

CシリーズおよびEシリーズサーバ用のCisco IMC Supervisorの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[UCS C シリーズ サーバ](#)

[UCS E シリーズ サーバ](#)

[ファームウェアの最低バージョン](#)

[サポートされる PCIe カード](#)

[サポートされるハイパーバイザのバージョン](#)

[背景説明](#)

[設定](#)

[Cisco IMC Supervisorの導入](#)

[デフォルトパスワードの変更](#)

[ライセンス情報](#)

[サーバの検出](#)

[ラックグループの追加](#)

[ラックアカウントの追加](#)

[メール セットアップの設定](#)

[Firmware Upgrade](#)

[テクニカルサポートデータのリモートサーバへのエクスポート](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Cisco Integrated Management Controller(IMC)Supervisor for C-Series and E-Series Serversの設定方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Cシリーズサーバ
- Cisco Eシリーズサーバ

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

Cisco IMC Supervisorは、大規模なラックマウントサーバを管理できる管理システムです。

Cisco IMC Supervisorを使用して、ラックマウントサーバに対して次のタスクを実行できます。

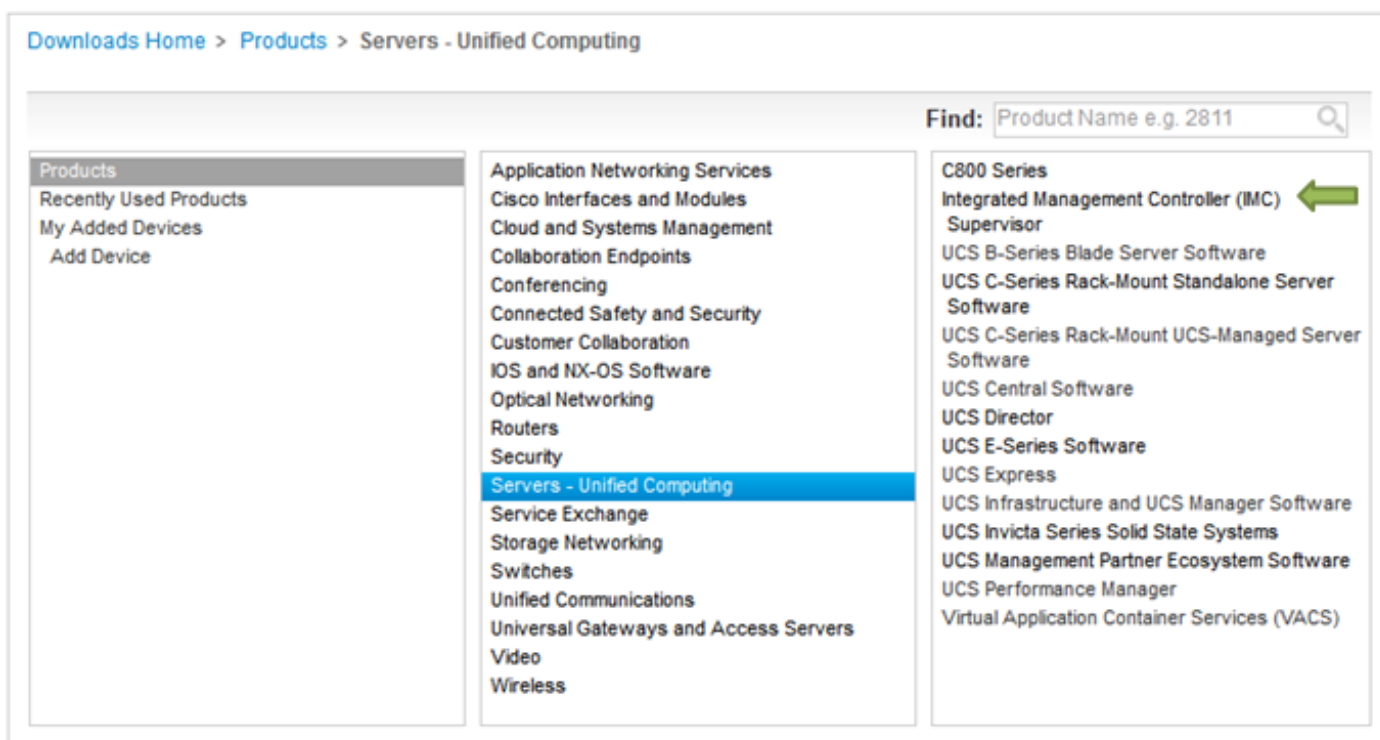
- サーバの論理グループ化およびグループごとのサマリー表示のサポート
- サーバ インベントリの収集
- サーバおよびグループのモニタリング
- ファームウェアのダウンロード、アップグレード、アクティベーションを含むファームウェア管理
- 電源制御、LED制御、ログ収集、キーボード/ビデオ/マウス(KVM)の起動、CIMCユーザインターフェイスの起動、電子メールアラートなどのスタンドアロンサーバアクションの管理
- アクセスと機能を制限するためのロールベースアクセスコントロール(RBAC)

設定

Cisco IMC Supervisorの導入

1. Cisco IMC Supervisorを導入するには、次の手順を実行します。

ステップ1: Cisco.comからCisco IMC Supervisorのzipファイルをダウンロードするには、図に示すように、[Products] > [Servers-Unified Computing] > [Integrated Management Controller (IMC Supervisor)]に移動します。



ステップ2 : 図に示すように、IMC Supervisor 1.0を選択します。

The screenshot shows a web interface for downloading software. The breadcrumb path is "Downloads Home > Products > Servers - Unified Computing > Integrated Management Controller (IMC) Supervisor". A search bar at the top right contains "Product Name e.g. 2811". On the left, a sidebar lists navigation options: "Products", "Recently Used Products", "My Added Devices", and "Add Device". The main content area is a list of products under the heading "C800 Series". The product "Integrated Management Controller (IMC) Supervisor" is highlighted in blue. To the right of this list, a larger view of the selected product "IMC Supervisor 1.0" is shown.

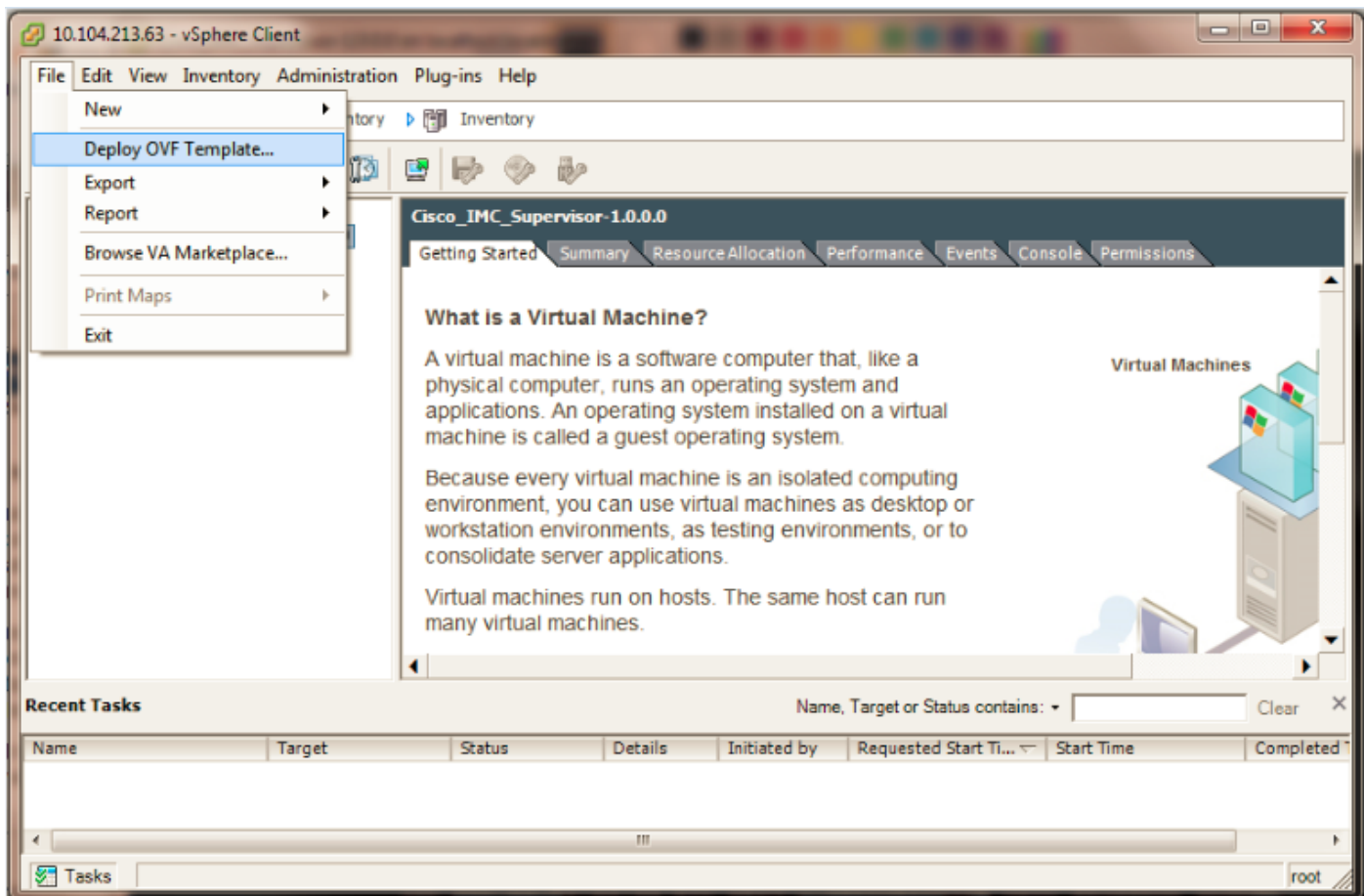
ステップ3 : 図に示すように、[Download]をクリックします。

IMC Supervisor 1.0

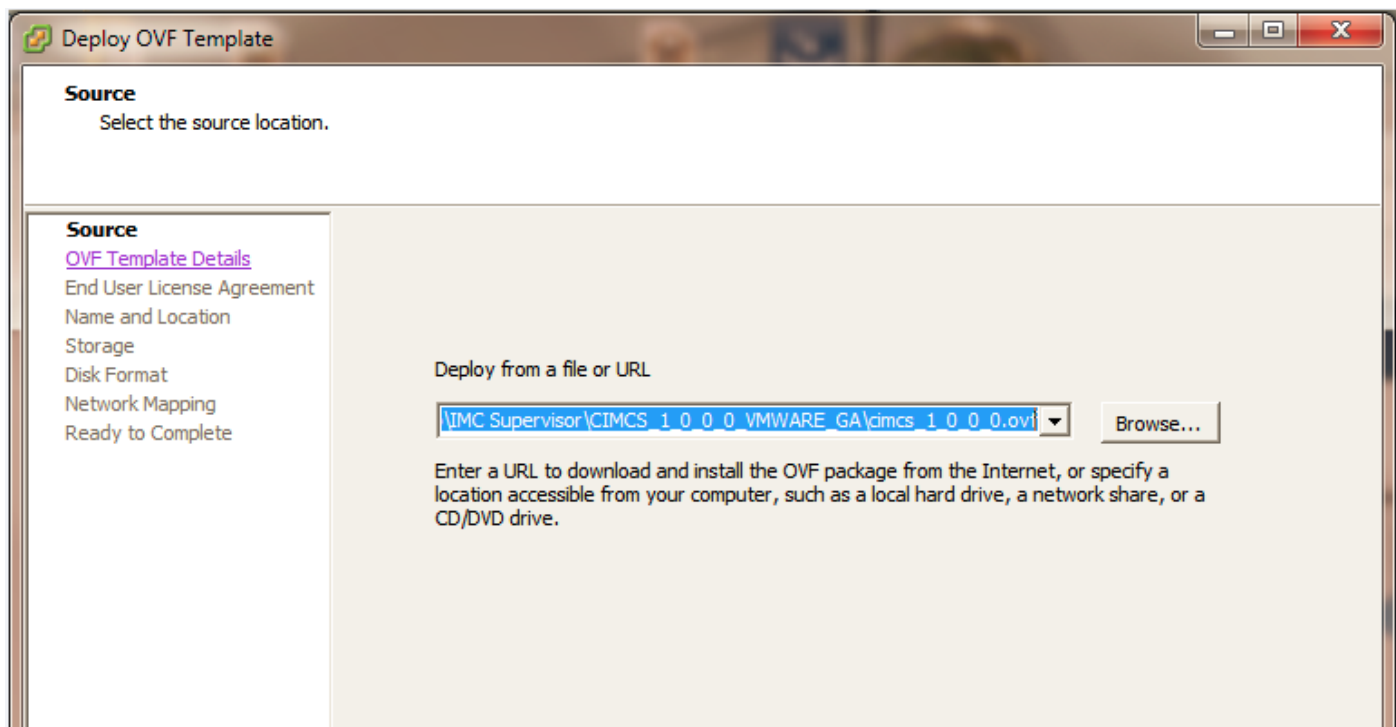
The screenshot shows the product page for "IMC Supervisor 1.0". At the top, there is a search bar and a "Release 1" section. On the right side, there are two icons: "Add Devices" and "Add Notification". Below this, there is a table with columns for "File Information", "Release Date", and "Size". The table contains one row with the following information: "Cisco Integrated Management Controller Supervisor 1.0 (MD5 Checksum - 4 a2803e35b40b63c497e8d5371ab118e)", "24-NOV-2014", and "2705.08 MB". To the right of this row, there are three buttons: "Download", "Add to cart", and "Publish". On the left side, there is a sidebar with a search bar and a list of release categories: "Latest", "All Releases", and "1".

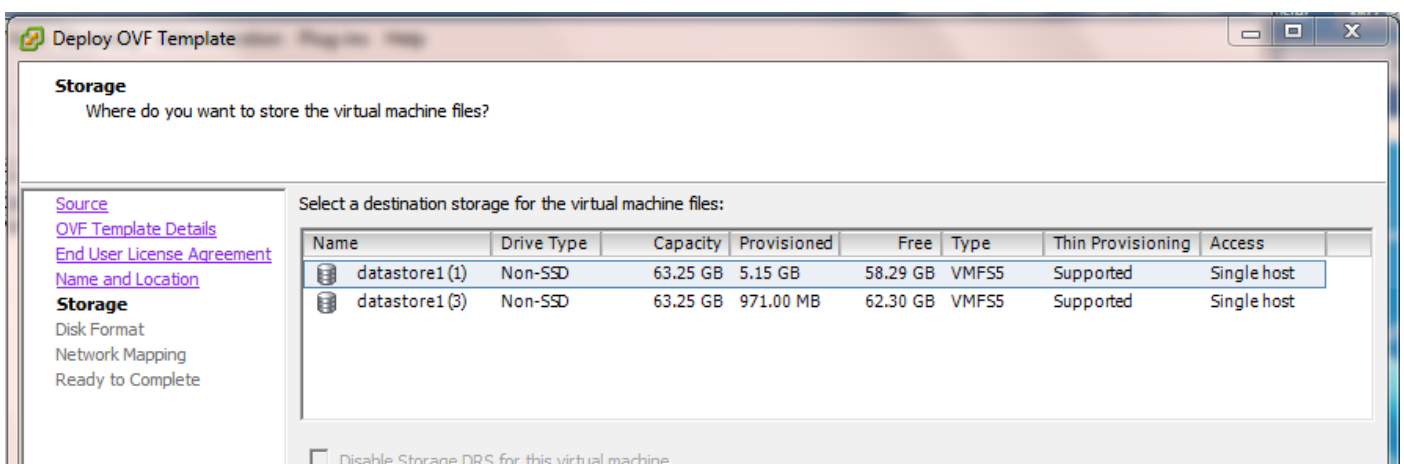
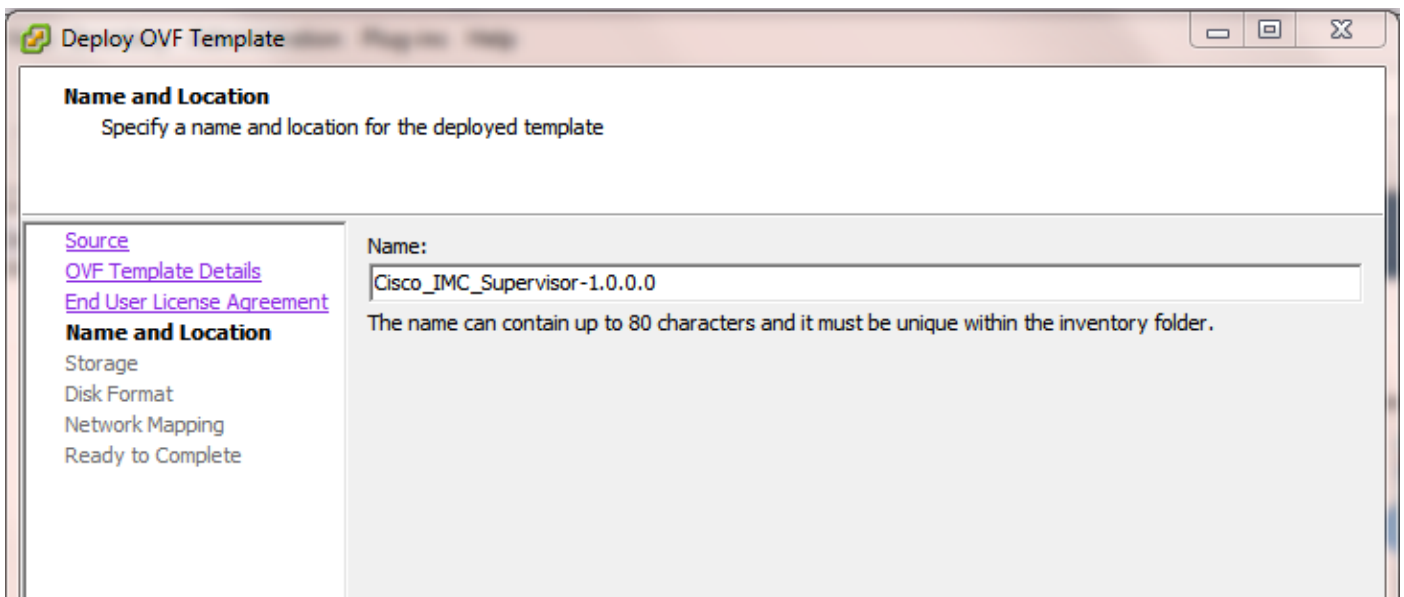
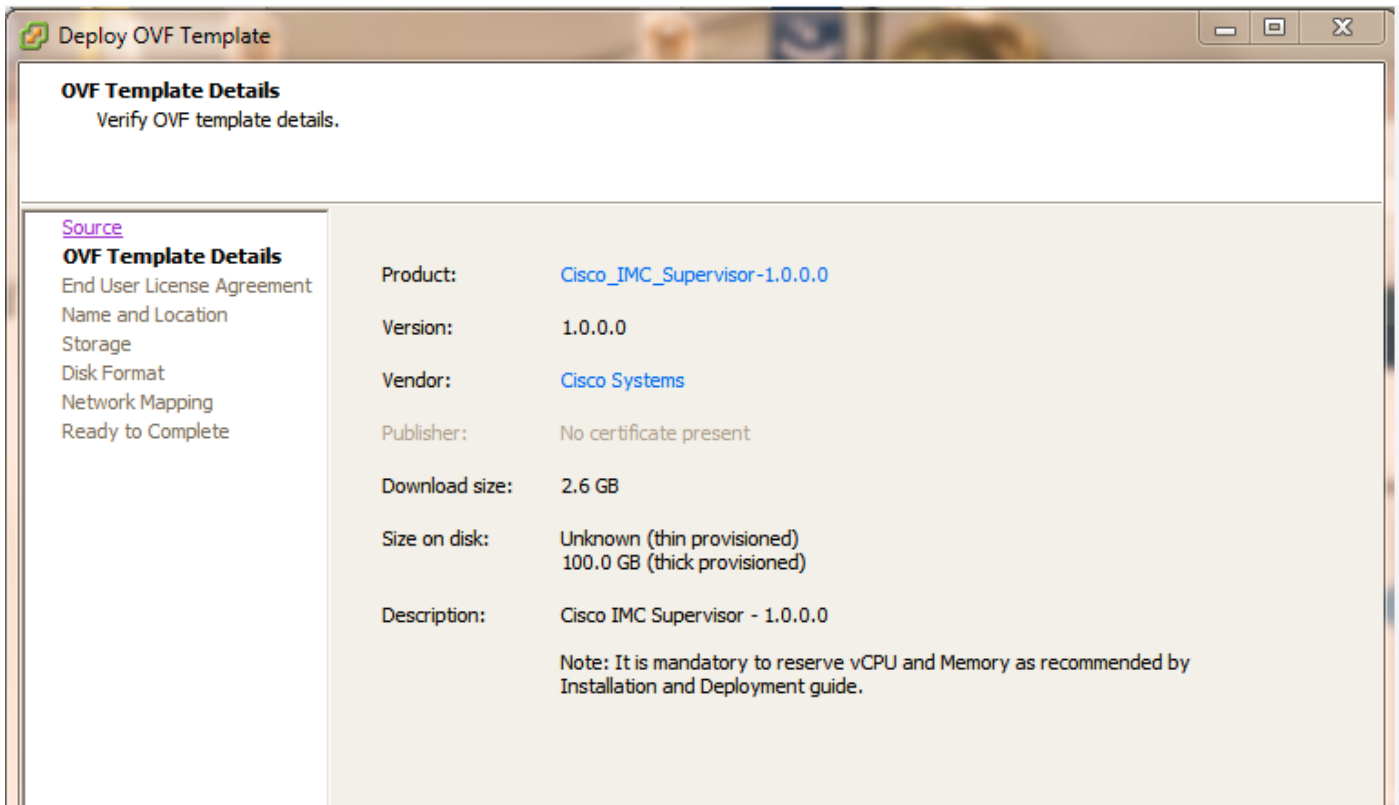
File Information	Release Date	Size
Cisco Integrated Management Controller Supervisor 1.0 (MD5 Checksum - 4 a2803e35b40b63c497e8d5371ab118e) CIMCS_1_0_0_0_VMWARE_GA.zip	24-NOV-2014	2705.08 MB

ステップ4 : 図に示すように、Open Virtual Appliance(OVA)を導入するには、[File] > [Deploy OVF Template]に移動します。



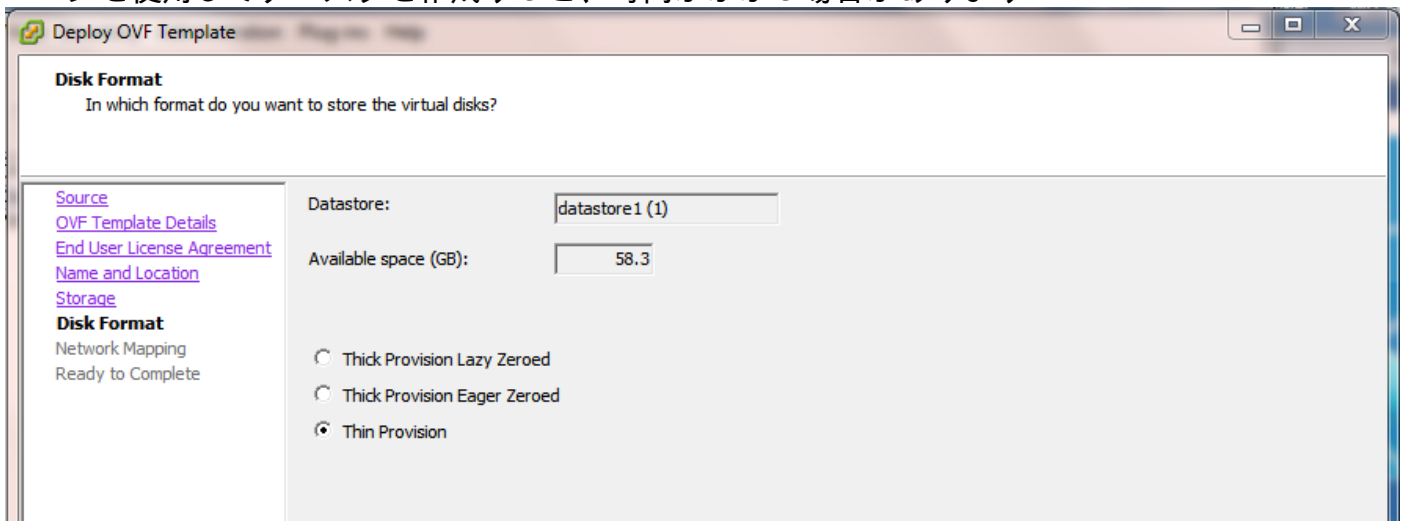
ステップ5 : 図に示すように、Open Virtualization Format(OVF)テンプレートを導入するには、ステップごとのプロセスを続行します。



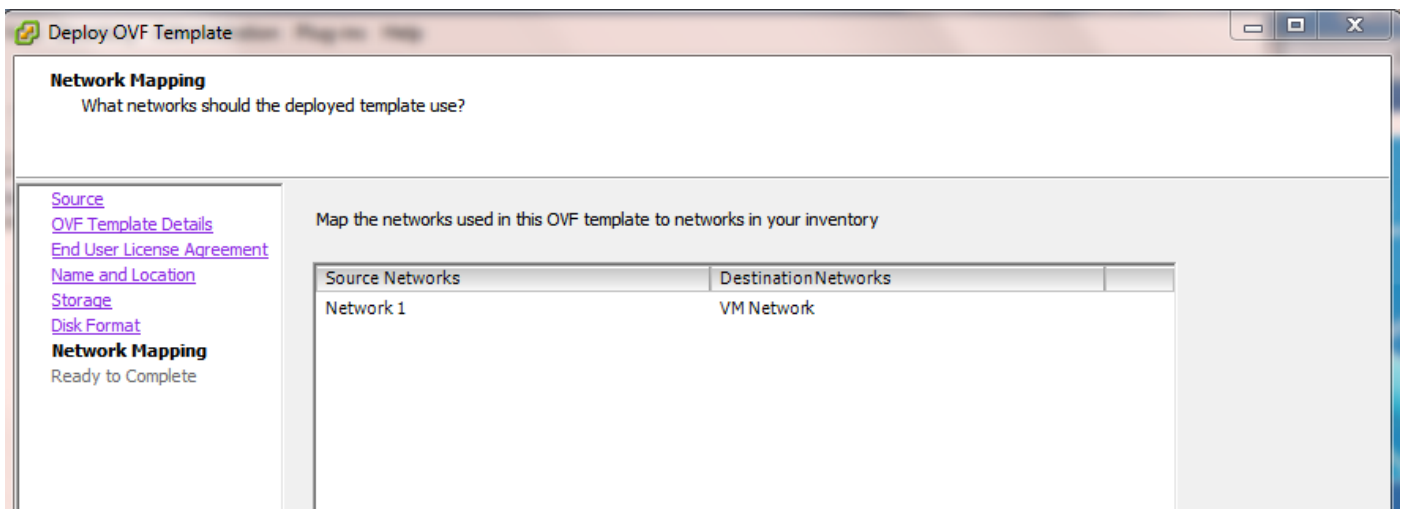


[ディスクフォーマット]ペインで、オプションボタンを1つ選択し、図に示すように[次へ]をクリックします。

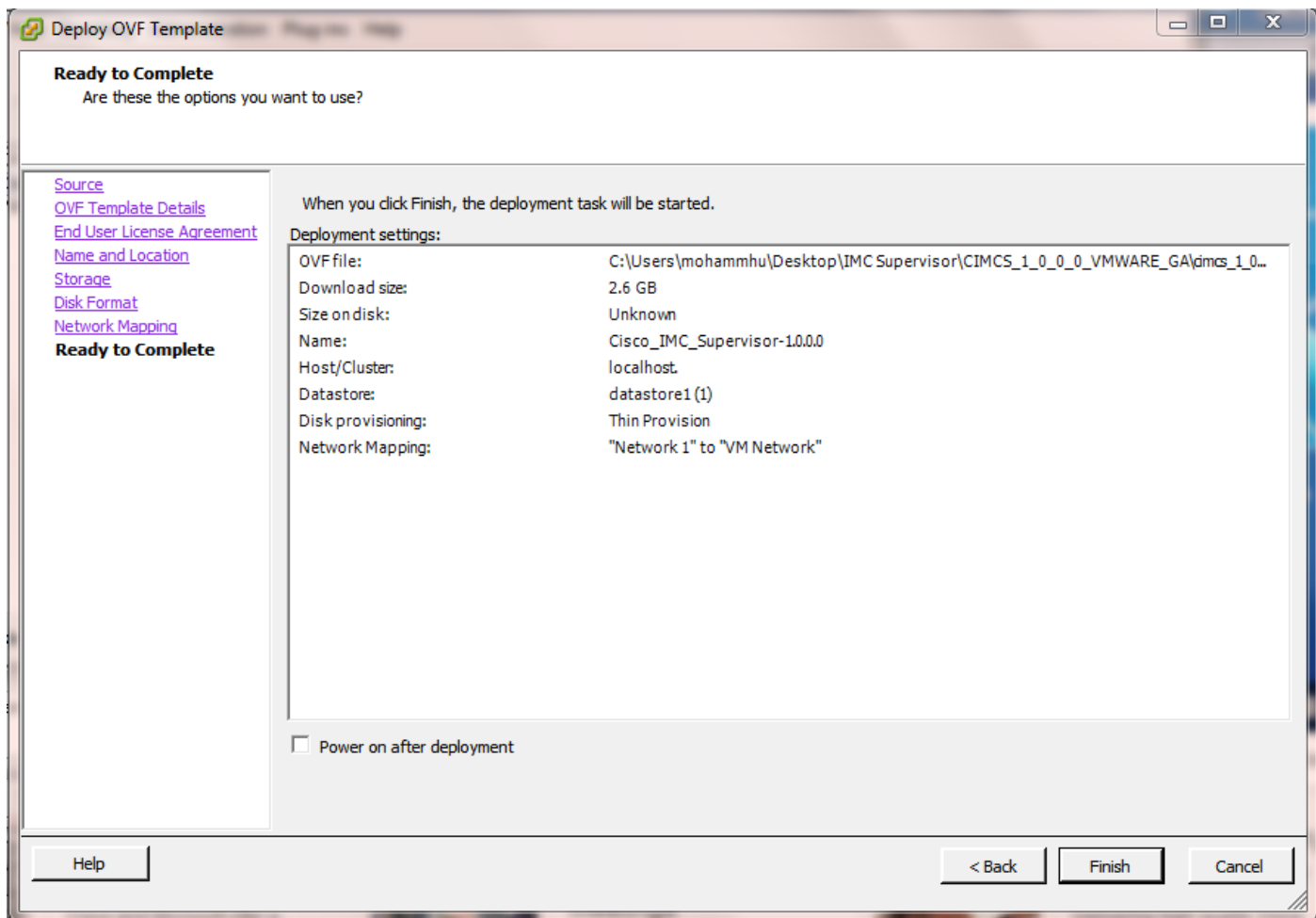
- シンプロビジョニング：データがディスクに書き込まれるときにストレージをオンデマンドで割り当てるために使用します。
- Thick Provision Lazy Zeroed：シック形式ですぐにストレージを割り当てるために使用します。
- Thick Provision Eager Zeroed：シック形式でストレージを割り当てるために。このオプションを使用してディスクを作成すると、時間がかかる場合があります



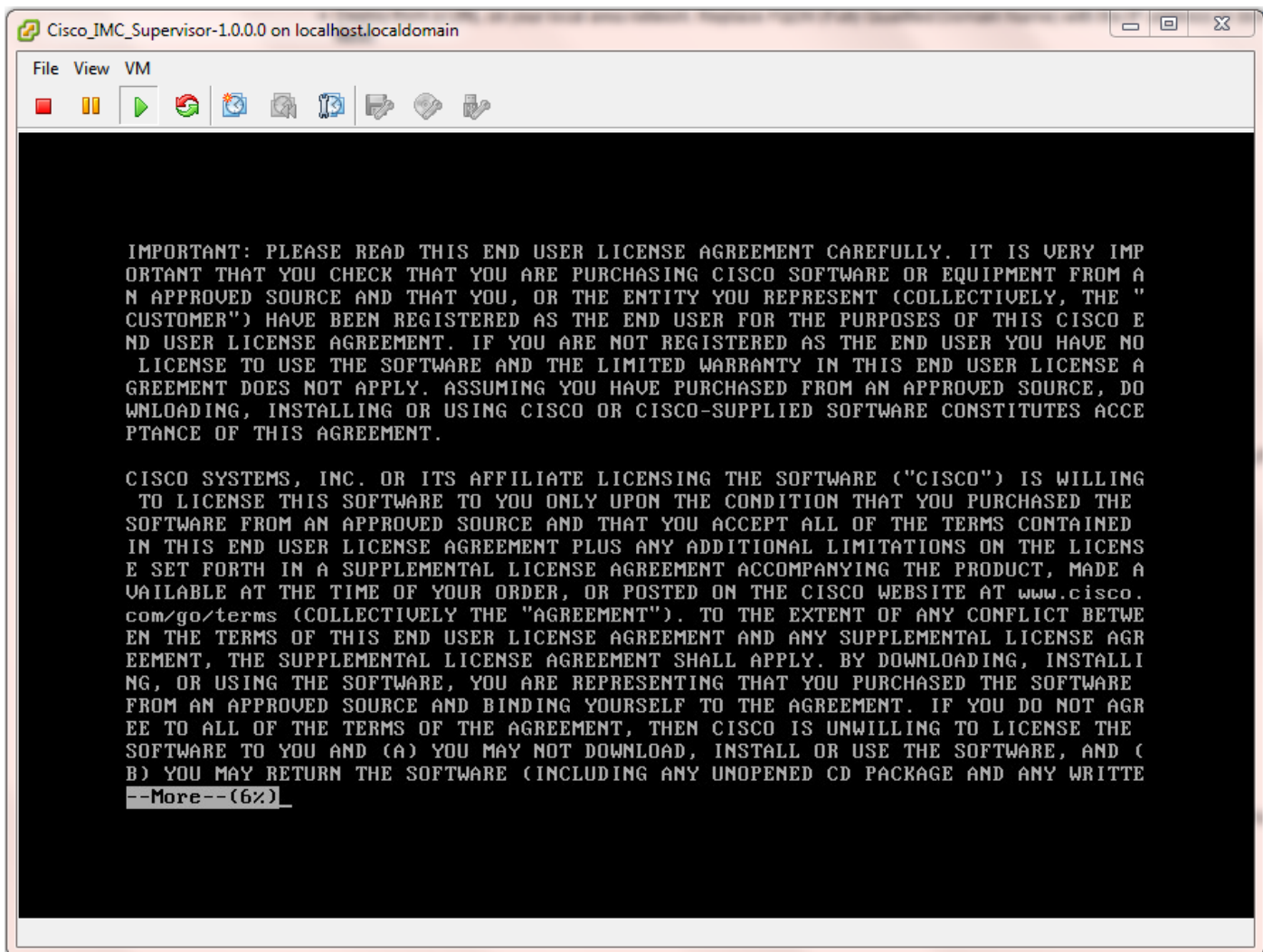
ステップ6：図に示すように、仮想マシン(VM)ネットワークに適切なポートグループを選択します。



ステップ7：図に示すように[Finish]をクリックします。



ステップ8 : 図に示すように、VMのコンソールを開き、ライセンス契約に同意します。



ステップ9: 完了したら、yと入力して、図に示すようにスタティックIPを設定します。

ステップ10:DHCPを使用する場合は、nを入力して、IPアドレスが自動的に割り当てられていることを確認します。

```
not imply a partnership relationship between Cisco and any other company.

Do you agree with the terms of the End User License Agreement?
yes/no [no]: yes

Regenerating ssh host keys...
openssh-daemon is stopped
Generating SSH1 RSA host key: [ OK ]
Generating SSH2 RSA host key: [ OK ]
Generating SSH2 DSA host key: [ OK ]
Starting sshd: [ OK ]
Regenerating keys for the root user...
Generating public/private rsa key pair.
Created directory '/root/.ssh'.
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
d7:34:b7:18:89:a2:27:3b:45:a6:96:72:97:7d:f3:de root@localhost
Generating SSL certificates for sfc in /opt/vmware/etc/sfc
Generating SSL certificates for lighttpd in /opt/vmware/etc/lighttpd
This script is executed on first boot only.
Configuring static IP configuration

Do you want to Configure static IP [y/n]? : y_
```

ステップ11：スタティックIPアドレスを使用する場合は、yと入力して、IPv4またはIPv6を選択するよう求められます。V4と入力して、図に示すように情報をを入力します。

- IP アドレスネットマスクゲートウェイ

注：現在、スタティックIPアドレスを設定するためにサポートされているのはIPv4だけです。

```
Cisco_IMC_Supervisor-1.0.0.0 on localhost.localdomain
File View VM
Regenerating keys for the root user...
Generating public/private rsa key pair.
Created directory '/root/.ssh'.
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
d7:34:b7:18:89:a2:27:3b:45:a6:96:72:97:7d:f3:de root@localhost
Generating SSL certificates for sfcbl in /opt/vmware/etc/sfcbl
Generating SSL certificates for lighttpd in /opt/vmware/etc/lighttpd
This script is executed on first boot only.
Configuring static IP configuration

Do you want to Configure static IP [y/n]? : y
Do you want to configure IPv4/IPv6 [v4/v6] ? : v4

Configuring static IP for appliance. Provide the necessary access credentials

IP Address: 10.104.213.77
Netmask: 255.255.255.0
Gateway: 10.104.213.1

Configuring Network with : IP(10.104.213.77), Netmask(255.255.255.0), Gateway(10.104.213.1)

Do you want to continue [y/n]? : y_
```

```
Cisco_IMC_Supervisor-1.0.0.0 on localhost.localdomain
File View VM
Cisco_IMC_Supervisor-1.0.0.0 - 1.0.0.0
To manage this VM browse to https://10.104.213.77:443/

*Login
Configure Network
Set Timezone (Current:UTC)

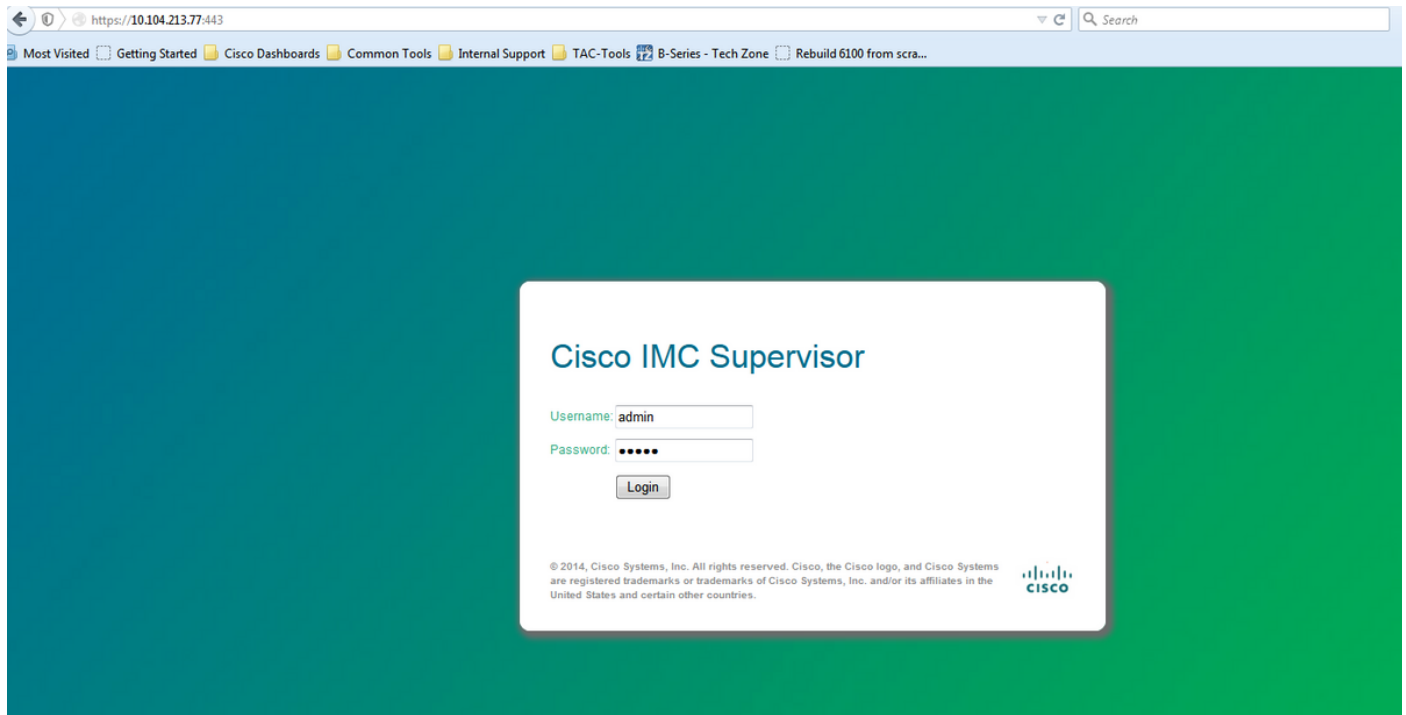
Use Arrow Keys to navigate
and <ENTER> to select your choice.
```

ステップ12 : アプライアンスが起動したら、サポートされているWebブラウザにCisco IMC Supervisor IPアドレスを転送して、ログインページにアクセスします。

[Login]ページで、[Username]にadmin、[Password]にadminを入力します。

注：この初回ログインの後、admin パスワードを変更できます。

Cisco IMC Supervisorのユーザインターフェイス(UI)を図に示します。



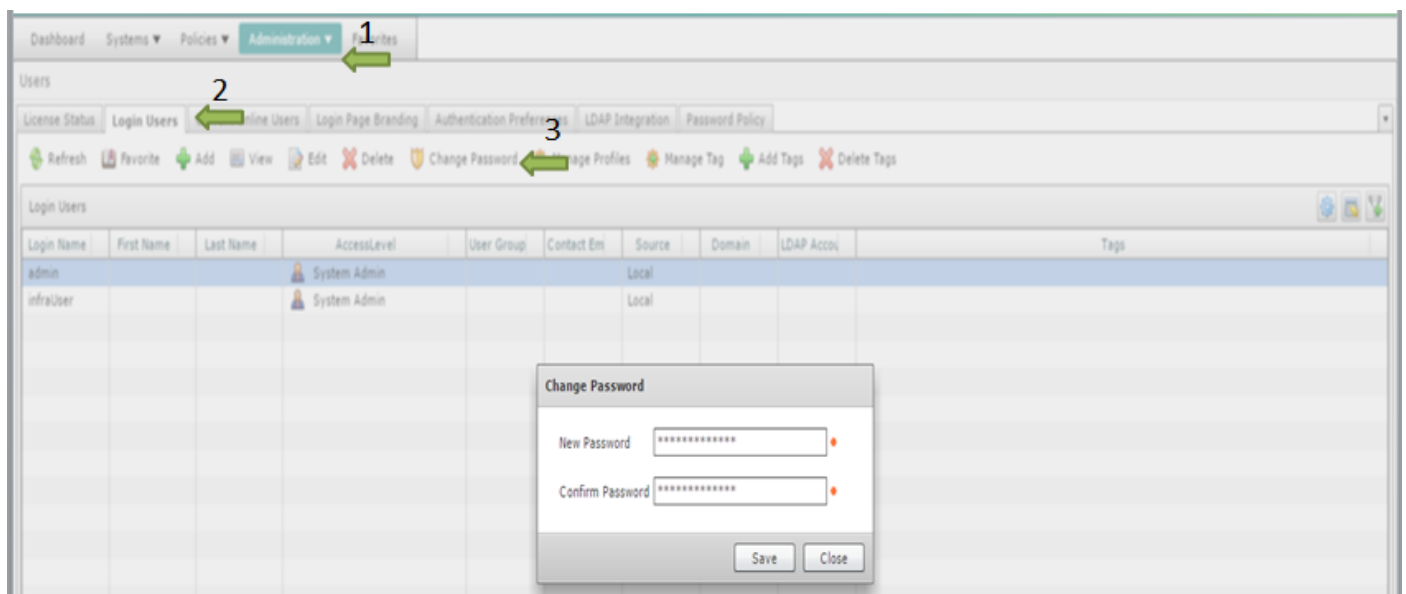
デフォルトパスワードの変更

2.デフォルトパスワードを変更するには、次の手順を実行します。

ステップ1:[Administration] > [Users]に移動します。

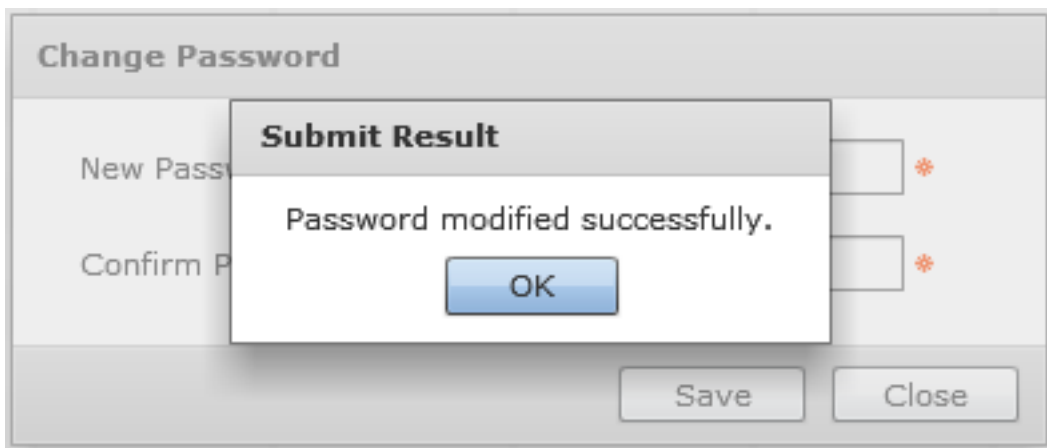
ステップ2:[Login Users]タブをクリックします。

ステップ3：ユーザのリストから、図に示すように、パスワードを変更するユーザロールを選択します。



ステップ4：新しいパスワードを指定した後、図に示すように、[Save]をクリックして、[Submit

Result]の[OK]をクリックします。



ライセンス情報

3. Cisco IMC Supervisorには、次の有効なライセンスが必要です。

- Cisco IMC Supervisor 基本ライセンス。
- 図に示すように、Cisco IMC Supervisor基本ライセンスの後にインストールするCisco IMC Supervisorバルクエンドポイント有効化ライセンス。

Dashboard Systems Policies Administration Favorites

License

License Keys License Utilization Resource Usage Data

Refresh Favorite Update License Run License Audit

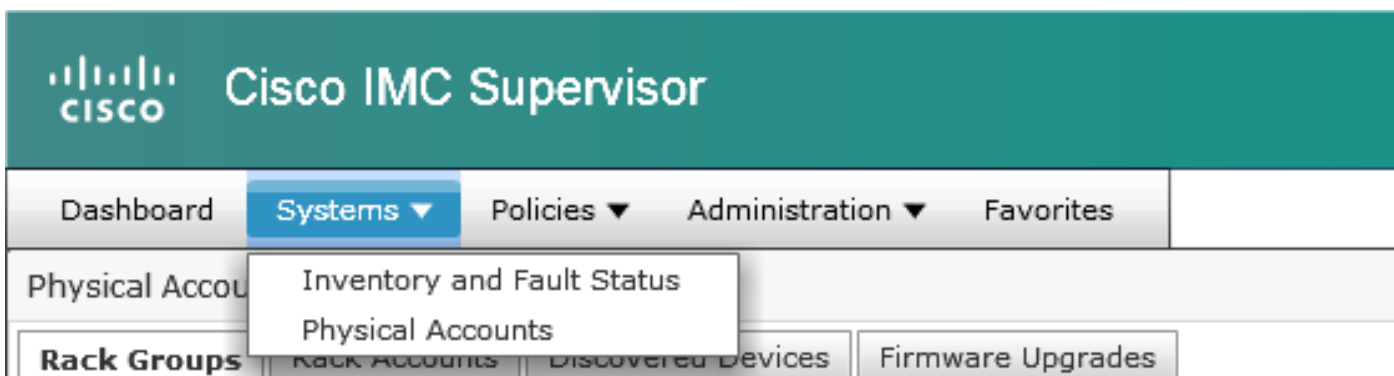
License Utilization					
License	Licensed Lim	Available	Used	Status	Remarks
CIMC SUP Base	1		1	✔ Licensed	
Physical Servers	200	200	0	✔ Licensed	Licensed Limit = CIMC-SUP-B01(=2) * 100+ CIMC-SUP-B02(=0) * 250+ CIMC-SUP-B10(=0) * 1000

注：これらのライセンスがない限り、サーバをラックアカウントにグループ化するなどのタスクは実行できません。

サーバの検出

4.サーバを検出するには、次のアクションを実行します。

ステップ1：図に示すように、[System] > [Physical Accounts] > [Discovered Devices]に移動します。



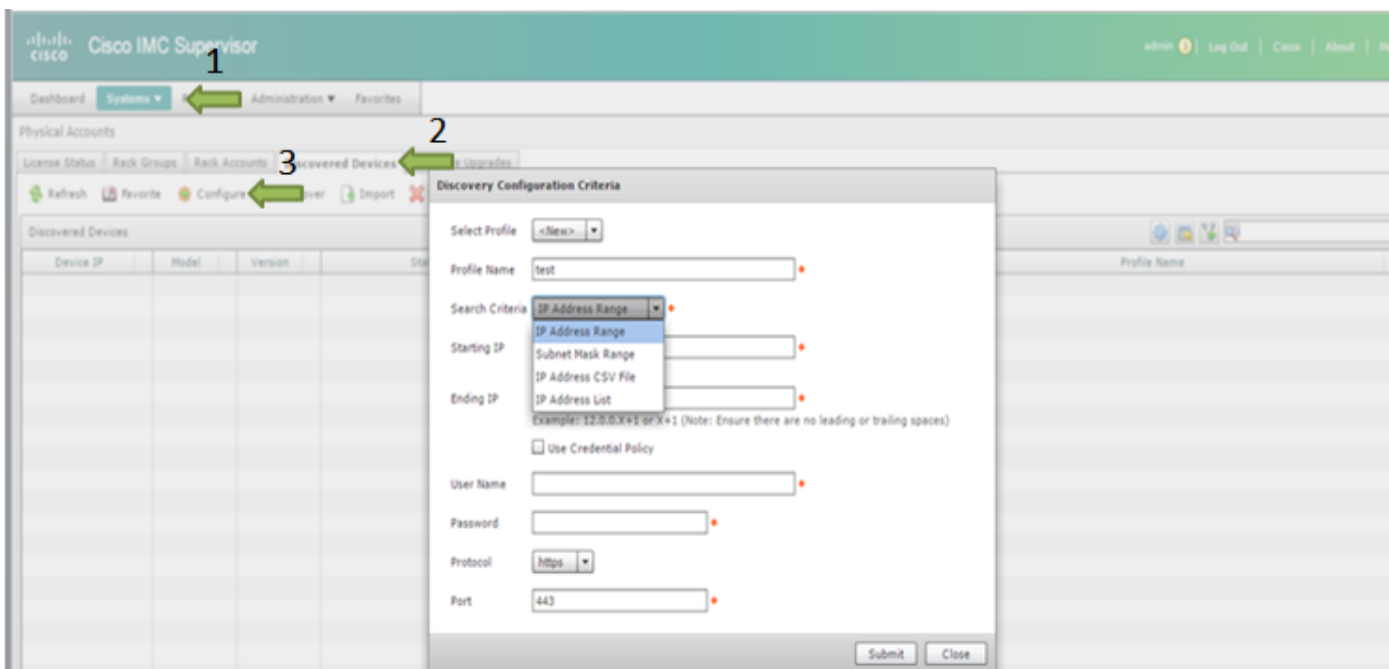
ステップ2:[Configure]をクリックします。

ステップ3:[検出構成の基準(Discovery Configuration Criteria)]ダイアログボックスで、新しいプロファイルを作成するか、既存のプロファイルを編集できます。

ステップ4：新しいプロファイルの作成を図に示します。

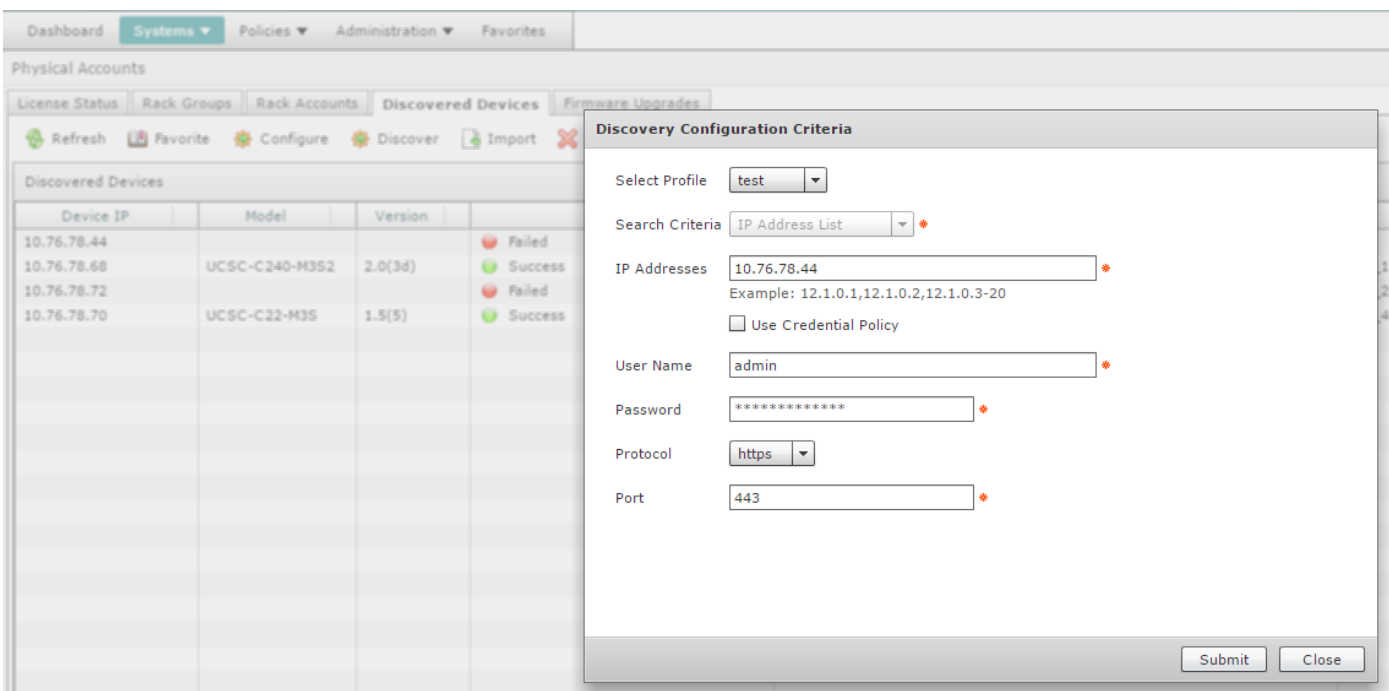
ステップ5:[Search Criteria]で、サーバを検出するための適切な方法を選択できます。

ステップ6：この例で[IP Address List]を選択します。

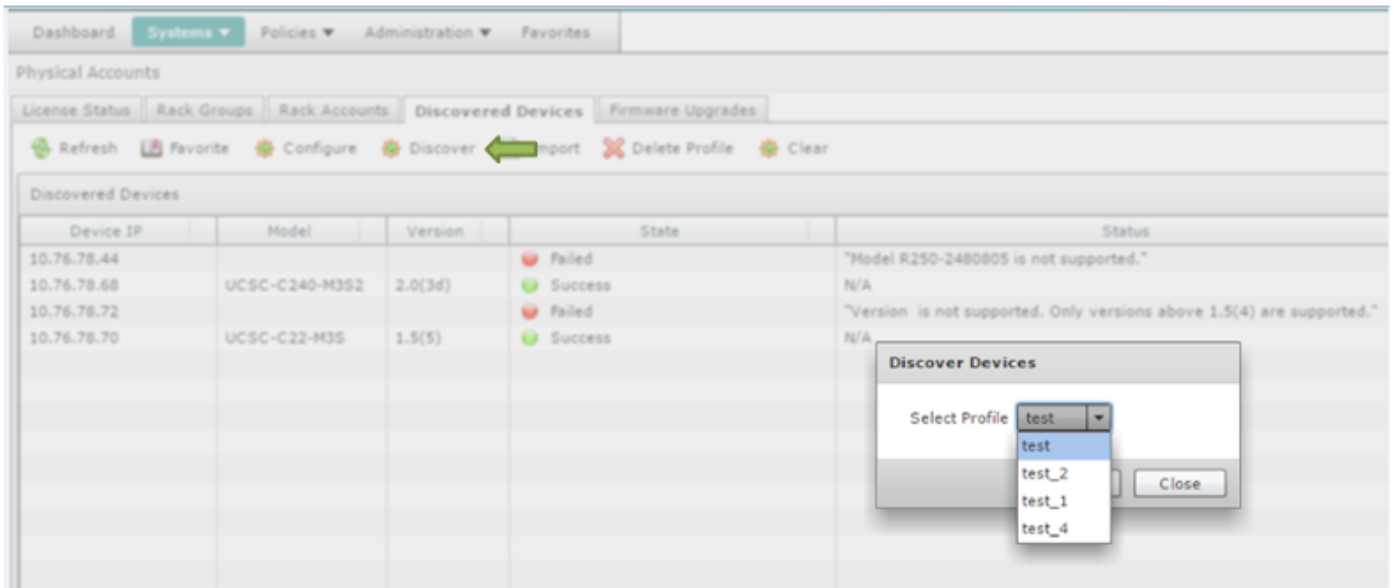


ステップ7：検出するサーバのIPアドレスを入力します。

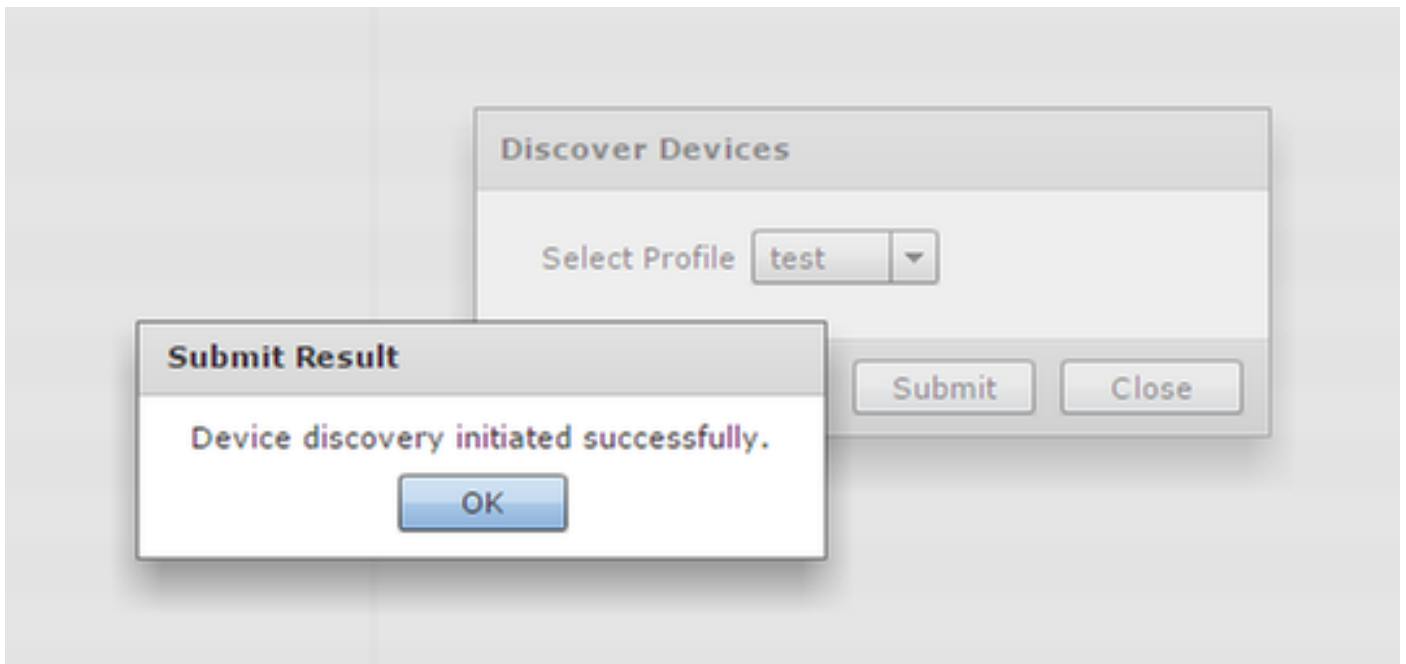
ステップ8：図に示すように、サーバへのログインに使用するユーザ名とパスワード (CIMCクレデンシャル) を入力します。



ステップ9 : プロファイルが作成されたら、図に示すように、ドロップダウンリストから [Discover and Select Profile] をクリックします。



ステップ10 : 適切なプロファイルを選択した後、[送信(Submit)]をクリックし、図に示す[結果の送信(Submit Result)]で[OK]をクリックします。



ステップ11 : プロファイル内のデバイスがサポートされている最小条件と一致しない場合、デバイスが検出されない理由は、図に示すように [Status] セクションに示されます。

Device IP	Model	Version	State	Status	
10.76.78.44			Failed	"Model R250-2480805 is not supported."	test
10.76.78.68	UCSC-C240-M352	2.0(3d)	Success	N/A	test_1
10.76.78.72			Failed	"Version is not supported. Only versions above 1.5(4) are supported."	test_2
10.76.78.70	UCSC-C22-M35	1.5(5)	Success	N/A	test_4

ラックグループの追加

5. Cisco IMC Supervisorに新しいラックグループを追加する場合は、この手順を実行します。

ステップ1:[システム(Systems)] > [物理アカウント(Physical Accounts)] > [ラックグループ(Rack Groups)]に移動します。

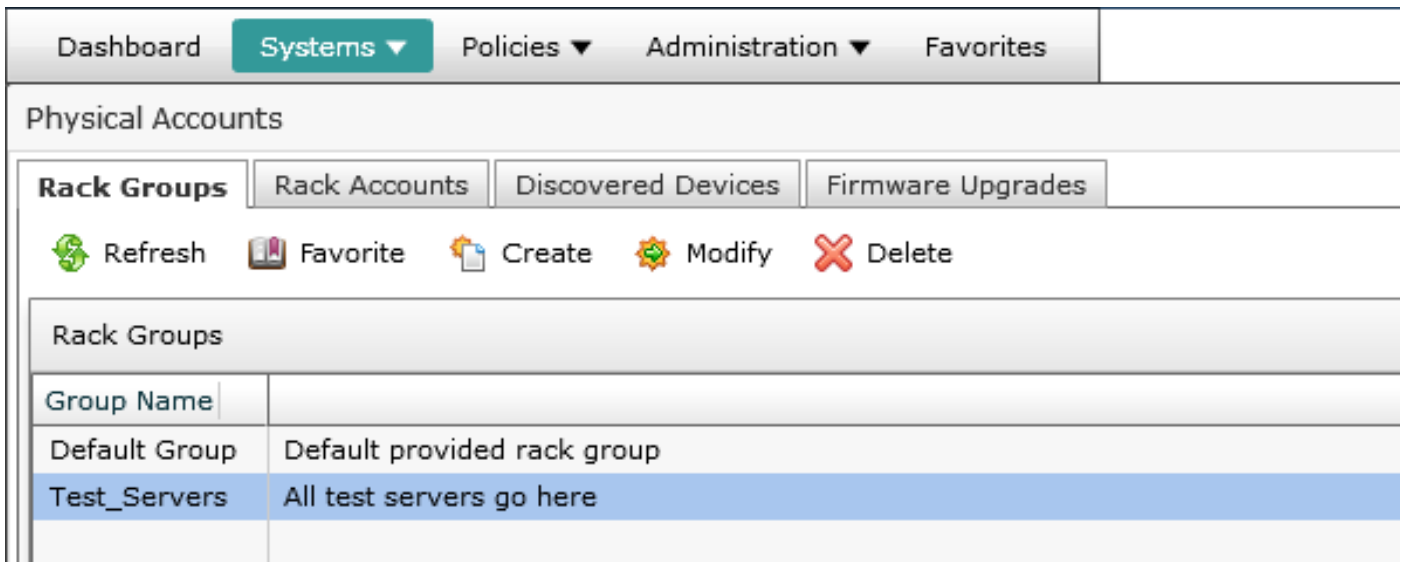
ステップ2:[Create]をクリックします。

ステップ3:[Create Rack Group]ボックスでグループ名と説明を指定します。

ステップ4 : 図に示すように[Create]をクリックします。

Group Name	Description
Default Group	Default provided rack group

ステップ5 : グループ名を作成したら、図に示すようにグループ名が表示されます。



ラックアカウントの追加

6. Cisco IMC Supervisorに新しいラックグループを追加する場合は、この手順を実行します。

ステップ1: メニューバーから[システム]を選択します。

1:

ステップ2: タブをクリックします。

手順3: をクリックします。

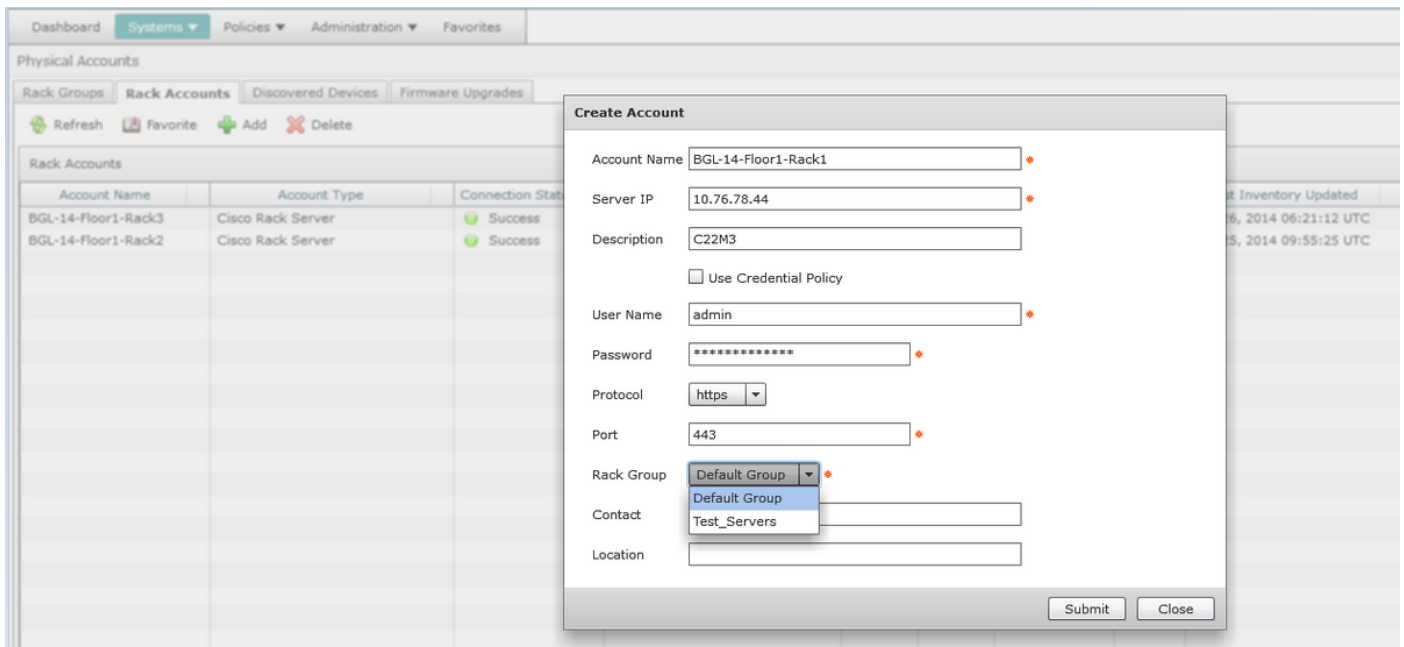
ステップ4: [アカウントの作成]ダイアログボックスで、次のフィールドに値を入力します。

4:

フィールド	説明
フィールド	ラックアカウントのわかりやすい名前
フィールド	ラックマウントサーバのIPアドレス
[Description] フィールド	(オプション) ラックアカウントの説明
ド	
チェックボックス	(オプション) クレデンシャルポリシーをすでに作成している場合、このチェックボックスをオンにすると、
ドロップダウンリスト	ドロップダウンリストからポリシーを選択します
チェックボックス	オフにした場合
フィールド	ラックマウントサーバのログインID
[Password] フィールド	ラックマウントサーバのログインIDのパスワード
ド	
[Protocol] ドロップダウンリスト	リストから[https]または[http]を選択します
[Port] フィールド	選択したプロトコルに関連付けられているポート番号
[Rack Group] ドロップダウンリスト	リストからラックグループを選択します。
[Contact] フィールド	(オプション) アカウントの連絡先電子メールアドレス
[Location] フィールド	(オプション) アカウントの場所

ステップ1:[Rack Group]のドロップダウンリストで、図に示すように[Default Group]または以前に定義したグループを選択できます。

ステップ2: この操作が完了したら、指定したサーバが選択したラックグループに属する必要があります。



メール セットアップの設定

7. セットアップメールを設定するには、次の手順を実行します。

ステップ1: [Administration] > [Mail Setup] に移動します。

ステップ2: 要求された詳細を入力します。

ステップ3: 図に示すように、[Send Test Email] チェックボックスをオンにし、指定した電子メールアドレスでテストメールを受信したかどうかを確認できます。



System

[System Information](#)**Mail Setup**[System Tasks](#)[User Roles](#)[Email Alert Rules](#)

Outgoing Email Server (SMTP)



Outgoing SMTP Port



Outgoing SMTP User

Outgoing SMTP Password

Outgoing Email Sender Email Address



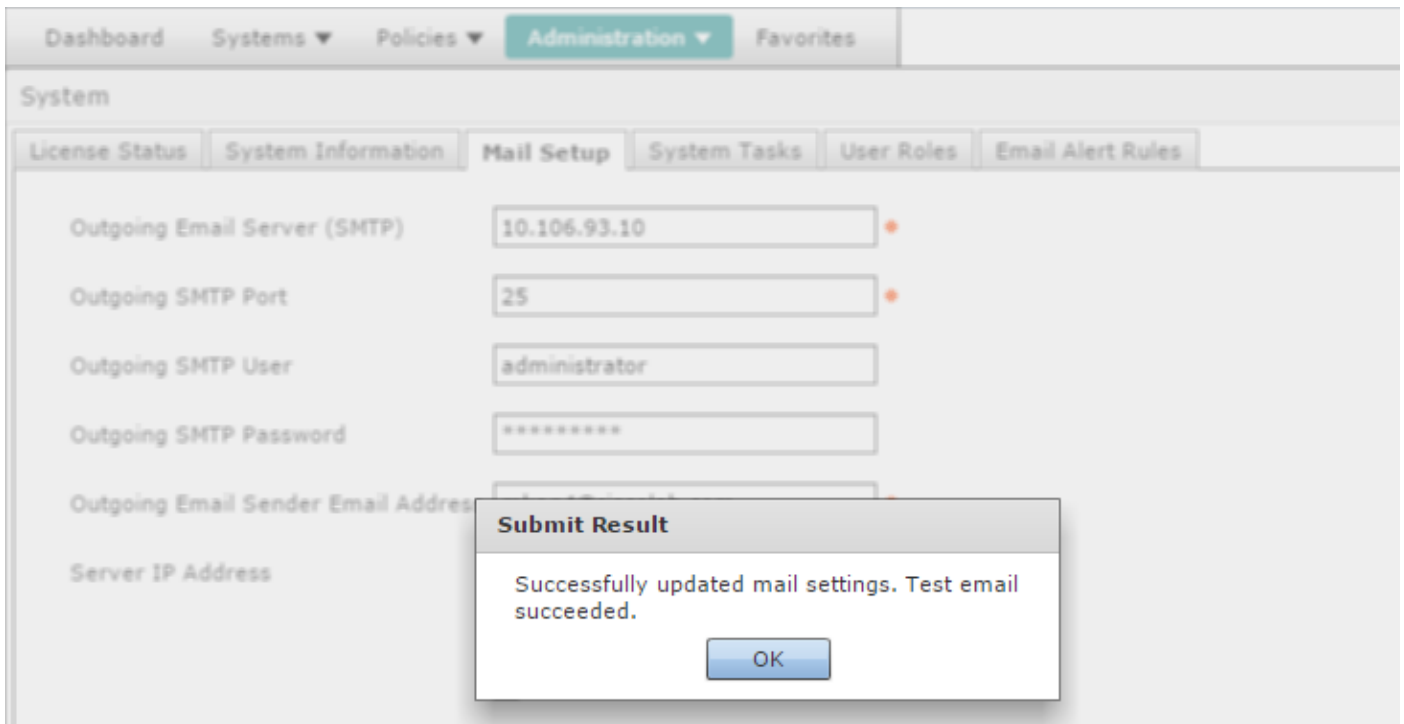
Server IP Address

 Send Test Email

Test Email Address

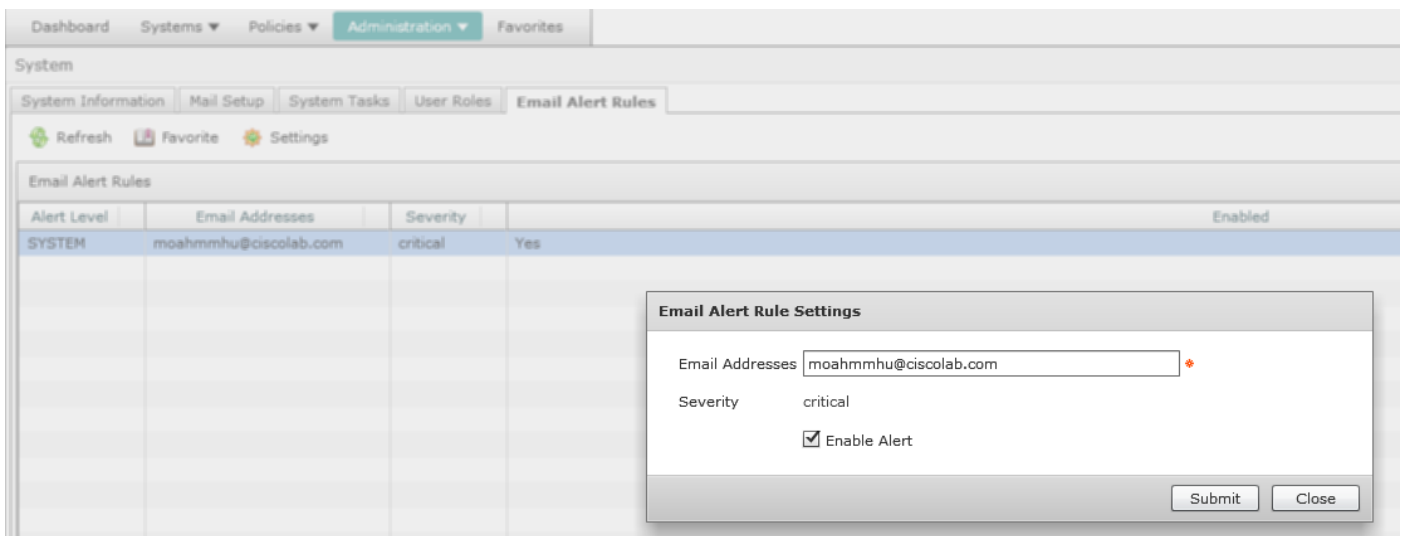


ステップ4 : 図に示すように、テストメールを受信する必要があります。



ステップ5：同じセクションで、[Email Alert Rules Settings]に移動し、図に示すように[Enable Alert]チェックボックスをオンにします。

注：現時点（Cisco IMC Supervisorリリース1.0を含む）では、重大レベル以上の障害に関する通知のみがサポートされています。



ステップ6：システムで重大な障害が発生した場合、メールの設定が正常に動作していれば、図に示すようにメールを受信する必要があります。

Server IP	Host name	Severity	Code	Cause	Description	Created	Affected DN
10.76.78.70	bgl-sv-c22-m3-01	critical	F1007	equipment-inoperable	Storage Virtual Drive 0 is inoperable: Check storage controller, or reseal the storage drive	Thu Dec 25 12:10:19 2014	sys/rack-unit-1/board /storage-SAS-SLOT-2/vd-0

Firmware Upgrade

8.ファームウェアをアップグレードする場合は、この手順を実行します。

ステップ1:[システム(Systems)] > [物理アカウント(Physical Accounts)]に移動します。

ステップ2 : タブをクリックします。

ステップ3:[Configure Profile]をクリックします。

ステップ4:[Download Firmware]ダイアログボックスで、新しいプロファイルを作成するか、既存のプロファイルを編集できます。

フィールド

説明

フィールド

ドロップダウンリストから[新規]を選択します。

ドロップダウンリスト

プロファイルの記述名。

次のオプションのいずれかを選択します。

- ローカルHTTPサーバ : .isoイメージはローカルのCisco IMCサーバーバイザに保存されます。

- ネットワークパス : .isoイメージはネットワークに保存されます。

フィールド

シスコのログイン ユーザ名を入力します。

フィールド

シスコのログイン パスワードを入力します。

チェックボックス

(オプション) このチェックボックスをオンにして、プロキシ設定効にし、次のフィールドに入力します。

- [Host Name]フィールド : プロキシ設定のホスト名を入力します。

- [Port]フィールド : プロキシ設定のポートを入力します。

[Enable Proxy Authentication] チェックボックス

(オプション) プロキシ認証を有効にするには、このチェックボックスをオンにし、次のフィールドに入力します。

- [Proxy User Name]フィールド : プロキシ認証のプロキシユーザ名を入力します。

- [Proxy Password]フィールド : プロキシユーザ名のパスワードを入力します。

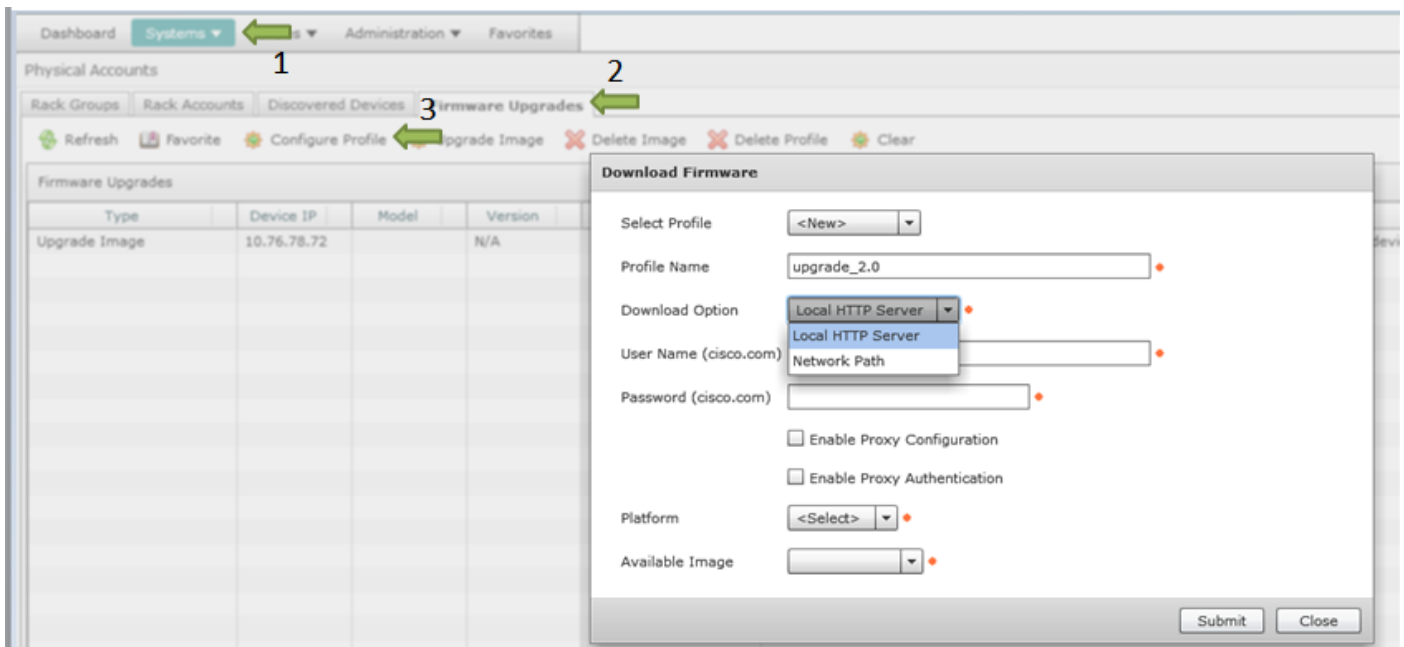
[Platform] ドロップダウンリスト

ドロップダウン リストからプラットフォームを選択します。

ドロップダウンリスト

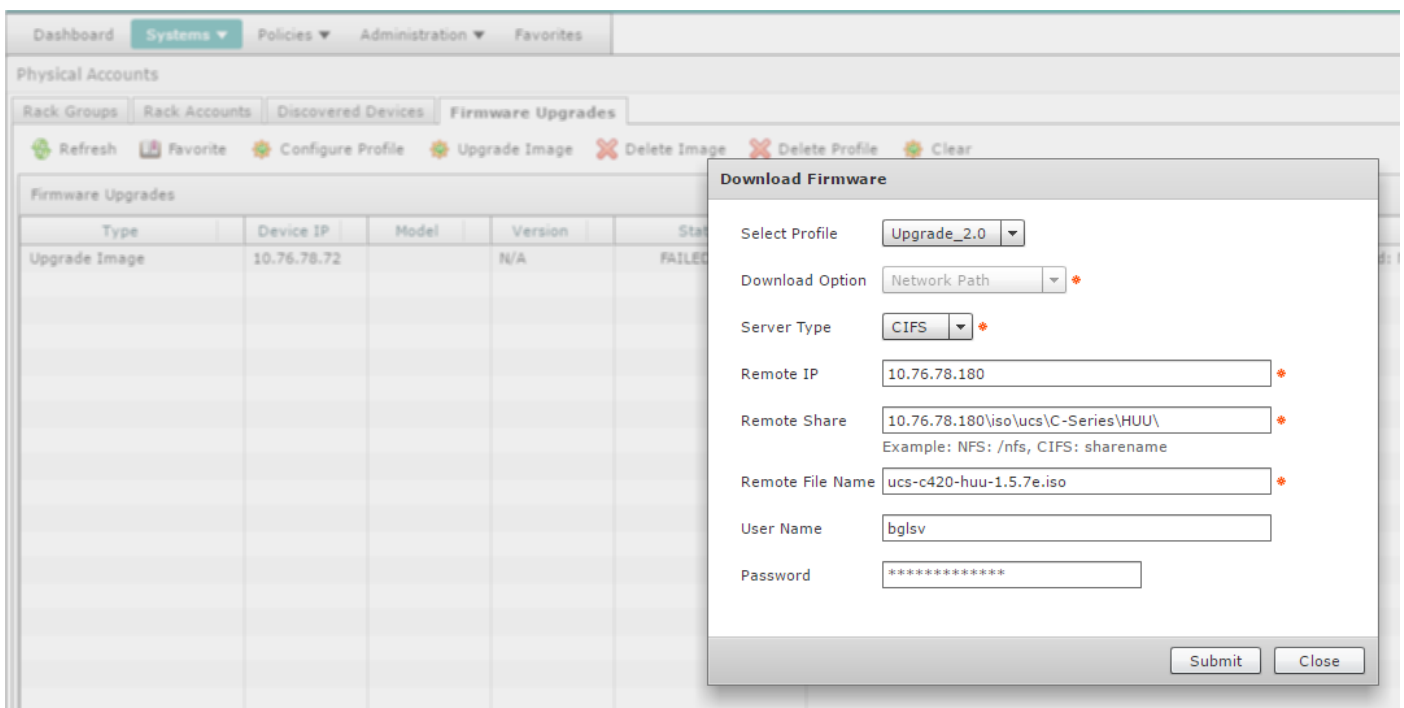
ドロップダウン リストから .iso イメージを選択します。

ステップ5 : 図に示すようにNewプロファイルを設定します。



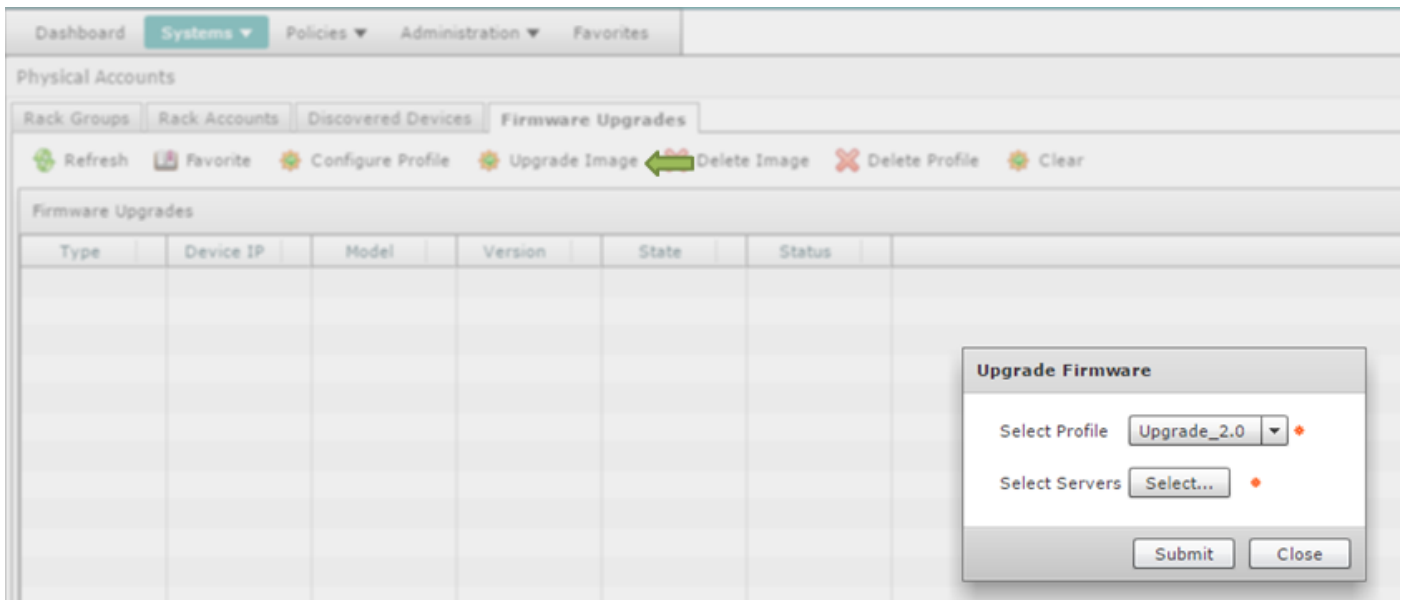
ステップ6：この例のダウンロードオプションとして[Network Path]を選択します。（オプションとしてCIFSとNFSがあります。）

ステップ7：図に示すように、[Submit]をクリックします。



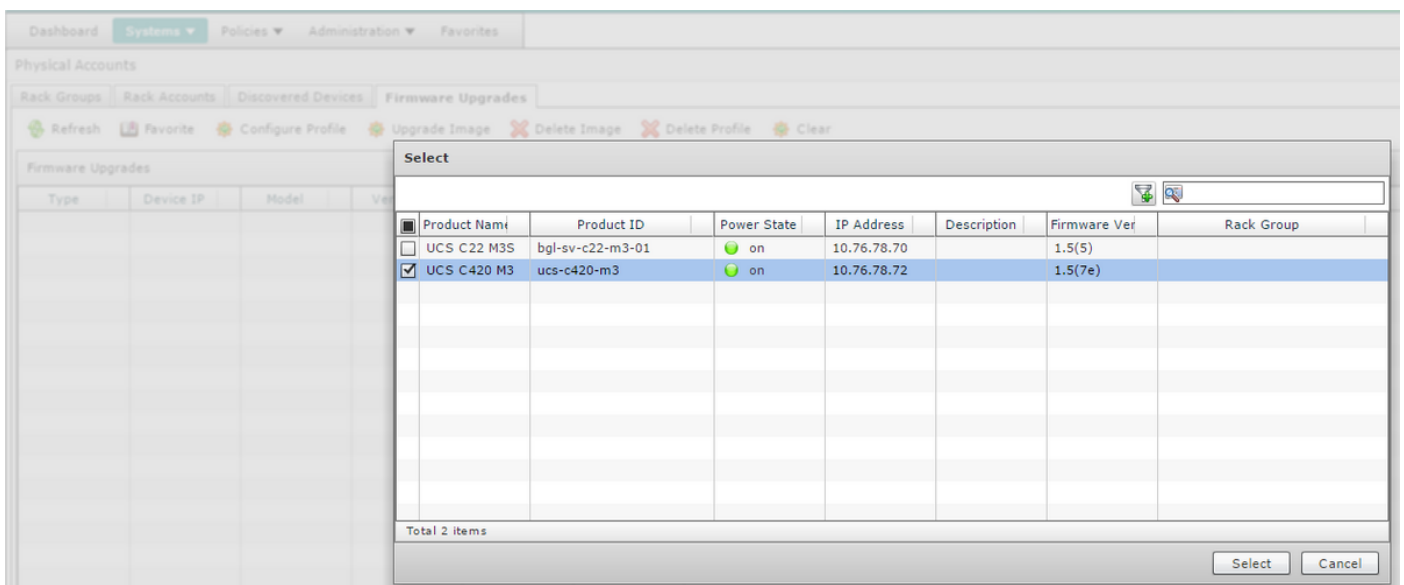
ステップ8:[Upgrade Image]をクリックします。

ステップ9:[Select...]をクリックします。図に示すように、アップグレードするサーバを選択します。



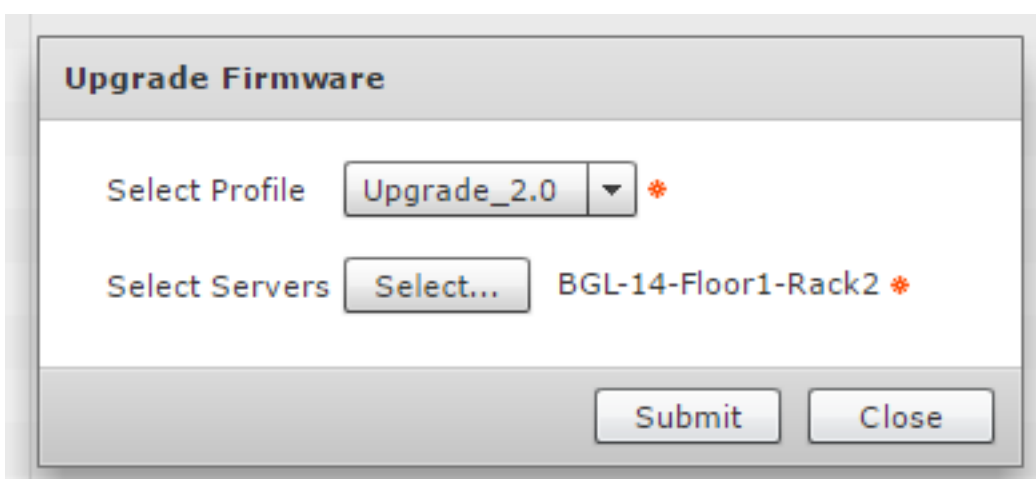
ステップ10：この例では、単一のサーバが選択されます。

ステップ11：図に示すように、[Select]をクリックします。



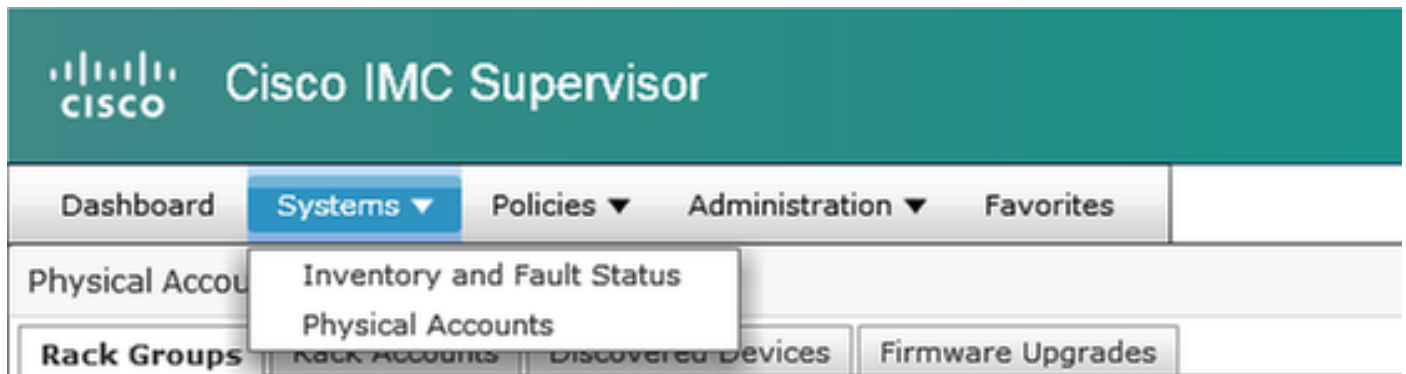
ステップ12：選択したサーバが表示されます。

ステップ13：図に示すように、[Submit]をクリックします。



注：Cisco IMCバージョン2.0(x)をアップグレードする場合は、デフォルトのCisco IMCパスワードを変更する必要があります。

ステップ14：アップグレードのステータスを確認するには、図に示すように、[System] > [Inventory and Fault Status]に移動します。

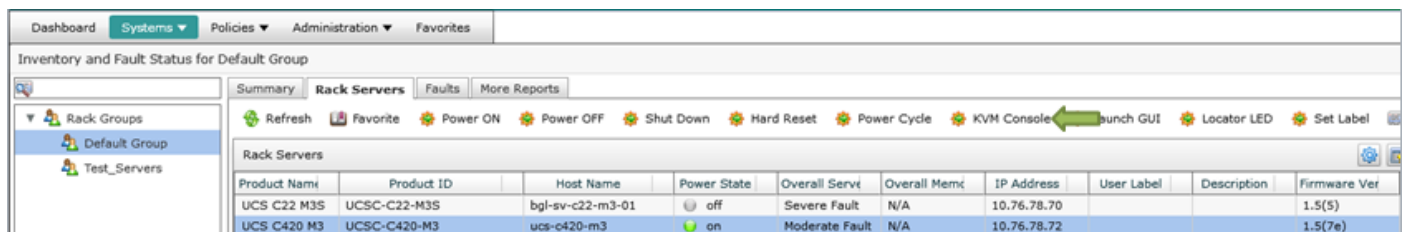


ステップ15:[Rack Groups]を展開し、サーバが以前に入力された適切なグループを選択します。

ステップ16:[ラックサーバ]をクリックし、適切なサーバを選択します。

ステップ17：これが完了したら、リモートオプションを含む追加の行がポップアップ表示されません。

ステップ18：この行から[KVM Console]をクリックすると、図に示すようにアップグレードのアクションが表示されます。



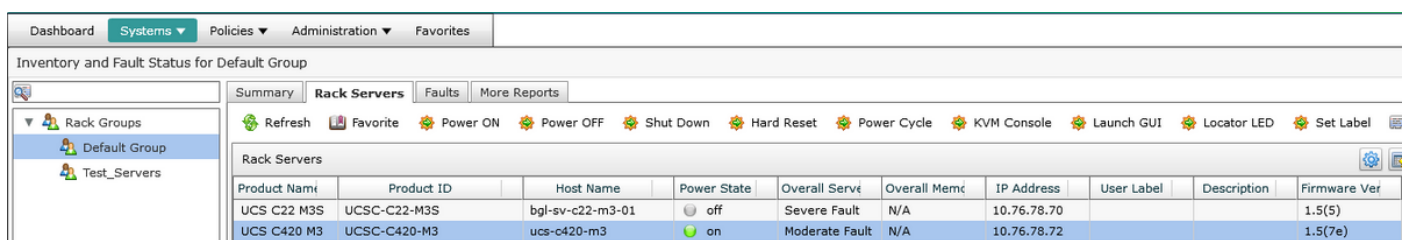
テクニカルサポートデータのリモートサーバへのエクスポート

9.テクニカルサポートデータを抽出するには、次のアクションを実行します。

ステップ1:[Systems] > [Inventory and Fault Status for Default Group]に移動します。

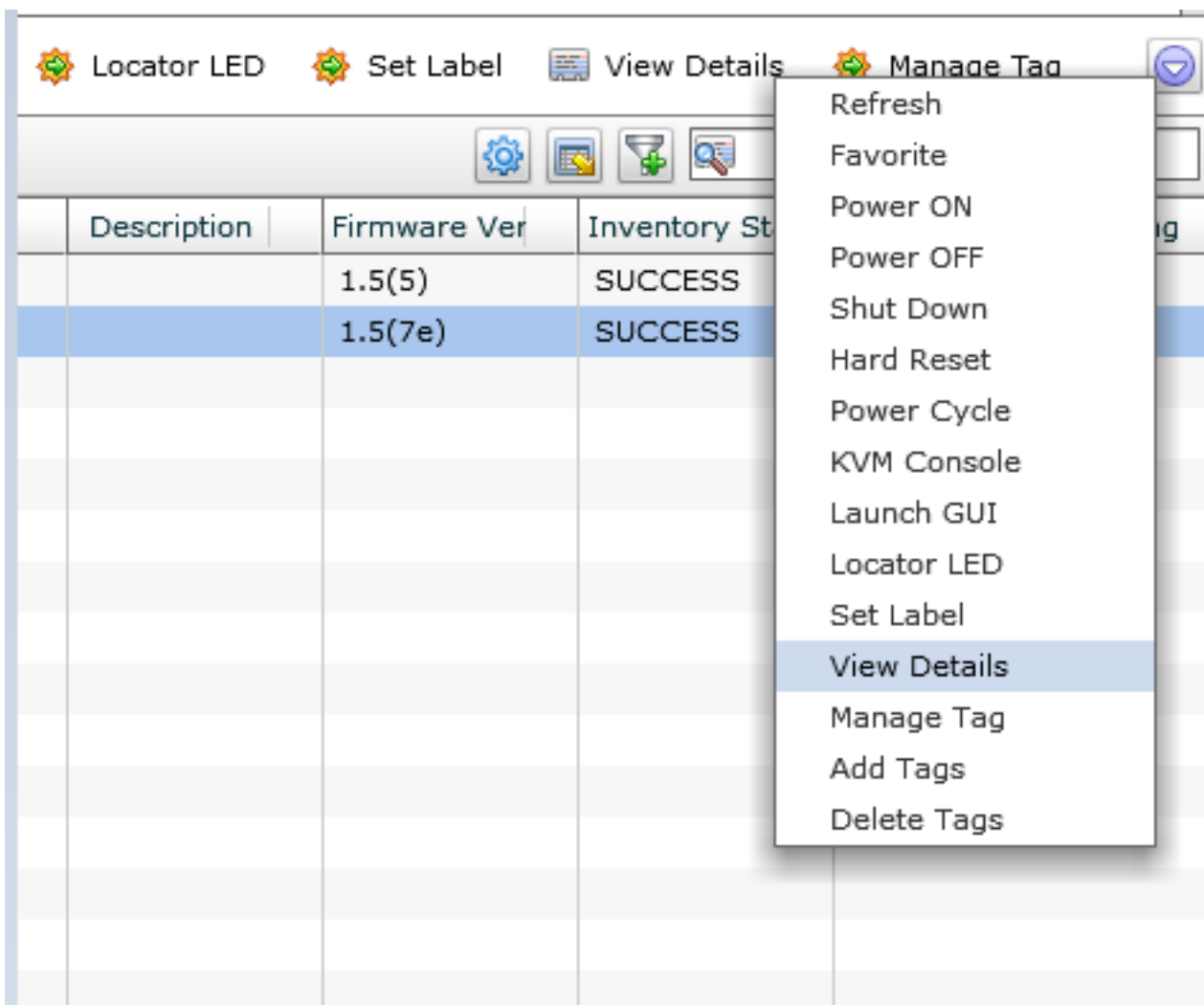
ステップ2:[ラックグループ]を展開し、サーバを含むラックグループを選択します。

ステップ3：図に示すように[Rack Servers]タブを選択します。



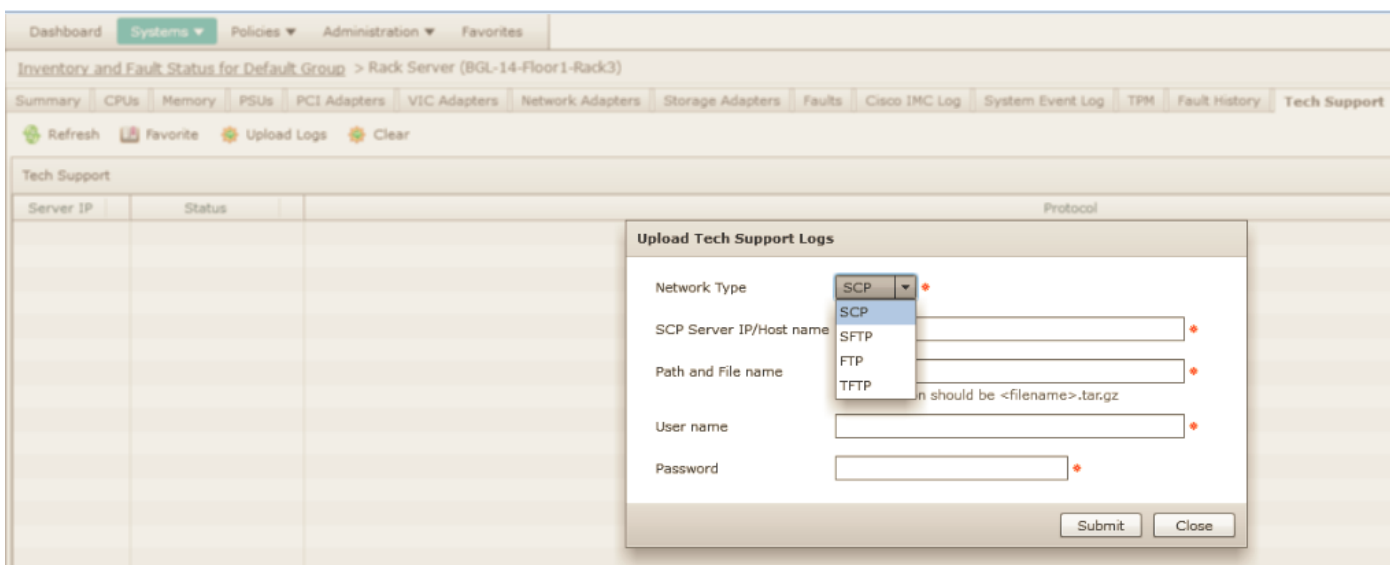
ステップ4：リストからサーバをダブルクリックして詳細を表示するか、リストからサーバをクリ

ックし、次に図に示すように、右端の下矢印から[View Details]をクリックします。



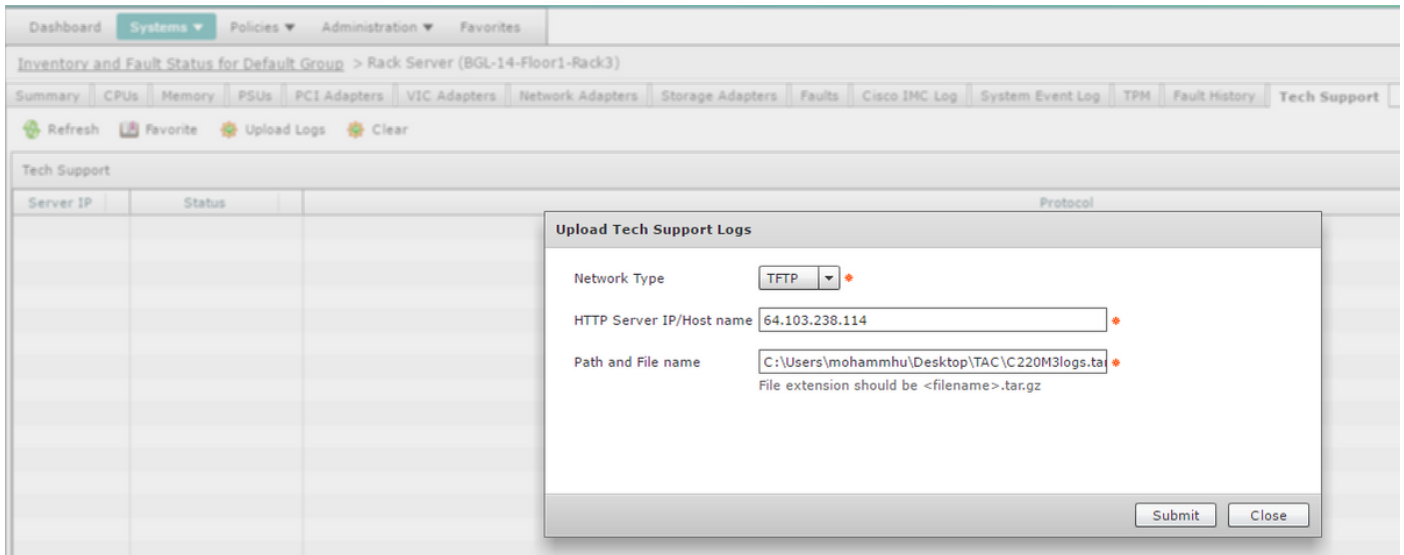
ステップ5:[Tech Support]タブをクリックしてください。

ステップ6：適切なネットワークタイプを選択して、図に示すようにファイルをアップロードします。

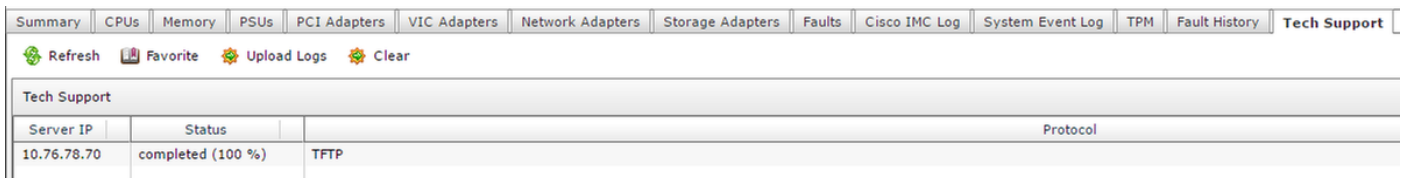


ステップ7：この例でTFTPを選択します。

ステップ8 : 図に示すように、[Submit]をクリックします。



ステップ9 : このスナップショットは、ログが指定された場所に正常にアップロードされたことを示します。



確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報ははありません。