得します。たとえば、4 ノード Azure Stack Hub システムに 5 番目のサーバを設置する場合、サーバのケーブル配線は次のようになります。



ステップ 5 電源を接続し、UCS サーバの検出が完了するまで待ちます。

検出フェーズでは、Cisco UCS Manager によって次のアクションが自動的に実行されます。

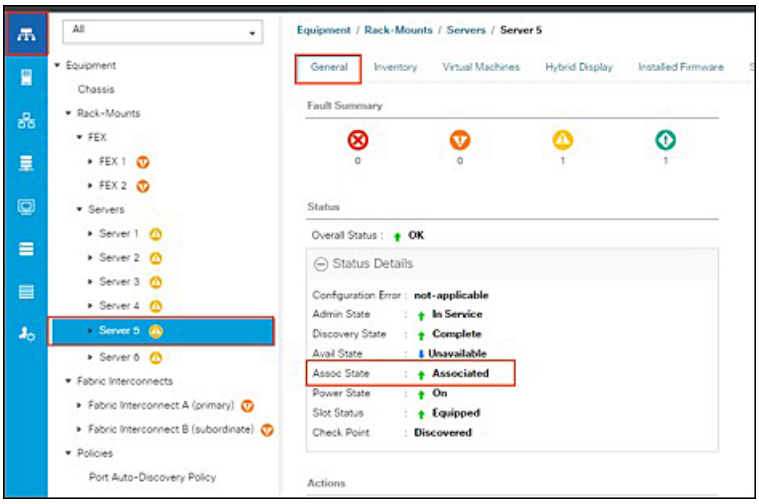
1. サーバおよびサーバ コンポーネントのインベントリ
2. 適切なサーバ プールにサーバを追加します。
3. サーバに新しいサービス プロファイルを作成します。

4. サービス プロファイルをサーバに関連付けます。
5. サービスプロファイルの関連付け中に、スタンプ内の他のサーバと一致するようにサーバファームウェアをアップグレードします。

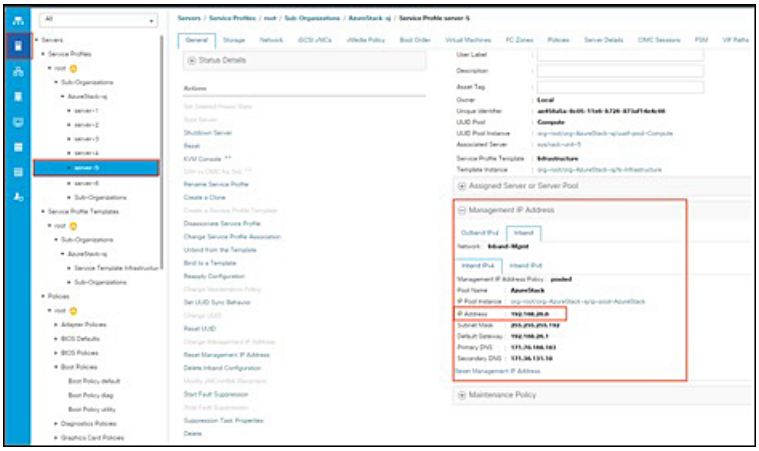
サーバの検出には、ファームウェアアップグレードが必要なサーバコンポーネントの数に応じて、40 分から 2 時間かかる場合があります。

ステップ 6 検出が完了したら、**[Equipment (機器)]** > **[Rack-Mounts (ラックマウント)]** > **[Servers (サーバ)]** > ***[Server <newly added server number> (サーバ <新規追加されたサーバ番号>)]*** > **[General (全般)]** の下の関連付け状態を確認します。

[Assoc State (関連付け状態)] が **[Associated (関連付け済み)]**である必要があります。



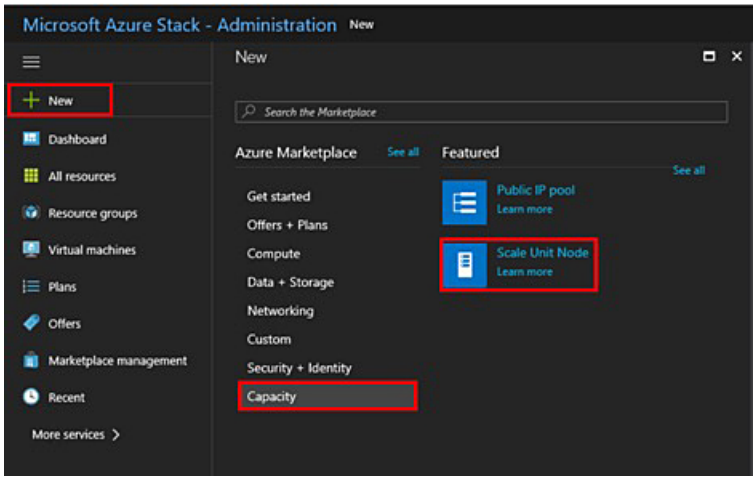
ステップ 7 [Navigation (ナビゲーション)] ペインの **[Server (サーバ)]** タブから、新しく設置されたサーバに関連付けられているサービス プロファイルを選択し、インバンド管理 IP アドレスをメモします。



ステップ 8 Azure Stack Hub 演算子として Azure Stack Hub 管理者ポータルにログインします。

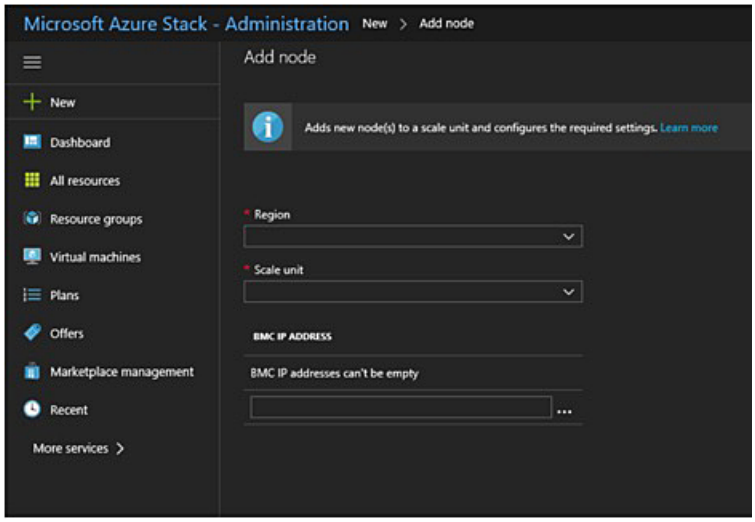
ステップ 9 **[New (新規)]** > **[Capacity (容量)]** > **[Scale Unit Node (スケール ユニット ノード)]**

に移動します。



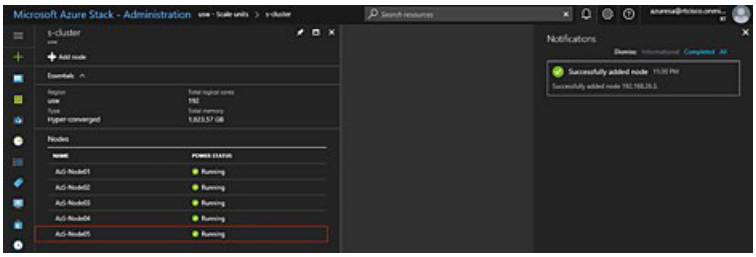
ステップ 10 **[Add Node (ノードの追加)]** ペインで、**[Region (領域)]** を選択してから、ノードを追加する **[Scale Unit (スケール ユニット)]**を選択します。また、追加するスケール ユニット ノードの BMC IP アドレス (手順 7 でメモしたインバンド管理 IP アドレス) を指定します。

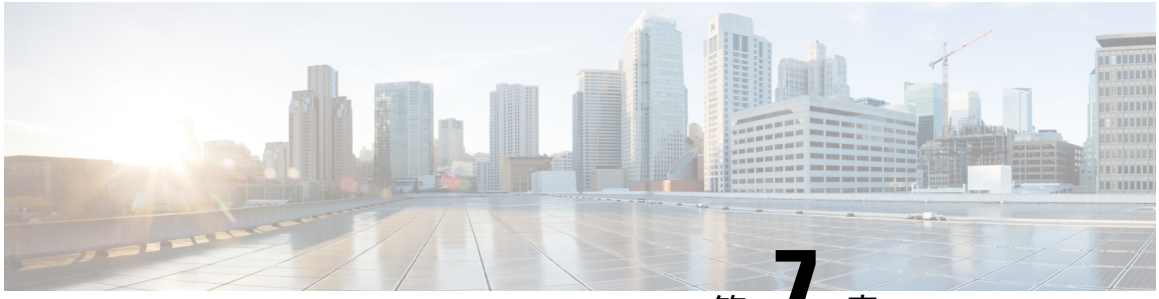
（注） 一度に追加できるノードは 1 つだけです。



ステップ 11 PowerShell を使用してノードを追加することもできます。詳細な手順については、『Microsoft Add node documentation』を参照してください。

（注） ノードの追加時には、スケール ユニットのステータスが **[Expanding (拡張)]** と表示され、このスケールユニットの拡張には非常に長い時間がかかります。最後に追加されたノードのステータスが **[Running (実行中)]** と表示されている限り、新しいノードをクラスタに追加できます。これにより、クラスタの展開が完了するまで待機する必要はありません。


Microsoft Azure Stack - Administration
s-cluster
Add node
Essentials
Nodes
Notifications
Successfully added node



第 7 章

ハードウェアの交換

- ハードウェアの交換 （39 ページ）
- ディスクの交換 （39 ページ）

ハードウェアの交換

次のリンクを使用して、障害のあるコンポーネントの交換について Microsoft 手順を実行します。

https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-replace-component?view=azs-1908

Cisco Azure Stack Hub のお客様によってのみ交換が可能なコンポーネントは、SAS ディスク ドライブの前面および背面に取り付けます。その他のすべてのコンポーネントの障害については、Cisco サポートにお問い合わせください。

ディスクの交換

Azure Stack Hub 管理者ポータルのディスク障害アラートで、障害が発生したディスクのサーバスロット情報とシリアル番号を提供します。

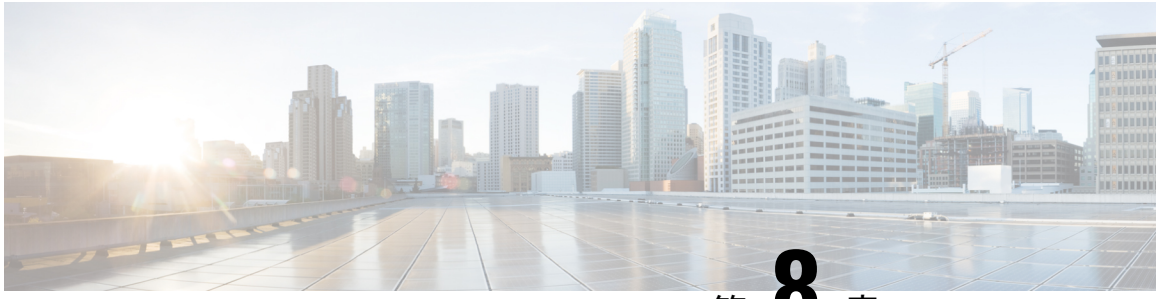
手順

ステップ 1 障害のあるディスクをサーバから見つけて取り外します。

ステップ 2 障害が発生したディスクのシリアル番号を使用して交換用ディスクを注文します。

交換用ディスクを注文するには、次のポータルを使用します: https://mycase.cloudapps.cisco.com/case。または、Cisco サポートまでお問い合わせください。

ステップ 3 交換用ディスクを受け取ったら、交換用ディスクをサーバにインストールし、Microsoft の手順に従ってディスクをアクティブにします。



第 8 章

システムの管理

- UCS の Call Home の概要 （41 ページ）
- Call Home の設定 （44 ページ）
- Call Home の有効化 （48 ページ）
- Call Home の無効化 （48 ページ）

UCS の Call Home の概要

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

重要 Call Home ではセキュア プロトコルは使用されません。この機能はデフォルトではディセーブルになっています。

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

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

メッセージを送信するように Call Home を設定すると、Cisco UCS Manager によって適切な CLI **show** コマンドが実行され、コマンド出力がメッセージに添付されます。

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

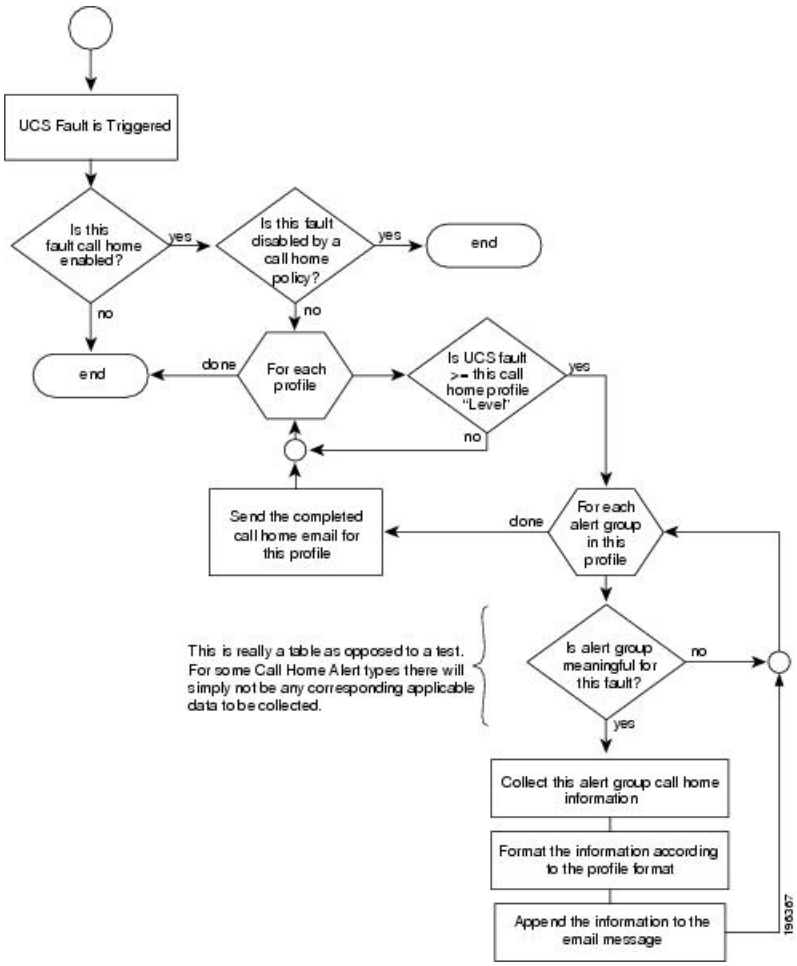
- 1 または 2 行で障害を説明する、ポケットベルや印刷レポートに適したショート テキスト フォーマット。

- 詳細な情報を十分に書式が整えられたメッセージで提供する、ユーザが読むのに適したフルテキストフォーマット。
- Extensible Markup Language（XML）と Adaptive Messaging Language（AML）XML Schema Definition（XSD）を使用する、コンピュータで読み取り可能な XML フォーマット。AML XSD は Cisco.com の Web サイトで公開されています。XML フォーマットでは、シスコの TAC との通信が可能になります。

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

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

図 *1*: 障害発生後のイベントの流れ



重要 Call Home は、デフォルトで [オフ（Off）] として設定されます。Call Home は非セキュア機能なので、明示的に有効にする必要があります。

Call Home の考慮事項とガイドライン

Call Home の設定方法は、機能の使用目的によって異なります。Call Home を設定する前に考慮すべき情報には次のものがあります。

宛先プロファイル

少なくとも 1 つの宛先プロファイルを設定する必要があります。使用する 1 つまたは複数の宛先プロファイルは、受信エンティティがポケットベル、電子メール、または自動化されたサービス（Cisco Smart Call Home など）のいずれであるかによって異なります。

宛先プロファイルで電子メール メッセージ配信を使用する場合は、Call Home を設定するときにシンプル メール転送プロトコル（SMTP）サーバを指定する必要があります。

連絡先情報

受信者が Cisco UCS ドメインからの受信メッセージの発信元を判別できるように、連絡先の電子メール、電話番号、および所在地住所の情報を設定する必要があります。

システム インベントリを送信して登録プロセスを開始した後、Cisco Smart Call Home はこの電子メール アドレスに登録の電子メールを送信します。

電子メール アドレスに #（ハッシュ記号）、スペース、&（アンパサンド）などの特殊文字が含まれていると、電子メール サーバが電子メール メッセージをそのアドレスに配信できないことがあります。RFC2821 および RFC2822 に準拠し、7 ビット ASCII 文字のみを含む電子メール アドレスを使用することをお勧めします。

電子メール サーバまたは HTTP サーバへの IP 接続

ファブリック インターコネクトに、電子メール サーバまたは宛先 HTTP サーバへの IP 接続を与える必要があります。クラスタ設定の場合は、両方のファブリック インターコネクトに IP 接続を与える必要があります。この接続により、現在のアクティブなファブリック インターコネクトで Call Home 電子メール メッセージを送信できることが保証されます。これらの電子メール メッセージの発信元は、常にファブリック インターコネクトの IP アドレスになります。クラスタ設定で Cisco UCS Manager に割り当てられた仮想 IP アドレスが、電子メールの発信元になることはありません。

Smart Call Home

Cisco Smart Call Home を使用する場合は、次のことが必要です。

- 設定するデバイスが、有効なサービス契約でカバーされている必要があります。
- Cisco UCS 内で Smart Call Home 設定と関連付けられるカスタマー ID は、Smart Call Home が含まれるサポート契約と関連付けられている CCO（Cisco.com）アカウント名にする必要があります。

Cisco UCSの障害と Call Home の重大度

Call Home は複数の Cisco 製品ラインにまたがって存在するため、独自に標準化された重大度があります。次の表に、基礎をなす Cisco UCS の障害レベルと Call Home の重大度とのマッピングを示します。Call Home のプロファイルにレベルを設定するときには、このマッピングを理解しておくことが必要です。

表 *1*: 障害と *Call Home* の重大度のマッピング

Call Home の重大度	Cisco UCS の障害	Call Home での意味
(9) Catastrophic	該当なし	ネットワーク全体に壊滅的な障害が発生しています。
(8) Disaster	該当なし	ネットワークに重大な影響が及びます。
(7) Fatal	該当なし	システムが使用不可能な状態。
(6) Critical	Critical	クリティカルな状態、ただちに注意が必要。
(5) Major	Major	重大な状態。
(4) Minor	Minor	軽微な状態。
(3) Warning	Warning	警告状態。
(2) Notification	Info	基本的な通知と情報メッセージ。他と関係しない、重要性の低い障害です。
(1) Normal	Clear	通常のイベント。通常の状態に戻ることを意味します。
(0) debug	該当なし	デバッグ メッセージ。

Call Home の設定

手順

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

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

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

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

重要　Call Home は、デフォルトで [オフ（Off）] として設定されます。Call Home は非セキュア機能なので、明示的に有効にする必要があります。

名前	説明
[State] フィールド	次のいずれかになります。 • **[Off]**：Call Home はこのCisco UCS ドメインには使用されません。 • **[On]**：Cisco UCSは、システムで定義された Call Home ポリシーおよびプロファイルに基づいて Call Home アラートを生成します。 （注）　Cisco UCS Manager GUIでは、このフィールドを **[on]** に設定すると、このタブに残りのフィールドが表示されます。
[Switch Priority] ドロップダウン リスト	次のいずれかになります。 • **[アラート（Alerts）]** • **[Critical]** • **デバッグ** • **緊急（Emergencies）** • **Errors** • **Information** • **通知** • **警告**
[Throttling] フィールド	同じイベントについて受信する重複メッセージの数を制限するかどうかを示します。次のいずれかになります。 • On：送信される重複メッセージの数が 2 時間以内に 30 件を越えると、そのアラートタイプに関するそれ以降のメッセージは破棄されます。 • [Off]：検出された数に関係なく、すべての重複メッセージが送信されます。

a) **[State]** フィールド で、[On] をクリックします。

（注）　Cisco UCS Manager GUIでは、このフィールドを **[on]** に設定すると、このタブに残りのフィールドが表示されます。

b) **[Switch Priority]** ドロップダウン リストから、次のいずれかのレベルを選択します。

- **[アラート（Alerts）]**
- **[Critical]**
- デバッグ
- 緊急（**Emergencies**）
- **Errors**
- **Information**
- 通知
- 警告

ファブリック インターコネクトの複数のペアがある大規模な Cisco UCS の展開の場合は、メッセージの受信者がメッセージの優先順位を判断できるようこのフィールドを使用して特定の 1 つの Cisco UCS ドメインからのメッセージに重大度を割り当てることができます。このフィールドは、小規模な Cisco UCS の展開（単一の Cisco UCS ドメイン など）には有用でないことがあります。

ステップ 5 [Contact Information] 領域で、次のフィールドに必要な連絡先情報を入力します。

名前	説明
[Contact] フィールド	主要 Call Home 連絡先。 255 文字以下の ASCII 文字で入力します。
[Phone] フィールド	主要連絡先の電話番号。 +（プラス記号）と国番号から始まる国際形式の番号を入力します。ハイフンは使用できますが、カッコは使用できません。
[Email] フィールド	主要連絡先の電子メール アドレス。 Cisco Smart Call Home によってこの電子メール アドレスに登録メールが送信されます。 （注） 電子メール アドレスに #（ハッシュ記号）、スペース、&（アンパサンド）などの特殊文字が含まれていると、電子メール サーバが電子メール メッセージをそのアドレスに配信できないことがあります。RFC2821 および RFC2822 に準拠し、7 ビット ASCII 文字のみを含む電子メール アドレスを使用することをお勧めします。
[Address] フィールド	主要連絡先の住所。 255 文字以下の ASCII 文字で入力します。

ステップ 6 [Ids] 領域で、Call Home が使用する ID 情報を次のフィールドに入力します。

ヒント　Smart Call Home を設定しない場合は、この手順を省略できます。

名前	説明
[Customer Id] フィールド	ライセンス上のサポート契約の契約番号を含むCisco.com ID。 510 文字以下の ASCII 文字を入力します。
[Contract Id] フィールド	お客様の Call Home 契約番号。 510 文字以下の ASCII 文字を入力します。
[Site Id] フィールド	お客様のサイトに固有の Call Home ID。 510 文字以下の ASCII 文字を入力します。

ステップ 7　[Email Addresses] 領域で、Call Home アラート メッセージの電子メール情報を次のフィールドに入力します。

名前	説明
[From] フィールド	システムによって送信される Call Home アラート メッセージの [From] フィールドに表示される電子メール アドレス。
[Reply To] フィールド	システムによって送信される Call Home アラート メッセージの [To] フィールドに表示される返信先電子メール アドレス。

ステップ 8　[SMTP Server] 領域で、Call Home が電子メール メッセージを送信する SMTP サーバに関する情報を次のフィールドに入力します。

名前	説明
[Host (IP Address or Hostname)] フィールド	SMTP サーバの IPv4 または IPv6 アドレスまたはホスト名。 （注）　IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメイン が Cisco UCS Central に登録されていない、または DNS 管理が**ローカル**に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン が Cisco UCS Central に登録されていて、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
[Port] フィールド	SMTP サーバとの通信に使用されるポート番号。 1 ～ 65535 の整数を入力します。デフォルトは 25 です。

ステップ 9　[Save Changes] をクリックします。

Call Home の有効化

この手順は任意です。ファームウェアのアップグレードを開始する前に Call Home をディセーブルにした場合にのみ、イネーブルにする必要があります。

手順

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

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

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

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

（注） Cisco UCS Manager GUIでは、このフィールドを **[on]** に設定すると、このタブに残りのフィールドが表示されます。

ステップ 5 [Save Changes] をクリックします。

Call Home の無効化

この手順は任意です。

Cisco UCS ドメインをアップグレードすると、アップグレードプロセスを完了するために Cisco UCS Manager によってコンポーネントが再起動されます。この再起動によって、サービスの中断およびコンポーネントの障害と同じイベントが発生し、Call Home アラートの送信がトリガーされます。アップグレードの開始前に Call Home をディセーブルにしない場合は、アップグレードに関連したコンポーネントの再起動によって生成されるアラートを無視してください。

手順

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

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

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

ステップ 4 [Admin] 領域で、**[State]** フィールド で [Off] をクリックします。

（注） このフィールドを [Off] に設定すると、Cisco UCS Manager はこのタブの残りのフィールドを非表示にします。

ステップ 5 [Save Changes] をクリックします。