Cisco UCS Performance Manager スタートアップ ガイド

初版:2017 年 6 月

リリース 2.5.0

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/

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。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. シスコの商標の一覧は、http://www.cisco.com/go/trademarks でご確認いただけます。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)

このマニュアルで使用している IP アドレスは、実際のアドレス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、および図は、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。

© 2014-2017 Cisco Systems, Inc. All rights reserved.

目次

このマニュアルについて 4

モニタリングのための準備 5
ネットワーク デバイスの準備 5
ストレージ デバイスの準備 6
サーバ デバイスの準備 7
ハイパーバイザ デバイスの準備 9
検査ツールを使用した設定の確認 9
オプション : IPv6 ネットワークでのモニタリングの有効化 9

ブラウザ インターフェイスへのアクセスの有効化 12

Cisco UCS Performance Manager のセットアップ 13
ライセンス契約への同意 13
ライセンス キーの提供 14
ユーザ設定 15
UCS セントラルの追加 15
UCS ドメインの追加 16
インフラストラクチャの追加 17
SMTP の設定 20
デバイス認証の詳細の更新 21
デバイス レコード情報の追加または編集 21

マルチホスト展開の開始と停止 23
Cisco UCS Performance Manager の起動 23
Cisco UCS Performance Manager の停止 24

デフォルトのサーバ パスワード 25
MariaDB パスワードの変更 26
RabbitMQ サーバ パスワードの変更 28
Zope 認証サーバ パスワードの変更 29

このマニュアルについて

『*Cisco UCS Performance Manager スタートアップ ガイド*』は、Cisco UCS Performance Manager Express および Cisco UCS Performance Manager を設定する方法とモニタリングのための環境を準備する方法について説明します。『Cisco UCS Performance Manager Installation Guide』に記載されている展開に必要なすべての手順を完了後、このガイドを使用してください。

- Cisco UCS Performance Manager Express では、Cisco UCS Central、Cisco UCS ドメイン、Linux および Microsoft Windows サーバ、ハイパーバイザ サーバおよびコントロール センターのモニタリングができます。
- Cisco UCS Performance Manager では、Cisco UCS Central、Cisco UCS ドメイン、Linux および Microsoft Windows サーバ、ハイパーバイザ サーバ、ネットワーク デバイス、ストレージ デバイスおよびコントロール センターのモニタリングができます。

便宜上、このマニュアルでは、総称して「Cisco UCS Performance Manager」を使用し、2 つのライセンス間の違いを明示的に記載します。

関連資料

タイトル	説明
『Cisco UCS Performance Manager Planning Guide』	Cisco UCS Performance Manager を展開するための準備に関する一般的な情報と固有の情報を提供します。
『Cisco UCS Performance Manager Installation Guide』	Cisco UCS Performance Manager をインストールするための詳細情報と手順を提供します。
『Cisco UCS Performance Manager Upgrade Guide』	既存の Cisco UCS Performance Manager 2.x インスタンスを新しいバージョンにアップグレードするための詳細な手順を提供します。
『Cisco UCS Performance Manager Migration Guide』	Cisco UCS Performance Manager バージョン 1.x からバージョン 2.x インスタンスにデータを移行する手順についての詳細な情報（該当する場合）を提供します。
『Cisco UCS Performance Manager スタートアップ ガイド』	インストール後に環境をモニタするために Cisco UCS Performance Manager を設定する手順について説明します。
『Cisco UCS Performance Manager ユーザ ガイド』	UCS 環境で Cisco UCS Performance Manager を使用するための詳細な手順について説明します。
『Cisco UCS Performance Manager Administration Guide』	Cisco UCS Performance Manager のアーキテクチャおよび機能の概要と、システムを使用する上で役立つ手順と例を提供します。
『Cisco UCS Performance Manager リリース ノート』	公開されているマニュアル セットにはまだ記載されていない既知の問題、解決済みの問題、および最新の情報について説明します。

マニュアルに関するフィードバック

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

モニタリングのための準備 1

Cisco UCS Performance Manager は、標準の管理 API を使用してパフォーマンス データを収集するため、モニタリング データを収集するための独自エージェントをインフラストラクチャ デバイスにインストールしません。ただし、次の章に示す情報を確認し、モニタするデバイスがデータの要求に応答する準備ができていることを確認することを推奨します。

インフラストラクチャでモニタする準備が整うと、Cisco UCS Performance Manager のセットアップ ウィザードで、EULA の受け入れ、ライセンス キーの提供、UCS セントラル デバイスの設定、UCS ドメインの設定、カテゴリ別とタイプ別でのデバイスの追加のプロセスが開始されます。

ネットワーク デバイスの準備

この章では、モニタリング用にデバイスを準備する手順について示します。

スイッチおよびルータの準備

モニタリング用のスイッチまたはルータ デバイスを準備するには、SNMP エージェントがインストールされ、現在デバイス上で実行されていることを確認します。

（注） ライセンスが Cisco UCS Performance Manager Express の場合は、このトピックをスキップしてください。

Cisco UCS ネットワーク デバイスの準備

Cisco UCS Performance Manager は、SNMP を使用して多くのシスコ製品に対してカスタマイズされたサポートまたは汎用サポートを提供します。

次の表に、シスコ製品とシスコ製品をサポートするカスタマイズされた Cisco UCS Performance Manager のデバイス タイプとの関係を示します。デバイス タイプは、[Add Infrastructure] ウィザードの [Network] 領域にリストされます。このウィザードは、セットアップ ウィザードの一部で、Cisco UCS Performance Manager ブラウザ インターフェイスから利用できます。

（注） 次のデバイス考慮事項が適用されます。

- Cisco Nexus 7000 および 9000 スイッチなど、サポート対象デバイスの中には、個別にモニタするエンドポイントが多数存在するものがあります。そのような高密度デバイスをモニタする場合に、どの程度のサイズの Cisco UCS Performance Manager の展開が必要となるかが不明な場合は、シスコ代理店にお問い合わせください。

- Cisco Nexus 9000 シリーズ デバイスをモニタするには、はじめにデバイスの機能マネージャ CLI コマンドで NX-API を有効にする必要があります。このタスクの実行に関する詳細な手順については、Nexus 9000 に関する*シスコのマニュアル*を参照してください。

シスコの製品	デバイス タイプ
Cisco Catalyst 6500 および 3560 シリーズ スイッチ	Cisco 6500（SNMP）
Cisco Nexus 5000 シリーズ スイッチ	Cisco Nexus 5000（SNMP + Netconf）
Cisco Nexus 7000 シリーズ スイッチ	Cisco Nexus 7000（SNMP + Netconf）
Cisco Nexus 2000 シリーズ ファブリック エクステンダ	Cisco Nexus 5000（SNMP + Netconf）
Cisco Nexus 1000v シリーズ スイッチ	Cisco Nexus 1000V（SNMP + Netconf）
Cisco Nexus 3000 シリーズ スイッチ	Cisco Nexus 3000（SNMP + Netconf）
Cisco Nexus 9000 シリーズ スイッチ	Cisco Nexus 9000（NX-API）
Cisco Catalyst 6500 シリーズ仮想スイッチング システム	Cisco VSS（SNMP）
Cisco MDS 9000 シリーズ マルチレイヤ スイッチ	Cisco MDS 9000（SNMP）

さらに、Cisco UCS Performance Manager では 2 つの汎用デバイス タイプが提供されます。

シスコの製品	デバイス タイプ
Cisco CatOS ベース スイッチまたはルータ	汎用スイッチまたはルータ（SNMP）
Cisco IOS ベース スイッチまたはルータ	Cisco IOS（SNMP）

ストレージ デバイスの準備

この項では、モニタリング用に NetApp と EMC のストレージ デバイスを準備する方法について説明します。

Cisco UCS Performance Manager Express のユーザは、このトピックをスキップできます。

レガシー NetApp ファイラ

Cisco UCS Performance Manager は、SNMP を使用して Data ONTAP® API（ZAPI）をサポートしていないレガシー NetApp ファイラをモニタします。

多くのオブジェクト（Aggregate、Volume、Plex および RAID グループ）の値は NetApp MIB で公開されていないため、収集されたデータは概算値です。

モニタリング用のレガシー NetApp ファイラを準備するには、SNMPv2 がインストールされていることを確認してから SNMP エージェントを起動します。

最新の NetApp ファイラ

Cisco UCS Performance Manager は、HTTP を使用して Data ONTAP® API（ZAPI）をサポートする NetApp ファイラをモニタします。

モニタリング用の最新の NetApp ファイラを準備するには、次の条件を確認します。

- ファイラが 7 モードまたは C モードで動作している。
- ZAPI のサポートされているバージョンがインストールされ、有効になっている。最低限必要なバージョンは 8.x です。

- ファイラ上のアカウントのユーザ名とパスワードに、ZAPI の使用が許可されている。

EMC ストレージ アレイ

Cisco UCS Performance Manager は、Web-Based Enterprise Management（WBEM）プロトコルを使用して、EMC VMAX および VNX ストレージ アレイに関連付けられた EMC Storage Management Initiative Specification（SMI-S）プロバイダーにクエリを送信します。

モニタリング用に EMC アレイを準備するには、以下が必要です。

- モニタするアレイのタイプごとに少なくとも 1 つの EMC SMI-S プロバイダーが実行されている必要があります。（VMAX と VNX のデータ モデルは異なります。）
- Cisco UCS Performance Manager に SMI-S プロバイダーを追加する前に、要求に応答していることを確認することを推奨します。

  SMI-S プロバイダー バージョン 4.6 がこのバージョンの Cisco UCS Performance Manager に対して認証されています。SMI-S プロバイダー バージョン 8.1 は、現時点ではサポートされていません。
- 次の情報が必要です。
  - 各 SMI-S プロバイダーでデータを収集する権限を持つアカウントのユーザ名とパスワード。
  - 各 SMI-S プロバイダーの IP アドレス。
  - 各 SMI-S プロバイダーがリクエストをリッスンするポート番号。
  - SSL を使用するかどうか。

（注） EMC デバイスで統計ログが無効になっている場合、EMC アレイのコンポーネント タイプのグラフには NaN と表示されます。ロギング機能はデフォルトのタイムアウト値が低いので、高い値に設定するか、ロギング機能を定期的にオンにする必要があります。

EMC デバイスでの SMI-S プロバイダーの確認

この手順を実行するには、モニタするアレイの SMI-S プロバイダーへのネットワーク パスを持つ Linux ホストが必要です。

（注） Cisco UCS Performance Manager のホストではこの手順を実行しないでください。

EMC アレイに関連付けられた SMI-S プロバイダーが正しく設定され、コマンド ライン ツールから WBEM クエリに応答していることを確認するには、次の手順を実行します。

1. Linux ホストに `root` として、またはスーパーユーザ権限を持つユーザとしてログインします。
2. `wbemcli` などの WBEM コマンドライン インターフェイス パッケージをインストールします。
3. SMI-S プロバイダーを確認します。変数をご使用の環境で有効な値に置換します。

   ```
   wbemcli IP-Address:Port -u admin \
    -p 'Password' -n root/emc --no-sslei('EMC DiskDrive')
   ```

   期待される結果は、ディスクドライブ クラスのリストです。

サーバ デバイスの準備

この項では、モニタリング用に Linux サーバおよび Windows サーバを準備する方法について説明します。

モニタリング用の Linux サーバの準備

Cisco UCS Performance Manager は、SNMP または SSH を使用して Linux サーバをモニタします。

SNMP モニタリングの場合は、SNMP パッケージをサーバ（たとえば、*Net-SNMP*）にインストールし、エージェントを起動します。

SSH モニタリングの場合は、次の手順を実行します。

- SSH サーバ パッケージ（たとえば、*OpenSSH*）をインストールし、SSH デーモンを起動します。
- Linux サーバを監視するには、Linux サーバ上で SSH を使用してリモートで `pvs`、`vgs`、`lvs`、`systemctl`、`initctl`、`service` コマンドを実行する機能が必要です。デフォルトでは、これらのコマンドのほとんどは、`root` ユーザがローカルで実行することしかできません。`root` ユーザがこれらのコマンドをリモートで実行できるようにするには、次の手順を実行します。

  1. サーバに `sudo` パッケージをインストールします。
  2. `root` ユーザが TTY なしで SSH 経由でコマンドを実行することを許可します。

     a. `/etc/sudoers` ファイルを編集します。
     b. `root ALL=(ALL) ALL` を含む行を見つけます。
     c. その下に次の行を追加します。

     ```
     Defaults:root !requiretty
     ```

     d. 変更を保存し、終了します。

  または、これらのコマンドをリモートで実行する非ルート ユーザを設定することもできます。次の手順を実行します。

  1. Linux サーバ上に、モニタリングを目的とした `zenmonitor` という名前のユーザを作成します。
  2. サーバに `sudo` パッケージをインストールします。
  3. `zenmonitor` ユーザが TTY なしで SSH 経由でコマンドを実行することを許可します。

     a. `sudoers.d` がサポートされていない場合は `/etc/sudoers.d/zenoss` または `/etc/sudoers` を編集し、ファイルの最後に次の行を追加します。

     ```
     Defaults:zenmonitor !requiretty
     Cmnd Alias ZENOSS LVM CMDS = /sbin/pvs, /sbin/vgs, /sbin/lvs, \
         /usr/sbin/pvs, /usr/sbin/vgs, /usr/sbin/lvs
     Cmnd Alias ZENOSS SVC CMDS = /bin/systemctl list-units *, \
         /bin/systemctl status *, /sbin/initctl list, /sbin/service --
     status-all, \
         /usr/sbin/dmidecode
     zenmonitor ALL=(ALL) NOPASSWD: ZENOSS LVM CMDS, ZENOSS SVC CMDS
     ```

     b. 変更を保存し、これらのコマンドのすべてのパスが正しいことを確認します。

モニタリング用の Windows サーバの準備

Cisco UCS Performance Manager は、SNMP または WinRM を使用して、次のように Microsoft Windows システムをモニタします。

- Microsoft Windows Server 2106：WinRM のみ。

  SNMP サポートは、Windows Server 2106 では存在しません。
- Microsoft Windows Server 2012 および 2012 R2：WinRM のみ。

  SNMP サポートは、Windows Server 2012 では存在しません。
- Microsoft Windows Server 2008 R2：SNMP v1/v2 または WinRM。

SNMP v3 のサポートは、Windows Server 2008 R2 では存在しません。

SNMP モニタリング用に Windows 2008 システムを準備するには、SNMP サービスを起動します。

WinRM モニタリング用に Windows システムを準備するには、付録の「Windows システムの準備」を参照してください。

ハイパーバイザ デバイスの準備

この項では、モニタリング用に vSphere および Hyper-V ハイパーバイザを準備する方法について説明します。

vSphere エンドポイント

Cisco UCS Performance Manager は、SOAP を使用して次のバージョンの vSphere を実行する VMware vSphere サーバをモニタします。

- 4.1
- 5.0
- 5.1
- 5.5
- 6.0

VMware vSphere サーバをモニタするための準備を行うには、次の手順を実行します。

- サポートされているバージョンのソフトウェアを実行していることを確認します。
- vSphere API を使用する権限を持つサーバでのアカウントのユーザ名とパスワードを取得します。
- SSL を使用するかどうかを決定します。

Hyper-V

Cisco UCS Performance Manager は、WinRM を使用して次の Microsoft Hyper-V システムをモニタします。

- Microsoft Hyper-V Server 2016
- Microsoft Hyper-V Server 2012 および 2012 R2
- Microsoft Hyper-V Server 2008 および 2008 R2

WinRM モニタリング用に Hyper-V システムを準備するには、付録の「Windows システムの準備」を参照してください。

検査ツールを使用した設定の確認

環境を設定したら、Inspector を使用して設定を確認できます。Inspector ツールは通常、コントロール センターのマスター ホストにインストールされ、ご使用の環境で読み取り専用チェックを実行し、潜在的な問題を解決するためのアドバイスを提供します。

Inspector ツールの詳細（ダウンロードおよびインストールの手順を含む）については、ナレッジ ベースの記事『*Inspector: A tool to validate configuration*』を参照してください。

オプション：IPv6 ネットワークでのモニタリングの有効化

この手順では、Cisco UCS Performance Manager を設定して、IPv6 ネットワーク上にあるデバイスのモニタリングを有効にする方法について説明します。コントロール センターが導入されている IPv4 ネットワーク環境からネットワークにアクセスできる必要があります。

この手順を使用して、Docker の仮想ブリッジ インターフェイス `docker0` を使用して IPv6 アドレス ブロックをコントロール センターにルーティングします。Cisco UCS Performance Manager は、ルーティングされたブロック内のアドレスを持つ IPv6 デバイスをモニタできます。

この手順を実行するには、コントロール センターのクラスタ内の各ノードにアップストリーム ルータによってルーティングされる一意の IPv6 プレフィックスが必要で、クラスタ内の各ノードで Docker Engine サービスを IPv6 パケットを転送するように設定する必要があります。

たとえば、1 つのマスター ホストと 3 つのデリゲートを含むマルチホスト展開では、次の表に示す IPv6 設定を適用することができます。

コントロール センターのホスト	IPv6 リンク プレフィックス	IPv6 ルーテッド プレフィックス
マスター	2001:DB8:ABCD:1000::500/64	2001:DB8:ABCD:2000::/64
デリゲート 1	2001:DB8:ABCD:1000::501/64	2001:DB8:ABCD:2001::/64
デリゲート 2	2001:DB8:ABCD:1000::502/64	2001:DB8:ABCD:2002::/64
デリゲート 3	2001:DB8:ABCD:1000::503/64	2001:DB8:ABCD:2003::/64

次の例に、アップストリームの Cisco ルータで前述の表に示すスタティック ルートを設定する方法を示します。

```
ipv6 route 2001:DB8:ABCD:2000::/64 2001:DB8:ABCD:1000::500
ipv6 route 2001:DB8:ABCD:2001::/64 2001:DB8:ABCD:1000::501
ipv6 route 2001:DB8:ABCD:2002::/64 2001:DB8:ABCD:1000::502
ipv6 route 2001:DB8:ABCD:2003::/64 2001:DB8:ABCD:1000::503
```

次の操作を行ってください。

1. コントロール センターのマスター ホストに `root` またはスーパーユーザ権限を持つユーザとしてログオンします。
2. IPv6 パケット転送を設定します。
   - **a** テキスト エディタで `/etc/sysctl.d/ipv6.conf` を開きます。
   - **b** 次の行を追加または編集します。

     ```
     net.ipv6.conf.all.forwarding=1
     ```

   - **c** ファイルを保存し、テキスト エディタを終了します。
3. ホストを再起動せずに IPv6 パケット転送を有効にします。

   ```
   sysctl -w net.ipv6.conf.all.forwarding=1
   ```

4. IPv6 通信用に Docker を設定します。
   - **a** テキスト エディタで `/etc/sysconfig/docker` を開きます。
   - **b** *OPTIONS* 宣言の最後に次のフラグを追加します。
     CIDR 表記で、*Subnet-Block* をコントロール センターにルーティングするための IPv6 サブネットに置き換えます。

     ```
     --ipv6 --fixed-cidr-v6="Subnet-Block"
     ```

   - **c** *OPTIONS* 宣言の区切り文字をアポストロフィ(`'`)に変更します。

     OPTIONS 宣言のデフォルトの区切り文字は引用符(`"`)で、これは `--fixed-cidr-ipv6` フラグで使用される区切り文字と同じです。
   - **d** ファイルを保存し、テキスト エディタを終了します。
5. Docker サービスを再起動します。

   ```
   systemctl restart docker
   ```

6 **zenping** サービスの Docker コンテナを使用して、既知の IPv6 アドレスに ping を実行します。

```
serviced service attach zenping ping6 -c 1 ipv6.google.com
```

ping が成功すると、Docker は IPv6 アドレスを解決でき、IPv6 ネットワーク上のデバイスをモニタできるようになります。

ブラウザ インターフェイスへのアクセスの有効化 2

コントロール センターと Cisco UCS Performance Manager には、独立した Web サーバによって提供される独立したブラウザ インターフェイスがあります。Web サーバは両方とも SSL/TLS 通信を使用するように設定されています。

コントロール センターの Web サーバがコントロール センターのマスター ホストのホスト名とポート 50443 でリッスンします。完全修飾ドメイン名（FQDN）が `cc-master.example.com` のコントロール センター マスター ホストの場合、ホスト名の URL は `https://cc-master:50443` です。URL のホスト名の部分は IP アドレスと置き換えることができます。

Cisco UCS Performance Manager Web サーバは、*ポート パブリック エンドポイント*と*仮想ホスト パブリック エンドポイント*でリッスンします。

- デフォルトの*ポート パブリック エンドポイント*は、コントロール センターのマスター ホストのホスト名とポート 443 です。FQDN が `cc-master.example.com` の場合、デフォルトのポート パブリック エンドポイントの URL は `https://cc-master` です。コントロール センターのマスター ホストに複数のネットワーク インターフェイスがある場合、異なるホスト名で追加のパブリック エンドポイントを設定できます。また、ポート パブリック エンドポイントの TLS 通信を無効にすることができます。

  ポート パブリック エンドポイントを使用して Cisco UCS Performance Manager のブラウザ インターフェイスにアクセスするには、ネットワークの名前解決エントリの追加が必要です。コントロール センターのマスター ホストのネットワーク インターフェイスには、デフォルトのエントリで十分です。
- デフォルトの*仮想ホスト パブリック エンドポイント*は、前に `ucspm` のテキストが付加されたコントロール センターのマスター ホストのホスト名とポート 50443 です。FQDN が `cc-master.example.com` の場合、デフォルトの仮想ホスト パブリック エンドポイントの URL は `https://ucspm.cc-master:50443` です。デフォルトの仮想ホストの名前を変更し、追加の仮想ホスト パブリック エンドポイントを設定できます。

  仮想ホスト パブリック エンドポイントを使用して Cisco UCS Performance Manager のブラウザ インターフェイスにアクセスするには、ご使用の環境の DNS サーバ用に仮想ホストの名前解決エントリを追加する必要があります。

Cisco UCS Performance Manager のセットアップ 3

この項では、Cisco UCS Performance Manager セットアップ ウィザードを使用して、エンドユーザ ライセンス契約書の同意、ライセンス キーの提供、ユーザとパスワードの定義、UCS セントラルと UCS ドメインのセットアップ、インフラストラクチャの追加、SMTP のセットアップを行う方法について説明します。

このウィザードは、Cisco UCS Performance Manager ブラウザ インターフェイスに初めてログインすると起動します。（サポートされているブラウザとクライアント オペレーティング システムの詳細については、『*Cisco UCS Performance Manager Release Notes*』を参照してください。

Cisco UCS Performance Manager のブラウザ インターフェイスを開くには、ポート パブリック エンドポイントまたは仮想ホスト ポートのパブリック エンドポイントに移動します。詳細については、12 ページの「*ブラウザ インターフェイスへのアクセスの有効化*」を参照してください。

（注） このウィザードは 20 分たっても完了していない場合タイムアウトします。再度開始するには、そのブラウザ ウィンドウまたはタブを閉じ、再度ログインします。

セットアップ ウィザードを完了するには、次の項目が必要です。

- 組織を代表して Cisco UCS Performance Manager のエンドユーザ ライセンス契約を受諾する権限。
- デフォルトの管理アカウント（`admin`）のパスワード。
- 1 つの別の管理アカウントのユーザ名とパスワード。
- 製品（Cisco UCS Performance Manager Express または Cisco UCS Performance Manager）のライセンス キー。ライセンス キーを取得するには、シスコの担当者にご連絡ください。
- ご使用の環境の UCS セントラルおよび UCS ドメインのホスト名または IP アドレス。
- モニタする予定のリソースへの読み取りアクセスを許可された各サーバでのアカウントのユーザ名とパスワード。

ウィザードには [Add Infrastructure] ページが含まれていますが、これは任意です。[Add Infrastructure] ページは Cisco UCS Performance Manager インターフェイスの標準コンポーネントであるため、いつでも利用できます。

ライセンス契約への同意

Cisco UCS Performance Manager を仮想マシンにインストールし、コントロール センターを開始した後で、この手順を実行します。

1. Web ブラウザで、Cisco UCS Performance Manager インターフェイスのログイン ページに移動します。

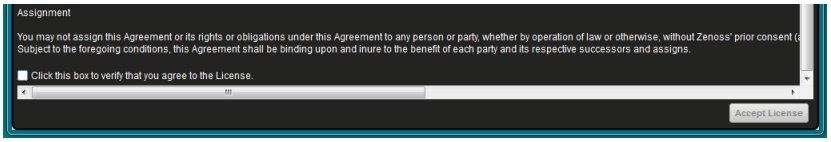
   Cisco UCS Performance Manager は、最初のログイン試行を [Setup] ページにリダイレクトします。このページには [End User License Agreement]（EULA）ダイアログ ボックスがあります。

（注） ホスト名を解決できない場合は、DNS サーバを確認するか、またはクライアント マシンで `hosts` ファイルへのエントリを追加します。詳細については、12 ページの「*ブラウザ インターフェイスへのアクセスの有効化*」を参照してください。

2 同意書を確認します。

3 [EULA] ダイアログ ボックスの下部にあるチェック ボックスをオンにして契約を確認し、[Accept License] をクリックします。

図 1：[EULA] ダイアログ ボックスの下部

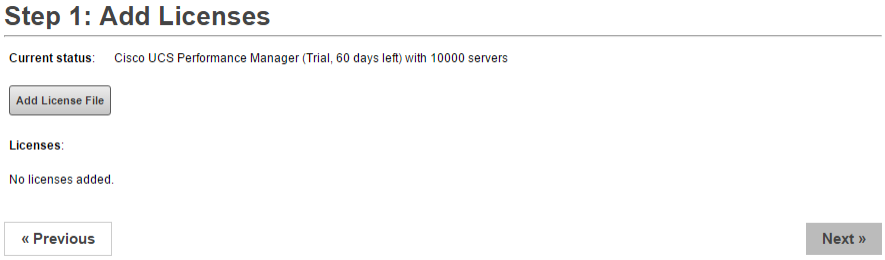


ライセンス キーの提供

EULA に同意した後、次の手順を実行します。Cisco UCS Performance Manager Express または Cisco UCS Performance Manager のライセンス キー ファイルが必要です。ライセンス キー ファイルは、Cisco UCS Performance Manager のブラウザ インターフェイスにアクセスできるワークステーションに配置する必要があります。ライセンス キー ファイルを取得する方法の詳細については、シスコ代理店にお問い合わせください。

1 [Cisco UCS Performance Manager Setup] ページで、[Get Started] をクリックします。

2 [Add Licenses] ページで、[Add License File] をクリックします。



（注） ライセンス ファイルがまだない場合は、最大 30 日間のトライアル バージョンを使用できます。ブラウザ インターフェイスからライセンス ファイルを後で入力できます。詳細については、『*Cisco UCS Performance Manager Administration Guide*』の「Product Licensing」の項を参照してください。

3 [Open] ダイアログ ボックスで、ライセンス ファイルを選択し、[Open] をクリックします。

4 [Current Status] フィールドの製品名とサーバ数を購入した製品と比較し、次のように進みます。

- 情報が購入内容と一致する場合は、[Next] をクリックして [Setup Users] ステップに進みます。
- 情報が購入内容と一致しない場合は、[Remove] をクリックし、シスコ代理店にお問い合わせください。

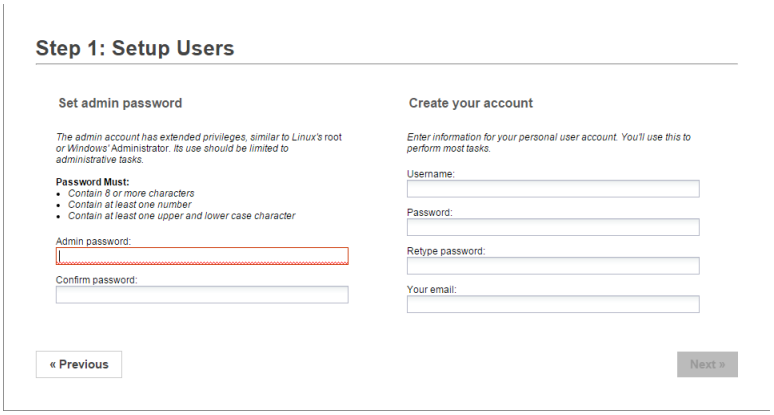
（注） Cisco UCS Performance Manager のブラウザ インターフェイスには、ライセンス キーを変更するためのオプションが含まれています。

ユーザ設定

次の手順を実行して、管理ユーザのパスワードを作成し、少なくとも 1 つの追加のユーザ アカウントを作成します。

1 [Set admin password] 領域で、管理者ユーザ アカウントのパスワードを入力し、確認します。

パスワードには、8 文字以上が必要です（大文字 1 つと数字 1 つを含む）。



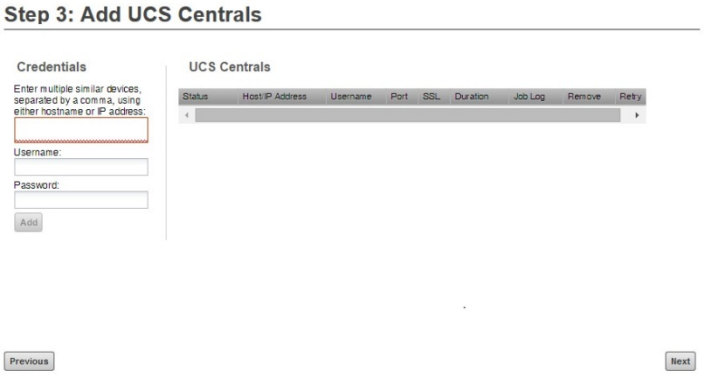
2 [Create your account] 領域で、追加の管理ユーザ アカウント名とパスワードを 1 つ作成します。

3 [Next] をクリックして、[Add UCS Centrals] に移動します。

UCS セントラルの追加

この手順は任意です。UCS セントラルをモニタリングしていない場合は、[Next] をクリックして次の手順にスキップします。モニタリングしている場合は、次の手順に従って UCS セントラルを追加します。

1 [Add UCS Centrals] ページで、1 つ以上の UCS セントラルの接続クレデンシャルを提供します。



a UCS セントラル ホストの完全修飾ドメイン名または IP アドレスを指定します。

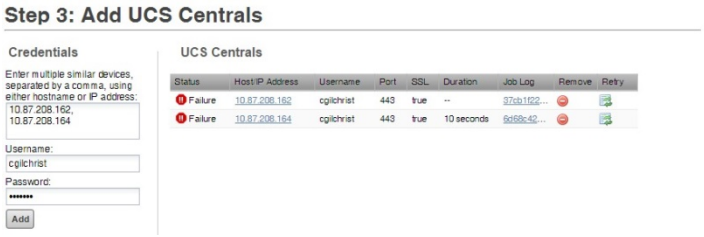
複数のデバイスをリストするには、ホスト名または IP アドレスをカンマで区切ります。

b [Username] に、モニタする予定のリソースへの読み取りアクセスを許可された UCS セントラルのユーザ アカウントの名前を指定します。

c 指定したユーザ名のパスワードを指定します。

d [Add] をクリックします。

2 [UCS Centrals] テーブルで、[Status] 列を確認し、次のように進みます。

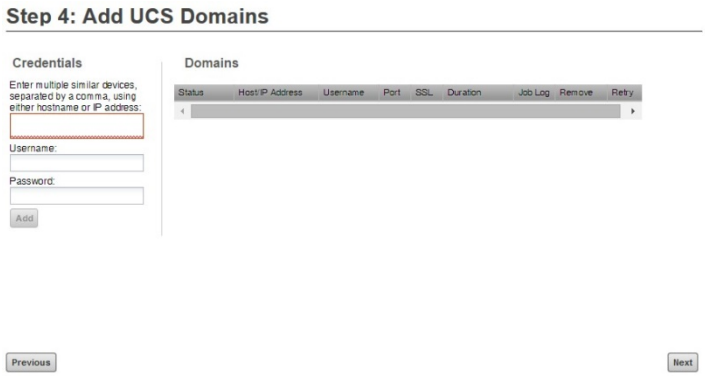


- 最後のメッセージが `Failure` の場合は、[Remove] をクリックし、再度ドメインの追加を試行します。
- 最後のメッセージが `Success` の場合は、必要に応じて、別のドメインを追加し、[Next] をクリックします。

UCS ドメインの追加

この手順は任意です。接続クレデンシャルが無い場合、または後で入力する場合は、[Next] をクリックして次の手順にスキップします。それ以外の場合は、次の手順に従って UCS ドメインを追加します。

1 [Add UCS Domains] ページで、1 つ以上の UCS ドメインの接続クレデンシャルを提供します。



a UCS ドメイン サーバの完全修飾ドメイン名または IP アドレスを指定します。

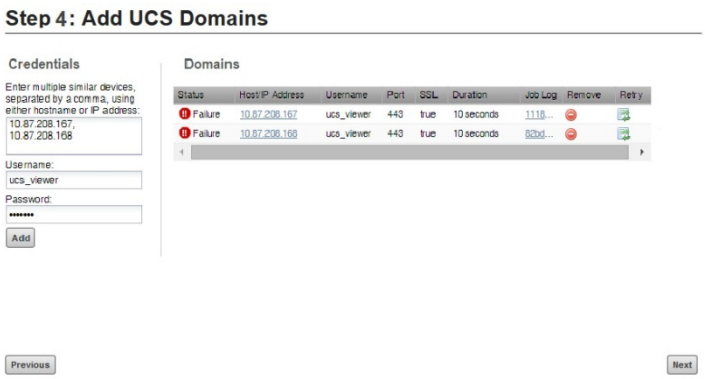
複数のデバイスをリストするには、ホスト名または IP アドレスをカンマで区切ります。

b [Username] に、モニタする予定のリソースへの読み取りアクセスを許可された UCS ドメインのユーザ アカウントの名前を指定します。

c 指定したユーザ名のパスワードを指定します。

d [Add] をクリックします。

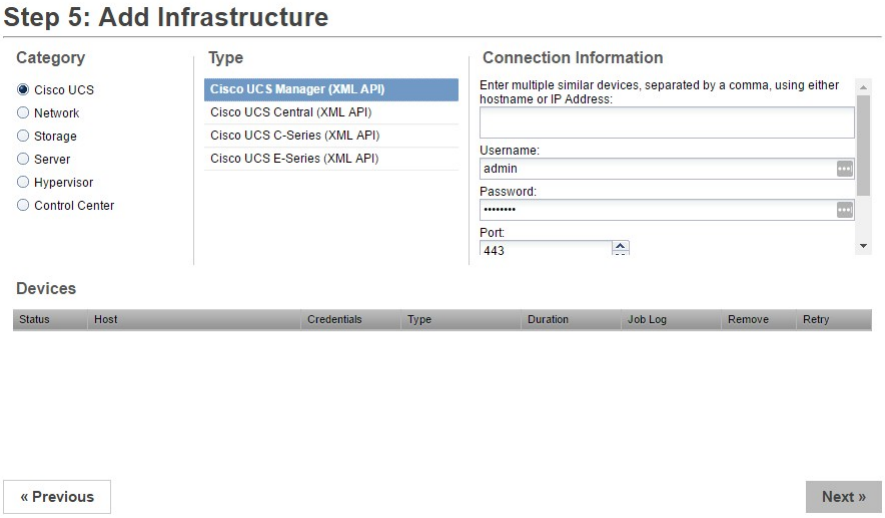
2 [Domains] テーブルで、[Status] 列を確認し、次のように進みます。



- 最後のメッセージが `Failure` の場合は、[Remove] をクリックし、再度ドメインの追加を試行します。
- 最後のメッセージが `Success` の場合は、必要に応じて、別のドメインを追加し、[Next] をクリックします。

インフラストラクチャの追加

インフラストラクチャの追加手順はオプションです。いつでも Cisco UCS Performance Manager の [Add Infrastructure] ページからデバイスを追加できます。



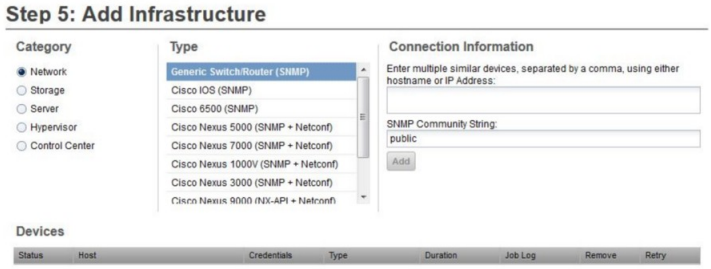
ウィザードとインフラストラクチャを後で終了する場合は、[Finish] をクリックします。ダッシュボードが表示されます。

ネットワーク デバイスの追加

この手順を実行するには、Cisco UCS Performance Manager のライセンスが必要です。ライセンスが Cisco UCS Performance Manager Express の場合は、19 ページの「*サーバ デバイスの追加*」に進みます。

このオプションの手順は、セットアップ ウィザードの**インフラストラクチャの追加**手順用です。

1 [Category] 領域で、[Network] を選択します。



2 [Type] リストで、追加するスイッチまたはルータの製品モデルを選択します。

デバイスからデータを収集するために使用されるプロトコルが、このリストのカッコ内に記載されています。

（注） Nexus 7000 および 9000 スイッチなど、[Type] リストのデバイスの一部では、多数の個別のモニタリング エンドポイントを表します。選択した Cisco UCS Performance Manager の仮想マシンのサイズが、モニタしたい高密度なデバイスの数をサポートしているかどうか不明な場合は、シスコ代理店にお問い合わせください。

---

3 [Connection Information] 領域で、追加するデバイスを指定します。選択するネットワーク デバイスのタイプによって、入力する接続情報フィールドが異なります。次のフィールドが無い場合は、選択が適用されません。

a [Enter multiple similar devices, separated by a comma, using either hostname or IP Address] フィールドに、ネットワーク上の 1 つ以上のスイッチまたはルータ デバイスのホスト名または IP アドレスを入力します。

b [SNMP Community String] フィールドで、必要に応じてデフォルト（`public`）を変更します。

このフィールドは、選択したデバイスが SNMP と NETCONF の両方をサポートしていて、ユーザがユーザ名とパスワードを入力している場合は使用されません。

c [Username] フィールドまたは [Netconf Username] フィールドに、デバイス上のユーザ アカウントの名前を入力します。

d [Password] フィールドまたは [Netconf Password] フィールドに、前のフィールドで指定したユーザ アカウントのパスワードを入力します。

e [Add] をクリックします。

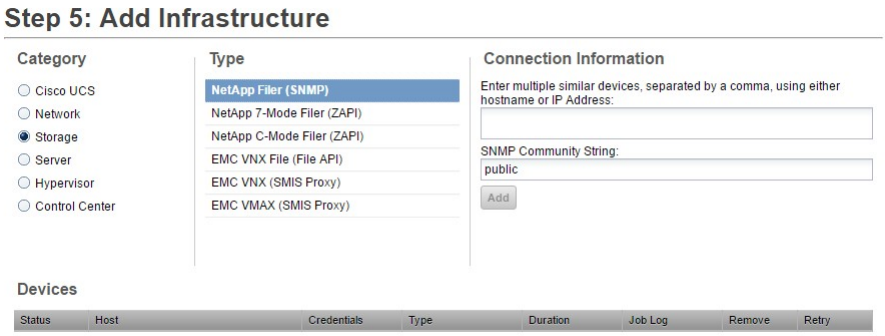
ネットワーク デバイスの追加が終了したら、[Next] をクリックします。

ストレージ デバイスの追加

この手順を実行するには、Cisco UCS Performance Manager のライセンスが必要です。ライセンスが Cisco UCS Performance Manager Express の場合は、19 ページの「*サーバ デバイスの追加*」に進みます。

このオプションは、セットアップ ウィザードのステップ 5 の一部です。

1 [Category] 領域で、[Storage] を選択します。



2 [Type] リストで、追加するストレージ デバイスの製品モデルを選択します。

デバイスからデータを収集するために使用されるプロトコルが、このリストのカッコ内に記載されています。

3 [Connection Information] 領域で、追加するデバイスを指定します。

   a [Enter multiple similar devices, separated by a comma, using either hostname or IP Addresses] フィールドに、ネットワーク上の少なくとも 1 つのストレージ デバイスのホスト名または IP アドレスを入力します。

   b 任意：[Username] フィールドに、デバイスのユーザ アカウントの名前を入力します。

   このフィールドは、デバイス プロトコルが SNMP である場合は表示されません。

   c 任意：[Password] フィールドに、前のフィールドで指定したユーザ アカウントのパスワードを入力します。

   このフィールドは、デバイス プロトコルが SNMP である場合は表示されません。

   d 任意：[Port] フィールドに、デバイスがデータ収集要求をリッスンするポートを入力します。

   このフィールドは、デバイス プロトコルが SMIS Proxy の場合にのみ表示されます。

   e セキュアな通信を使用してデータを収集するには [Use SSL?] チェックボックスをオンにして、非セキュアな通信を使用する場合はチェックボックスをオフにします。

   このフィールドは、デバイス プロトコルが SNMP である場合は表示されません。

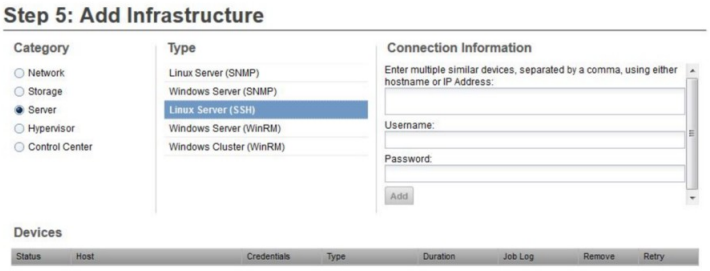
   f [Add] をクリックします。

ストレージ デバイスの追加が終了したら、[Next] をクリックします。

サーバ デバイスの追加

このオプションは、セットアップ ウィザードのステップ 5 の一部です。

1 [Category] 領域で、[Servers] を選択します。



2 [Type] リストで、追加するサーバのオペレーティング システムとモニタリング プロトコルを選択します。

デバイスからデータを収集するために使用されるプロトコルが、このリストのカッコ内に記載されています。

3 [Connection Information] 領域で、追加するサーバを指定します。

   a [Enter multiple similar devices, separated by a comma, using either hostname or IP Addresses] フィールドに、ネットワーク上の 1 つ以上のサーバ デバイスのホスト名または IP アドレスを入力します。

   b 任意：[SNMP Community String] フィールドで、必要に応じてデフォルト（`public`）を変更します。

   このフィールドは、デバイス プロトコルが SNMP である場合にのみ表示されます。

   c 任意：[Username] フィールドに、デバイスのユーザ アカウントの名前を入力します。

   このフィールドは、デバイス プロトコルが SNMP である場合は表示されません。

   d 任意：[Password] フィールドに、前のフィールドで指定したユーザ アカウントのパスワードを入力します。

   このフィールドは、デバイス プロトコルが SNMP である場合は表示されません。

   e 任意：[AD Domain Controller] フィールドに、ネットワーク上の Active Directory ドメイン コントローラの IP アドレスまたはホスト名を入力します。

   このフィールドは、デバイス プロトコルが WinRM である場合にのみ表示されます。

   f [Add] をクリックします。

サーバ デバイスの追加が終了したら、[Next] をクリックします。

ハイパーバイザ デバイスの追加

このオプションは、セットアップ ウィザードのステップ 5 の一部です。

1 [Category] 領域で、[Hypervisor] を選択します。

2 [Type] リストで、追加するハイパーバイザ サービスを選択します。
3 [Connection Information] 領域で、追加するサービスを指定します。
   a [Device Name] フィールドに、ハイパーバイザ サービスの名前を入力します。
   b [Hostname / IP Address] フィールドに、ハイパーバイザ サービスのホスト名または IP アドレスを入力します。
   c [Username] フィールドに、ホストにあるユーザ アカウントの名前を入力します。
   d [Password] フィールドに、前のフィールドで指定したユーザ アカウントのパスワードを入力します。
   e 任意：セキュアな通信を使用してデータを収集するには [Use SSL?] チェックボックスをオンにします（推奨）。

      このフィールドは、デバイス プロトコルが SOAP である場合にのみ表示されます。
   f 任意：[AD Domain Controller]、[Version]、[HTTP or HTTPS]、および [Port] フィールドに情報を入力します。

      これらのフィールドは、デバイス プロトコルが WinRM である場合にのみ表示されます。
   g [Add] をクリックします。

ハイパーバイザ デバイスの追加が終了したら、[Finish] をクリックします。

コントロール センターの追加

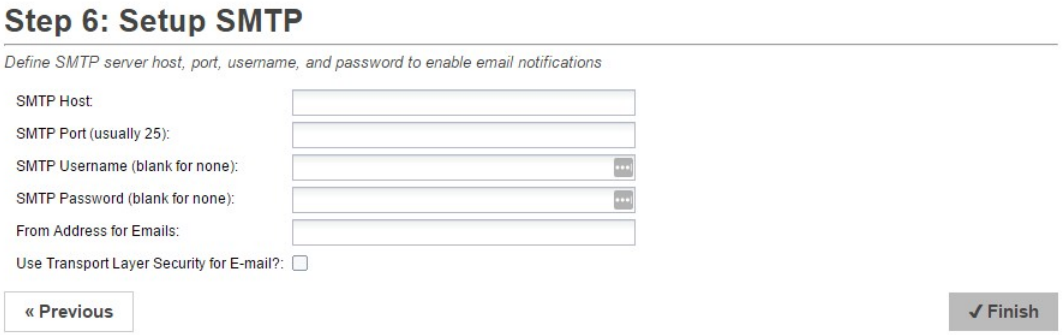
コントロール センターは、内部アプリケーション管理とオーケストレーション システムです。内部コンポーネントとそれらのパフォーマンス データを表示できるように、管理型リソースとしてコントロール センターが自動的に追加されます。

デバイスの追加が終了したら、[Finish] をクリックします。デバイスは後でいつでもさらに追加できます。

SMTP の設定

既存の電子メール サーバを使用するように Cisco UCS Performance Manager を設定するには、次の手順を使用します。

1 [Setup SMTP] ページで、Cisco UCS Performance Manager で使用する電子メール サーバに関する情報を指定します。



a [SMTP Host] フィールドに、既存の電子メール サーバの IP アドレスまたはホスト名を入力します。

b [SMTP Port (usually 25)] フィールドに、サーバが受信メッセージをリッスンするポートを入力します。

c [SMTP Username (blank for none)] フィールドに、サーバにメッセージを転送する権限を持つアカウントの名前を入力します。

d [SMTP Password (blank for none)] フィールドに、メッセージをサーバに転送する権限を持つアカウントのパスワードを入力します。

e [From Address for Emails] フィールドに、サーバに転送されたメッセージの送信元アドレスを入力します。

f TLS を有効にするには、[Use Transport Layer Security for E-mail] チェックボックスをオンにします。

2 [Finish] をクリックします。

デバイス認証の詳細の更新

データベースに追加され、適切なデバイス クラスに設定された各デバイスについて、Cisco UCS Performance Manager は、追加の認証情報または別の認証情報を要求してからでないと、デバイス情報の収集やデバイスの監視を行うことができない場合があります。

たとえば、/Server/Windows クラスのデバイスの場合は、システムがデバイスを監視できるようにするには、Windows のユーザ名とパスワードを指定する必要があります。次の手順を実行します。

1 デバイス リストの中からデバイス名をクリックします。
[Device summary] ページが表示されます。

2 左側のパネルから [Configuration Properties] を選択します。

3 zWinRMUser 構成プロパティをダブルクリックして、[Edit Config Property] ダイアログを表示します。

4 [Value] フィールドに Windows ユーザ名を入力し、[Submit] をクリックします。

5 zWinRMPassword 構成プロパティをダブルクリックして、[Edit Config Property] ダイアログを表示します。

6 [Value] フィールドに Windows パスワードを入力し、[Submit] をクリックします。

同様に、/Server/SSH/GenericLinux クラスのデバイスの場合は、SSH ユーザ名とパスワードを指定する必要があります。これらの値は、デバイスの zCommandUsername および zCommandPassword 構成プロパティで設定します。

（注） 変更を加えた後、デバイスのモデルを変えてみて、認証の変更が有効であることを確認する必要があります。

（注） Cisco UCS Performance Manager は、256 ビット キー サイズの Advanced Encryption Standard（AES）を使用してすべてのパスワードを暗号化し、Zope オブジェクト データベースに格納します。

デバイス レコード情報の追加または編集

デバイスの詳細を追加または編集することができます。

情報を追加または編集するには、次の手順を実行します。

1. デバイス リストの中からデバイス名をクリックします。デバイスの概要ページが表示されます。
2. 変更する値を選択するか、編集する値のラベルの横にある「edit」リンクをクリックして値を編集します。1 つ以上の領域で情報を入力または変更し、[Save] をクリックして変更を保存します。

マルチホスト展開の開始と停止 4

この章の手順を使用して、Cisco UCS Performance Manager のマルチホスト展開を開始および停止します。

Cisco UCS Performance Manager の起動

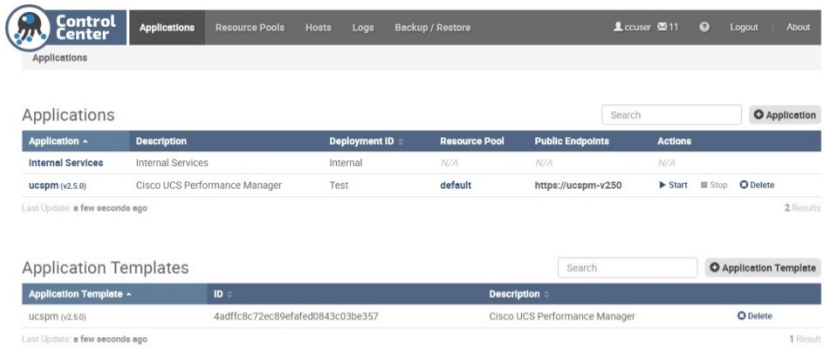
この手順を実行するには、以下が必要です。

- Cisco UCS Performance Manager のゲスト システムをホストするハイパーバイザ サーバへの管理アクセス
- サポートされているクライアント システムとブラウザ
- コントロール センターのブラウザ インターフェイスへのアクセス権を持つコントロール センターのマスター ホストでのユーザ アカウント

詳細については、『*Cisco UCS Performance Manager Installation Guide*』を参照してください。

1. Cisco UCS Performance Manager のゲスト システムをホストするハイパーバイザ サーバにログインします。
2. 各 Cisco UCS Performance Manager のゲスト システムを可能な限り同じ時間で起動します。
3. コントロール センター ブラウザ インターフェイスにログインします。

   ブラウザ インターフェイスをサポートする Web サーバは、起動するのに 1 ～ 2 分かかります。



4. [Applications] テーブルの [Actions] 列で、[ucspm] の [Start] をクリックします。
5. [Start Service] ダイアログで、[Start Service and 33 Children] をクリックします。
6. オプション：必要に応じて、起動を監視します。
   - **a** [Applications] テーブルで、[ucspm] をクリックします。
   - **b** [Services] テーブルまでスクロールし、各サービスの [Health] アイコンを確認します。

     サービスが開始されると、[Health] アイコンがチェック マークに変わります。

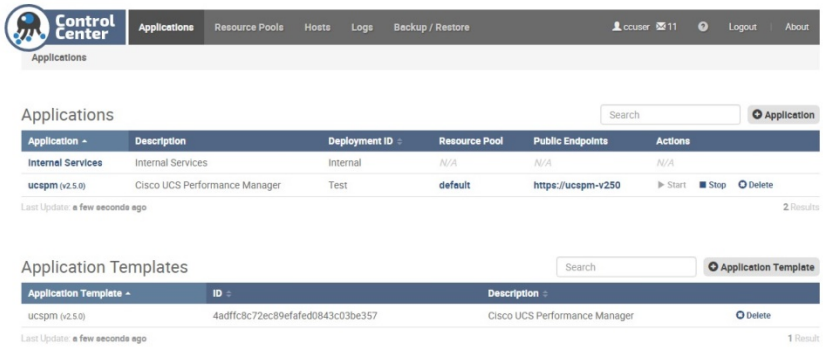
Cisco UCS Performance Manager の停止

この手順を実行するには、以下が必要です。

- Cisco UCS Performance Manager のゲスト システムをホストするハイパーバイザ サーバへの管理アクセス
- サポートされているクライアント システムとブラウザ
- コントロール センターのブラウザ インターフェイスへのアクセス権を持つコントロール センターのマスター ホストでのユーザ アカウント

詳細については、『*Cisco UCS Performance Manager Installation Guide*』を参照してください。

1 コントロール センター ブラウザ インターフェイスにログインします。



2 [Applications] テーブルの [Actions] 列で、[ucspm] の [Stop] をクリックします。

3 [Stop Service] ダイアログで、[Stop Service and 33 Children] をクリックします。

4 オプション：必要に応じて、停止を監視します。

a [Applications] テーブルで、[ucspm] をクリックします。

b [Services] テーブルまでスクロールし、各サービスの [Status] メッセージを確認します。

サービスが停止すると、[Status] メッセージが [Stopped] に変わります。

5 Cisco UCS Performance Manager のゲスト システムをホストするハイパーバイザ サーバにログインします。

6 各 Cisco UCS Performance Manager のゲスト システムを停止します。

デフォルトのサーバ パスワード 5

Cisco UCS Performance Manager は、すべてのサービスのランタイム環境（Docker コンテナ）にグローバル設定パラメータを追加します。パラメータには、2 つの MariaDB データベース サーバ、RabbitMQ サーバ、Zope 認証サーバのデフォルト パスワードが含まれています。デフォルト パスワードは、すべての Cisco UCS Performance Manager のディストリビューションで同じです。セキュリティ上の問題を避けるために、上記のサーバのデフォルト パスワードを変更することを推奨します。

（注） グローバル設定パラメータの変更は、アップグレード全体にわたって維持されます。

次のリストに、影響を受けるサーバ、それらの Cisco UCS Performance Manager サービス、およびそれらのアカウント情報の関連付けを示します。

（注） リストには、アカウント名とパスワードの両方が含まれています。各アカウントのパスワードを変更することを推奨します。アカウント名の変更は絶対に避けてください。

イベント データベースの MariaDB サーバ

サービス：**mariadb-events**

管理者アカウント：`global.conf.zep-admin-user`

管理者パスワード：`global.conf.zep-admin-password`

ユーザ アカウント：`global.conf.zep-user`

ユーザ パスワード：`global.conf.zep-password`

モデル データベースの MariaDB サーバ

サービス：**mariadb-model**

管理者アカウント：`global.conf.zodb-admin-user`

管理者パスワード：`global.conf.zodb-admin-password`

ユーザ アカウント：`global.conf.zodb-user`

ユーザ パスワード：`global.conf.zodb-password`

RabbitMQ サーバ

サービス：**RabbitMQ**

ユーザ アカウント：`global.conf.amqpuser`

ユーザ パスワード：`global.conf.amqppassword`

Zope 認証サーバ

サービス：**Zauth**

ユーザ アカウント：`global.conf.zauth-username`

ユーザ パスワード：`global.conf.zauth-password`

MariaDB パスワードの変更

イベント データおよびモデル データ用の MariaDB データベースのパスワードを変更するには、次の手順を使用します。

この手順を実行するには、Cisco UCS Performance Manager の **mariadb-events** および **mariadb-model** 子サービスが実行されている必要があります。

1 イベント データベース サーバのパスワードを変更します。

   a **mariadb-events** サービスの Docker コンテナに `zenoss` としてログインします。

```
serviced service attach mariadb-events su - zenoss
```

   b インタラクティブなセッションを開始します。

```
export TERM=dumb; mysql -u root
```

   c 管理データベースにアクセスします。

```
USE mysql
```

   d `root` ユーザのパスワードを設定します。
   New-Password を新しいパスワードに置き換えます。

```
SET PASSWORD FOR 'root'@'127.0.0.1' = PASSWORD('New-Password');
SET PASSWORD FOR 'root'@'localhost' = PASSWORD('New-Password');
```

   以降の手順で使用するために、パスワードを記録します。

   e `zenoss` ユーザのパスワードを更新します。
   New-Password を新しいパスワードに置き換えます。

```
SET PASSWORD FOR 'zenoss'@'127.0.0.1' = PASSWORD('New-Password');
SET PASSWORD FOR 'zenoss'@'%' = PASSWORD('New-Password');
```

   以降の手順で使用するために、パスワードを記録します。

   f インタラクティブなセッションを終了します。

```
QUIT
```

   MariaDB サーバは、`SET PASSWORD` のようなアカウント管理ステートメントが使用されると即座に付与テーブルをメモリにロードするので、`FLUSH PRIVILEGES` ステートメントは必要ありません。

   g Docker コンテナからログアウトします。

```
exit
```

2 モデル データベース サーバのパスワードを変更します。

   a **mariadb-model** サービスの Docker コンテナに `zenoss` としてログインします。

```
serviced service attach mariadb-model su - zenoss
```

   b インタラクティブなセッションを開始します。

```
export TERM=dumb; mysql -u root
```

c 管理データベースにアクセスします。

```
USE mysql
```

d `root` ユーザのパスワードを設定します。
New-Password を新しいパスワードに置き換えます。

```
SET PASSWORD FOR 'root'@'127.0.0.1' = PASSWORD('New-Password');
SET PASSWORD FOR 'root'@'localhost' = PASSWORD('New-Password');
```

以降の手順で使用するために、パスワードを記録します。

e `zenoss` ユーザのパスワードを更新します。
New-Password を新しいパスワードに置き換えます。

```
SET PASSWORD FOR 'zenoss'@'127.0.0.1' = PASSWORD('New-Password');
SET PASSWORD FOR 'zenoss'@'%' = PASSWORD('New-Password');
```

以降の手順で使用するために、パスワードを記録します。

f インタラクティブなセッションを終了します。

```
QUIT
```

g Docker コンテナからログアウトします。

```
exit
```

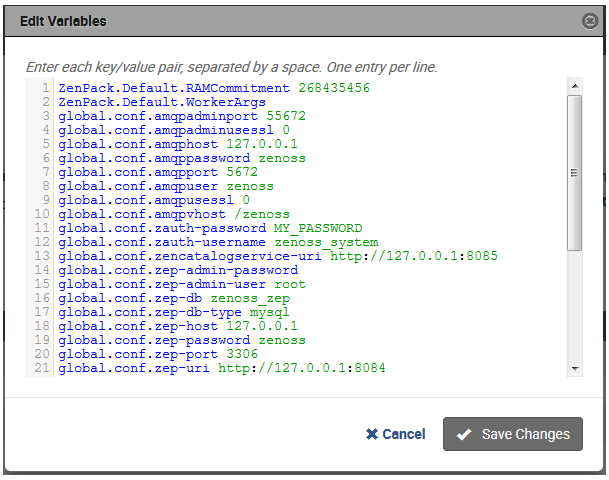
3 コントロール センター ブラウザ インターフェイスにログインします。

4 [Applications] テーブルで、[ucspm] をクリックします。

5 アプリケーション タイトル行で、[Edit Variables] をクリックします。

最初、アプリケーション タイトル行は、ページ上部のコントロール センターのバナーのすぐ下に表示されます。ページを下にスクロールすると、アプリケーション タイトル行はページの上部に表示され続けます。

図 2: [Edit Variables] ダイアログ



6 イベント データベース サーバのパスワードを更新します。

a [Edit Variables] ダイアログで、`global.conf.zep-password` 変数を検索します。

b その値を、イベント データベース サーバの `zenoss` ユーザに対して以前に指定したパスワードに置き換えます。

c `global.conf.zep-admin-password` 変数を検索します。

d その値を、イベント データベース サーバの `root` ユーザに対して以前に指定したパスワードに置き換えます。

7 モデル データベース サーバのパスワードを更新します。
   a `global.conf.zodb-password` 変数を検索します。
   b その値を、モデル データベース サーバの `zenoss` ユーザに対して以前に指定したパスワードに置き換えます。
   c `global.conf.zodb-admin-password` 変数を検索します。
   d その値を、モデル データベース サーバの `root` ユーザに対して以前に指定したパスワードに置き換えます。
   e [Edit Variables] ダイアログの下部で、[Save Changes] をクリックします。
8 アプリケーション タイトル行で、[Restart] をクリックします。

RabbitMQ サーバ パスワードの変更

RabbitMQ サーバのパスワードを変更するには、次の手順を実行します。

この手順を実行するには、Cisco UCS Performance Manager の **mariadb-model** 子サービスが実行されている必要があります。

1 `zenoss` ユーザのパスワードを変更します。
   a **RabbitMQ** サービスの Docker コンテナに `root` としてログインします。

```
serviced service attach rabbitmq
```

   b パスワードを変更します。
   New-Password を新しいパスワードに置き換えます。

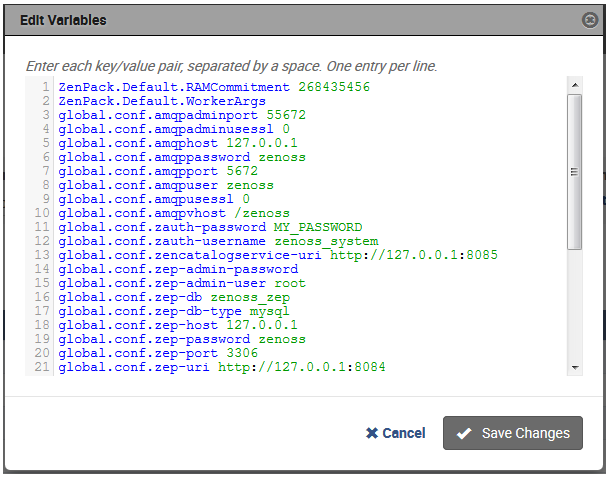
```
rabbitmqctl change password zenoss New-Password
```

   以降の手順で使用するために、パスワードを記録します。
   c Docker コンテナからログアウトします。

```
exit
```

2 コントロール センター ブラウザ インターフェイスにログインします。
3 [Applications] テーブルで、[ucspm] をクリックします。
4 アプリケーション タイトル行で、[Edit Variables] をクリックします。
   最初、アプリケーション タイトル行は、ページ上部のコントロール センターのバナーのすぐ下に表示されます。ページを下にスクロールすると、アプリケーション タイトル行はページの上部に表示され続けます。

図 3:[Edit Variables] ダイアログ



5 RabbitMQ サーバのパスワードを変更します。

a [Edit Variables] ダイアログで、`global.conf.amqppassword` 変数を検索します。
b その値を、以前指定した新しいパスワードに置き換えます。
c [Edit Variables] ダイアログの下部で、[Save Changes] をクリックします。

6 **RabbitMQ** サービスを再起動します。
a [Services] テーブルまでスクロール ダウンし、**RabbitMQ** サービスを検索します。
b サービスの [Actions] 列で、[Restart] コントロールをクリックします。

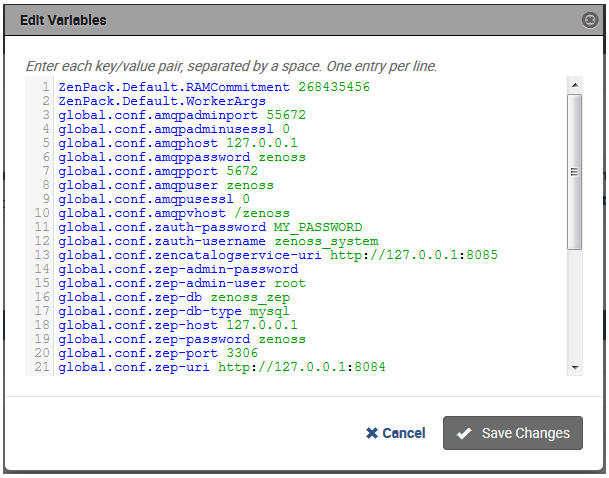
Zope 認証サーバ パスワードの変更

Zope 認証サーバのパスワードを変更するには、次の手順を実行します。

この手順を実行するには、Cisco UCS Performance Manager アプリケーションが実行されている必要があります。この手順では、Cisco UCS Performance Manager を再起動する必要があります。

1 Cisco UCS Performance Manager のブラウザ インターフェイスに `zenoss_system` としてログインします。
デフォルトのパスワードは `MY_PASSWORD` です。
2 [ADVANCED] タブをクリックし、[Settings] をクリックします。
3 左側の列から、[Users] を選択します。
4 [UserId] テーブルで、**zenoss_system** リンクをクリックします。
5 [USER SETTINGS] 領域で、[Set New Password] フィールドに新しいパスワードを入力してから、[Confirm New Password] フィールドに再度入力します。
以降の手順で使用するために、パスワードを記録します。
6 [Current Password for zenoss_system] フィールドに、`zenoss_system` としてログインするために使用したパスワードを入力します。
7 [Save Settings] をクリックしてから、ブラウザ インターフェイスからログアウトします。
8 コントロール センター ブラウザ インターフェイスにログインします。
9 [Applications] テーブルで、[ucspm] をクリックします。
10 アプリケーション タイトル行で、[Edit Variables] をクリックします。

図 4: [Edit Variables] ダイアログ



11 `zenoss_system` ユーザ アカウントのパスワードを更新します。
a [Edit Variables] ダイアログで、`global.conf.zauth-password` 変数を検索します。
この変数は、Zope 認証サーバのパスワードを設定するものです。
b その値を、`zenoss_system` ユーザ アカウントに対して以前に指定したパスワードに置き換えます。
c [Edit Variables] ダイアログの下部で、[Save Changes] をクリックします。

12 アプリケーション タイトル行で、[Restart] コントロールをクリックします。