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

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、次のソフトウェアとハードウェアのバージョンに基づいています。

- Internet Explorer 8 以降
- Google Chrome 4.1 以降
- Firefox 3.5 以上
- Safari 4.0 以降（Apple Mac または Microsoft Windows の場合）
- ブラウザには Adobe Flash Player プラグイン バージョン 11 以降がインストールされている必要があります。

UCS C シリーズ サーバ

- Cisco UCS C-220 M3
- Cisco UCS C-240 M3
- Cisco UCS C-220 M4
- Cisco UCS C-240 M4
- Cisco UCS C-22 M3
- Cisco UCS C-24 M3
- Cisco UCS C-420 M3
- Cisco UCS C-460 M4

UCS E シリーズ サーバ

- Cisco UCS E-140S M2
- Cisco UCS E-160D M2
- Cisco UCS EN120E M2
- Cisco UCS EN120S M2
- Cisco UCS E-180D M2
- Cisco UCS E-140S M1
- Cisco UCS E-140D M1
- Cisco UCS E-160D M1
- Cisco UCS E-140DP M1
- Cisco UCS E-160DP M1

ファームウェアの最低バージョン

サーバ	ファームウェアの最低バージョン
UCS C シリーズ サーバ	1.5(4) 以降
UCS E シリーズ サーバ	2.3.1 以降

サポートされる PCIe カード

- Cisco UCS 仮想インターフェイス カード（VIC）1225
- Cisco UCS VIC 1225T

サポートされるハイパーバイザのバージョン

- ESXi 5.1

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。

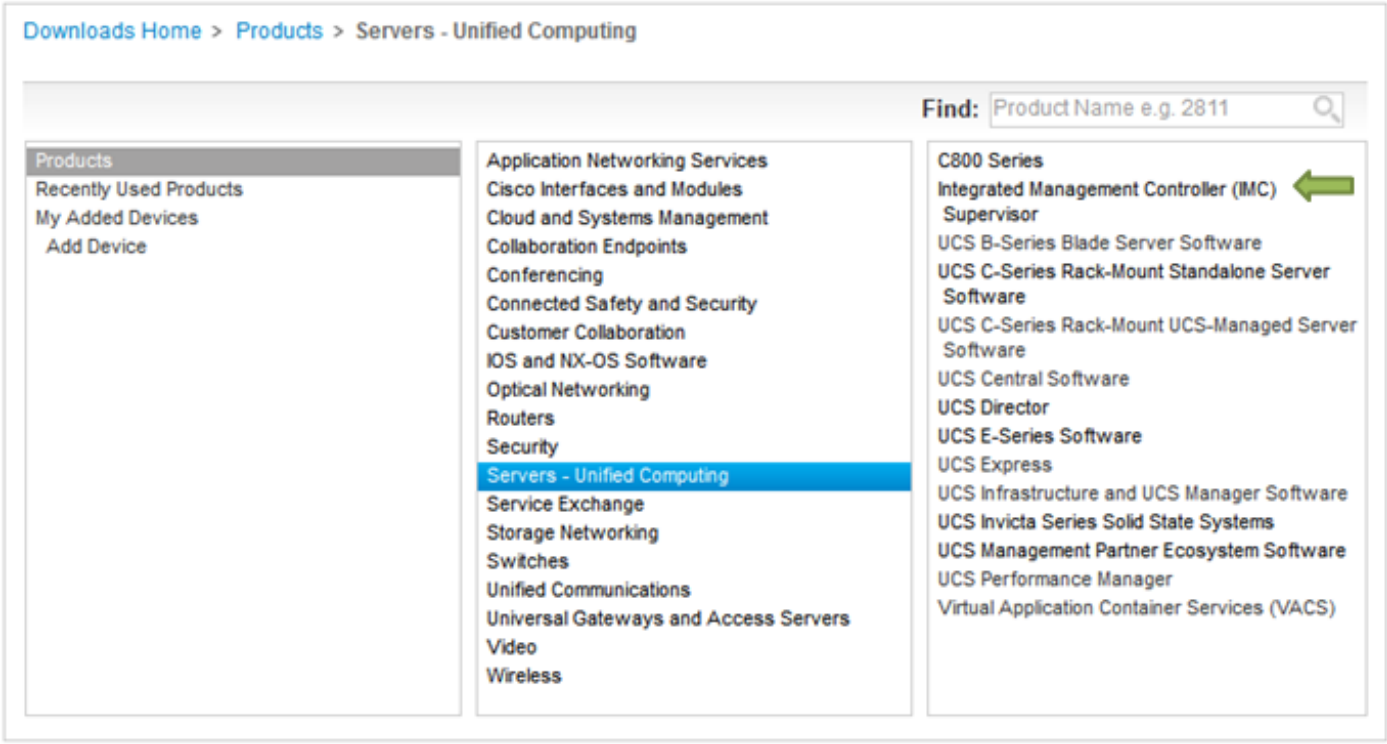
- サーバの論理グループ化およびグループごとのサマリー表示のサポート
- サーバ インベントリの収集
- サーバおよびグループのモニタリング
- ファームウェアのダウンロード、アップグレード、アクティベーションを含むファームウェア管理
- 電源制御、LED制御、ログ収集、キーボード/ビデオ/マウス(KVM)の起動、CIMCユーザインターフェイスの起動、電子メールアラートなどのスタンドアロンサーバアクションの管理
- アクセスと機能を制限するためのロールベースアクセスコントロール(RBAC)

設定

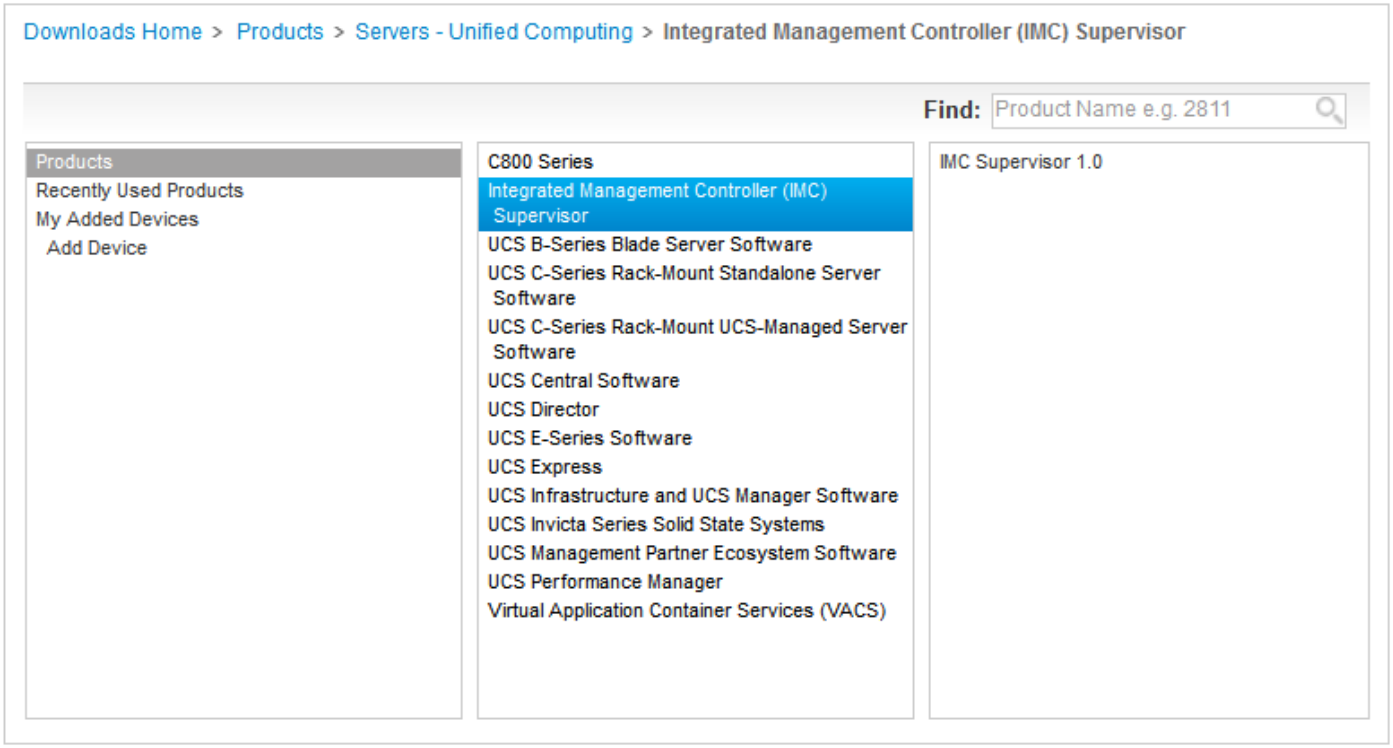
Cisco IMC Supervisorの導入

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

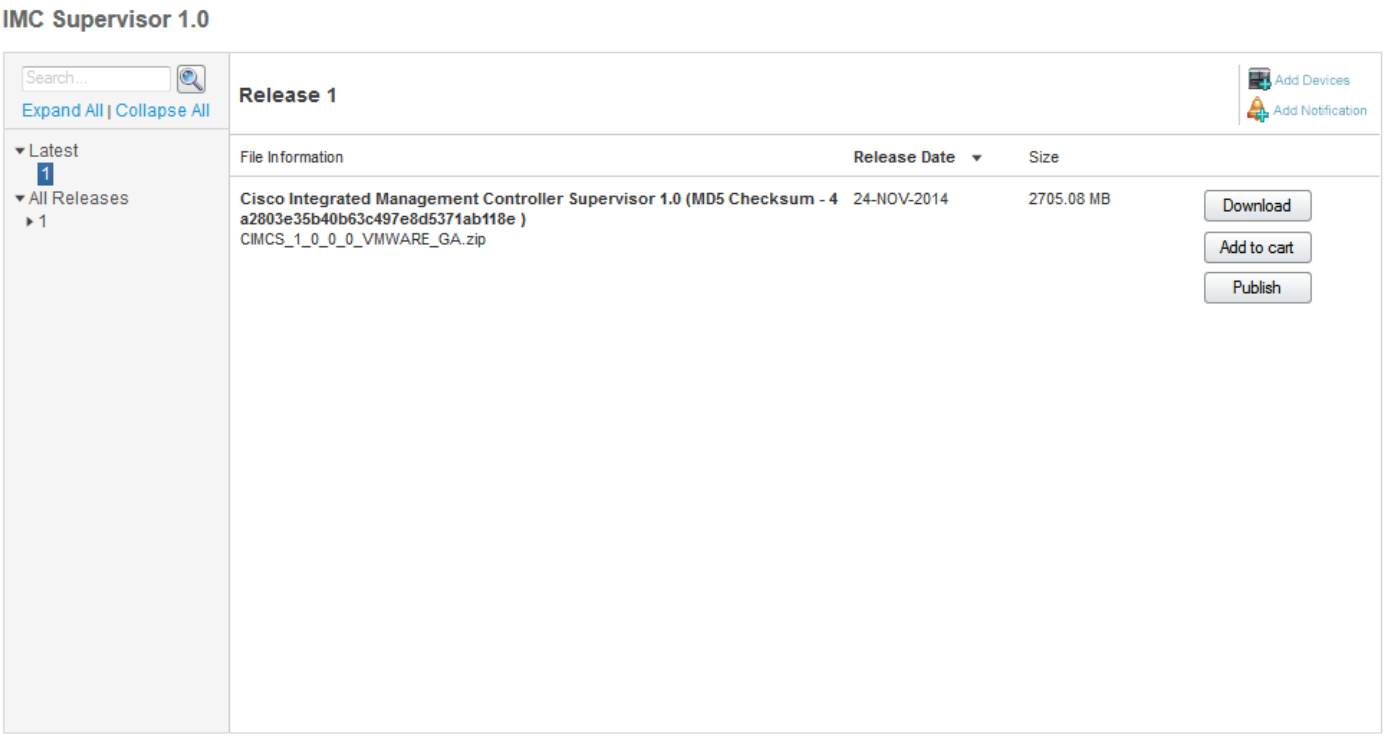
ステップ1:Cisco.comからCisco IMC Supervisorのzipファイルをダウンロードするには、図に示すように、**[Products] > [Servers-Unified Computing] > [Integrated Management Controller (IMC) Supervisor]に移動します。**



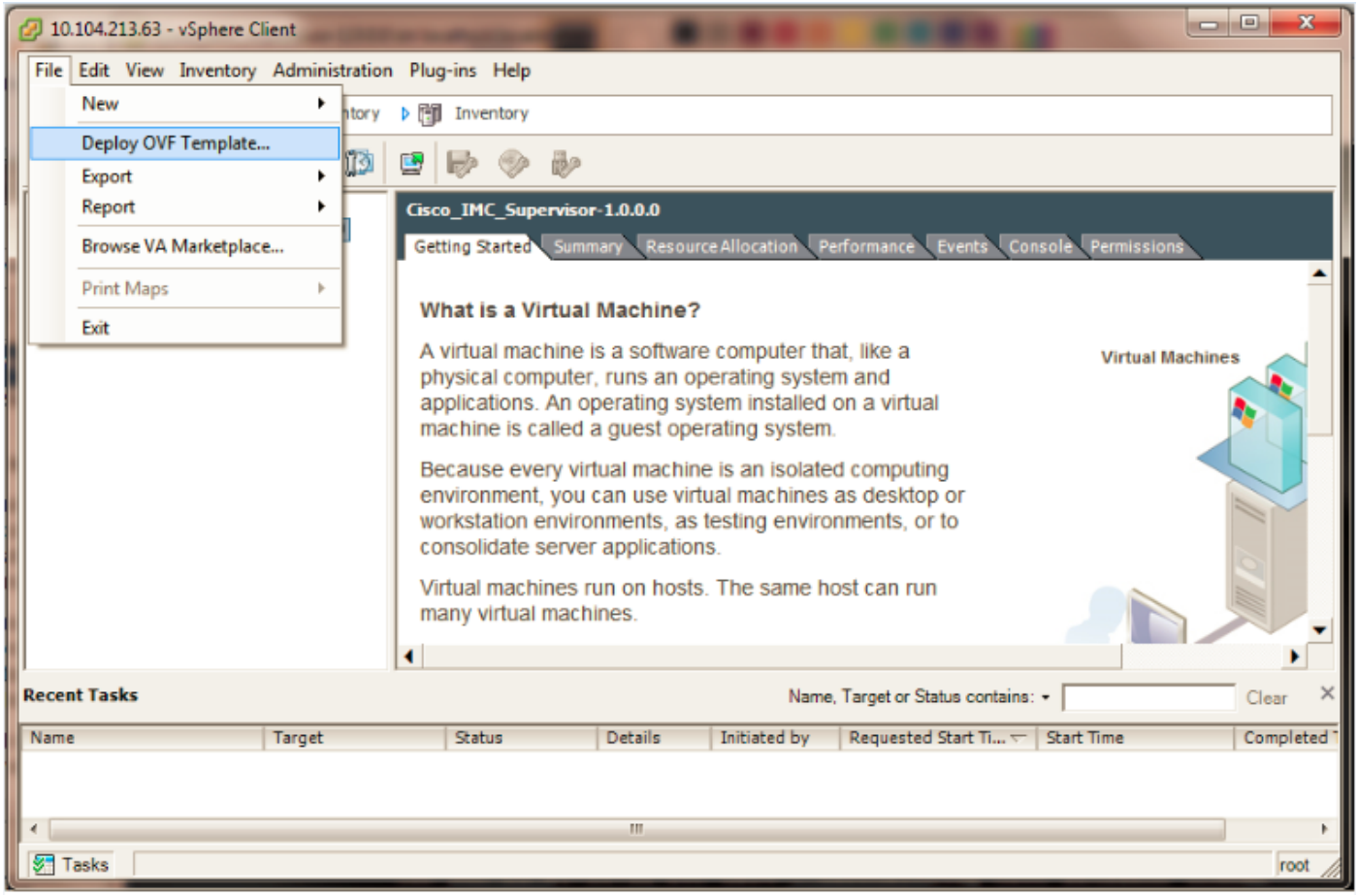
ステップ2：図に示**すように、IMC Supervisor 1.0**を選択します。



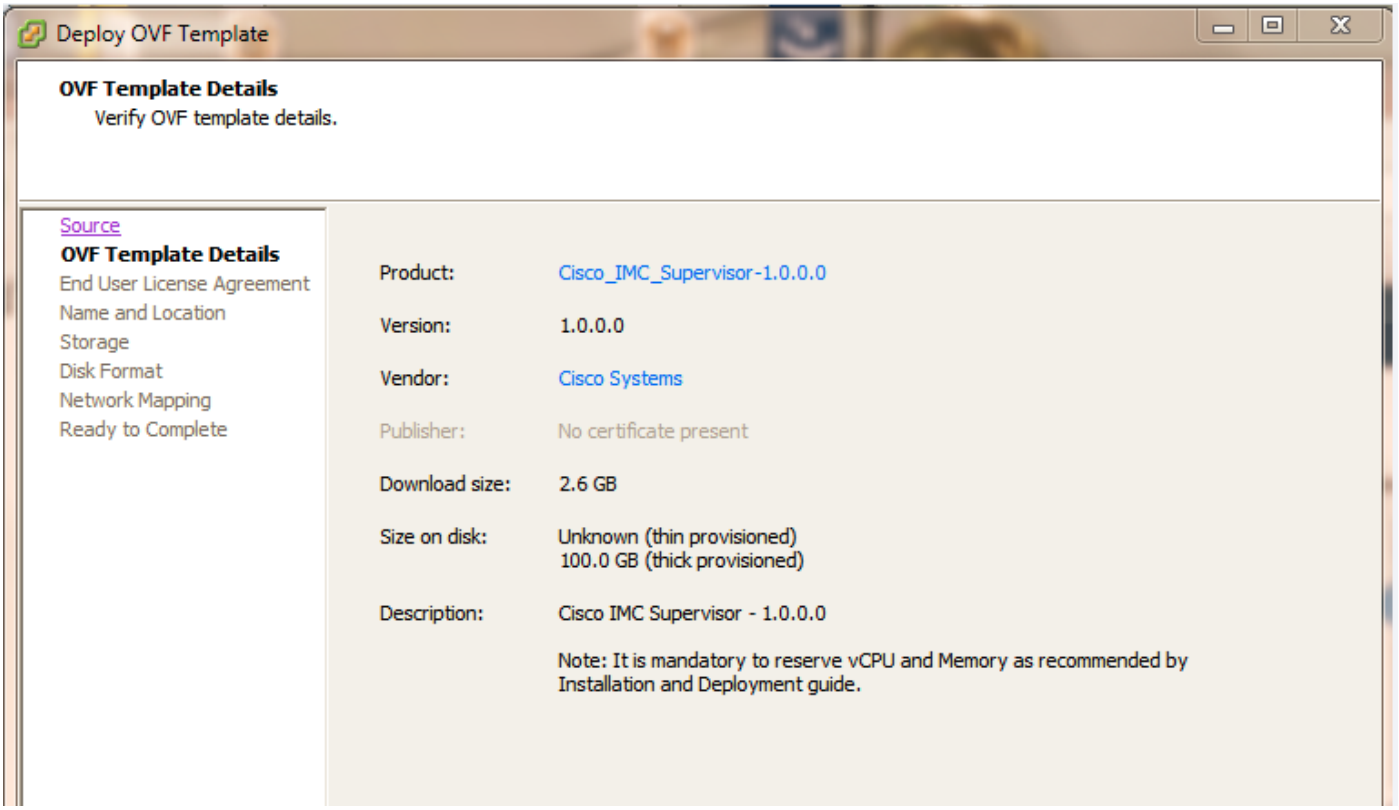
ステップ3：図に示すように、**[Download]**をクリックします。

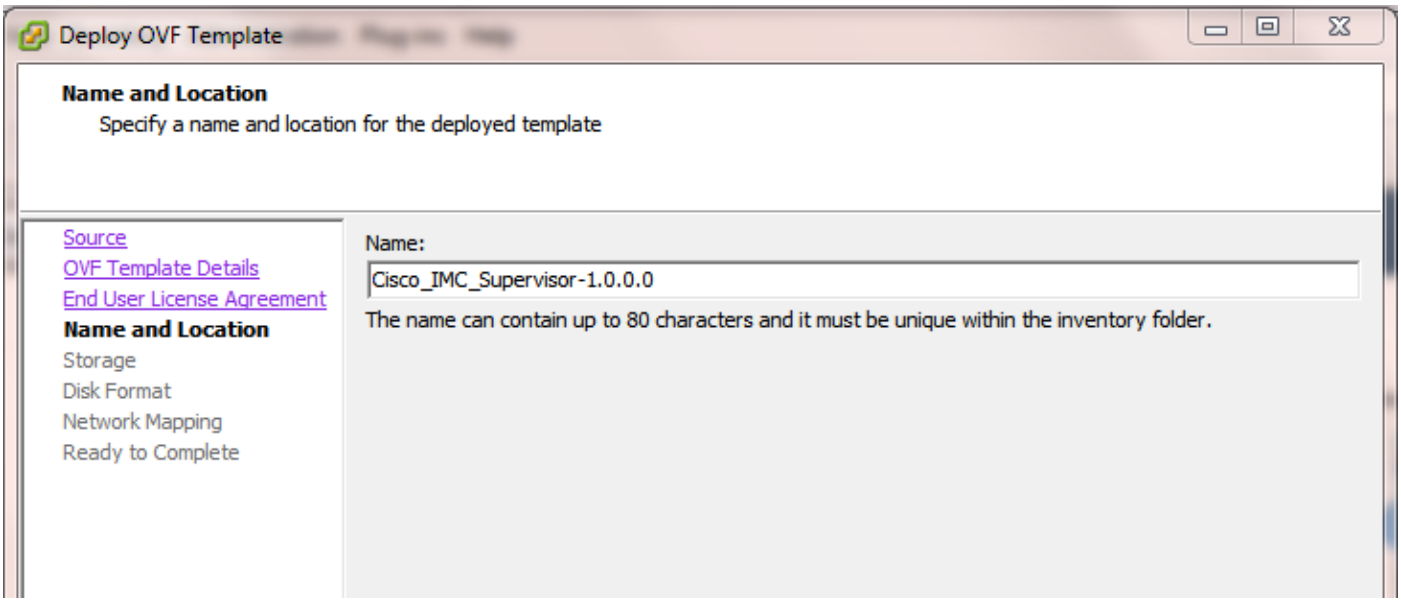


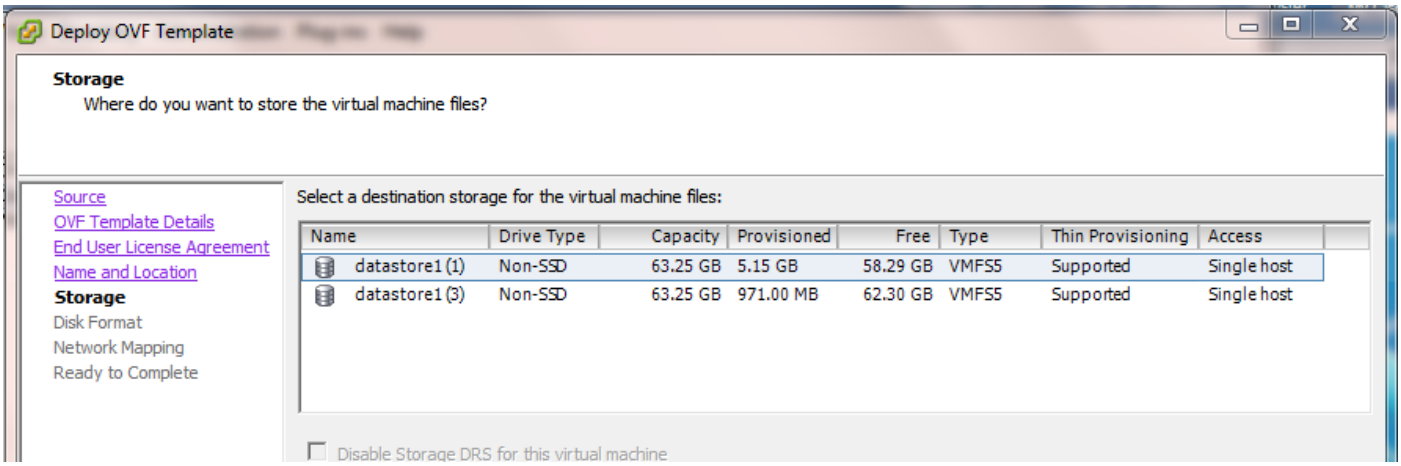
ステップ4：図に示すように、Open Virtual Appliance(OVA)を導入するには、**[File] > [Deploy OVF Template]に移動**します。



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。

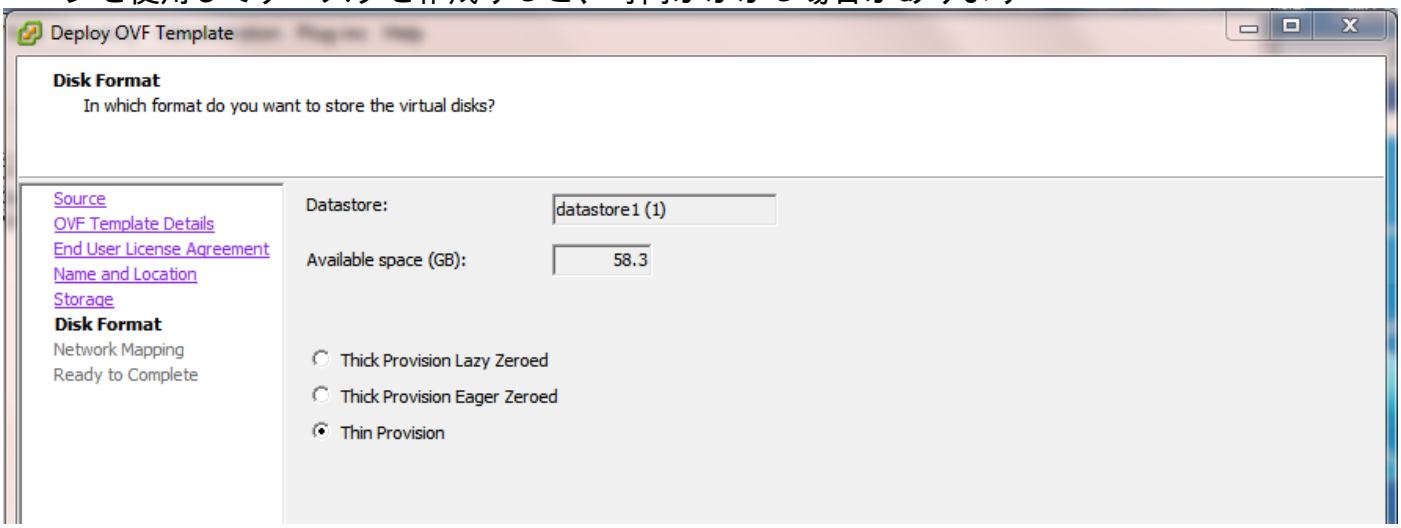




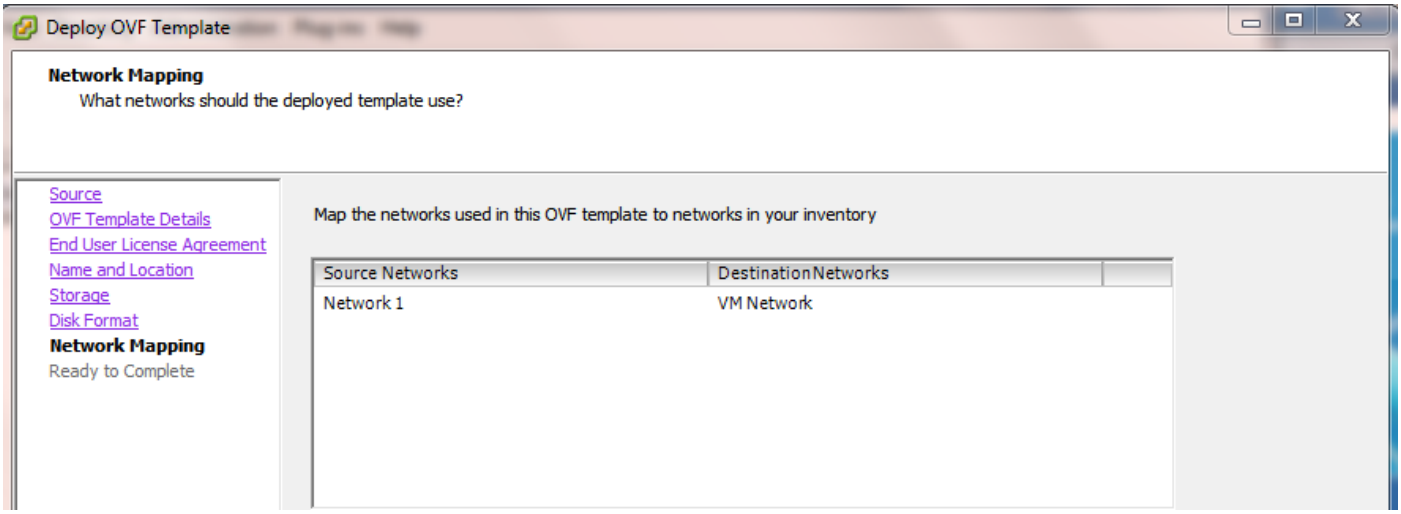


[ディスクフォーマット]ペインで、オプションボタンを1つ選択し、図に示すように[次へ]をクリックします。

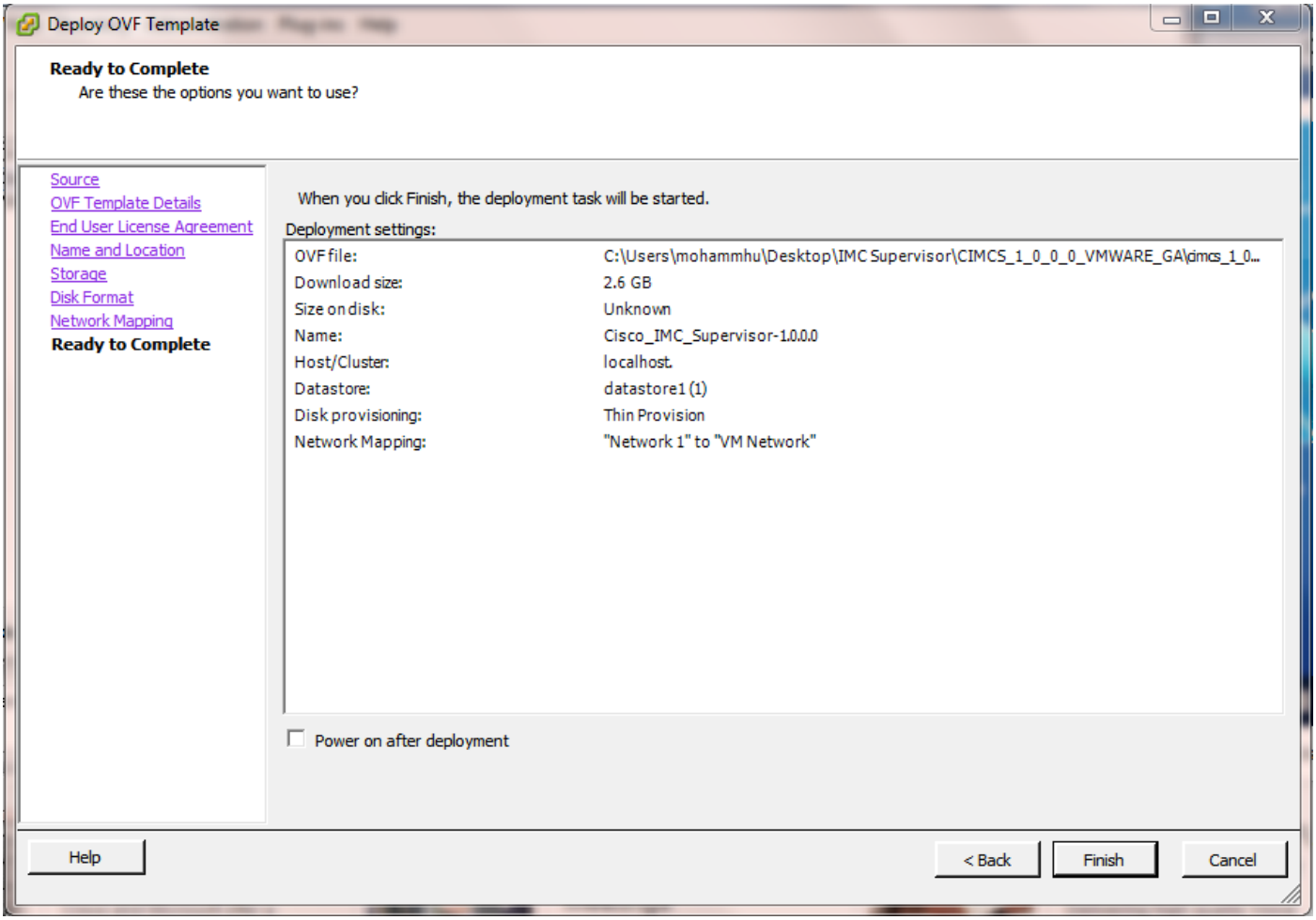
- シンプロビジョニング：データがディスクに書き込まれるときにストレージをオンデマンドで割り当てるために使用します。
- Thick Provision Lazy Zeroed：シック形式ですぐにストレージを割り当てるために使用します。
- Thick Provision Eager Zeroed：シック形式でストレージを割り当てるために。このオプションを使用してディスクを作成すると、時間がかかる場合があります



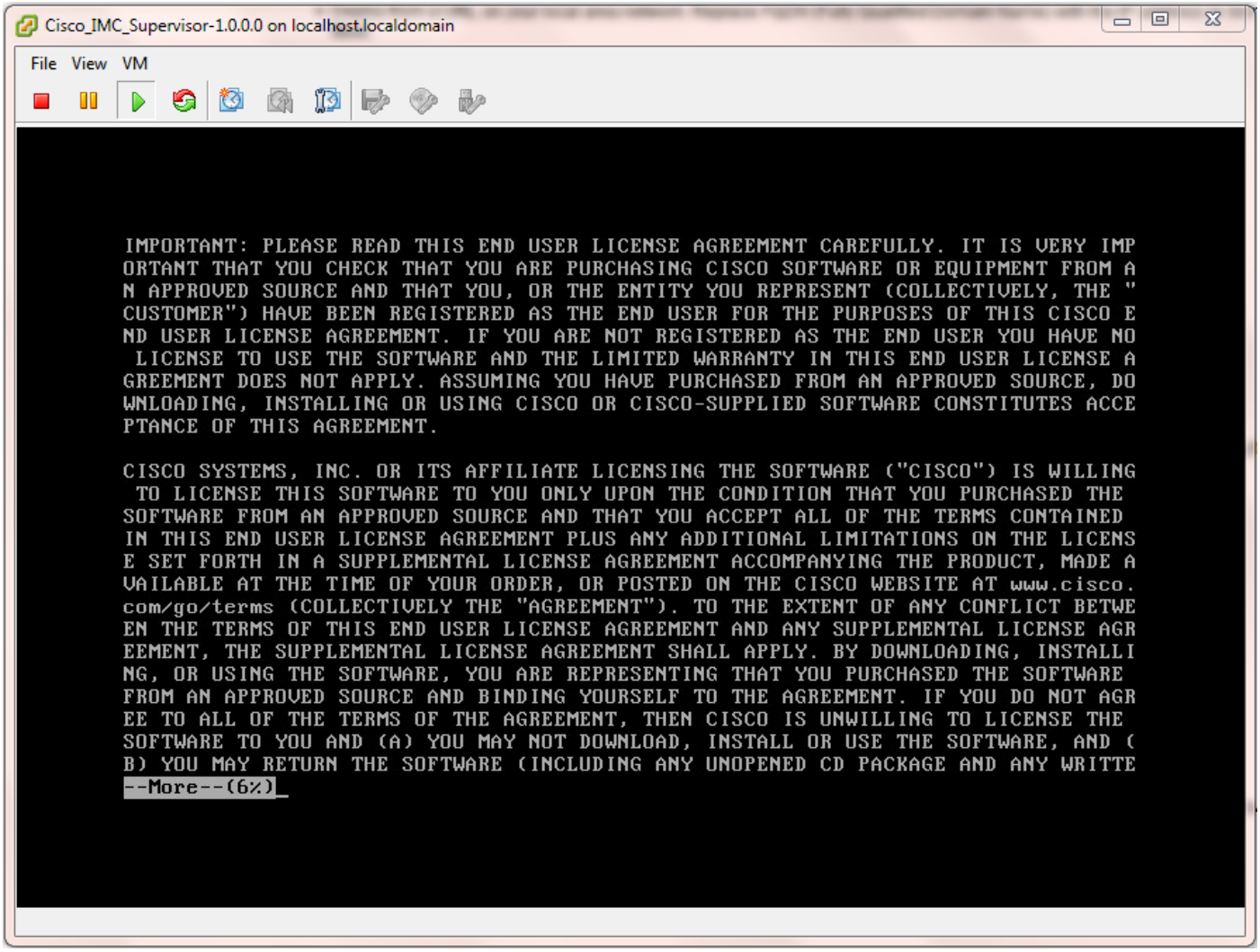
ステップ6：図に示すように、仮想マシン(VM)ネットワークに適切なポートグループを選択します。



ステップ7：図に示すように**[Finish]**をクリックします。

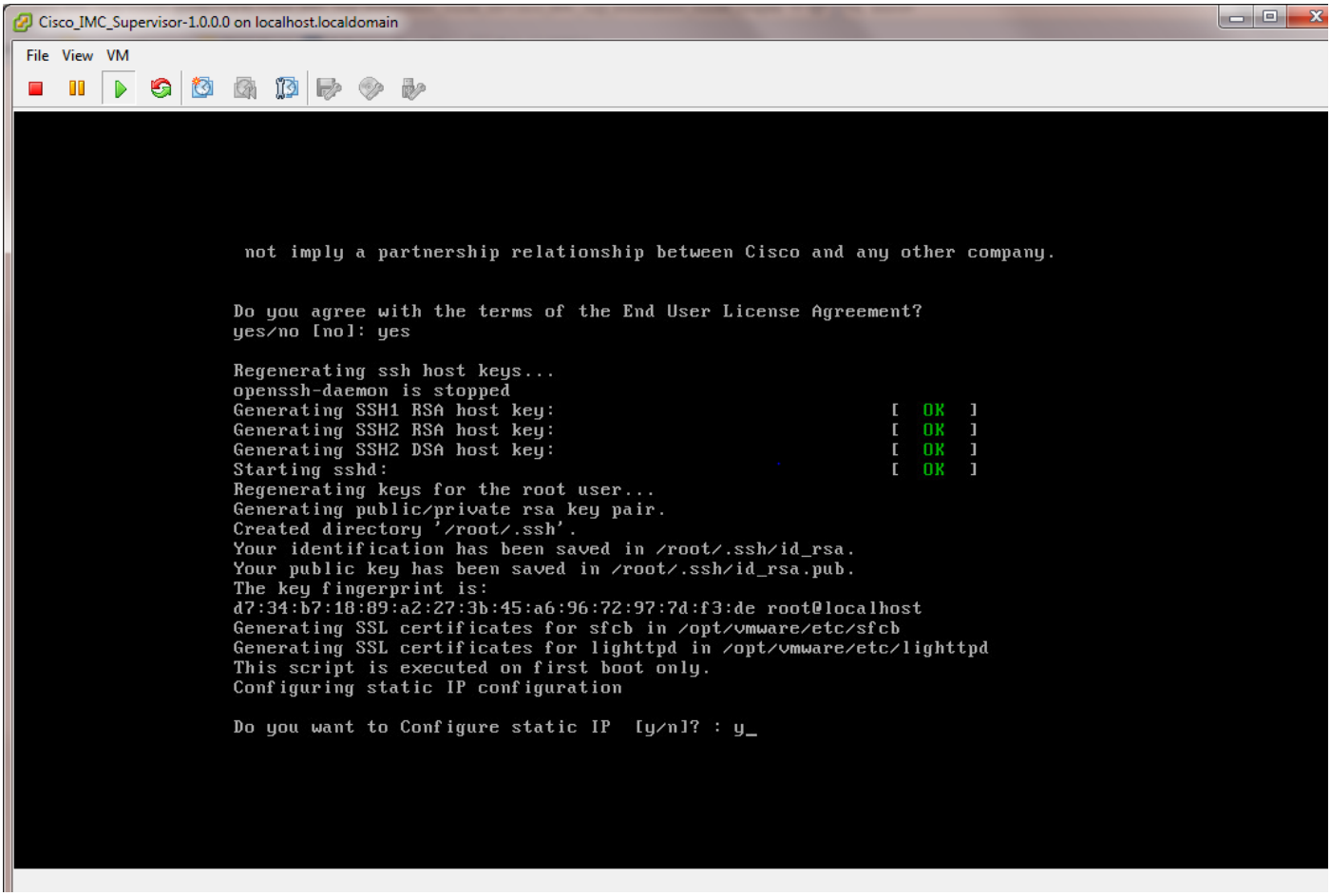


ステップ8：図に示すように、VMのコンソールを開き、ライセンス契約に同意します。



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。

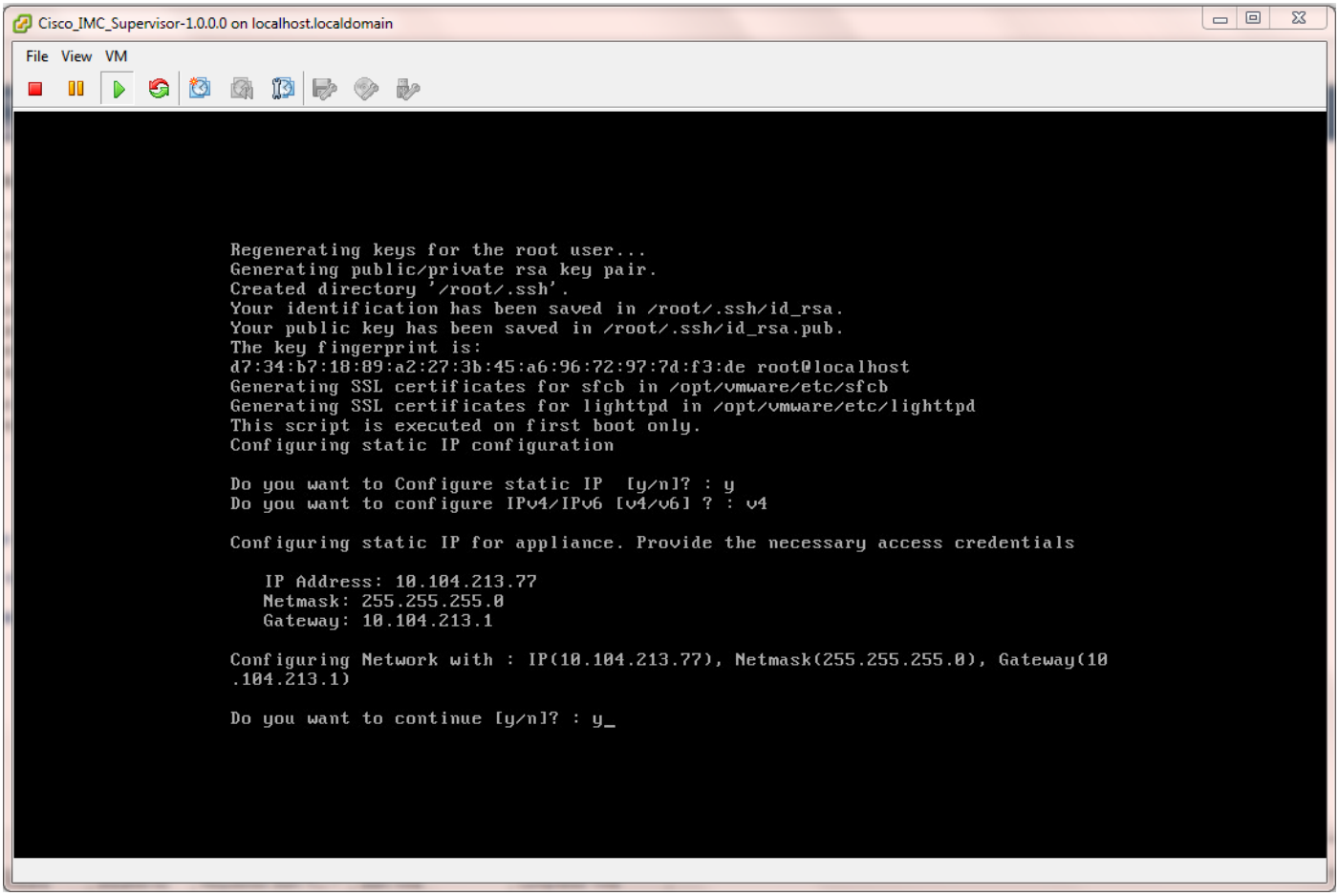
ステップ10:DHCPを使用する場合は、**n**を入力して、IPアドレスが自動的に割り当てられていることを確認します。

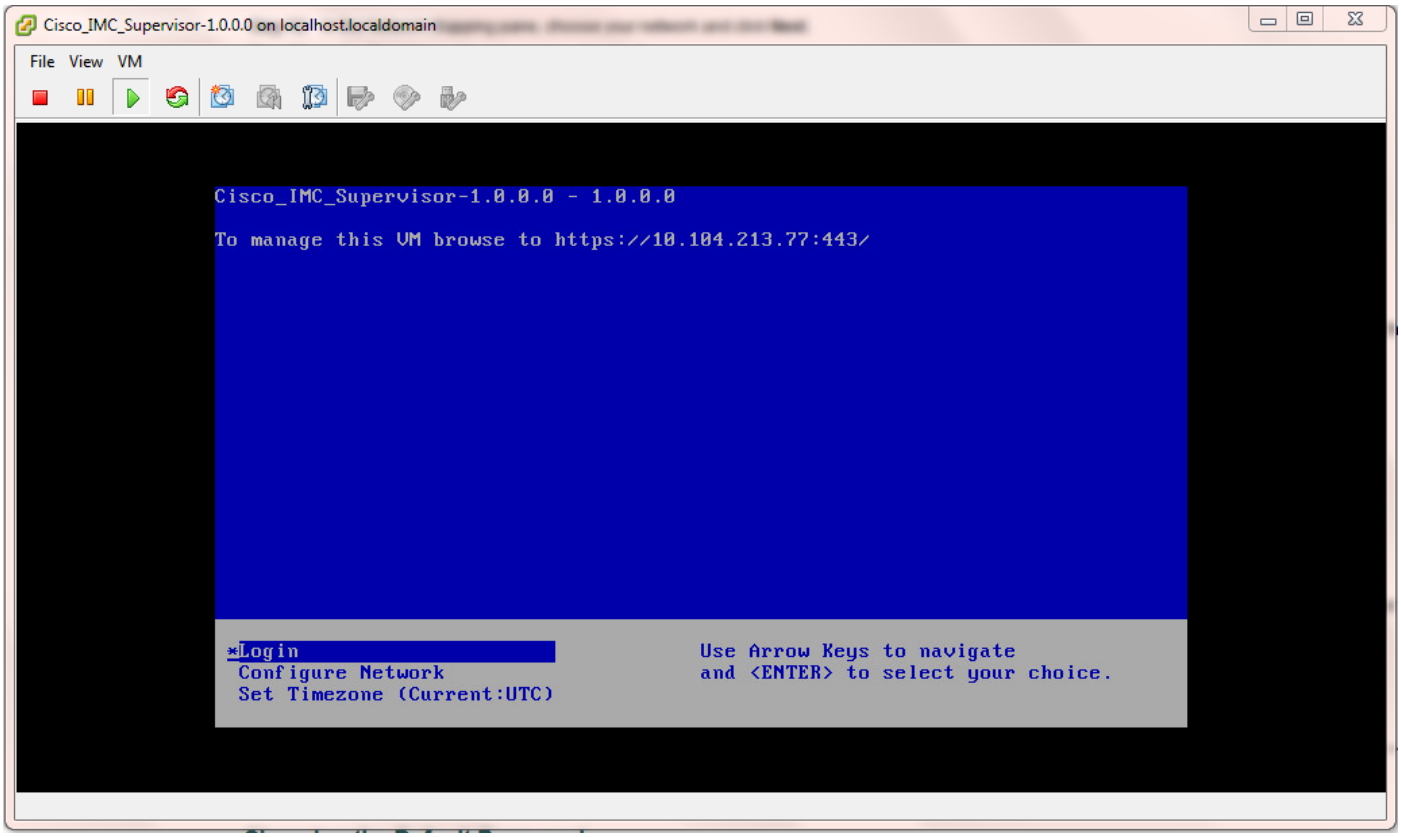


ステップ11：スタティックIPアドレスを使用する場合は、yと入力して、IPv4またはIPv6を選択するよう求められます。V4と入力して、図に示すように情報をを入力します。

- 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。



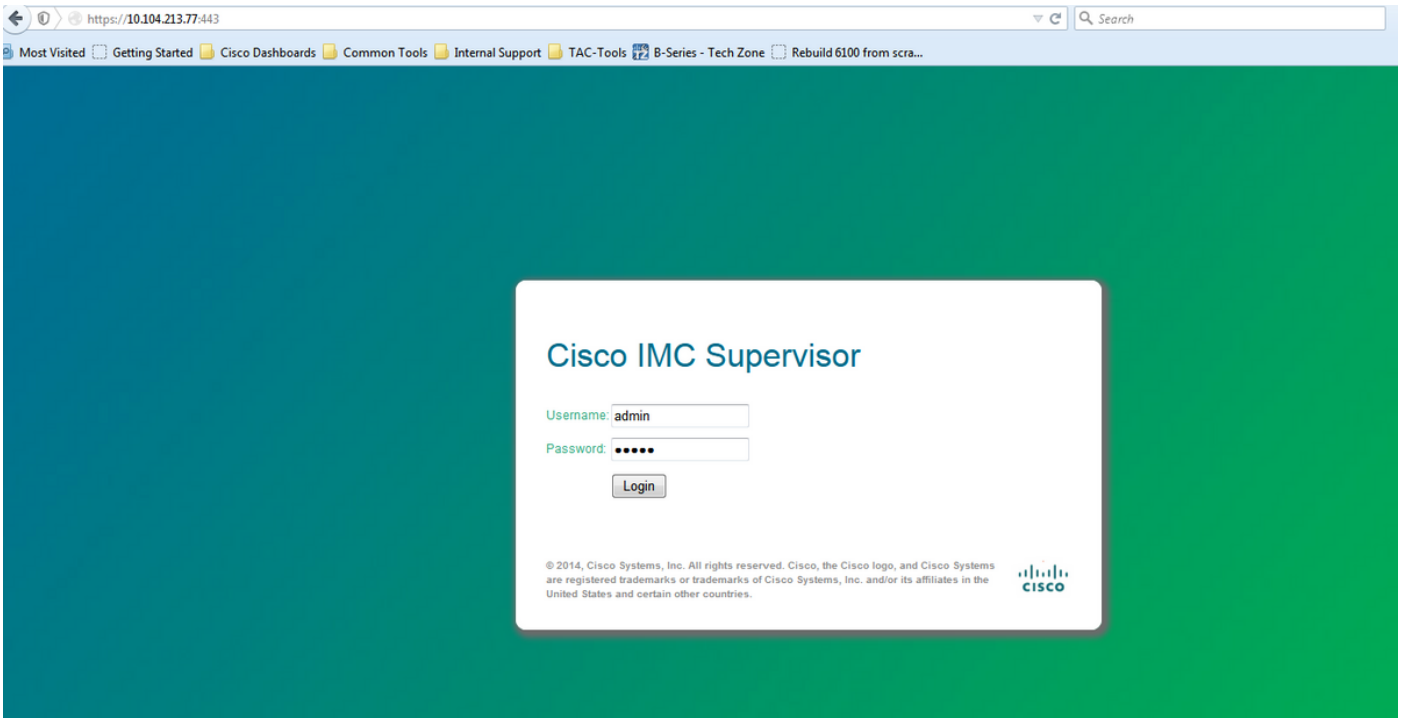


ステップ12：アプライアンスが起動したら、サポートされているWebブラウザにCisco IMC Supervisor IPアドレスを転送して、ログインページにアクセスします。

[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。



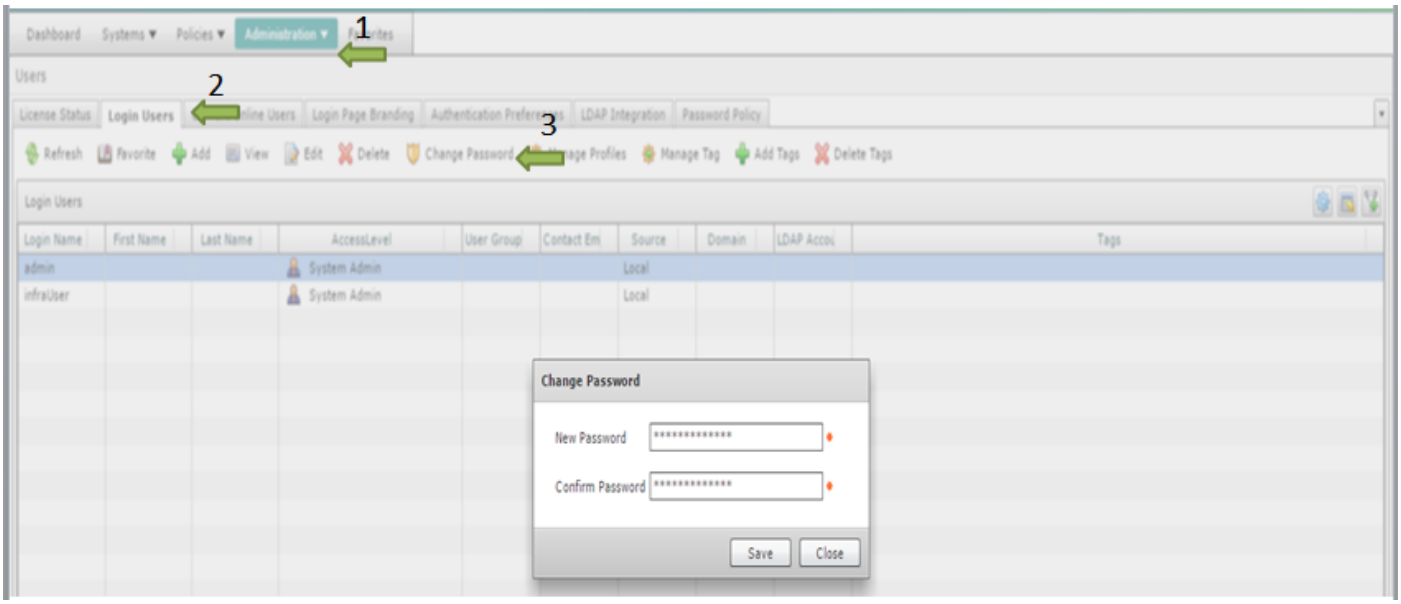
デフォルトパスワードの変更

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**。

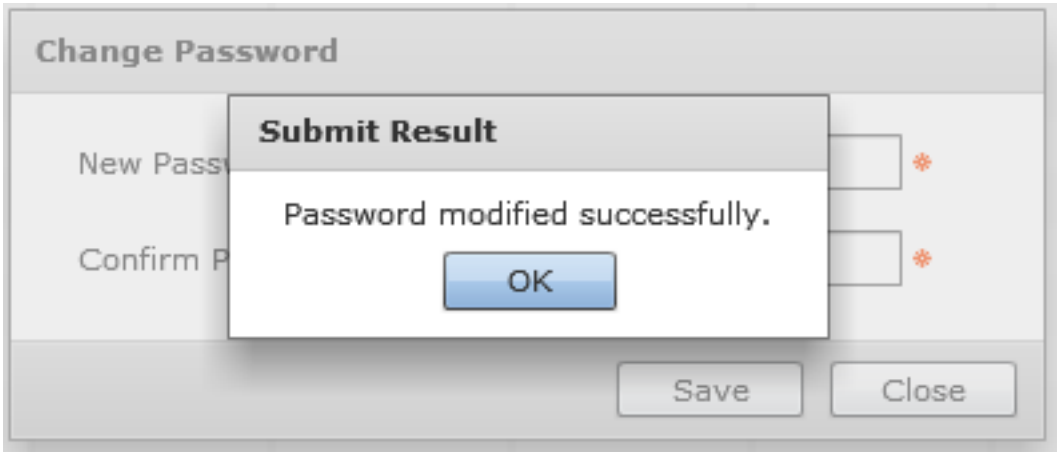
ステップ2:[Login Users]タブを**クリック**します。

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**

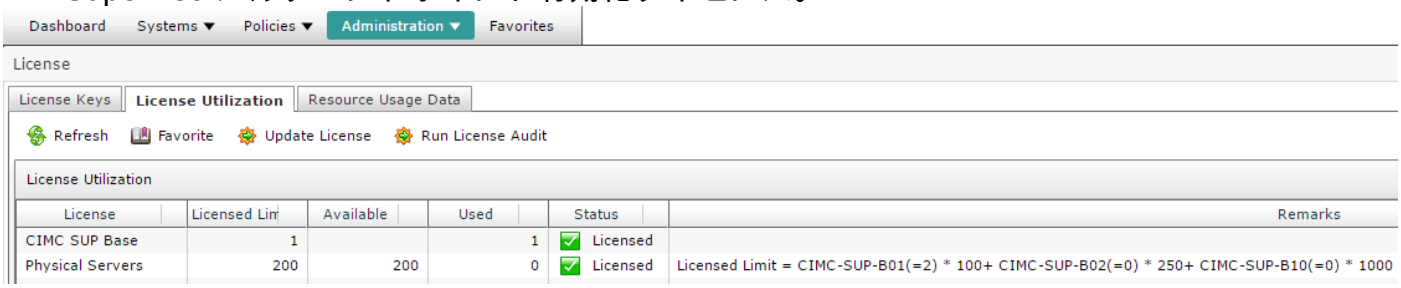
Result]の[OK]をクリックします。



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。

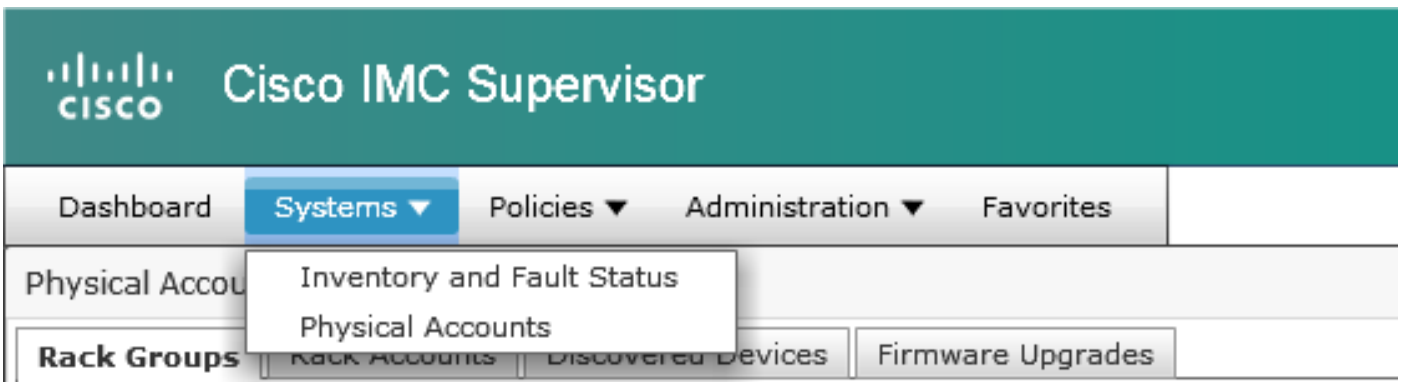


> **注**：これらのライセンスがない限り、サーバをラックアカウントにグループ化するなどのタスクは実行できません。

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。



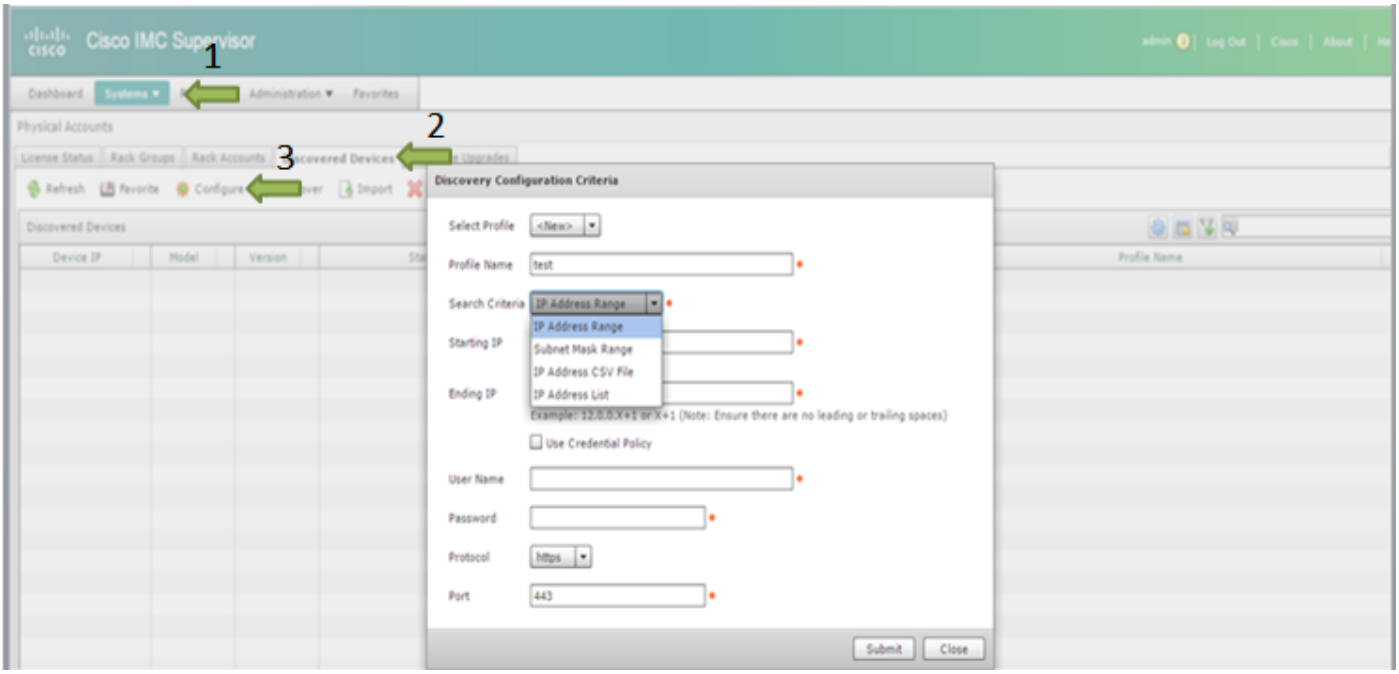
ステップ2:[Configure]をクリックします。

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。

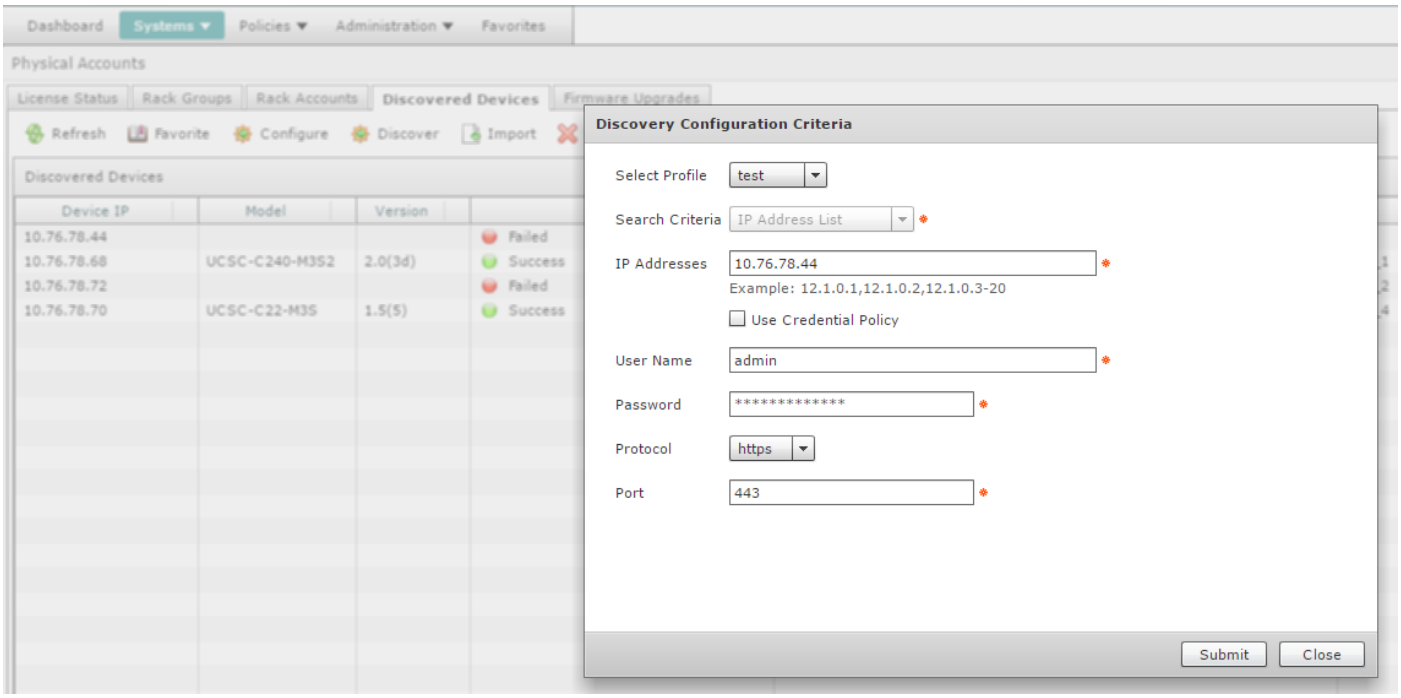
ステップ5:[Search Criteria]で、サーバを検出するための適切な方法を選択できます。

ステップ6：この例で[IP Address List]を選択します。

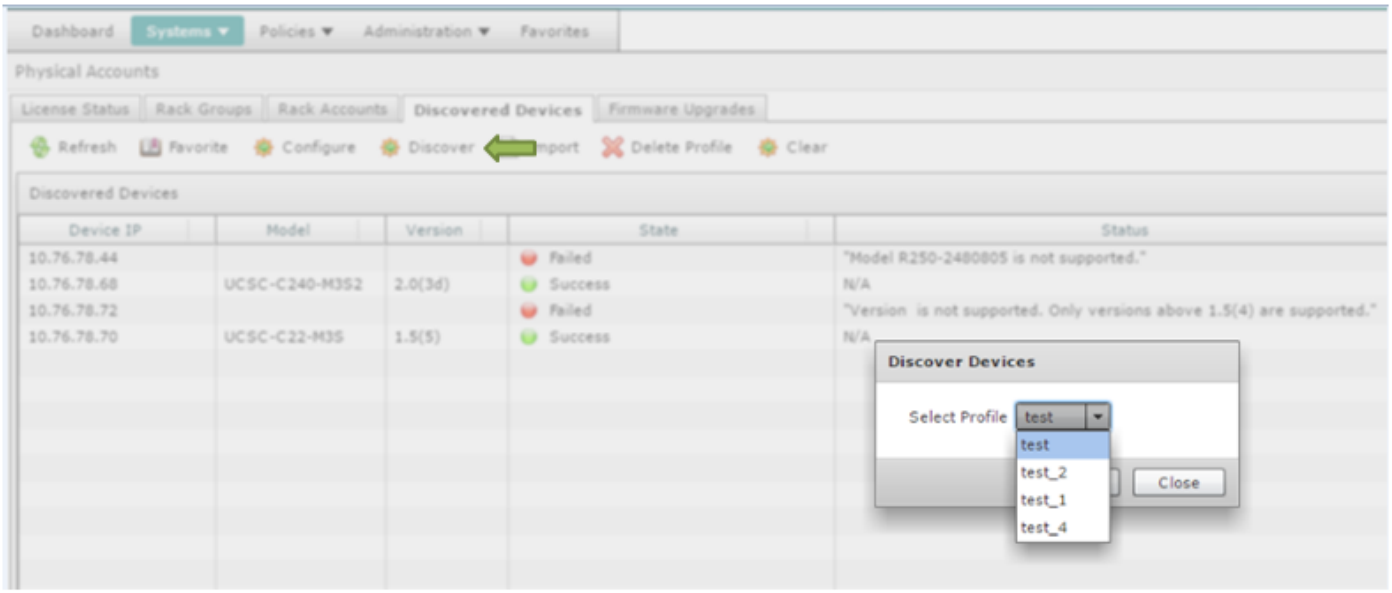


ステップ7：検出するサーバのIPアドレスを入力します。

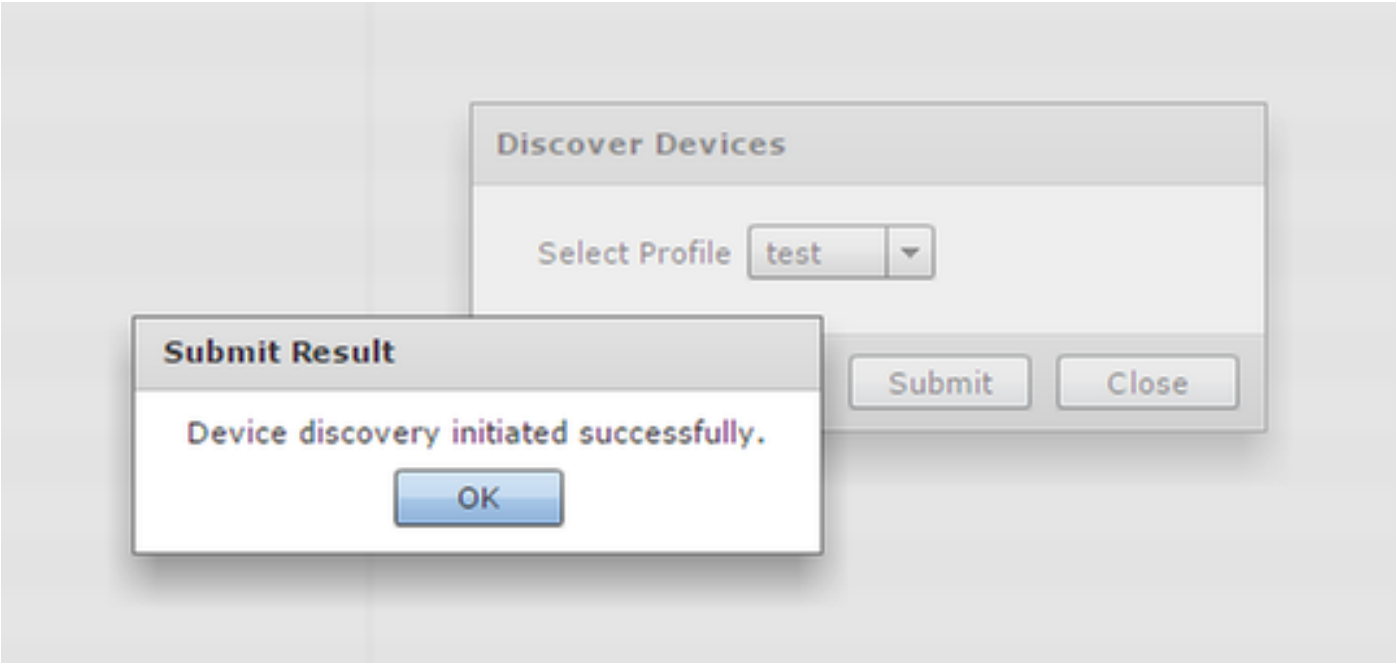
ステップ8：図に示すように、サーバへのログインに使用するユーザ名とパスワード（CIMCクレデンシャル）を入力します。



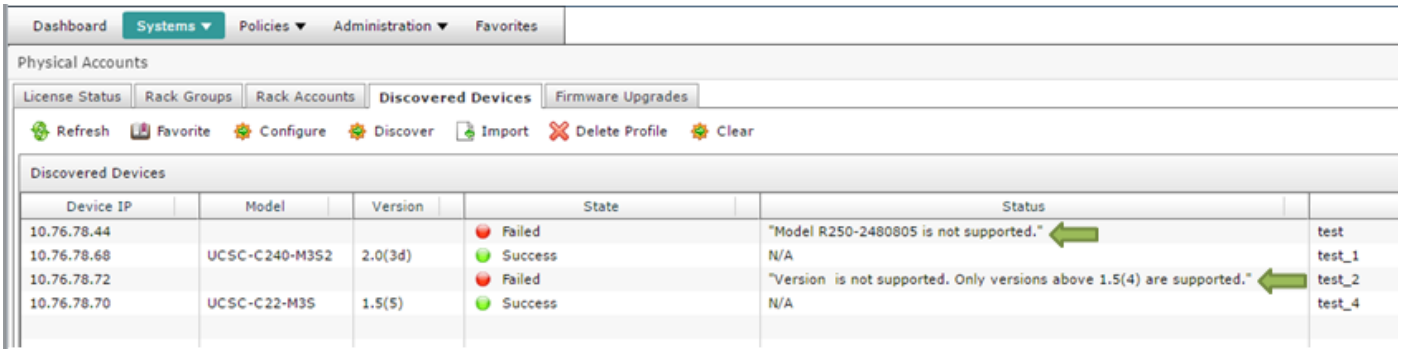
ステップ9：プロファイルが作成されたら、図に示すように、ドロップダウンリストから[**Discover** and Select Profile]をクリックします。



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。



ラックグループの追加

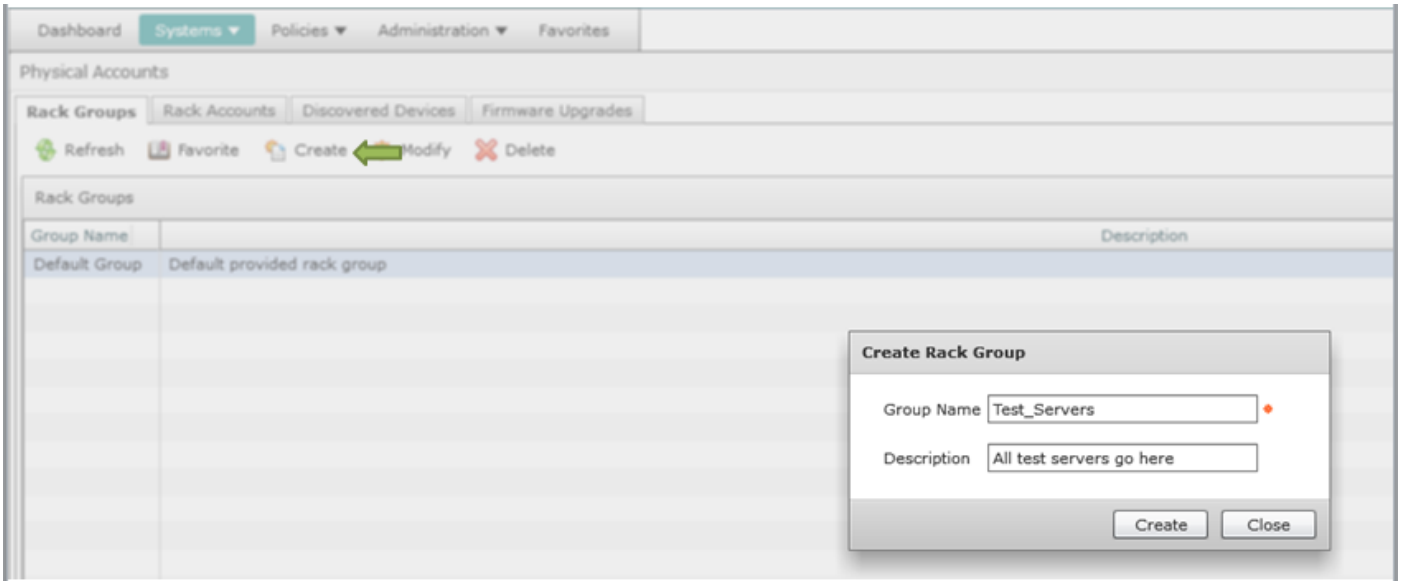
5. Cisco IMC Supervisorに新しいラックグループを追加する場合は、この手順を実行します。

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。

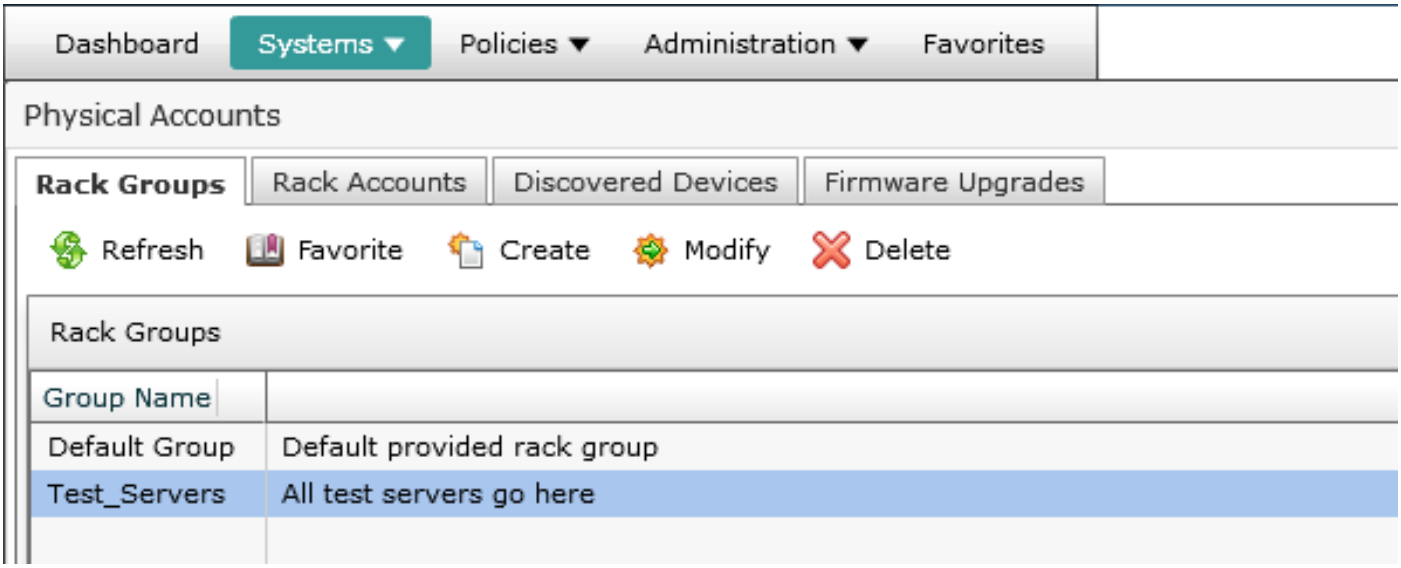
ステップ2:[Create]をクリックします。

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。



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

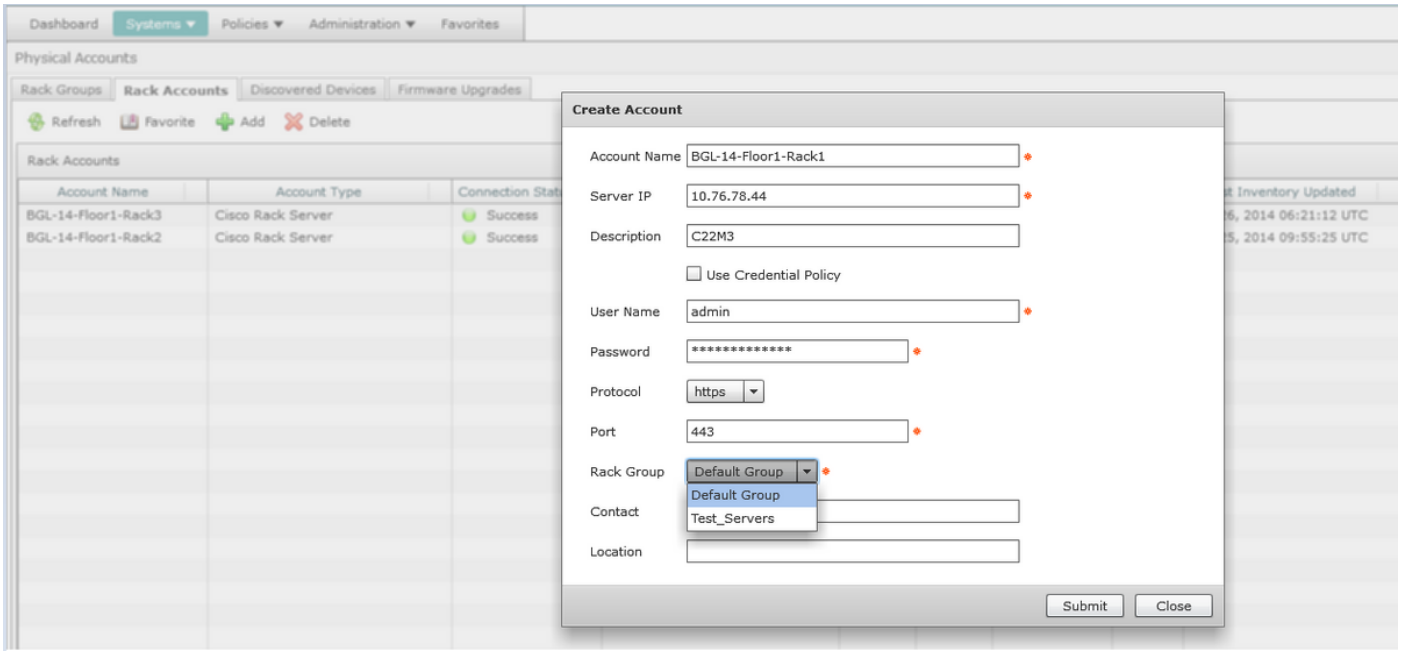
6. Cisco IMC Supervisorに新しいラックグループを追加する場合は、この手順を実行します。

ステップ1：　メニューバーから[システム]を**選択します。**
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。

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
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は
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
チェックボックスをオフにした場合	
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
[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。



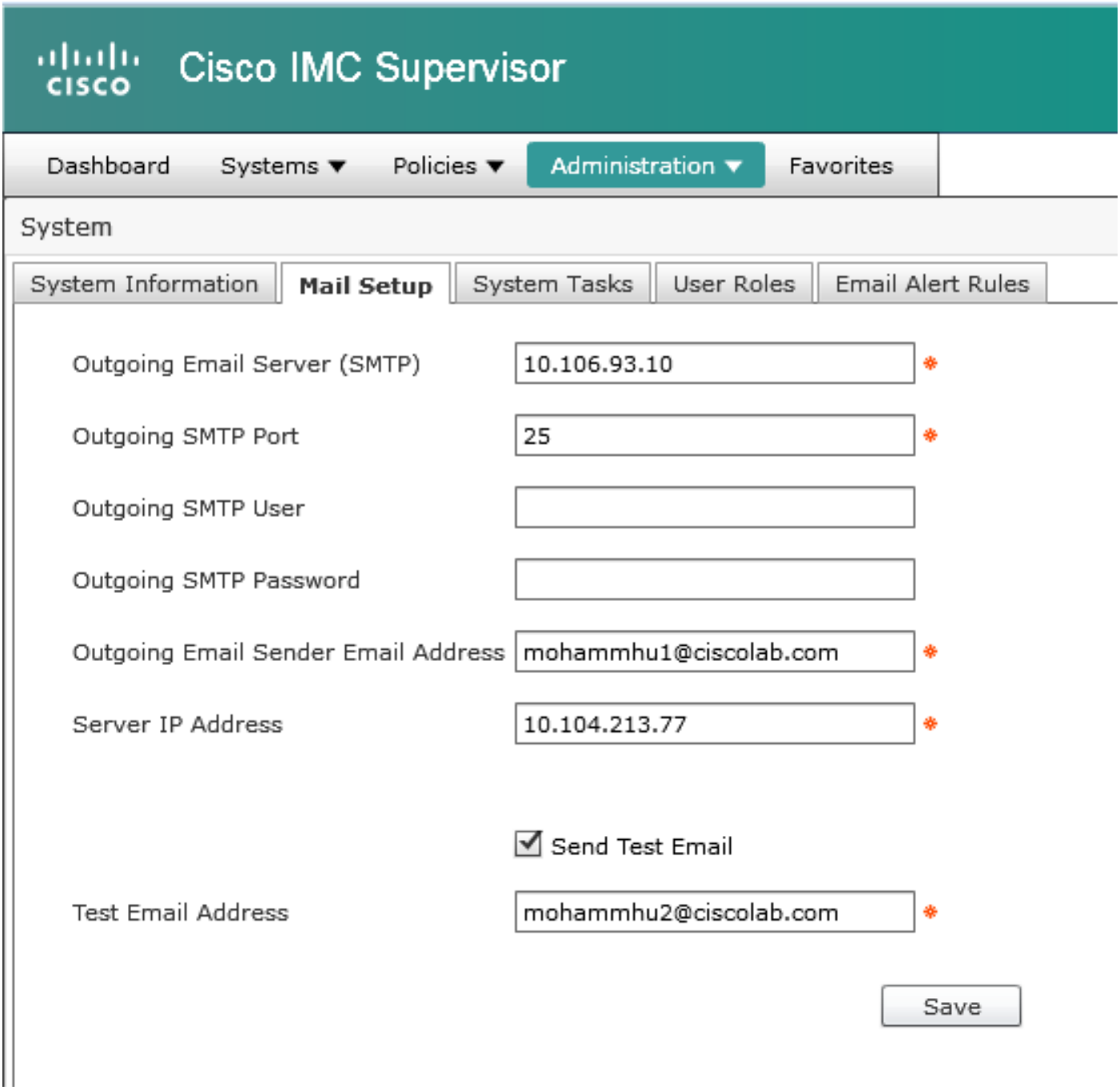
メール セットアップの設定

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。

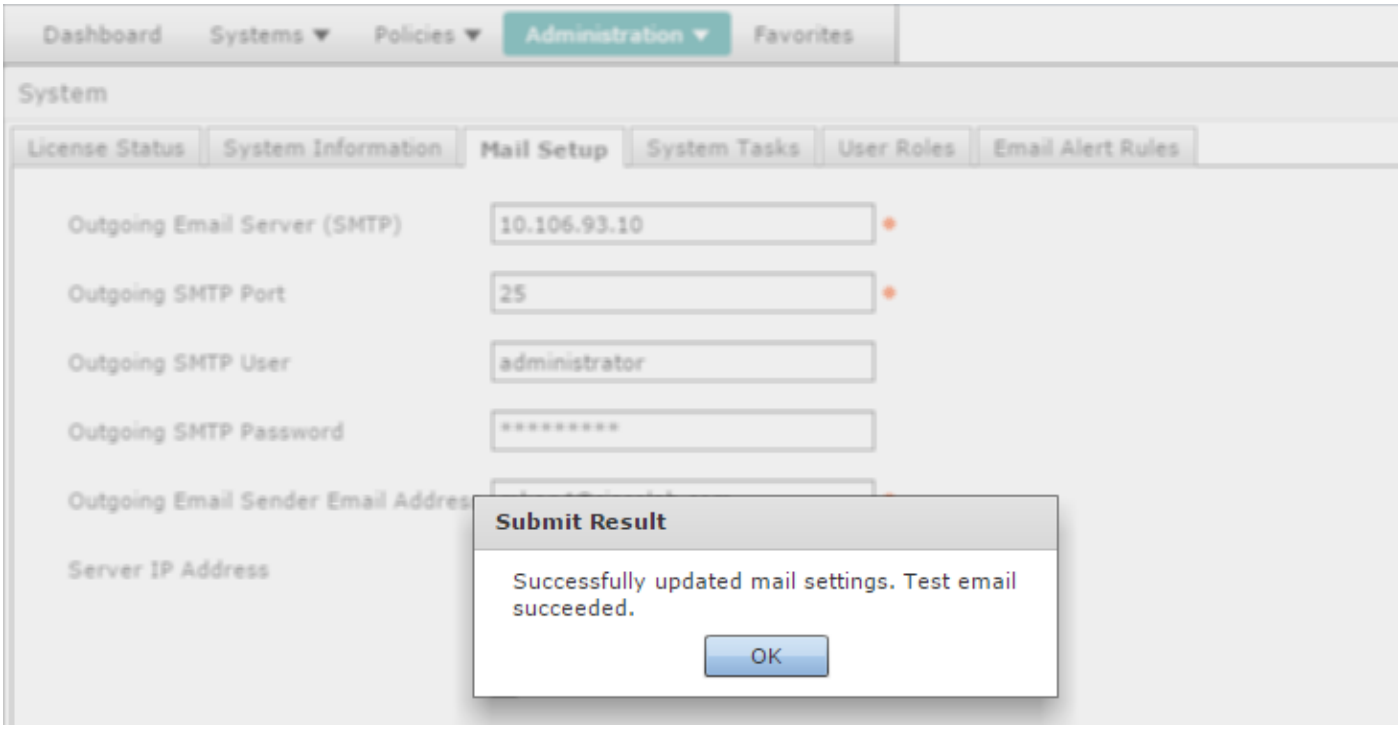
ステップ1:[Administration] > [**Mail Setup]に移動します。**

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。

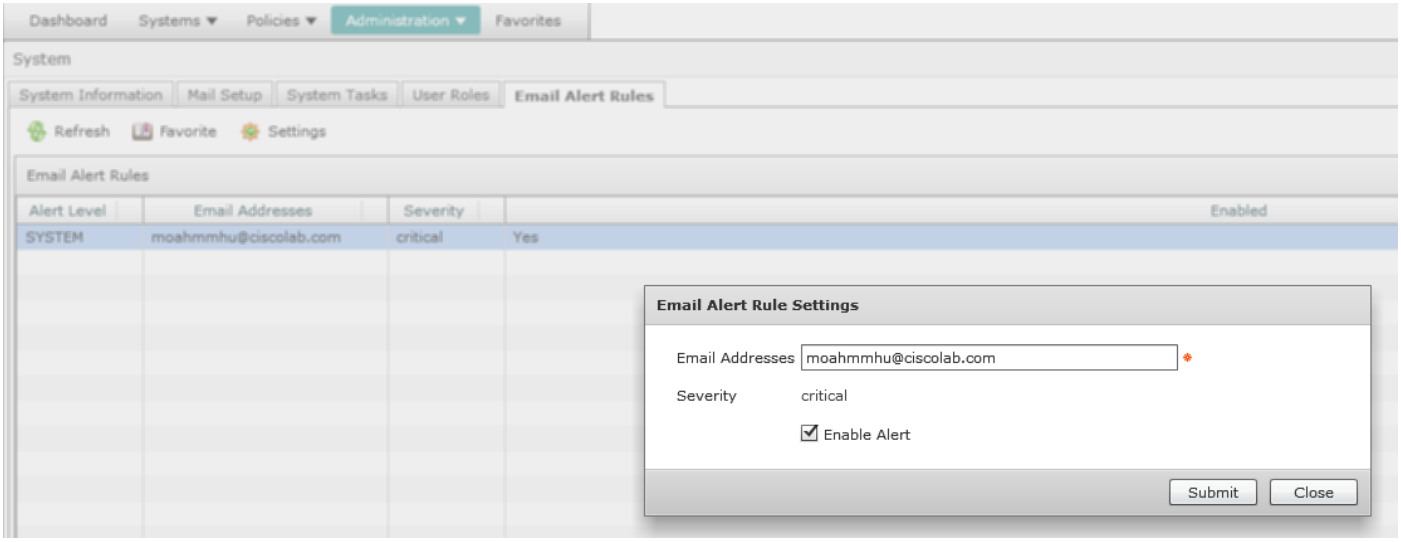


ステップ4：図に示すように、テストメールを受信する必要があります。



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 reseat 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**。

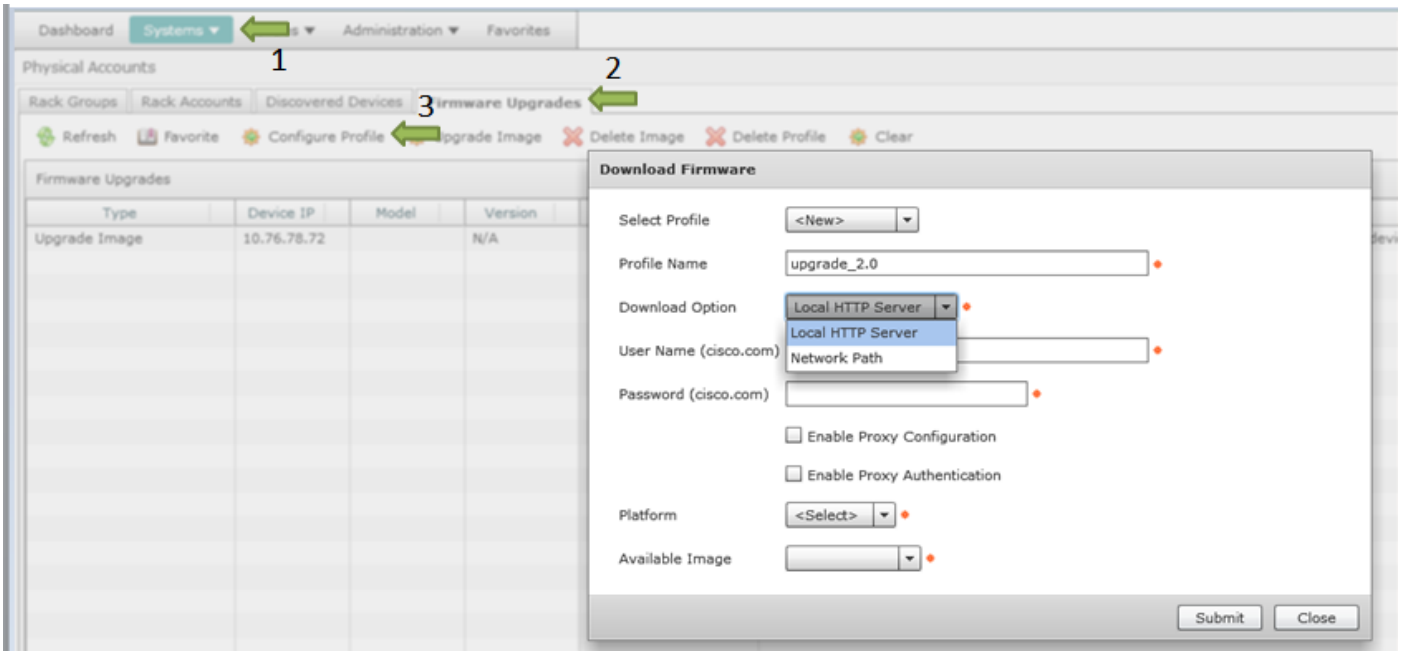
ステップ2：タブをクリック**します**。

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。

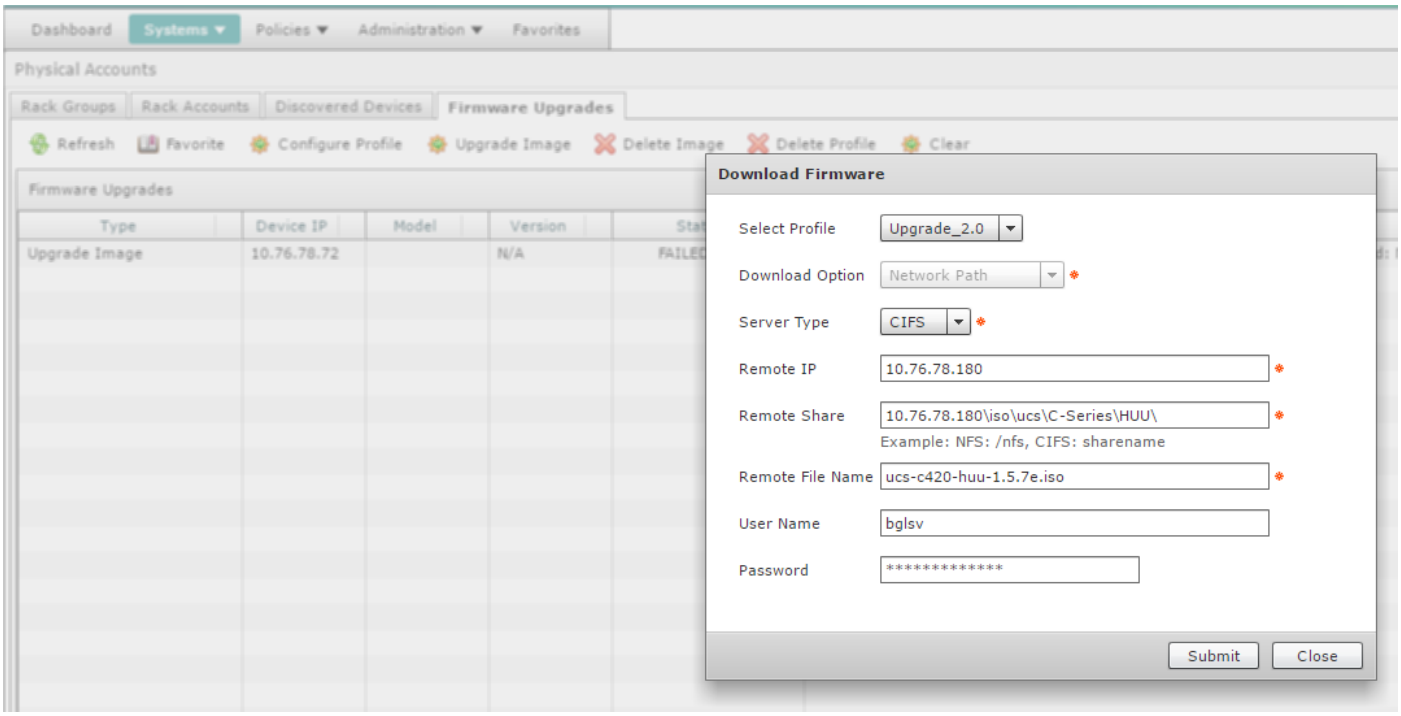
フィールド	**説明**
	ドロップダ**ウン**リストから[新規]を選択します。
フィールド	プロファイルの記述名。
ドロップダウンリスト	次のオプションのいずれかを選択します。 • ローカルHTTPサーバ：.isoイメージはローカルのCisco IMCスーバイザに保存されます。 • ネットワークパス：.isoイメージはネットワークに保存されま
フィールド	シスコのログイン ユーザ名を入力します。
フィールド	シスコのログイン パスワードを入力します。
チェックボックス	（オプション）このチェックボックスをオンにして、プロキシ設定効にし、次のフィールドに入力します。 • [Host Name]フィールド：プロキシ設定のホスト名を入力しま • [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。



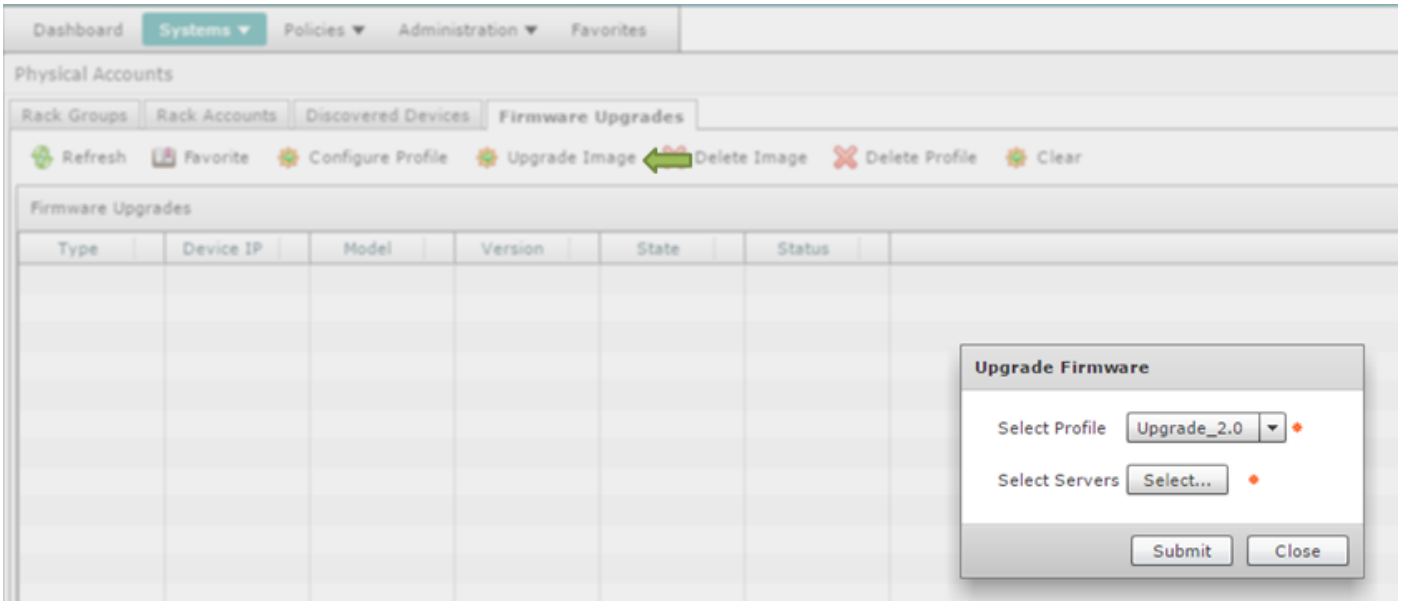
ステップ6：この例のダウンロード**オプション**として[Network Path]を選択します。（オプションとして CIFS と NFS があります。）

ステップ7：図に示すように、[**Submit**]をクリックします。



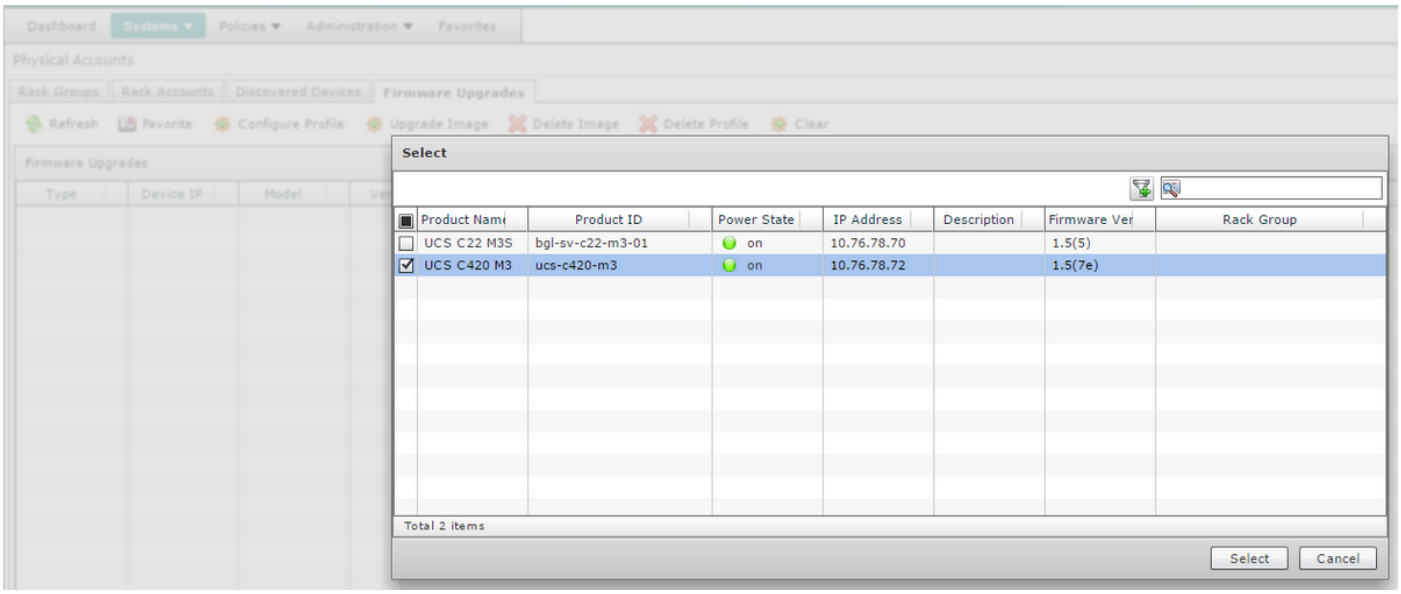
ステップ8:[Upgrade **Image**]をクリ**ックします。**

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。



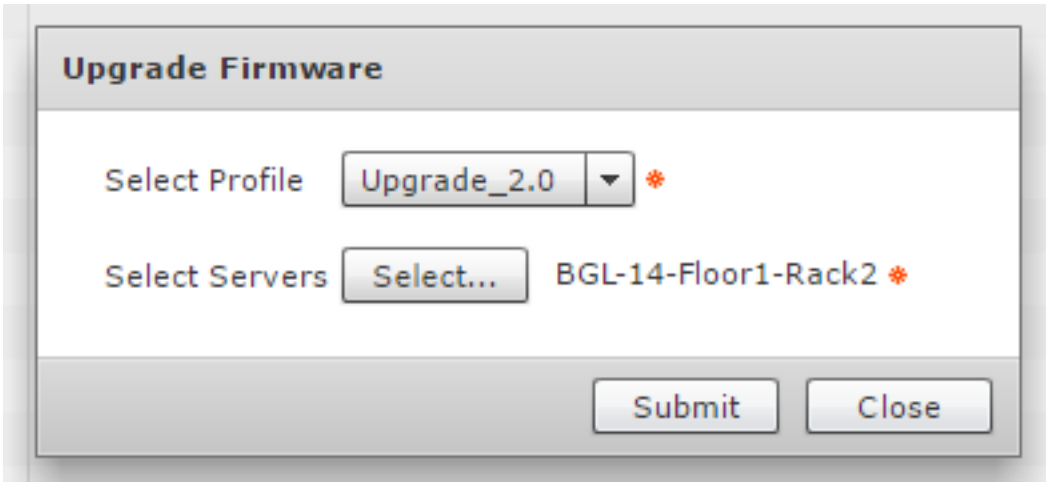
ステップ10：この例では、単一のサーバが選択されます。

ステップ11：図に示すように、[Select]をクリックします。



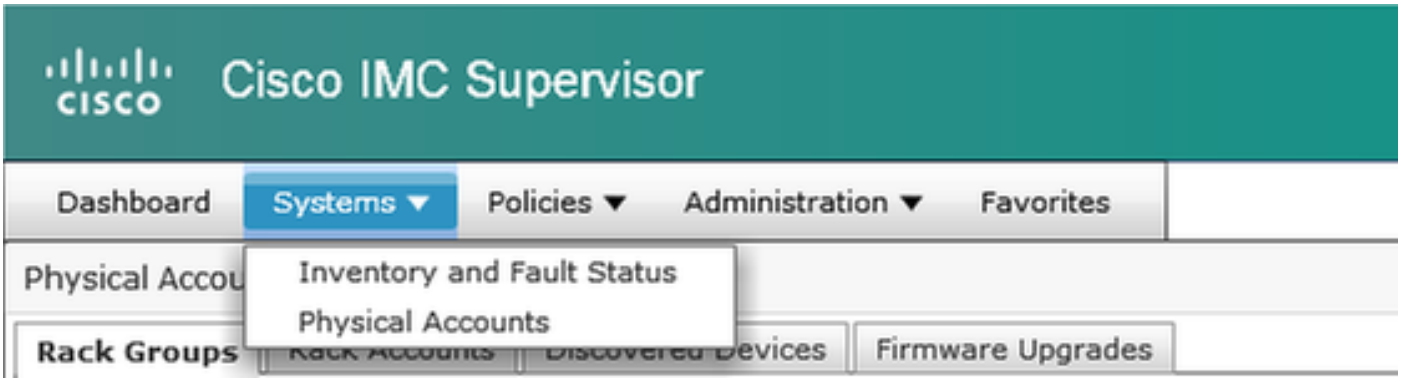
ステップ12：選択したサーバが表示されます。

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。

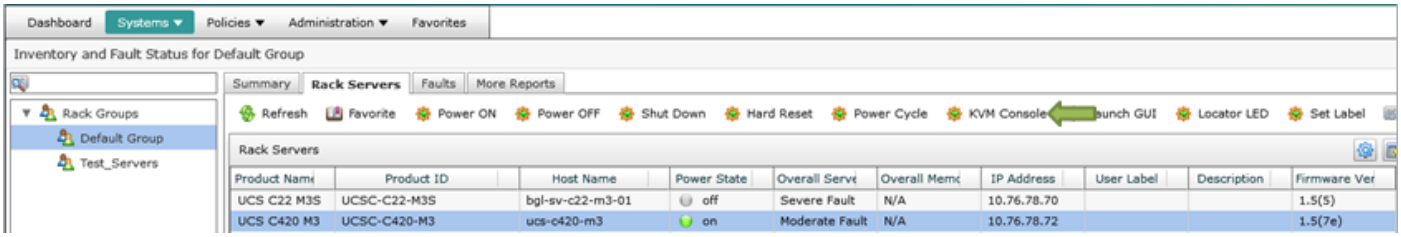


ステップ15:**[Rack Groups]**を展開し、サーバが以前に入力された適切なグループを選択します。

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す。

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。



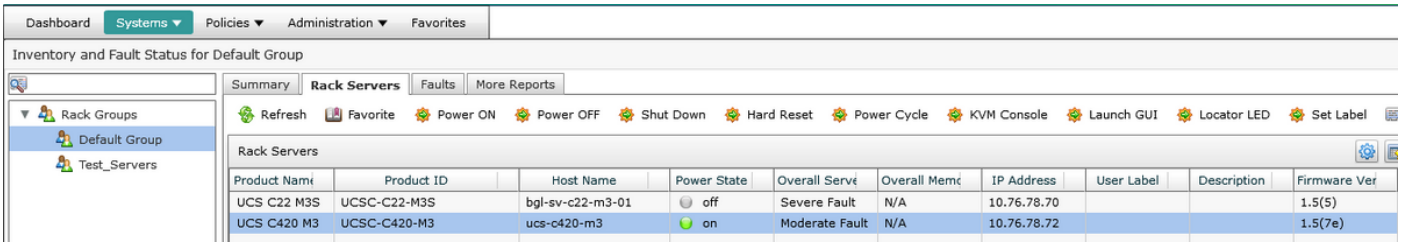
テクニカルサポートデータのリモートサーバへのエクスポート

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**。

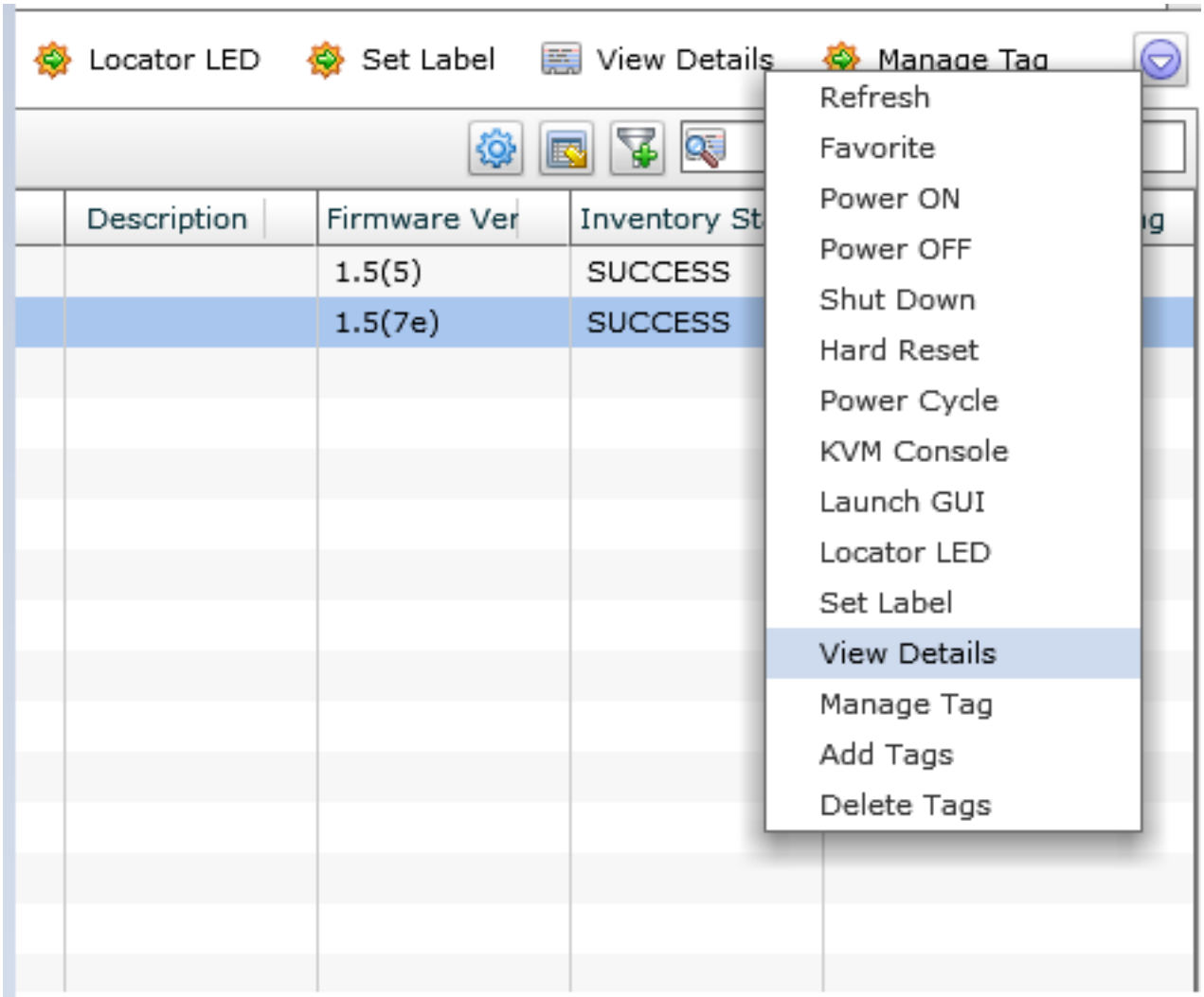
ステップ2:**[ラックグループ]を展開**し、サーバを含むラックグループを選択します。

ステップ3：図に示すように**[Rack Servers]**タブを選択します。



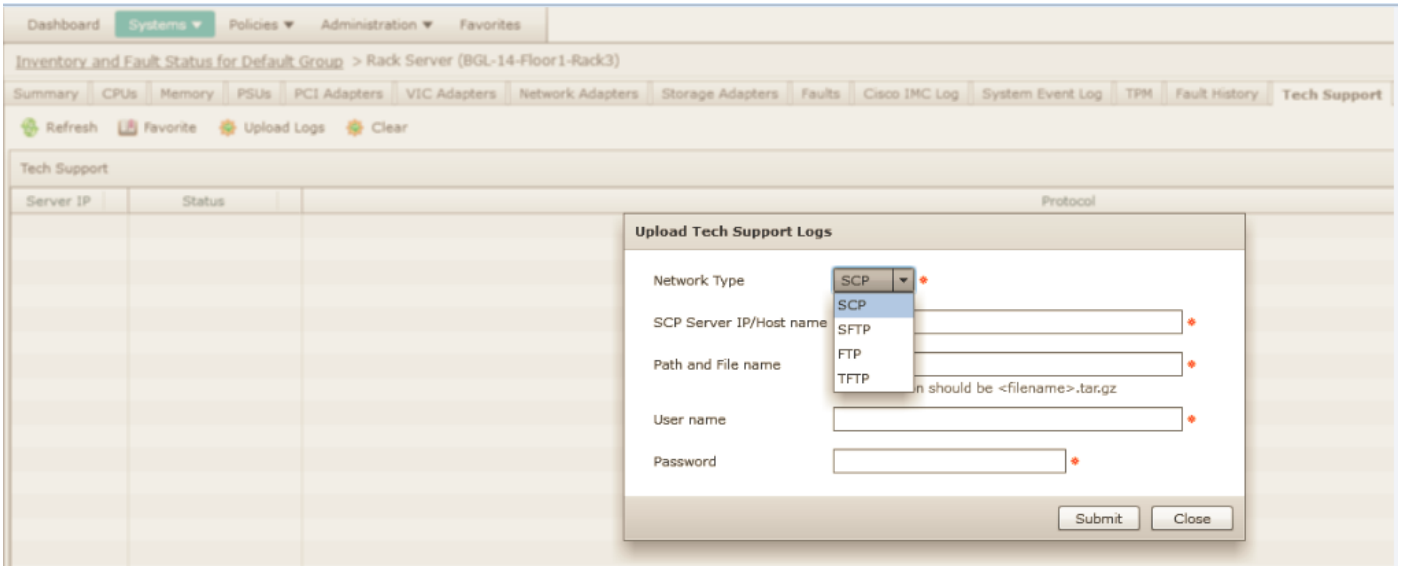
ステップ4：リストからサーバをダブルクリックして詳細を表示するか、リストからサーバをクリ

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。**



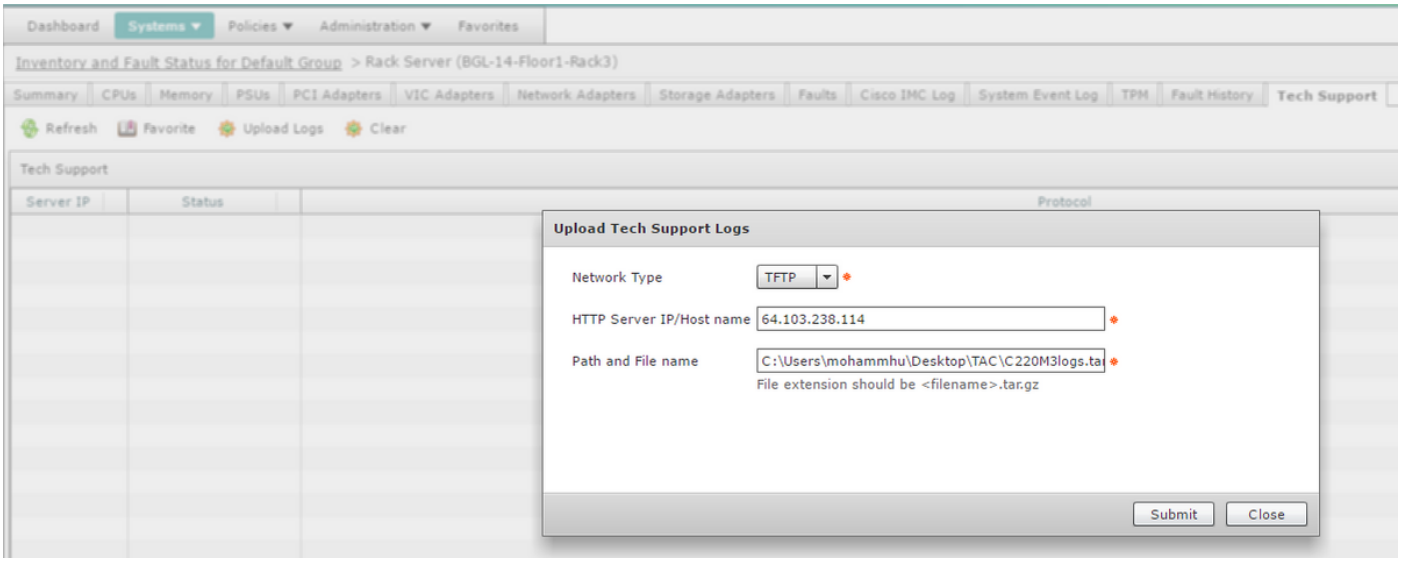
ステップ5:[Tech Support]タブを**クリックし**てください。

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。

トラブルシュート

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ありません。