VMware vSphere 5.1 搭載 FlexPod データセンターおよび Citrix CloudPlatform 4.2.1

VMware vSphere 5.X 搭載 FlexPod および Citrix CloudPlatform 4.2.1 Powered by Apache 導入ガイド

最終更新日：2014 年 2 月 5 日

Cisco Validated Design

ビジネス上の課題を解決するアーキテクチャの構築

【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。

執筆者について

Deepak Natarajan

Ramesh Kamath

Frank Zhang

Deepak、シスコ SAVBU 所属テクニカル マーケティング エンジニア

Deepak Natarajan は、シスコのデータセンター グループ（DCG）のテクニカル マーケティング エンジニアであり、データセンター ソリューションのスペシャリストです。データセンター クラウドを構築するためのアーキテクチャ デザイン、キャパシティ プランニング、アプリケーション パフォーマンスの分野で 11 年以上の幅広い経験を持っています。テクニカル マーケティング エンジニアとして、または現場支援、顧客、現場担当の立場から、さまざまな組織のコンピューティング、ストレージ、ネットワーク、クラウド管理の製品ポートフォリオを横断するクラウド ソリューションの構築に取り組み、貢献してきました。コンピュータ サイエンスの学位を取得し、Cisco Certified Network Professional（CCNA）にも認定されています。Deepak には、Cisco UCS システム、データセンター ネットワーク、NetApp ストレージ、および仮想化の領域での優れた経歴もあります。

Ramesh Kamath、NetApp 社データセンター ソリューション グループ所属テクニカル マーケティング エンジニア

Ramesh Kamath は、NetApp 社の Citrix ソリューション担当のテクニカル マーケティング エンジニアです。主に、NetApp インフラストラクチャにおける Citrix XenServer、ShareFile、および XenDesktop ベース ソリューションの開発、検証、普及に従事しています。Ramesh は、データ ストレージ業界に 6 年以上携わり、バンガロールの R V College Of Engineering で学士号を取得しています。

Frank Zhang、Citrix 社クラウド プラットフォーム グループ所属 CloudPlatform 開発者

Frank Zhang は Citrix 社の CloudPlatform の中心的な開発メンバーです。
Baremetal-as-a-Service の開発や、CloudPlatform での Cisco UCS の統合を担当しています。

謝辞

シスコ検証済みデザインの設計、検証、作成に関する支援および貢献に対し、下記の諸兄諸姉に感謝の念を申し上げます。

- Mike Brennan
- Siva Sivakumar
- Vadiraja Bhatt
- Roger Barlow
- Manan Shah
- Troy Mangum
- Abhinav Joshi
- Rachel Zhu
- David La Motta
- Kim White
- Animesh Chaturvedi
- Susan Wu
- Parth Jagirdar
- Karthick Radhakrishnan
- Sridhara C

Copyright © 2013 Cisco Systems, Inc. All rights reserved.

Cisco Validated Design（CVD）プログラムについて

CVD プログラムは、お客様による信頼性の高い、確実かつ迅速な導入を促進するために設計、テスト、および文書化されたシステムとソリューションで構成されています。詳細は次のサイトを参照してください。

http://www.cisco.com/go/designzone

このマニュアルに記載されているデザイン、仕様、表現、情報、および推奨事項（総称して「デザイン」）は、障害も含めて本マニュアル作成時点のものです。シスコおよびそのサプライヤは、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、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、シスコおよびそのサプライヤは、このデザイン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サプライヤ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。

デザイン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デザインの使用は、すべてユーザ側の責任になります。これらのデザインは、シスコ、そのサプライヤ、パートナーの技術的な助言や他の専門的な助言に相当するものではありません。ユーザは、デザインを実装する前に技術アドバイザーに相談してください。シスコによるテストの対象外となった要因によって、結果が異なることがあります。

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S.and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2013 Cisco Systems, Inc. All rights reserved.

VMware vSphere 5.1 搭載 FlexPod データセンターおよび Citrix CloudPlatform 4.2.1

要約

この『Cisco Validated Design Guide』には、Cisco Unified Computing System（UCS）と共有 NetApp ストレージに Citrix CloudPlatform 4.2.1 を導入する上でのデザイン上の考慮事項とガイドラインが記載されています。このマニュアルでは、統一プロトコル（ブロックまたはファイル）で Citrix CloudPlatform 4.2.1 を構築するために、Cisco UCS でのコンピューティング、ストレージ、ネットワークのインフラストラクチャ レイアウトをデザインする方法について説明します。このマニュアルで説明する導入シナリオは、システムの可用性と拡張性を高め、システムをクラウド環境で効果的に統合し集中管理できるように、Cisco UCS のベスト プラクティスと推奨事項に基づいています。

はじめに

世界中の企業が、現在のビジネス モデルを中断することなくクラウド コンピューティングのメリットを活かす効果的な戦略を探しています。業界がクラウド コンピューティングに乗り出した今、サービス プロバイダーと企業は、IT の総所有コストを削減し、オンデマンドのキャパシティ追加、提供サービスへのチャージバックまたはショーバック、および顧客の獲得と維持を行える能力を取得して、さらに市場シェアを拡大してゆくため、より効率的で差別化されたクラウド ソリューションを求めています。既存の投資を十分に活用し、自社のクラウドにとってできる限り最善のコンポーネントを選択できるように、ベンダーが固定されないオープンで柔軟なクラウド ソリューションが必要とされています。エンタープライズクラスのサポートとサービスを保持しながら、付加価値サービスを更新および構築するには、ソース コードとオープン API にアクセスする必要があります。顧客は、自らの環境に適したアーキテクチャとハイパーバイザを選びたいと考えています。一方で、企業は、より俊敏性に優れた柔軟なオンデマンドの IT サービスを実現できるクラウドを求めています。どちらの場合でも、クラウド サービスを構築、拡張、および管理するための適切なソリューションを必要としているのです。

この統合ソリューションは複数の基本要素から成り、具体的には、VMware ESXi 5.1 ハイパーバイザ、Citrix CloudPlatform 4.2.1、Cisco Unified Computing System、Nexus の物理および仮想スイッチ、UCS B シリーズ サーバ、Cluster Mode Data ONTAP 8.1.2 が設定された NetApp FAS 3270 ストレージなどで構成されています。これらの構成要素を組み合わせることで、シームレスなクラウド インフラストラクチャ管理システムが完成します。

リファレンス アーキテクチャでは、Cisco Nexus® 5000 シリーズ スイッチで NetApp FAS 3270 ストレージ アレイに接続された Cisco Unified Computing System™（Cisco UCS®）B200 M3 ブレード サーバ上で、VMware vSphere ESXi 5.1、Citrix CloudPlatform™ バージョン 4.2.1 powered by Apache CloudStack の設定および導入を行うためのベスト プラクティスを提案します。このソリューションでは、第 2 および第 3 世代の Cisco® UCS ハードウェアおよびソフトウェアを使用します。Citrix CloudPlatform 4.2.1 は、市場で認められた Apache CloudStack パッケージ製品を含む広範なソリューションです。Cisco UCS は、非常にスケーラブルでプログラム可能な、自動化されたクラウドに最適なインフラストラクチャです。

対象読者

このマニュアルは、ソリューション アーキテクト、セールス エンジニア、およびコンサルタントが、Cisco UCS 上で CloudPlatform Version 4.2.1 を評価、計画、デザイン、および導入する場合に役立つように作成されています。読者は、Cisco UCS、Cisco Nexus 5500 シリーズ スイッチ、Citrix CloudPlatform 4.2.1、NetApp FAS 3270 Storage、NetApp Data ONTAP 8.1.2 Cluster Mode、および関連ソフトウェアについて技術的に理解していることを前提としています。

ソリューションのコンポーネント

Citrix CloudPlatform 4.2.1 を Cisco Unified System デザインに導入するには、次のコンポーネントが必要です。

- ハードウェア コンポーネント
  - Cisco Unified Computing System
  - Cisco Nexus 5500 シリーズ スイッチ
  - NetApp FAS ストレージ システム
- ソフトウェア コンポーネント
  - VMware vSphere ESXi 5.1 Hypervisor
  - Citrix CloudPlatform 4.2.1
  - Cisco UCS Manager 2.1(2)

Cisco Unified Computing System

概要

Cisco UCS は、ブレードおよびラック サーバ コンピューティングに対する次世代のアプローチです。Cisco UCS は、コンピューティング、ネットワーク、ストレージ アクセス、仮想化を統合して 1 つのシステムにまとめる革新的なデータセンター プラットフォームであり、総所有コスト（TCO）を削減し、ビジネスの俊敏性を高めるように設計されています。このシステムでは、低遅延でロスレスの 10 ギガビット イーサネット ユニファイド ネットワーク ファブリックと、エンタープライズクラスの x86 アーキテクチャ サーバを統合しています。このシステムは、統合されたスケーラブルなマルチシャーシ プラットフォームであり、このプラットフォームのすべてのリソースは統合管理ドメインに参加します。Cisco UCS は、サーバが 1 台の場合でも、サーバが 160 台で数千の仮想マシンを持つ場合であっても関係なく、単一のシステムとして管理されるので、複雑さを伴わずに拡張できます。仮想化されたシステムと仮想化されていないシステムの両方でエンドツーエンドのプロビジョニングおよび移行をサポートし、新しいサービスの提供も容易に、確実かつ安全に進められます。

仮想化をクラウド実現のための理想的なプラットフォームにしているコンセプトの多くは Cisco UCS に適用できるので、Cisco UCS もまたクラウド展開にとって理想的です。次のような共通するコンセプトがあります。

- 完全な制御を可能にする、シングル ポイントでのインフラストラクチャ管理
- ポリシーベースのインフラストラクチャ管理
- 最適な状態をキャプチャしてその後の導入を容易にするためにテンプレートを使用
- インフラストラクチャ全体のプログラムによる制御

このデザインには、従来のアーキテクチャと比べて Cisco UCS が優れている、クラウド ソリューションのデザインおよびメンテナンスの簡略化に役立つ 3 つの鍵となる領域があります。

Cisco UCS は、デザインソリューションで上記のコンセプトを実現する次の機能を提供します。

ユニファイド ファブリック

ユニファイド ファブリックでは、すべてのネットワーク トラフィックを親ファブリック インターコネクトに渡し、そこでトラフィックに優先順位を付け、処理し、集中管理できるので、ネットワーク アダプタ、ブレード/サーバ間のスイッチ、ケーブル、および管理タッチ ポイントの数を大幅に削減できます。このアプローチは、パフォーマンス、アジリティ、および効率性を改善し、電力供給、冷却、セキュリティ保護、管理の必要なデバイスの数を大幅に低減します。

組み込みマルチロール管理

Cisco UCS Manager は、ファブリック スイッチに組み込まれている集中管理アプリケーションです。Cisco UCS は、単一の冗長な管理ドメイン内のすべての Cisco UCS 要素を制御します。これらの要素には、システム設定および操作のすべての側面が含まれるので、システム コンポーネントごとに個別の要素マネージャを複数使用する必要がなくなります。管理モジュールおよびコンソールの数と、すべてのハードウェア上の（個別に管理し更新する必要がある）常駐エージェントの大幅な削減が、Cisco UCS がもたらす重要なメリットです。Cisco UCS Manager では、ロールベースのアクセスと可視性を使用して、部門間の通信を効率的にし、データセンター ロール間でのコラボレーションを促進して、生産性を高めます。

Cisco Extended Memory Technology

Cisco Extended Memory Technology は、複数の Cisco UCS サーバの空きメモリ容量を大幅に拡張することにより、要求の厳しい仮想化および大きなデータセットのワークロードに対するパフォーマンスの増強に役立ちます。これによりデータセンターは、個々のサーバに非常に高い仮想マシン密度を導入できるだけでなく、データベースに常駐メモリ容量を提供することができます。必要なプロセッサ 2 つだけで、メモリを増やすことで大きなメリットが得られます。DIMM（Dual In-Line Memory Module）メモリ スロットが多いので、ユーザは、小型で安価な DIMM を使用してコスト効率よく容量を拡張できます。

Cisco Data Center VM-FEX 仮想化サポートおよび仮想化アダプタ

Cisco Data Center VM-FEX では、仮想マシンに、物理リンクと同様に仮想マシンを管理できる仮想リンクが用意されています。仮想リンクは集中的に設定および管理でき、従来のシステムのように仮想化環境に複数のスイッチング レイヤを介在させる複雑さはなくなります。I/O 構成およびネットワーク プロファイルは仮想マシンに付随して移行するため、複雑性が軽減され、セキュリティと効率性を向上させることができます。Cisco Data Center VM-FEX は、パフォーマンスの改善と、ネットワーク インターフェイス カード（NIC）インフラストラクチャの軽減に役立ちます。

サービス プロファイルを使用したダイナミック プロビジョニング

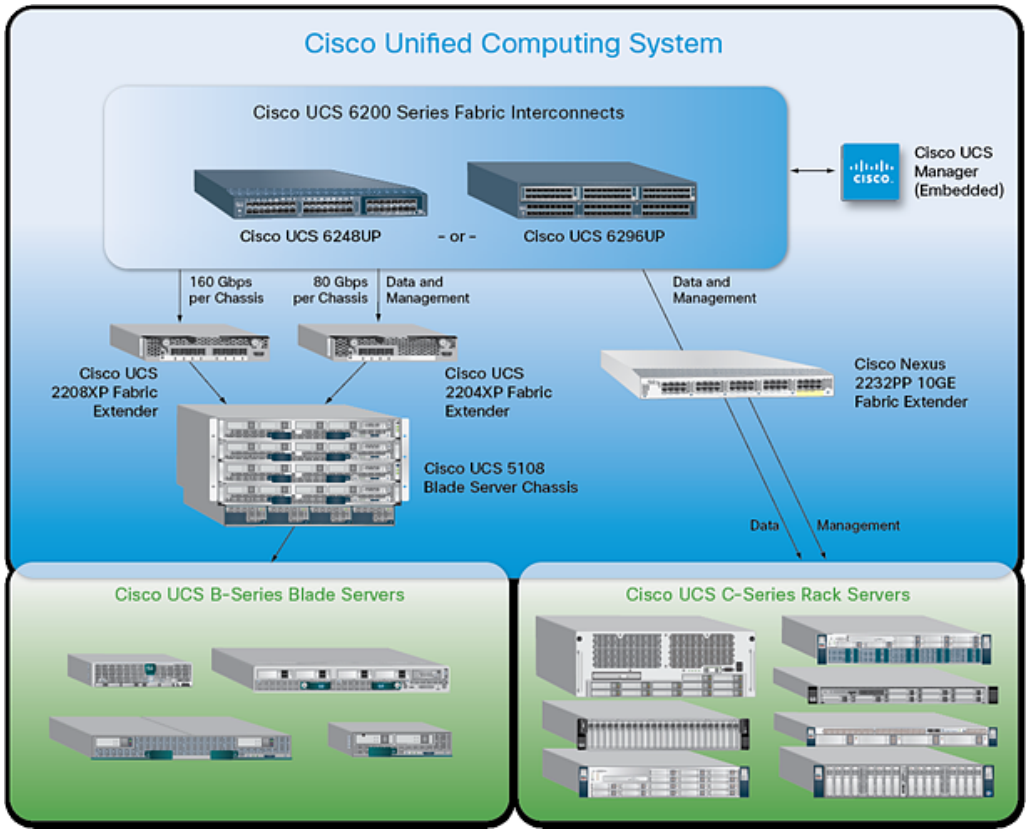
Cisco UCS Manager は、抽出されたサーバ状態情報を含んだサービス プロファイルを提供するので、サーバに関する一意の情報すべてがファブリックに保存され、物理サーバは割り当て先の別のリソースに過ぎなくなる環境ができあがります。Cisco UCS Manager は、サービス プロファイルおよびテンプレートに焦点を当てたロールベースおよびポリシーベースの管理を実装します。これらのメカニズムは、1 台または複数のサーバとそのネットワーク接続を、数時間や数日ではなく数分で完全にプロビジョニングします。

Cisco UCS のコンポーネント

この項では、UCS デザイン上の Citrix CloudPlatform 4.2.1 で使用される個々の Cisco UCS 製品について説明します。

ユニファイド ファブリックを使用した Cisco Unified Computing System™ は、ネットワーク トラフィックを親ファブリック インターコネクトに渡すことにより、必要なネットワーク アダプタ、ブレード/サーバ間のスイッチ、ケーブルの数が大幅に低減します。これらのインターコネクトがトラフィックを処理および集中管理して、パフォーマンスを高めます。また、電力供給、冷却、セキュリティ保護、および管理の必要なデバイスの数も低減します。設定および操作を管理するためにファブリック インターコネクトに組み込まれたマルチロール管理により、個別管理の必要性もなくなります。さらに、Cisco VN-Link 仮想化のサポートにより、仮想マシンに接続したネットワーク リンクには、物理リンクと同じステータスが与えられます。I/O 構成およびネットワーク プロファイルは仮想マシンに付随して移行するため、複雑性が軽減され、セキュリティと効率性を向上させることができます。この仮想ネットワーク インターフェイス カード（vNIC）機能により、パフォーマンスが向上し、NIC インフラストラクチャが低減します。

図 1　　Cisco UCS のコンポーネント



Cisco UCS ファブリック インターコネクト

Cisco UCS ファブリック インターコネクトは、Cisco UCS 全体にユニファイド ネットワーク ファブリックを作成します。ネットワークとストレージの両方への統一したアクセスを可能にするので、柔軟でプログラム可能なリソース プールに基づいて完全に仮想化された環境を導入する障壁がなくなります。Cisco ファブリック インターコネクトは、ラインレート、低遅延、ロスレスの 10 ギガビット イーサネット、IEEE データセンター ブリッジング（DCB）、および FCoE インターコネクト スイッチの

ファミリから構成されています。Cisco Nexus® 5000 シリーズ スイッチと同じスイッチング テクノロジーをベースにした Cisco UCS 6200 シリーズ ファブリック インターコネクトは、追加機能や管理機能を装備し、Cisco UCS の中枢を担っています。Cisco UCS Manager ソフトウェアは、Cisco UCS ファブリック インターコネクト内部で動作します。Cisco UCS 6100 シリーズ ファブリック インターコネクトは、Cisco UCS ネットワーク ポートフォリオを拡張し、容量の増加、ポート密度の上昇、および電力消費の低減を実現しています。これらのインターコネクトが、Cisco UCS B シリーズ ブレード サーバおよび Cisco UCS ブレード サーバ シャーシの管理および通信のバックボーンとなります。インターコネクトに接続したすべてのシャーシとすべてのブレードは、可用性の高い単一の管理ドメインに属しています。Cisco UCS 6100 シリーズでは、ユニファイド ファブリックをサポートすることによって、設定時にドメイン内のすべてのブレードで LAN 接続と SAN 接続をサポートするという柔軟性が得られます。Cisco UCS ファブリック インターコネクトは通常、冗長ペアで導入され、ネットワークとストレージの両方へのアクセスを統一し、完全に仮想化された環境を促進します。

Cisco UCS ファブリック インターコネクトのポートフォリオは現在、Cisco 6100 および 6200 シリーズ ファブリック インターコネクトから構成されています。このデザインでは、Cisco 6248UP FI を使用しています。

- Cisco UCS 6248UP 48 ポート ファブリック インターコネクト

  Cisco UCS 6248UP 48 ポート ファブリック インターコネクトは、1 ラック ユニット（1 RU）の 10 ギガビット イーサネット、IEEE DCB、および FCoE インターコネクトであり、低遅延で 1 テラバイト/秒（Tbps）以上のスループットが可能です。32 のファイバ チャネル固定ポート、10 ギガビット イーサネット、IEEE DCB、および FCoE Enhanced Small Form-Factor Pluggable（SFP+）ポートを備えています。

1 つの拡張モジュール スロットにより、さらに最高 16 のファイバ チャネル、10 ギガビット イーサネット、IEEE DCB、および FCoE SFP+ ポートを追加できます。

Cisco UCS ファブリック エクステンダ

Cisco UCS 2100 および 2200 シリーズ ファブリック エクステンダは、シャーシ内のブレード サーバのすべてのトラフィックを多重化し、10 Gbps のユニファイド ファブリック リンクを介して親 Cisco UCS ファブリック インターコネクトに転送します。同じシャーシ上のブレード間や同じブレード上の仮想マシン間のトラフィックを含め、すべてのトラフィックは親インターコネクトに転送され、ネットワーク プロファイルはそこでファブリック インターコネクトによって効率的および効果的に管理されます。Cisco UCS ファブリック エクステンダの中核には、すべてのトラフィックを多重化する特定用途向け集積回路（ASIC）プロセッサがあります。

最高 2 台のファブリック エクステンダをブレード シャーシに配置できます。このデザインでは、Cisco UCS 2208XP ファブリック エクステンダが配置されています。

- Cisco UCS 2208XP ファブリック エクステンダ

  ファブリック インターコネクトにブレード シャーシを接続する 8 つの 10 ギガビット イーサネット、FCoE 対応、SFP+ ポートを備えています。それぞれの Cisco UCS 2208XP には 32 の 10 ギガビット イーサネット ポートが装備され、ミッドプレーンを通じてシャーシ内の各ハーフ幅スロットに接続しています。2 台のファブリック エクステンダは通常、冗長性のためにペアで設定され、シャーシに最高 160 Gbps の I/O をもたらします。

Cisco UCS 仮想インターフェイス カード

Cisco UCS VIC 1240 および 1280 により、ポリシーベースでステートレス、かつ俊敏性に優れたサーバ インフラストラクチャが実現します。PCI Express（PCIe）標準準拠のインターフェイスを最大 256 個までホストに提供可能で、NIC または HBA として動的に構成できます。さらに、Cisco UCS VIC 1280 は、Cisco UCS ファブリック インターコネクトのポートを仮想マシンまで拡張する Cisco Data Center VM-FEX テクノロジーをサポートしているため、サーバ仮想化の導入が容易になります。

- Cisco UCS VIC 1240

シスコが提供する革新的な Cisco UCS 仮想インターフェイス カード（VIC）1240 は、M3 世代の Cisco UCS B シリーズ ブレード サーバ専用デザインである 4 つの 10 ギガビット イーサネット ポートを備えた、FCoE 対応のモジュール型 LAN on Motherboard（mLOM）です。Cisco UCS VIC 1240 の機能は、オプションのポート エクスパンダと組み合わせて使用することにより、10 ギガビット イーサネット ポートを 8 つまで拡張できます。

- Cisco UCS VIC 1280

  シスコが提供する革新的な Cisco UCS VIC 1280 は、Cisco UCS B シリーズ ブレード サーバ専用デザインである、8 つの 10 ギガビット イーサネット ポートを備えた、FCoE 対応のメザニン カードです。

Cisco UCS 5100 シリーズ ブレード サーバ シャーシ

Cisco UCS 5108 ブレード サーバ シャーシは、最高 8 台のハーフ サイズの Cisco UCS B シリーズ ブレード サーバ、または最高 4 台のフル サイズの Cisco UCS B シリーズ ブレード サーバ、あるいはこれらを組み合わせて収容できる 6 ラックユニットのブレード シャーシです。Cisco UCS 5108 は、自動ロード シェアリングおよびフェールオーバー機能を備えた冗長電源を 4 基と、Cisco UCS 2100 または 2200 シリーズ ファブリック エクステンダを 2 台収容できます。このシャーシは、Cisco UCS シャーシ管理コントローラで管理されます。このコントローラは、Cisco UCS ファブリック エクステンダ内に取り付けられ、Cisco UCS Manager と連動してシャーシおよびそのコンポーネントを制御します。

理論上は単一の Cisco UCS 管理ドメインで、最高 40 台の個別のシャーシと 320 台のブレード サーバまで拡張できます。この場合、Cisco UCS は最高 20 台の個別のシャーシと 160 台のブレード サーバをサポートします。

10 Gbps ユニファイド ネットワーク ファブリックに基づいて I/O インフラストラクチャを構築することにより、Cisco UCS には、単純だが総合的な I/O オプション セットを伴う合理化されたシャーシが実現します。その結果、シャーシの基本コンポーネントは次の 5 つだけになります。

- パッシブ ミッドプレーンとアクティブ環境モニタリング回路を備えた物理的なシャーシ
- 背面に電力入力が設けられた 4 つの電源ベイと、前面パネルからアクセスできるホットスワップ可能な電源ユニット
- それぞれ 2 つのファンを備えた、ホットスワップ可能な 8 つのファン トレイ
- 背面パネルからアクセス可能な 2 つの Cisco UCS ファブリック エクステンダ スロット
- 前面パネルからアクセス可能な 8 つの Cisco UCS ブレード サーバ スロット

Cisco UCS B200 M3 ブレード サーバ

Cisco UCS B200 M3 ブレード サーバは、妥協することなくパフォーマンス、汎用性、および高密度を提供します。IT および Web インフラストラクチャから分散データベースまで、最も広範なワークロード セットに対処します。定評のある Cisco UCS B200 M2 ブレード サーバを基盤とするエンタープライズクラスの Cisco UCS B200 M3 ブレード サーバは、ハーフ幅のブレード フォーム ファクタ内で Cisco UCS ポートフォリオの機能をさらに拡大します。Cisco UCS B200 M3 は、最新の Intel Xeon プロセッサ E5-2600 製品ファミリの能力を活用し、最高 384 GB の RAM（16 GB DIMM を使用）、2 基のディスク ドライブを搭載でき、最高デュアル 4x 10 ギガビット イーサネットのスループットを実現できます。さらに、Cisco UCS には、各ブレード シャーシ内のスイッチへの給電と冷却が不要になるという構造上の利点もあります。シスコは、ブレード サーバごとの電力バジェットを拡大することによって、妥協のない拡張性と機能性を備えたブレード サーバを設計することができ、これは、業界随一のメモリ スロットとドライブ容量を備えた新しい Cisco UCS B200 M3 で実証されています。

Cisco Nexus 5500 シリーズ スイッチ

データセンター環境用にデザインされた Cisco Nexus 5000 シリーズ スイッチには、一貫性のある低遅延のイーサネット ソリューションを可能にするカットスルー テクノロジーが採用されています。前面から背面、または背面から前面へ冷却するデザインで、データ ポートも背面にあるため、サーバの近くに設置してケーブル配線を短くシンプルにまとめることもできます。また、ホットプラグ可能な冗長電源とファン モジュールを備えているため、保守にも優れています。OS にはデータセンター クラスの Cisco NX-OS ソフトウェアを採用し、高い信頼性と容易な管理を実現します。

このスイッチは、高密度、低遅延のマルチレイヤ サービスに向けた革新的進歩を実現するために、専用の 10 ギガビット イーサネットのデータセンター クラス スイッチである Cisco Nexus 5000 シリーズの業界トップクラスの汎用性をさらに拡張しています。Cisco Nexus 5500 シリーズ スイッチは、さまざまな物理環境、仮想環境、ストレージ アクセス環境、およびハイパフォーマンス コンピューティング（HPC）のデータセンター環境における、エンタープライズ データセンターのサーバ アクセス レイヤへの導入に適しています。

- Cisco Nexus 5548UP

  Cisco Nexus 5548UP は、1 ラックユニットの 10 ギガビット イーサネット（10 GE）、ファイバ チャネル（FC）、Fibre Channel over Ethernet（FCoE）スイッチで、最高 960 Gbps のスループットと最高 48 のポートを実現します。このスイッチには 32 のユニファイド ポートと 1 つの拡張スロットがあり、10 ギガビット イーサネットおよび FCoE ポートを備えたモジュール、または 8/4/2/1 Gbps のファイバ チャネル スイッチ ポートを備えたファイバ チャネル SAN への接続、あるいはその両方をサポートします。

NetApp ストレージ

NetApp FAS3270 は、現在の多様な仮想化されたワークロードを処理し、将来の拡張にも簡単に対応できます。NetApp FAS3270 シリーズはコスト効率よく、仮想環境と従来の環境の両方でビジネス アプリケーションからの強力なニーズを満たします。仮想環境での要求の厳しいビジネス アプリケーションにとって理想であり、NetApp FAS3270 の非常に効率的なストレージの使用によって、raw ストレージ、電力、冷却、およびスペースの消費を大幅に削減します。

NetApp FAS3270 は、FC、FCoE、IP SAN（iSCSI）、NFS、CIFS、HTTP、FTP ストレージ ネットワークをサポートします。Alternate Control Path（ACP）、イーサネットベースのサービス プロセッサ、Data ONTAP 管理インターフェイスなどの高可用性機能を提供し、ホットスワップ可能で冗長なコントローラ、冷却ファン、電源、および光モジュールを備えています。さらに、コントローラ フェールオーバーとマルチパス HA ストレージによるアクティブ-アクティブ コントローラや、ストレッチ（スイッチレス）とファブリック接続した MetroCluster V-Series Storage Acceleration Appliance SA320 によるアクティブ-アクティブ コントローラなどの、高可用性コントローラ設定をサポートします。

VMware vSphere ESXi 5.1

仮想化は、単一の物理サーバ上で複数の仮想マシンを実行できるようにする実績のあるテクノロジーです。それぞれの仮想マシンは、他のマシンから完全に分離され、基盤となるホストとは、ハイパーバイザと呼ばれるソフトウェアのシン レイヤによって切り離されています。このため、それぞれの仮想マシンで異なるオペレーティング システムおよびアプリケーションを実行することが可能になります。マシンは基盤のホストから切り離されているので、ゲストをある物理サーバ ホストから実稼働環境または開発環境の別のサーバ ホストに移動させることができます。これはライブ マイグレーションと呼

ばれています。このような特質によって、仮想コンピューティングに対する組織のアプローチが変容してきました。VMware が提供する幅広い製品は、進化の著しい IT インフラストラクチャのビジネスニーズに対応しています。

ESXi 5.1 は、強力な vSphere ハイパーバイザに基づいて構築された、完全な管理サーバ仮想化プラットフォームです。ESXi テクノロジーは、業界で最も高速でセキュアな仮想化ソフトウェアとして広く認められています。ESXi は仮想サーバを効率的に管理し、サーバを経済的に統合して、ビジネスの継続性を確保できます。

Citrix CloudPlatform 4.2.1

Citrix CloudPlatform powered by Apache Cloudstack は、単一のユニファイド クラウド管理プラットフォーム内で、既存のスケールアップ エンタープライズ ワークロードと、スケールアウト クラウドネイティブ アプリケーション ワークロードの両方を確実に統合できることが実証された、将来性のある唯一のアプリケーション中心のクラウド ソリューションです。Citrix CloudPlatform は、CRM や ERP などのエンタープライズ ワークロードに最適なプライベート クラウド基盤を、ソーシャル アプリケーション、ビッグ データ、HPC などのクラウドネイティブ アプリケーション ワークロードに適した真の Amazon スタイルの規模、弾力性、および業務の効率化と組み合わせます。

CloudPlatform 4.2.1 を使用したスケールアップおよびスケールアウト ワークロードの有効化

Citrix CloudPlatform は、テナントが、低コストの分散インフラストラクチャで高いパフォーマンスと大量の並行ワークロードに対応できる、ワークロード固有のアベイラビリティ ゾーンおよびリージョンを作成できるようにします。企業は、クラス最高の仮想化およびネットワークで複雑なエンタープライズ ワークロードを実行して、真のプライベート クラウドの分離を実現し、ミッション クリティカルなワークロードを実行するための SLA、コンプライアンス、セキュリティ、および可用性を確保できます。クラウドネイティブ アプリケーション ワークロードを配信している組織の場合、Citrix CloudPlatform なら、パブリック クラウドでもプライベート クラウドでもリージョンあたり 40,000 以上のホストを収容できる実証済みの拡張性があるので、可用性、ストレージ、およびネットワークを顧客に提供することができます。

専用プライベート クラウドの分離

クラウド インフラストラクチャ レイヤ（ゾーン、Pod、クラスタ、およびホスト）と、仮想マシン リソース（CPU、メモリ、ストレージ、およびネットワーク）は、真のマルチテナント プライベート クラウドを導入するために、分離されたさまざまな論理パーティションに細かくグループ化できます。コンプライアンス、セキュリティ、およびパフォーマンスの要件を満たすために、仮想プライベート クラウドの使用例をサポートするように専用リソースを任意のインフラストラクチャ レイヤに適用することができます。

論理的な分離

企業は CloudPlatform を使用して、アベイラビリティ ゾーンまたリージョン（それぞれは 1 つまたは複数の物理的なデータセンター内のリソースから構成されます）を含む複数の個別の論理的な抽象化レイヤにプライベート クラウドを編成できます。CloudPlatform は、ドメイン、サブドメイン、アカウント、およびユーザを含む論理的なユーザ分離階層を使用します。使用量のクォータを階層内のどのレイヤにでも適用できます。この論理的な分離階層を使用して、ドメイン内の通常の企業における組織構造をモデル化して事業単位を表すことができます。また、チームを表すアカウントにユーザをグループ化することもできます。サブドメインを、より大きな事業単位における区分として表すこともできます。

アカウントが個々の顧客を表すことのあるサービス プロバイダーの状況にも、同じ分離階層を適用できます。CloudPlatform は、すべてのメモリ、CPU、ネットワーク、およびストレージ リソースを利用可能にしながらユーザ アカウントごとに分離できるようにします。

リージョン

クラウド管理者は、複数のゾーンまたはデータセンターから構成されるアベイラビリティ リージョンを定義できます。リージョンを実装するメリットは、拡張性と可用性、地理的な可用性が高まり、遅延がより低くなり、企業コンプライアンスが確保されることです。リージョンは、同じテンプレートから複数のアベイラビリティ ゾーンにわたって、アプリケーション ワークロードを起動し導入できるようにします。サービスをサポートする VM が複数のゾーンで実行されるので、あるゾーンに障害が発生した場合でも、アプリケーションの可用性は影響を受けません。

ハイパーバイザを限定しない

CloudPlatform は、Citrix® XenServerTM、VMware® vSphere® Oracle® VM（OVM）、KVM など、商品としてサポートされる業界随一のハイパーバイザをサポートしています。ハイパーバイザを使用しないベア メタル インフラストラクチャもサポートされます。顧客は、単一のベンダーによるテクノロジーに縛られずに、自らのワークロードに適した 1 つまたは複数のハイパーバイザを自由に選択できます。

従来のアプリケーション アベイラビリティ ゾーンは通常、VM のライブ マイグレーションをサポートする VMware® vSphere や Citrix XenServerTM など、ベア メタルまたはサポート対象のハイパーバイザから始まります。CloudPlatform には、2 層のストレージ階層があります。ルートおよびデータ ボリュームは、パフォーマンスのために通常はホスト ローカル ストレージ、FC、iSCSI、または NFS 上に置かれるプライマリ ストレージ層に保存されます。VM テンプレートおよびボリューム スナップショットは、通常は NFS またはオブジェクト ストレージに置かれるセカンダリ ストレージ層に保存されます。

仮想マシンの操作および管理

CloudPlatform では、作成やメンテナンスなどの仮想マシンのライフサイクル管理を単一のプラットフォーム下で効率的に行います。ルートおよびデータ ボリュームは、プライマリ ストレージ層に置かれ、VM の作成時に作成されます。VM が破棄されると、ルート ボリュームも破棄されます。VM に接続されたデータ ボリュームの場合、VM が破棄されるときにこれらのボリュームは破棄されません。したがって、管理者は、ボリュームのスケジュールされたスナップショットまたはアドホックなスナップショットを取得して、バックアップまたはデータ リカバリのために設定状態を保持できます。セカンダリ ストレージ層のゾーンまたはリージョンで、OS および ISO テンプレートをインポート、作成、保存でき、ストレージ効率を最適化できます。

高度な VMware の統合

仮想化は、過去 10 年にわたり、企業やサービス プロバイダーに広範に採用されています。CloudPlatform が VMware® vCenter® と統合することによって、組織は、データセンターからクラウドにエンタープライズ ワークロードをシームレスに移動させることができ、既存の VMware への投資、設定、および専門知識を引き続き活用することができます。仮想ハードウェアのホット アド、vMotion®、VMware HA & DRS、Storage vMotion、CPU および RAM の過大割り当てなどの vCenter® の機能がすべて、CloudPlatform で有効化されています。CloudPlatform は、VMware の dvSwitch および PVLAN 機能を活用して、同じネットワーク上でのさらなるネットワーク セグメンテーションと VM 分離を実現します。追加のストレージ統合によって、VM レベルのスナップショットとボリューム レベルのスナップショットが可能になります。

セキュリティ グループを使用したゲストの分離

ゲスト インスタンスには、同じゾーン内で実行する他のインスタンスからの分離が必要です。ゲスト VM がネットワークを介して互いに通信する必要がある場合、CloudPlatform には、セキュリティ グループと VLAN という 2 つの分離モードが用意されています。セキュリティ グループは、ベーシックとアドバンスド ネットワーキング モデルの両方で実装できますが、VLAN はアドバンスド ネットワーキングでのみ使用できます。アドバンスド ネットワーキングでは、クラウド管理者は、さまざまなアカウントにカスタム IP 範囲を提供できます。ベーシック ネットワーキング セットアップでは、ゲスト インスタンスは、基盤の CloudPlatform およびハイパーバイザ アーキテクチャと同じ IP 範囲を使用します。

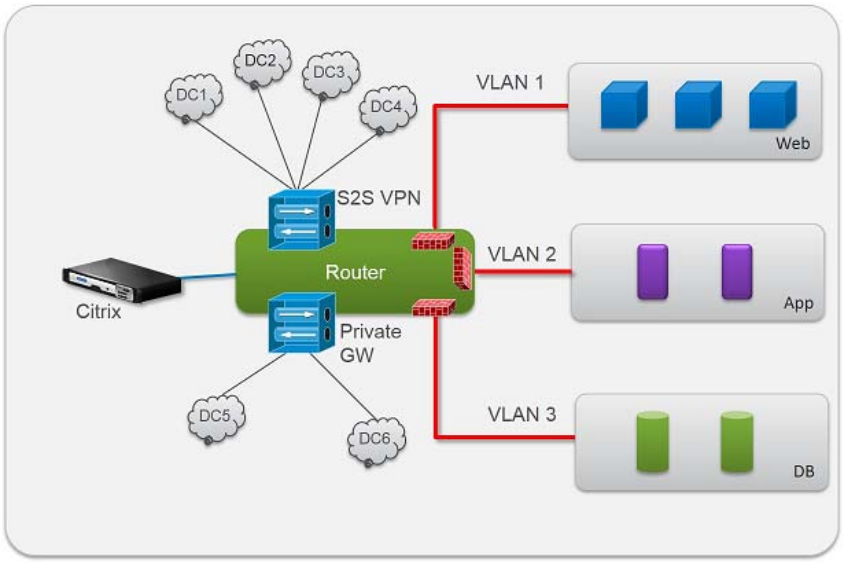
セキュリティ グループを使用する場合、自動的に作成されるデフォルトのセキュリティ グループがそれぞれのアカウントに割り当てられます。新しいインスタンスが作成されると、1 つまたは複数のセキュリティ グループに割り当てられます。ユーザは、いつでも追加のセキュリティ グループを作成できます。ゲスト インスタンス間の通信は、同じセキュリティ グループに割り当てられている場合にのみ行えます。セキュリティ グループでイングレスとイーグレス ルールを使用して、グループで送受信されるトラフィックのフローを制御します。

仮想プライベート クラウド

仮想プライベート クラウド（VPC）は、CloudPlatform 内のリソースをグループ化してプライベートに分離したものです。従来のデータセンターにおける企業アプリケーションには、データベースへの接続、ロード バランシング、およびファイアウォールのためにネットワーク層が接続しています。VPC では、従来の物理ネットワークに類似した独自の仮想ネットワーク トポロジを使用できます。

クラウド管理者は、VPC 機能を使用してプライベート アドレスを含む仮想ネットワーク内で VM を起動して、IP 範囲や VLAN など、従来の企業アプリケーションのネットワーク アーキテクチャを再現することができます。IP アドレス範囲やネットワーク層定義に基づいて同種のインスタンスをグループ化する機能により、データセンターのクラウド コンピューティングへの変容が容易になります。従来のアプリケーション用にネットワークを細かくセグメント化するなどの従来の企業ネットワーク トポロジを再現することにより、クラウド コンピューティングへの遷移を単純化できます。

図 2　　n 階層アプリケーション



従来のマルチティア アプリケーションでは、ネットワーク隔離の構成とトラフィック フローの修正に VLAN が以前から使用されてきました。上記のマルチティアの例では、アプリケーションは、Web フロント エンド層、アプリケーション層、データベース層から構成されます。各層は、個々の VLAN によって分離されています。大規模な導入の場合、管理者は Citrix CloudPlatform でこの n 階層アプリケーション アーキテクチャを使用して、ネットワーク、ルーティング、ファイアウォール、およびロード バランシングの細かなポリシーを作成したり、個々の階層に対してアフィニティ /反アフィニティ ルールを作成します。

アドバンスド クラウド ネットワーキング

クラウド オペレータは、Portable IP 機能、グローバル サーバ ロード バランシング（GSLB）、AWS ライクなヘルス チェックなどのアドバンスド クラウド ネットワーキング設定および Network-as-a-Service オファリングを作成して、アプリケーションの可用性を確保できます。さらに、CloudPlatform には、DHCP、Network Address Translation（NAT）、ロード バランシング、ファイアウォール、およびポート フォワーディングなどのネットワーク サービスを細かく制御する仮想ルータが組み込まれています。

CloudPlatform は、エンタープライズ クラスのアプリケーション デリバリ コントローラ（ADC）と統合して、サーバのロード バランシングを行います。ADC で見られる圧縮、接続の多重化、キャッシング、および SSL オフロードなどの高度な機能は、負荷のかかり過ぎたネットワークおよびサーバから負荷を軽減する際にますます役立つようになり、アプリケーションの可用性を増大させています。CloudPlatform は、Citrix Netscaler®、F5 ロード バランサ、Cisco ハードウェアおよびソフトウェア（UCS、Nexus 1000v、ASA1000v）、Juniper ファイアウォール、および VMware Distributed Virtual Switch など、ADC およびネットワーキング デバイスの広範なエコシステムをサポートしています。アーキテクチャ、規模、SLA、ロード バランシングに関するアドバンスド ネットワーキングの要件は、最も要求の厳しいクラウドネイティブ アプリケーションのワークロードおよび可用性の要件に最適なネットワーキング ソリューションを使用して満たすことができます。

特に、複数のサイトにわたるトラフィックの分散を可能にし、ディザスタ リカバリの管理に役立つ Citrix NetScaler グローバル サーバ ロードバランシング（GSLB）機能が CloudPlatform を通じて有効化されます。GSLB では、分散インターネット環境で最もパフォーマンスのよい GSLB サイトに DNS 要求を転送することにより、システムが着信クライアント要求をルーティングする方法を制御します。事前に定義された NetScaler ポリシーと設定を CloudPlatform で統合して、トラフィックを送信することができます。たとえば、最も近いアベイラビリティ ゾーン、遅延が最低または負荷が最低量のリージョン、または停止の場合にはセカンダリ データセンターにトラフィックを転送するようにポリシーで指定できます。

Citrix Netscaler などのインテリジェントなロード バランサは、CloudPlatform を通じてバックエンド サービスの AWS スタイルのヘルス チェックを実行するように設定できます。NetScaler は、モニタ対象の一連のサービス レベル パラメータに基づいて、バックエンド サービスに対し定期的なチェックを実行します。VM がヘルス チェックに失格すると、Citrix Netscaler は自動的に VM をロード バランサプールから削除し、接続要求を正常な VM にのみルーティングします。VM がヘルス チェックに再び合格すると、ロード バランサは VM をリソース プールに元どおり追加します。

CloudPlatform と Citrix NetScaler を組み合わせると AutoScale テクノロジーを使用でき、ビジネスの需要に応じて自動的にクラウドを拡張および収縮できるようになります。Citrix Netscaler には、CPU 使用量、サーバ ヘルス、またはアプリケーションの応答性をモニタする機能があります。CloudPlatform と連動した場合、アプリケーションの負荷の変化によって、対応するバックエンド サービスまたはゲスト VM を拡大または縮小するように Citrix Netscaler に要求できます。

Citrix NetScaler は、物理アプライアンスとして設定するか、Citrix XenServer 上で稼働する仮想マシンとして設定するかを選択できます。CloudPlatform は Citrix NetScaler を他のインフラストラクチャ リソースと同様に取り扱うので、リソース プールに追加できます。

オブジェクト ストレージ

オブジェクト ストレージを利用するクラウドネイティブ アプリケーション ワークロードは、地理的および論理的に定義された場所にわたるストレージ オブジェクトに透過的にアクセスできます。リージョン内または複数のゾーンにわたるオブジェクト ストレージにアクセスできるので、ワークロードの可用性と操作効率が向上します。オブジェクト ストレージは、ゾーンの障害があった場合に、永続的データの保存に使用できます。また、同じオブジェクト ストレージで、Infrastructure-as-a Service および Storage-as-a-Service 用のセカンダリ ストレージを確保することもできます。

Cisco と Citrix：実稼働クラウドに望ましい組み合わせ

200 以上のクラウドを稼働している Citrix CloudPlatform は、世界で最も要求の厳しいワークロードを統合する信頼性の高いクラウド管理プラットフォームです。Bell Canada、BT、COLT、サンパウロ大学などの主要な通信企業や高等教育機関から Edmunds.com などの Web 中心の企業に至る幅広い組織で、クラウドの運用と拡張に Cisco UCS と Citrix CloudPlatform が選ばれてきました。

Cisco UCS Manager

Cisco UCS Manager は、Cisco UCS をシングル ポイントで管理する、統合された管理マネージャです。Cisco UCS Manager には、直感的な GUI、コマンドライン インターフェイス（CLI）、または包括的なオープン XML API からアクセスできます。サーバやストレージの物理的なアセットおよび LAN 接続を管理し、複数の主要ハイパーバイザ ベンダーとの統合を通じて仮想ネットワーク接続の管理を簡略化するように設計されています。IT 部門はこのマネージャを使用して、ユーザがシステム全体を管理できるようにすることも、サーバ、ストレージ、またはネットワーク ハードウェア アセットのマネージャとしての各自のロールに基づいて特定の管理機能を個々のユーザに割り当てることもできます。システムで使用できるすべてのコンポーネントを自動的に検出し、リソース使用のステートレス モデルを有効化することによって、操作を簡略化します。

Cisco UCS Manager が管理する要素は次のとおりです。

1. CloudPlatform は、UCS コンバージド インフラストラクチャのプログラマビリティを活用することによって、クラウドを簡単に拡張できるようにするために、サービスとしてベア メタル ホストをプロビジョニングできるようにします。CloudPlatform は、UCS 環境、サーバ プロファイルなどを自動的に把握できる UCS プラグインを提供するので、CloudPlatform 管理者は、Cisco UCS システム上にベア メタル OS を導入できます。UCS を CloudPlatform と併用するための手順の概要は次のとおりです。
2. Cisco のマニュアルに従って、Cisco UCS ブレード サーバ、プロファイル、および Cisco UCS Manager を設定する
3. Cisco UCS Manager を CloudPlatform に登録する
4. サービス プロファイルを UCS ブレードに関連付ける
5. 記述に従って、ベア メタル ホストとしてブレードをプロビジョニングする

リファレンス アーキテクチャ

この項では、プライベート クラウド導入を構築するために Citrix CloudPlatform と組み合わせた NetApp ストレージ上での VMware ESXi 5.1 の仮想化を使用した Cisco UCS のネットワーキングおよびコンピューティングに関する物理的および論理的な高レベルのデザイン上の考慮事項について説明します。

クラウド インフラストラクチャのネットワーキング コンポーネントにシスコのユニファイド ファブリックを使用すると、ケーブルを接続した後にクラウドのワークロード要件に変更があっても、ケーブルを配線しなおす必要がなくなります。Cisco UCS は、迅速かつ自動的にサーバを提供できるようにします。

FlexPod 上の Citrix CloudPlatform 4.2.1 の概要

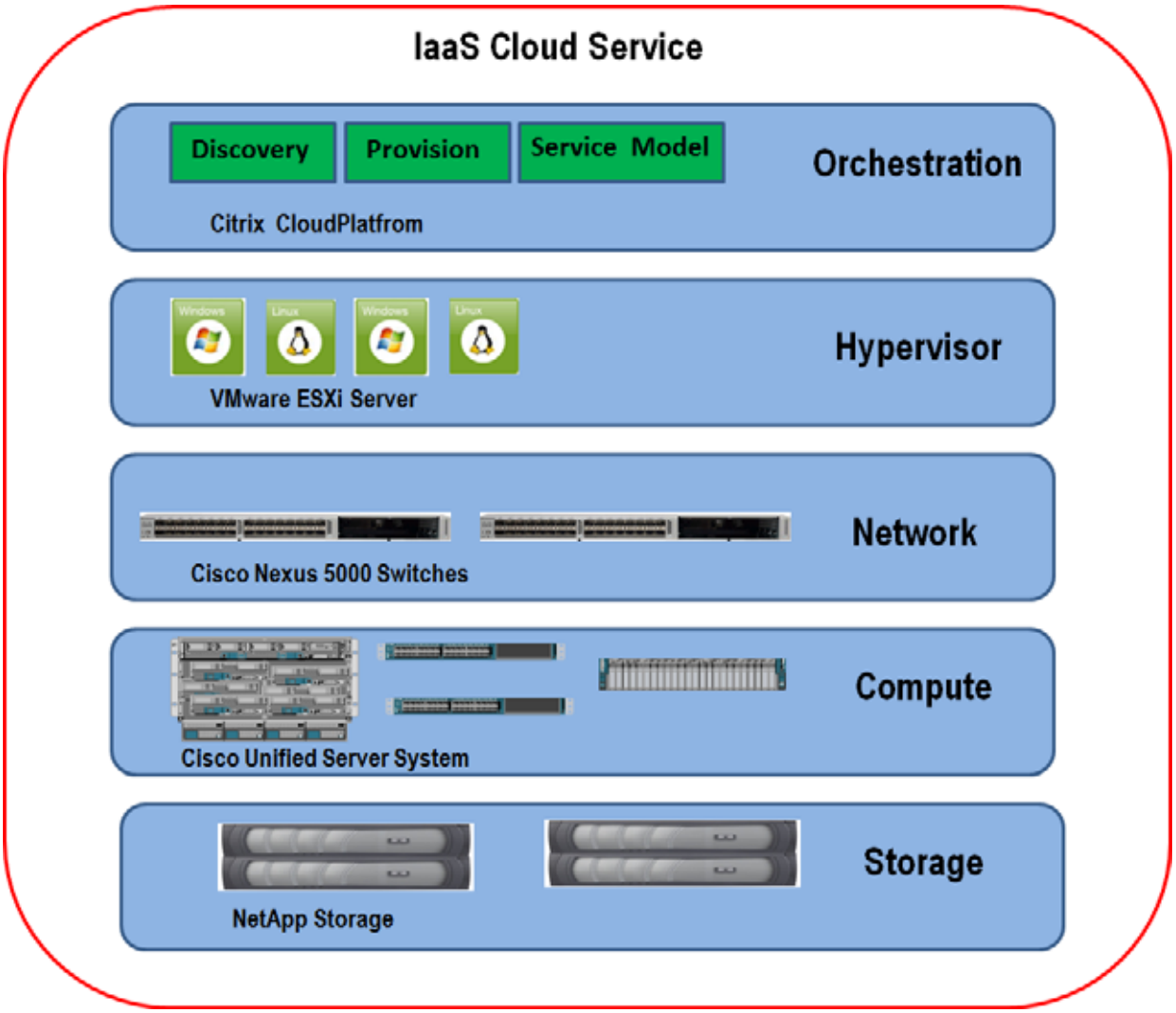
Cisco Flexpod と、Citrix CloudPlatform powered by Apache Cloudstack は、Cisco と NetApp によって開発されたコンバージド コンピューティング、ネットワーキング、およびストレージ ソリューションを、Citrix の定評あるアプリケーション中心のターンキー オーケストレーション ソリューションと組み合わせて、仮想サーバとストレージ リソースにオンデマンドでアクセスできる非常にセキュアでスケーラブルな IT インフラストラクチャを実現します。

CloudPlatform は、エンタープライズ プライベート クラウドに非常に適しており、オンデマンドで容量を提供できるシステムを実現するため、ユーザはポリシーに基づいて独自のリソースをプロビジョニングし、内部顧客、部門、または事業単位へのチャージバックまたはショーバックを行うことができます。

このマニュアルでは、以下のコンポーネントに基づいた IaaS（Infrastructure as a Service）の導入に従って、スケーラブルでダイナミックなマルチテナントのクラウド ソリューションの導入モデルを構築する設計方法について説明します。

- Cisco Unified Computing System
- Cisco Nexus 物理および仮想スイッチ
- NetApp FAS ストレージ
- VMware vSphere ESXi Hypervisor
- Citrix CloudPlatform 4.2.1

図 3　　IaaS クラウド サービス モデル



Cisco Unified Compute System

Cisco UCS は、プログラム可能で自動統合できるよう一から設計されています。サーバのファームウェアおよび設定からネットワーク プロファイルまで、サーバのハードディスク スタック全体が、モデルベースの管理を通じて設定されます。Cisco 仮想インターフェイス カード（VIC）では、I/O インターフェイスの数とタイプも動的にプログラムされ、サーバはいつでも電源を入れてどのようなワークロードも処理できます。

モデルベースの管理機能では、管理者が希望するシステム構成モデルを操作し、モデルのサービス プロファイルをハードウェア リソースへ関連付けできます。これによりシステムはそのモデルに合致するよう自動設定を行います。こうした自動化により、プロビジョニングやワークロードの移行が高速化され、正確かつ迅速な拡張性をもたらします。その結果、IT スタッフの生産性とコンプライアンスが向上し、一貫性のない設定に起因する障害のリスクが低減します。

Cisco Nexus ユニファイド ネットワーク システム

シスコ ユニファイド ファブリックは、信頼性、拡張性、俊敏性、およびコスト効率に優れたネットワーク サービスをサーバ、ストレージ、およびアプリケーションに提供すると共に、ユーザ エクスペリエンスを向上させるソリューションです。シスコ ユニファイド ファブリックを導入することにより、仮想化とクラウド サービスに対するサポートを強化できます。また、スタッフ稼働率の向上、リソース使用の効率化（サーバおよびストレージのロード向上）、低遅延オプション、TCO の削減、復元力と稼働率の向上が実現します。これは、ハイパフォーマンス、低遅延、および高可用性を備えたネットワークを実現します。このようなネットワークは、データセンターの多様なニーズに応えることができます。ニーズにはブロックレベルのストレージ トラフィックのロスレス要件が含まれます。シスコ ユニファイド ファブリック ネットワーク上では、ストレージを接続するさまざまなプロトコルのトラフィック、および、一般のデータ トラフィックが流れます。ストレージ接続技術の例としては、Fibre Channel、FCoE、Small Computer System Interface over IP（iSCSI）、Network Attached Storage（NAS）などがあります。FCoE を使用した場合、Fibre Channel トラフィックを、それ自身のファブリック上でも統合ファブリック上でも転送することができます。シスコ ユニファイド ファブリックでは、LAN 環境と SAN 環境の両方を最大限に活用できます。ストレージ ネットワーク ユーザはシスコ ユニファイド ファブリックを導入することにより、パフォーマンスの向上に加えて、スケール メリットを活かすこと、強固なベンダー コミュニティ、イーサネットの活発なパフォーマンス ロードマップの活用、および、Fibre Channel ネットワークのロスレス特性を利用することができます。

NetApp ユニファイド ストレージ システム

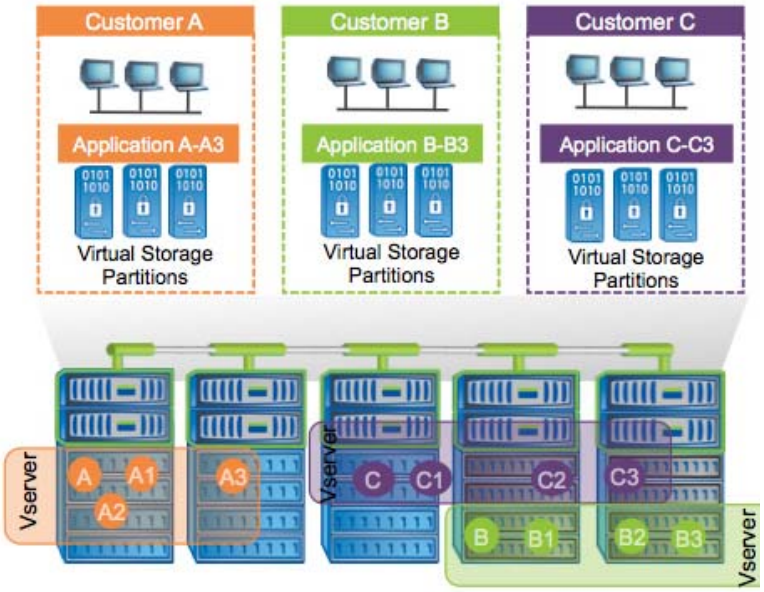
NetApp のソリューションは、すべての NetApp ストレージ システム上で実行する基盤ソフトウェアである clustered Data ONTAP 8.2.1 から始まります。Data ONTAP 8.2.1 は、NAS と SAN の混在環境と、ファイバ チャネル、iSCSI、FCoE、NFS、CIFS などの幅広いプロトコルをサポートする非常に最適化されたスケーラブルなオペレーティング システムです。

clustered Data ONTAP は、エンタープライズ プライベート クラウドとパブリック クラウドの両方のサービス プロバイダーにとって魅力的な価値をもたらします。ソフトウェアのユニファイド アーキテクチャは、仮想化環境、スケールアウト NAS、および企業アプリケーションにわたる最も要求の厳しいワークロードから最も独特なワークロードまで幅広く対応します。昨年、あらゆる業界の企業が clustered Data ONTAP を採用し、クラスタ化したノードが 4 倍に増加し、この結果、前四半期比 100% で導入が増大しました。継続した運用実績に事業評価が左右されるクラウド プロバイダーは、NetApp および Cisco による FlexPod® と clustered Data ONTAP を使用して、データセンターでの集中管理を実現しています。この新しいソフトウェアによって、組織およびクラウド サービス プロバイダーは、アプリケーションの稼働時間を最大に確保しながら、新しいサービスおよび容量を迅速かつコスト効率よく提供することができます。clustered Data ONTAP 8.2 は、パフォーマンス、可用性、および効率性に対する従来のハードウェア サイロの限界をなくし、IT 部門がビジネスおよびアプリケーションの需要の変化に、ストレージ インフラストラクチャを停止させずに対応できるようにします。

clustered Data ONTAP の業界随一の機能は次のとおりです。

- 99.999% 以上の信頼性を持つ無停止運転。これにより、スケジュールされたダウンタイムおよび動的なロード バランシング中に、データ移行を中断せずに連続的にデータにアクセスできます。
- 最高 69 PB のストレージと 24 のコントローラ ノード、49,000 の LUN、12,000 の NAS ボリュームによるシームレスな拡張性。100,000 以上のクライアントと単一のコンテナで最高 20 PB まで対応
- 大企業および中小企業のニーズを満たすユニファイドおよびマルチテナント アーキテクチャ内での実証済みのストレージおよび運用効率

図 4　NetApp Clustered ONTAP ストレージ アーキテクチャ



ストレージ プラットフォームを増やすための多数の NetApp ツールおよび拡張機能を使用できます。これらのツールは、導入、バックアップ、リカバリ、レプリケーション、管理、およびデータ保護を支援します。このソリューションは、これらのツールおよび拡張機能の一部を活用します。セキュアなマルチテナント機能を通じてクラウドを導入すれば、セキュアなテナント データの分離、アドレス空間、認証、高可用性、およびデータ保護が得られ、クラウドの中核コンポーネントである共有ストレージ インフラストラクチャを正常に実現できます。

VMware ESXi サーバ クラウド ハイパーバイザ システム

VMware ESXi ハイパーバイザは、強力な ESXi ハイパーバイザに基づいて構築された、完全な管理サーバ仮想化プラットフォームです。ESXi テクノロジーは、業界で最も高速でセキュアな仮想化ソフトウェアとして広く認められています。ESXi サーバは、仮想サーバを効率的に管理するためにデザインされ、コスト効果の高いサーバ統合およびビジネス継続性をもたらします。

クラウド プロバイダーは VMware ESXi Server を使用して重要な IT プロセスを自動化し、仮想環境用のサービス提供とビジネス継続性を改善でき、この結果、応答性に優れた IT サービスを提供しつつ時間と費用を節約できます。クラウド環境内の一部の重要な機能は次のとおりです。

- 高可用性：VM、ハイパーバイザ、またはサーバのレベルで障害が発生した場合、自動的に仮想マシンを再起動します。自動再起動機能により、ユーザは、すべての仮想化されたアプリケーションを保護し、ビジネスでの可用性を高めることができます。メモリ最適化は、ホスト サーバ上の VM 間で未使用のサーバ メモリを共有することにより、コストを削減し、アプリケーションのパフォーマンスと保護を改善します。
- 動的ワークロード：バランシングは、自動的にリソース プール内の 2 台の仮想マシンのバランスをとることによって、システム使用率を改善し、アプリケーション パフォーマンスを高めます。ワークロード バランシングは、アプリケーション要件を使用可能なハードウェア リソースと照合することによって、リソース プール内の最も適切なホストに VM をインテリジェントに配置します。

- 自動 VM 保護およびリカバリ：クラウド管理者はスナップショットおよびアーカイブ ポリシーを作成できます。スナップショットを定期的にスケジュールしておけば、VM に障害が発生した場合にデータの損失を防止できます。確立されたポリシーは、スナップショット タイプ、頻度、保持される履歴データ量、およびアーカイブ ロケーションに基づきます。VM の回復は、最新の既知のアーカイブを選択するだけで完了します。
- Storage ESXiMotion：ローカル ストレージおよび共有ストレージを活用して、リソース プール内およびリソース プール間で、実行中の仮想マシンとその関連仮想ディスク イメージを移動します。これにより、ユーザは、ストレージ容量によって VM が制限されたときにストレージの階層間で VM を移動させ、ダウンタイムなしでメンテナンスおよびアップグレードを実行できます。
- サイト リカバリ：サイト間でのディザスタ リカバリ プランニングおよびサービスを仮想環境に提供します。サイト リカバリはセットアップが簡単で、回復が迅速です。また、ディザスタ リカバリ プランが引き続き有効であるかを頻繁にテストする機能があります。
- ホスト電力管理：内蔵のハードウェア機能を利用して、動的に VM を少数のシステムに統合し、サービスの需要の変動に応じて利用率の低いサーバの電源を切ることによって、データセンターの電力消費を低減します。

Citrix CloudPlatform クラウド オーケストレータ システム

Citrix CloudPlatform は、パブリック、プライベート、またはハイブリッド導入で事実上無制限のコンピューティング パワーを可能にし、オンデマンドでアクセスでき、リアルタイムの利用状況と実際の使用データの測定値を表示します。これは、ロード バランシング、データ セキュリティ、およびコンプライアンスに関する定義済みのポリシーに準拠しながら、コンピューティング、ネットワーク、およびストレージの分散を自動化するのに役立ちます。セルフサービス プロビジョニングを、カスタム ビルド、事前定義されたマシン イメージのカタログと組み合わせることにより、サービス提供を簡略化し促進します。また、クラウド環境内でのリアルタイムの可視性およびレポート機能を取得して、コンプライアンス、セキュリティ、および顧客利用率を算定します。

CloudPlatform の構築および導入には、Citrix Xen Server、VMWare vSphere™、および KVM などの業界標準のハイパーバイザをクラウド内で実行するための管理サーバと拡張機能が含まれます。この管理サーバは、サーバ ファーム上に導入され、ホスト、ストレージ、デバイス、IP アドレスなどのリソースを管理できます。

CloudPlatform には、オンデマンド提供、セルフサービス VM インスタンス、ストレージ ボリューム、およびインターネット経由でのネットワーキング設定、または、オンプレミスのプライベート クラウドをセットアップするために必要なすべてのものが揃っています。CloudPlatform は、集約ストレージ、IP プール、CPU、メモリ、およびクラウドで使用されるその他のリソースに対する視認性をもたらすとともに、その中のイベントを時間順に表示することによって管理します。クラウドが構築されると、追加のアカウントのセットアップ、VM のインポート、およびコントロールの開発およびモニタを行うことができます。

Cisco UCS と Citrix CloudPlatform のネットワーク

この項では、Citrix CloudPlatform 4.2.1 をマルチテナント環境に導入した場合の、Cisco UCS のネットワーキング デザインに関する考慮事項について説明します。（マルチテナントとは、企業のプライベート クラウドの複数の内部顧客、またはサービス プロバイダーのパブリック クラウドの複数の外部顧客を意味します）。このデザインでは、同じ Cisco UCS インフラストラクチャを使用して、クラウド環境にデータ セキュリティをもたらすようにイーサネット アップリンク ポートと論理 VLAN ネットワークを物理的に定義することによって、マルチテナント管理、ゲスト、および対応するストレージのネットワーク トラフィックが分離されます。このデザインは、マルチテナント ネットワーク トラフィックを処理するために個別の専用物理サーバおよびスイッチが導入されたトポロジに比べ、OpEx と CapEx も削減されます。

図 5 は、物理トポロジの詳細構成となっており、アーキテクチャのさまざまなレベルと、クラウド ネットワーク デザインにおける Cisco UCS のいくつかの主要コンポーネントが示しています。

図 5　　Cisco UCS ネットワーク トポロジでの Citrix CloudPlatform 4.2.1

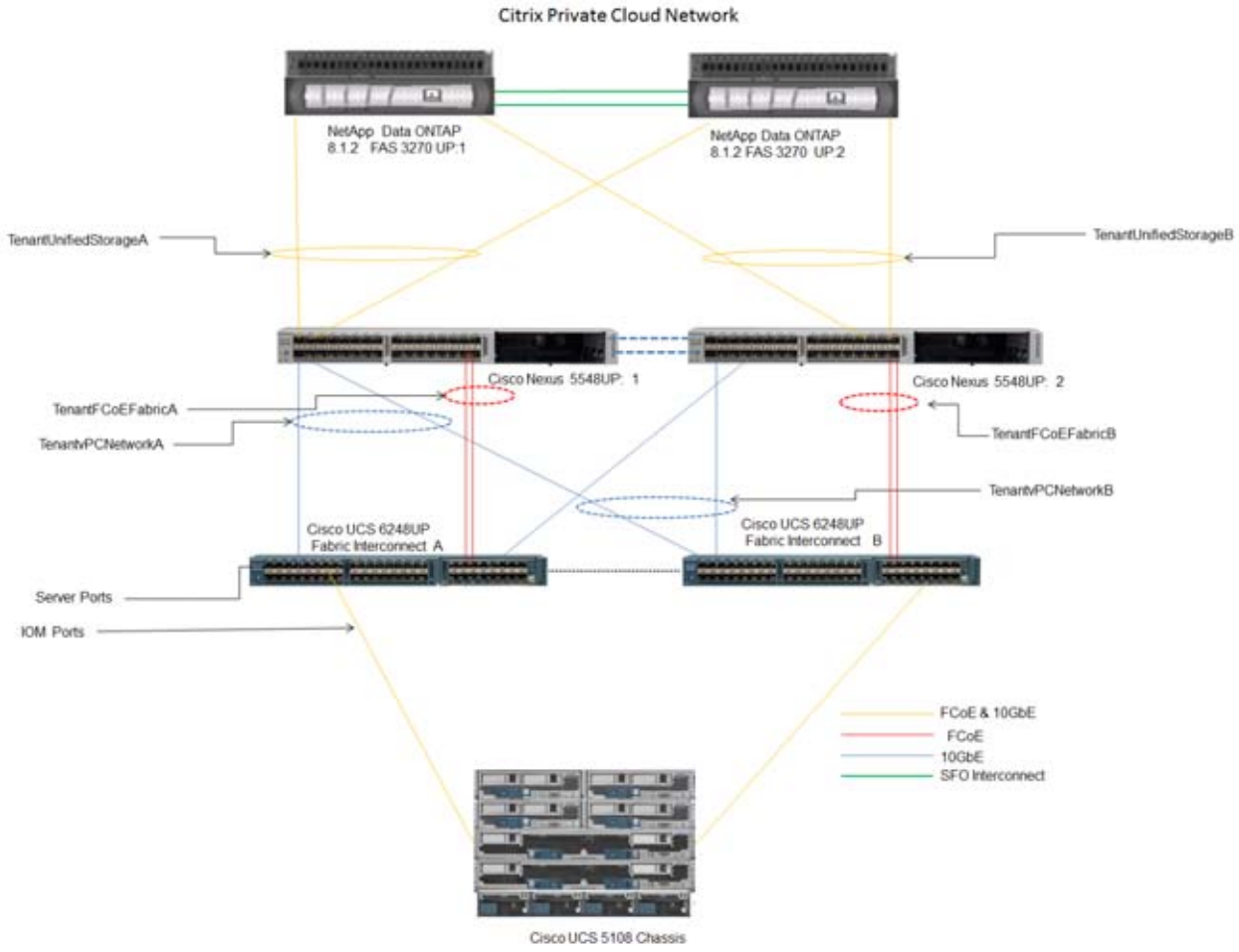


図 5 に示すように、ペアの Cisco UCS 6248UP ファブリック インターコネクトが、Cisco Nexus 5548UP スイッチを使用して、Cisco UCS ブレード サーバからのクラウド マルチテナント ネットワーク トラフィックを伝送します。Cisco UCS 6248UP ファブリック インターコネクトと Cisco Nexus 5548UP スイッチの両方が、それらの間のピア リンクでクラスタ化され、高可用性がもたらされます。Cisco UCS ブレード サーバが Cisco Nexus スイッチとノースバウンド接続を確立するためのネットワーク アクセス パスを提供するように設定された 2 つの仮想ポート チャンネル（vPC）があります。各 vPC には、クラウド テナント管理、ゲスト、ストレージ ネットワーク データ パスに対する VLAN が作成されています。ノースバウンド Nexus スイッチ上の NetApp コントローラからのストレージ ネットワーク パスをもたらすために、他に 2 つの仮想ポート チャネル（vPC）が設定されています。

ネットワーク データ トラフィックを扱えるように専用の物理イーサネット アップリンク ポートと論理 VLAN を備えた個別の vPC をプロビジョニングすることによって、同じクラウド ネットワーク デザインを複製して、単一の Cisco UCS でのクラウドで複数のマルチテナント ネットワーク分離を実現することができます。

Cisco UCS vPC では、クラウドでのネットワーク拡張性と大きなマルチテナント ネットワーク データ トラフィック帯域幅を処理するために、より多くのイーサネット アップリンク ポートをオンザフライで動的に追加して、オンデマンドでクラウド ネットワーク帯域幅に対処できるようにしています。

ネットワーク デバイスのケーブル配線情報

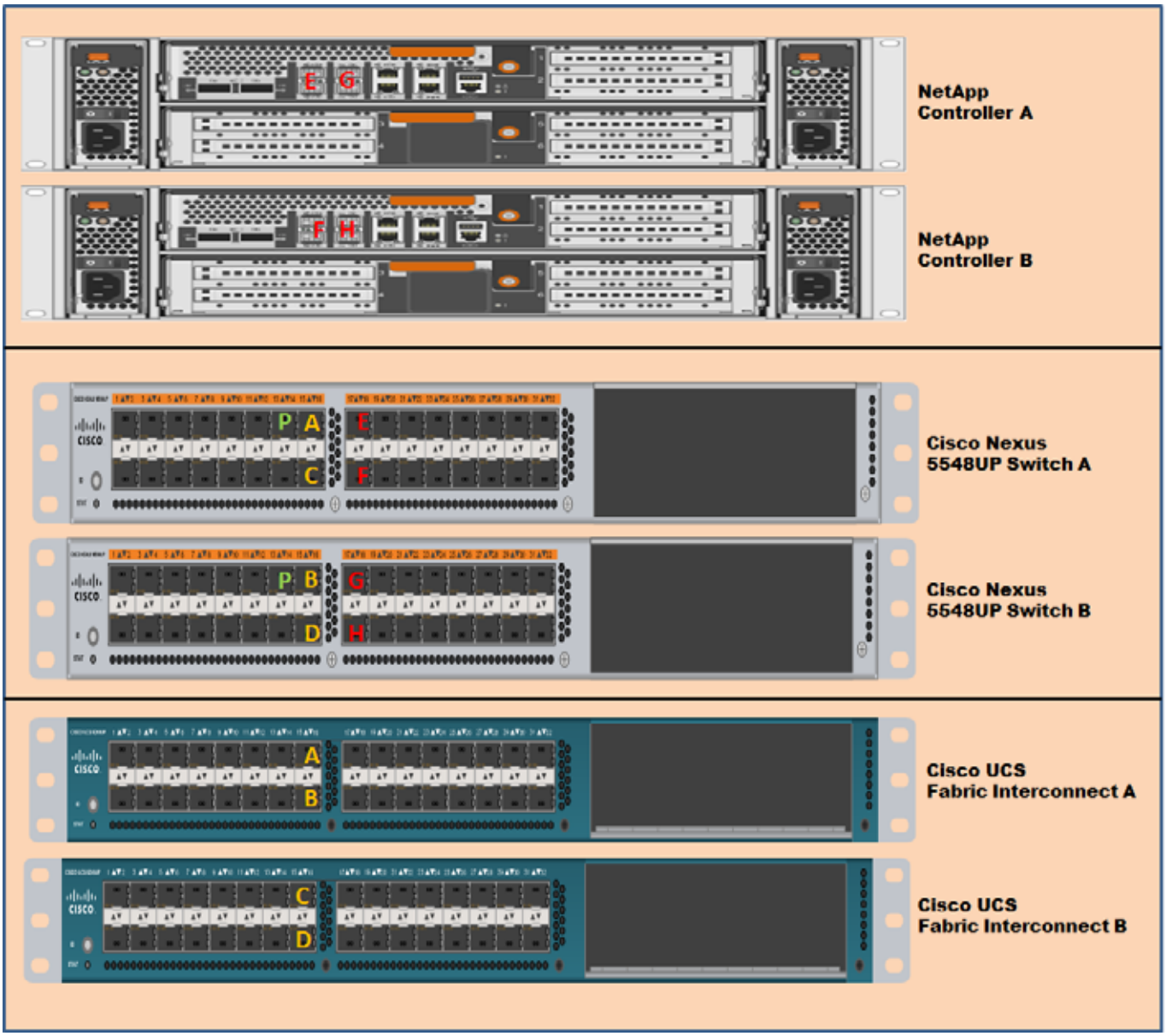
Citrix CloudPlatform 4.2.1 では、次のケーブル配線情報が、物理装置のケーブル配線に関するリファレンスとして提供されています。ここに示した表では、ケーブル配線要件を簡略化するために、ローカルとリモートの両方のデバイスとポートの位置について記しています。

このマニュアルでは、アウトオブバンド管理ポートが導入サイトの既存の管理インフラストラクチャに接続されていることを想定しています。

必ずここで示すケーブル配線手順に従ってください。従わない場合、特定のポート位置が指示されるので、後の導入手順で変更する必要が生じます。

図 6 には、Citrix CloudPlatform 4.2.1 のネットワーク ケーブル配線図が示されています。ラベルは、物理デバイス上のポート番号ではなく、エンド ポイントへの接続を示しています。たとえば、接続 A は Cisco Nexus 5548UP スイッチ A から Cisco ファブリック インターコネクト A に接続した 10 Gb vPC ポートであり、接続 P は、Cisco Nexus 5548UP スイッチ A から Cisco Nexus 5548UP スイッチ B に接続した 10 Gb vPC ピア リンクです。

図 6　　Citrix クラウド ネットワーク ケーブル配線図



次の表は、アーキテクチャの主要ケーブル配線セクションを示します。

1. 内部スイッチ リンク
2. 仮想ポート チャネル接続
3. インフラストラクチャ接続

表 1 には、Cisco Nexus 5548UP スイッチ A、Cisco UCS ファブリック インターコネクト A および B、ローカル デバイスおよび NetApp ストレージ コントローラ A および B、ローカル ポート チャネルおよびリモート デバイス ポートのイーサネット ケーブル配線情報が示されています。

表 1　Cisco Nexus スイッチ A のイーサネット ケーブル配線

両端のケーブル ID	イーサネット インターフェイス	VLAN	モード	速度	ポート チャネル	リモート デバイス ポート
A	Eth1/15	1,602 ～ 603、192 ～ 193、200、300	トランク	10G	101	ファブリック インターコネクト A 1/15
C	Eth1/16	1,602 ～ 603、192 ～ 193、200、300	トランク	10G	102	ファブリック インターコネクト B 1/15
G	Eth 1/11	1,602 ～ 603、1000 ～ 1001	トランク	1G	なし	Nexus 1100-A LOM A
H	Eth 1/12	1,602 ～ 603、1000 ～ 1001	トランク	1G	なし	Nexus 1100-B LOM A
P	Eth1/13	100	トランク	10G	100	vPC ピア リンク
E	Eth1/17	192	アクセス	10G	103	NetApp コントローラ A E1a
F	Eth 1/18	192	アクセス	10G	104	NetApp コントローラ B E1a
表示なし	Eth1/14	1,602 ～ 603、192 ～ 193、200、300	トランク	10G	なし	インフラストラクチャ ネットワークへのアップリンク

表 2 には、Cisco Nexus 5548UP スイッチ B、UCS ファブリック インターコネクト A および B、ローカル デバイスおよび NetApp ストレージ コントローラ A および B、ローカル ポート チャネル リモート デバイス ポートに関するイーサネット ケーブル配線情報が表示されています。

表 2　Cisco Nexus スイッチ B のイーサネット ケーブル配線

両端のケーブル ID	イーサネット インターフェイス	VLAN	モード	速度	ポート チャネル	リモート デバイス ポート
B	Eth1/15	1,602 ～ 603、192 ～ 193、200、300	トランク	10G	101	ファブリック インターコネクト A 1/16
D	Eth1/16	1,602 ～ 603、192 ～ 193、200、300	トランク	10G	102	ファブリック インターコネクト B 1/16

表 2　　Cisco Nexus スイッチ B のイーサネット ケーブル配線

I	Eth 1/11	1,602 ～ 603、1000 ～ 1001	トランク	1G	なし	Nexus 1100-A LOM B
J	Eth 1/12	1,602 ～ 603、1000 ～ 1001	トランク	1G	なし	Nexus 1100-B LOM B
P	Eth1/13	100	トランク	10G	100	vPC ピア リンク
G	Eth 1/17	192	アクセス	10G	103	NetApp コントローラ B E1b
H	Eth 1/18	192	アクセス	10G	104	NetApp コントローラ B E1b
表示なし	Eth1/14	1,602 ～ 603、192 ～ 193、200、300	トランク	10G	なし	インフラストラクチャ ネットワークへのアップリンク

表および対応する画像に示されたように、すべてのケーブルを接続してください。

Cisco Nexus スイッチ A のイーサネット ケーブル配線と Cisco Nexus スイッチ B のイーサネット ケーブル配線には、Citrix クラウドでの vPC ドメインと対応する vPC 名および ID を使用した Cisco Nexus 5548UP vPC 構成が示されています。レイヤ 2 および 3 のスイッチングを提供するために、アップストリーム スイッチングを備えた Cisco Nexus 5548UP スイッチのペアが導入されているので、Cisco UCS に障害が発生した場合に高可用性が得られ、管理、ゲスト、およびストレージのデータ トラフィックを処理できます。Cisco Nexus 5548UP トポロジでは、高可用性、障害の発生時の高速なコンバージェンス、およびスループットの増大を実現するために、単一の vPC 機能が有効化されています。

Cisco UCS およびクラウド ストレージ デザイン

この項では、Citrix CloudPlatform 4.2.1 をマルチテナント環境に導入した場合の、Cisco UCS およびクラウド ストレージ デザインに関する考慮事項について説明します クラウドでは、各テナントのストレージ ネットワーク トラフィックは、仮想論理 SAN ネットワーク（VSAN）を作成することによって、物理的および論理的に完全に分離されています。これにより、完全に分離されたファブリック トポロジの作成が可能になり、それぞれは、拡張可能な共通の物理インフラストラクチャの上に独自のファブリック サービス セットを保持します。各 VSAN は独自のゾーニング サービスを保持しているので、ゾーニングはそれぞれの VSAN 内で独立して設定され、他の VSAN およびゾーニング サービスに影響しません。クラウド マルチテナント ストレージ トラフィックを処理するために個別の専用物理スイッチが導入されたトポロジに比べ、このデザインでは OpEx と CapEx も削減されます。

Cisco UCS および Cisco Nexus ファブリックでは、拡張性に対応するために、ポート チャネルを作成することにより、複数の物理インターフェイスを 1 つの論理インターフェイスに集約し、より集約度の高い帯域幅、ロード バランシング、リンク冗長性を実現できるようにしています。

この導入モデルでは、マルチテナント ストレージ データ トラフィックを分離するために VSAN を作成し、リンク集約のために FC ポート チャネルを作成します。

ストレージ デバイスのケーブル配線情報

Citrix CloudPlatform 4.2.1 環境では、次の情報が、物理装置のケーブル配線に関するリファレンスとして提供されています。ここに示した表では、ケーブル配線要件を簡略化するために、ローカルとリモートの両方のデバイスとポートの位置について記しています。

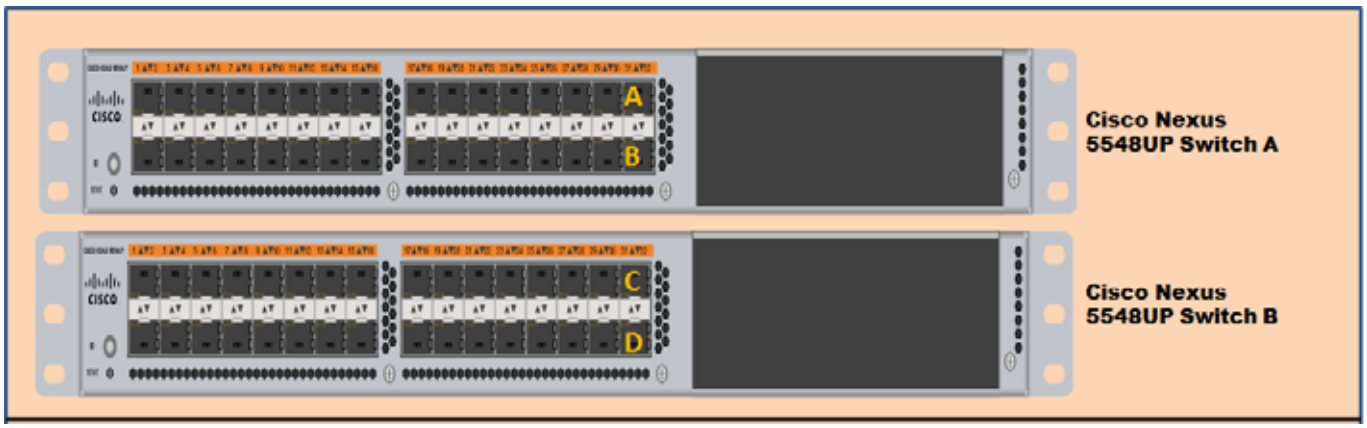
このマニュアルでは、アウトオブバンド管理ポートが導入サイトの既存の管理インフラストラクチャに接続されていることを想定しています。

記述の導入手順では特定のポート位置を使用します。必ずここで示すケーブル配線手順に従ってください。ポート位置を変更すると、結果として導入手順に変更が生じます。

開始する前に、ここに示した表と図に記された設定に一致していることを確認してください。

図 7 には、Citrix CloudPlatform 4.2.1 のネットワーク ケーブル配線図が示されています。ラベルは、物理デバイス上のポート番号ではなく、エンド ポイントへの接続を示しています。たとえば接続 A は、Cisco Nexus 5548UP スイッチ A から Cisco ファブリック インターコネクト A に接続した FCoE 10-gb ユニファイド FCoE ポートです。

図 7　　Citrix CloudPlatform 4.2.1 のアップリンク ネットワーク ケーブル配線



Cisco UCS Quality-of-Service システムおよびポリシー

マルチテナント クラウド環境で、サービス レベルの可用性は、クラウド インフラストラクチャに基づいて構築されるさまざまなクラウド サービスを定義する場合に、主要な役割を果たします。インフラストラクチャの 1 つが、内部および外部でデータ トラフィックを処理するためのクラウド ネットワークです。このマニュアルでは、クラウド マルチテナントのデータ トラフィックを処理するために後からプロビジョニング可能な、提供されるイーサネット ネットワーク帯域幅に基づいたネットワーク サービスレベル合意書を定義する方法を中心に取り上げます。

Cisco UCS は、IEEE データセンター ブリッジング（DCB）を使用して、Cisco UCS 内のすべてのトラフィックを処理します。イーサネットに対するこの業界標準の機能拡張では、イーサネットの帯域幅が 8 つの仮想レーンに分割されています。Cisco UCS プラットフォーム全体にわたり、これらの仮想レーンで DCB 帯域幅がどのように割り当てられるかは、システム クラスによって決定されます。

各システム クラスは、特定のタイプのトラフィックに対し帯域幅の特定のセグメントを予約し、過剰にサブスクライブされたシステムでも、保証されたレベルのトラフィック管理を提供します。たとえば、ファイバ チャネル プライオリティ システム クラスを設定して、FCoE トラフィックに割り当てられる DCB 帯域幅の割合を決定することができます。

表 3　Quality of Service に従って定義されたシステム クラス

システム クラス	説明
• プラチナ プライオリティ • ゴールド プライオリティ • シルバー プライオリティ • ブロンズ プライオリティ	これらのクラスは、すべてのサーバの Quality of Service（QoS）を設定します。QoS システム クラスは、サーバに関連付けられたサービス プロファイルに定義されます。これらのシステム クラスはそれぞれ、1 レーンのトラフィックを管理します。これらのシステム クラスのプロパティはすべて、カスタム設定やポリシーを割り当てるために使用できます。
ベスト エフォート プライオリティ	このクラスは、基本イーサネット トラフィックに予約されたレーンの QoS を設定します。このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。たとえば、このクラスには、必要に応じてデータ パケットをドロップできるようにするドロップ ポリシーがあります（データ パケットがドロップされる理由を記述できますか。どのような状況ですか）。
ファイバ チャネル プライオリティ	このクラスは、FCoE トラフィックに予約されたレーンの QoS を設定します。このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。たとえば、このクラスには、データ パケットが絶対にドロップされないことを保証するためのドロップなしポリシーがあります。

マルチテナント ネットワーク要件に対する、Citrix CloudPlatform 4.2.1 環境でのネットワークベースのサービスレベル合意書を提供するために、次のシステム クラス SLA が定義されています。これらの SLA は、クラウド ネットワーク オファリングに直接対応付けられ、コストに基づいてネットワーク インフラストラクチャを選択できるようにクラウド テナントに提供されます。

- プラチナ ネットワーク SLA

  マルチテナント ネットワーク要件を満たす、つまりより高い帯域幅と低遅延を実現するために、Cisco UCS QoS システム クラスでは、最高の重み（帯域幅）を持ち、大きなクラウド I/O ネットワークの処理に 9000 の最大伝送単位（MTU）が定義されたシステムに、プラチナ クラスが与えられます。

  たとえば、クラスタ内のサーバ プール間の仮想マシンの移行を扱う場合、管理ネットワーク ボンディング インターフェイスの一部である Cisco UCS 静的 vNIC に適用される管理トラフィックに対してプラチナ ネットワーク SLA ポリシーを定義します。

- ゴールド ネットワーク SLA

  マルチテナント ネットワーク要件に対しプラチナ ネットワーク SLA に比べてわずかに低い帯域幅と低遅延のネットワークを実現するために、Cisco UCS QoS システム クラスでは、2 番目に高い重み（帯域幅）を持ち、大きなクラウド I/O ネットワーク トラフィックの処理に 9000 の最大伝送単位（MTU）が定義されたシステムに、ゴールド ネットワーク SLA を与えます。

- シルバー ネットワーク SLA

  同じクラウド ネットワーク SLA 要件で、マルチテナント ネットワーク要件に対しさらに低い帯域幅と低い遅延のネットワークを実現するために、シルバー ネットワーク SLA が定義されています。Cisco UCS QoS システム クラスでは、3 番目の重み（帯域幅）を持ち、大きなクラウド I/O ネットワーク トラフィックの処理に 9000 の最大伝送単位（MTU）が定義されたシステムに、シルバー ネットワーク SLA を与えます。

（注） このマニュアルでは、特定の顧客ニーズに関連し、クラウド ネットワーク インフラストラクチャ オファリングに応じて変更することができる、記述済みのクラウド ネットワーク SLA オファリングに基づいて Cisco UCS QoS ポリシーを定義します。

より高いネットワーク帯域幅とより低い遅延を必要とするクラスタ内のサーバ プールでの VM 移行を処理するために、管理トラフィックに対するプラチナ ネットワーク SLA ポリシーが定義され、後で管理ネットワーク ボンディング インターフェイスの一部である Cisco UCS 静的 vNIC に適用されます。NFS ストレージ トラフィックを処理するため、クラウド VM バックアップ/復元、テンプレート、ISO、VM を保存するためのプライマリ ストレージなど、より適切な帯域幅を必要とする操作を処理に対して、すべてのストレージ関連のトラフィックを処理するためのゴールド ネットワーク SLA ポリシーが定義され、後でストレージ ネットワーク ボンディング インターフェイスの一部である Cisco UCS 静的 vNIC に適用されます。VM のパブリックまたはプライベート トラフィックを処理するため、このようなゲスト トラフィックに対するシルバー ネットワーク SLA ポリシーが定義され、後でゲスト ネットワーク ボンディング インターフェイスの一部である Cisco UCS 静的 vNIC に適用されます。

クラウド ネットワーク SLA を定義した後、Cisco UCS で、vNIC の発信トラフィックに割り当てられる QoS ポリシーを定義できます。QoS ポリシーは vNIC ポリシーに含める必要があり、このポリシーは次に、vNIC を設定するためにサービス プロファイルに含められます。

表 4 には、QoS ポリシー名が、対応するプライオリティ、重み、および MTU 値とともに一覧表示されています。これらの値は、Microsoft SQL Server 導入環境における静的および動的 vNIC に適用されます。

表 4　Cisco UCS QoS ポリシーおよびネットワーク SLA

ポリシー名	プライオリティ	重み（パーセント）	MTU
Platinum-Net-SLA	Platinum	10	9000
Gold-Net-SLA	Gold	9	9000
Silver-Net-SLA	Silver	8	9000

デバイスの設定

この項では、ユニファイド デザインでハードウェア デバイスを設定する手順について説明します。

この項では、UCS にストレージおよび CloudPlatform 4.2.1 を導入する準備ができるように、UCS を設定および導入する方法について詳しく説明します。

- Cisco Nexus スイッチの設定
- Cisco UCS の導入
- アップリンク ポート チャネルの作成
- ストレージの設定

Cisco Nexus スイッチの設定

この項では、スイッチおよび他のコンポーネントの設定およびセットアップで準拠する vPC デザインについて説明します。ポート、機能、VLAN、およびイーサネット インターフェイスを Nexus スイッチ上で設定する手順を段階的に示します。次のタスクについて詳しく説明します。

- スイッチでの vPC マッピング

- Cisco Nexus スイッチの設定
- 機能およびグローバル設定の有効化
- VLAN の設定
- ポート チャネルの設定
- 仮想ポート チャネルの設定
- ポート チャネルの設定
- イーサネット インターフェイスの設定

スイッチでの vPC マッピング

仮想ポート チャネル（vPC）は、物理的には 2 台の異なる Cisco Nexus 5000 シリーズ デバイスに接続されているリンクを、第 3 のデバイスには単一のポートに見えるようにします。第 3 のデバイスは、スイッチ、サーバ、ポート チャネルをサポートするその他の任意のネットワーキング デバイスのいずれでもかまいません。vPC は、ノード間の複数の並列パスを可能にし、トラフィックのロード バランシングを可能にすることによって、冗長性を作り、バイセクショナルな帯域幅を増やすレイヤ 2 マルチパスを提供できます。

表 5 には、Cisco Nexus 5548UP vPC 設定の vPC ドメインと、クラウド内での対応する vPC 名および ID が示されています。レイヤ 2 および 3 のスイッチングを提供するために、アップストリーム スイッチングを備えた Cisco Nexus 5548UP スイッチのペアが導入されているので、Cisco UCS に障害が発生した場合に高可用性が得られ、管理、ゲスト、およびストレージのデータ トラフィックを処理できます。Cisco Nexus 5548UP トポロジでは、高可用性、障害の発生時の高速なコンバージェンス、およびスループットの増大を実現するために、単一の vPC 機能が有効化されています。

表 5　　vPC マッピング

vPC ドメイン	vPC 名	vPC ID
100	TenantvPCNetworkA	101
100	TenantvPCNetworkAB	102
100	TenantUnifiedStorageA	103
100	TenantUnifiedStorageB	104
100	TenantFCoEFabric	10

vPC デザイン テーブルで、単一の vPC ドメインである Domain 100 は、Cisco Nexus 5548UP メンバ スイッチにわたって作成され、特定のネットワーク トラフィックを伝送する vPC を定義します。このトポロジは、ID が 101 から 104 の 4 つの vPC を定義します。vPC ID 101 および 102 は、Cisco UCS ファブリック インターコネクトからのトラフィックについて定義され、vPC ID 103 および 104 は、iSCSI トラフィックについて定義され、vPC 105 および 106 は、NetApp ストレージ上の NFS トラフィックについて定義されます。これらの vPC は、Cisco UCS ファブリック インターコネクトと NetApp ストレージ システムを接続する Cisco Nexus 5548UP 内で管理されます。

Cisco Nexus スイッチの設定

Cisco Nexus 5000 シリーズに初めてアクセスすると、セットアップ プログラムが実行され、イーサネット インターフェイス経由で通信するために必要な IP アドレスおよびその他の情報の入力を要求するプロンプトが表示されます。この情報は、スイッチを設定および管理するために必要です。

スイッチを設定するための準備

初めて Cisco Nexus 5000 シリーズ スイッチを設定する前に、次の情報が必要になります。

- 管理者パスワード

（注） パスワードが弱い（短く、解読されやすい）場合、パスワード設定が拒否されます。必ず強固なパスワードを設定するようにしてください。

- 管理インターフェイスに IPv4 アドレスを使用する場合は、次の情報が必要です。
  - スイッチの管理インターフェイスの IPv4 サブネット マスク
  - デフォルト ゲートウェイの IPv4 アドレス（任意）
- スイッチの SSH サービス（任意）

  このサービスをイネーブルにするには、SSH のキー タイプ（dsa/rsa/rsa1）とキーのビット数（768 ～ 2048）を選択します。
- NTP サーバの IPv4 アドレス（任意）
- SNMP コミュニティ ストリング（任意）
- スイッチ名（任意）

  スイッチのプロンプトになります。
- 追加ログイン アカウントおよびパスワード（任意）

（注） IPv4 を使用する場合、SNMP アクセスをイネーブルにするには、必ず IPv4 ルート、IPv4 デフォルト ネットワーク アドレス、および IPv4 デフォルト ゲートウェイ アドレスを設定してください。

デフォルトのログイン

スイッチには必ず、デフォルトのユーザであるネットワーク管理者（admin）が設定されています。デフォルトのユーザはどの時点でも変更できません。

デフォルトのパスワードはないので、強固なパスワードを明示的に設定する必要があります。パスワードを設定した後で忘れた場合には、パスワードを回復するオプションがあります。

（注） write erase コマンドを入力してスイッチをリロードした場合、設定手順を使用して、デフォルトのユーザ（admin）パスワードを再設定する必要があります。

Cisco Nexus 5548 スイッチで初期設定を行うには、次の手順を実行します。

Cisco Nexus A および Cisco Nexus B の場合

NX-OS のセットアップは、初期ブートとスイッチのシリアルまたはコンソール ポートへの接続時に自動的に開始されます。Cisco Nexus スイッチを設定するには、次のコマンドを入力します。

1. Enter yes to enforce secure password standards: yes
2. Enter the password for the administrator (adminuser): <xxxxx>
3. Enter the password a second time to commit the password; <xxxxx>
4. Enter yes to enter the basic configuration dialog: yes

5. Create another login account (yes/no) [n]: Enter
6. Configure read-only SNMP community string (yes/no) [n]: Enter
7. Configure read-write SNMP community string (yes/no) [n]: Enter
8. Enter the switch name: <Nexus A スイッチ名> Enter
9. Continue with out-of-band (mgmt0) management configuration?(yes/no) [y]: Enter
10. Mgmt0 IPv4 address: <Nexus A mgmt0 IP> Enter
11. Mgmt0 IPv4 netmask: <Nexus A mgmt0 ネットマスク> Enter
12. Configure the default gateway?(yes/no) [y]: Enter
13. IPv4 address of the default gateway: <Nexus A mgmt0 gateway> Enter
14. Enable the telnet service?(yes/no) [n]: Enter
15. Enable the ssh service?(yes/no) [y]: Enter
16. Type of ssh key you would like to generate (dsa/rsa):rsa
17. Number of key bits <768–2048>:1024 Enter
18. Configure the ntp server?(yes/no) [y]: n Enter
19. NTP server IPv4 address: <*NTP Server IP*> Enter
20. Enter basic FC configurations (yes/no) [n]: Enter
21. Would you like to edit the configuration?(yes/no) [n]: Enter

（注） 必ず、設定を有効にする前に要約を確認してください。

22. Use this configuration and save it?(yes/no) [y]: Enter

（注） 設定は、コンソールからか SSH を使用して続行できます。SSH を使用するには、Nexus A または B の mgmt0 アドレスに接続します。

（注） すでに入力したパスワードでユーザ admin としてログインします。

機能およびグローバル設定の有効化

機能のイネーブル化

デバイス上で vPC を有効化して、リンクされたデバイス間の通信を定義するには、LACP（Link Aggregation Control Protocol）、仮想ポート チャネル（vPC）、およびインターフェイス VLAN 機能を、両方の Cisco Nexus スイッチ上でアクティブ化する必要があります。2 台のスイッチ上でのこれらの機能を設定するには、次の手順を実行します。

Cisco Nexus A および Cisco Nexus B の場合：

1. configure t と入力し、グローバル コンフィギュレーション モードに入ります。
2. feature lacp と入力します。
3. feature interface-vlan と入力します。
4. feature vpc と入力します。

グローバル設定の指定

vPC は、スパニングツリー プロトコル（STP）でブロックされたポートを解消し、グローバル設定として有効化され、これにより、Cisco Nexus スイッチ上のすべてのポートがネットワーク ポートとして表示されるようになります。STP グローバル設定を行うには、次の手順を実行します。

Cisco Nexus A および Cisco Nexus B の場合：

1. グローバル コンフィギュレーション モードから、spanning-tree port type network default と入力し、このポートがデフォルトでスパニングツリーの観点からネットワーク ポートとして見なされるようにします。
2. spanning-tree port type edge bpduguard default と入力し、デフォルトですべてのエッジ ポート上で bpduguard を有効化します。
3. spanning-tree port type edge bpdufilter default と入力し､デフォルトですべてのエッジ ポート上で bpdufilter を有効化します。

VLAN の設定

VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションによって論理的にセグメント化されているスイッチド ネットワークの端末のグループです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。

この項では、両方の Nexus スイッチ上で VLAN を設定する方法について詳しく説明します。

このデザインでは、VLAN は表 6 に示すように定義されています。

表 6　　Citrix CloudPlatform 4.2.1 用の VLAN のセットアップ

VLAN 名	VLAN の目的	このマニュアルで使用される ID	ネットワーク アドレス
Management	管理および VM 移行トラフィック	602	10.65.121.0/24
BareMetal-VLAN20	Baremetal ホスト PXE ブート トラフィック	20	20.1.1.0/24
Guest-VLAN	ゲスト VM パブリック トラフィック	603	10.65.122.0/24
Guest-VLAN-1000	ゲスト VM プライベート トラフィック	1000	10.1.0.0/24
Guest-VLAN-1001	ゲスト VM プライベート トラフィック	1001	10.2.0.0/24
NFS	NFS ストレージ トラフィック	193	193.191.1.0/24
VMotion	vMotion トラフィック	192	192.191.1.0/24

Cisco Nexus A および Cisco Nexus B の場合

両方の Cisco Nexus スイッチ上で VLAN を設定するには、次の手順を実行します。

1. config-t と入力します。

2. vlan <管理 VLAN ID> と入力します。
3. name Management と入力します。
4. exit と入力します。
5. vlan <BareMetal-VLAN20 VLAN ID> と入力します。
6. name BareMetal-VLAN と入力します。
7. exit と入力します。
8. vlan <ゲスト VLAN ID> と入力します。
9. name guest-VLAN と入力します。
10. exit と入力します。
11. vlan <ゲスト VLAN ID> と入力します。
12. name guest-VLAN-1000 と入力します。
13. exit と入力します。
14. vlan <ゲスト VM VLAN ID> と入力します。
15. name guest-VLAN-1001 と入力します。
16. exit と入力します。
17. vlan <NFS VLAN ID> と入力します。
18. name NFS と入力します。
19. exit と入力します。
20. vlan <vMotion VLAN ID> と入力します。
21. name vMotion と入力します。
22. exit と入力します。
23. vlan <FCoE VLAN ID> と入力します。
24. name VLAN0200 と入力します。
25. fcoe vsan <ID 200> と入力します。
26. state <active> と入力します。
27. no <shutdown> と入力します。
28. exit と入力します。
29. vlan <FCoE VLAN ID> と入力します。
30. name VLAN0300 と入力します。
31. fcoe vsan <ID 300> と入力します。
32. state <active> と入力します。
33. no <shutdown> と入力します。
34. exit と入力します。

ポート チャネルの設定

この項では、トラブルシューティング手順および検証のために、個々のポートの記述を作成し設定する方法について詳しく説明します。Cisco Nexus スイッチ A および B へのポート チャネルを作成するには、次の手順を実行します。

Cisco Nexus 5548 A

1. グローバル コンフィギュレーション モードから、interface Eth1/13 と入力します。
2. description <VPC ピア リンク> と入力します。
3. exit と入力します。
4. interface Eth1/15 と入力します。
5. description <Cisco UCS Manager A:Eth1/5> と入力します。
6. exit と入力します。
7. interface Eth1/16 と入力します。
8. description <Cisco UCS Manager B: Eth1/5> と入力します。
9. exit と入力します。
10. interface Eth1/17 と入力します。
11. description <NetApp Controller Flexpod A:E1a> と入力します。
12. exit と入力します。
13. interface Eth1/18 と入力します。
14. description <NetApp Controller Flexpod B:E1a> と入力します。
15. exit と入力します。
16. interface Eth1/31 と入力します。
17. description <FCoE Uplink To Nexus 5548 B> と入力します。
18. exit と入力します。
19. interface Eth1/32 と入力します。
20. description <FCoE Uplink To Nexus 5548 B> と入力します。
21. exit と入力します。

Cisco Nexus 5548 B

1. グローバル コンフィギュレーション モードから、interface Eth1/13 と入力します。
2. description <VPC ピア リンク> と入力します。
3. exit と入力します。
4. interface Eth1/15 と入力します。
5. description <Cisco UCS Manager A:Eth1/5> と入力します。
6. exit と入力します。
7. interface Eth1/16 と入力します。
8. description <Cisco UCS Manager B:Eth1/5> と入力します。
9. exit と入力します。
10. interface Eth1/17 と入力します。
11. description <NetApp Controller Flexpod A:E1b> と入力します。
12. exit と入力します。
13. interface Eth1/18 と入力します。

14. description <NetApp Controller Flexpod B:E1b> と入力します。
15. exit と入力します。
16. interface Eth1/31 と入力します。
17. description <FCoE Uplink To Nexus 5548 B> と入力します。
18. exit と入力します。
19. interface Eth1/32 と入力します。
20. description <FCoE Uplink To Nexus 5548 B> と入力します。
21. exit と入力します。

仮想ポート チャネルの設定

仮想ポート チャネル（vPC）は、物理的には 2 台の異なる Cisco Nexus 5000 シリーズ デバイスに接続されているリンクを、第 3 のデバイスには単一のポートに見えるようにします。Cisco Nexus スイッチ A および B 上で仮想ポート チャネル（vPC）を設定するには、次の手順を実行します。

Cisco Nexus 5548 A

1. グローバル コンフィギュレーション モードから、vpc domain <Nexus vPC ドメイン ID> と入力します。
2. role priority 10 と入力します。
3. peer-keepalive destination <Nexus B mgmt0 IP> source <Nexus A mgmt0IP> と入力します。
4. exit と入力します。
5. interface Port-Channel 100 と入力します。
6. vpc peer-link と入力します。
7. exit と入力します。
8. interface Port-Channel 101 と入力します。
9. vpc 101 と入力します。
10. exit と入力します。
11. interface Port-Channel 102 と入力します。
12. vpc 102 と入力します。
13. exit と入力します。
14. interface Port-Channel 103 と入力します。
15. vpc 103 と入力します。
16. exit と入力します。
17. interface Port-Channel 104 と入力します。
18. vpc 104 と入力します。
19. exit と入力します。
20. interface Port-Channel 10 と入力します。
21. exit と入力します。
22. copy run start と入力します。

Cisco Nexus 5548 B

1. グローバル コンフィギュレーション モードから、vpc domain <Nexus vPC ドメイン ID> と入力します。
2. role priority 20 と入力します。
3. peer-keepalive destination <Nexus A mgmt0 IP> source <Nexus B mgmt0IP> と入力します。
4. exit と入力します。
5. interface Port-Channel 100 と入力します。
6. vpc peer-link と入力します。
7. exit と入力します。
8. interface Port-Channel 101 と入力します。
9. vpc 101 と入力します。
10. exit と入力します。
11. interface Port-Channel 102 と入力します。
12. vpc 102 と入力します。
13. exit と入力します。
14. interface Port-Channel 103 と入力します。
15. vpc 103 と入力します。
16. exit と入力します。
17. interface Port-Channel 104 と入力します。
18. vpc 104 と入力します。
19. exit と入力します。
20. interface Port-Channel 10 と入力します。
21. exit と入力します。
22. copy run start と入力します。

ポート チャネル設定の追加

ポート チャネルを作成した後、デザイン要件を満たすようにそれらを個別に設定する必要があります。ポートは、前述の 表 6 で定義された vPC マッピングに従って設定されます。Cisco Nexus スイッチ A および B でポート チャネル設定を追加するには、次の手順を実行します。

Cisco Nexus 5548 A

1. グローバル コンフィギュレーション モードから、interface Port-Channel 100 と入力します。
2. switchport mode trunk と入力します。
3. switchport trunk native vlan <ネイティブ VLAN ID> と入力します。
4. switchport trunk allowed vlan <MGMT VLAN ID, BareMetal-VLAN VLAN ID GUESTVM VLAN ID, guest-VLAN-1000 VLANID, guest-VLAN-1001 VLANID, NFS VLAN ID, vMotion VLAN ID> と入力します。
5. spanning-tree port type network と入力します。
6. no shutdown と入力します。

7. exit と入力します。
8. interface Port-Channel 101 と入力します。
9. switchport mode trunk と入力します。
10. switchport trunk native vlan <デフォルト VLAN ID> と入力します。
11. switchport trunk allowed vlan <MGMT VLAN ID, BareMetalk-VLAN VLANID, guest-VLAN VLAN ID, guest-VLAN-1000 VLAN ID, guest-VLAN-1001 VLAN ID, NFS VLAN ID, vMotion VLAN ID> と入力します。
12. spanning-tree port type edge trunk と入力します。
13. no shut と入力します。
14. exit と入力します。
15. interface Port-Channel 102 と入力します。
16. switchport mode trunk と入力します。
17. switchport trunk native vlan <ネイティブ VLAN ID> と入力します。
18. switchport trunk allowed vlan <NFS VLAN ID> と入力します。
19. spanning-tree port type edge trunk と入力します。
20. no shut と入力します。
21. exit と入力します。
22. interface Port-Channel 103 と入力します。
23. switchport mode trunk と入力します。
24. switchport trunk native vlan <ネイティブ VLAN ID> と入力します。
25. switchport trunk allowed vlan <NFS VLAN ID> と入力します。
26. no shut と入力します。
27. exit と入力します。
28. interface Port-Channel 104 と入力します。
29. switchport mode trunk と入力します。
30. switchport trunk native vlan <ネイティブ VLAN ID> と入力します。
31. no shut と入力します。
32. exit と入力します。
33. interface Port-Channel 10 と入力します。
34. switchport mode trunk と入力します。
35. switchport trunk native vlan <ネイティブ VLAN ID> と入力します。
36. switchport trunk allowed vlan <200> と入力します。
37. no shut と入力します。
38. exit と入力します。
39. copy run start と入力します。

Cisco Nexus 5548 B

1. グローバル コンフィギュレーション モードから、interface Port-Channel 100 と入力します。

2. switchport mode trunk と入力します。
3. switchport trunk native vlan <ネイティブ VLAN ID> と入力します。
4. switchport trunk allowed vlan <MGMT VLAN ID, BareMetalVlan VLANID, guestVM VLAN ID, guest-VLAN-1000 VLANID, guest-VLAN-1001 VLANID,NFS VLAN ID, vMotion VLAN ID> と入力します。
5. spanning-tree port type network と入力します。
6. no shutdown と入力します。
7. exit と入力します。
8. interface Port-Channel 101 と入力します。
9. switchport mode trunk と入力します。
10. switchport trunk native vlan <デフォルト VLAN ID> と入力します。
11. switchport trunk allowed vlan <MGMT VLAN ID, BareMetalVlan VLANID, guest-VLAN VLAN ID, guest-VLAN-1000 VLANID, guest-VLAN-1001 VLANID, NFS VLAN ID, vMotion VLAN ID> と入力します。
12. spanning-tree port type edge trunk と入力します。
13. no shut と入力します。
14. exit と入力します。
15. interface Port-Channel 102 と入力します。
16. switchport mode trunk と入力します。
17. switchport trunk native vlan <ネイティブ VLAN ID> と入力します。
18. switchport trunk allowed vlan <MGMT VLAN ID, BareMetalVlan VLANID, guest-Vlan VLAN ID, guest-VLAN-1000 VLANID, guest-VLAN-1001 VLANID, NFS VLAN ID, vMotion VLAN ID> と入力します。
19. spanning-tree port type edge trunk と入力します。
20. no shut と入力します。
21. exit と入力します。
22. interface Port-Channel 103 と入力します。
23. switchport mode trunk と入力します。
24. switchport trunk native vlan <ネイティブ VLAN ID> と入力します。
25. no shut と入力します。
26. exit と入力します。
27. interface Port-Channel 104 と入力します。
28. switchport mode trunk と入力します。
29. switchport trunk native vlan <ネイティブ VLAN ID> と入力します。
30. no shut と入力します。
31. exit と入力します。
32. interface Port-Channel 10 と入力します。
33. switchport mode trunk と入力します。
34. switchport trunk native vlan <ネイティブ VLAN ID> と入力します。

35. switchport trunk allowed vlan <300> と入力します。
36. no shut と入力します。
37. exit と入力します。
38. copy run start と入力します。

イーサネット インターフェイスの設定

作成されたすべてのポート チャネルには、適切な VLAN に参加するようにインターフェイスが設定されている必要があります。デバイス間のポート チャネル上でイーサネット インターフェイスを設定するには、次の手順を実行します。

Cisco Nexus 5548 A

1. グローバル コンフィギュレーション モードから、interface Eth1/13 と入力します。
2. channel-group 100 mode active と入力します。
3. no shutdown と入力します。
4. exit と入力します。
5. interface Eth1/15 と入力します。
6. channel-group 101 mode active と入力します。
7. no shutdown と入力します。
8. exit と入力します。
9. interface Eth1/16 と入力します。
10. channel-group 102 mode active と入力します。
11. no shutdown と入力します。
12. exit と入力します。
13. interface Eth1/17 と入力します。
14. channel-group 103 mode active と入力します。
15. no shutdown と入力します。
16. exit と入力します。
17. interface Eth1/18 と入力します。
18. channel-group 104 mode active と入力します。
19. no shutdown と入力します。
20. exit と入力します。
21. interface Eth1/17 と入力します。
22. channel-group 103 mode active と入力します。
23. no shutdown と入力します。
24. exit と入力します。
25. interface vfc 17 と入力します。
26. bind interface Ethernet 1/17 と入力します。
27. switch port trunk allowed vsan 200 と入力します。

28. exit と入力します。
29. interface vfc 18 と入力します。
30. bind interface Ethernet 1/18 と入力します。
31. switch port trunk allowed vsan 200 と入力します。
32. exit と入力します。
33. copy run start と入力します。

Cisco Nexus 5548 B

1. グローバル コンフィギュレーション モードから、interface Eth1/13 と入力します。
2. channel-group 100 mode active と入力します。
3. no shutdown と入力します。
4. exit と入力します。
5. interface Eth1/15 と入力します。
6. channel-group 101 mode active と入力します。
7. no shutdown と入力します。
8. exit と入力します。
9. interface Eth1/16 と入力します。
10. channel-group 102 mode active と入力します。
11. no shutdown と入力します。
12. exit と入力します。
13. interface Eth1/17 と入力します。
14. channel-group 103 mode active と入力します。
15. no shutdown と入力します。
16. exit と入力します。
17. interface Eth1/18 と入力します。
18. channel-group 104 mode active と入力します。
19. no shutdown と入力します。
20. exit と入力します。
21. interface vfc 17 と入力します。
22. bind interface Ethernet 1/17 と入力します。
23. switch port trunk allowed vsan 200 と入力します。
24. exit と入力します。
25. interface vfc 18 と入力します。
26. bind interface Ethernet 1/18 と入力します。
27. switch port trunk allowed vsan 200 と入力します。
28. exit と入力します。
29. copy run start と入力します。

Nexus 1100 イーサネット ポートの設定

この項では、トラブルシューティング手順および検証のために、個々のポートの記述を作成し設定する方法について詳しく説明します。Cisco Nexus スイッチ A および B へのイーサネット ポートを作成するには、次の手順を実行します。

Cisco Nexus 5548 A

1. グローバル コンフィギュレーション モードから、interface Eth1/11 と入力します。
2. description <Nexus 1100 – A LOM A> と入力します。
3. switchport mode trunk と入力します。
4. switchport trunk allowed vlan 602,603,1000,1001,50 と入力します。
5. exit と入力します。
6. interface Eth1/12 と入力します。
7. description <Nexus 1100 – B LOM A> と入力します。
8. switchport mode trunk と入力します。
9. switchport trunk allowed vlan 602,603,1000,1001,50 と入力します。
10. exit と入力します。
11. copy run start と入力します。

Cisco Nexus 5548 B

1. グローバル コンフィギュレーション モードから、interface Eth1/11 と入力します。
2. description <Nexus 1100 – A LOM B> と入力します。
3. switchport mode trunk と入力します。
4. switchport trunk allowed vlan 602,603,1000,1001,50 と入力します。
5. exit と入力します。
6. interface Eth1/12 と入力します。
7. description <Nexus 1100 – B LOM B> と入力します。
8. switchport mode trunk と入力します。
9. switchport trunk allowed vlan 602,603,1000,1001,50 と入力します。
10. exit と入力します。
11. copy run start と入力します。

FlexPod Cisco Nexus 1000V vSphere

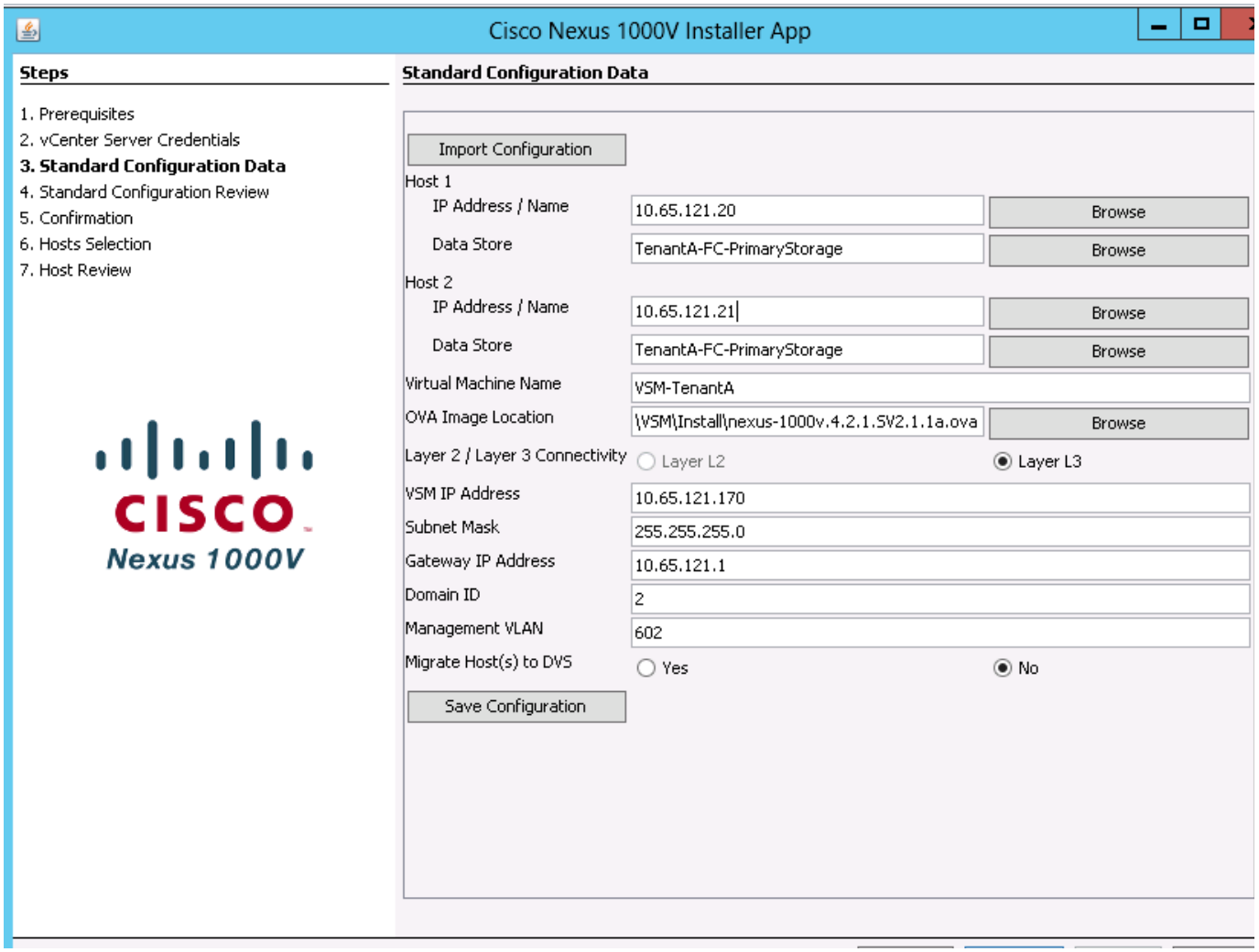
次の項では、FlexPod 構成に、ペアの高可用性（HA）Cisco Nexus 1000V ソフトウェア DVS スイッチをインストールする手順を詳しく説明します。プライマリおよびスタンバイの Cisco Nexus 1000V 仮想スーパーバイザ モジュール（VSM）が、個別の ESX ホストにインストールされます。この説明の終盤で、Cisco Nexus 1000V 分散仮想スイッチ（DVS）をプロビジョニングします。

この手順では、Cisco Nexus 1000V ソフトウェア バージョン 4.2.1(1)SV2(1.1a) が www.cisco.com からダウンロードされ、展開されていると想定しています。また、2 つの ESX ホストに、VMware vSphere 5.1 が Enterprise Plus ライセンスを使用してインストールされ、Infrastructure Pod の一部である VMware vCenter 5.1 アプリケーションがインストールされていることも想定しています。

プライマリおよびセカンダリ Cisco Nexus 1000V VSM のインストール

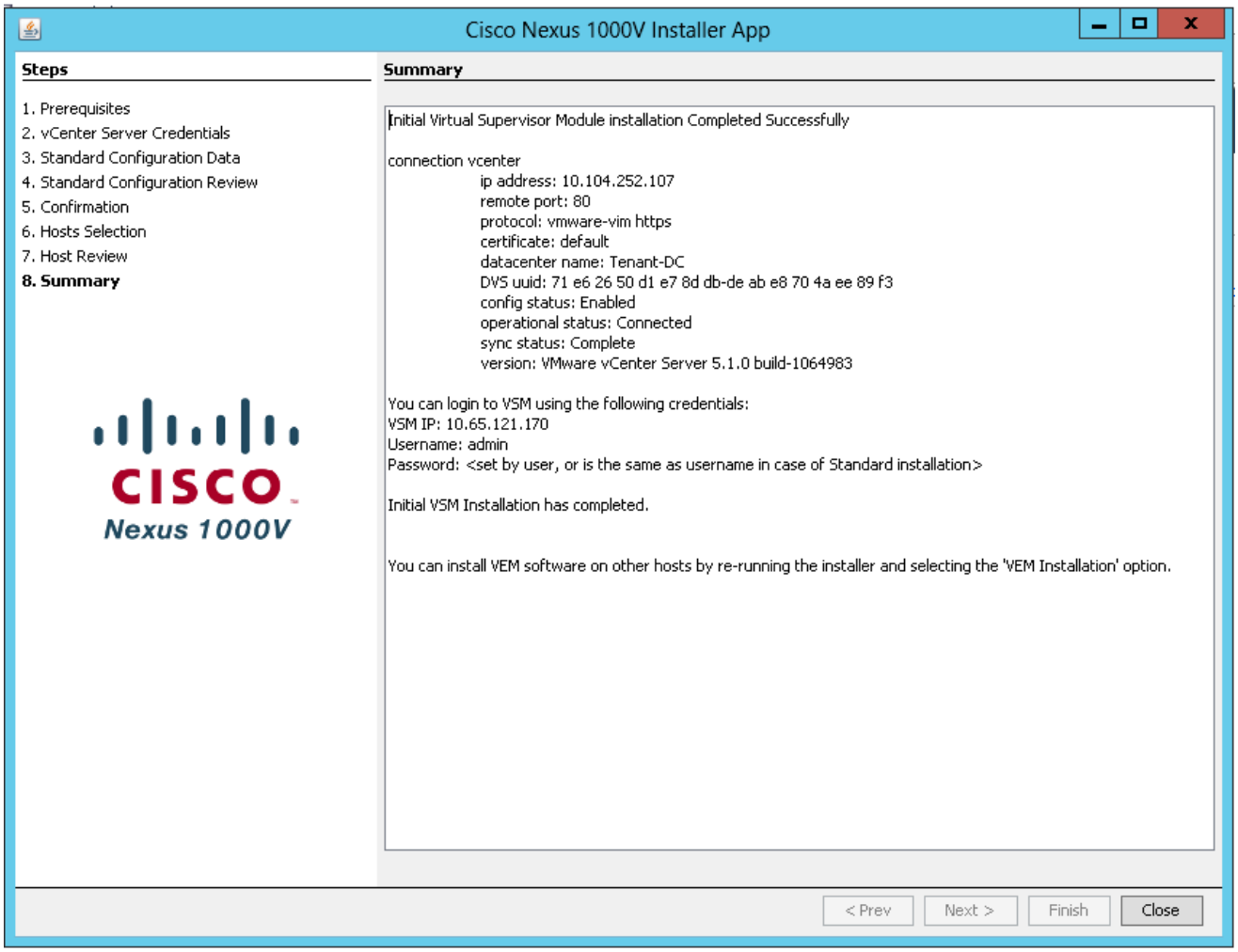
1. Infrastructure Windows クライアントでコマンド プロンプトから Nexus1000V-install_CNX.jar ファイルを起動します。
2. [Cisco Nexus 1000V Complete Installation] オプション ボタンをクリックします。
3. [Standard Type] を選択します。
4. [Next] をクリックします。
5. vCenter IP アドレス <xx.xx.xx.xx> を入力し、ユーザ ID <管理者> およびパスワード <XXXXXX> を入力します。
6. [Next] をクリックします。
7. ESX ホスト 1 の IP アドレス <xx.xx.xx.xx> と共有データ ストア <xxxxxxxx> を入力するか参照します。
8. ESX ホスト 2 の IP アドレス <xx.xx.xx.xx> と共有データ ストア <xxxxxxxx> を入力するか参照します。
9. 仮想マシン名 <VSM-TenantA> を入力します。
10. ローカル Nexus 1000V ソフトウェア <nexus-1000v.4.2.1.1.SV2.1.1a.ova> ファイルへのパスを参照します。
11. [Layer 2 / Layer 3 Connectivity] には、デフォルトで [Layer 3] オプション ボタンが選択されています。

図 8　　Cisco Nexus 1000V 標準設定データの詳細



12. [Next] をクリックします。
13. 標準設定レビュー データを確認します。
14. [Next] をクリックします。
15. [Do you want to add more modules] で [No] オプション ボタンをクリックします。
16. [Next] をクリックします。
17. [Host Selection] で [Next] をクリックします。
18. [Host Review] で [Finish] をクリックします。

図 9　　Cisco Nexus 1000V 標準インストールの概要の詳細



Cisco Nexus 1000V 仮想アプライアンスの設定

Cisco Nexus 1000V

Cisco Nexus 1000-V VSM-TenantA-1 を設定するには、次の手順を実行します。

1. VMware VI クライアントを使用して ESX ホスト 10.65.121.20 上の VSM-TenantA-1 VM にログインします。

```
Enter the User Name <<admin>>
Enter Password <<admin>>
Enter <<Conf Terminal>>
Enter <<feature ssh>> <<feature telnet>> <<feature http-server>>
Enter <<Copy run start>>
```

2. プライマリ VSM の基本設定を実行します。

プライマリ VSM の基本設定を実行するには、次の手順を実行します。

1. SSH クライアントを使用して、プライマリ Cisco Nexus 1000V VSM に admin としてログインします。
2. 次のコンフィギュレーション コマンドを実行します。

```
config t
ntp server <<var_global_ntp_server_ip>> use-vrf management
vlan <<var_ib-mgmt_vlan_id 602>>
name IB-MGMT-VLAN
vlan <<var_guest_vlan_id 603>>
name guestVM-VLAN
vlan <<var_guest_vlan_id 1000>>
name guestVM-VLAN1000
vlan <<var_guest_vlan_id 1001>>
name guestVM-VLAN1001
exit
port-profile type ethernet TenantA-guest-Uplink
vmware port-group
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<default 1>>,<<var_ib-mgmt_vlan_id 602>>, <<
var_guest_vlan_id 603>>,<<var_guest_vlan_id 1000>>, <<var_N1KV_Ctrl_vlan_id 50>>, <<
var_guest_vlan_id 1001>>
channel-group auto mode on mac-pinning
no shutdown
system vlan <<var_ib-mgmt_vlan_id 602>>, << var_guest_vlan_id 603>>,
<<var_guest_vlan_id 1000>>, << var_guest_vlan_id 1001>>
system mtu 9000
state enabled
port-profile type vethernet TenantA-VSM-VEM-Network
vmware port-group
switchport mode access
switchport access vlan <<var_ib-mgmt_vlan_id 602>>
no shutdown
capability l3control
system vlan <<var_ib-mgmt_vlan_id 602>>
state enable
exit
copy run start
```

Cisco UCS の導入

次の項では、FlexPod 環境で使用できるように Cisco Unified Computing System を設定する手順について詳しく説明します。これらの手順には正確に従ってください。そうしないと不適切な設定になってしまう可能性があります。

この項では、Cisco UCS の設定に役立つ次のタスクを実行する方法について説明します。

- Cisco UCS 6248 ファブリック インターコネクトの設定
- シャーシ ディスカバリ ポリシーの変更
- アップリンク ポート チャネルの作成
- ジャンボ フレームの有効化
- Cisco UCS 6248 ファブリック インターコネクトでの QoS ポリシーの有効化
- Cisco Nexus 5548UP スイッチでの QoS 認定の有効化
- Cisco UCS 6248 ファブリック インターコネクトでの VLAN の設定

Cisco UCS 6248 ファブリック インターコネクトの設定

Cisco UCS 6248 ファブリック インターコネクト A および B で初期セットアップを行うには、次の手順を実行します。

ファブリック インターコネクト A

1. 最初の Cisco UCS 6248 ファブリック インターコネクト上のコンソール ポートに接続します。
2. 設定方法を入力するように求められたら、console と入力して続行します。
3. 新しいセットアップを行うか、バックアップから復元するか尋ねられたら、setup と入力して続行します。
4. y と入力して、新しいファブリック インターコネクトのセットアップを続行します。
5. y と入力して、強力なパスワードを強制します。
6. 管理者ユーザのパスワードを入力します。
7. 同じパスワードを繰り返し入力して、管理者ユーザのパスワードを確認します。
8. このファブリック インターコネクトがクラスタの一部であるかどうかを尋ねられたら、y と答えて続行します。
9. スイッチ ファブリックに A と入力します。
10. システム名にクラスタ名を入力します。
11. Mgmt0 の IPv4 アドレスを入力します。
12. Mgmt0 の IPv4 ネットマスクを入力します。
13. デフォルト ゲートウェイの IPv4 アドレスを入力します。
14. クラスタの IPv4 アドレスを入力します。
15. DNS を設定するには、y と答えます。
16. DNS の IPv4 アドレスを入力します。
17. y と答えて、デフォルト ドメイン名を設定します。
18. デフォルト ドメイン名を入力します。
19. コンソールに出力された設定を確認し、正しければ yes と答えて設定を保存します。
20. ログイン プロンプトが表示されるまで待機し、設定が保存されたことを確認します。

ファブリック インターコネクト B

1. 2 番目の Cisco UCS 6248 ファブリック インターコネクト上のコンソール ポートに接続します。
2. 設定方法を入力するように求められたら、console と入力して続行します。
3. インストーラはパートナーのファブリック インターコネクトを検出し、クラスタにそのファブリック インターコネクトを追加します。y を入力し、インストールを続行します。
4. 最初のファブリック インターコネクトの管理者パスワードを入力します。
5. Mgmt0 の IPv4 アドレスを入力します。
6. yes と答えて、設定を保存します。
7. ログイン プロンプトが表示されるまで待機し、設定が保存されたことを確認します。

Cisco UCS Manager へのログイン

Cisco UCS ファブリック インターコネクトが設定されたら、次の手順で、Cisco UCS Manager ソフトウェアをダウンロードし、使用開始します。Cisco UCS Manager にログインするには、対の手順を実行します。

1. Web ブラウザを開き、Cisco UCS 6248 ファブリック インターコネクトのクラスタ アドレスに移動します。
2. [Launch] リンクを選択して、Cisco UCS Manager ソフトウェアにアクセスします。
3. セキュリティ証明書を承諾するように求められたら、必要に応じて承諾します。
4. プロンプトが表示されたら、ユーザ名に admin と入力し、管理者パスワードを入力して、[Login] をクリックして Cisco UCS Manager にログインします。
5. 左ペインの [Equipment] タブをクリックします。
6. [Fabric Interconnects A] を選択します。
7. 右ペインで、[General] タブをクリックします。
8. [Configure Unified Ports] を選択します。
9. [Yes] を選択してウィザードを起動します。
10. スライダ ツールで 1 つの位置を左に動かして、最後の 2 つのポート（31 と 32）を FC アップリンク ポートとして設定します。
11. ポート 31 と 32 には、FC アップリンク ポートとして再設定されたことを示す「B」インジケータが付けられます。
12. [Finish] をクリックします。
13. [OK] をクリックします。
14. プライマリ ファブリック インターコネクトが再起動すると、Cisco UCS Manger GUI が閉じます。
15. 正常に再起動したら、Web ブラウザを開いて、Cisco UCS 6248 ファブリック インターコネクトのクラスタ アドレスに移動します
16. プロンプトが表示されたら、ユーザ名に admin と入力し、管理者パスワードを入力します。

シャーシ ディスカバリ ポリシーの変更

基本アーキテクチャに、Cisco UCS シャーシに取り付けられた各ファブリック エクステンダからの 2 つのアップリンクが含まれるので、この項では、シャーシ ディスカバリ ポリシーを変更する方法について詳しく説明します。

クラウド上のワークロードが、ネットワーク中心になると予想される場合、B200 M3 ブレード サーバの帯域幅を増やすことができます。UCS シャーシのファブリック エクステンダ（IOM）とファブリック インターコネクト間のリンク数を増やすと、帯域幅のオーバーサブスクリプションは減少します。物理的なリンク数に一致するように、機器の下の「シャーシ ディスカバリ ポリシー」でリンク数を変更します。できれば、シャーシ ディスカバリ ポリシーは、サーバ ポートの設定前に変更してください。シャーシが検出された後に、ファブリック インターコネクトとファブリック エクステンダ間のリンクを追加または削除する場合、「シャーシの確認」を行う必要があります。

（注） シャーシの確認では、シャーシ内のサーバはリブートしません。

シャーシ ディスカバリ ポリシーを変更するには、Cisco UCS Manager にログインして、次の手順を実行します。

1. 左ペインの [Equipment] タブをクリックします。

2. 右ペインで、[Policies] タブをクリックします。
3. [Global Policies] の下で、[Chassis Discovery Policy] を [2-link] に変更します。
4. [Save Changes] をクリックします。

ポート チャネルの設定

ポート チャネルを設定するには、次の手順を実行します。

1. 左ペインの [Equipment] タブをクリックします。
2. [Fabric Interconnects A] を選択します。
3. 右ペインの [Actions] の下で、[LAN UpLinks Manager] タブをクリックします。
4. [Create Port Channel] をクリックしてから [Fabric A] を選択します。
5. ID を「101」に、名前を「Tenant1CloudVPCNetworkA」に指定します。
6. [Add Ports] で、[Ports] をクリックし、「5」と「6」の番号を指定します。
7. [Finish] をクリックします。
8. デフォルトでは、「Tenant1CloudVPCNetworkB」のポート チャネルは無効になっています。[Enable] をクリックします。
9. ファブリックを「有効化/無効化」するように求める警告メッセージが表示されたら、[Yes] をクリックします。
10. [Fabric Interconnects B] を選択します。
11. 右ペインの [Actions] の下で、[LAN UpLinks Manager] タブをクリックします。
12. [Create Port Channel] を右クリックして、[Fabric A] を選択します。
13. ID を「102」に、名前を「Tenant1CloudVPCNetworkB」に指定します。
14. [Add Ports] で、[Ports] をクリックし、「5」と「6」の番号を指定します。
15. [Finish] をクリックします。
16. デフォルトでは、「Tenant1CloudVPCNetworkB」のポート チャネルは無効になっています。[Enable] をクリックします。
17. ファブリック B を「有効化/無効化」するように求める警告メッセージが表示されたら、[Yes] をクリックします。

（注） Cisco Nexus 5548UP を vPC で設定する場合、すべての vPC のステータスが接続されているイーサネット ポートに対して「アップ」であることを確認します。

Cisco Nexus 5548UP コマンド出力でのポート チャネル ステータス：

```
N5548-Switch-A(config-if)# sh vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                     : 100
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status       : success
Type-2 consistency status         : success
Type-2 consistency reason         : QoSMgr Qos configuration incompatible
vPC role                          : primary
Number of vPCs configured         : 2
Peer Gateway                      : Disabled
```

```
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled
vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po100  up     1,192-195,602-603,607,20
vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
101    Po101       up     success     success         1,602-603,1000-1001,192-193,20
102    Po102       up     success     success         1,602-603,1000-1001,192-193,20
103    Po103       up     success     success            1,192-193,200-300
104    Po104       up     success     success            1,192-193,200-300
N5548-Switch-B(config-if)# sh vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                   : 100
Peer status                     : peer adjacency formed ok
vPC keep-alive status           : peer is alive
Configuration consistency status: success
Per-vlan consistency status     : success
Type-2 consistency status       : success
Type-2 consistency reason       : QoSMgr Qos configuration incompatible
vPC role                        : primary
Number of vPCs configured       : 2
Peer Gateway                    : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled
vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po100  up     1,192-195,602-603,607,20
vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
101    Po101       up     success     success        1,1000-10001,602-603,192-193,20
102    Po102       up     success     success        1,1000-10001,602-603,192-193,20
103    Po103       up     success     success           1,192-193,200,300
104    Po104       up     success     success           1,192-193,200,300
```

アップリンク イーサネット ポートの作成

LAN トラフィックは、アップリンク ポートを使用してファブリック インターコネクト上で Cisco UCS システムに入出力します。さまざまなタイプのアップリンク ポートがあり、ここでは、アップリンク ポート チャネルは NetApp ストレージに接続するように設定されています。

Cisco UCS 環境で必要なアップリンク ポート チャネルを作成し設定するには、Cisco UCS Manager にログインして次の手順を実行します。

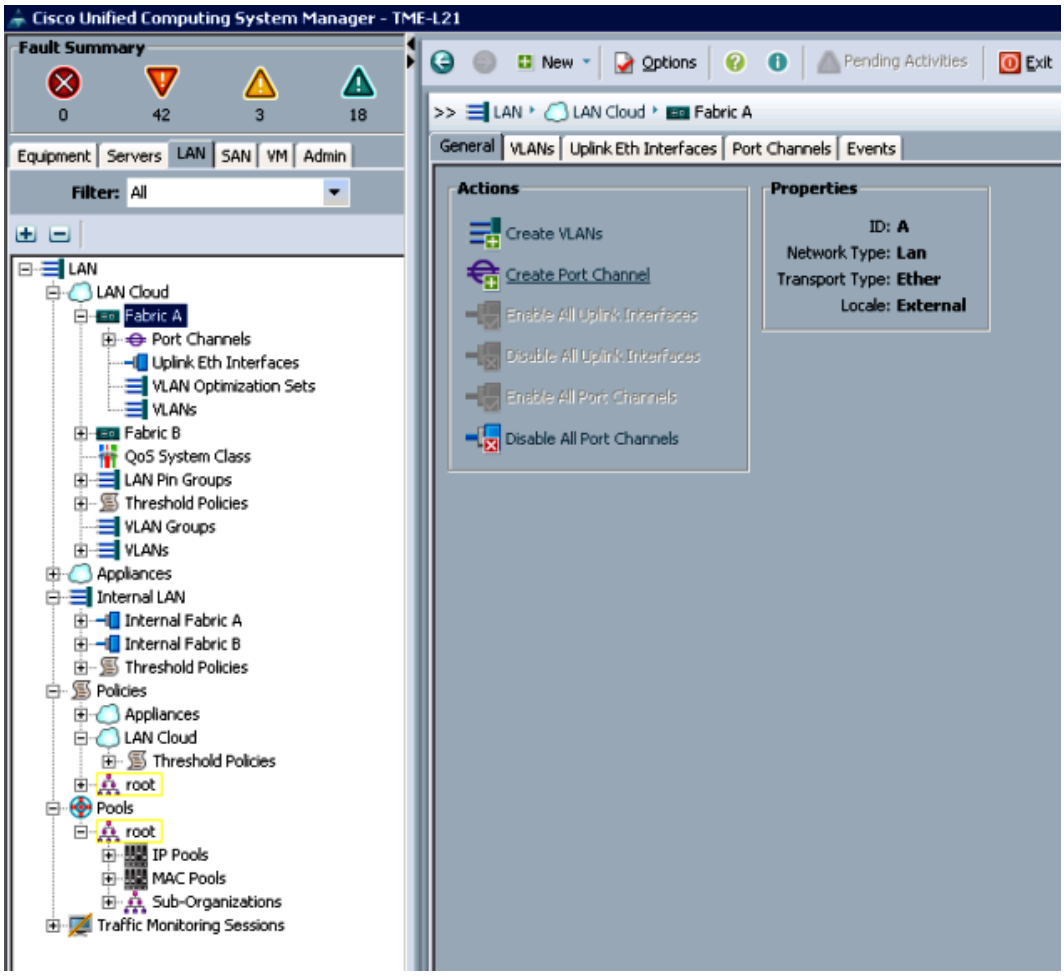
ファブリック インターコネクト A

1. 左ペインで [LAN] タブをクリックします。

（注） 一方はファブリック A から両方の Cisco Nexus 5548 スイッチに、もう一方はファブリック B から両方の Cisco Nexus 5548 スイッチに接続する 2 つのポート チャネルが作成されます。

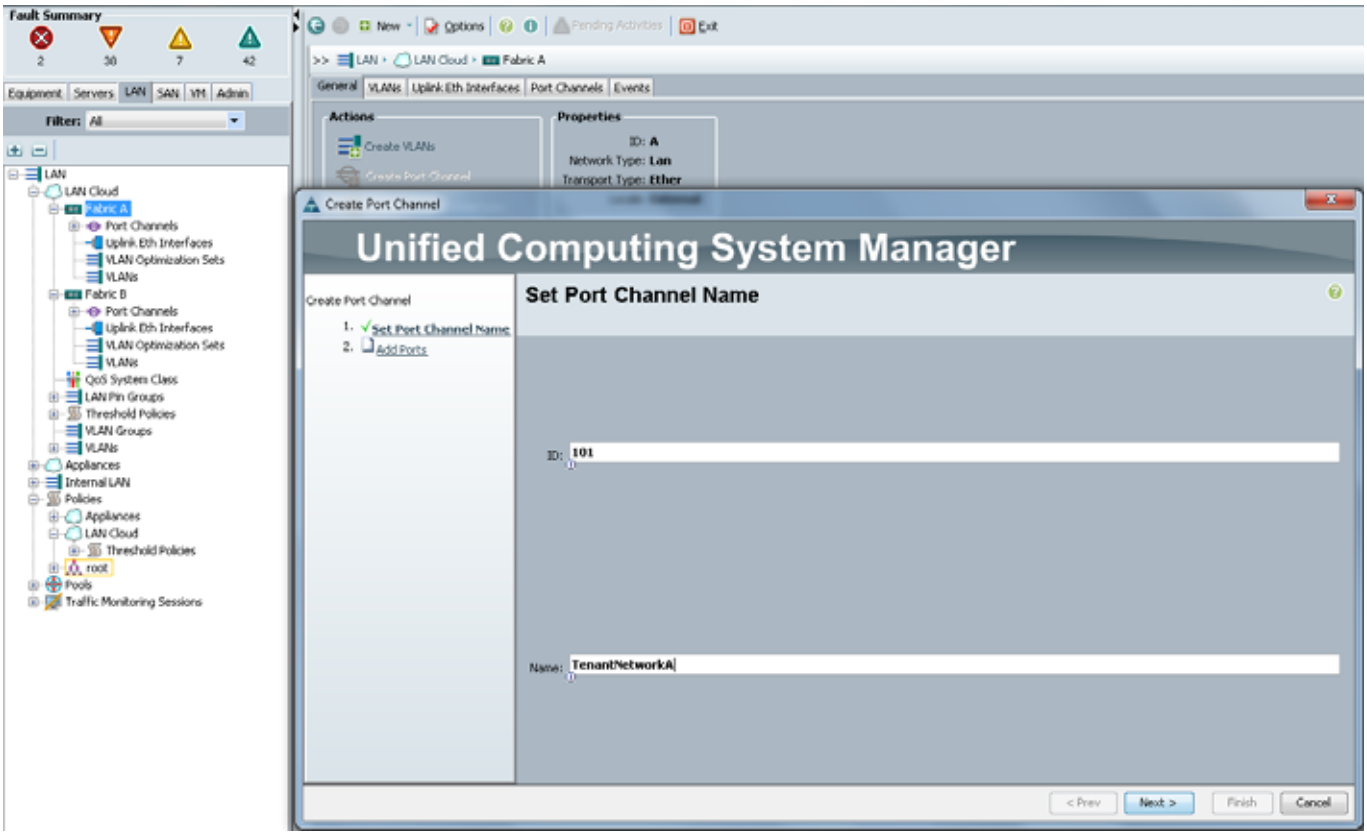
2. [LAN Cloud] の下で [Fabric A] ツリーを展開します。
3. 右ペインの [General] タブの下で、[Create Port Channel] をクリックします。

図 10　　アップリンク ポート チャネルの作成



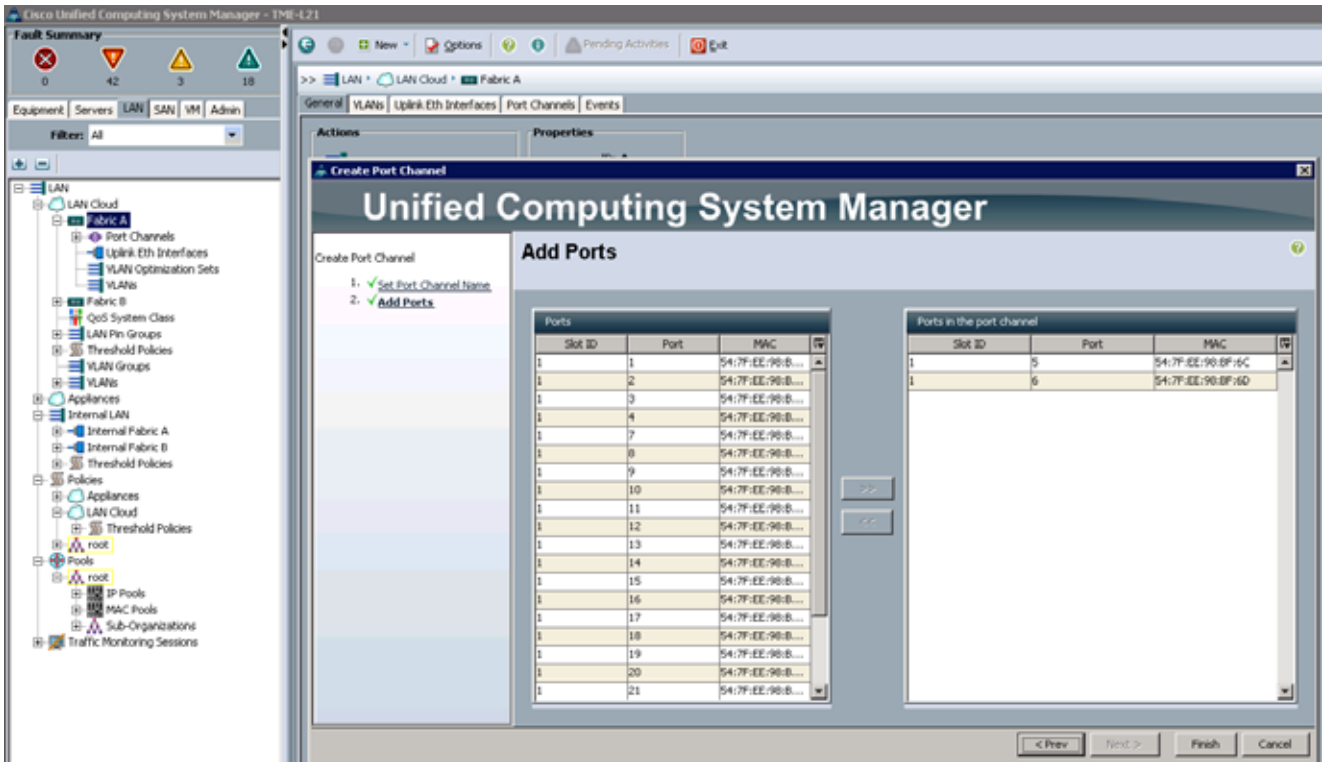
4. ポート チャネルの一意の ID として 101 を入力します。
5. ポート チャネルの名前として Tenant Network A と入力します。
6. [Next] をクリックします。

図 11　　ポート チャネルの名前設定



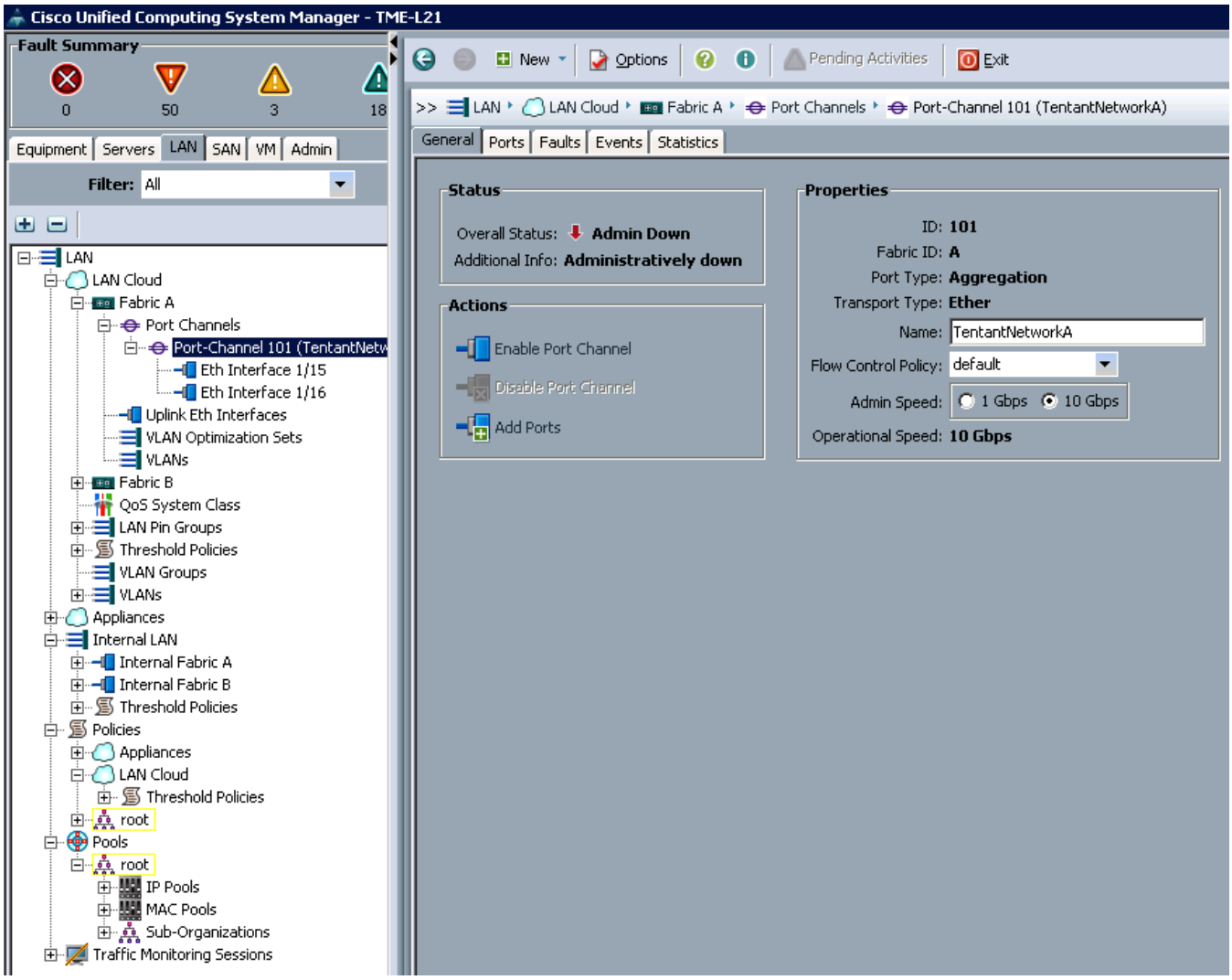
7. [Ports] リストから、[Slot ID] が 1 で [Port] が 5 のポートと、[Slot ID] が 1 で [Port] が 6 のポートを選択します。
8. [>>] をクリックして、ポート チャネルにポートを追加します。

図 12　　ポートの選択と追加



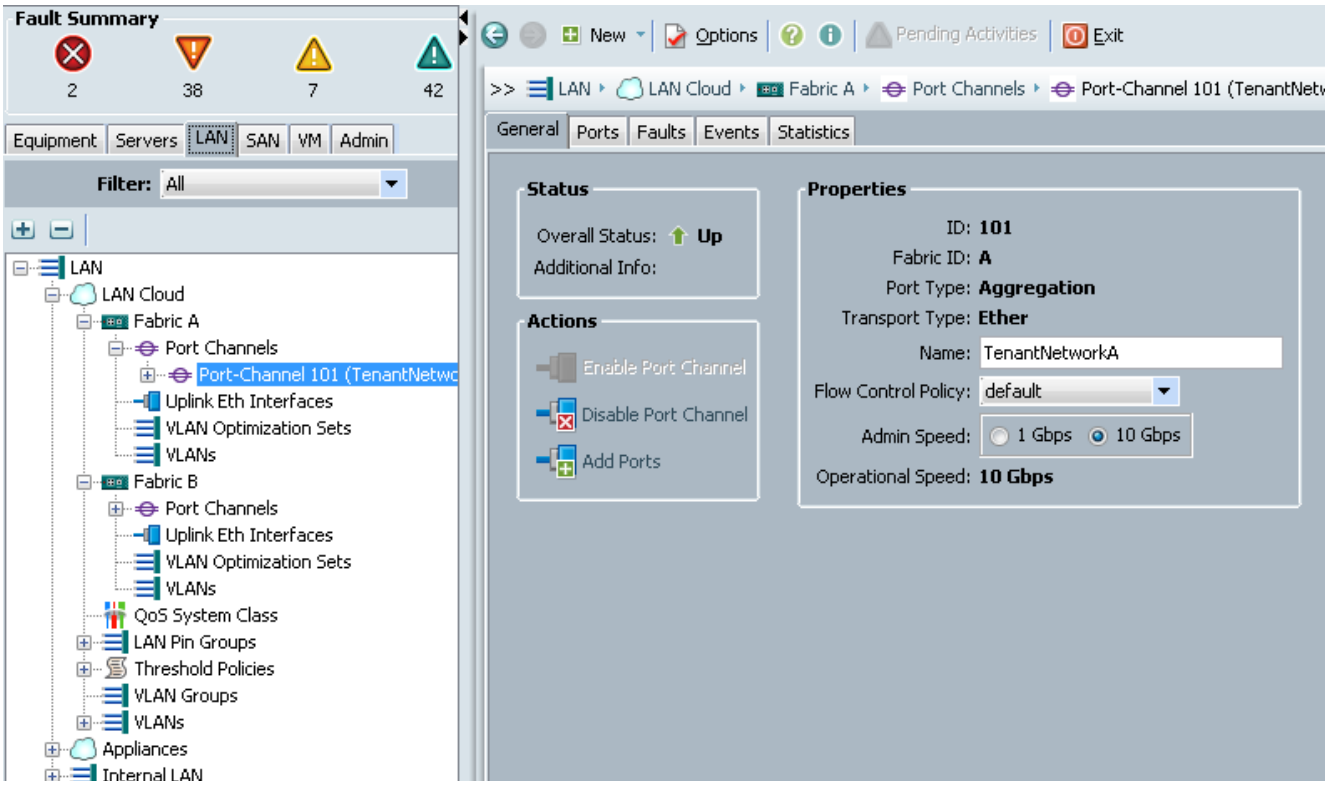
9. [Finish] をクリックしてポート チャネルを作成します。
10. [Show navigator for Port-Channel 101 (Fabric A)] チェックボックスをオンにします。
11. [OK] をクリックします。
12. [Actions] 領域で [Enable Port Channel] を選択します。
13. ポップアップ ボックスで [Yes] をクリックし、[OK] をクリックしてポート チャネルを有効化します。

図 13　　ポート チャネルの有効化



14. ポート チャネルの全体的なステータスがアップになるまで待機します。
15. [OK] をクリックしてナビゲータを閉じます。

図 14　　ポート チャネル ステータスの確認



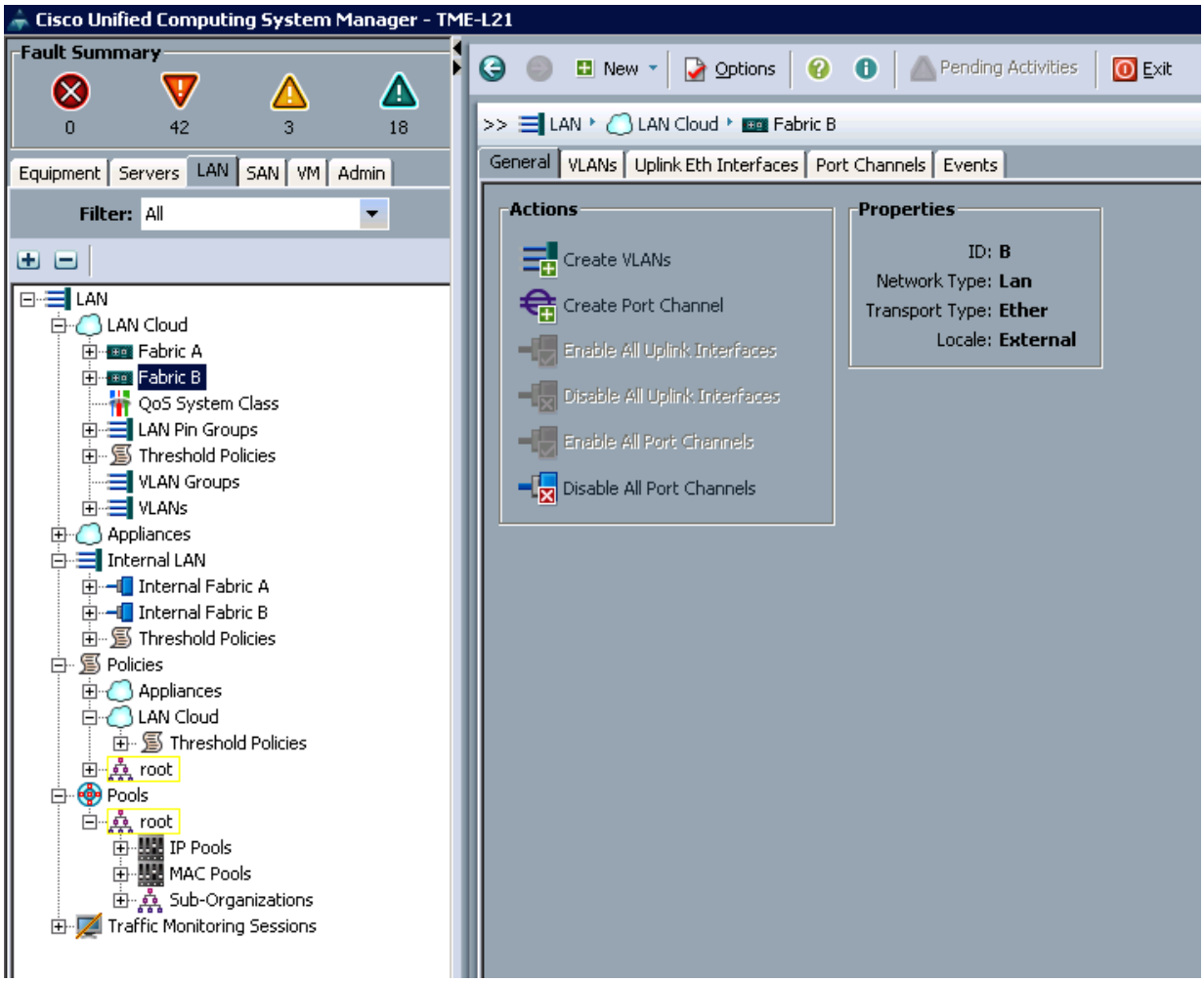
ファブリック インターコネクト B

1. 左ペインで [LAN] タブをクリックします。

（注）　一方はファブリック A から両方の Cisco Nexus 5548 スイッチに、もう一方はファブリック B から両方の Cisco Nexus 5548 スイッチに接続する 2 つのポート チャネルが作成されます。

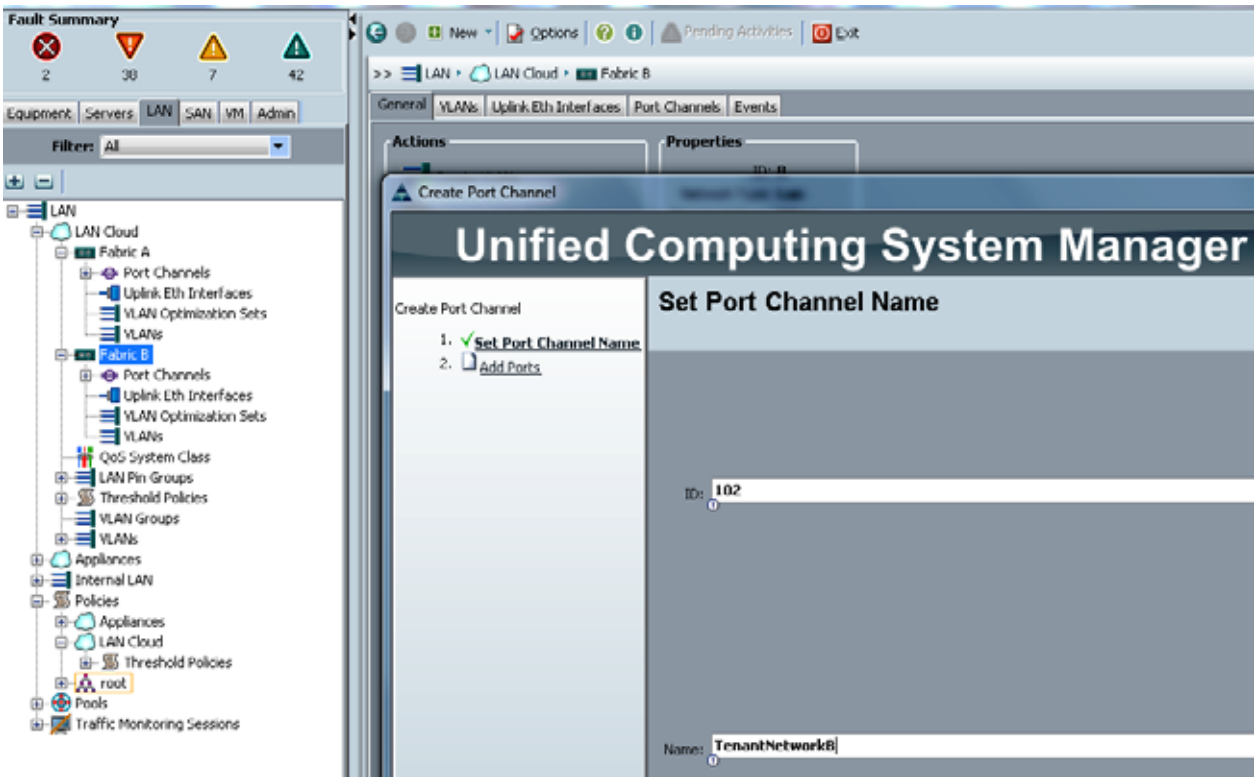
2. [LAN Cloud] の下で [Fabric B] ツリーを展開します。
3. 右ペインの [General] タブの下で、[Create Port Channel] をクリックします。

図 15　　ポート チャネルの作成



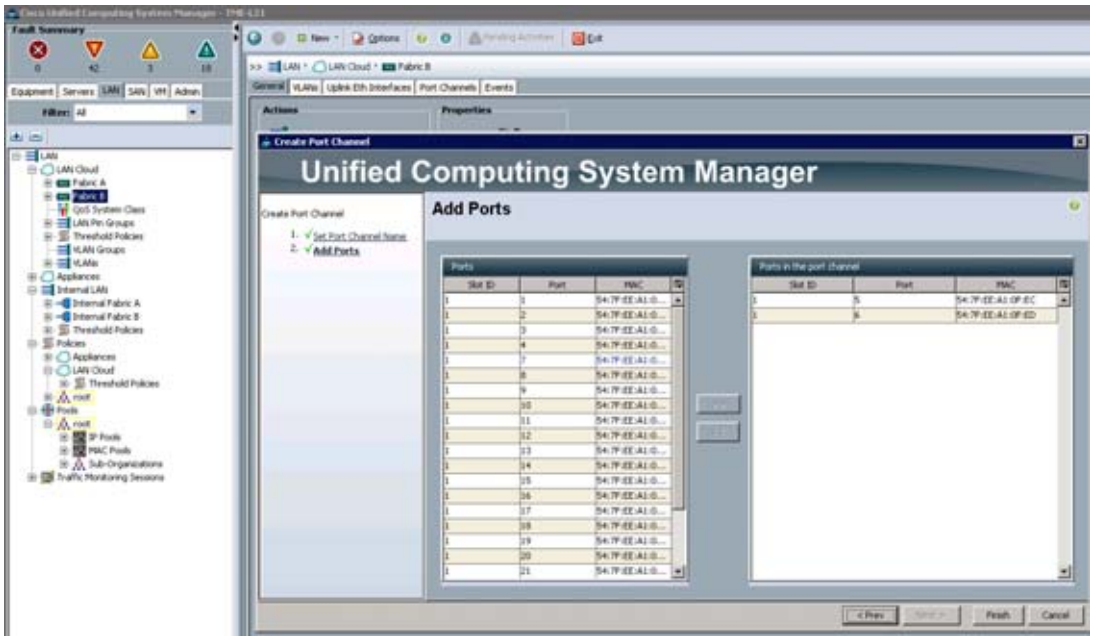
4. ポート チャネルの一意の ID として 102 を入力します。
5. ポート チャネルの名前として Tenant Network B と入力します。
6. [Next] をクリックします。

図 16　　ポート チャネルの ID および名前の設定



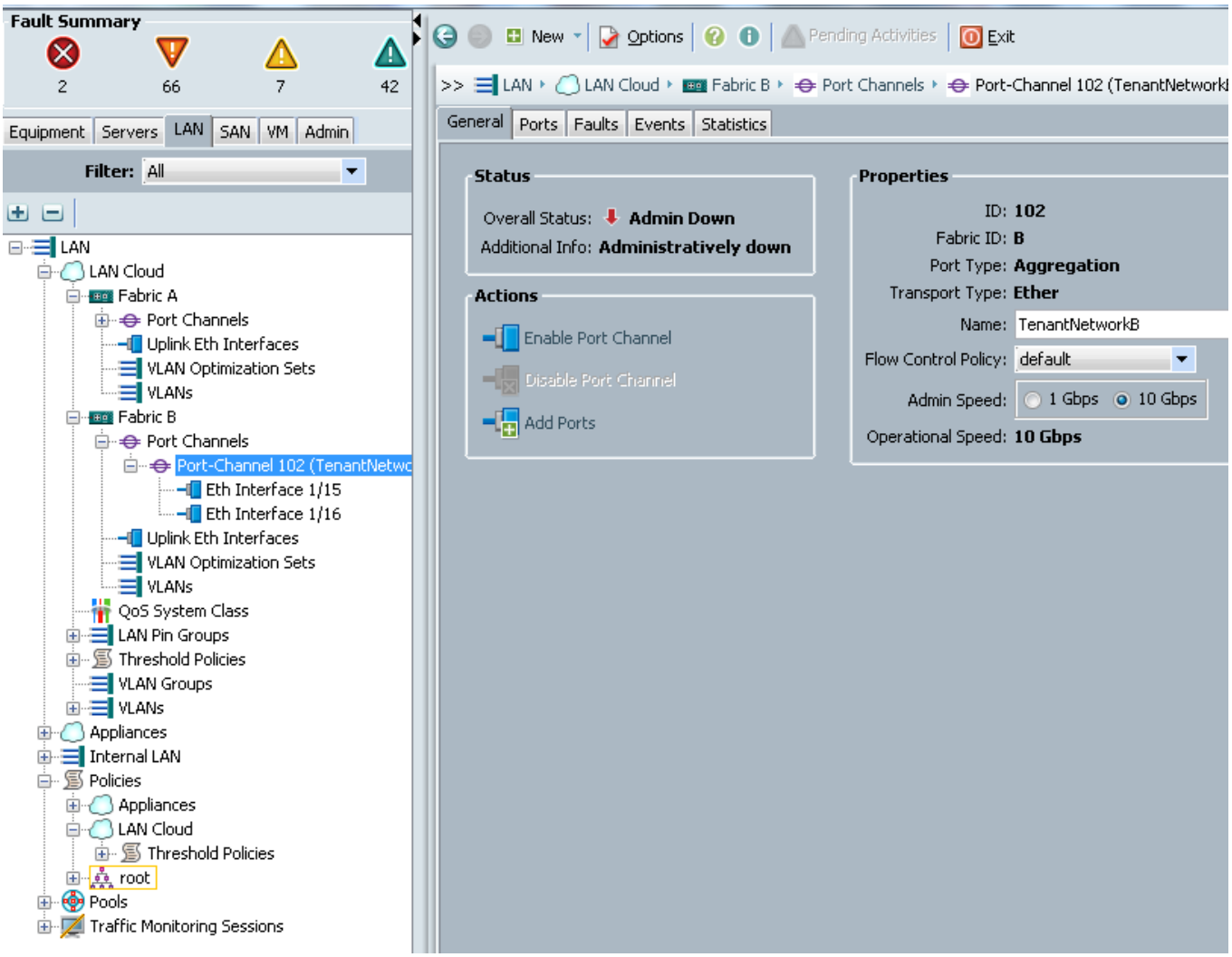
7. [Ports] リストから、[Slot ID] が 1 で [Port] が 5 のポートと、[Slot ID] が 1 で [Port] が 6 のポートを選択します。
8. [>>] をクリックして、ポート チャネルにポートを追加します。

図 17　　ポートの選択と追加



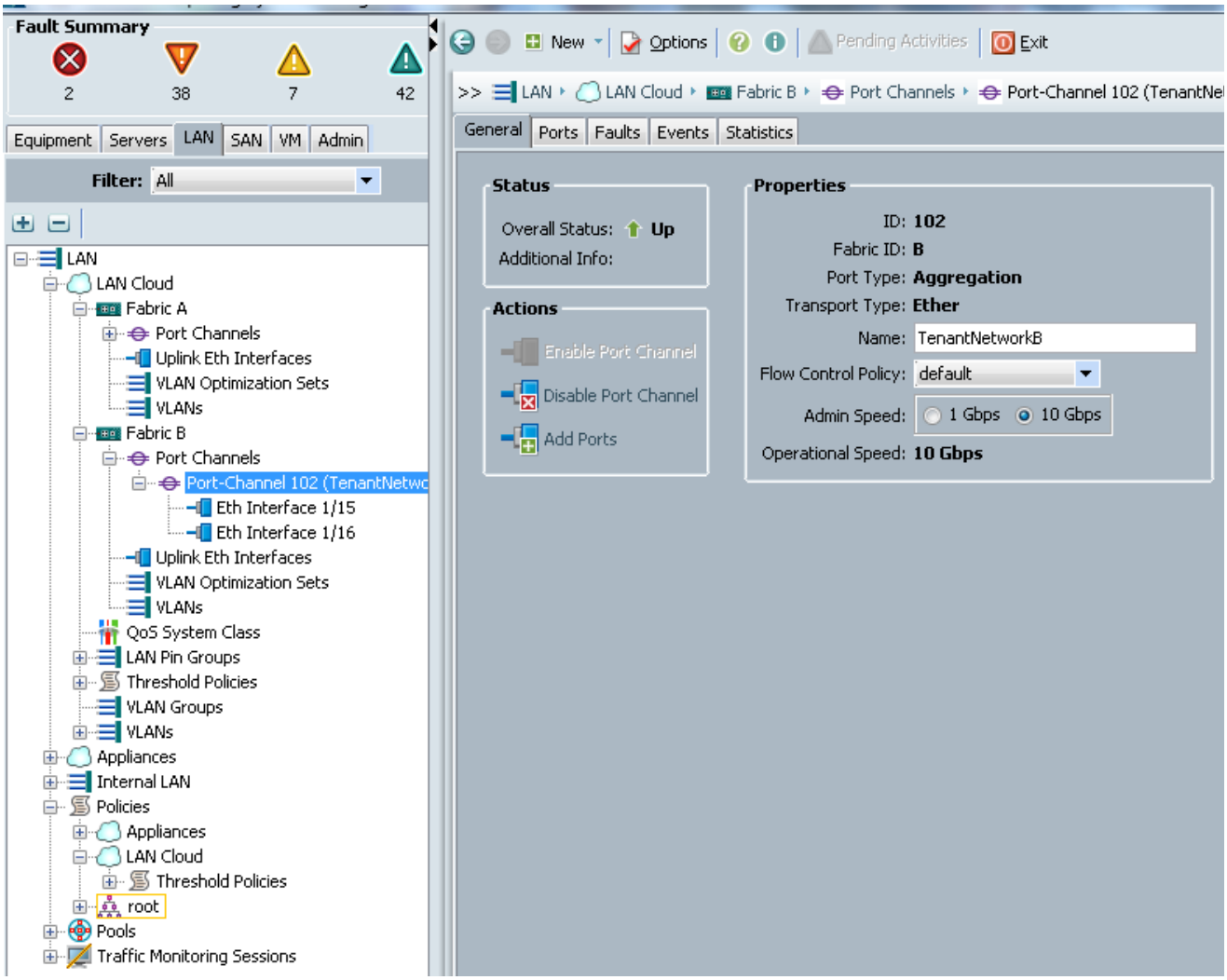
9. [Finish] をクリックしてポート チャネルを作成します。
10. [Show navigator for Port-Channel 101 (Fabric A)] チェックボックスをオンにします。
11. [OK] をクリックして作業を続行します。
12. [Actions] 領域で [Enable Port Channel] を選択します。
13. ポップアップ ボックスで [Yes] をクリックし、[OK] をクリックします。

図 18　　ポート チャネルの有効化



14. ポート チャネルの全体的なステータスがアップになるまで待機します。
15. [OK] をクリックしてナビゲータを閉じます。

図 19　　ポート チャネル ステータスの確認



ジャンボ フレームの有効化

Cisco UCS Manager から、Cisco UCS ファブリック内の定義済み Quality of Service クラスにジャンボ フレーム（9000 バイトのフレーム）を設定するには、次の手順を実行します。

1. 左ペインで [LAN] タブをクリックします。
2. [LAN Cloud] > [QoS System Class] の順に選択します。
3. 右ペインで、[General] タブをクリックします。
4. プラチナ、ゴールド、シルバー、ブロンズのプライオリティ値に対応する [MTU] ボックスに 9000 と入力します。
5. [Save Changes] をクリックします。
6. [OK] をクリックして作業を続行します。

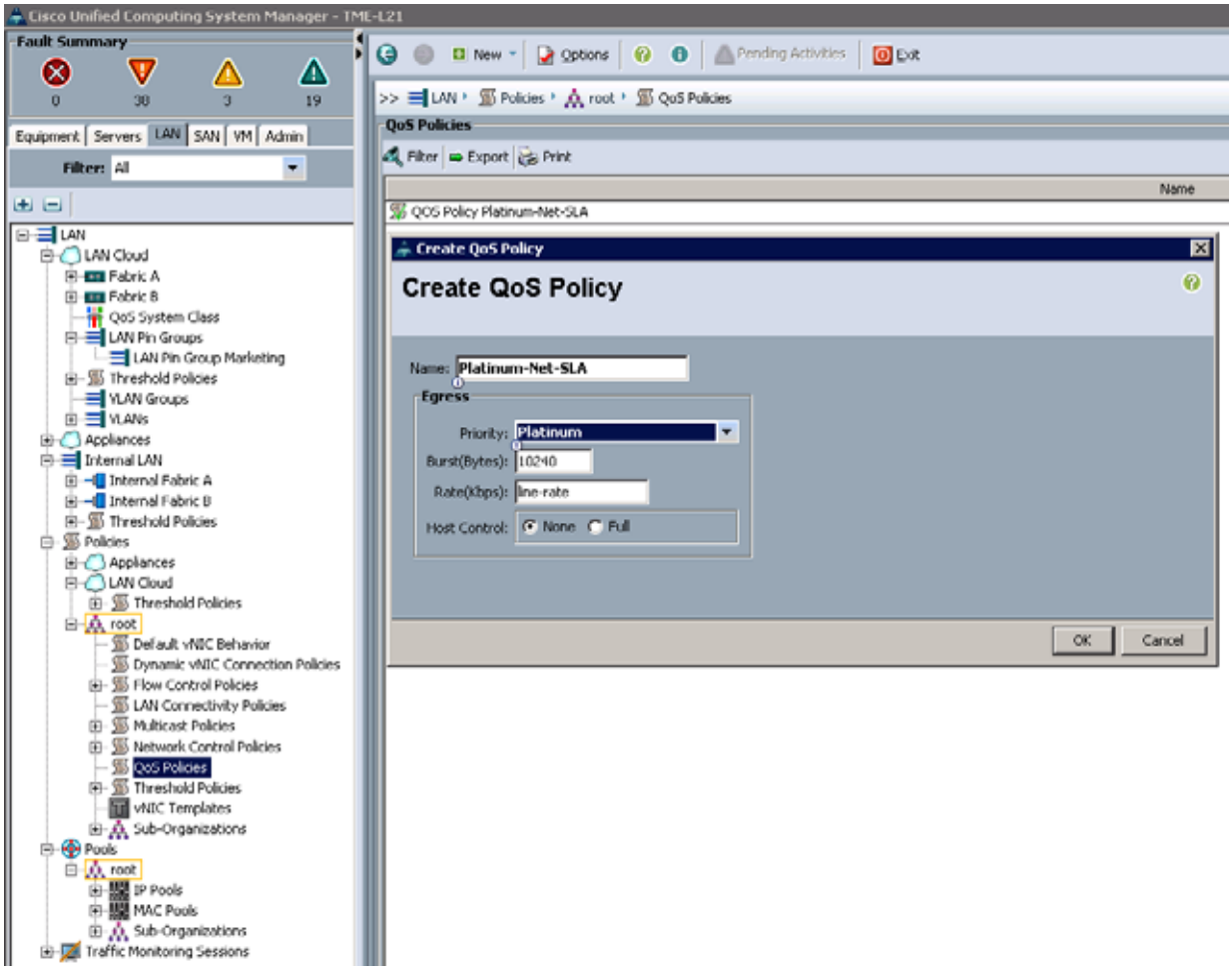
Cisco UCS 6248 ファブリック インターコネクトでの QoS の有効化

この項では、Quality of Service（QoS）ポリシー（プラチナ、ゴールド、シルバー、ブロンズ、およびファイバ チャネル）がソリューション デザインの Cisco UCS ファブリック上に作成され、有効化されます。

以前に定義した Quality of Service ポリシーを Cisco UCS ファブリック上で有効化するには、Cisco UCS Manager にログインして次の手順を実行します。

1. [LAN] > [Policies] > [QoS Policies] の順に選択します。
2. [QoS Policies] を右クリックします。
3. [Create QoS Policy] を選択します。
4. QoS ポリシー名として Platinum-Net-SLA と入力します。
5. プライオリティを [Platinum] に変更します。[Burst(Bytes)] のデフォルト値（10240）、[Rate (Kbps)] のデフォルト値（line-rate）、および [Host Control] のデフォルト値（None）をそのままにします。
6. [OK] をクリックします。

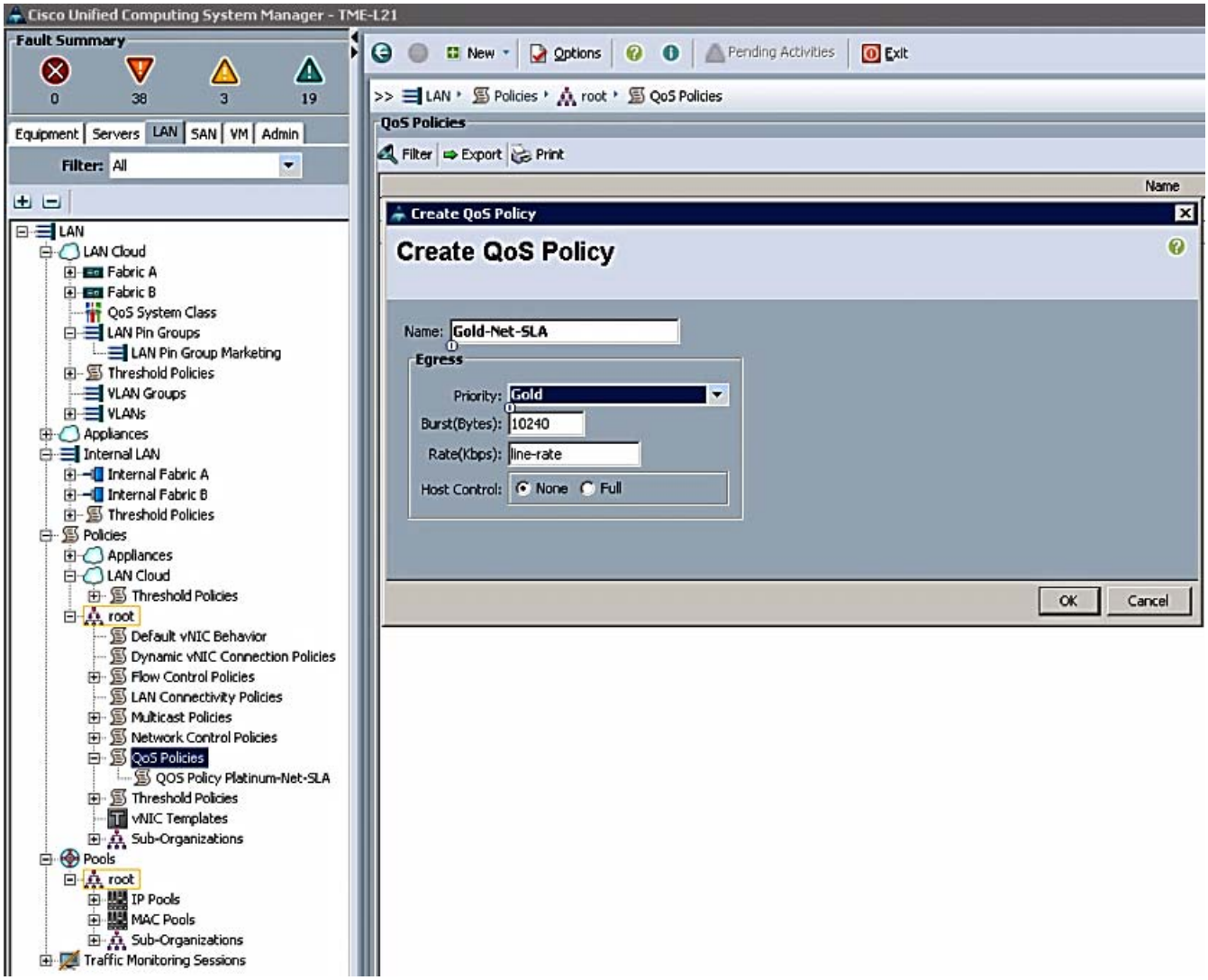
図 20　　プラチナ QoS ポリシーの名前指定と設定



7. [QoS Policies] を右クリックします。

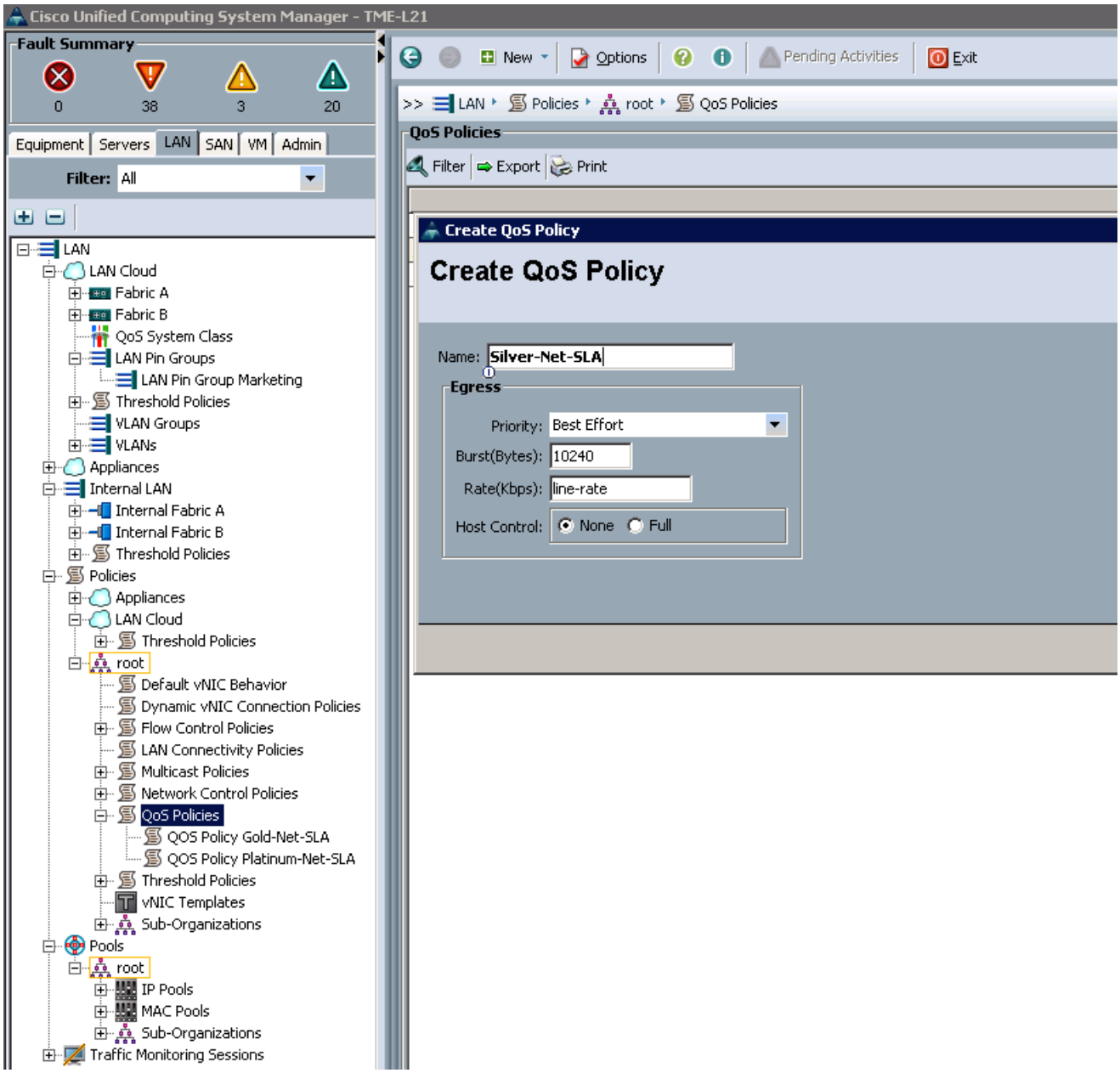
8. [Create QoS Policy] を選択します。
9. QoS ポリシー名として Gold-Net-SLA と入力します。
10. プライオリティを [Gold] に変更します。[Burst(Bytes)] のデフォルト値（10240）、[Rate (Kbps)] のデフォルト値（line-rate）、および [Host Control] のデフォルト値（None）をそのままにします。
11. [OK] をクリックします。

図 21　　ゴールド QoS ポリシーの名前指定と設定



12. [QoS Policies] を右クリックします。
13. [Create QoS Policy] を選択します。
14. QoS ポリシー名として Silver-Net-SLA と入力します。
15. プライオリティを [Silver] に変更します。[Burst(Bytes)] のデフォルト値（10240）、[Rate (Kbps)] のデフォルト値（line-rate）、および [Host Control] のデフォルト値（None）をそのままにします。
16. [OK] をクリックします。

図 22　　シルバー QoS ポリシーの名前指定と設定



17. [QoS Policies] を右クリックします。
18. [Create QoS Policy] を選択します。
19. QoS ポリシー名として FC Net-SLA と入力します。
20. プライオリティを [FC] に変更します。[Burst(Bytes)] のデフォルト値（10240）、[Rate (Kbps)] のデフォルト値（line-rate）、および [Host Control] のデフォルト値（None）をそのままにします。
21. [OK] をクリックします。

図 23　　FC QoS ポリシーの名前指定と設定

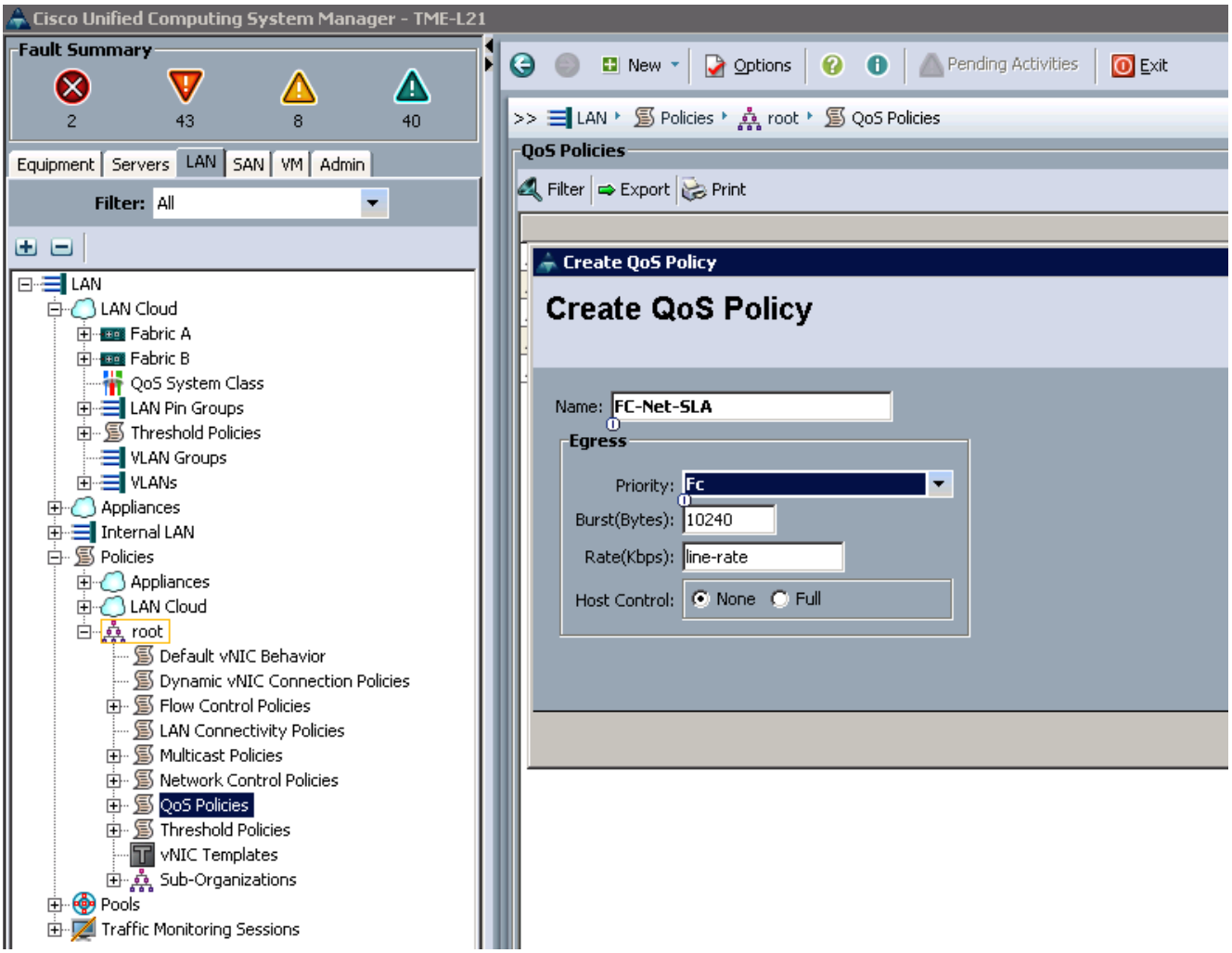
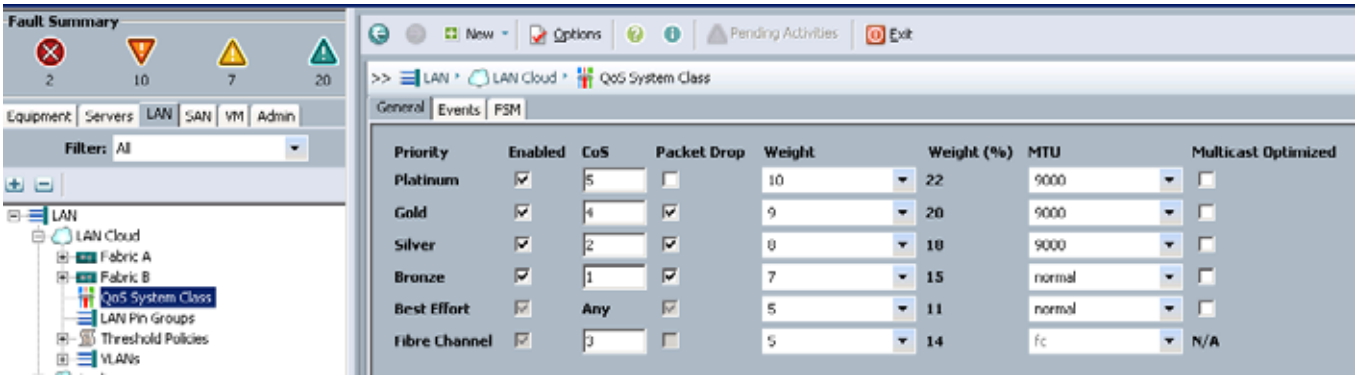


図 24 には、Microsoft SQL Server iSCSI ネットワークにアクセスするために静的および動的 vNIC でのアプリケーション用に定義された Cisco UCS QoS システム クラスと QoS ポリシー設定が示されています。

図 24　　Cisco UCS QoS ポリシー設定の定義



Cisco Nexus 5548UP スイッチの QoS 設定

Cisco UCS からアップストリーム スイッチ（Cisco Nexus 5548UP スイッチ）に至るシステム全体に QoS を適用するには、Cisco UCS QoS クラスに対応した適切なサービス クラス（CoS）値で、同様の QoS クラスおよびポリシー タイプを設定することが不可欠です。

すべてのサービス クラスに対して QoS 設定を定めるには、システム コンソールから各 Nexus 5548UP で次の手順を実行します。

1. グローバル コンフィギュレーション モードから、spanning-tree port type network default と入力して、これらのポートがデフォルトでスパニングツリーの観点からネットワーク ポートとして見なされるようにします。
2. spanning-tree port type edge bpduguard default と入力し、デフォルトですべてのエッジ ポート上で bpduguard を有効化します。
3. spanning-tree port type edge bpdufilter default と入力し、デフォルトですべてのエッジ ポート上で bpdufilter を有効化します。
4. class-map type qos match-any class -- Platinum/Gold/Silver/Bronze/FCoE と入力します。

   プラチナ クラス：

   a. description Platinum Class which is mapped to Platinum-Network-SLA と入力します。
   b. match cos 5 と入力します。
   c. exit と入力します。

   ゴールド クラス：

   a. description Gold Class which is mapped to Gold-Network-SLA と入力します。
   b. match cos 4 と入力します。
   c. exit と入力します。

   シルバー クラス：

   a. description Gold Class which is mapped to Silver-Network-SLA と入力します。
   b. match cos 2 と入力します。
   c. exit と入力します。

   FCoE クラス：

   a. match cos 3 と入力します。
   b. exit と入力します。
5. policy-map type qos system_qos_policy と入力します。

   プラチナ クラス：

   a. class type qos class-Platinum と入力します。
   b. set qos-group 5 と入力します。
   c. exit と入力します。

   ゴールド クラス：

   a. class type qos class-Gold と入力します。
   b. set qos-group 4 と入力します。
   c. exit と入力します。

シルバー クラス：

a. class type qos class-Silver と入力します。
b. set qos-group 2 と入力します。
c. exit と入力します。

FCoE クラス：

a. class type qos class-fcoe と入力します。
b. set qos-group 1 と入力します。
c. exit と入力します。

6. class-map type queuing match-all class- と入力します。

プラチナ クラス：

a. class-map type queuing match-all class-Platinum と入力します。
b. description Platinum Class which is mapped to Platinum-Network-SLA と入力します。
c. match qos-group 5 と入力します。
d. exit と入力します。

ゴールド クラス：

a. class-map type queuing match-all class-Gold と入力します。
b. description Gold Class which is mapped to Gold-Network-SLA と入力します。
c. match qos-group 4 と入力します。
d. exit と入力します。

シルバー クラス：

a. class-map type queuing match-all class-Silver と入力します。
b. description Gold Class which is mapped to Silver-Network-SLA と入力します。
c. match qos-group 2 と入力します。
d. exit と入力します。

FCoE クラス：

a. class-map type queuing match-all class-fcoe と入力します。
b. match qos-group 1 と入力します。
c. exit と入力します。

7. policy-map type queuing system_q_in_policy と入力します。

プラチナ クラス：

a. class type qos class-Platinum と入力します。
b. bandwidth percent 30 と入力します。
c. exit と入力します。

ゴールド クラス：

a. class type qos class-Gold と入力します。
b. set bandwidth percent 20 と入力します。
c. exit と入力します。

シルバー クラス：

a. class type qos class-Silver と入力します。
b. set bandwidth percent 15 と入力します。
c. exit と入力します。

デフォルト クラス：

a. class type qos class-default と入力します。
b. set bandwidth percent 1 と入力します。
c. exit と入力します。

FCoE クラス：

a. class type qos class-FCoE と入力します。
b. set bandwidth percent 34 と入力します。
c. exit と入力します。
d. exit と入力します。

8. policy-map type queuing system_q_out_policy と入力します。

プラチナ クラス：

a. class type qos class-Platinum と入力します。
b. bandwidth percent 30 と入力します。
c. exit と入力します。

ゴールド クラス：

a. class type qos class-Gold と入力します。
b. set bandwidth percent 20 と入力します。
c. exit と入力します。

シルバー クラス：

a. class type qos class-Silver と入力します。
b. set bandwidth percent 15 と入力します。
c. exit と入力します。

デフォルト クラス：

a. class type qos class-default と入力します。
b. set bandwidth percent 1 と入力します。
c. exit と入力します。

FCoE クラス：

a. class type qos class-fcoe と入力します。
b. set bandwidth percent 34 と入力します。
c. exit と入力します。
d. exit と入力します。

9. class-map type network-qos class- と入力します。

プラチナ クラス：

a. class-map type network-qos class-Platinum と入力します。

b. description Platinum Class which is mapped to Platinum-Network-SLA と入力します。

c. match qos-group 5 と入力します。

d. exit と入力します。

ゴールド クラス：

a. class-map type network-qos class-Gold と入力します。

b. description Gold Class which is mapped to Gold-Network-SLA と入力します。

c. match qos-group 4 と入力します。

d. exit と入力します。

シルバー クラス：

a. class-map type network-qos class-Silver と入力します。

b. description Platinum Class which is mapped to Silver-Network-SLA と入力します。

c. match qos-group 2 と入力します。

d. exit と入力します。

FCoE クラス：

a. class-map type network-qos class-fcoe と入力します。

b. match qos-group 1 と入力します。

c. exit と入力します。

10. policy-map type network-qos system_nq_policy と入力します。

プラチナ クラス：

a. class type qos class-Platinum と入力します。

b. set と入力します。

c. set cos 5 と入力します。

d. mtu 9000 と入力します。

e. exit と入力します。

ゴールド クラス：

a. class type qos class-Gold と入力します。

b. set と入力します。

c. set cos 4 と入力します。

d. mtu 9000 と入力します。

e. exit と入力します。

シルバー クラス：

a. class type qos class-Silver と入力します。

b. set と入力します。

c. set cos 2 と入力します。

d. mtu 9000 と入力します。

e. exit と入力します。

FCoE クラス：

a. class type qos class-fcoe と入力します。

b. set と入力します。
c. set cos 1 と入力します。
d. mtu 9000 と入力します。
e. pause no-drop と入力します。
f. exit と入力します。

デフォルト クラス：

a. class type qos class-defaut と入力します。
b. set と入力します。
c. mtu 9000 と入力します。
d. exit と入力します。

11. system qos と入力します。
12. service-policy type qos input system_qos_policy と入力します。
13. service-policy type queuing input system_q_in_policy と入力します。
14. service-policy type queuing output system_q_out_policy と入力します。
15. service-policy type network-qos system_nq_policy と入力します。
16. exit と入力します。
17. interface port-channel 103 と入力します。
18. service-policy type qos input system_qos_policy と入力します。
19. service-policy type queuing input system_q_in_policy と入力します。
20. service-policy type queuing output system_q_out_policy と入力します。
21. interface port-channel 104 と入力します。
22. service-policy type qos input system_qos_policy と入力します。
23. service-policy type queuing input system_q_in_policy と入力します。
24. service-policy type queuing output system_q_out_policy と入力します。
25. copy run start と入力します。

（注） VPC クラスタに含まれる Nexus 5548UP スイッチ B で同じ QoS ポリシーを設定します。Nexus 5548UP スイッチ B で手順 1 ～ 25 を繰り返してください。

以下のコマンドは、Cisco Nexus 5548UP スイッチ A および B 両方での QoS 設定出力を示します。

```
sh class-map type queuing
  Type queuing class-maps
  ========================
  class-map type queuing class-Gold
      match qos-group 4
class-map type queuing class-fcoe
      match qos-group 1
     class-map type queuing class-Silver
      match qos-group 2
    class-map type queuing class-default
      match qos-group 0
    class-map type queuing class-Platinum
      match qos-group 5
    class-map type queuing class-all-flood
```

```
      match qos-group 2
    class-map type queuing class-ip-multicast
      match qos-group 2
N5548-L21-A(config)# sh class-map type network-qos
  Type network-qos class-maps
  ===========================
    class-map type network-qos class-Gold
      match qos-group 4
    class-map type network-qos class-fcoe
      match qos-group 1
    class-map type network-qos class-Silver
      match qos-group 2
    class-map type network-qos class-default
      match qos-group 0
    class-map type network-qos class-Platinum
      match qos-group 5
    class-map type network-qos class-all-flood
      match qos-group 2
    class-map type network-qos class-ip-multicast
      match qos-group 2
N5548-L21-A(config)# sh class-map type queuing
  Type queuing class-maps
  =======================
    class-map type queuing class-Gold
      match qos-group 4
    class-map type queuing class-fcoe
      match qos-group 1
    class-map type queuing class-default
      match qos-group 0
    class-map type queuing class-Platinum
      match qos-group 5
    class-map type queuing class-all-flood
      match qos-group 2
    class-map type queuing class-ip-multicast
      match qos-group 2
sh policy-map type queuing
  Type queuing policy-maps
  ========================
  policy-map type queuing default-in-policy
    class type queuing class-default
      bandwidth percent 100
  policy-map type queuing system_qos_policy
    class type queuing class-Silver
      priority
    class type queuing class-default
      bandwidth percent 100
  policy-map type queuing default-out-policy
    class type queuing class-default
      bandwidth percent 100
  policy-map type queuing system_q_in_policy
    class type queuing class-Platinum
      bandwidth percent 30
    class type queuing class-Gold
      bandwidth percent 20
    class type queuing class-Silver
      bandwidth percent 15
    class type queuing class-fcoe
      bandwidth percent 34
    class type queuing class-default
      bandwidth percent 1
  policy-map type queuing system_q_out_policy
    class type queuing class-Platinum
      bandwidth percent 30
    class type queuing class-Gold
```

```
      bandwidth percent 20
    class type queuing class-Silver
      bandwidth percent 15
    class type queuing class-fcoe
      bandwidth percent 34
    class type queuing class-default
      bandwidth percent 1
  policy-map type queuing fcoe-default-in-policy
    class type queuing class-fcoe
      bandwidth percent 50
    class type queuing class-default
      bandwidth percent 50
  policy-map type queuing fcoe-default-out-policy
    class type queuing class-fcoe
      bandwidth percent 50
    class type queuing class-default
      bandwidth percent 50
sh policy-map type qos
Type qos policy-maps
  ====================
 policy-map type qos default-in-policy
    class type qos class-default
      set qos-group 0
  policy-map type qos system_qos_policy
    class type qos class-Platinum
      set qos-group 5

    class type qos class_fcoe
      set qos-group 3
    class type qos class-default
      set qos-group 0
  policy-map type qos fcoe-default-in-policy
    class type qos class-fcoe
      set qos-group 1
    class type qos class-default
      set qos-group 0
sh policy-map type network-qos
 Type network-qos policy-maps
  ==============================
  policy-map type network-qos system_nq_policy
    class type network-qos class-Platinum
    set cos 5
      mtu 9000
    class type network-qos class-fcoe
    mtu 2158
      set cos 3
      pause no-drop
    class type network-qos class-Gold
      mtu 9000
    class type network-qos class-Silver
     mtu 9000
     class type network-qos class-default
    mtu 1500
   multicast-optimize
  policy-map type network-qos default-nq-policy
    class type network-qos class-default
    mtu 9000
      multicast-optimize
  policy-map type network-qos fcoe-default-nq-policy
    class type network-qos class-fcoe
    pause no-drop
      mtu 2158
    class type network-qos class-default
      mtu 1500
```

```
multicast-optimize
```

NetApp ストレージ QoS 設定

（注） Cisco Nexus 5548UP アップストリーム スイッチで、ポリシー タイプで正しい QoS クラスと MTU 値がポート チャネル ポート（eth 19 および eth 20）に適用されていることを確認します。ネットワーク パケットに Nexus 5548 ファブリックからタグ付けできるように、ポート チャネルは、NetApp FAS3270HA（コントローラ Flexpod A および B）、10 ギガビット イーサネット インターフェイス（e1c および e1d）に接続されます。これは、NetApp ストレージがネットワーク パケットに MTU および QoS 値をタグ付けしないために行われます。

次のコマンドは、ポート チャネル上のストレージから発信したタグ付けされていないパケットに対し、Nexus 5548 で CoS を設定する方法を示しています。

Cisco Nexus 5548UP Application1 での CLI コマンド

```
Switch# Configure Terminal
Switch(Conf)# Interface port channel 105
Switch(Conf-if)#untagged cos 2
Switch# sh policy-map type qos
Switch# Configure Terminal
Switch(Conf)# Interface port channel 106
Switch(Conf-if)#untagged cos 2
Switch# sh policy-map type qos
```

Cisco Nexus 5548UP Application2 での CLI コマンド

```
Switch# Configure Terminal
Switch(Conf)# Interface port channel 105
Switch(Conf-if)#untagged cos 2
Switch# sh policy-map type qos
Switch# Configure Terminal
Switch(Conf)# Interface port channel 106
Switch(Conf-if)#untagged cos 2
Switch# sh policy-map type qos
```

MTU が 9000 に設定されていることと、ジャンボ フレームが Cisco UCS 静的および動的 vNIC 上、およびアップストリーム Cisco Nexus 5548UP スイッチ上で有効化されていることを確認します。

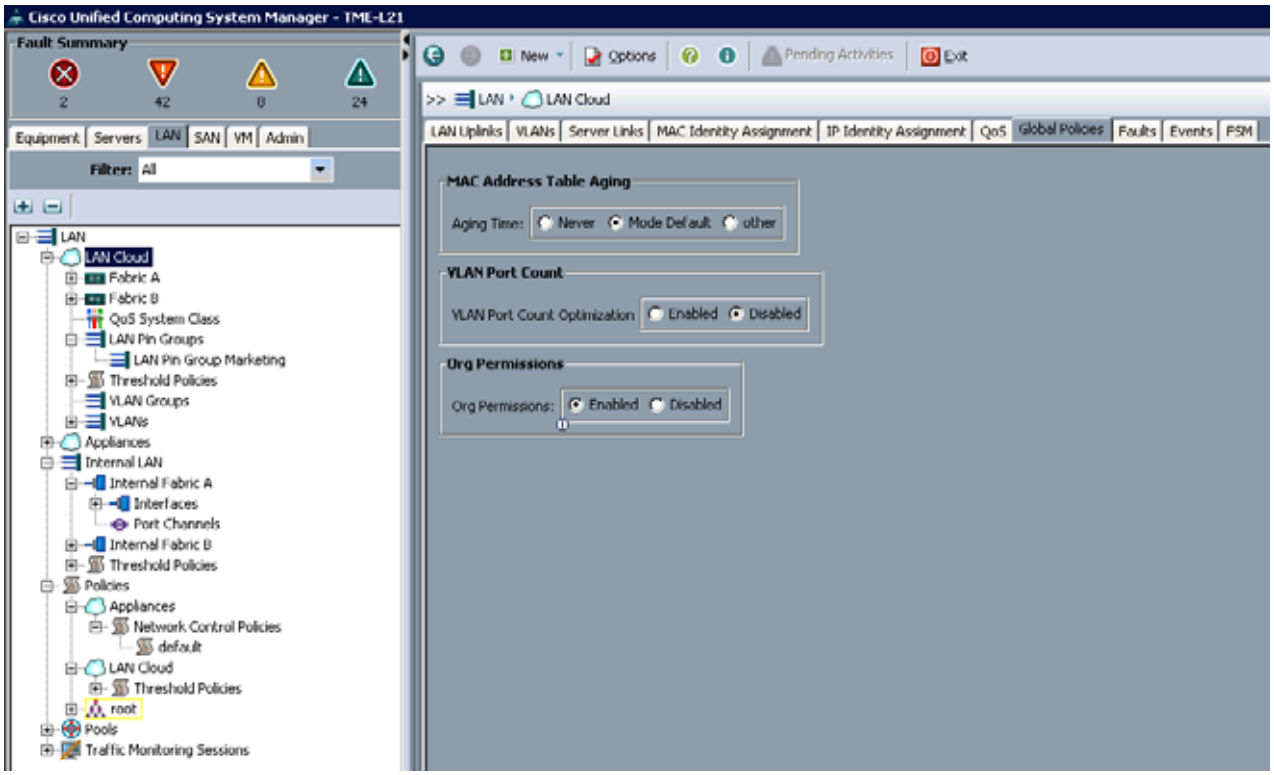
Cisco UCS 6248UP ファブリック インターコネクトでの VLAN の設定

マルチテナント クラウド環境において、ネットワーク データ アクセスの分離は、セキュリティ対策に従った重要な要件です。Cisco UCS では、特定の組織単位専用にしてそのユニットからアクセスできる論理 VLAN を作成できます。

Cisco UCS で、組織単位専用の必要な VLAN を設定するには、次の手順を実行します。

1. 右ペインで [LAN] タブをクリックし、[Global Policies] をクリックします。
2. 右ペインの [Org Permissions] 領域の下で [Enabled] オプション ボタンをクリックします。
3. [Save Changes] をクリックします。

図 25　　組織単位に対する VLAN の設定

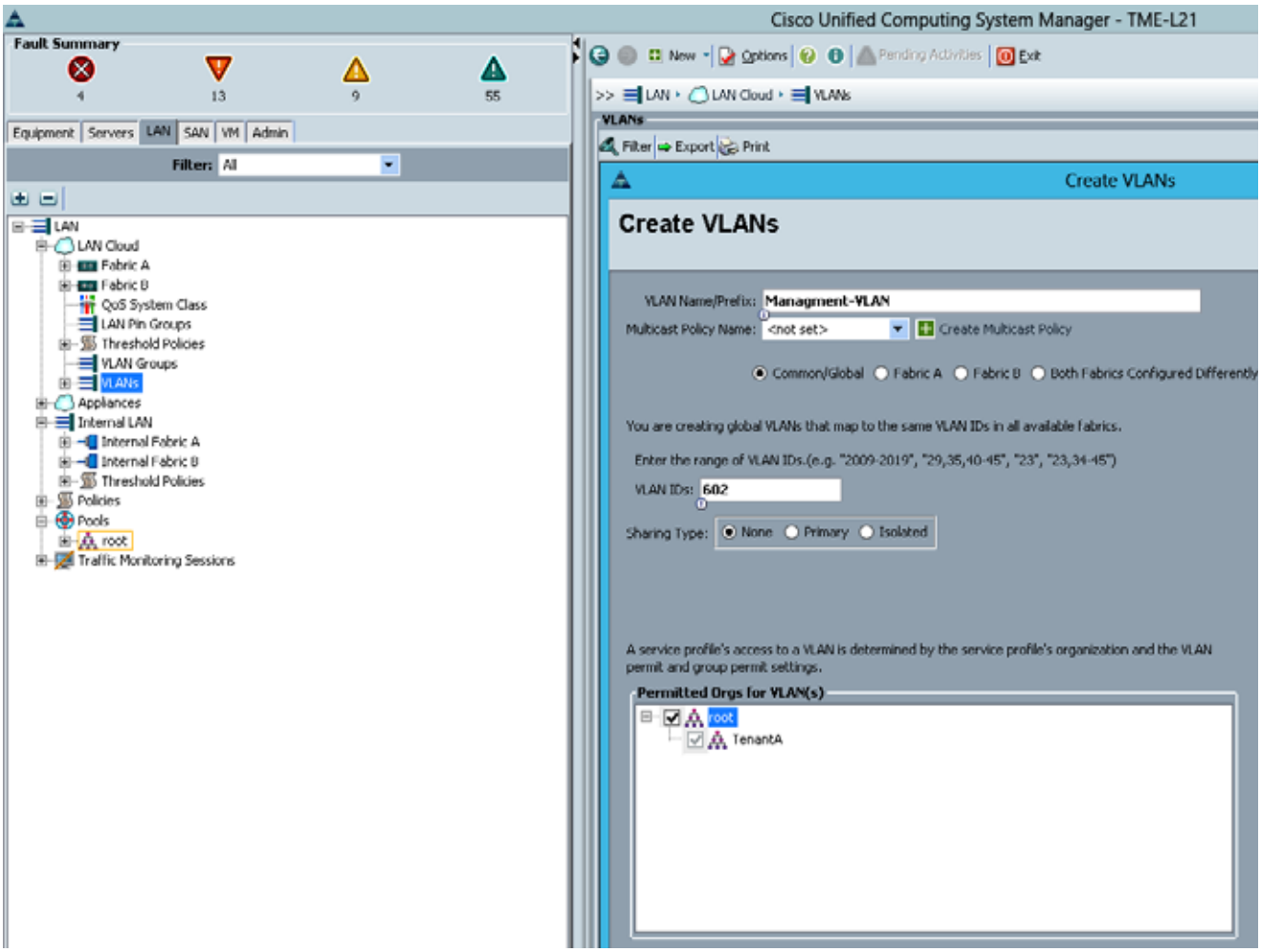


4. 左ペインで [LAN] タブをクリックします。
5. [LAN Cloud] を選択します。
6. [VLANs] を右クリックします。（管理 VLAN の作成）
7. [Create VLANs] を選択します。
8. [Name] フィールドに Management-VLAN と入力します。

（注）　この VLAN は管理トラフィックに使用されます。

9. [Multicast Policy Name] の下でデフォルト設定を選択します。
10. VLAN の範囲で [Common/Global] オプションを選択したまま維持します。
11. 管理 VLAN に対して定義された VLAN ID を入力します。[Sharing Type] を [None] のままにしておきます。
12. [Permitted Orgs for VLAN(s)] で、[Root] と [TenantA] の組織単位を選択します。
13. [OK] をクリックします。

図 26　　管理 VLAN プロパティの定義

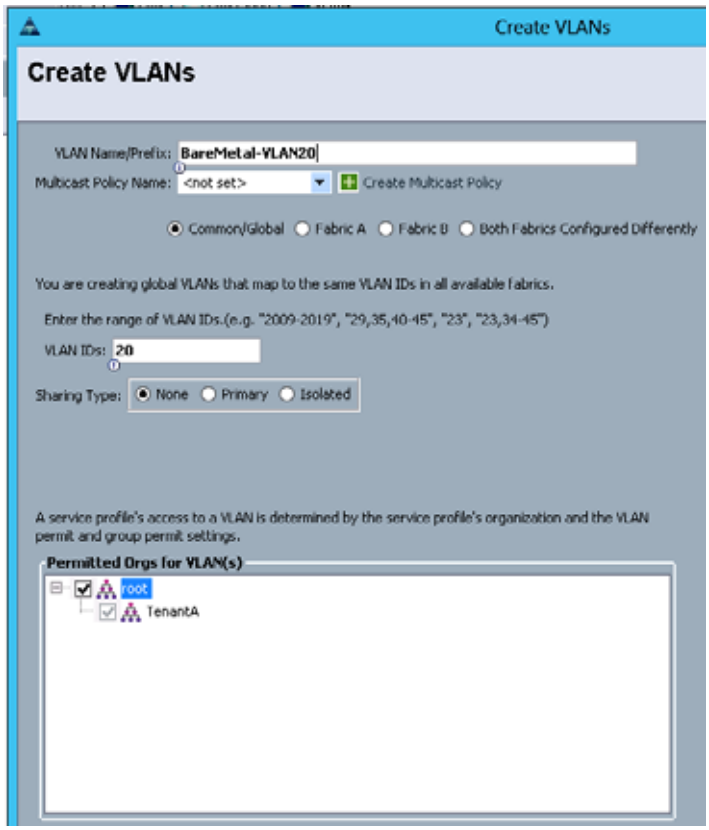


14. [VLANs] をクリックします。（BareMetal-PXE VLAN の作成）
15. [Create VLANs] を選択します。
16. [Name] フィールドに BareMetal-VLAN と入力します。

（注）　この VLAN は、BareMetal ホスト PXE ブート トラフィックに使用されます。

17. [Multicast Policy Name] の下でデフォルト設定を選択します。
18. VLAN の範囲で [Common/Global] オプションを選択したまま維持します。
19. [BareMetal-PXE VLAN] に VLAN ID を入力します。
20. [Permitted Orgs for VLAN(s)] で、[root] 組織単位を選択します。
21. [OK] をクリックします。

図 27　　BareMetal-PXE VLAN プロパティの定義

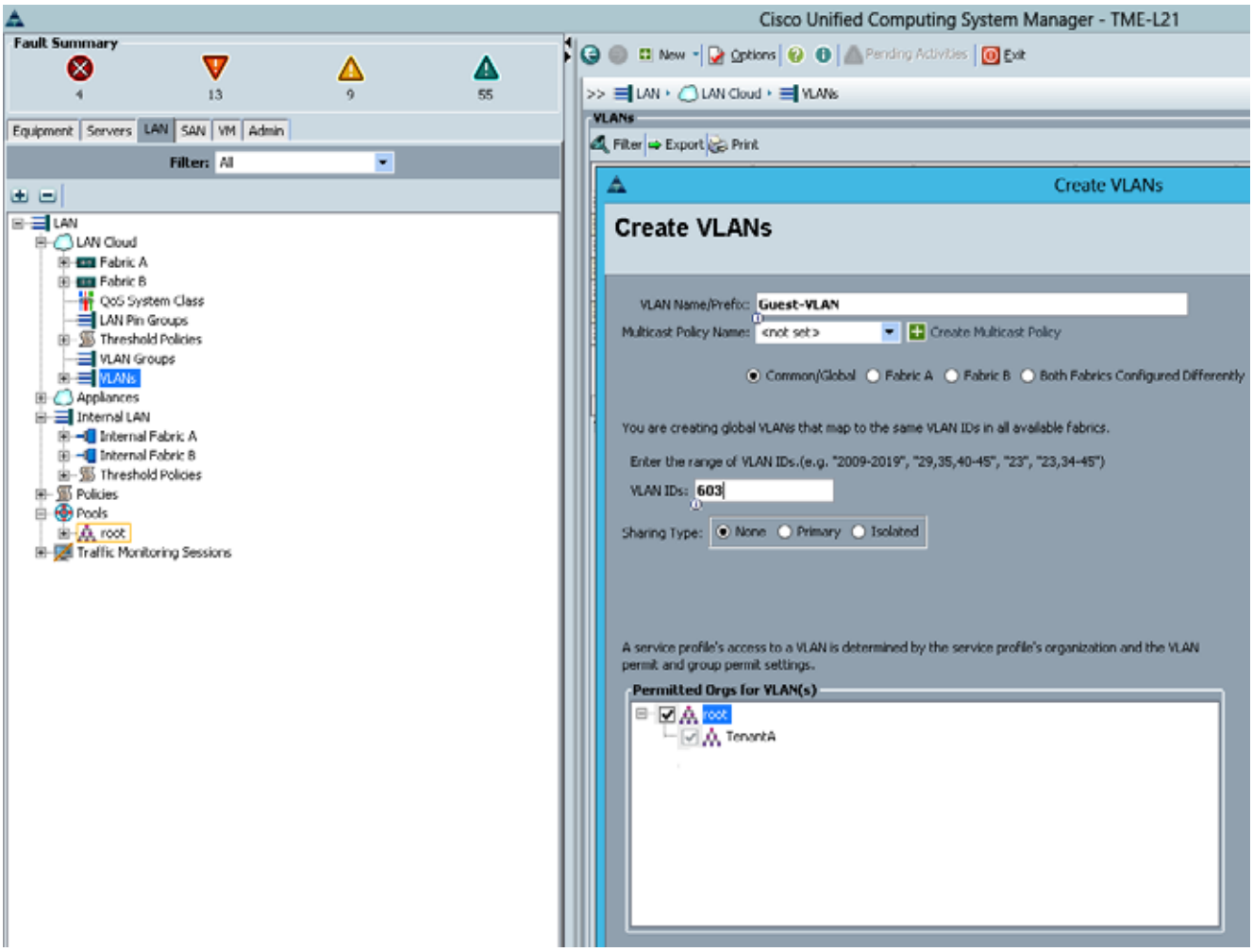


22. [VLANs] を右クリックします。（ゲスト VLAN の作成）
23. [Create VLANs] を選択します。
24. [Name] フィールドに guest-VLAN と入力します。

（注）　この VLAN はゲスト VLAN トラフィックに使用されます。

25. [Multicast Policy Name] の下で [Default] 設定を選択します。
26. VLAN の範囲で [Common/Global] オプションを選択したまま維持します。
27. ゲスト VLAN の VLAN ID を入力します。
28. [Permitted Orgs for VLAN(s)] で、[Root] と [TenantA] の組織単位を選択します。
29. [OK] をクリックします。

図 28　　ゲスト VLAN プロパティの定義

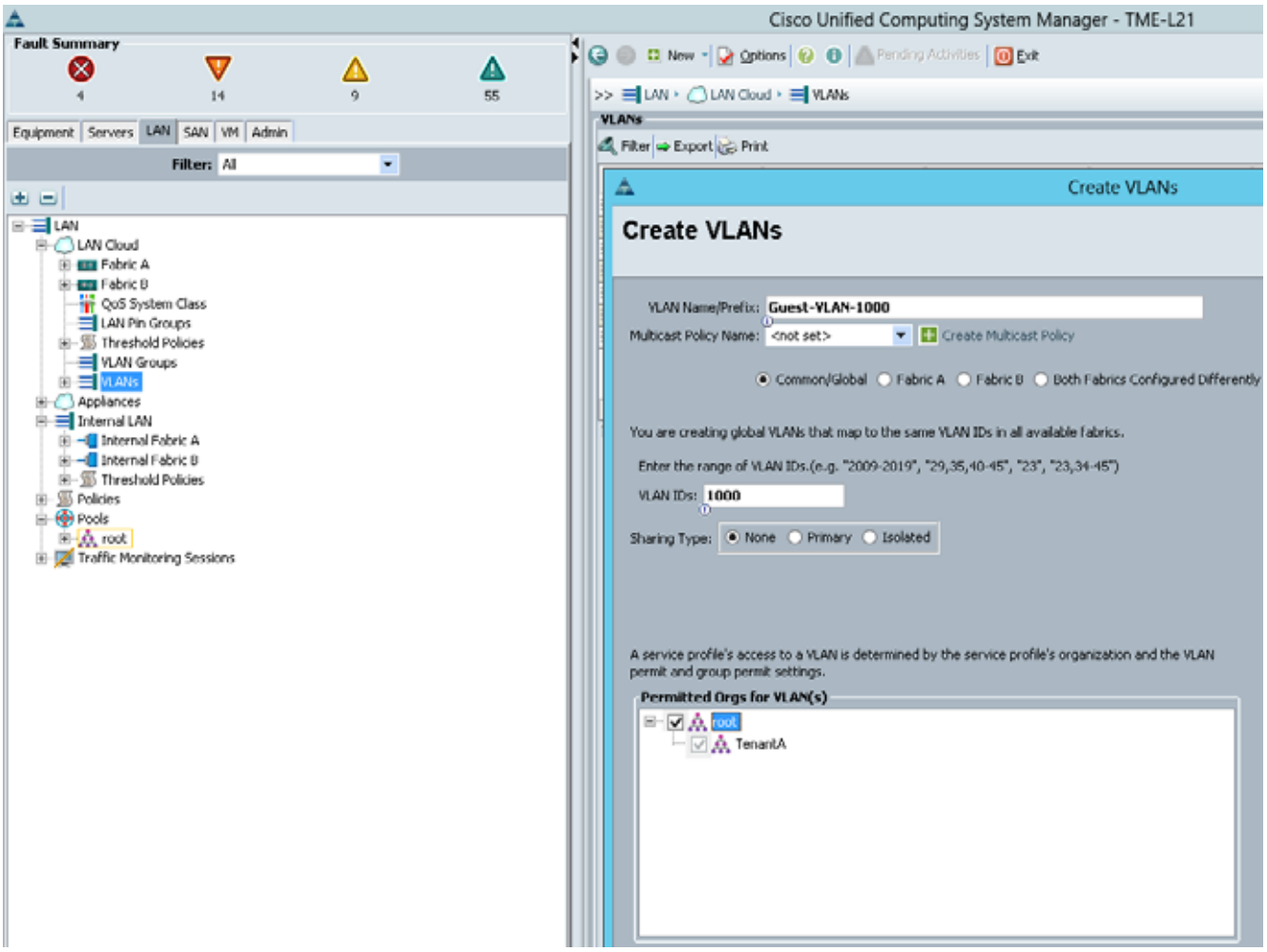


30. [VLANs] を右クリックします。（ゲスト VLAN の作成）
31. [Create VLANs] を選択します。
32. [Name] フィールドに guest-VLAN-1000 と入力します。

（注）　この VLAN はゲスト VLAN トラフィックに使用されます。

33. [Multicast Policy Name] の下で [Default] 設定を選択します。
34. VLAN の範囲で [Common/Global] オプションを選択したまま維持します。
35. ゲスト VLAN の VLAN ID を入力します。
36. [Permitted Orgs for VLAN(s)] で、[Root] と [TenantA] の組織単位を選択します。
37. [OK] をクリックします。

図 29　　ゲスト VLAN 1000 プロパティの定義

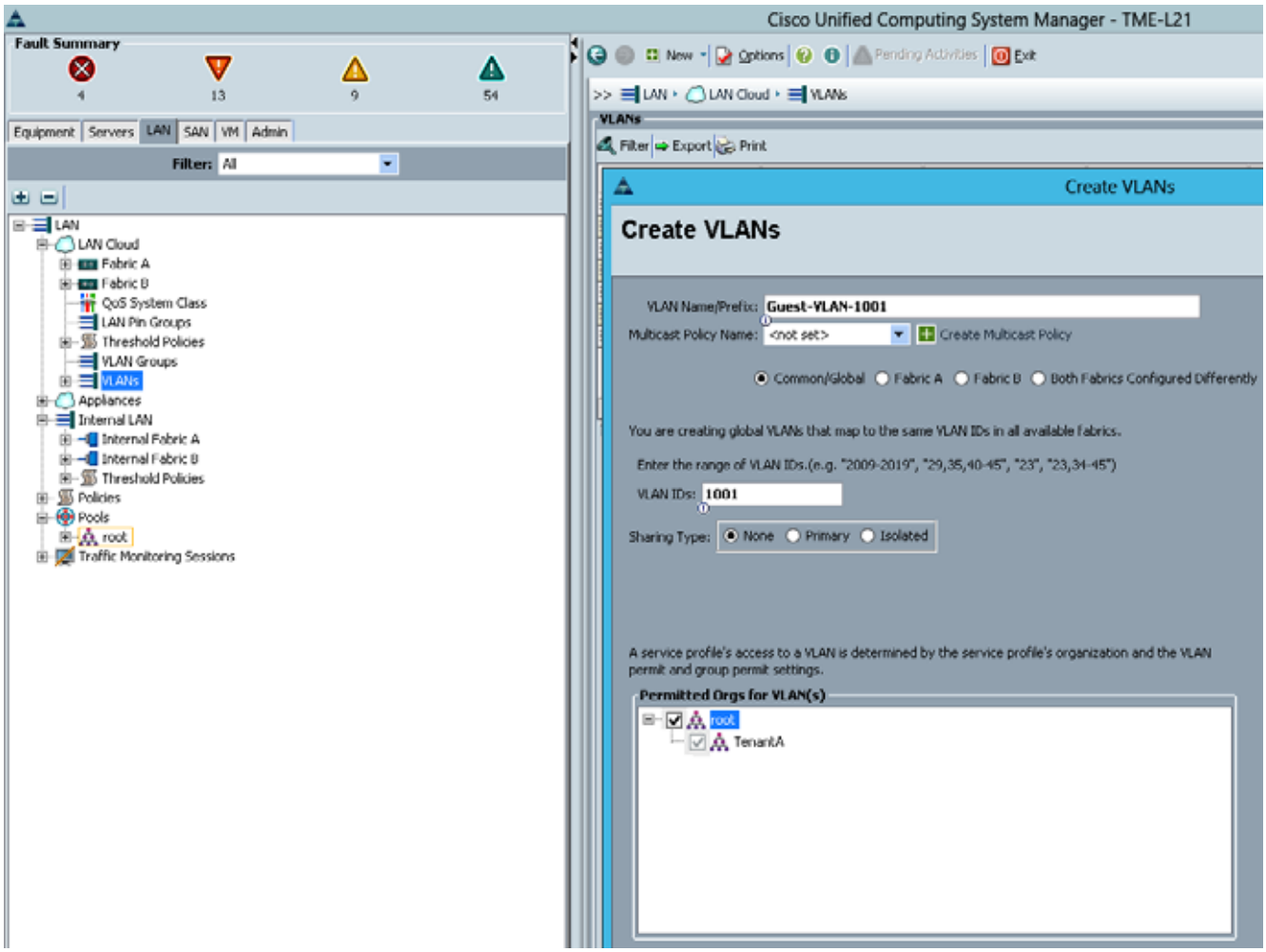


38. [VLANs] を右クリックします。（ゲスト VLAN の作成）
39. [Create VLANs] を選択します。
40. [Name] フィールドに guest-VLAN-1001 と入力します。

（注）　この VLAN はゲスト VLAN トラフィックに使用されます。

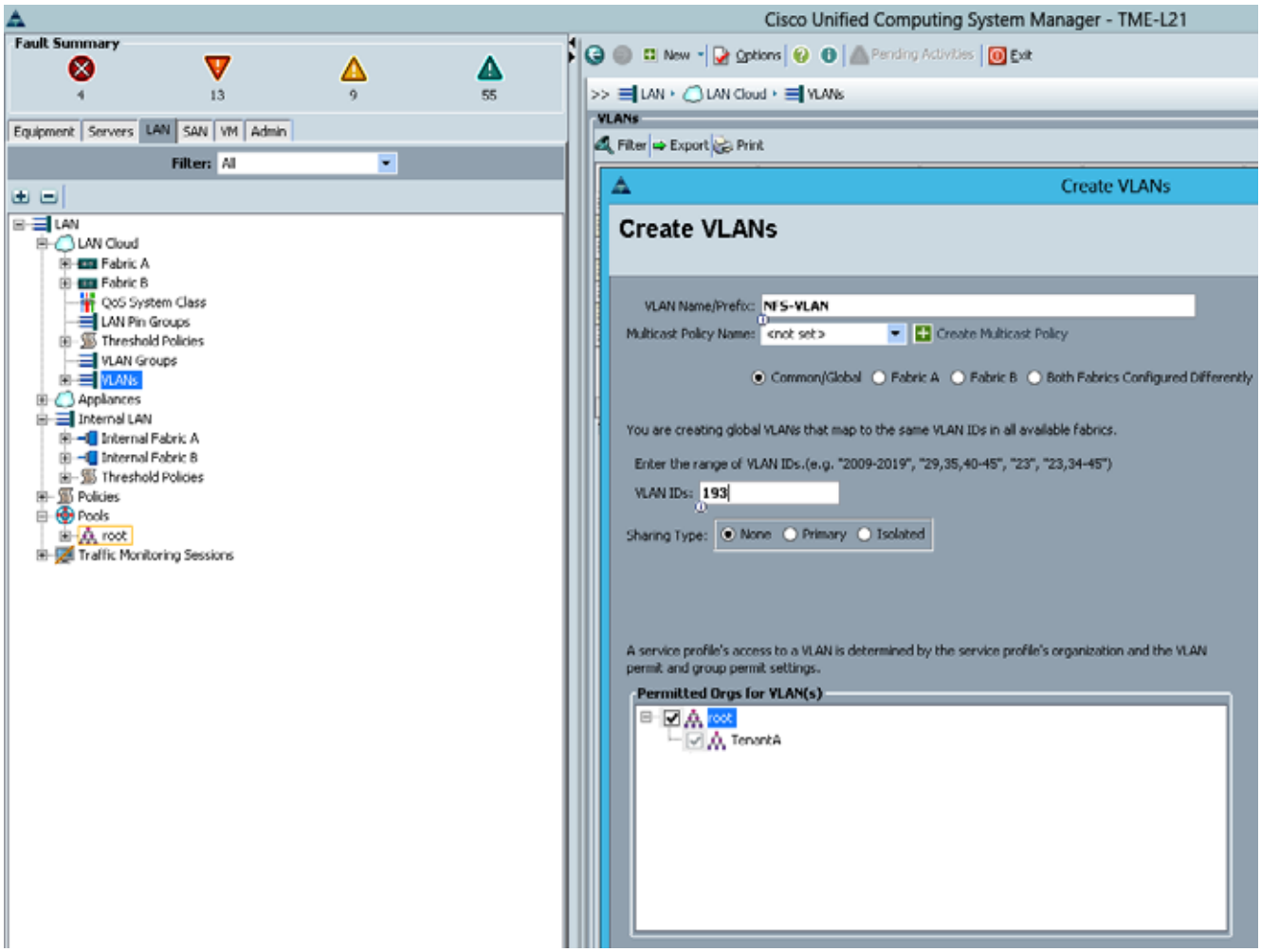
41. [Multicast Policy Name] の下で [Default] 設定を選択します。
42. VLAN の範囲で [Common/Global] オプションを選択したまま維持します。
43. ゲスト VLAN の VLAN ID を入力します。
44. [Permitted Orgs for VLAN(s)] で、[Root] と [TenantA] の組織単位を選択します。
45. [OK] をクリックします。

図 30　　ゲスト VLAN 1001 プロパティの定義



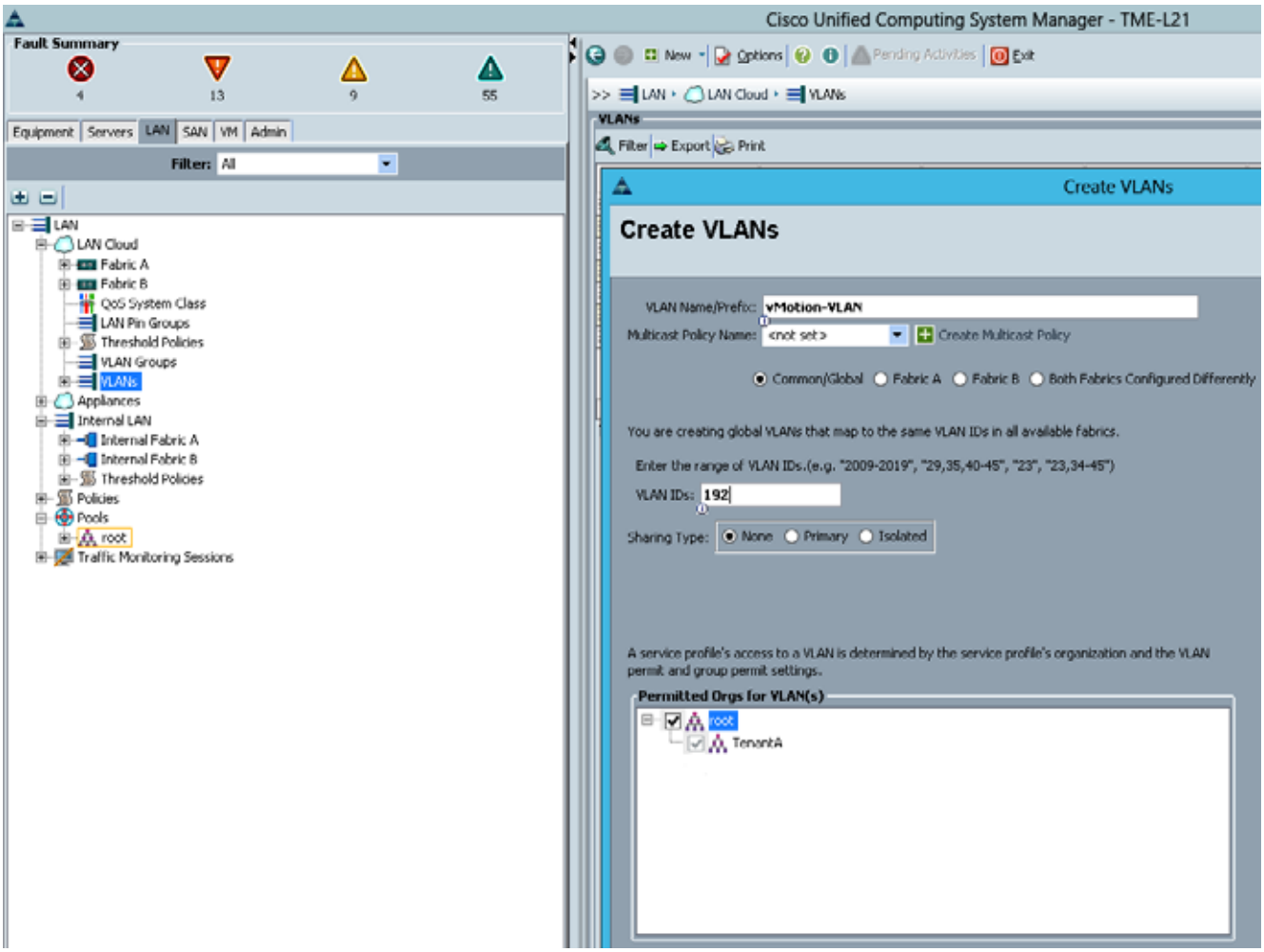
46. [VLANs] を右クリックします。(NFS VLAN の作成)
47. [Create VLANs] を選択します。
48. [Name] フィールドに NFS-VLAN と入力します。この VLAN は、セカンダリ ストレージ NFS VLAN トラフィックに使用されます。
49. [Multicast Policy Name] の下で [Default] 設定を選択します。
50. VLAN の範囲で [Common/Global] オプションを選択したまま維持します。
51. NFS VLAN の VLAN ID を入力します。
52. VLAN の範囲で [Common/Global] オプションを選択したまま維持します。
53. [Permitted Orgs for VLAN(s)] で、[TenantA] 組織単位を選択します。
54. [OK] をクリックします。

図 31　　NFS VLAN プロパティの定義



55. [VLANs] を右クリックします。（vMotion VLAN の作成）
56. [Create VLANs] を選択します。
57. [Name] フィールドに vMotion-VLAN と入力します。この VLAN は、VM の vMotion VLAN トラフィックに使用されます。
58. [Multicast Policy Name] の下で [Default] 設定を選択します。
59. VLAN の範囲で [Common/Global] オプションを選択したまま維持します。
60. vMotion VLAN の VLAN ID を入力します。
61. [Permitted Orgs for VLAN(s)] で、[TenantA] 組織単位を選択します。
62. [OK] をクリックします。

図 32　　vMotion VLAN プロパティの定義



ストレージの設定

この項では、シスコ ストレージ デザインの考慮事項に対応するために必要なすべての設定およびセットアップ手順について詳しく説明します。この説明では、マルチテナント ストレージ データ トラフィックを分離するための仮想論理 SAN ネットワーク（VSAN）を作成し、リンク集約のための FCoE ポート チャネルを作成します。

次のタスクについて説明します。

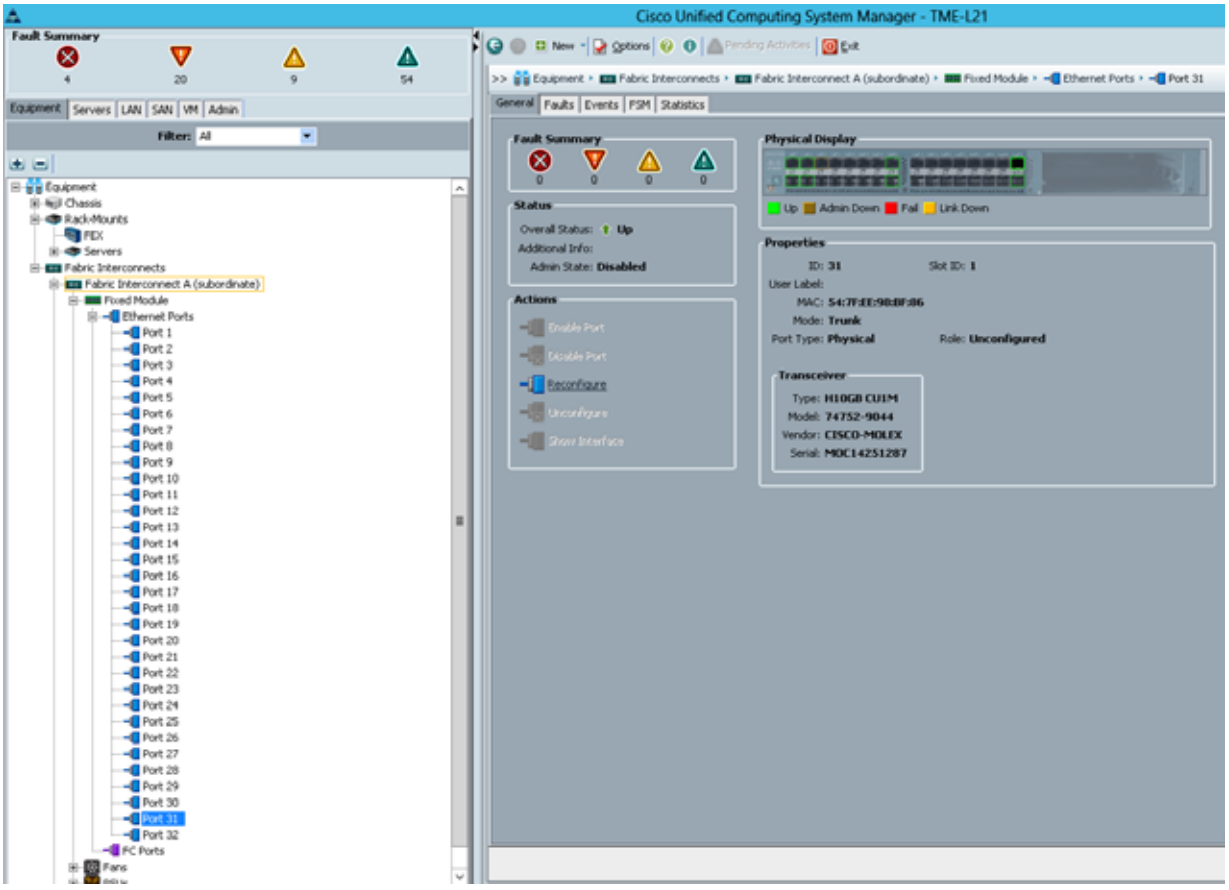
- FCoE ポートの設定
- VSAN の作成
- VSAN および SAN ポート チャネルの定義
- FI での FCoE ポート チャネルの設定

FCoE ポートの設定

FCoE ポートは、イーサネットでファイバ チャネルのトラフィックを伝送するように設定できる、6200 シリーズのファブリック インターコネクト上のポートです。これらのポートは予約されていません。これらは設定するまで、Cisco UCS ドメインで使用できません。Cisco UCS 環境で未設定のイーサネット ポートを FCoE アップリンク ポートに変更するには、次の手順を実行します。

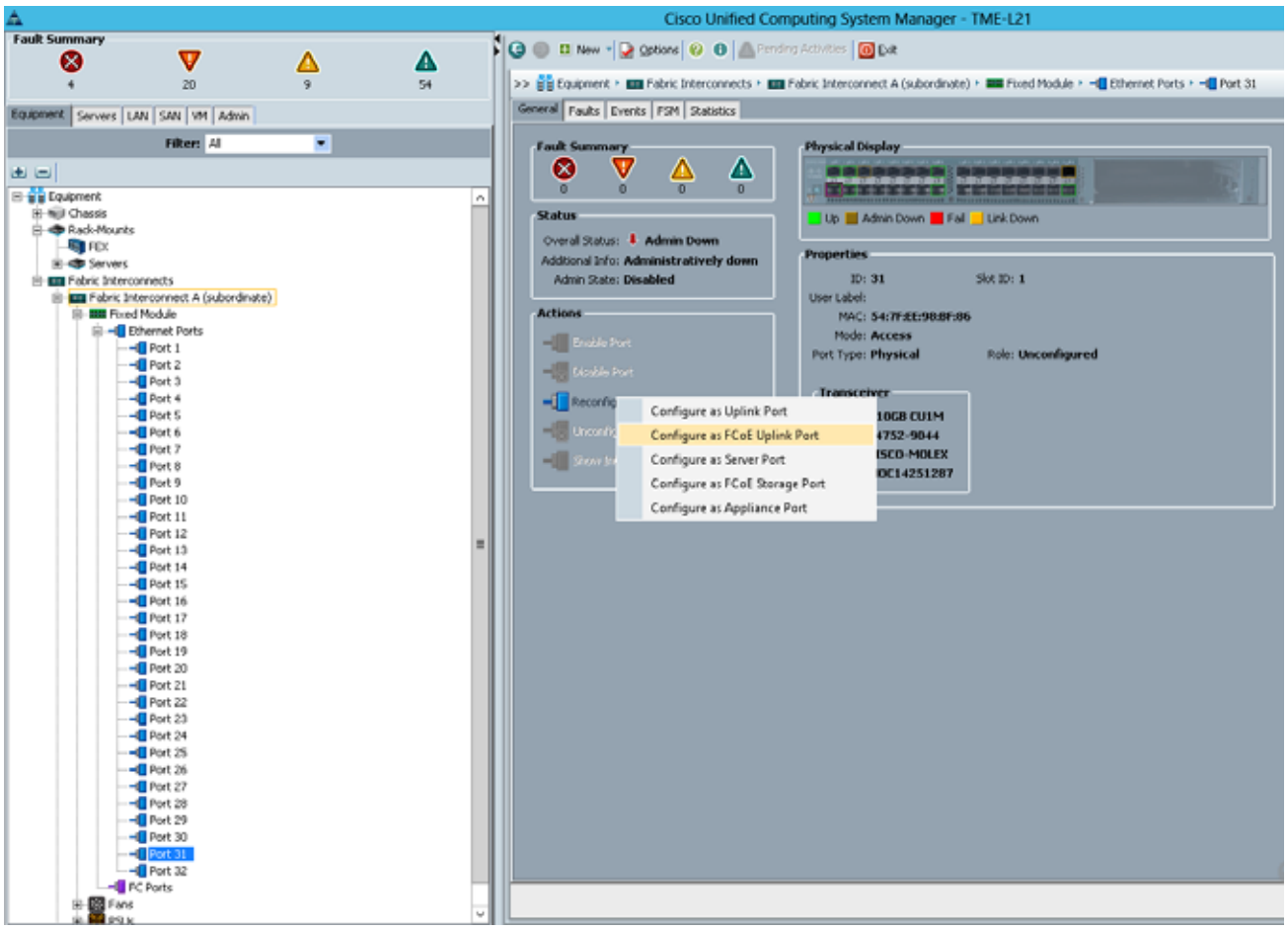
1. Cisco UCS Manager GUI の左ペインで [Equipment] タブをクリックします。（FI A で FCoE ポートを設定）
2. [Fabric Interconnects A] を選択します。
3. [Ethernet Ports] を選択します。
4. [Port 31] を選択します。
5. 右ペインで、[General] タブをクリックします。
6. [Reconfigure] を選択します。

図 33　　イーサネット ポートを FCoE アップリンク ポートに再設定します。



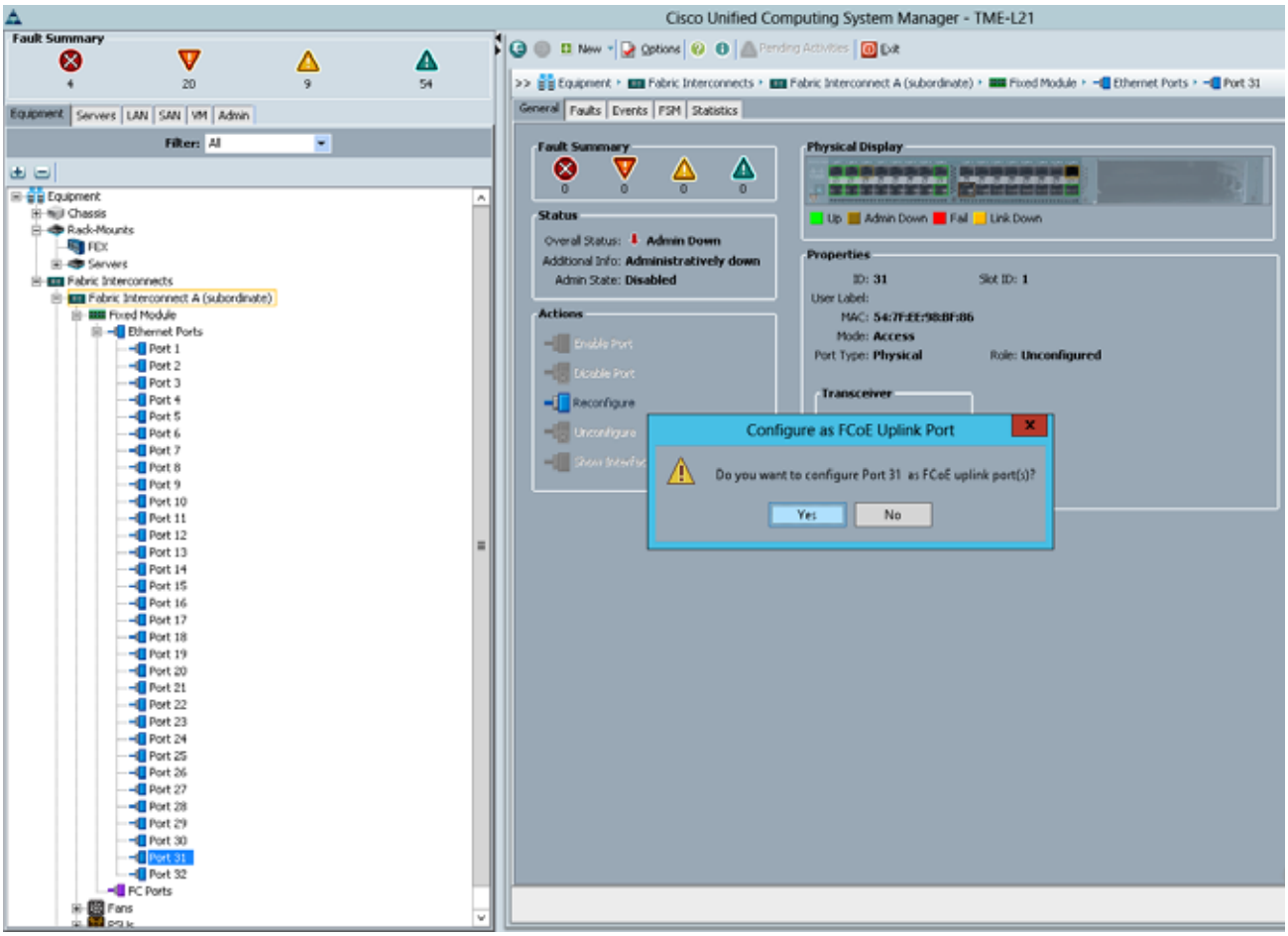
7. [Configure as FCoE Uplink Port] を選択します。

図 34　　アップリンク ポートとして設定



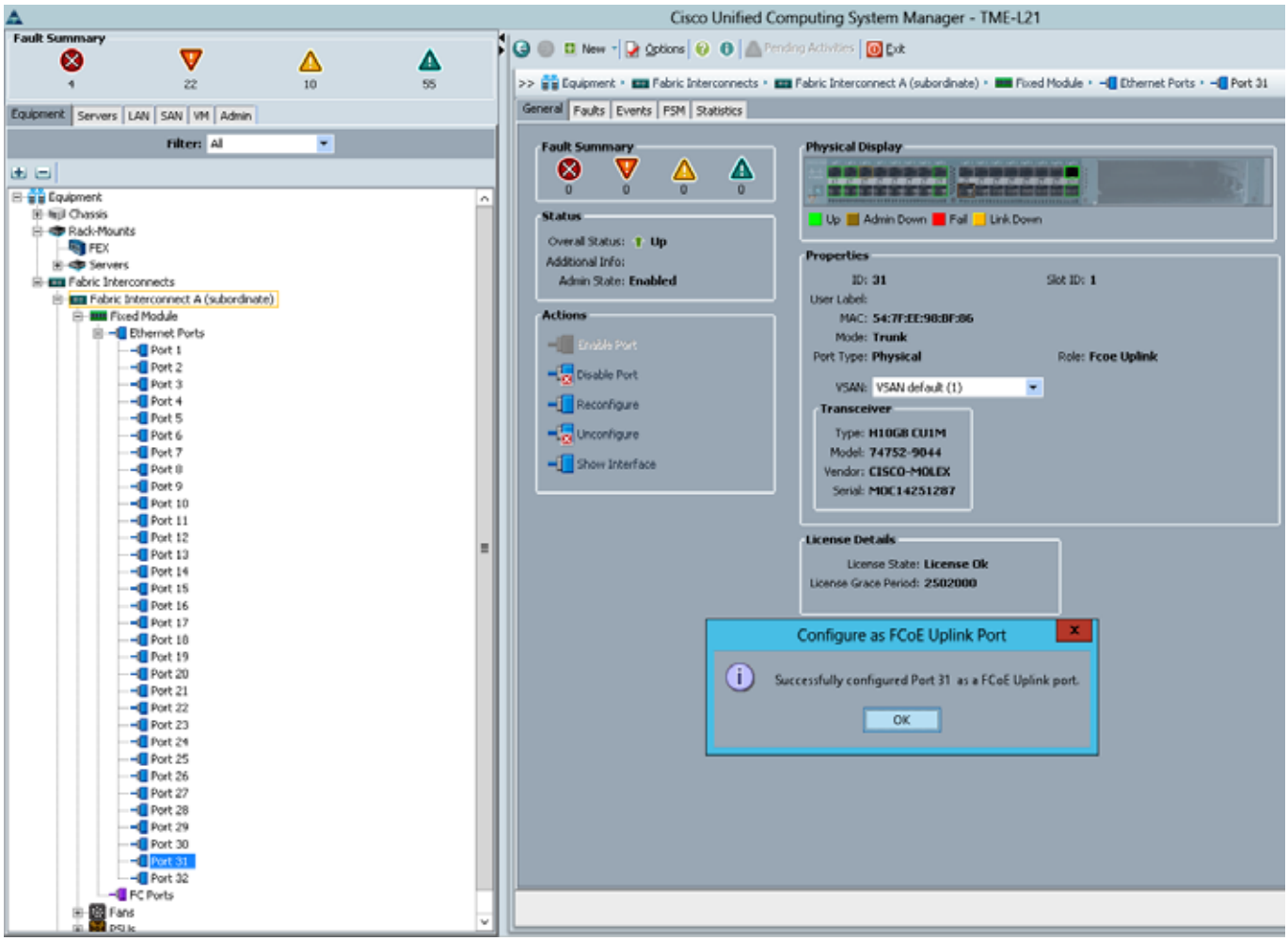
8. 確認のために [Yes] をクリックします。

図 35　　FCoE アップリンク ポートの設定



9. [OK] をクリックします。
10. プライマリ ファブリック インターコネクトが再起動すると、Cisco UCS Manger GUI が閉じます。
11. [OK] をクリックします。

図 36　　FCoE アップリンク ポートの設定



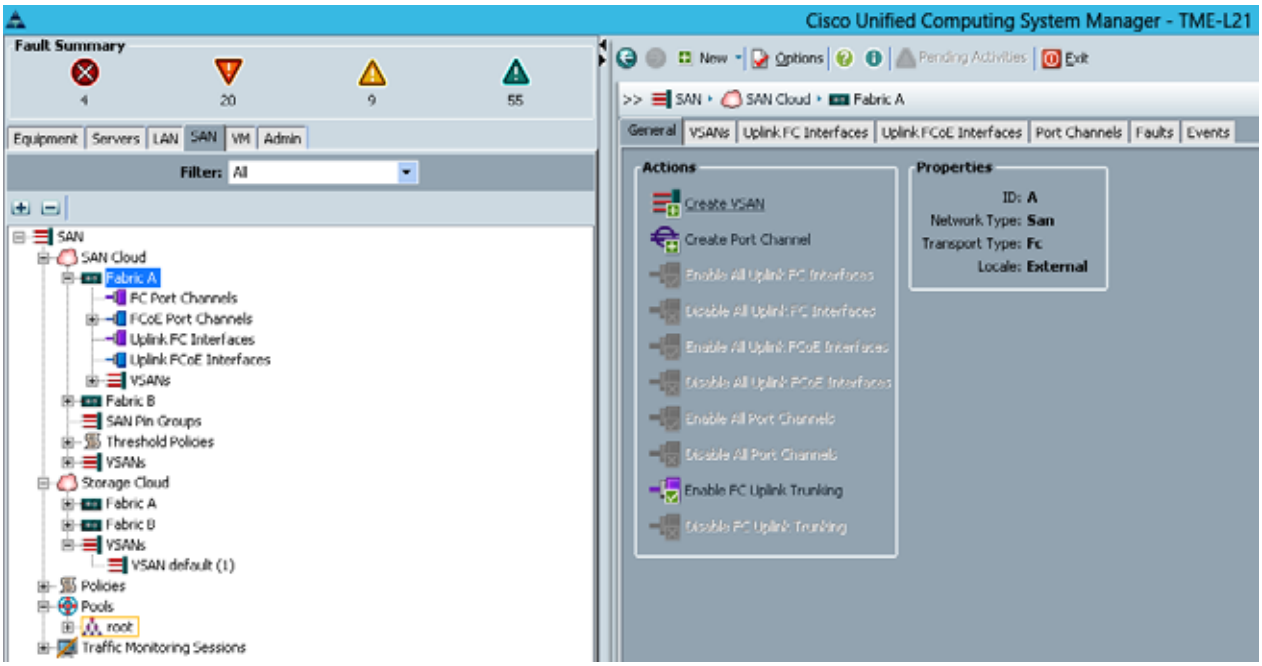
12. ポート 32 で同じ手順を繰り返し、FI A 上で FCoE ポートを設定します。
13. ポート 31 と 32 で同じ手順を繰り返し、VSAN を作成している FI 上で FCoE ポートを設定します。

VSAN では、一般の物理インフラストラクチャで複数の論理 SAN を作成できます。各 VSAN には最大 239 台のスイッチを組み込めます。それぞれの VSAN は、異なる VSAN で同じファイバ チャネル ID（FC ID）を同時に使用できる独立したアドレス領域を持ちます。VSAN を作成する前に、VSAN に対して、アプリケーション固有のパラメータを設定できます。VSAN を作成するには、Cisco UCS Manager にログインし、次の手順を実行します。

ファブリック インターコネクト A

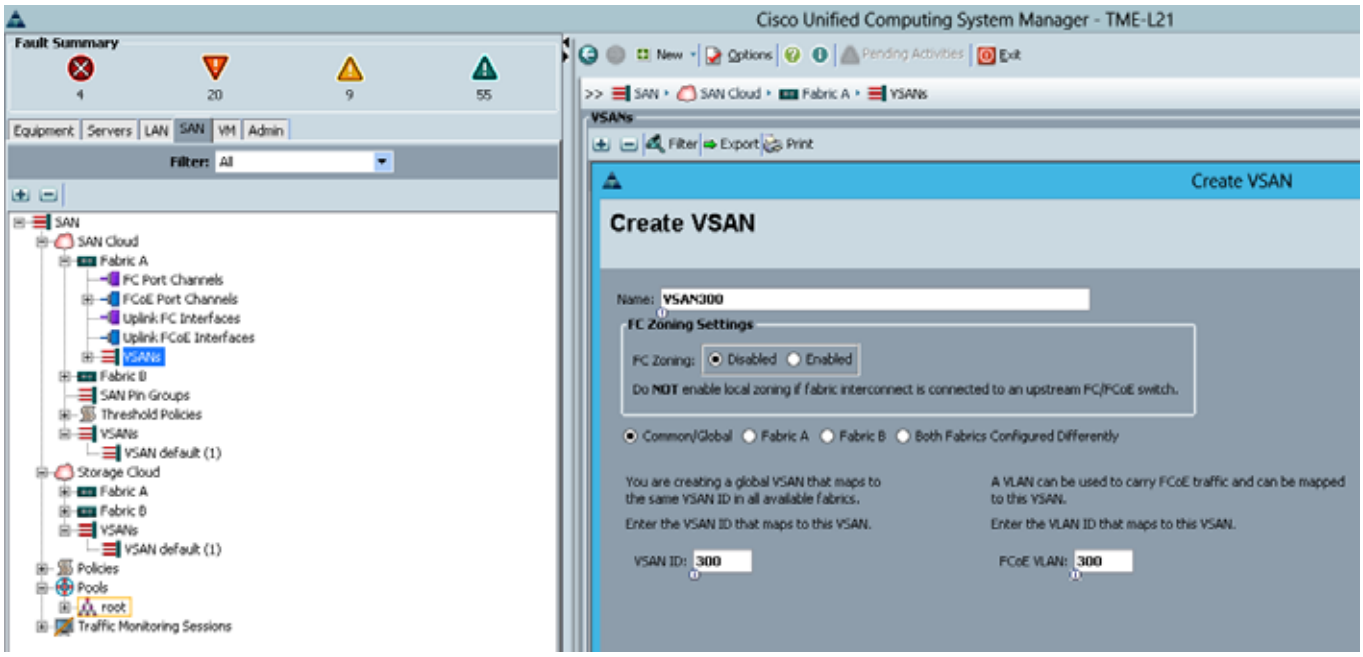
1. 左ペインで [SAN] タブをクリックします。
2. [SAN Cloud] ツリーを展開します。
3. [Fabric A] をクリックします。
4. 右ペインの [General] タブの下で [Create VSAN] をクリックします。

図 37　　VSAN の作成



5. [VSAN name] フィールドに VSAN300 と入力します。
6. [Default Zoning] に対し [Disabled] オプションを選択したままにします。
7. [Common/Global] オプション ボタンをクリックします。
8. VSAN ID 300 と入力します。
9. FCoE VLAN ID 300 と入力します。
10. [OK] をクリックします。

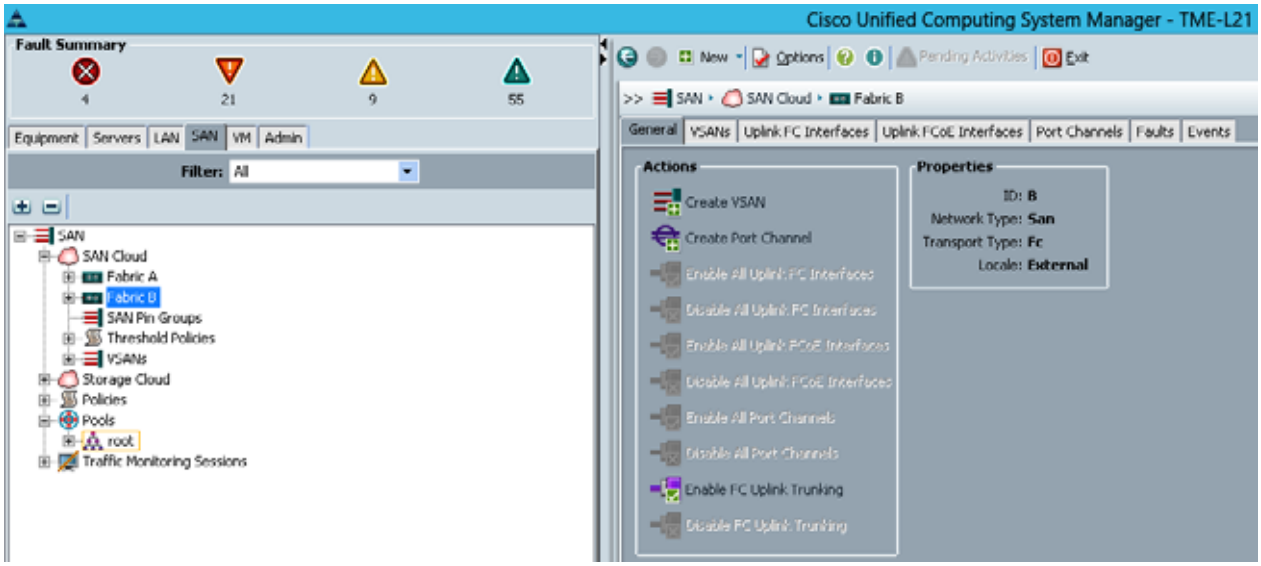
図 38　　共通 / グローバル VSAN の定義



ファブリック インターコネクト B

1. 左ペインで [SAN] タブをクリックします。[SAN Cloud] ツリーを展開します。
2. [Fabric A] をクリックします。
3. 右ペインの [General] タブの下で [Create VSAN] をクリックします。

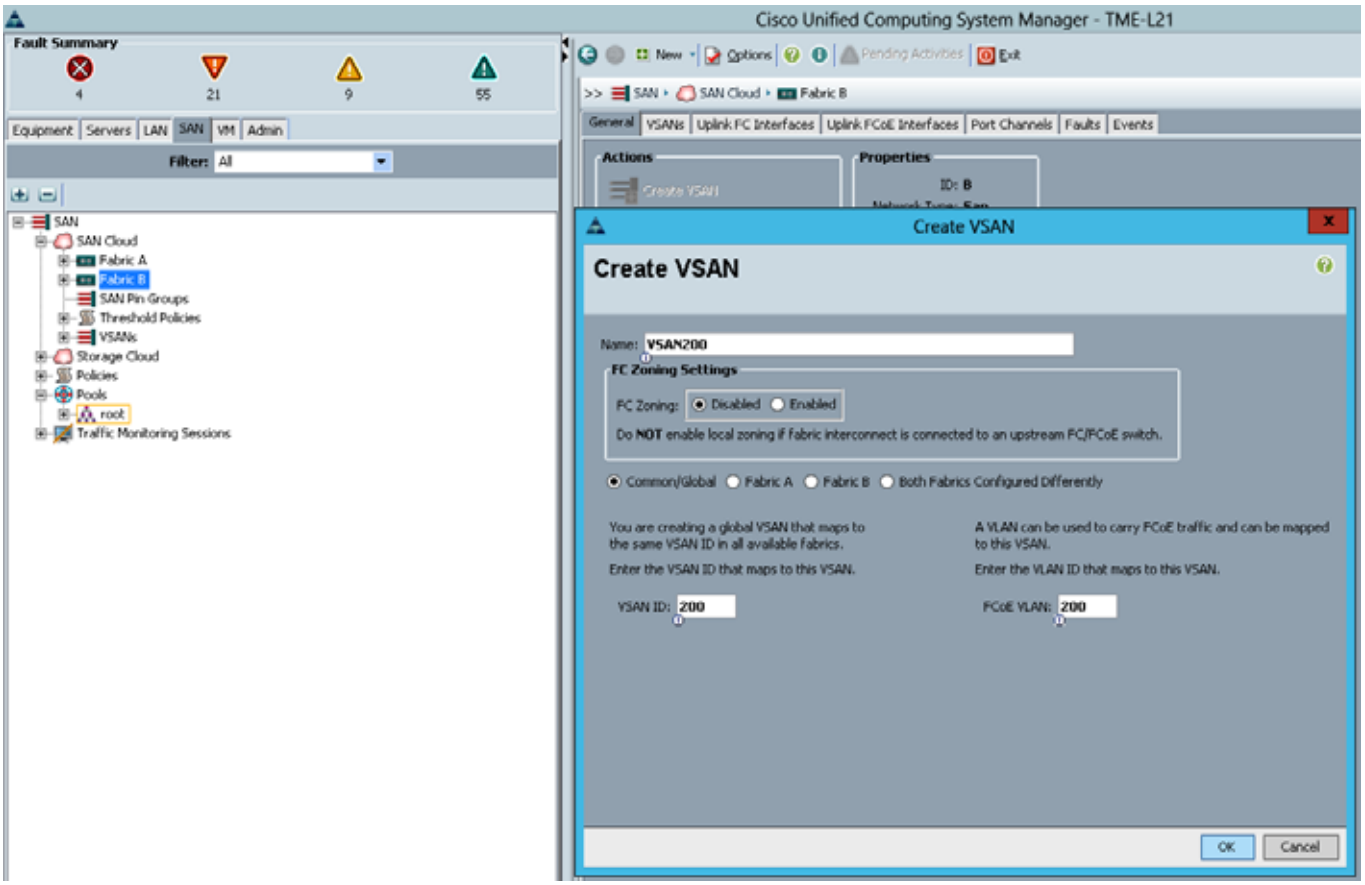
図 39　　VSAN の作成



4. [VSAN name] フィールドに VSAN200 と入力します。
5. [Default Zoning] に対し [Disabled] オプションを選択したままにします。

6. [Common/Global] オプション ボタンをクリックします。
7. VSAN ID 200 と入力します。
8. FCoE VLAN ID 200 と入力します。
9. [OK] をクリックします。

図 40　　共通 / グローバル VSAN の定義

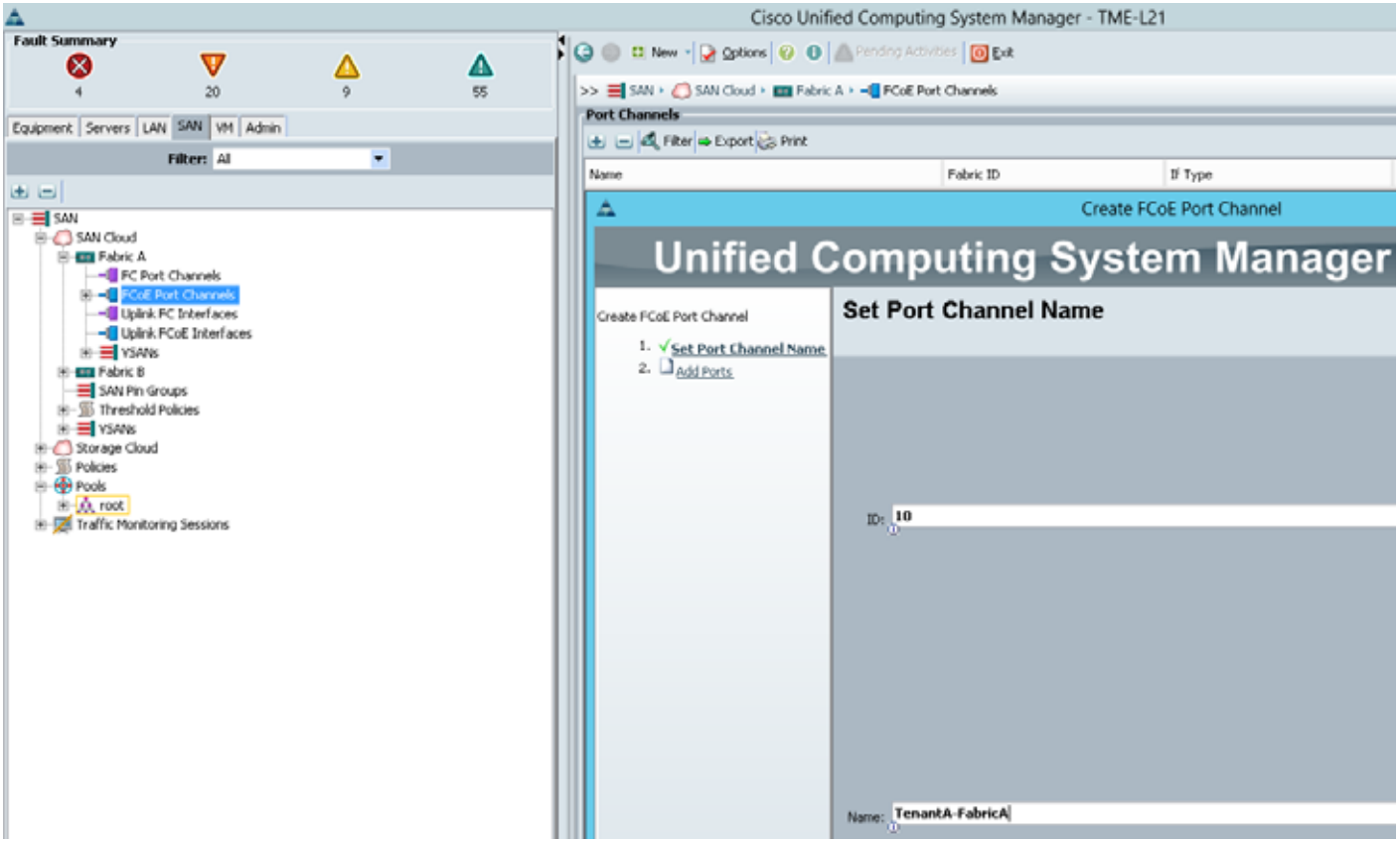


Cisco UCS 6248 ファブリック インターコネクト上でのポート チャネルの作成

ファブリック インターコネクト A

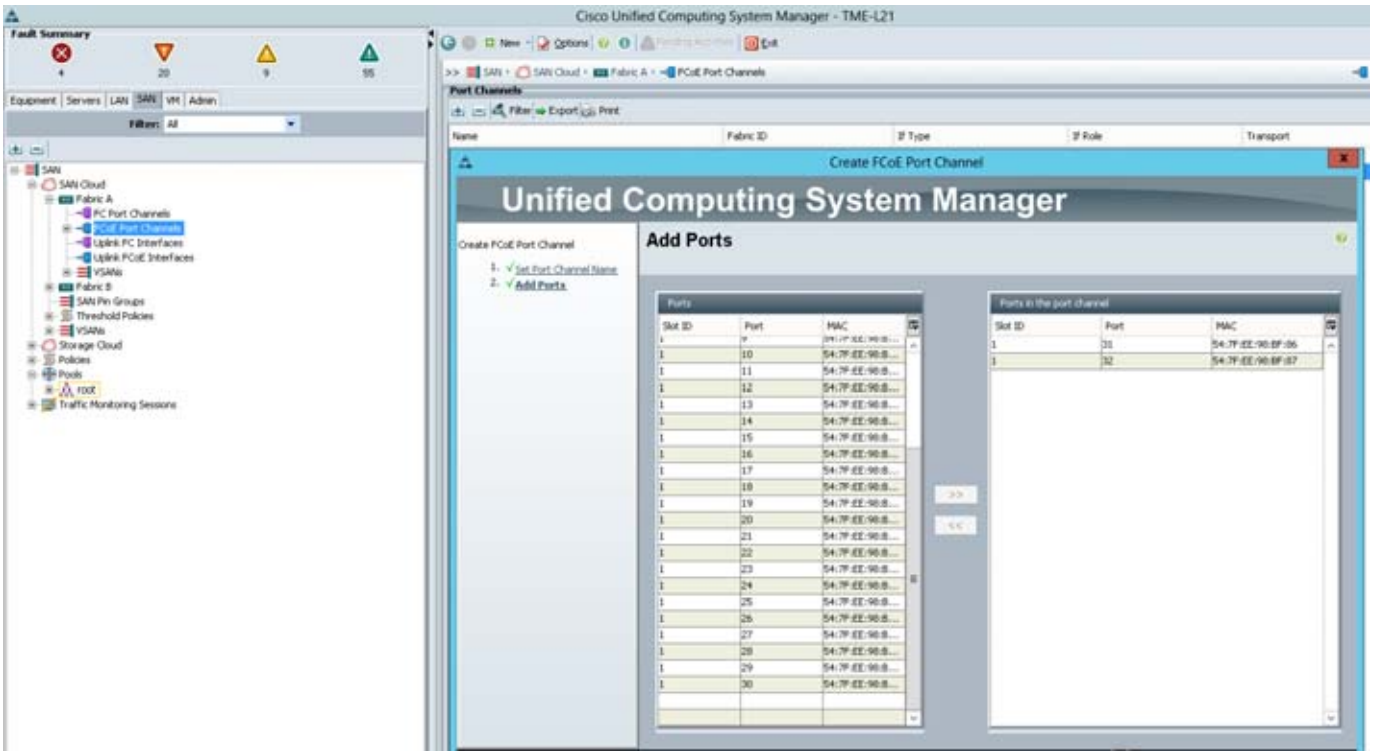
1. [SAN Cloud] の下で [Fabric A] ツリーを展開します。
2. [FCoE Port Channels] を右クリックします。
3. [Create Port Channel] を選択します。
4. [Yes] をクリックします。
5. [Port Channel ID] フィールドに 10 と入力し、[Port Channel name] フィールドに Tenant-Fabric-A と入力します。
6. [Next] をクリックします。

図 41　FCoE ポート チャネルの名前および ID の定義



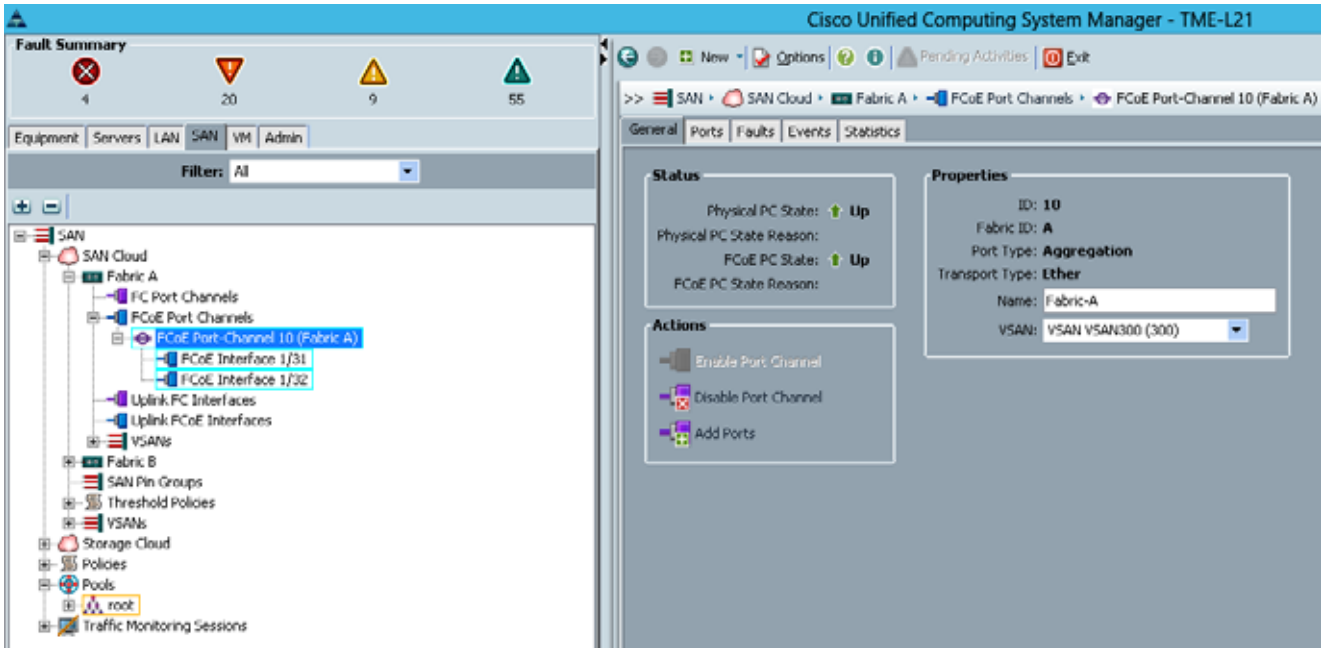
7. ポート 31 と 32 を選択し、[>>] をクリックしてポートを FCoE ポート チャネルに追加します。
8. [Finish] をクリックします。

図 42　　ポートの選択および FCoE ポート チャネルへの追加



9. [OK] をクリックして、FCoE ポート チャネルの作成を完了します。
10. [VSAN] プルダウンで [VSAN300] を選択します。
11. [Save Changes] をクリックし、[OK] をクリックします。

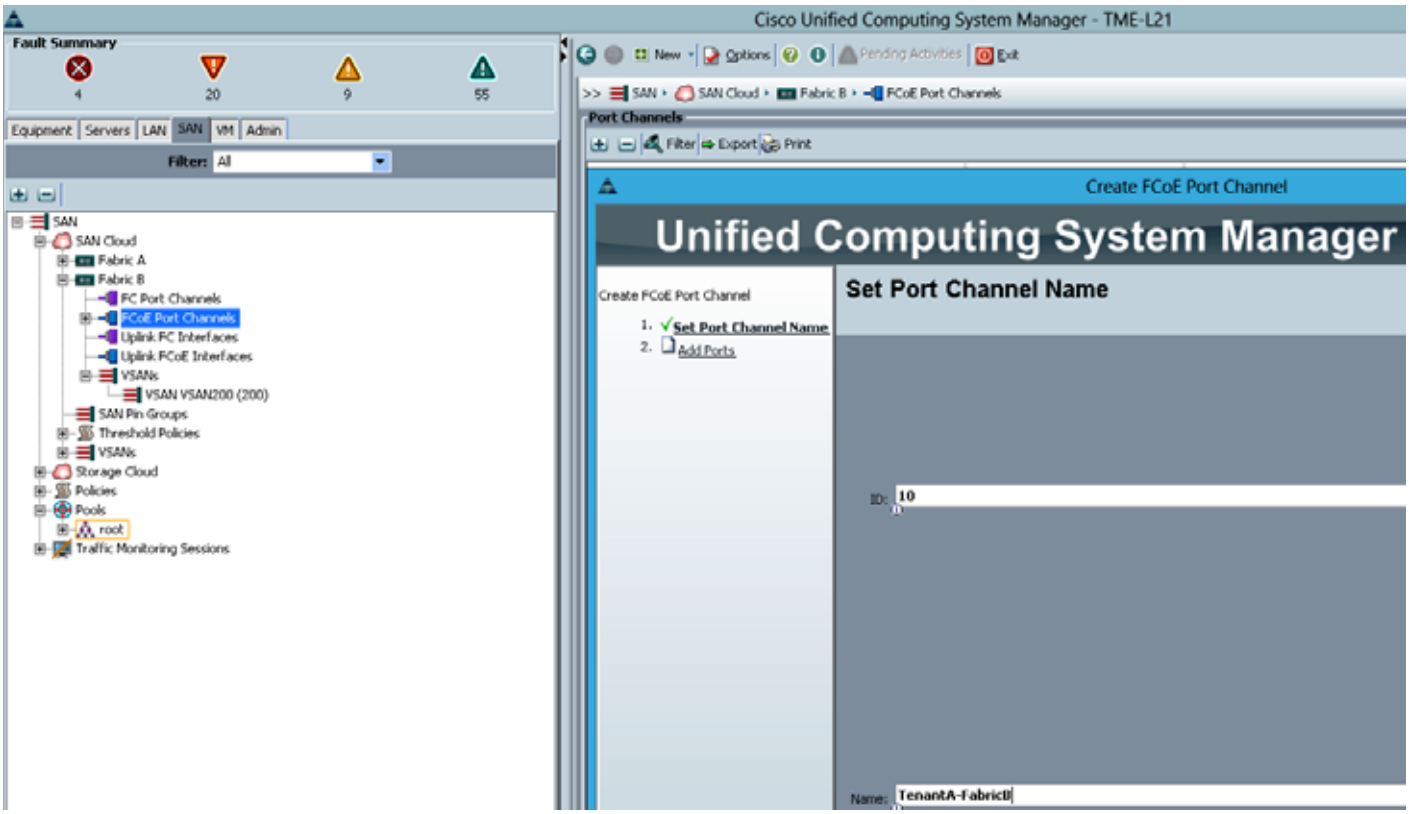
図 43　　FCoE ポート チャネルの VSAN ID の選択



ファブリック インターコネクト B

1. [SAN Cloud] の下で [Fabric B] ツリーを展開します。
2. [FCoE Port Channels] を右クリックします。
3. [Create Port Channel] を選択します。
4. [Yes] をクリックし、[Port Channel ID] フィードに 10 と入力し、[FCoE Port Channel name] フィールドに Tenant-Fabric-B と入力します。
5. [Next] をクリックします。

図 44　　FCoE ポート チャネルの名前と ID の入力

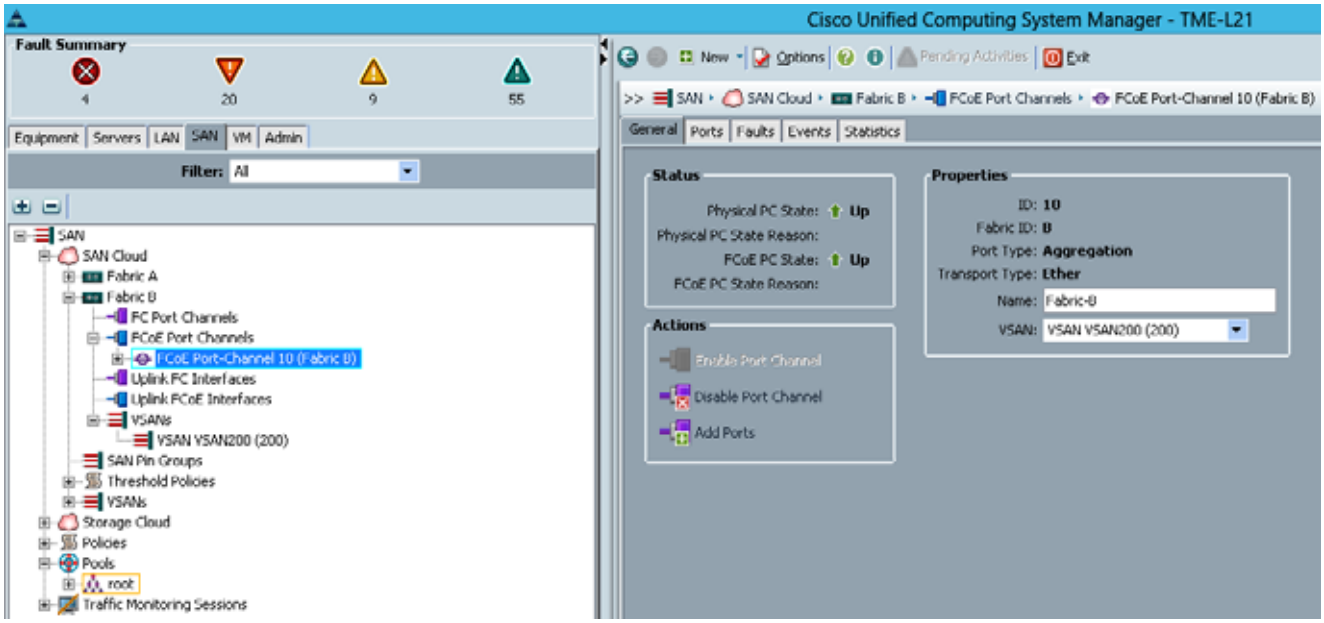


6. ポート 31 と 32 を選択し、[>>] をクリックしてポートを FCoE ポート チャネルに追加します。
7. [Finish] をクリックします。

図 45　　FCoE ポートの選択および FCoE ポート チャネルへの追加

8. [OK] をクリックして、FCoE ポート チャネルの作成を完了します。
9. [VSAN] プルダウンで [VSAN200] を選択します。
10. [Save Changes] をクリックします。

図 46　　FCoE ポート チャネルのプロパティ



SAN ポート チャネルの作成

同じペアの Cisco Nexus 5548UP スイッチをストレージのアクセスに使用できます。Cisco UCS 6248UP ファブリック インターコネクト上の FCoE ポートには、Nexus 5548UP スイッチ間の仮想 SAN（vSAN）で SAN トラフィックを伝送する FCoE SAN ポート チャネルが設定されます。SAN のセキュリティを実現するため、インフラストラクチャおよびテスト サーバが認識できる正しいストレージ システムの論理ユニット番号（LUN）にアクセスできるように、Cisco Nexus 5548UP スイッチ上でゾーニングが設定されました。

この項では、Cisco UCS および Cisco Nexus ネットワーク クラウド環境で必要な VSAN および SAN ポート チャネルを設定する方法について詳しく説明します。

この導入モデルでは、クラウド テナント A のストレージ トラフィックを処理するためにテナント A- ファブリック A とテナント A- ファブリック B とで個別の FCoE SAN ポート チャネル VSAN 10 を作成します。同様の方法で、クラウド内のマルチテナントに対してさまざまな VSAN を作成して、ストレージ ネットワーク マルチテナントを提供できます。

Cisco Nexus 5548UP スイッチ A

SAN ポート チャネルは、デフォルト値で作成されます。デフォルト設定は、他の物理インターフェイスと同様に変更できます。グローバル コンフィギュレーション モードで SAN ポート チャネルを設定するには、Nexus スイッチにログインし、次のコマンドを実行します。

1. feature fport-channel-trunk と入力します。
2. vsan database と入力します。
3. vsan 200 と入力します。
4. exit と入力します。
5. interface port-channel 1 と入力します。
6. switch mode trunk と入力します。
7. switch trunk allowed vlan 200 と入力します。
8. exit と入力します。
9. interface Ethernet 1/31 と入力します。
10. switchport mode trunk と入力します。
11. switchport trunk allowed vlan 200 と入力します。
12. channel-group 10 mode acive と入力します。
13. exit と入力します。
14. interface Ethernet 1/32 と入力します。
15. switchport mode trunk と入力します。
16. switchport trunk allowed vlan 200 と入力します。
17. channel-group 10 mode acive と入力します。
18. exit と入力します。

Cisco Nexus 5548UP スイッチ B

SAN ポート チャネルは、デフォルト値で作成されます。デフォルト設定は、他の物理インターフェイスと同様に変更できます。グローバル コンフィギュレーション モードで SAN ポート チャンネルを設定するには、次のコマンドを実行します。

1. feature fport-channel-trunk と入力します。
2. vsan database と入力します。
3. vsan 300 と入力します。
4. exit と入力します。
5. interface port-channel 10 と入力します。
6. switch mode trunk と入力します。
7. switch trunk allowed vlan 300 と入力します。
8. exit と入力します。
9. interface Ethernet 1/31 と入力します。
10. switchport mode trunk と入力します。
11. switchport trunk allowed vlan 300 と入力します。
12. channel-group 10 mode acive と入力します。
13. exit と入力します。
14. interface Ethernet 1/32 と入力します。
15. switchport mode trunk と入力します。
16. switchport trunk allowed vlan 300 と入力します。
17. channel-group 10 mode acive と入力します。
18. exit と入力します。

NetApp ストレージ

この項では、Citrix CloudPlatform 4.2.1 構築用のストレージ インフラストラクチャを導入するためのクラウド ストレージ レイアウトのデザイン上の考慮事項について説明します。マルチテナント クラウド環境で共有ストレージ インフラストラクチャのさまざまなサービス レベルをサポートするために、NetApp では次のような多彩な機能が用意されています。

- 複数のワークロードをサポートするユニファイド データ ストレージ アーキテクチャ。
- クラウド コンピューティングの動的な需要に対応するシームレスな多元的スケーリング。
- 容量要件とコストの 50 % 以上の削減に役立つストレージ効率。
- 共有サーバ、ストレージ、およびネットワーク リソースを分離して提供するセキュアなマルチテナント セグメント。
- ストレージのプロビジョニング、包括的な可視性、およびモニタを自動化するサービスの自動化および分析。
- 共有クラウド ストレージ リソースの無停止のデータ可用性を可能にする中断のない連続的な操作。
- バックアップ、ディザスタ リカバリ、アーカイブ、コンプライアンス、およびセキュリティ サービス レベル合意書への対応に役立つ統合されたデータ保護。

- アプリケーション アフィニティとワークロードに基づいてデータの移動を自動化する仮想ストレージの階層化。
- ロールベースの管理、暗号化、ウイルス対策を通じてデータ資産を保護する組み込みのデータ セキュリティ。

NetApp アグリゲーション レイヤは、Citrix CloudPlatform 4.2.1 によってオンデマンドで使用されるストレージ容量およびディスク IOPS の大型の仮想化プールを提供します。アグリゲーション レイヤのサイジングは、テナント データを保存し、想定されたワークロードのストレージ容量、パフォーマンス、スナップショット コピー バックアップの要件に対応するための、Citrix CloudPlatform 4.2.1 のホスティングのストレージ要件に基づきます。環境に対してサイジングするときに、必要なプランニングを実行して、個々の要件に対する正確なストレージ設定を判断します。アグリゲーション レイヤ 0（Aggr0）は、NetApp ストレージ構成の操作に NetApp clustered Data ONTAP オペレーティング システムを使用するルート NetApp フレキシブル ボリューム（FlexVol® ボリューム）をホストするために定義されます。NetApp ストレージ コマンド オプションの詳細については、http://now.netapp.com/NOW/public/knowledge/docs/ontap/rel732/pdfs/ontap/210-04499.pdf を参照してください。

（注） このデザインでは、Citrix クラウド環境での仮想マシンのホスティング用のプライマリおよびセカンダリ ストレージを、TenantA ホストでプロビジョニングするために、集約、フレキシブル ボリューム、FC および iSCSI LUN、igroup、NFS マウント ポイントを作成します。

ストレージ設定

コントローラ FAS32xx シリーズ

表 7　　コントローラ FAS32XX シリーズの要件

要件	参照先	注
ストレージ システムを設置する必要のある実際の設置場所が準備されている必要がある	Site Requirements Guide	「Site Preparation」の項を参照してください。
ストレージ システムの接続性要件	Site Requirements Guide	「System Connectivity Requirements」の項を参照してください。
ストレージ システムの総所要電力	Site Requirements Guide	「Circuit Breaker, Power Outlet Balancing, System Cabinet Power Cord Plugs, and Console Pinout Requirements」の項を参照してください。
ストレージ システム モデル固有の要件	Site Requirements Guide	「FAS32xx/V32xx Series Systems」の項を参照してください。

System Configuration Guides

『System configuration guides』には、特定の clustered Data ONTAP バージョンでサポートされるハードウェアとソフトウェア コンポーネントが記されています。これらのオンライン ガイドには、clustered Data ONTAP ソフトウェアで現在サポートされているすべての NetApp ストレージ アプライアンスの構成情報が記載されています。また、コンポーネントの互換性の表も記載されています。次のドキュメントは、この説明で導入した clustered Data ONTAP 8.1.2 ソフトウェアに適用されます。

1. NetApp Support サイトにある『System Configuration Guides』をチェックして、ハードウェアとソフトウェア コンポーネントが、インストールする予定の Data ONTAP のバージョンでサポートされていることを確認してください。
2. 『System Configuration Guide』で、該当する NetApp ストレージ アプライアンスをクリックしてから、表示するコンポーネントをクリックします。または、ストレージ アプライアンス別にコンポーネントを比較するには、コンポーネントをクリックしてから、表示する NetApp ストレージ アプライアンスをクリックします。

コントローラ

NetApp Support サイトにある FAS32xx のドキュメントに記された、コントローラの実際の設置手順に従ってください。

ディスク シェルフ DS2246 シリーズ

DS2246 ディスク シェルフ

「Disk Shelf Installation and Setup section of the DS2246 Disk Shelf Overview」の手順に従って、新しいストレージ システムのディスク シェルフを設置します。

『SAS Disk Shelves Universal SAS and ACP Cabling Guide』に記されたコントローラ モデルに適したケーブル配線手順に従います。

次の情報が DS2246 ディスク シェルフに適用されます。

- SAS ディスク ドライブはソフトウェアベースのディスクのオーナーシップを使用します。ディスク ドライブのオーナーシップは、ストレージ システムの物理的な接続のトポグラフィーを使用するのではなく、ソフトウェア オーナーシップ情報をディスク ドライブに書き込むことにより、特定のストレージ システムに割り当てられます。
- 使用される接続用語：シェルフ ツー シェルフ（デイジー チェーン）、コントローラ ツー シェルフ（上部接続）、シェルフ ツー コントローラ（下部接続）。
- ストレージ システムごとに一意のディスク シェルフ ID を設定する必要があります（0 ～ 98 の数字）。
- デジタル ディスプレイのシェルフ ID を変更するには、ディスク シェルフの電源を入れる必要があります。デジタル ディスプレイはディスク シェルフの前面にあります。
- シェルフ ID を変更した後に有効にするには、ディスク シェルフの電源を再投入する必要があります。
- Data ONTAP を実行している既存のストレージ システムに含まれるディスク シェルフでシェルフ ID を変更した場合、Data ONTAP が古いディスク シェルフ アドレスを適切に削除し、新しいディスク シェルフ アドレスのコピーを更新できるように、電源を入れなおす前に少なくとも 30 秒待つ必要があります。

- 新たに設置されたストレージ システム（ディスク シェルフではまだ Data ONTAP を実行していない）に含まれるディスク シェルフでシェルフ ID を変更した場合は待つ必要はありません。すぐにディスク シェルフの電源を再投入できます。

Cisco Nexus 5596 クラスタ スイッチ設定

Cisco Nexus 5596 クラスタ ネットワーク スイッチ設定の前提条件は次のとおりです。

- 新規導入する Cisco Nexus 5596 スイッチ用のラックおよび接続電源。
- スイッチのシリアル コンソール ポート（9600、8、n、1）に接続するターミナル セッションの提供。
- ネットワークを管理し、IP アドレス情報の提供のために用意された mgmt() ポートに接続。
- 管理者のパスワードの取得。
- スイッチ名の決定。
- SSH キー タイプ（dsa、rsa、または rsa1）を識別
- Cisco Smart Call Home 用の電子メール サーバの設定、およびこのスイッチと電子メール サーバ間の IP 接続の設定。
- Cisco Smart Call Home 用の SNMP 連絡先情報（名前、電話番号、番地）の提供。
- Cisco Smart Call Home の適切な Cisco SMARTnet® サービス契約に関連する CCO ID の識別。

Cisco Nexus 5596 クラスタ インターコネクトの初期設定

最初に Cisco Nexus 5596 クラスタ インターコネクトにアクセスした際に、セットアップ プログラムが実行され、管理イーサネット インターフェイスを通して通信するためにスイッチに必要な IP アドレスやその他の設定情報を入力するためのプロンプトが表示されます。この情報は、スイッチを設定および管理するために必要です。構成が後で変更された場合、EXEC モードで `setup` コマンドを実行してセットアップ ウィザードに再度アクセスできます。

Cisco Nexus 5596 クラスタ インターコネクトをセットアップするには、次の手順を実行します。これらの手順は、両方のクラスタ インターコネクトで実行する必要があります。

1. Cisco Nexus 5596 クラスタ インターコネクトに表示されるセットアップ プロンプトに適切な応答を入力します。

```
Do you want to enforce secure password standard (yes/no): yes
Enter the password for the "admin": <password>
Confirm the password for "admin": <password>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name: <switchname>
Continue with out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address: <ic_mgmt0_ip>
Mgmt0 IPv4 netmask: <ic_mgmt0_netmask>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <ic_mgmt0_gw>
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa): rsa
Number of key bits <768-2048> : 1024
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address: <ntp_server_ip>
```

```
Enter basic FC configurations (yes/no) [n]: Enter
```

2. セットアップの最後に、設定での選択が表示されます。情報を確認し設定を保存します。

```
Would you like to edit the configuration? (yes/no) [n]: <n>
Use this configuration and save it?  (yes/no) [y]: <y>
```

NetApp Cluster スイッチ ソフトウェアのダウンロードとインストール

Cisco Nexus 5596 を Data ONTAP 8.1.2 を搭載したクラスタ ネットワーク スイッチとして使用する場合、NX-OS バージョン 5.2(1)N1(1) が実行されている必要があります。スイッチのコマンドライン インターフェイスから `show version` コマンドを入力すると、スイッチで現在実行中のスイッチ バージョンが表示されます。現在実行中のバージョンが 5.2(1)N1(1) でない場合、NetApp Support サイトを開き Cisco Nexus 5596 スイッチ用の NX-OS 5.2(1)N1(1) をダウンロードしインストールします。両方のクラスタ インターコネクトで NX-OS バージョン 5.2(1)N1(1) を実行していることを確認してください。

NetApp クラスタ スイッチ リファレンス コンフィギュレーション ファイルのダウンロードとマージ

クラスタ ネットワーク スイッチおよびマネジメント ネットワーク スイッチはコンフィギュレーション ファイルがインストールされずに出荷されます。これらのファイルは、導入時にスイッチにダウンロードする必要があります。クラスタ ネットワーク スイッチおよびマネジメント ネットワーク スイッチを初めてインストールするとき、または Cisco スイッチ ソフトウェアを更新または再インストールしたときはコンフィギュレーション ファイルをダウンロードする必要があります。

初期セットアップが終わると、NetApp クラスタ ネットワーク スイッチ リファレンス コンフィギュレーションをスイッチに転送して既存のコンフィギュレーションとマージする必要があります。この処理の手順および適切なスイッチに対するリファレンス コンフィギュレーション ファイルは、NetApp Support サイトから入手できます。

コンフィギュレーション ファイルをホストにダウンロードして Cisco Nexus 5596 スイッチにインストールするには、両方のクラスタ インターコネクトで次の手順を実行します。

1. スイッチに対してコンソール接続します。`show run` コマンドを実行して既存のコンフィギュレーションを確認します。
2. スイッチにログインします。ホストがネットワーク上でこのスイッチを認識しているか確認します（たとえば、ping ユーティリティを使用して）。
3. 次のコマンドを入力します。

```
copy <transfer protocol>: bootflash: vrf management
```

4. コンフィギュレーション ファイルがダウンロードされたか確認します。
5. このコンフィギュレーション ファイルを既存の running-config にマージします。次のコマンドを <config file name> をスイッチ タイプのファイル名に置き換えて実行します。各ポートが設定されるたびに PortFast に関する一連の警告が表示されます。

```
copy <config file name> running-config
```

6. コンフィギュレーションのマージが成功したかを `show run` コマンドを実行して確認し、その結果出力とダウンロードしたコンフィギュレーション ファイル（.txt ファイル）の内容を比較します。
7. インストールベースのスイッチと新しいスイッチの両方に対する出力は、コンフィグレーション ファイルの以下の項目の内容が同一である必要があります。
   - バナー（該当するバージョンに一致している）
   - Cluster Node x のようなスイッチ ポートの説明

- 新しい ISL アルゴリズム ポート - チャネル ロードバランス イーサネット ソース - 宛先ポート

8. 新しいスイッチに対する出力は、コンフィグレーション ファイルの以下の項目の内容が同一である必要があります。
   - ポート チャネル
   - ポリシー マップ
   - System QoS
   - インターフェイス
   - ブート
9. インストールベース スイッチへの出力には、以下の項目に対する値 on を受信および送信するフロー制御が必要になります。
   - インターフェイス ポート チャネル 1 および 2
10. イーサネット インターフェイス 1/41 からイーサネット インターフェイス 1/48。
11. running-config を startup-config にコピーします。

```
copy running-config startup-config
```

Cisco Smart Call Home のセットアップ

Smart Call Home を Cisco Nexus 5596 スイッチに設定するには、次の手順を実行します。

1. グローバル コンフィギュレーション モードで snmp-server contact コマンドを使用して必須システム接点を入力します。次に、callhome コマンドを実行して callhome コンフィギュレーション モードを開始します。

```
NX-5596#config t
NX-5596(config)#snmp-server contact <sys-contact>
NX-5596(config)#callhome
```

2. 必須連絡先情報（電話番号、電子メール アドレス、および番地）を設定します。

```
NX-5596(config-callhome)#email-contact <email-address>
NX-5596(config-callhome)#phone-contact <+1-000-000-0000>
NX-5596(config-callhome)#streetaddress <a-street-address>
```

3. 必須電子メール サーバ情報を設定します。サーバ アドレスは、Call Home によって送信される電子メール メッセージの宛先 SMTP サーバの IPv4 アドレス、IPv6 アドレス、またはドメイン名です。オプションのポート番号（デフォルトは 25）および VRF が設定される場合もあります。

```
NX-5596(config-callhome)#transport email smtp-server <ip-address> port 25 use-vrf
<vrf-name>
```

4. 接続先プロファイル CiscoTAC-1 電子メール アドレスを callhome@cisco.com に設定します。

```
NX-5596(config-callhome)#destination-profile CiscoTAC-1 email-addr callhome@cisco.com
vrf management
```

5. 定期的インベントリを有効にし、間隔を設定します。

```
NX-5596(config-callhome)#periodic-inventory notification
NX-5596(config-callhome)#periodic-inventory notification interval 30
```

6. callhome を有効にし、コンフィギュレーション モードを終了した後で設定を保存します。

```
NX-5596(config-callhome)#enable
NX-5596(config-callhome)#end
NX-5596#copy running-config startup-config
```

7. 登録処理を開始するために callhome インベントリ メッセージを送信します。

```
NX-5596#callhome test inventory
trying to send test callhome inventory message
successfully sent test callhome inventory message
```

8. スイッチの登録に関するシスコからの電子メールを確認してください。電子メールの指示に従って Smart Call Home への登録を完了します。

SNMP モニタリングのセットアップ

ガイドラインとして次の例を使用して SNMP を構成します。この例では、SNMPv1 トラップ用のホスト レシーバを設定し、そしてすべてのリンクのアップまたはダウンのトラップを有効にしています。

```
NX-5596(config)# snmp-server host <ip-address> traps { version 1 } <community>
[udp_port <number>]
NX-5596(config)# snmp-server enable traps link
```

clustered Data ONTAP 8.1.2

ノード 1

1. ストレージ システムのコンソール ポートに接続します。「Loader-A」というプロンプトが表示されます。しかし、ストレージ システムがリブート ループに含まれる場合、次のメッセージが表示されたら Ctrl+C を押して自動ブートを終了します。

   ```
   Starting AUTOBOOT press Ctrl-C to abort
   ```

2. 「Loader-A」プロンプトで次を入力します。

   ```
   printenv
   ```

3. last-OS-booted-ver パラメータが 8.1.2 に設定されていない場合、手順 4 に進み Data ONTAP 8.1.2 ソフトウェアをロードします。Data ONTAP 8.1.2 がすでにロードされている場合、手順 16 に進みます。

4. システムに起動を許可します。

   ```
   boot_ontap
   ```

5. 「Press Ctrl-C for Boot Menu」というメッセージが表示されたら Ctrl+C を押します。

（注） Data ONTAP 8.1.2 が起動されたソフトウェアのバージョンではない場合、次の手順で新しいソフトウェアをインストールします。Data ONTAP 8.1.2 が起動されたバージョンの場合、オプション 8 および yes を選択してノードをリブートします。ステップ 5 に進みます。

6. 新しいソフトウェアをインストールするには、最初にオプション 7 を選択します。

   ```
   7
   ```

7. 無停止のアップグレードを実施するには yes と回答します。

   ```
   y
   ```

8. ダウンロードに使用するネットワーク ポートには e0M を選択します。

   ```
   e0M
   ```

9. yes を選択してすぐにリブートします。

   ```
   y
   ```

10. e0M の IP アドレス、ネットマスク、およびデフォルト ゲートウェイをそれぞれの位置に入力します。

    ```
    <<var_node01_mgmt_ip>> <<var_node01_mgmt_mask>> <<var_node01_mgmt_gateway>>
    ```

11. このソフトウェアのある URL を入力します。

（注） この Web サーバは ping に応答可能である必要があります。

```
<<var_url_boot_software>>
```

12. ユーザ名で Enter キーを押して、ユーザ名がないことを示します。

```
Enter
```

13. yes と入力して、新しくインストールしたソフトウェアを今後のリブートで使用するデフォルトとして設定します。

```
y
```

14. yes と入力して、ノードをリブートします。

```
y
```

（注） 新しいソフトウェアをインストールする際に、システムで BIOS およびアダプタ カードのファームウェアのアップグレードが実行される場合があり、リブートが開始されて「LOADER」プロンプトで停止する可能性があります。これらの動作が起こると、この手順から外れてしまいます。

15. 次のメッセージが表示されたら Ctrl+C を押して自動ブートを終了します。

```
Starting AUTOBOOT press Ctrl-C to abort…
```

16.「LOADER-A」プロンプトで次を入力します。

```
printenv
```

（注） bootarg.init.boot_clustered true が一覧表示されない場合、clustered Data ONTAP で起動するようにシステムが設定されていません。

17. clustered Data ONTAP で起動するようにシステムが設定されていない場合、「LOADER」プロンプトで、clustered Data ONTAP でシステムが確実に起動するように次のコマンドを入力します。

```
setenv bootarg.init.boot_clustered true
setenv bootarg.bsdportname e0M
```

18.「LOADER-A」プロンプトで次を入力します。

```
autoboot
```

19.「Press Ctrl-C for Boot Menu」と表示されたら次を入力します。

```
Ctrl - C
```

20. 設定をクリアしすべてのディスクを初期化するために、オプション 4 を選択します。

```
4
```

21.「Zero disks」に yes と回答し、設定をリセットし新しいファイル システムをインストールします。

```
y
```

22. ディスク上のデータすべてを削除するには yes と入力します。

```
y
```

（注） ルート ボリュームの初期化および作成を完了するには、接続されているディスクの数にもよりますが 75 分以上かかります。初期化完了後、ストレージ システムがリブートされます。ノード 01 のディスクのゼロ化中にノード 02 を設定できます。

ノード 2

1. ストレージ システムのコンソール ポートに接続します。「Loader-A」というプロンプトが表示されます。しかし、ストレージ システムがリブート ループに含まれる場合、次のメッセージが表示されたら Ctrl+C を押して自動ブートを終了します。

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2.「Loader-A」プロンプトで次を入力します。

```
printenv
```

3. last-OS-booted-ver パラメータが 8.1.2 に設定されていない場合、手順 4 に進み Data ONTAP 8.1.2 ソフトウェアをロードします。Data ONTAP 8.1.2 がすでにロードされている場合、手順 16 に進みます。
4. システムに起動を許可します。

```
boot_ontap
```

5. 「Press Ctrl-C for Boot Menu」が表示されたら Ctrl+C を押します。

```
Ctrl-C
```

（注） Data ONTAP 8.1.2 が起動されたソフトウェアのバージョンではない場合、次の手順で新しいソフトウェアをインストールします。Data ONTAP 8.1.2 が起動されたバージョンの場合、オプション 8 および yes を選択してノードをリブートします。ステップ 15 に進みます。

6. 新しいソフトウェアをインストールするには、最初にオプション 7 を選択します。

```
7
```

7. 無停止のアップグレードを実施するには yes と回答します。

```
y
```

8. ダウンロードに使用するネットワーク ポートには e0M を選択します。

```
e0M
```

9. yes を選択してすぐにリブートします。

```
y
```

10. e0M の IP アドレス、ネットマスク、およびデフォルト ゲートウェイをそれぞれの位置に入力します。

```
<<var_node02_mgmt_ip>> <<var_node02_mgmt_mask>> <<var_node02_mgmt_gateway>>
```

11. このソフトウェアのある URL を入力します。

（注） この Web サーバに到達可能である必要があります。

```
<<var_url_boot_software>>
```

12. ユーザ名で Enter を入力して、ユーザ名がないことを示します。

```
Enter
```

13. yes を選択して、新しくインストールしたソフトウェアを今後のリブートで使用するデフォルトとして設定します。

```
y
```

14. yes を選択して、ノードをリブートします。

```
y
```

（注） 新しいソフトウェアをインストールする際に、システムで BIOS およびアダプタ カードのファームウェアのアップグレードが実行される場合があり、リブートが開始されて「LOADER」プロンプトで停止する可能性があります。これらの動作が起こると、この手順から外れてしまいます。

15. 次のメッセージが表示されたら Ctrl+C を押して自動ブートを終了します。

```
Starting AUTOBOOT press Ctrl-C to abort…
```

16. 「LOADER-A」プロンプトで次を入力します。

```
printenv
```

（注） bootarg.init.boot_clustered true が一覧表示されない場合、clustered Data ONTAP で起動するようにシステムが設定されていません。

17. clustered Data ONTAP で起動するようにシステムが設定されていない場合、「LOADER」プロンプトで、clustered Data ONTAP でシステムが確実に起動するように次のコマンドを入力します。

```
setenv bootarg.init.boot_clustered true
setenv bootarg.bsdportname e0M
```

18. 「LOADER-A」プロンプトで次を入力します。

```
autoboot
```

19. プロンプトが表示されたら、ブート メニューを開くために Ctrl+C を押します。

```
Ctrl - C
```

20. 設定をクリアしすべてのディスクを初期化するために、オプション 4 を選択します。

```
4
```

21. 「Zero disks」に yes と回答し、設定をリセットし新しいファイル システムをインストールします。

```
y
```

22. ディスク上のデータすべてを削除するには yes と入力します。

```
y
```

（注） ルート ボリュームの初期化および作成を完了するには、接続されているディスクの数にもよりますが 75 分以上かかります。初期化が完了すると、ストレージ システムがリブートされます。

clustered Data ONTAP でのクラスタ作成

表 8　clustered Data ONTAP でのクラスタ作成の前提条件

クラスタ詳細	クラスタ詳細値
クラスタ名	<<var_clustername>>
clustered Data ONTAP 基本ライセンス	<<var_cluster_base_license_key>>
クラスタ管理 IP アドレス	<<var_clustermgmt_ip>>
クラスタ管理ネットマスク	<<var_clustermgmt_mask>>
クラスタ管理ポート	<<var_clustermgmt_port>>
クラスタ管理ゲートウェイ	<<var_clustermgmt_gateway>>
クラスタ Node01 IP アドレス	<<var_node01_mgmt_ip>>
クラスタ Node01 ネットマスク	<<var_node01_mgmt_mask>>
クラスタ Node01 ゲートウェイ	<<var_node01_mgmt_gateway>>

クラスタ内の最初のノードでクラスタ作成処理が実行されます。他のすべてのノードでは、クラスタ結合処理が実行されます。クラスタ内の最初のノードは Node01 とみなします。

1. 最初のノードの起動中に、コンソール上で Cluster Setup ウィザードの実行が始まります。

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
```

```
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

（注） Cluster Setup ウィザードではなくログイン プロンプトが表示される場合、工場出荷時設定を利用してログインしてウィザードを開始してから、クラスタ セットアップ コマンドを入力します。

2. 次のコマンドを入力し、新しいクラスタを作成します。

```
create
```

3. システム デフォルトが表示されます。

```
System Defaults:
Private cluster network ports [e1a,e2a].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.
Do you want to use these defaults? {yes, no} [yes]:
```

4. NetApp ではシステム デフォルトを使用することをお奨めします。システム デフォルトを使用するには Enter を押します。

（注） クラスタが作成されます。この処理には 1 ～ 2 分かかります。

5. クラスタを作成するための手順が表示されます。

```
Enter the cluster name: <<var_clustername>>
Enter the cluster base license key: <<var_cluster_base_license_key>>
Creating cluster <<var_clustername>>
Enter additional license key[]:
```

（注） この確認済みアーキテクチャ用に、SnapRestore、NFS、FCP、FlexClone、および SnapManager Suite のライセンス キーをインストールすることをお奨めします。ライセンス キーの入力を終えたら Enter を押します。

```
Enter the cluster administrators (username “admin”) password: <<var_password>>
Retype the password: <<var_password>>
Enter the cluster management interface port [e0a]: e0a
Enter the cluster management interface IP address: <<var_clustermgmt_ip>>
Enter the cluster management interface netmask: <<var_clustermgmt_mask>>
Enter the cluster management interface default gateway: <<var_clustermgmt_gateway>>
```

6. DNS ドメイン名を入力します。

```
Enter the DNS domain names:<<var_dns_domain_name>>
Enter the name server IP addresses:<<var_nameserver_ip>>
```

（注） ネーム サーバの IP アドレスが複数ある場合はカンマで区切ります。

7. ノードをセットアップします。

```
Where is the controller located []:<<var_node_location>>
Enter the node management interface port [e0M]: e0b
Enter the node management interface IP address: <<var_node01_mgmt_ip>>
enter the node management interface netmask:<<var_node01_mgmt_mask>>
Enter the node management interface default gateway:<<var_node01_mgmt_gateway>>
```

（注） ノード管理インターフェイスは、クラスタ管理インターフェイス内ではなく別のサブネット内にある必要があります。ノード管理インターフェイスはアウトオブバンド管理ネットワークに常駐でき、クラスタ管理インターフェイスはインバンド管理ネットワークに常駐できます。

8. Enter を押し、AutoSupport メッセージを受信します。
9. ノード 01 をリブートします。

```
system node reboot <<var_node01>>
y
```

10. プロンプトが表示されたら、ブート メニューを開くために Ctrl+C を押します。

```
Ctrl - C
```

11. 5 を選択してメンテナンス モードで起動します。

```
5
```

12.「Continue with boot?」というプロンプトが表示されたら、y と入力します。
13. 使用している環境の HA ステータスを確認するには、次のコマンドを実行します。

```
ha-config show
```

（注） どちらのコンポーネントも HA モードでない場合は、ha-config modify コマンドを使用してコンポーネントを HA モードにします。

14. 所有されていないディスク数を確認するには、次の行を入力します。

```
disk show -a
```

（注） このリストでは所有されているディスクはありません。

15. ディスクを割り当てます。

（注） このリファレンス アーキテクチャでは、各コントローラにディスクの半数を割り当てます。しかし、ワークロード設計は異なる割合を示す可能性があります。

```
disk assign -n <<var_#_of_disks>>
```

16. コントローラをリブートします。

```
halt
```

17.「LOADER-A」プロンプトで次を入力します。

```
autoboot
```

clustered Data ONTAP へのクラスタ結合

表 9 clustered Data ONTAP へのクラスタ結合の前提条件

クラスタ詳細	クラスタ詳細値
クラスタ名	<<var_clustername>>
クラスタ管理 IP アドレス	<<var_clustermgmt_ip>>
クラスタ Node02 IP アドレス	<<var_node02_mgmt_ip>>

表 9　clustered Data ONTAP へのクラスタ結合の前提条件

クラスタ Node02 ネットマスク	<<var_node02_mgmt_mask>>
クラスタ Node02 ゲートウェイ	<<var_node02_mgmt_gateway>>

クラスタ内の最初のノードでクラスタ作成処理が実行されます。他のすべてのノードでは、クラスタ結合処理が実行されます。クラスタ内の最初のノードは Node01 とみなし、この例でクラスタに結合するノードを Node02 とします。

1. ノードの起動の際に、コンソールで実行する Cluster Setup ウィザードが開始します。

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

（注）　Cluster Setup ウィザードではなくログイン プロンプトが表示される場合、工場出荷時設定を利用してログインしてウィザードを開始してから、クラスタ セットアップ コマンドを入力します。

2. 次のコマンドを入力し、クラスタを結合します。

```
join
```

3. システム デフォルトが表示されます。

```
System Defaults:
Private cluster network ports [e1a,e2a].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.
Do you want to use these defaults? {yes, no} [yes]:
```

4. NetApp ではシステム デフォルトを使用することをお奨めします。システム デフォルトを使用するには Enter を押します。

（注）　クラスタの作成には 1 ～ 2 分かかります。

5. クラスタを作成するための手順が表示されます。

```
Enter the name of the cluster you would like to join [<<var_clustername>>]:Enter
```

（注）　ノードによってクラスタ名が検索されます。

6. ノードをセットアップします。

```
Enter the node management interface port [e0M]: e0b
Enter the node management interface IP address: <<var_node02_mgmt_ip>>
Enter the node management interface netmask: Enter
Enter the node management interface default gateway: Enter
```

7. ノード管理インターフェイスは、クラスタ管理インターフェイス内ではない別のサブネット内にある必要があります。ノード管理インターフェイスはアウトオブバンド管理ネットワークに存在でき、クラスタ管理インターフェイスはインバンド管理ネットワークに存在できます。

8. Enter を押し、AutoSupport メッセージを受信します。

9. 管理者ユーザ ID および <<var_password>> を使用して Cluster Interface にログインします。
10. ノード 02 をリブートします。

```
system node reboot <<var_node02>>
y
```

11. プロンプトが表示されたら、ブート メニューを開くために Ctrl+C を押します。

```
Ctrl - C
```

12. 5 を選択してメンテナンス モードで起動します。

```
5
```

13.「Continue with boot?」というプロンプトが表示された場合、次の行を入力します。

```
y
```

14. 使用している環境の HA ステータスを確認するには、次のように入力します。

```
ha-config show
```

（注） どちらのコンポーネントも HA モードでない場合は、`ha-config modify` コマンドを使用してコンポーネントを HA モードにします。

15. 所有されていないディスク数を確認するには、次の行を入力します。

```
disk show -a
```

16. ディスクを割り当てます。

（注） このリファレンス アーキテクチャでは、各コントローラにディスクの半数を割り当てます。しかし、ワークロード設計は異なる割合を示す可能性があります。残りのすべてのディスクをノード 02 に割り当てます。

```
disk assign -n <<var_#_of_disks>>
```

17. コントローラをリブートします。

```
halt
```

18.「LOADER-A」プロンプトで次を入力します。

```
autoboot
```

19. プロンプトが表示されたら、ブート メニューを開くために Ctrl+C を押します。

```
Ctrl-C
```

クラスタへのログイン

クラスタ IP またはホスト名への SSH 接続を開き、事前に提供されているパスワードで管理ユーザにログインします。

すべてのスペア ディスクのゼロ化

クラスタ内のすべてのスペア ディスクをゼロにします。

```
disk zerospares
```

クラスタ管理の Auto-Revert の設定

クラスタ管理インターフェイスで auto-revert パラメータを設定するには、次のように入力します。

```
network interface modify –vserver <<var_clustername>> -lif cluster_mgmt –auto-revert
true
```

clustered Data ONTAP でのフェールオーバー グループ管理

管理ポート フェールオーバー グループを作成します。

```
network interface failover-groups create -failover-group fg-cluster-mgmt -node
<<var_node01>> -port e0a
network interface failover-groups create -failover-group fg-cluster-mgmt -node
<<var_node02>> -port e0a
```

管理フェールオーバー グループのクラスタ管理 LIF への割り当て

管理ポート フェールオーバー グループをクラスタ管理 LIF に割り当てます。

```
network interface modify –vserver <<var_clustername>> -lif cluster_mgmt
–failover-group fg-cluster-mgmt
```

clustered Data ONTAP でのフェールオーバー グループ ノード管理

管理ポート フェールオーバー グループを作成します。

```
network interface failover-groups create -failover-group fg-node-mgmt-01 -node
<<var_node01>> -port e0b
network interface failover-groups create -failover-group fg-node-mgmt-01 -node
<<var_node01>> -port e0M
network interface failover-groups create -failover-group fg-node-mgmt-02 -node
<<var_node02>> -port e0b
network interface failover-groups create -failover-group fg-node-mgmt-02 -node
<<var_node02>> -port e0M
```

ノード管理フェールオーバー グループのノード管理 LIF への割り当て

管理ポート フェールオーバー グループをクラスタ管理 LIF に割り当てます。

```
network interface modify –vserver <<var_node01>> -lif mgmt1 –auto-revert true
–use-failover-group enabled –failover-group fg-node-mgmt-01
network interface modify –vserver <<var_node02>> -lif mgmt1 –auto-revert true
–use-failover-group enabled –failover-group fg-node-mgmt-02
```

clustered Data ONTAP での Flash Cache

各ノードで Flash Cache を有効にするには、次の手順を実行します。

クラスタ管理インターフェイスから次のコマンドを実行します。

```
system node run -node <<var_node01>> options flexscale.enable on
system node run -node <<var_node01>> options flexscale.lopri_blocks off
system node run -node <<var_node01>> options flexscale.normal_data_blocks on
system node run -node <<var_node02>> options flexscale.enable on
system node run -node <<var_node02>> options flexscale.lopri_blocks off
system node run -node <<var_node02>> options flexscale.normal_data_blocks on
```

（注） Data ONTAP 8.1 以降では、Flash Cache 用に別のライセンスは必要ありません。

（注） メタデータ モードまたは低優先度キャッシュ モードでの Flash Cache の設定方法の指示については、『TR-3832: Flash Cache Best Practices Guide』を参照してください。設定をカスタマイズする前に、カスタム設定が必要かどうか、つまりデフォルト設定で十分ではないのかを決定します。

clustered Data ONTAP での 64 ビット アグリゲート

ルート ボリュームを含む 64 ビット アグリゲートは Data ONTAP セットアップ処理の際に作成されます。追加の 64 ビットアグリゲートを作成するには、アグリゲート名、アグリゲートを作成するノード、およびアグリゲートを構成するディスク数を決定します。

1. 次のコマンドを実行して、新しいアグリゲートを作成します。

```
aggr create -aggregate aggr01 -nodes <<var_node01>> -B 64 -s <<var_raidsize>>
-diskcount <<var_num_disks>>
aggr create -aggregate aggr02 -nodes <<var_node02>> -B 64 -s <<var_raidsize>>
-diskcount <<var_num_disks>>
```

（注） 最低 1 台のディスク（最大容量のディスクを選択）はスペアとして構成内に保持してください。最善の方法は、ディスクのタイプと容量ごとに最低 1 台のスペアを設定することです。

（注） アグリゲート内に 12 台から 20 台のディスク（SAS ディスク用）のほぼバランスのとれた（サイズの同じ）RAID グループを構成できるように RAID グループのサイズを計算します。たとえば、52 台のディスクがアグリゲートに割り当てられる場合、RAID グループのサイズには 18 を選択します。RAID グループのサイズを 18 にすると、ディスク 18 台の RAID グループが 2 つとディスク 16 台の RAID グループが 1 つできます。ここでデフォルトの RAID グループ サイズは 16 ディスクであり、RAID グループ サイズが大きいほど障害時のディスクの再構築に時間がかかることに注意してください。

（注） アグリゲートはディスクのゼロ化が完了するまで作成できません。aggr show コマンドを使用して、アグリゲート作成状況を表示します。aggr01 および aggr02 の両方がオンラインになってから手順を次へ進めます。

1. 作成したばかりの 2 つのデータ アグリゲートの Snapshot コピーを無効にします。

```
node run <<var_node01>> aggr options aggr01 nosnap on
node run <<var_node02>> aggr options aggr02 nosnap on
```

2. この 2 つのデータ アグリゲートの既存の Snapshot コピーをすべて削除します。

```
node run <<var_node01>> snap delete -A -a -f aggr01
node run <<var_node02>> snap delete -A -a -f aggr02
```

3. ノード 02 上のこのアグリゲートの命名規則に一致するようにノード 01 上のルート アグリゲートの名前を変更します。

```
aggr show
aggr rename -aggregate aggr0 -newname <<var_node01_rootaggrname>>
```

サービス プロセッサ

ネットワークおよび AutoSupport 設定に関する情報を収集してから、サービス プロセッサ（SP）を設定します。

DHCP またはスタティック アドレス設定を使用して SP を設定します。SP でスタティック IP アドレスが使用される場合、以下の SP 前提条件を満たしているか確認してください。

- 利用可能なスタティック IP アドレス
- ネットワーク ネットマスク
- ネットワーク ゲートウェイ IP
- AutoSupport 情報

最適な方法は、SP を設定する前に AutoSupport 受信者を設定しておくことです。Data ONTAP から自動で AutoSupport 設定が SP に送信され、AutoSupport で指定されたシステム管理受信者にアラートおよび通知を SP から AutoSupport を介して送信できるようになります。SP を設定する際、プロンプトが表示されたら AutoSupport メール ホストの名前と IP アドレスを入力します。

サービス プロセッサはノードごとにセットアップする必要があります。

ノード単位のサービス プロセッサの最新リリースへのアップグレード

リモート管理デバイスで使用可能な最新アップデートの利点を使用するためには、Data ONTAP 8.1.2 を使用して、サービス プロセッサ（SP）ファームウェアを最新にアップグレードして必要があります。

1. Web ブラウザを使用して、http://support.netapp.com/NOW/cgi-bin/fw に接続します。
2. 使用しているストレージ プラットフォームに対応する [Data ONTAP] プロンプト ページから、インストールするサービス プロセス イメージに移動します。
3. 使用しているストレージ プラットフォームに対応する SP ファームウェアの最新リリースをダウンロードするページに進みます。
4. このページの指示にしたがって、クラスタの両方のノードで SP を更新します。クラスタ管理インターフェイスからアクセス可能な Web サーバに .zip ファイルをダウンロードする必要があります。指示の手順 1a の代わりに以下のコマンドを実行し、次に手順 2 ～ 6 を各ノード上で実行します。

```
system image get -node * -package http://web_server_name/path/SP_FW.zip. Also, instead
of run local, use system node run <<var_nodename>>,
```

ノード 01 のサービス プロセッサの設定

1. クラスタのシェルから、次のコマンドを入力します。

```
system node run <<var_node01>> sp setup
```

2. 次のように入力して SP をセットアップします。

```
Would you like to configure the SP? Y
Would you like to enable DHCP on the SP LAN interface? no
Please enter the IP address of the SP[]: <<var_node01_sp_ip>>
Please enter the netmask of the SP[]: <<var_node01_sp_mask>>
Please enter the IP address for the SP gateway[]: <<var_node01_sp_gateway>>
```

ノード 02 のサービス プロセッサの設定

1. クラスタのシェルから、次のコマンドを入力します。

```
system node run <<var_node02>> sp setup
```

2. 次のように入力して SP をセットアップします。

```
Would you like to configure the SP? Y
Would you like to enable DHCP on the SP LAN interface? no
Please enter the IP address of the SP[]: <<var_node02_sp_ip>>
Please enter the netmask of the SP[]: <<var_node02_sp_mask>>
Please enter the IP address for the SP gateway[]: <<var_node02_sp_gateway>>
```

clustered Data ONTAP でのストレージ フェールオーバー

フェールオーバーのペアで以下のコマンドを実行して、ストレージ フェールオーバーを有効にします。

1. 2 つのノードのうちの 1 つでフェールオーバーを有効にします。

```
storage failover modify -node <<var_node01>> -enabled true
```

（注） 1 つのノードでフェールオーバーを有効にすると、両方のノードでフェールオーバーが有効になります。

2. 2 つのノードを持つクラスタに対してのみ HA モードを有効にします。
3. フェールオーバーで問題が発生する原因になるため、2 つより多いノードを持つクラスタではこのコマンドは実行しないでください。

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

4. ハードウェア アシストが正しく設定されていることを確認し、必要に応じてパートナー IP アドレスを変更します。

```
storage failover hwassist show
storage failover modify -hwassist-partner-ip <<var_node02_mgmt_ip>> -node
<<var_node01>>
storage failover modify -hwassist-partner-ip <<var_node01_mgmt_ip>> -node
<<var_node02>>
```

clustered Data ONTAP での IFGRP LACP

このタイプのインターフェイス グループには 2 つ以上のイーサネット インターフェイスおよび LACP をサポートするスイッチが必要です。このため、スイッチが正しく設定されていることを確認してください。

コマンドラインで以下のコマンドを実行し、インターフェイス グループ（ifgrp）を作成します。

```
ifgrp create -node <<var_node01>> -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e3a
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e4a
ifgrp create -node <<var_node02>> -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e3a
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e4a
```

（注） インターフェイス グループに追加する前に、すべてのインターフェイスが down ステータスである必要があります。

（注） インターフェイス グループ名は a0x の標準命名規則に従う必要があります。

clustered Data ONTAP での VLAN

NFS VLAN の作成

次のコマンドを実行します。

```
network port vlan create –node <<var_node01>> -vlan-name a0a-<<var_nfs_vlan_id>>
network port vlan create –node <<var_node02>> -vlan-name a0a-<<var_nfs_vlan_id>>
```

clustered Data ONTAP でのジャンボ フレーム

ジャンボ フレーム（通常、9000 バイトの MTU のある）を使用する clustered Data ONTAP ネットワーク ポートを設定するには、クラスタ シェルから次のコマンドを実行します。

```
network port modify –node <<var_node01>> -port a0a-<<var_nfs_vlan_id>> -mtu 9000

WARNING: Changing the network port settings will cause a serveral second interruption
in carrier.
Do you want to continue? {y|n}: y
network port modify –node <<var_node02>> -port a0a-<<var_nfs_vlan_id>> -mtu 9000
WARNING: Changing the network port settings will cause a serveral second interruption
in carrier.
Do you want to continue? {y|n}: y
```

clustered Data ONTAP での NTP

クラスタ上での時刻の同期を設定するには、次の手順を実行します。

1. クラスタの時間帯を設定します。

```
timezone <<var_timezone>>
```

（注） たとえば、米国東部では、時間帯は `America/New_York` となります。

2. クラスタの時刻を設定します。

```
date <ccyymmddhhmm>
```

（注） 日付の形式は <[世紀][年][月][日][時間][分]> で、たとえば 201208081240 となります。

3. クラスタ内の各ノードに対するネットワーク タイム プロトコル（NTP）を設定します。

```
system services ntp server create -node <<var_node01>> -server
<<var_global_ntp_server_ip>> system services ntp server create -node <<var_node02>>
-server <<var_global_ntp_server_ip>>
```

4. クラスタの NTP を有効にします。

```
system services ntp config modify -enabled true
```

clustered Data ONTAP での SNMP

1. ロケーションや宛先などの SNMP 基本情報を設定します。ポーリングの際に、この情報は SNMP の sysLocation および sysContact 変数として表示されます。

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. DFM サーバや別の障害管理システムなどのリモート ホストに送信する SNMP トラップを設定します。

```
snmp traphost add <<var_oncommand_server_fqdn>>
```

clustered Data ONTAP での SNMPv1

1. コミュニティと呼ばれる共有秘密プレーン テキスト パスワードを設定します。

```
snmp community delete all
snmp community add ro <<var_snmp_community>>
```

（注） delete all コマンドの使用には注意が必要です。コミュニティ ストリングが他のモニタリング製品に使用されている場合、delete all コマンドによってこれらの製品が削除されます。

clustered Data ONTAP での SNMPv3

SNMPv3 では、ユーザが認証用に定義され設定されている必要があります。

1. snmpv3user というユーザを作成します。

```
security login create -username snmpv3user -authmethod usm -application snmp
```

2. デフォルトの信頼できるエンティティをすべて選択して、認証プロトコルとして md5 を選択します。
3. プロンプトが表示されたら、認証プロトコル用に 8 文字の最少文字数パスワードを入力します。
4. プライバシー プロトコルとして des を選択します。
5. プロンプトが表示されたら、プライバシー プロトコル用に 8 文字の最少文字数パスワードを入力します。

clustered Data ONTAP での AutoSupport HTTPS

AutoSupport はサポート サマリー情報を NetApp through HTTPS に送信します。

次のコマンドを実行して、AutoSupport を設定します。

```
system node autosupport modify -node * -state enable –mail-hosts <<var_mailhost>>
-transport https -support enable -noteto <<var_storage_admin_email>>
```

clustered Data ONTAP での Cisco Discovery プロトコル

次の手順にしたがって、NetApp ストレージ コントローラで Cisco Discovery プロトコル（CDP）を有効にします。

（注） 実際に使用するには、スイッチやルータなど直接接続されているネットワーク機器でも CDP が有効である必要があります。

NetApp ストレージ コントローラで CDP を有効にするには、次の手順を実行します。

1. Data ONTAP で CDP を有効にします。

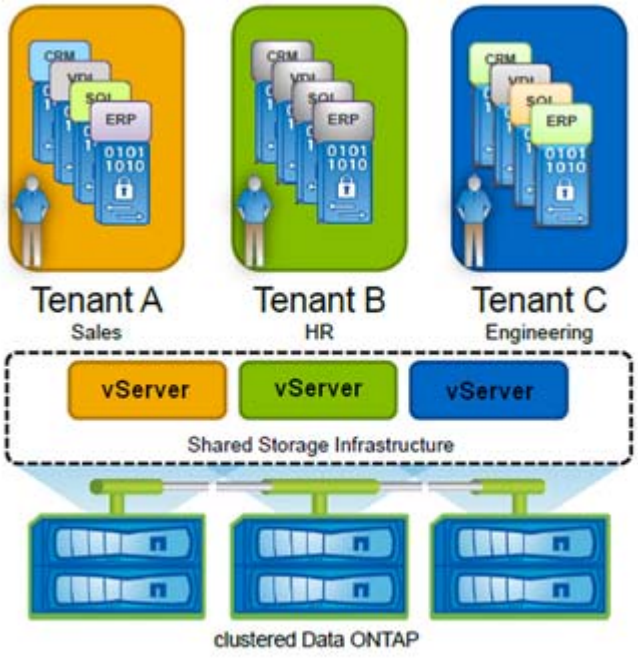
```
node run -node <<var_node01>> options cdpd.enable on
node run -node <<var_node02>> options cdpd.enable on
```

Vserver：ストレージ仮想マシン（SVM）

セキュア マルチテナントは、複数の個別テナント間で物理環境を共有する目的のための共有物理ストレージ環境内のセキュア仮想パーティションの使用法です。たとえば、ストレージ サービス プロバイダーは 3 つの異なるカスタマーそれぞれにアレイのディスク容量およびネットワーク リソースの一定部分がプロビジョニングされるような方法でストレージ アレイを設定する場合があります。セキュア マルチテナント環境では、各カスタマーはそのカスタマーに対して明確にプロビジョニングされたリソースに対してのみアクセス権があります。カスタマーは他のカスタマーのデータへのアクセス権がないばかりか、他のカスタマーの存在や共有物理アレイを共有していることさえわかりません。

それを介して clustered Data ONTAP 内のデータをアクセスするセキュア論理ストレージ パーティションは、vServer として知られ、ストレージ仮想マシン（SVM）とも呼ばれます。クラスタは最低 1 つ、場合によって複数の vServer を介してデータを提供します。vServer は、クラスタの物理リソースのセットを示す論理的な抽象概念です。データ ボリュームおよび論理ネットワーク インターフェイス（LIF）が作成されて vServer に割り当てられ、vServer がアクセス権を与えられたクラスタ内のすべてのノードに存在する可能性があります。vServer は複数のノードで同時にリソースを所有していて、これらのリソースを無停止で 1 つのノードから別のノードへ移動することができます。これは、複数のデータ プロトコルを同時にサポートする機能です。vServer 内のボリュームは単一の NAS ネームスペースを形成するためにまとめて結合でき、このネームスペースで vServer のすべてのデータを単一共有または NFS および CIFS クライアントへのマウント ポイントを介して使用可能にできます。

図 47　　vServer（ストレージ仮想マシン）



vServer（SVM）の詳細については、『TR-4160: Secure Multi-tenancy in Clustered DATA Ontap』を参照してください。

名前 Infra_Vserver を使用して vServer を作成する手順を以下に示します。また同じ手順で、必要に応じてサービス プロバイダー内または共有環境内で分離するための追加の vServer を作成できます。

インフラストラクチャ vServer を作成するには、次の手順を実行します。

1. vServer セットアップ ウィザードを実行します。

```
vserver setup

Welcome to the Vserver Setup Wizard, which will lead you through
the steps to create a virtual storage server that serves data to clients.

You can enter the following commands at any time:
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the Vserver Setup Wizard. Any changes
you made before typing "exit" will be applied.

You can restart the Vserver Setup Wizard by typing "vserver setup". To accept a
default
or omit a question, do not enter a value.

Step 1. Create a Vserver.
You can type "back", "exit", or "help" at any question.
```

2. vServer 名を入力します。

```
Enter the Vserver name:Infra_Vserver
```

3. 設定する vServer データ プロトコルを選択します。

```
Choose the Vserver data protocols to be configured {nfs, cifs, fcp, iscsi}:nfs, fcp
```

4. 設定する vServer クライアント サービスを選択します。

```
Choose the Vserver client services to configure {ldap, nis, dns}:Enter
```

5. vServer のルート ボリューム アグリゲートを入力します。

```
Enter the Vserver's root volume aggregate {aggr01, aggr02} [aggr01]:aggr01
```

6. vServer 言語セットアップを入力します。英語がデフォルト [C] です。

```
Enter the Vserver language setting, or "help" to see all languages [C]:Enter
```

7. vServer のセキュリティ スタイルを入力します。

```
Enter the Vservers root volume’s security style {unix, ntfs, mixed]} [unix]: Enter
```

8. 「Do you want to create a data volume?」に no と回答します。

```
Do you want to create a data volume?  {yes, no} [Yes]: no
```

9. 「Do you want to create a logical interface?」に no と回答します。

```
Do you want to create a logical interface?  {yes, no} [Yes]: no
```

10. 「Do you want to Configure FCP?」に no と回答します。

```
Do you want to Configure FCP? {yes, no} [yes]: no
```

11. 2 つのデータ アグリゲートを NetApp 仮想コンソールの `Infra_Vserver` アグリゲート リストに追加します。

```
vserver modify -vserver Infra_Vserver -aggr-list aggr01, aggr02
```

clustered Data ONTAP での vServer ルート ボリュームのロード シェアリング ミラーの作成

1. インフラストラクチャ vServer ルート ボリュームのロード シェアリング ミラーとなるボリュームをノードごとに作成します。

```
volume create -vserver Infra_Vserver -volume root_vol_m01 -aggregate aggr01 -size 20MB
-type DP volume create -vserver Infra_Vserver -volume root_vol_m02 -aggregate aggr02
-size 20MB -type DP
```

2. ミラーリング関係を作成します。

```
snapmirror create -source-path //Infra_Vserver/root_vol -destination-path
//Infra_Vserver/root_vol_m01 -type LS
snapmirror create -source-path //Infra_Vserver/root_vol -destination-path
//Infra_Vserver/root_vol_m02 -type LS
```

3. ミラーリング関係を初期化します。

```
snapmirror initialize-ls-set -source-path //Infra_Vserver/root_vol
```

4. 1 時間ごとの（毎時 5 分に）更新スケジュールをミラーリング関係ごとに設定します。

```
snapmirror modify -source-path //Infra_Vserver/root_vol -destination-path * -schedule
hourly
```

clustered Data ONTAP での FC サービス

FC サービスを各 vServer に作成します。また、このコマンドで FC サービスが開始され、FC エイリアスが vServer の名前に設定されます。

```
fcp create -vserver Infra_Vserver
```

clustered Data ONTAP での HTTPS アクセス

ストレージ コントローラへのセキュアなアクセスを設定する必要があります。

1. 証明書コマンドにアクセスするためには特権レベルを上げます。

```
set -privilege advanced
Do you want to continue? {y|n}: y
```

2. 通常、自己署名証明書はすでにあります。これは次のコマンドで確認します。

```
security certificate show
```

3. 自己署名証明書を生成しインストールするための 1 度きりのコマンドとして以下のコマンドを実行します。

（注） また、`security certificate delete` コマンドを使用して期限切れの証明書を削除できます。

```
security certificate create -vserver Infra_Vserver -common-name
<<var_security_cert_vserver_common_name>> -size 2048 -country <<var_country_code>>
-state <<var_state>> -locality <<var_city>> -organization <<var_org>> -unit
<<var_unit>> -email <<var_storage_admin_email>>
security certificate create -vserver <<var_clustername>> -common-name
<<var_security_cert_cluster_common_name>> -size 2048 -country <<var_country_code>>
-state <<var_state>> -locality <<var_city>> -organization <<var_org>> -unit
<<var_unit>> -email <<var_storage_admin_email>>
security certificate create -vserver <<var_node01>> -common-name
<<var_security_cert_node01_common_name>> -size 2048 -country <<var_country_code>>
-state <<var_state>> -locality <<var_city>> -organization <<var_org>> -unit
<<var_unit>> -email <<var_storage_admin_email>>
security certificate create -vserver <<var_node02>> -common-name
<<var_security_cert_node02_common_name>> -size 2048 -country <<var_country_code>>
-state <<var_state>> -locality <<var_city>> -organization <<var_org>> -unit
<<var_unit>> -email <<var_storage_admin_email>>
```

4. SSL および HTTPS アクセスを設定および有効にし、Telnet アクセスを無効にします。

```
system services web modify -external true -sslv3-enabled true
```

```
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http -action allow
system services firewall policy create -policy mgmt -service http -action deny
-ip-list 0.0.0.0/0
system services firewall policy delete -policy mgmt -service telnet -action allow
system services firewall policy create -policy mgmt -service telnet -action deny
-ip-list 0.0.0.0/0
security ssl modify –vserver Infra_Vserver –certificate
<<var_security_cert_vserver_common_name>> -enabled true
y
security ssl modify -vserver <<var_clustername>> -certificate
<<var_security_cert_cluster_common_name>> -enabled true
y
security ssl modify -vserver <<var_node01>> -certificate
<<var_security_cert_node01_common_name>> -enabled true
y
security ssl modify -vserver <<var_node02>> -certificate
<<var_security_cert_node02_common_name>> -enabled true
y
set –privilege admin
vserver services web modify –name spi|ontapi|compat –vserver * -enabled true
vserver services web access create –name spi –role admin –vserver <<var_clustername>>
vserver services web access create –name ontapi –role admin –vserver
<<var_clustername>>
vserver services web access create –name compat –role admin –vserver
<<var_clustername>>
```

（注） これらのコマンドの一部では、エントリが存在しないというエラー メッセージが返されることは正常です。

clustered Data ONTAP での NFSv3

vServer に NFS を設定するすべてのコマンドを実行します。

1. デフォルト エクスポート ポリシーにはデフォルト ルールを保証して、FlexPod エクスポート ポリシーを作成します。

```
vserver export-policy rule modify –vserver Infra_Vserver –policyname default
–ruleindex 1 -rorule never –rwrule never -superuser never
vserver export-policy create –vserver Infra_Vserver FlexPod
```

2. FlexPod エクスポート ポリシーには新しいルールを作成します。

（注） 作成する ESXi ホストそれぞれにルールを作成します。各ホストには、それ自体のルール インデックスがあります。1 番目の ESXi ホストにはルール インデックス 1 があり、2 番目の ESXi ホストにはルール インデックス 2 があり、という順に進みます。

```
vserver export-policy rule create –vserver Infra_Vserver -policyname FlexPod
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_host1_nfs_ip>> -rorule sys –rwrule
sys -superuser sys –allow-suid false
```

3. FlexPod エクスポート ポリシーをインフラストラクチャ vServer ルート ボリュームに割り当てます。

```
volume modify –vserver Infra_Vserver –volume root_vol –policy FlexPod
```

clustered Data ONTAP での FlexVol

FlexVol を作成するには、ボリューム名およびサイズ、およびそのボリュームが存在するアグリゲートの情報が必要です。2 つの VMware データストア ボリューム、サーバ起動ボリューム、および OnCommand データベース LUN を保持するボリュームを作成します。また、vServer ルート ボリュームのロード シェアリング ミラーを更新し、NFS マウントをアクセス可能にします。

```
volume create –vserver Infra_Vserver –volume infra_datastore_1 –aggregate aggr02 -size
500g –state online –policy FlexPod –junction-path /infra_datastore_1 –space-guarantee
none –percent-snapshot-space 0
volume create –vserver Infra_Vserver –volume infra_swap –aggregate aggr01 –size 100g
–state online –policy FlexPod –junction-path /infra_swap –space-guarantee none
–percent-snapshot-space 0 –snapshot-policy none

volume create –vserver Infra_Vserver –volume TenantADataSecNFS_datastore_1 –aggregate
aggr02 –size 20g –state online –policy FlexPod –junction-path / TenantADataSecNFS 1
–space-guarantee none –percent-snapshot-space 0
volume create –vserver Infra_Vserver –volume TenantA-PrimaryNFS-Storage datastore_1
–aggregate aggr02 –size 20g –state online –policy FlexPod –junction-path /
TenantADataSecNFS 1 –space-guarantee none –percent-snapshot-space 0
volume create –vserver Infra_Vserver –volume TenantA_SecondaryNFS-Storage datastore_1
–aggregate aggr02 –size 20g –state online –policy FlexPod –junction-path /
TenantADataSecNFS 1 –space-guarantee none –percent-snapshot-space 0


volume create –vserver Infra_Vserver –volume esxi_boot –aggregate aggr01 –size 100g
–state online –policy default –space-guarantee none –percent-snapshot-space 0
volume create –vserver Infra_Vserver –volume OnCommandDB –aggregate aggr02 –size 200g
–state online –policy default –space-guarantee none –percent-snapshot-space 0
snapmirror update-ls-set –source-path //Infra_Vserver/root_vol
```

clustered Data ONTAP での LUN

2 つのブート LUN、VM-Host-Infra-01 および VM-Host-Infra-02、および Baremetal 用の LUN、VM-BareMetalHost-Infra-02 を作成します。以下のコマンドを実行します。

```
lun create –vserver Infra_Vserver –volume esxi_boot –lun VM-Host-Infra-01 –size 20g
–ostype vmware –space-reserve disabled
lun create –vserver Infra_Vserver –volume esxi_boot –lun VM-Host-Infra-02 –size 20g
–ostype vmware –space-reserve disabled
lun create –vserver Infra_Vserver –volume esxi_boot –lun VM-BareMetalHost-Infra-02
–size 20g –ostype vmware –space-reserve disabled
```

clustered Data ONTAP での igroup

3 つの igroup、TenantA-ESX-HostA-Platinum-FC-igroup、TenantA-ESX-HostB-Platinum-FC-igroup、および TenantA-ESX-BareMetalHostA-Platinum-FC-igroup を作成します。

```
igroup create -igroup TenantA-ESX-HostA-Platinum-FC-igroup -protocol fcp -ostype
vmware -initiator 20:00:00:25:b5:01:01:02,20:00:00:25:b5:01:01:03 -vserver
Infra_vserver
igroup create -igroup TenantA-ESX-HostB-Platinum-FC-igroup -protocol fcp -ostype
vmware -initiator 20:00:00:25:b5:01:01:04,20:00:00:25:b5:01:01:05 -vserver
Infra_vserver
igroup create -igroup TenantA-ESX-BareMetalHost-Platinum-FC-igroup -protocol fcp
-ostype vmware -initiator 20:00:00:25:b5:04:01:06,20:00:00:25:b5:04:01:05 -vserver
Infra_vserver
```

clustered Data ONTAP での重複排除

適切なボリュームで重複排除を有効にします。

```
volume efficiency on –vserver Infra_Vserver -volume infra_datastore_1
volume efficiency on –vserver Infra_Vserver -volume TenantADataSecNFS
volume efficiency on –vserver Infra_Vserver -volume TenantA-PrimaryNFS-Storage
volume efficiency on –vserver Infra_Vserver –volume TenantA_SecondaryNFS-Storagevolume
efficiency on –vserver Infra_Vserver -volume esxi_boot
volume efficiency on –vserver Infra_Vserver –volume OnCommandDB
```

clustered Data ONTAP でのフェールオーバー グループ NAS

NFS ポート フェールオーバー グループを作成します。

```
network interface failover-groups create -failover-group fg-nfs-<<var_nfs_vlan_id>>
-node <<var_node01>> -port a0a-<<var_nfs_vlan_id>>
network interface failover-groups create -failover-group fg-nfs-<<var_nfs_vlan_id>>
-node <<var_node01>> -port a0a-<<var_nfs_vlan_id>>
```

clustered Data ONTAP での NFS LIF

NFS 論理インターフェイス（LIF）を作成します。

```
network interface create -vserver Infra_Vserver -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_node01>> -home-port a0a-<<var_nfs_vlan_id>>
–address 193.191.1.20 -netmask 255.255.255.0 -status-admin up –failover-policy
nextavail –firewall-policy data –auto-revert true –use-failover-group enabled
–failover-group fg-nfs-<<var_nfs_vlan_id>>

network interface create -vserver Infra_Vserver -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_node01>> -home-port a0a-<<var_nfs_vlan_id>>
–address 193.191.1.30 -netmask 255.255.255.0 -status-admin up –failover-policy
nextavail –firewall-policy data –auto-revert true –use-failover-group enabled
–failover-group fg-nfs-<<var_nfs_vlan_id>>
```

clustered Data ONTAP での FCP LIF

各ノードに 2 つずつ、4 つの FCoE LIF を作成します。

```
network interface create -vserver Infra_Vserver -lif fcp_lif01a -role data
-data-protocol fcp -home-node <<var_node01>> -home-port 3a
network interface create -vserver Infra_Vserver -lif fcp_lif01b -role data
-data-protocol fcp -home-node <<var_node02>> -home-port 4a
network interface create -vserver Infra_Vserver -lif fcp_lif02a -role data
-data-protocol fcp -home-node <<var_node01>> -home-port 3a
network interface create -vserver Infra_Vserver -lif fcp_lif02b -role data
-data-protocol fcp -home-node <<var_node02>> -home-port 4a
```

インフラストラクチャ vServer 管理者の追加

以下のコマンドを使用して、アウトオブバンド管理ネットワークにインフラストラクチャ vServer 管理者および vServer 管理論理インターフェイスを追加します。

```
network interface create –vserver Infra_Vserver –lif vsmgmt –role data –data-protocol
none –home-node <<var_node02>> -home-port e0a –address <<var_vserver_mgmt_ip>>
–netmask <<var_vserver_mgmt_mask>> -status-admin up –failover-policy nextavail
–firewall-policy mgmt –auto-revert true –use-failover-group enabled –failover-group
fg-cluster-mgmt

network routing-groups route create –vserver Infra_Vserver –routing-group
d<<var_clustermgmt_ip>> -destination 0.0.0.0/0 –gateway <<var_clustermgmt_gateway>>
security login password –username vsadmin –vserver Infra_Vserver
Please enter a new password:  <<var_vsadmin_password>>
Please enter it again:  <<var_vsadmin_password>>

security login unlock –username vsadmin –vserver Infra_Vserver
```

Cisco UCS 上のクラウド インフラストラクチャ

この項では、Citrix CloudPlatform 4.2.1 を構築するための Cisco UCS コンピュート インフラストラクチャを導入する際の設計上の考慮事項について詳しく説明します。マルチテナント クラウド環境管理では、共有インフラストラクチャ リソースのプロビジョニング、可用性、およびサービス レベルはクラウド プロバイダーの主要業務の一環です。

短い時間間隔でクラウド インフラストラクチャを構築および再構築することは、クラウド環境での主要な課題です。Cisco Unified Computing System（UCS）は、コンピューティング、ネットワーク、ストレージ アクセス、および仮想化を統合して 1 つのシステムにまとめるデータセンター プラットフォームを提供します。Cisco UCS Manager は、MAC アドレス、UUID、WWPN、WWNN、アダプタ ポリシー、ファームウェア、および BIOS 設定などの設定の固定セットを各コンピュート ノードが持たないステートレス コンピューティングを可能にします。すべてが中央で設定され、サービス プロファイルの形式でサーバに適用されます。これは、TCO を削減しビジネスの俊敏性を向上させ、Citrix CloudPlatform 4.2.1 での一貫した設定および再目的化計算の簡素化を可能にします。

この項では、次のクラウド コンポーネントの設計および導入の手順を詳しく説明します。

- クラウド管理設計および導入
- クラウド コンピュートの設計および導入

クラウド管理設計および導入

Cisco UCS では、ポリシー、プール、サービス プロファイル、テンプレート、およびサービス定義の質などの一意のリソースを使用して各クラウド テナントに専用の分離された管理ドメインを提供する論理エンティティに、Cisco UCS ドメインの大規模物理インフラストラクチャを分割する組織単位（OU）を提供します。コンピュート セキュリティ動作フロントでは、アクセス コントロールを提供するために、ロールと特権を使用してユーザを指定する OU ロケールが Cisco UCS Manager によって提供されます。

（注） このマニュアルでは、クラウド操作を実行する管理ロールでクラウド ユーザを指定するためのアクセス ロールを使用して単一組織単位 Tenant A を作成します。

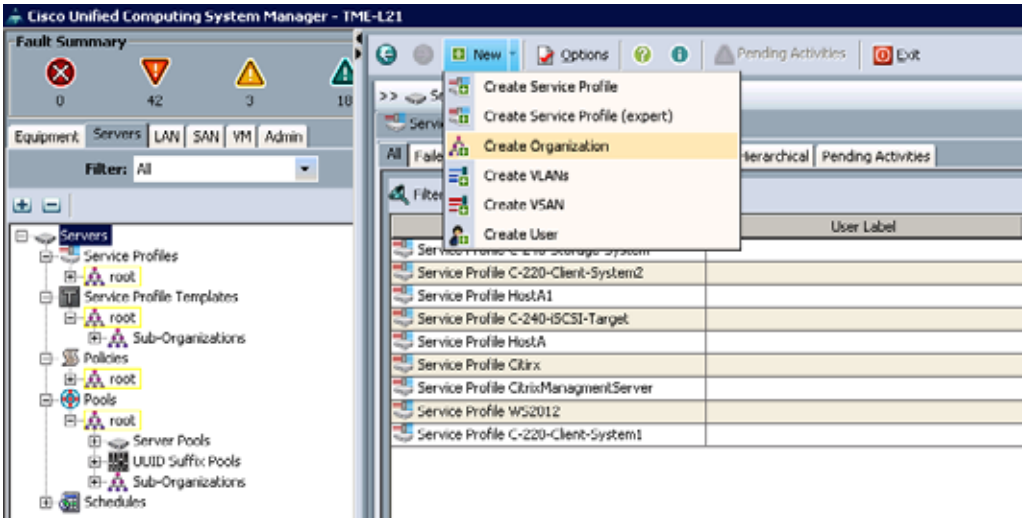
組織の作成

これらの手順は、Cisco UCS 環境での組織の設定の詳細を示します。組織は、プール（MAC、PWWN、管理 IP、およびサーバ）、ポリシー（BIOS、ファームウェア、およびアダプタ）の作成などのいろいろなリソースの組織化とアクセス制御、および IT 組織内のサービス プロファイル テンプレートの定義の手段として使用され、それによってコンピュート リソースのマルチテナント機能を可能にします。これらのリソースを作成するために必要な手順は次のとおりです。

組織を作成するには、Cisco UCS Manager にログインして以下の手順を実行します。

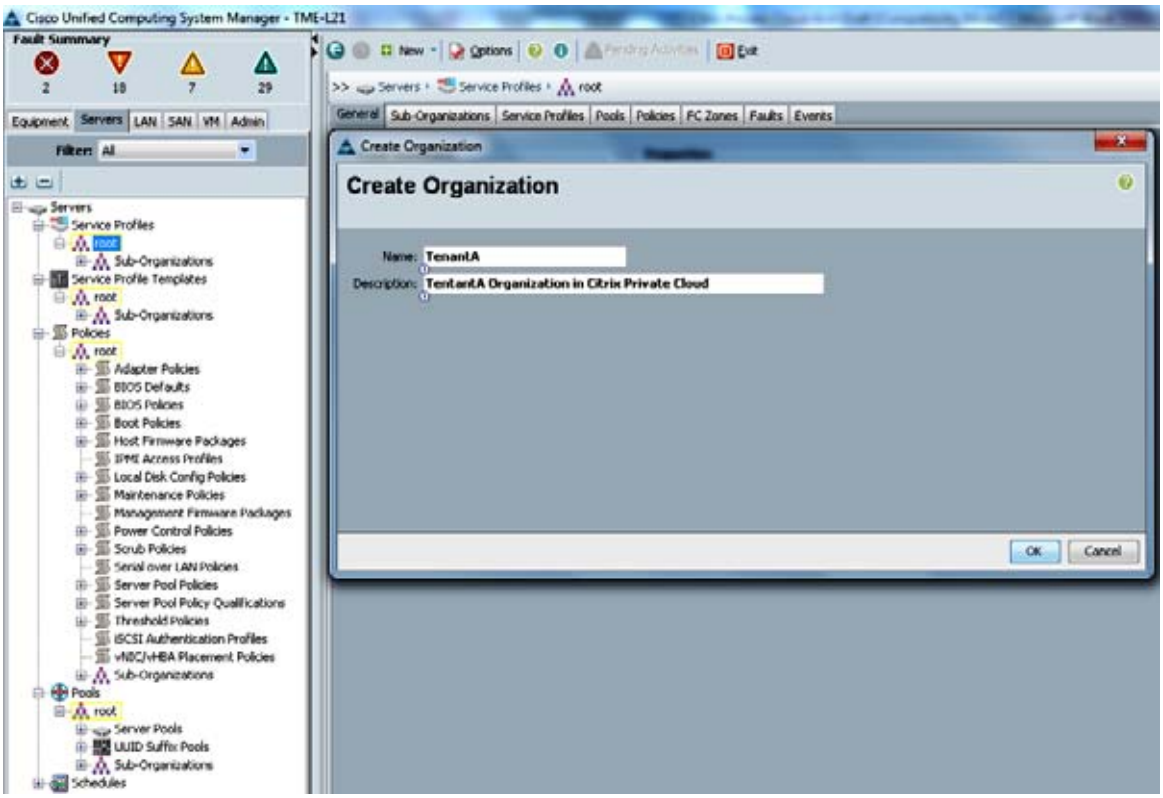
4. Cisco UCS Manager の [Servers] タブ（左ペインで [Servers] ノードが強調表示されている）を表示し、右ペインに表示されている最上部のコントロール バーから [New] > [Create Organization] を選択します。

図 48　　組織の作成と設定



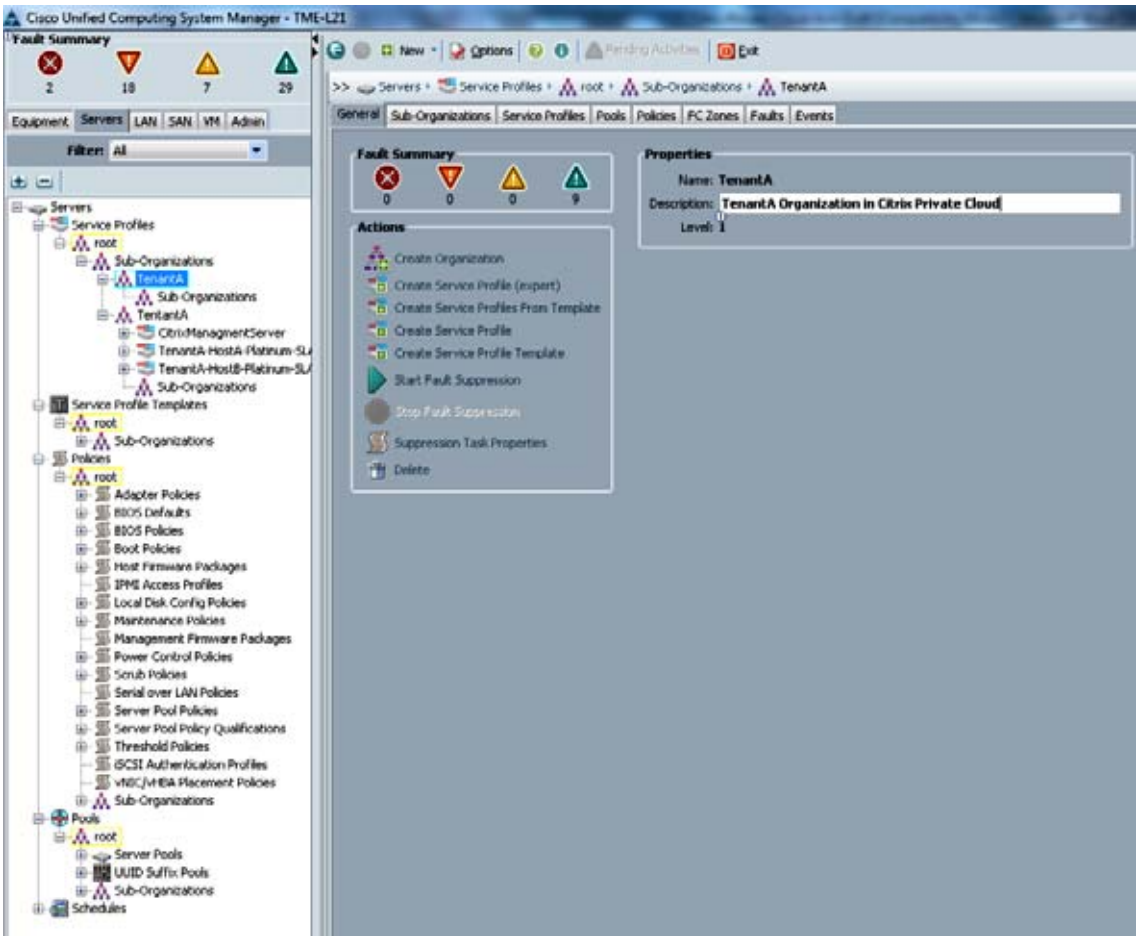
5. [Name] フィールドに組織名を入力します。
6. [Description] フィールドに組織の説明（任意）を入力します。

図 49　　組織への名前と説明の追加



7. [OK] をクリックします。
8. [OK] をクリックします。

図 50　　組織プロパティの確認

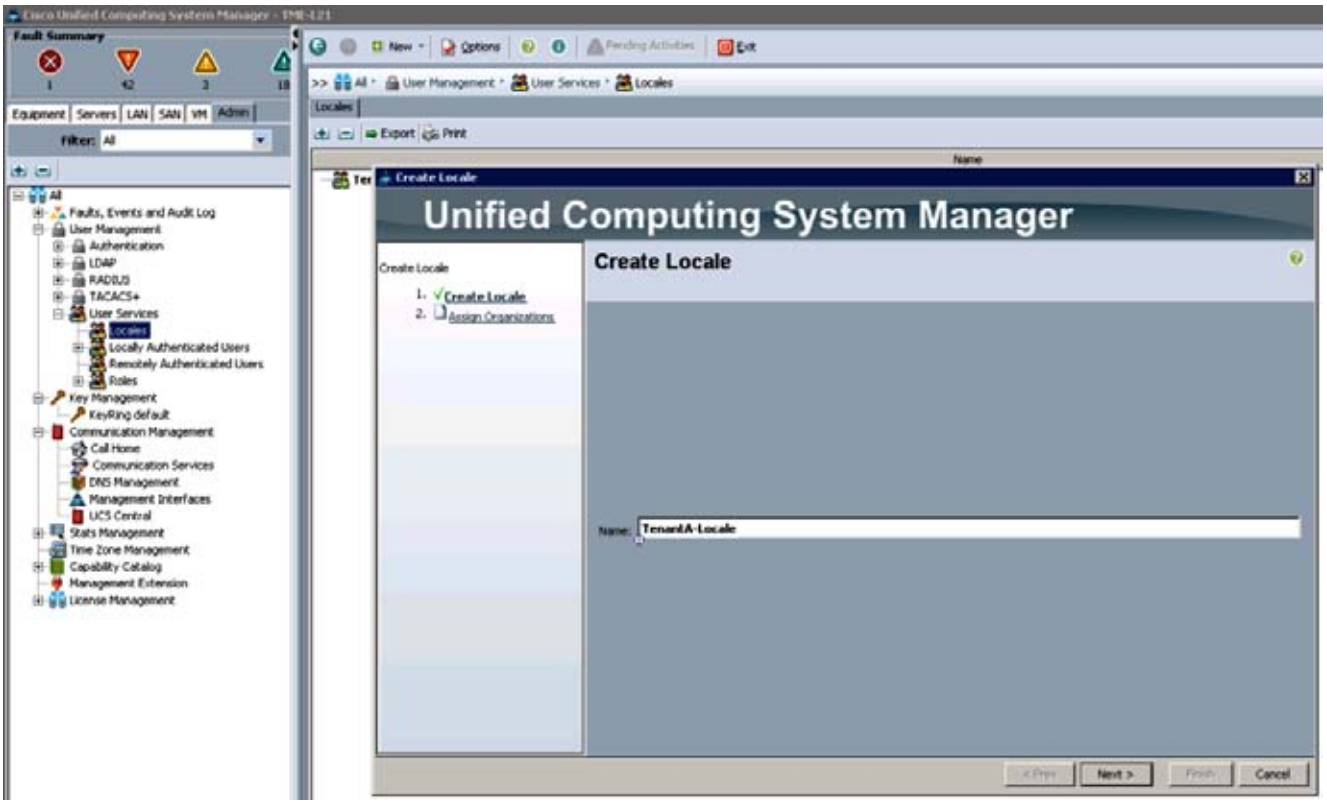


組織のロケールの作成

Cisco UCS Manager でロケールを作成するには、次の手順を実行します。

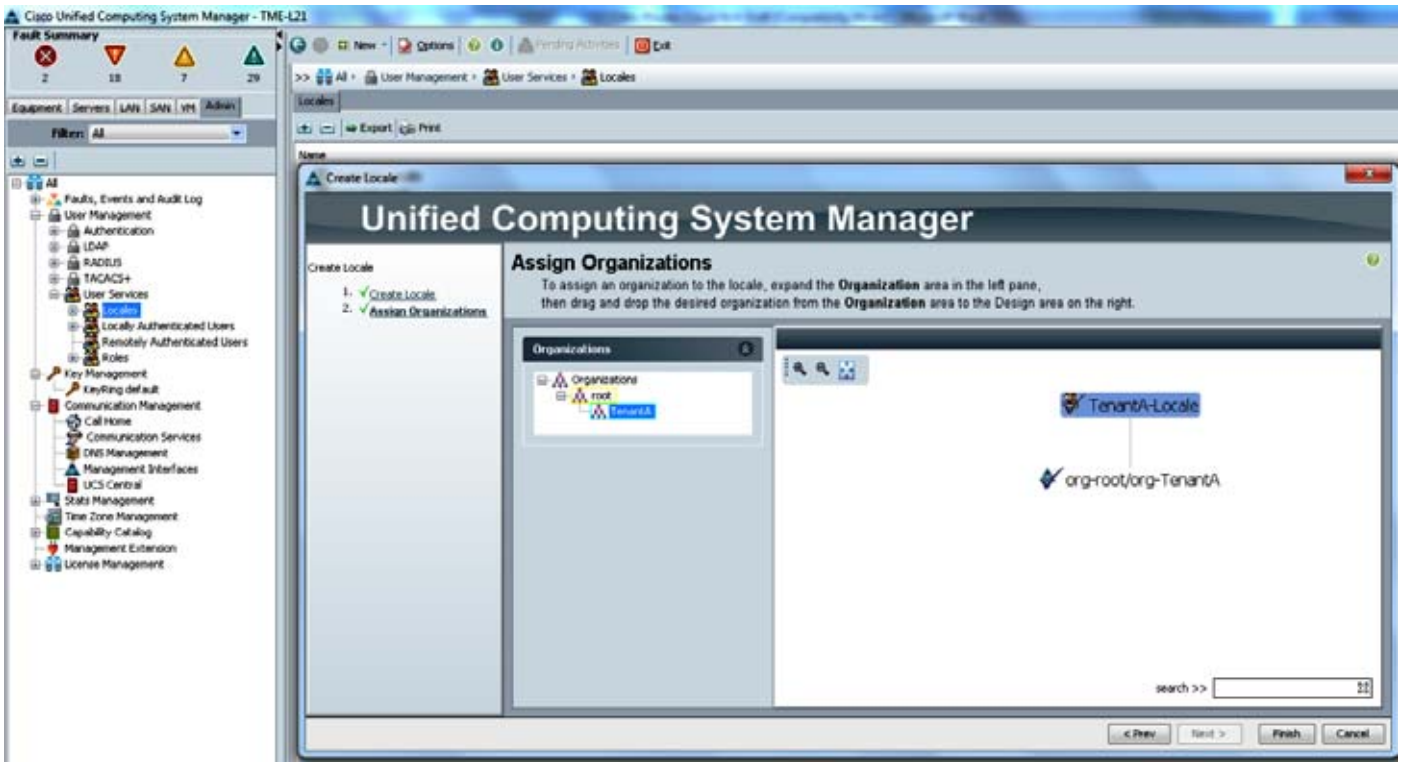
1. 左ペインの [Admin] タブで、[User Management] の下の [User Services] をクリックします。
2. [Locales] を右クリックして [Create Locale] をクリックします。
3. 名前 TenantA-Locale を入力します。

図 51　　ロケールへの名前の追加



4. [Next] をクリックします。
5. [Organizations] を選択し、[root] を展開し、[TenantA] を選択して [Org-root/org-Tenant A] にドラッグします。
6. [Finish] をクリックします。

図 52　　組織のロケールへの割り当て

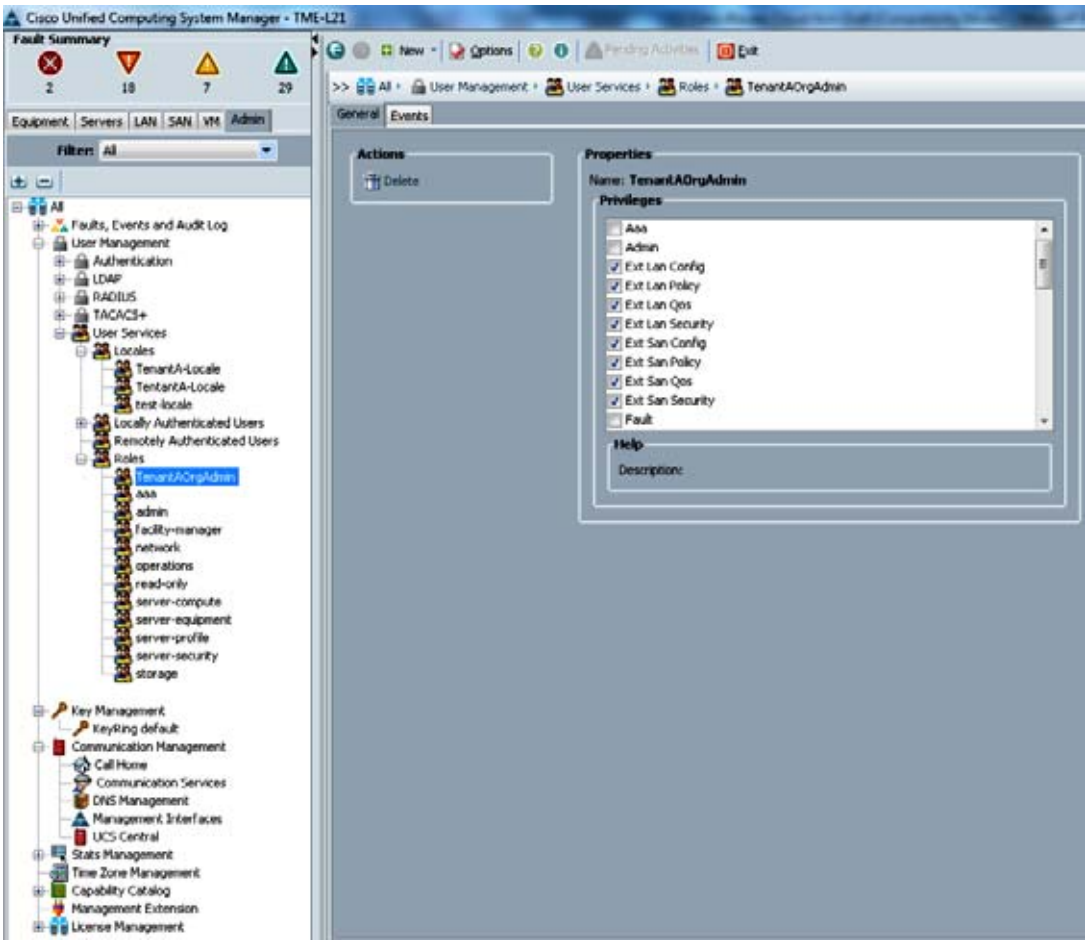


組織のロールの作成

Cisco UCS Manager でユーザ ロールを作成するには、次の手順を実行します。

7. 左ペインの [Admin] タブで [User Roles] をクリックします。
8. [Create Role] を右クリックします。
9. Name TenantAOrgAdmin と入力し、組織 TenantA を管理するために適切な権限を選択します。
10. [Aaa]、[Admin]、[Operations]、および [Fault Privileges] チェックボックスにはチェックを入れないでください。

図 53　　プロパティおよび特権の定義

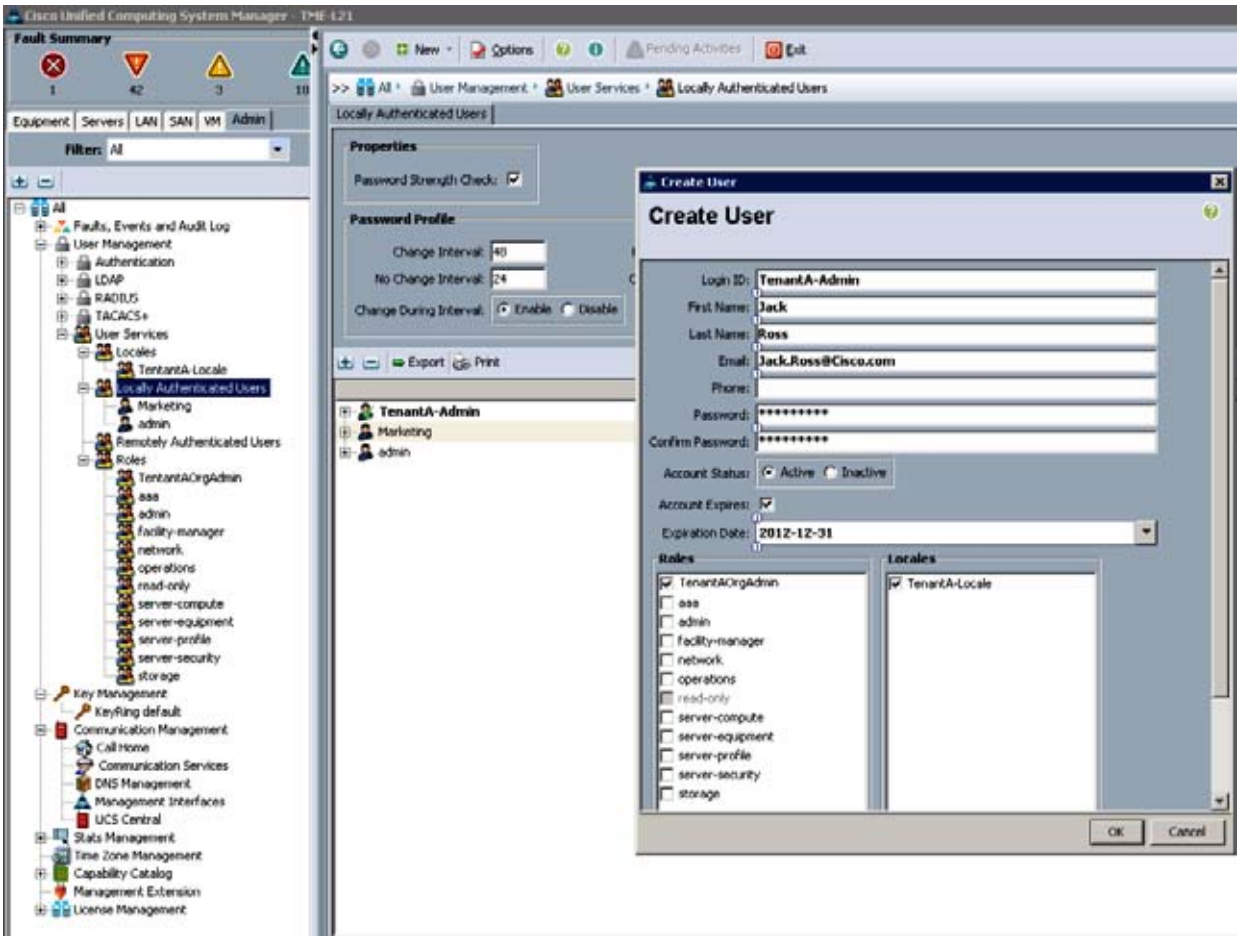


ユーザの作成および組織のロールの割り当て

ユーザを作成し組織にロールを割り当てるには、Cisco UCS Manager にログインして次の手順を実行します。

1. 左ペインの [Admin] タブで [LocallyAuthenticatedUsers] をクリックします。
2. [Create User] をクリックします。
3. [Name] フィールドに Tenant A-Admin と入力します。
4. ロール（TenantAOrgAdmin）とロケール（TenantA-Locale）を選択します。
5. [OK] をクリックします。

図 54　　ユーザ プロファイルのプロパティの定義



クラウド コンピュートの設計および導入

マルチテナント クラウド環境では、操作を簡素化しスケーラビリティを向上させてリスクを軽減するのに役立つデータセンターの自動化を Cisco UCS Manager がサポートします。統合された組み込みポリシーベースの Cisco UCS Manager は、エコシステムと親和性の良いアプローチによって、ほとんどの IT 予算で最大費目に含まれる管理コストの削減に役立ちます。Cisco UCS Manager では、複数のシャーシに格納された最大 160 台のサーバおよび数千の Cisco UCS コンポーネントを管理可能です。

- サーバ、ネットワーク、およびストレージ アクセスを統合する統合組み込み管理インターフェイス
- サービス プロファイル使用し、簡素さを向上しリスクを軽減するポリシーおよびモデルベースの管理方法
- 追加または変更するシステム コンポーネントを検出、インベントリ、管理、およびプロビジョニングする自動検出機能
- 既存のスキルの上に構築され規則に従ったコラボレーションをサポートするロールベース管理方法

Cisco UCS プールは、サーバ UUID、MAC アドレス、WWNN、WWPN などの UCS ブレードの属性に対して事前に決められた範囲を提供します。これらの範囲は、別の属性を使用してグローバル レベルで定義されてサービス プロファイル テンプレートの形式で物理ブレードに適用され、導入時間を短縮しステートレスなクラウド コンピュート環境を実現できます。

仮想ネットワーク インターフェイス カード（vNIC）、MAC アドレス、仮想ホスト バス アダプタ（vHBA）、WWPN アドレス、WWWN アドレス、ブート ポリシー、アダプタ ポリシー、配置ポリシー、ファームウェアのリビジョン、サーバ プール、およびその他のエレメントなどのサーバのプロパティ設定の値がサービス プロファイルに含まれます。これらの設定をブレード サーバからプロファイルに取り込むことによって、サーバを Cisco UCS 内のどのブレード サーバにも導入できます。さらに、このプロファイルはシャーシ内で 1 つのブレードから別のブレードにいつでも移行できます。

サービス レベルおよび管理設定に基づいたコンピュート識別情報を論理的に切り離したマルチテナント環境では、Cisco UCS Manager でサーバの UUID、MAC、WWPN、WWNN、およびサーバの UCS プールの定義ができます。

サービス レベル合意：定義

マルチテナント コンピュート要求に対して Citrix CloudPlatform 4.2.1 環境でコンピュート ベースのサービス レベル合意を提供し、管理設定を切り離すために、次のコンピュート ベース オファリングの SLA が定義されています。これらの SLA は、費用に基づいてコンピュート インフラストラクチャを選ぶためにクラウド テナントに提供されるクラウド ネットワーク オファリングに直接マッピングされます。

- Platinum-Compute

  マルチテナント クラウド コンピュート サービス レベル要件を満たし、高い CPU 能力とメモリ容量を提供するために、サーバの UUID、MAC、WWPN、WWNN、および IP 管理に対応する管理識別情報を使用して UCS Server のプールが定義されています。

- Gold-Compute

  マルチテナント クラウド コンピュート サービス レベル要件を満たし、Platinum-Compute に比べてわずかに低い CPU 能力とメモリ容量を提供するために、サーバの UUID、MAC、WWPN、WWNN、および IP 管理に対応する管理識別情報を使用して UCS Server のプールが定義されています。

- Silver-Compute

  マルチテナント クラウド コンピュート サービス レベル要件を満たし、Gold-Compute に比べてわずかに低い CPU 能力とメモリ容量を提供するために、サーバの UUID、MAC、WWPN、WWNN、および IP 管理に対応する管理識別情報を使用して UCS Server のプールが定義されています。

- Bronze-Compute

  マルチテナント クラウド コンピュート サービス レベル要件を満たし、Silver-Compute に比べてわずかに低い CPU 能力とメモリ容量を提供するために、サーバの UUID、MAC、WWPN、WWNN、および IP 管理に対応する管理識別情報を使用して UCS Server のプールが定義されています。

この項では、上記で定義したさまざまな Compute-SLA に対する異なる UCS プール、ポリシー、LAN ピン グループ、および SAN ピン グループを作成します。これらのプールおよびポリシーは、クラウド TenantA カスタマー用にすでに作成済みの組織単位 TenantA 内の対応する Gold サービス プロファイル テンプレートに適用します。

この項では、前出のサービス レベル定義に従って次の作業を完了するために実行する必要のある手順を説明します。

- UUID サフィクス プールの作成
- MAC アドレス プールの作成
- WWNN プールの作成
- WWPN プールの作成
- IP プールの作成
- サーバ プールの作成
- サーバ プールの資格情報の作成
- サーバ BIOS ポリシーの作成
- ローカル ディスク設定ポリシーの作成
- ブート ポリシーの作成

UUID サフィクス プールの作成

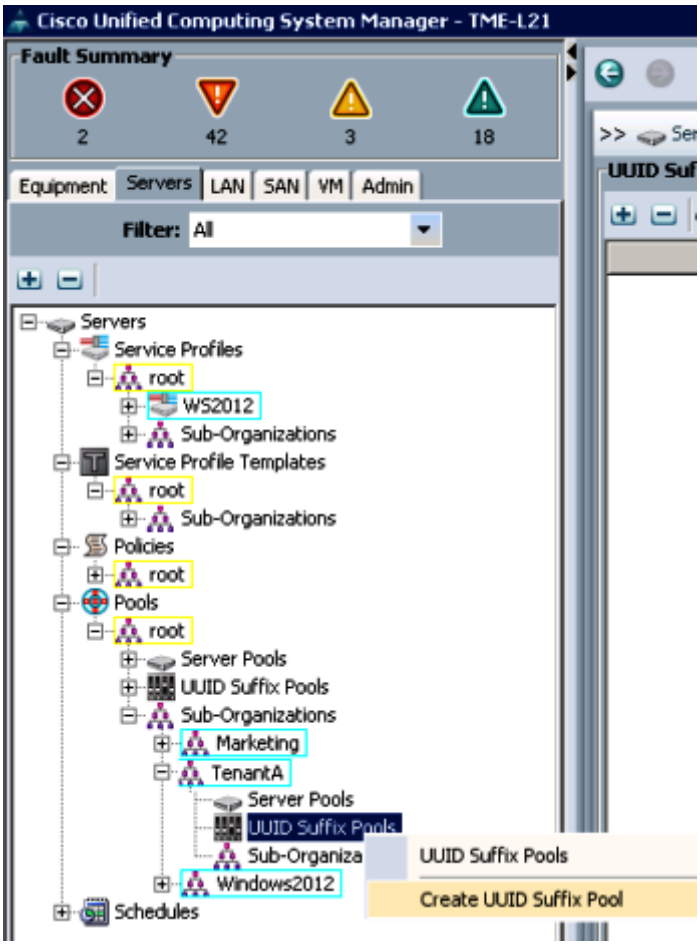
以下の手順で、Platinum サービス クラスに対する Cisco UCS 環境に必要な UUID サフィクス プールの作成および設定の詳細について説明します。

Platinum-Compute-UUID

組織 Tenant A に対して作成済みのユーザ TenantA-Admin を使用して、Cisco UCS Manager にログインします。

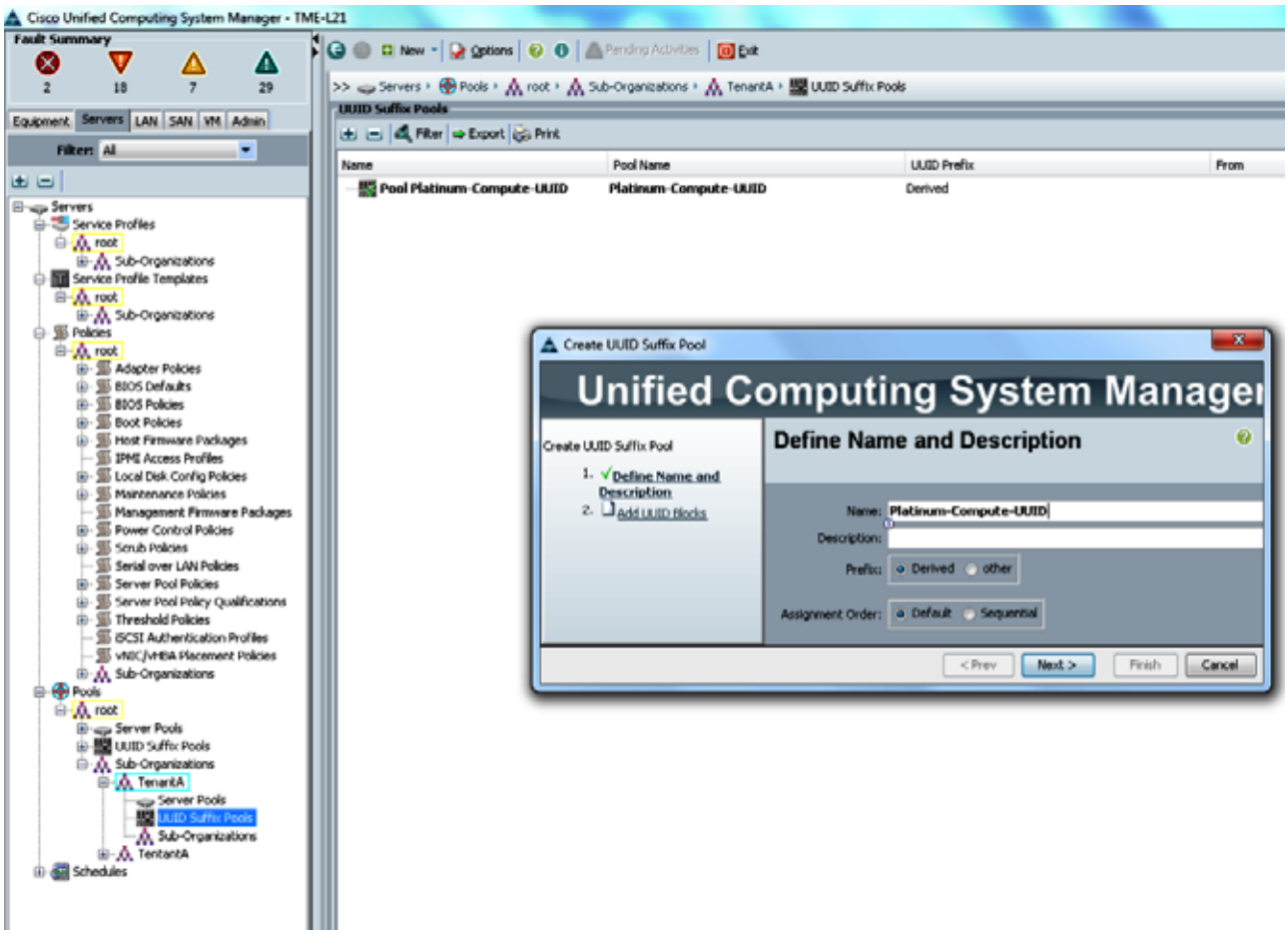
1. 左ペインで、[Servers] タブをクリックします。
2. [Pools] > [Sub-Organizations] を選択します。
3. [Sub-Organizations] を展開します。
4. [UUID Suffix Pools] を右クリックします。
5. [Create UUID Suffix Pool] を選択します。

図 55　　UUID サフィクス プールの作成



6. UUID サフィクス プールに Platinum-Compute-UUID という名前を付けます。
7. （任意）UUID サフィクス プールの説明を入力します。
8. 取得オプションとしてこのサフィクスを残します。
9. [Next] をクリックして続行します。

図 56　　UUID への名前と説明の追加

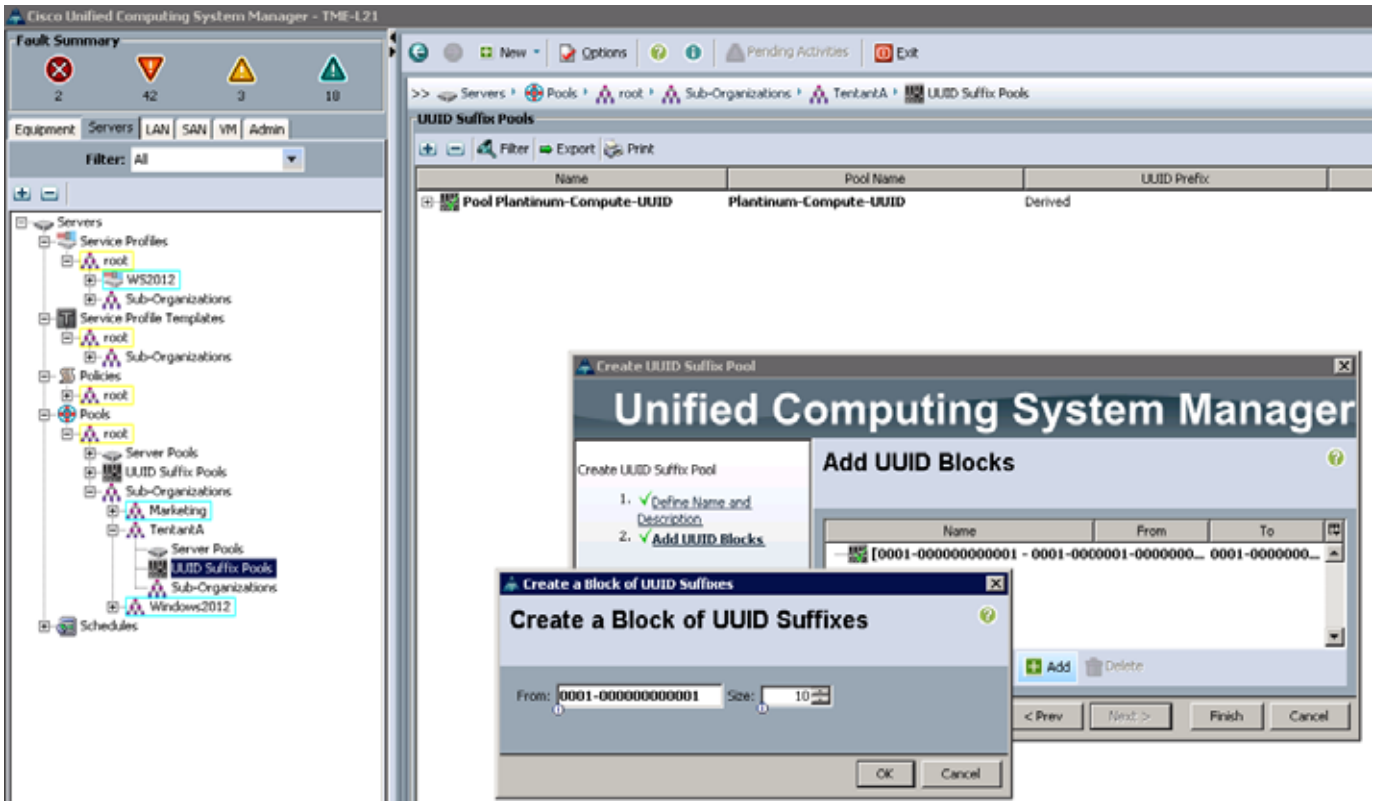


10. [Add] をクリックして UUID のブロックを追加します。
11. [From] フィールド タイプに、UUID サフィクス値 0001-000000000000 を指定します。
12. UUID ブロックのサイズ 10 を指定します。

（注）　十分な数のブレード リソースが使用可能であることを確認します。

13. [OK] をクリックします。
14. [Finish] をクリックします。

図 57　　UUID ブロック サイズの指定

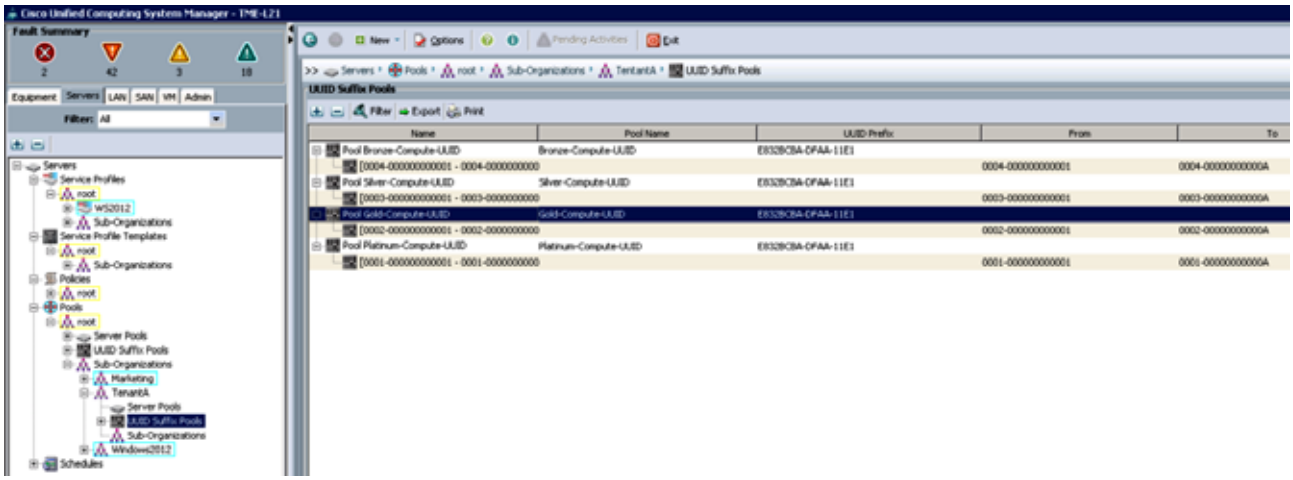


上記で説明した手順に従って、表 10 に記した UUID およびサイズで Gold、Silver、および Bronze サービス クラスの UUID プールを作成します。

表 10　　各サービス クラスの UUID ID およびサイズ

UUID プール名	UUID ID	サイズ
Platinum-Compute-UUID	0001-000000000000	10
Gold-Compute-UUID	0002-000000000000	10
Silver-Compute-UUID	0003-000000000000	10
Bronze-Compute-UUID	0004-000000000000	10

図 58　作成した UUID プールすべてのサマリー



MAC アドレス プールの作成

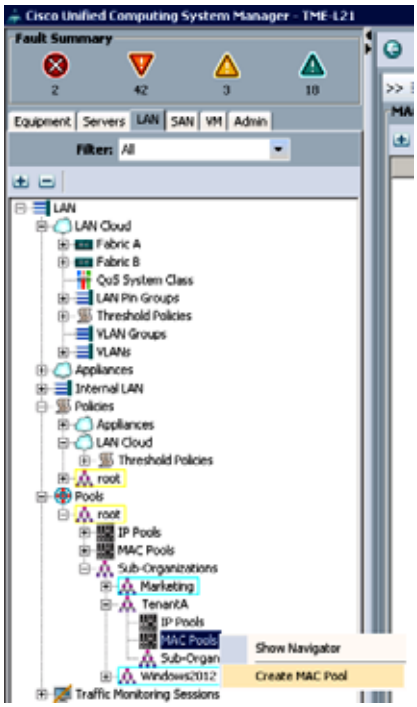
Cisco UCS 環境に必要な MAC アドレス プールを設定するには、以下の手順を実行します。

Platinum-Compute-MAC

組織 Tenant A に対して作成済みのユーザ TenantA-Admin を使用して Cisco UCS Manager にログインします。

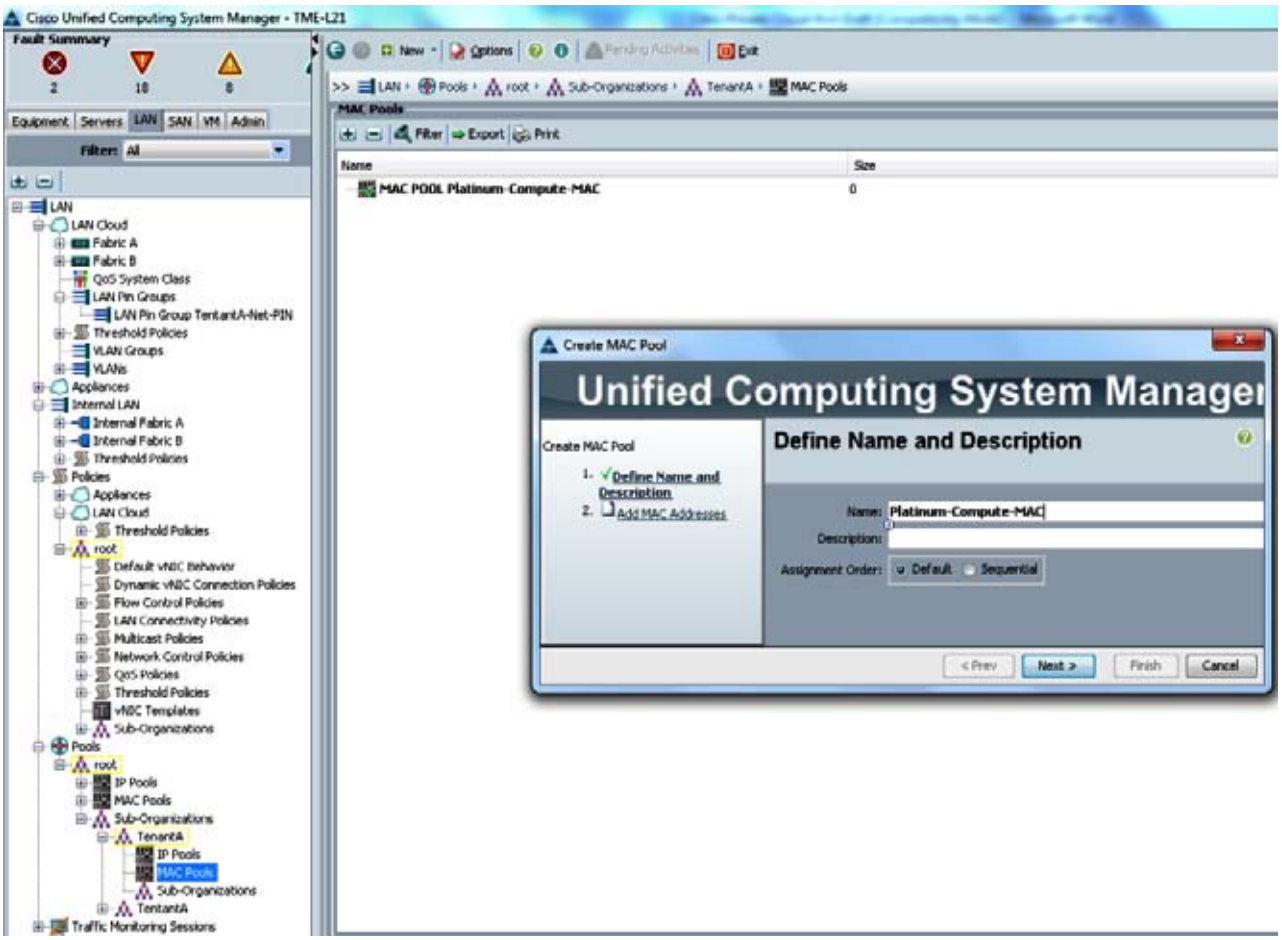
1. 左ペインで、[LAN] タブをクリックします。
2. [Pools] > [Sub-Organizations] を選択します。
3. [Sub-Organizations] を展開し、[TenantA] をクリックします。
4. [root] 組織の下にある [MAC Pools] を右クリックします。
5. [Create MAC Pool] を選択して MAC アドレス プールを作成します。

図 59　　MAC アドレスの MAC プールの作成



6. MAC プールの名前として MAC_Pool と入力します。
7. （任意）MAC プールの説明を入力します。
8. [Next] をクリックします。

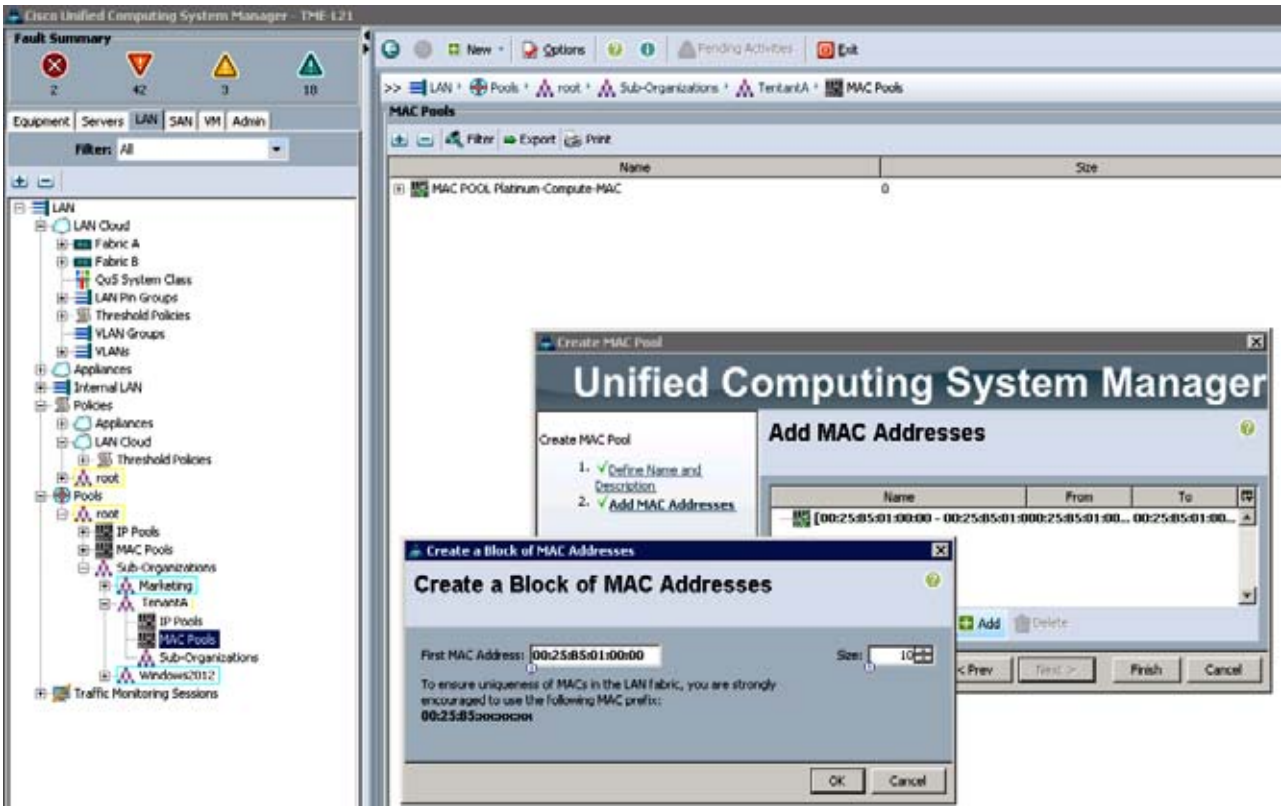
図 60　　MAC プールへの名前と説明の追加



9. [Add] をクリックします。
10. 開始 MAC アドレスを指定します。
11. MAC アドレス プールのサイズに 10 と指定します。

（注）　十分な数のブレード リソースが使用可能であることを確認します。

図 61　　MAC アドレス プールのブロック サイズの設定



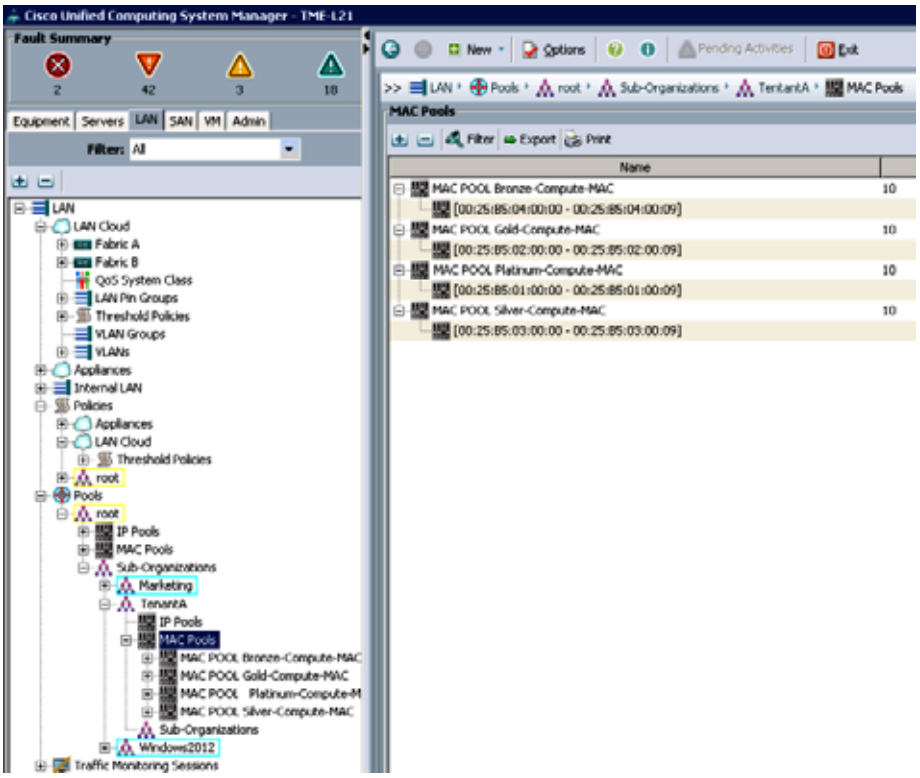
12. [OK] をクリックします。
13. [Finish] をクリックします。
14. 表示されているメッセージ ボックスで、[OK] をクリックします。

上記で説明した手順に従って、表 11 に記した MAC およびサイズで Gold、Silver、および Bronze サービス クラスの MAC プールを作成します。

表 11　　MAC プールのブロック サイズおよび ID

UUID プール名	UUID ID	サイズ
Platinum-Compute-UUID	00:25:B5:01:00:00	10
Gold-Compute-UUID	00:25:B5:01:00:00	10
Silver-Compute-UUID	00:25:B5:02:00:00	10
Bronze-Compute-UUID	00:25:B5:03:00:00	10

図 62　作成した MAC プールすべてのサマリー



WWNN プールの作成

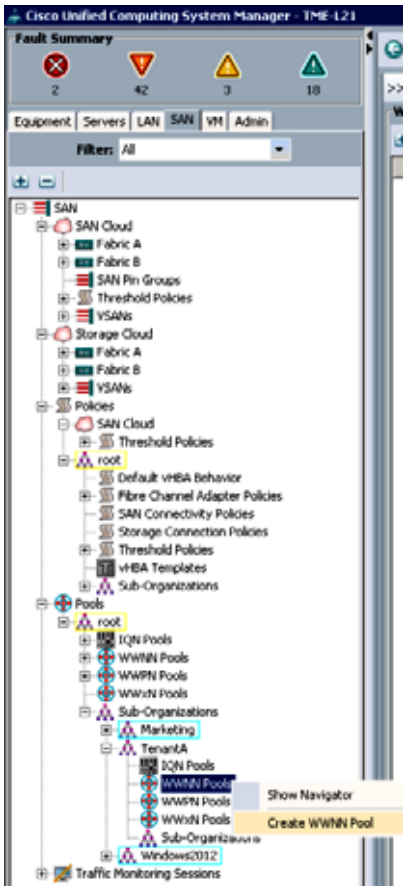
Cisco UCS 環境に必要な WWNN プールを設定するには、以下の手順を実行します。

Platinum-Compute-WWNN

組織 Tenant A に対して作成済みのユーザ TenantA-Admin を使用して Cisco UCS Manager にログインします。

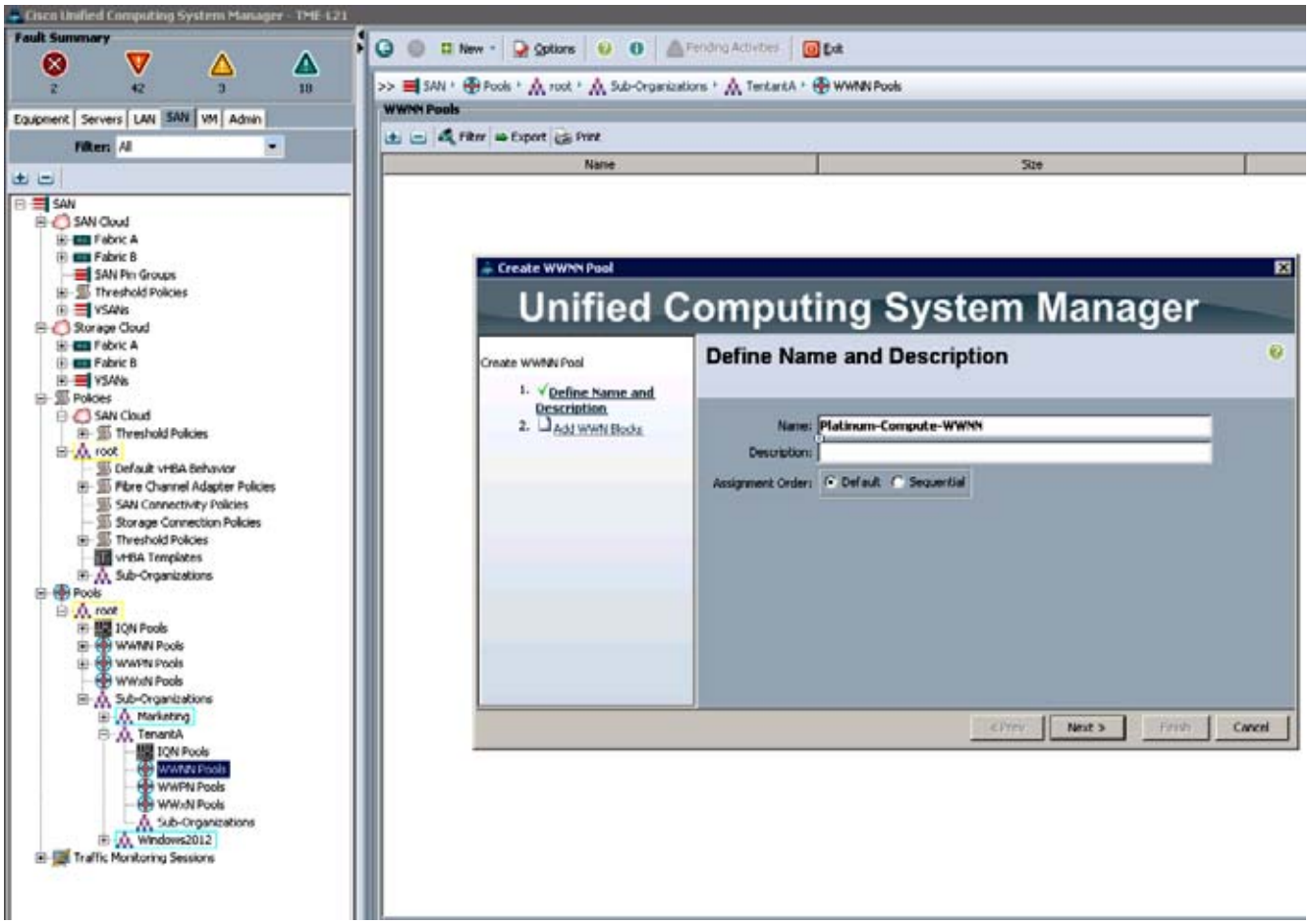
1. 左ペインで、[SAN] タブをクリックします。
2. [Pools] > [Sub-Organizations] を選択します。[TenantA] を展開します。
3. [WWNN Pools] を右クリックします。
4. [Create WWNN Pool] を選択します。

図 63　　WWNN プールの作成



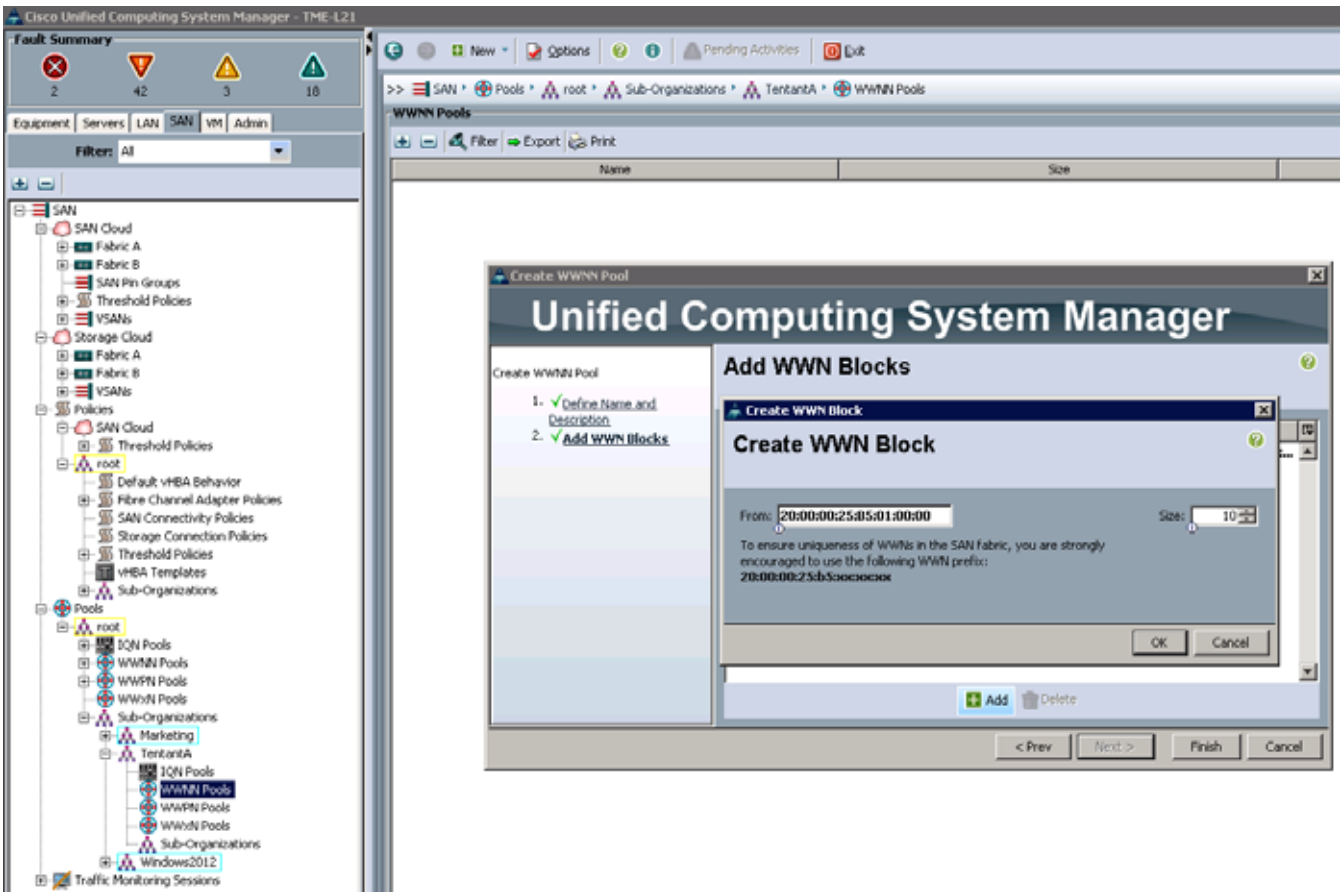
5. WWNN プールの名前として Platinum-Compute-WWNN と入力します。
6. （任意）WWNN プールの説明を追加します。
7. [Next] をクリックして続行します。

図 64　　WWNN プールの名前および説明の定義



8. [Add] をクリックして WWNN のブロック 20:00:00:25:B5:01:00:00 を追加します。
9. WWNN ブロックのサイズに 10 を指定します。十分な数のブレード リソースが使用可能であることを確認します。

図 65　　作成した WWN ブロックのサイズの指定



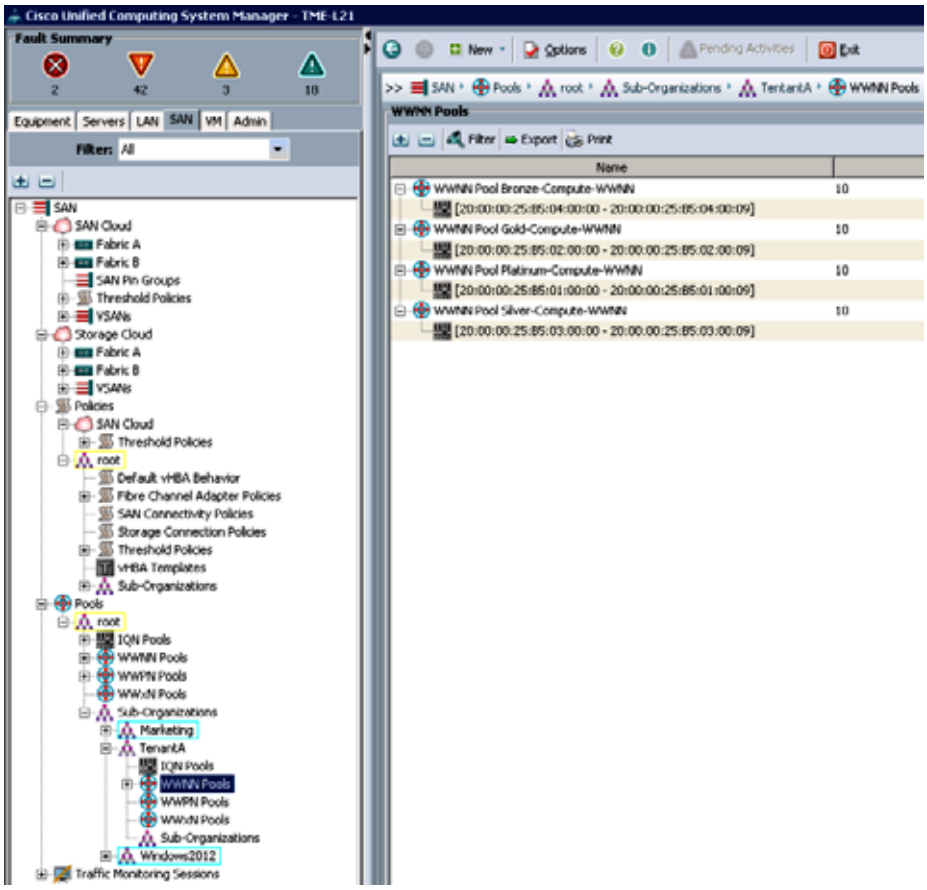
10. [OK] をクリックして続行します。
11. [Finish] をクリックして次に進みます。
12. [OK] をクリックして終了します。

上記と同じ手順に従って、以下の表 12 に記した WWNN およびサイズで Gold-Compute-WWNN、Silver-Compute-WWNN、および Bronze-Compute-WWNN に対する WWNN プールを作成します。

表 12　　すべてのサービス クラスの UUID ID およびサイズ

UUID プール名	UUID ID	サイズ
Platinum-Compute-WWNN	20:00:00:25:B5:01:00:00	10
Gold-Compute-WWNN	20:00:00:25:B5:02:00:00	10
Silver-Compute-WWNN	20:00:00:25:B5:03:00:00	10
Bronze-Compute-WWNN	20:00:00:25:B5:04:00:00	10

図 66　作成した WWNN プールすべてのサマリー



WWPN プールの作成

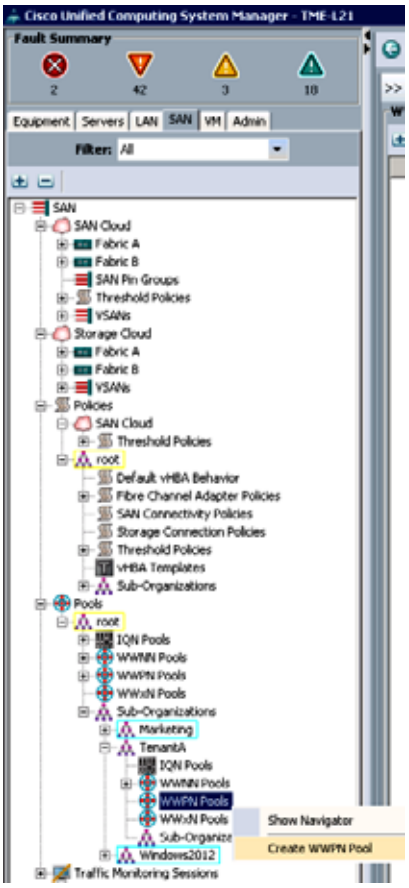
Cisco UCS 環境に必要な WWNN プールを設定するには、以下の手順を実行します。

Platinum-Compute-WWPN

組織 Tenant A に対して作成済みのユーザ TenantA-Admin を使用して Cisco UCS Manager にログインする。

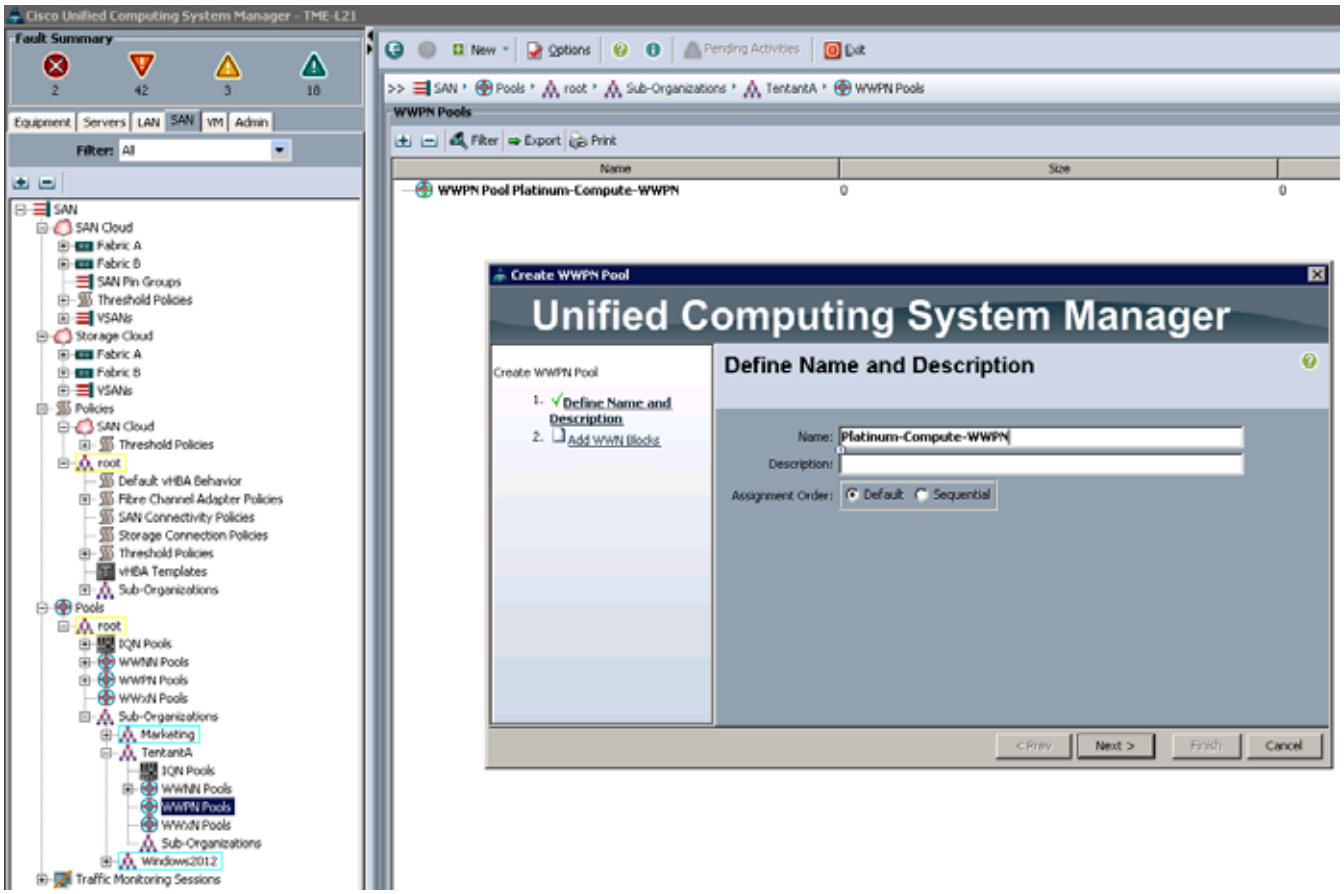
1. 左ペインで、[SAN] タブをクリックします。
2. [Pools] > [Sub-Organizations] を選択します。[TenantA] を展開します。
3. [WWPN Pools] を右クリックします。
4. [Create WWPN Pool] を選択します。

図 67　　[Create WWPN Pool] オプションの選択



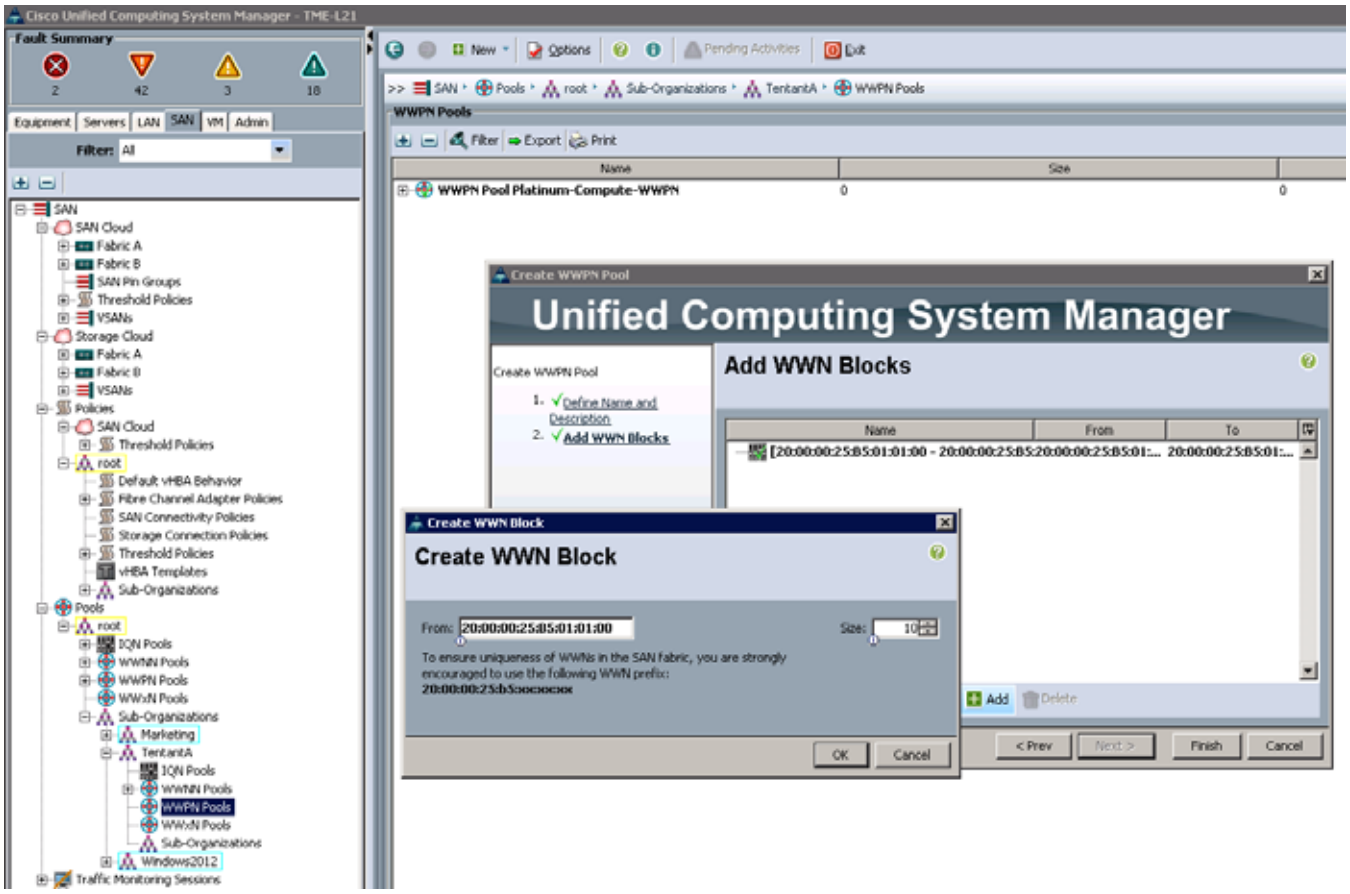
5. WWPN プールの名前として Platinum-Compute-WWPN と入力します。
6. （任意）WWPN プールの説明を追加します。
7. [Next] をクリックして続行します。

図 68　　WWPNN プールの名前および説明の追加



8. [Add] をクリックして WWNN のブロック 20:00:25:B5:01:01:00 を追加します。
9. WWNN ブロックのサイズに 10 を指定します（十分な数のブレード リソースが使用可能か確認します）。

図 69　　WWN ブロックのサイズの定義



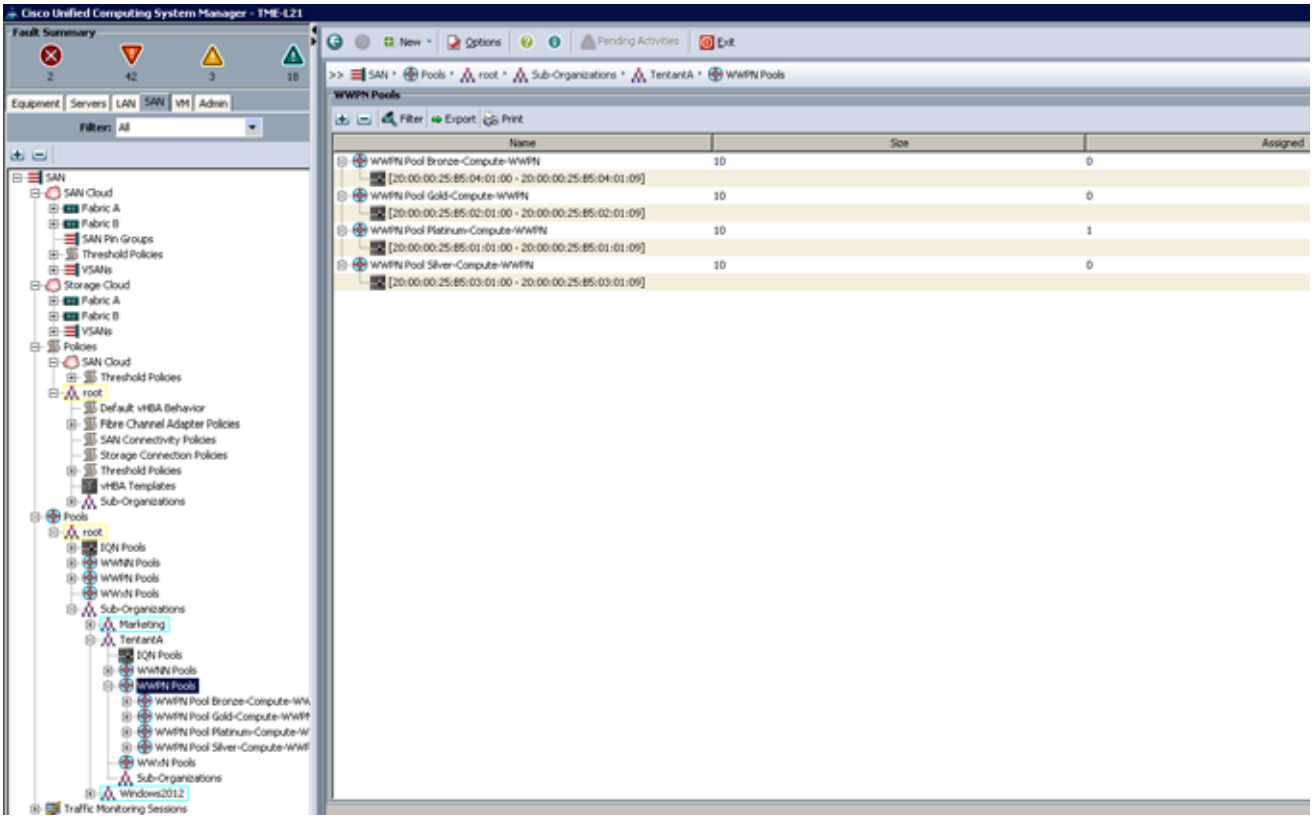
10. [OK] をクリックして続行します。
11. [Finish] をクリックして次に進みます。
12. [OK] をクリックして終了します。

上記と同じ手順に従って、以下の表 13 に記した WWPN およびサイズで Gold-Compute-WWPN、Silver-Compute-WWPN、および Bronze-Compute-WWPN に対する WWNN プールを作成します。

表 13　　WWPN UUID プール名および ID

UUID プール名	UUID ID	サイズ
Gold-Compute-WWPN	20:00:00:25:B5:02:01:00	10
Silver-Compute-WWPN	20:00:00:25:B5:03:01:00	10
Bronze-Compute-WWPN	20:00:00:25:B5:04:01:00	10

図 70　　4 つすべてのコンピュート UUID プールのサマリー



IP プールの作成

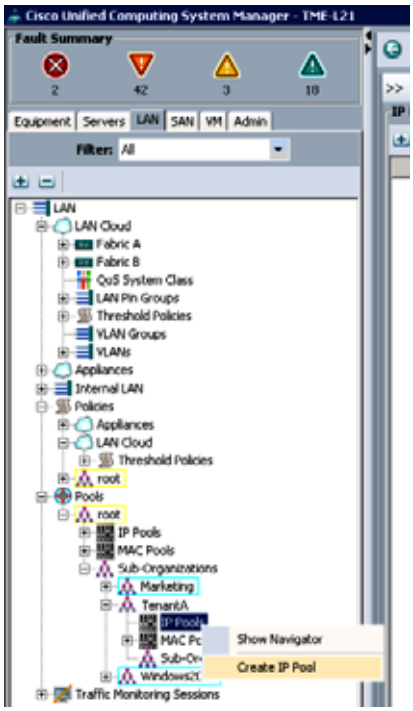
Cisco UCS 環境に必要な IP 管理プールを設定するには、以下の手順を実行します。

Platinum-Compute-IP

組織 Tenant A に対して作成済みのユーザ TenantA-Admin を使用して Cisco UCS Manager にログインします。

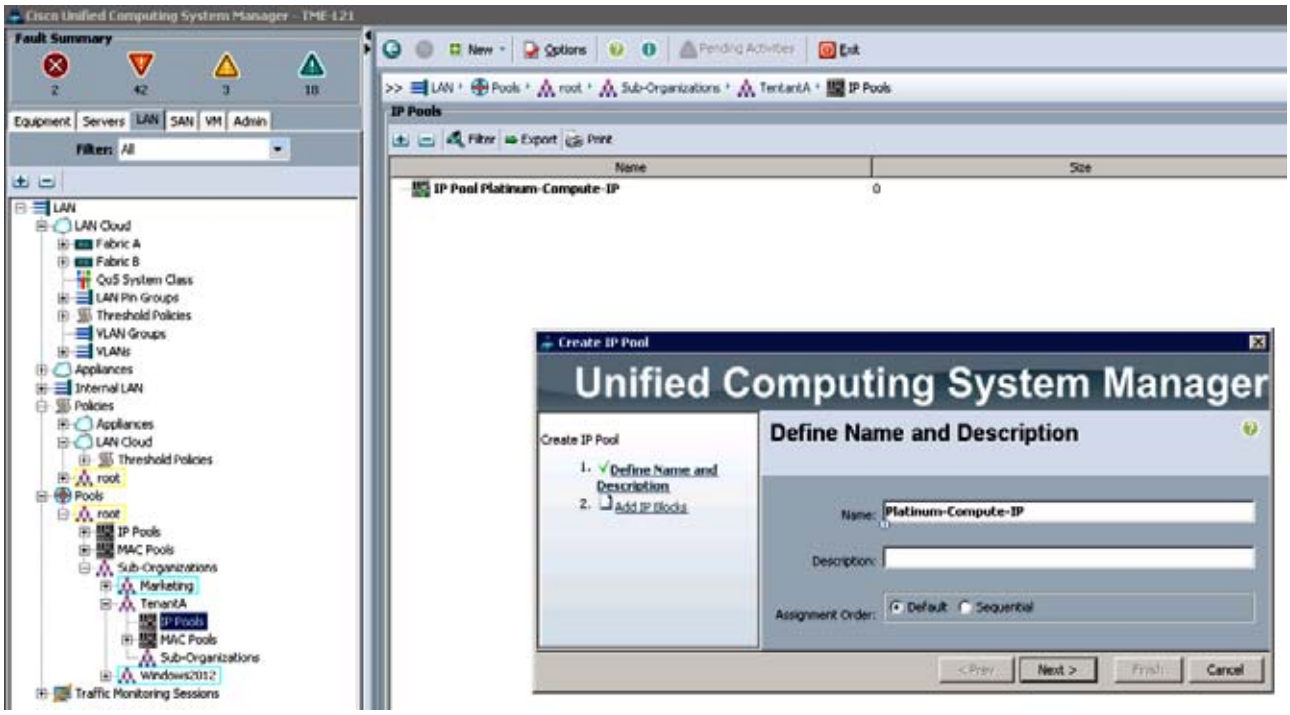
1. 左ペインで、[LAN] タブをクリックします。
2. [Pools] > [Sub-Organizations] を選択します。
3. [TenantA] を展開します。
4. [IP Pools] を右クリックします。
5. [Create IP Pool] を選択します。

図 71　　ストレージの IP プールの作成



6. IP プールの名前として Platinum-Compute-IP と入力します。
7. （任意）IP プールの説明を追加します。
8. [Next] をクリックして続行します。

図 72　　IP プールに対する名前および説明の定義



9. [Add] をクリックして、IP 10.65.121.50 のブロックを追加します。
10. IP ブロックのサイズに 10 を指定します。

（注）　十分な数のブレード リソースが使用可能であることを確認します。

IP アドレスおよびブロック サイズおよび DNS の指定

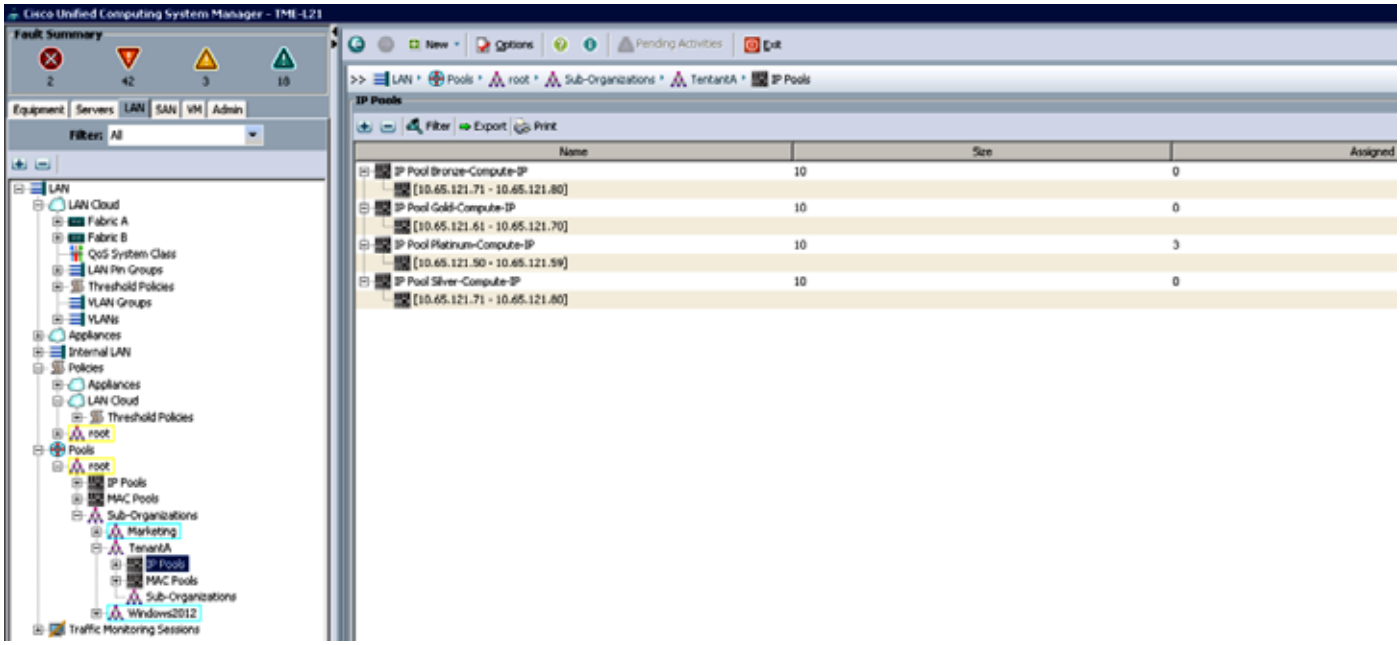
11. [OK] をクリックして続行します。
12. [Finish] をクリックして次に進みます。
13. [OK] をクリックして終了します。

上記で説明した手順に従って、表 14 に記した WWPN およびサイズで Gold-Compute-IP、Silver-Compute-IP、および Bronze-Compute-IP に対する IP プールを作成します。

表 14　　すべての UUID プールに対する WWPN およびサイズ

UUID プール名	UUID ID	サイズ
Platinum-Compute-WWPN	10.65.121.50	10
Gold-Compute-WWPN	10.65.121.61	10
Silver-Compute-WWPN	10.65.121.71	10
Bronze-Compute-WWPN	10.65.121.81	10

図 73　　作成した IP プールすべてのサマリー



vNIC テンプレートおよび vHBA テンプレート

シスコの Cisco UCS Manager では、再利用を容易にし導入を迅速にするために主要オブジェクト（vNIC および vHBA）のテンプレートを提供します。vNIC および vHBA リソースは、1 つが各サイドにバインドされている特定の FI（A サイドまたは B サイドのファブリック インターコネクト）に常に関連付けられています。vNIC（または vHBA）テンプレートは、両方の MAC アドレス プール（または WWPN プール）関連付けをカプセル化するために使用できます。

ここでは、2 セットの vNIC テンプレートと vHBA テンプレートを Baremetal および仮想ホスト サービス プロファイル テンプレート用に作成します。

（注）　管理、アプリケーション、NFS、および vMotion LAN トラフィックを取り扱うために 6 つの vNIC テンプレートを作成し、TenantA Zone での仮想マシン実行用 VMWare ESXi 5.1 ハイパーバイザ ホストを実行するための SAN トラフィックを取り扱うために 2 つの vHBA テンプレートを作成します。

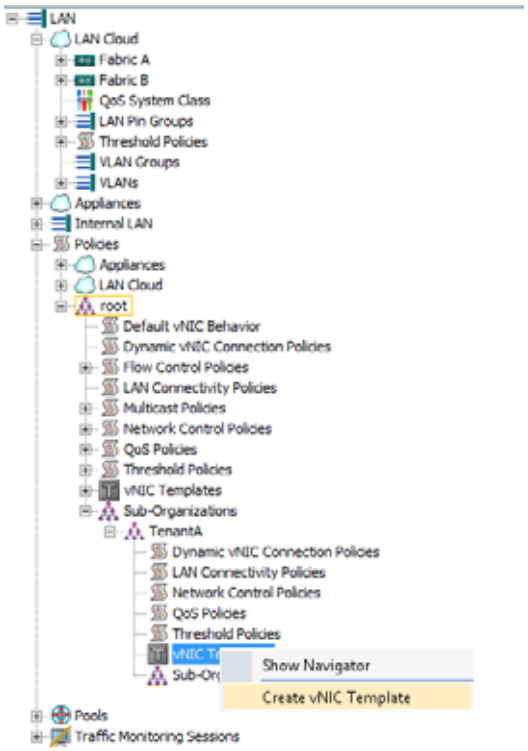
vNICS テンプレートの作成

この項では、ファブリック A およびファブリック B に BareMetal および VMware ESXi ホスト用に作成される vNIC テンプレート作成の詳細を説明します。

組織 Tenant A に対して作成済みのユーザ TenantA-Admin を使用して Cisco UCS Manager にログインします。

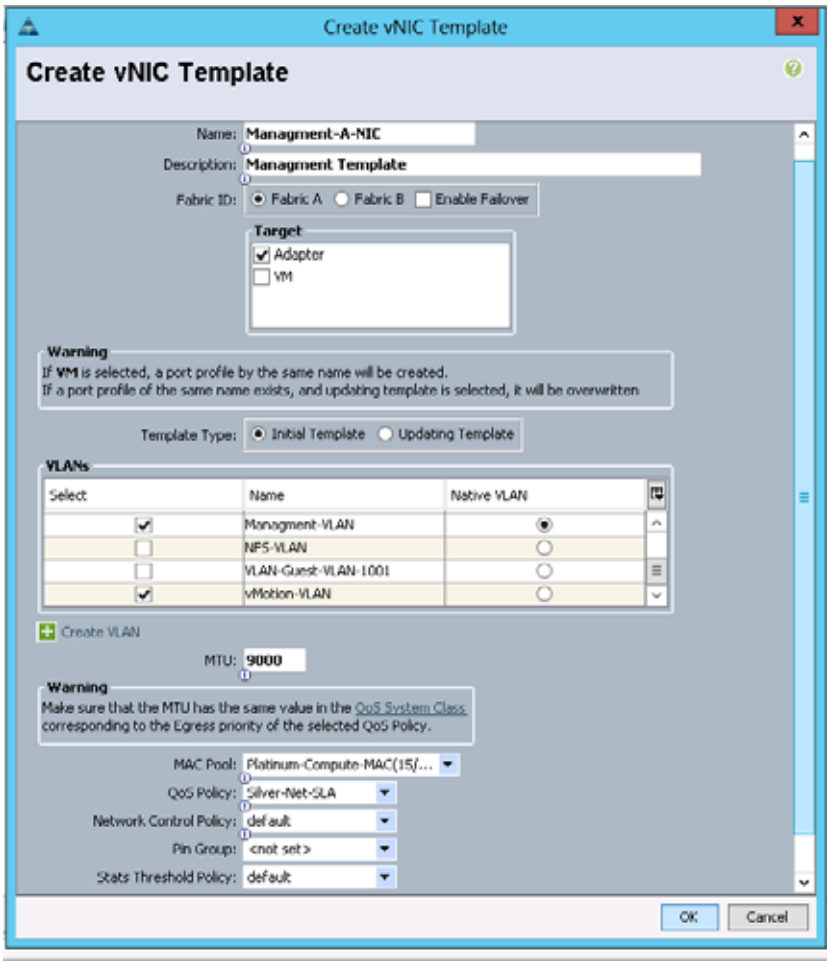
1. 左ペインで、[LAN] タブをクリックします。
2. [Pools] > [Sub-Organizations] を選択します。
3. [TenantA] を展開します。
4. [vNIC Templates] を選択し、[Create vNIC Template] を右クリックします。

図 74　vNIC テンプレートの作成



5. [Create vNIC Template] ウィンドウが開きます。
6. [Name] フィールドに Management-A-NIC と入力します。
7. [Description] フィールドに Management Template と入力します。
8. [Fabric ID] で [FabricA] オプション ボタンをクリックし、[Enable Failover] チェックボックスにチェックは入れません。
9. [Target] で [Adapater] チェックボックスにチェックを入れます。
10. [Template Type] で [Initial Template] オプション ボタンを選択します。
11. [VLANs] で、[Management-VLAN]、[vMotion-VLAN] チェックボックスにチェックを入れ、[Management-VLAN] として [Native VLAN] を選択します。
12. [MTU] フィールドに 9000 と入力します。
13. [MAC Address Assignment] リスト ボックスから [Platinum-Compute-MAC] プールを選択します。
14. [QoS Policy] リスト ボックスの [Silver-Net-SLA] を選択します。
15. [Network Control Policy] リスト ボックスの [default] を選択します。
16. [Pin Group] リスト ボックスの [<not set>] を選択します。
17. [Stats Thershold Policy] リスト ボックスの [default] を選択します。
18. [Dynamic vNIC Connection Policy] リスト ボックスの [<not set>] を選択します。
19. [OK] をクリックします。

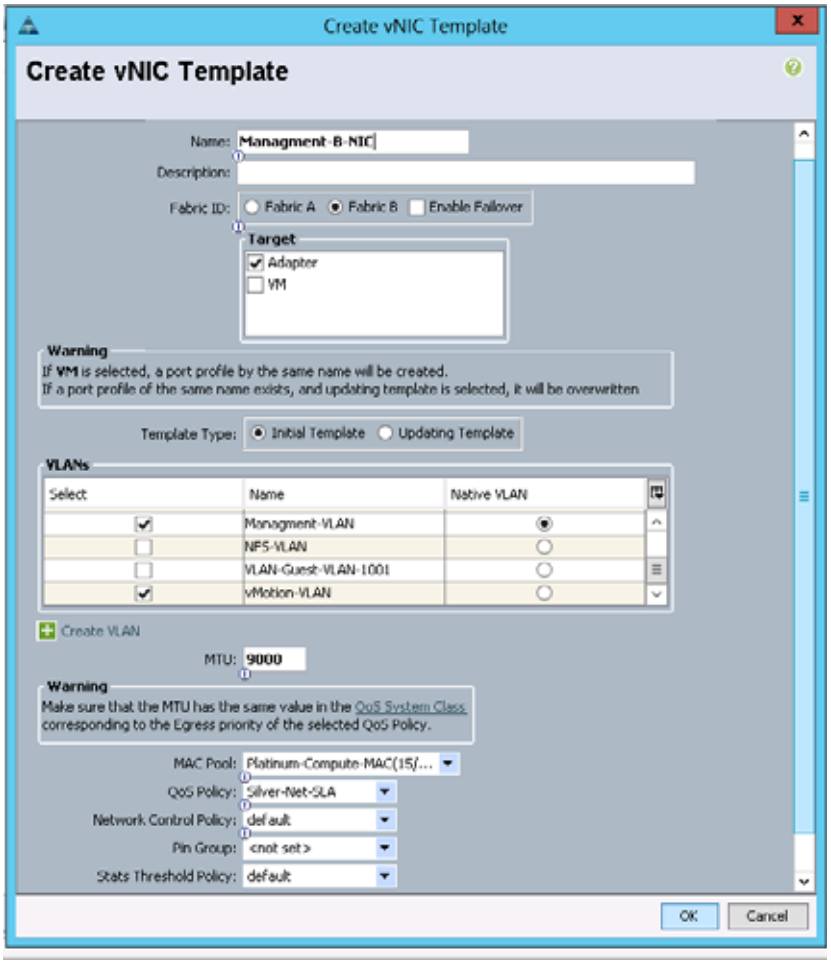
図 75　　管理 A-NIC 用の vNIC プロパティの定義



20. [Create vNIC Template] ウィンドウが開きます。
21. [Name] フィールドに Management-B-NIC と入力します。
22. [Description] フィールドに Management Template と入力します。
23. [Fabric ID] で [FabricB] オプション ボタンをクリックし、[Enable Failover] チェックボックスにチェックは入れません。
24. [Target] で [Adapater] チェックボックスにチェックを入れます。
25. [Template Type] で [Initial Template] オプション ボタンを選択します。
26. [VLANs] で、[Management-VLAN]、[vMotion-VLAN] チェックボックスにチェックを入れ、[Management-VLAN] として [Native VLAN] を選択します。
27. [MTU] フィールドに 9000 と入力します。
28. [MAC Address Assignment] リスト ボックスから [Platinum-Compute-MAC] プールを選択します。
29. [QoS Policy] リスト ボックスの [Silver-Net-SLA] を選択します。
30. [Network Control Policy] リスト ボックスの [default] を選択します。
31. [Pin Group] リスト ボックスの [<not set>] を選択します。
32. [Stats Thershold Policy] リスト ボックスの [default] を選択します。

33. [Dynamic vNIC Connection Policy] リスト ボックスの [<not set>] を選択します。
34. [OK] をクリックします。

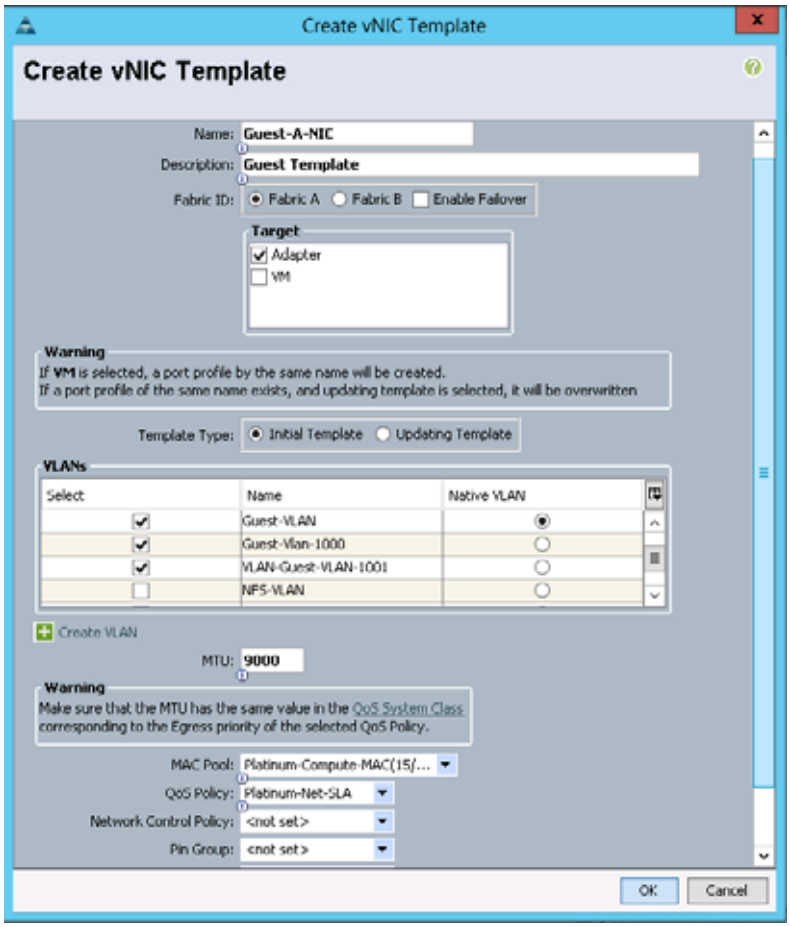
図 76　　管理 B-NIC 用の vNIC プロパティの定義



35. [Create vNIC Template] ウィンドウが開きます。
36. [Name] フィールドに Guest-A-NIC と入力します。
37. [Description] フィールドに Guest Template と入力します。
38. [Fabric ID] で [FabricA] オプション ボタンをクリックし、[Enable Failover] チェックボックスにチェックは入れません。
39. [Target] で [Adapater] チェックボックスにチェックを入れます。
40. [Template Type] で [Initial Template] オプション ボタンを選択します。
41. [VLANs] で、[Guest-VLAN]、[Guest-VLAN-1000]、[VLAN-Guest-VLAN-1001] にチェックを入れ、[Guest-VLAN] として [Native VLAN] を選択します。
42. [MTU] フィールドに 9000 と入力します。
43. [MAC Address Assignment] リスト ボックスから [Platinum-Compute-MAC] プールを選択します。
44. [QoS Policy] リスト ボックスの [Platinum-Net-SLA] を選択します。
45. [Network Control Policy] リスト ボックスの [default] を選択します。

46. [Pin Group] リスト ボックスの [<not set>] を選択します。
47. [Stats Thershold Policy] リスト ボックスの [default] を選択します。
48. [Dynamic vNIC Connection Policy] リスト ボックスの [<not set>] を選択します。
49. [OK] をクリックします。

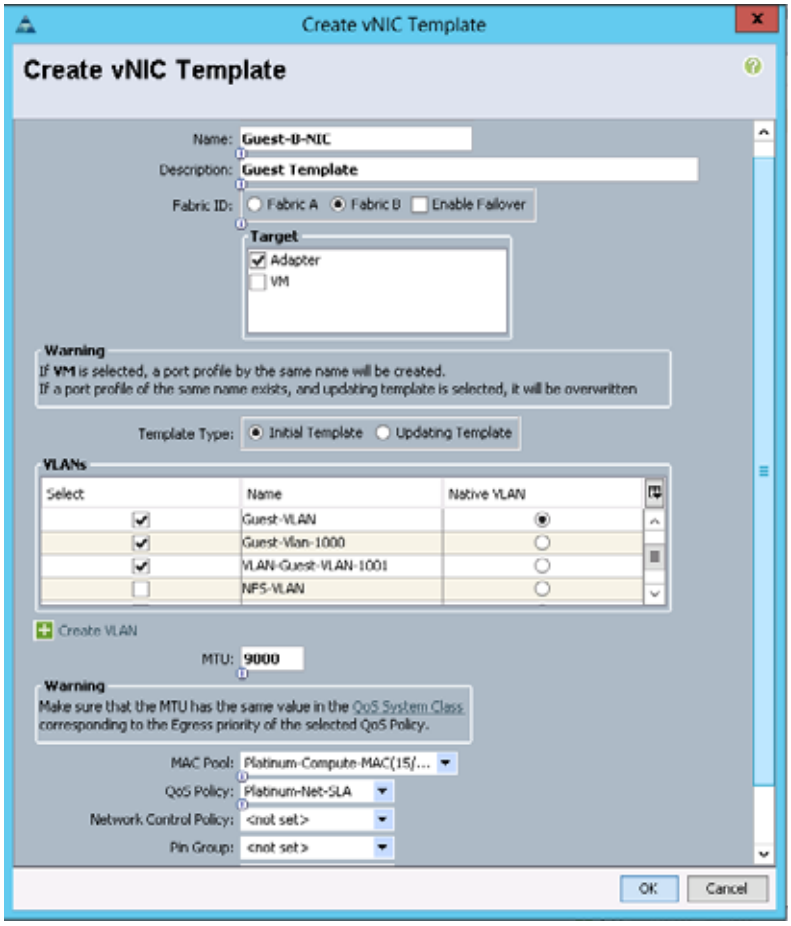
図 77　　Guest-A-NIC 用の vNIC プロパティの定義



50. [Create vNIC Template] ウィンドウが開きます。
51. [Name] フィールドに Guest-B-NIC と入力します。
52. [Description] フィールドに Guest Template と入力します。
53. [Fabric ID] で [FabricA] オプション ボタンをクリックし、[Enable Failover] チェックボックスにチェックは入れません。
54. [Target] で [Adapater] チェックボックスにチェックを入れます。
55. [Template Type] で [Initial Template] オプション ボタンを選択します。
56. [VLANs] で、[Guest-VLAN]、[Guest-VLAN-1000]、[VLAN-Guest-VLAN-1001] にチェックを入れ、[Guest-VLAN] として [Native VLAN] を選択します。
57. [MTU] フィールドに 9000 と入力します。
58. [MAC Address Assignment] リスト ボックスから [Platinum-Compute-MAC] プールを選択します。

59. [QoS Policy] リスト ボックスの [Platinum-Net-SLA] を選択します。
60. [Network Control Policy] リスト ボックスの [default] を選択します。
61. [Pin Group] リスト ボックスの [<not set>] を選択します。
62. [Stats Thershold Policy] リスト ボックスの [default] を選択します。
63. [Dynamic vNIC Connection Policy] リスト ボックスの [<not set>] を選択します。
64. [OK] をクリックします。

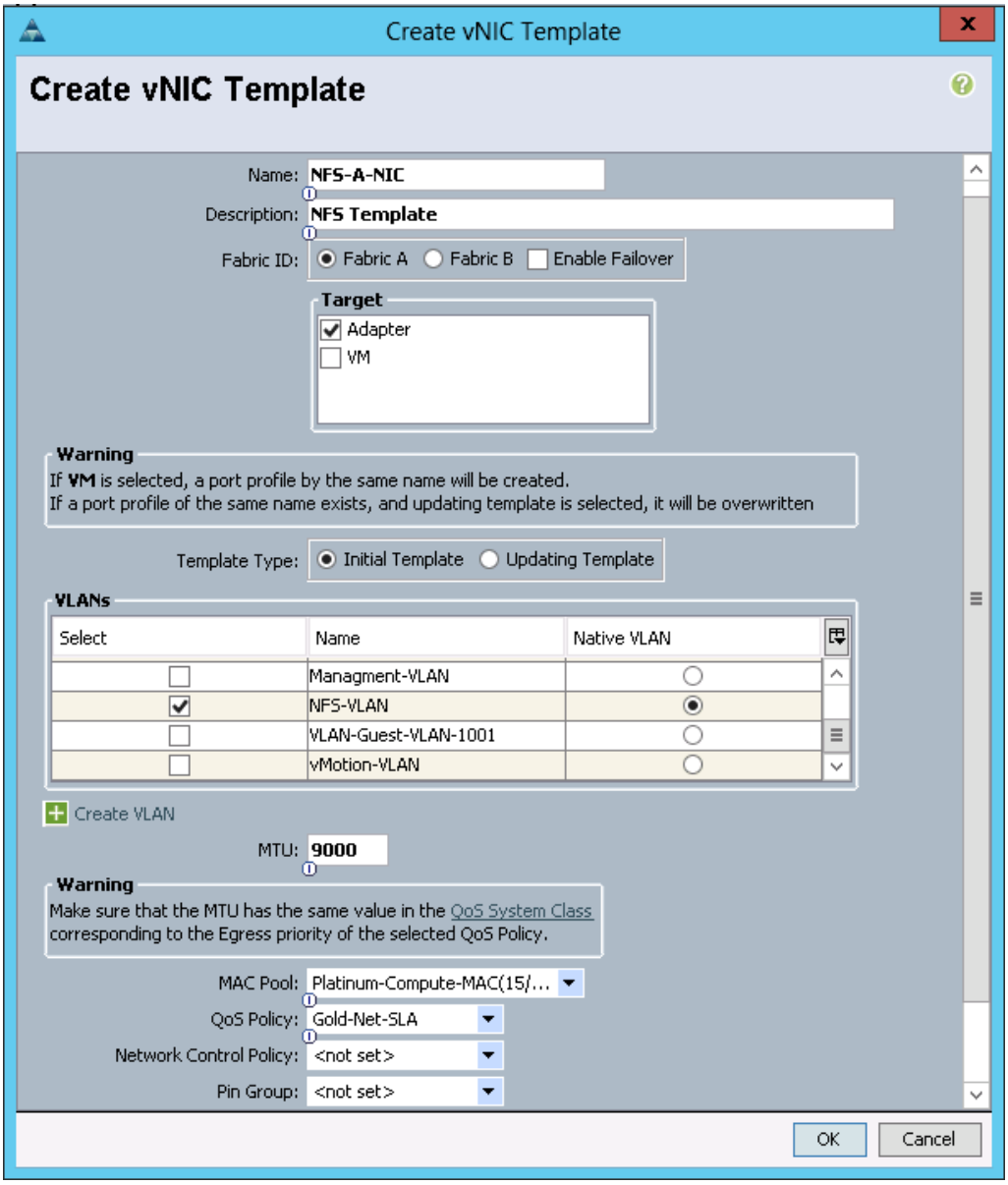
図 78　　Guest-B-NIC 用の vNIC プロパティの定義



65. [Create vNIC Template] ウィンドウが開きます。
66. [Name] フィールドに NFS-A-NIC と入力します。
67. [Description] フィールドに NFS Template と入力します。
68. [Fabric ID] で [FabricA] オプション ボタンをクリックし、[Enable Failover] チェックボックスにチェックは入れません。
69. [Target] で [Adapater] チェックボックスにチェックを入れます。
70. [Template Type] で [Initial Template] オプション ボタンを選択します。
71. [VLANs] で、[NFS-VLAN] にチェックを入れ、[NFS-VLAN] として [Native VLAN] を選択します。

72. [MTU] フィールドに 9000 と入力します。
73. [MAC Address Assignment] リスト ボックスから [Platinum-Compute-MAC] プールを選択します。
74. [QoS Policy] リスト ボックスの [Gold-Net-SLA] を選択します。
75. [Network Control Policy] リスト ボックスの [default] を選択します。
76. [Pin Group] リスト ボックスの [<not set>] を選択します。
77. [Stats Thershold Policy] リスト ボックスの [default] を選択します。
78. [Dynamic vNIC Connection Policy] リスト ボックスの [<not set>] を選択します。
79. [OK] をクリックします。

図 79　　NFS-A-NIC 用の vNIC プロパティの定義



80. [Create vNIC Template] ウィンドウが開きます。

81. [Name] フィールドに NFS-B-NIC と入力します。

82. [Description] フィールドに NFS Template と入力します。

83. [Fabric ID] で [FabricA] オプション ボタンをクリックし、[Enable Failover] チェックボックスにチェックは入れません。

84. [Target] で [Adapater] チェックボックスにチェックを入れます。

85. [Template Type] で [Initial Template] オプション ボタンを選択します。

86. [VLANs] で、[NFS-VLAN] にチェックを入れ、[NFS-VLAN] として [Native VLAN] を選択します。

87. [MTU] フィールドに 9000 と入力します。

88. [MAC Address Assignment] リスト ボックスから [Platinum-Compute-MAC] プールを選択します。

89. [QoS Policy] リスト ボックスの [Gold-Net-SLA] を選択します。

90. [Network Control Policy] リスト ボックスの [default] を選択します。

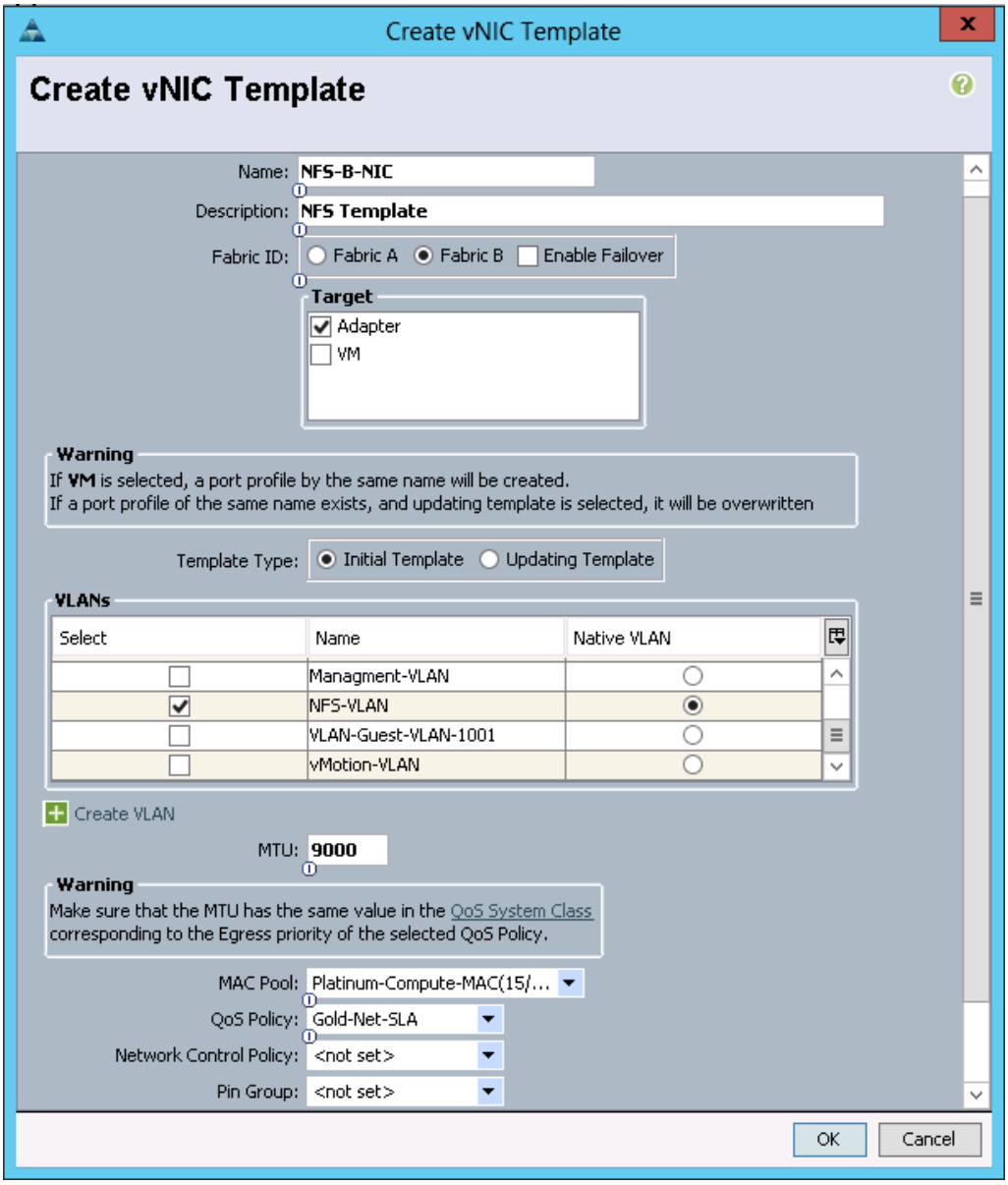
91. [Pin Group] リスト ボックスの [<not set>] を選択します。

92. [Stats Thershold Policy] リスト ボックスの [default] を選択します。

93. [Dynamic vNIC Connection Policy] リスト ボックスの [<not set>] を選択します。

94. [OK] をクリックします。

図 80　　NFS-B-NIC 用の vNIC プロパティの定義



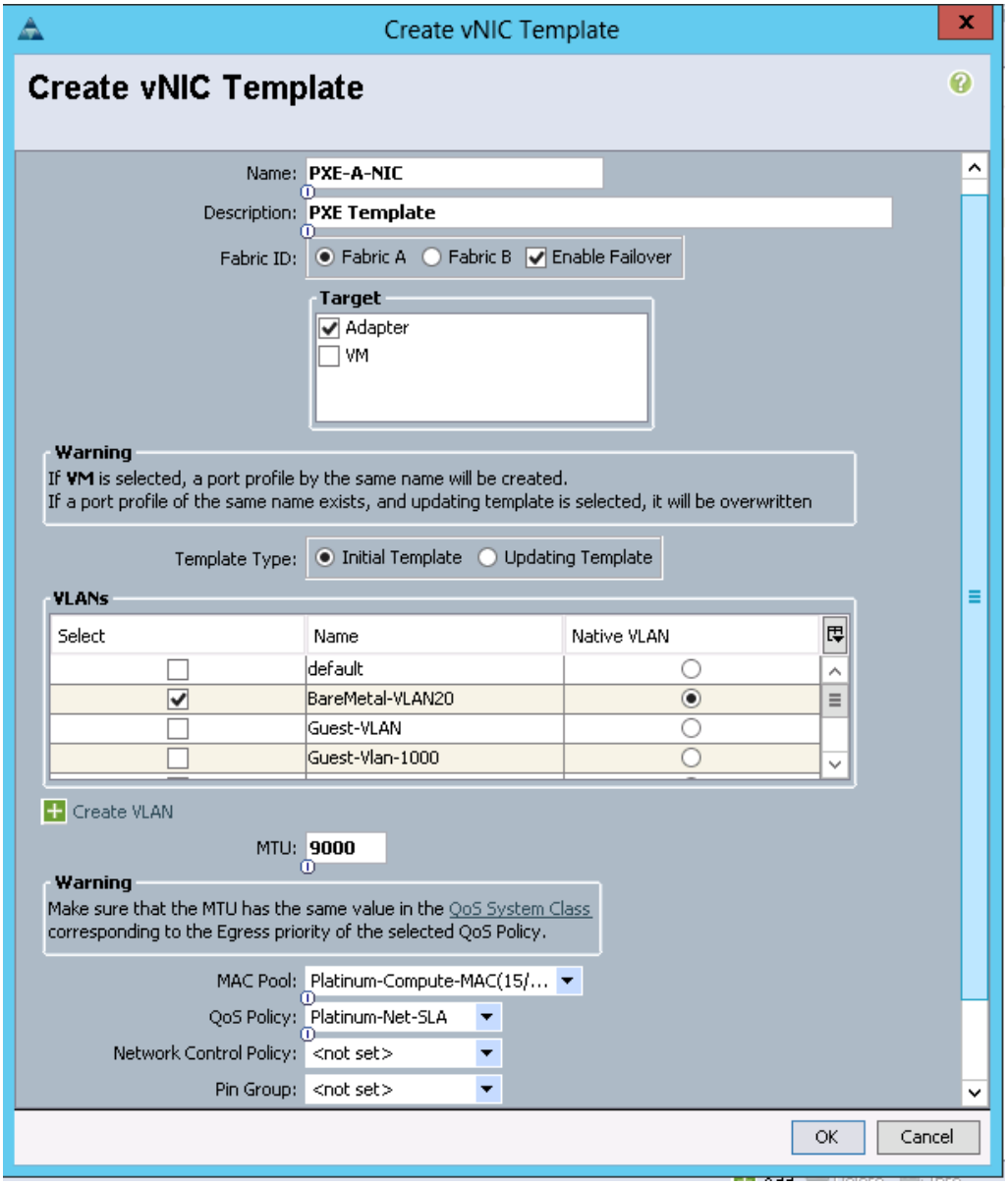
Baremetal ホスト vNIC テンプレート

PXE および管理 LAN トラフィックを取り扱うために 2 つの vNIC テンプレートを作成し、TenantA-BareMetal-Zone で Baremetal RHEL 6.3 ホストを実行するための SAN トラフィックを取り扱うために 2 つの vHBA テンプレートを作成します。

1. [Create vNIC Template] ウィンドウが開きます。
2. [Name] フィールドに PXE-A-NIC と入力します。
3. [Description] フィールドに PXE Template と入力します。
4. [Fabric ID] で [FabricA] オプション ボタンをクリックし、[Enable Failover] チェックボックスにチェックは入れません。
5. [Target] で [Adapater] チェックボックスにチェックを入れます。

6. [Template Type] で [Initial Template] オプション ボタンを選択します。
7. [VLANs] で、[Baremetal-VLAN20] にチェックを入れ、[Baremetal-VLAN20] として [Native VLAN] を選択します。
8. [MTU] フィールドに 9000 と入力します。
9. [MAC Address Assignment] リスト ボックスから [Platinum-Compute-MAC] プールを選択します。
10. [QoS Policy] リスト ボックスの [Platinium-Net-SLA] を選択します。
11. [Network Control Policy] リスト ボックスの [default] を選択します。
12. [Pin Group] リスト ボックスの [<not set>] を選択します。
13. [Stats Thershold Policy] リスト ボックスの [default] を選択します。
14. [Dynamic vNIC Connection Policy] リスト ボックスの [<not set>] を選択します。
15. [OK] をクリックします。

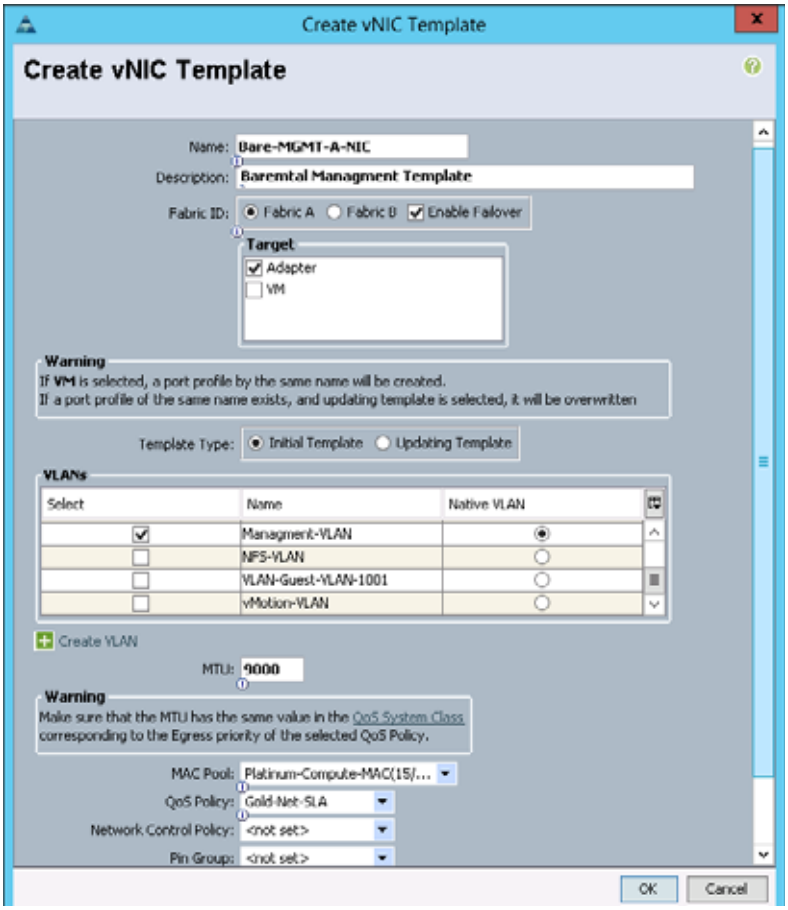
図 81　　PXE- A-NIC 用の vNIC プロパティの定義



16. [Create vNIC Template] ウィンドウが開きます。
17. [Name] フィールドに Bare-MGMT-A-NIC と入力します。
18. [Description] フィールドに Baremtal Magament Template と入力します。
19. [Fabric ID] で [FabricA] オプション ボタンをクリックし、[Enable Failover] チェックボックスにチェックは入れません。
20. [Target] で [Adapater] チェックボックスにチェックを入れます。
21. [Template Type] で [Initial Template] オプション ボタンを選択します。
22. [VLANs] で、[Baremetal-VLAN20] にチェックを入れ、[Baremetal-VLAN20] として [Native VLAN] を選択します。
23. [MTU] フィールドに 9000 と入力します。

24. [MAC Address Assignment] リスト ボックスから [Platinum-Compute-MAC] プールを選択します。
25. [QoS Policy] リスト ボックスの [GoldNet-SLA] を選択します。
26. [Network Control Policy] リスト ボックスの [default] を選択します。
27. [Pin Group] リスト ボックスの [<not set>] を選択します。
28. [Stats Thershold Policy] リスト ボックスの [default] を選択します。
29. [Dynamic vNIC Connection Policy] リスト ボックスの [<not set>] を選択します。
30. [OK] をクリックします。

図 82　　Bare-MGMT-A-NIC 用の vNIC プロパティの定義



Baremetal ホストおよび仮想ホストの vHBA テンプレート

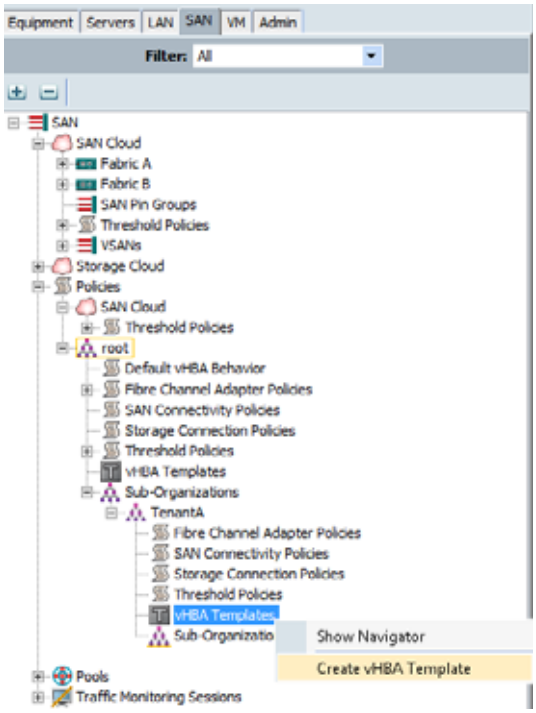
この項では、TenantA-BareMetal-Zone で Baremetal RHEL 6.3 ホストを、および TenantA ゾーンで Hypervisor ESXI 5.1 ホストをそれぞれ実行するための SAN トラフィックを取り扱う 2 つの vHBA テンプレートを作成します。

組織 Tenant A に対して作成済みのユーザ TenantA-Admin を使用して Cisco UCS Manager にログインします。

1. 左ペインで、[SAN] タブをクリックします。
2. [Pools] > [Sub-Organizations] を選択します。
3. [TenantA] を展開します。

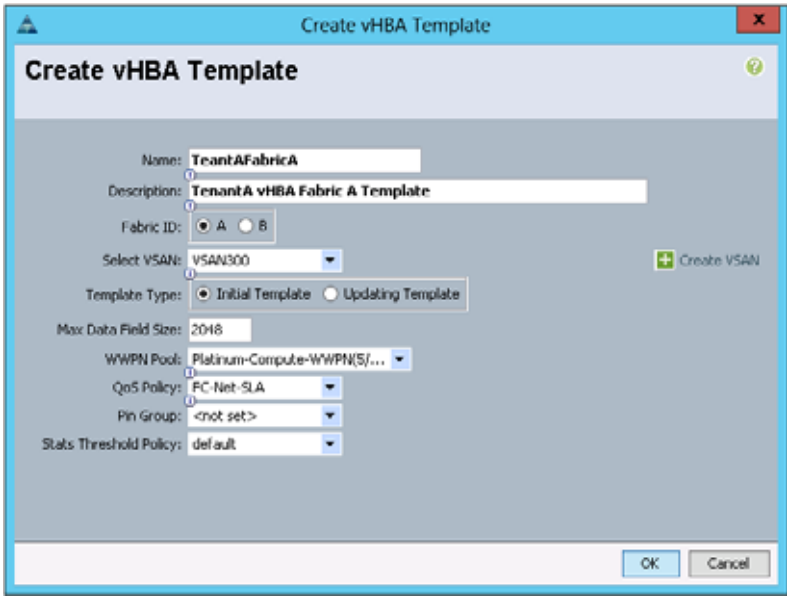
4. [vHBA Templates] を選択し、[Create vHBA Template] を右クリックします。

図 83　　vHBA テンプレートの作成



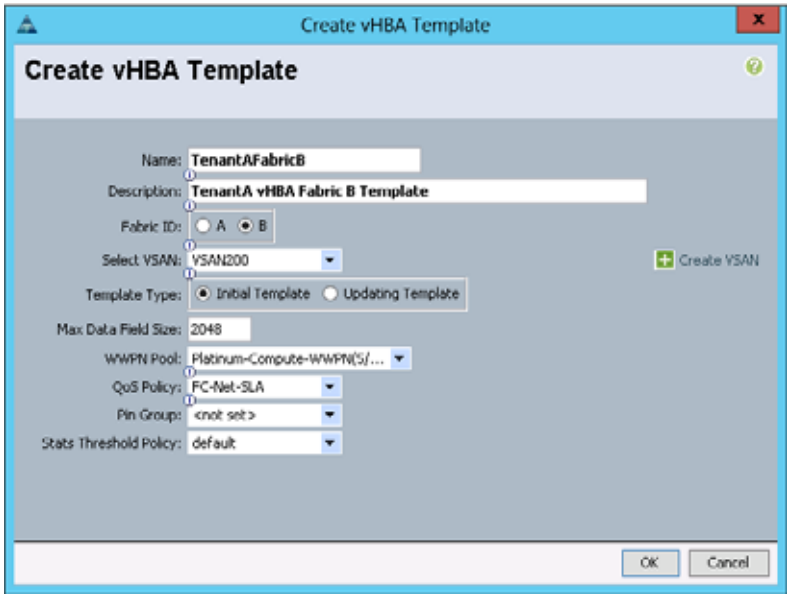
5. [Create vHBA Template] ウィンドウが開きます。
6. [Name] フィールドに TenantAFabricA と入力します。
7. [Description] フィールドに TenantA vHBA Fabric A Template と入力します。
8. [Fabric ID] で [FabricA] オプション ボタンをクリックします。
9. [VSAN] リスト ボックスの [VSAN300] を選択します。
10. [Template Type] で [Initial Template] オプション ボタンを選択します。
11. [Max Data field Size] フィールドに 2048 を入力します。
12. [WWPN Pool] リスト ボックスから [Platinum-Compute-WWPN] プールを選択します。
13. [QoS Policy] リスト ボックスの [FC-Net-SLA] を選択します。
14. [Pin Group] リスト ボックスの [<not set>] を選択します。
15. [Stats Thershold Policy] リスト ボックスの [default] を選択します。
16. [OK] をクリックします。

図 84　TenantAFabricA 用の vHBA プロパティの定義



17. [Create vHBA Template] ウィンドウが開きます。
18. [Name] フィールドに TenantAFabricA と入力します。
19. [Description] フィールドに TenantA vHBA Fabric A Template と入力します。
20. [**Fabric ID**] で [**FabricA**] オプション ボタンをクリックします。
21. [VSAN] リスト ボックスの [VSAN200] を選択します。
22. [Template Type] で [Initial Template] オプション ボタンを選択します。
23. [Max Data field Size] フィールドに 2048 を入力します。
24. [WWPN Pool] リスト ボックスから [Platinum-Compute-WWPN] プールを選択します。
25. [QoS Policy] リスト ボックスの [FC-Net-SLA] を選択します。
26. [Pin Group] リスト ボックスの [<not set>] を選択します。
27. [Stats Thershold Policy] リスト ボックスの [default] を選択します。
28. [OK] をクリックします。

図 85　TenantAFabricB 用の vHBA プロパティの定義



IPMI ポリシーの作成

Intelligent Platform Management Interface（IPMI）は、管理者がハードウェアおよびセンサーをモニタし、システム コンポーネントを制御し、重要なシステム イベントのログを取得してリモート管理およびリカバリを実行する方法を定義する、オープンな標準テクノロジーです。IPMI はサーバブレードの BMC（Baseboard Management Controller）上で実行されるので、オペレーティング システムから独立して動作します。IPMI がオペレーティング システムから独立して動作するので、IP を介して BMC にコマンドを送信してするときに、たとえオペレーティング システムが停止またはサーバの電源が落ちていても、管理者は IPMI を使用してシステムをモニタ、管理、診断、および復旧することができます。

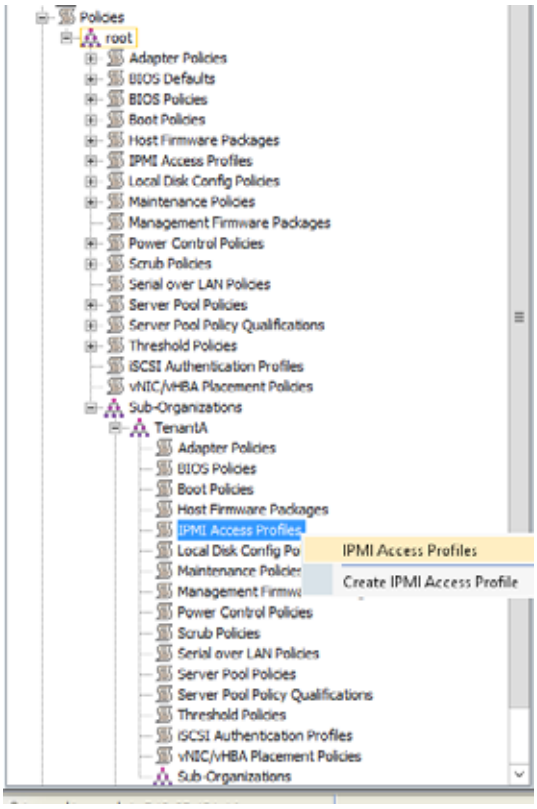
（注）　UCS システムでは、BMC は IPMI バージョン 2.0 のみをサポートします。

ここでは、リブート、シャットダウン、リセット、およびライフ サイクル管理のような Baremetal ホスト操作をテナントのクラウドで実行するために CloudPlatfrom 4.2.1 用の Cisco UCS Manager で IPMI Access ポリシーを作成します。

Cisco UCS Manager にルート ユーザでログインして、組織単位 TenantA を設定します。

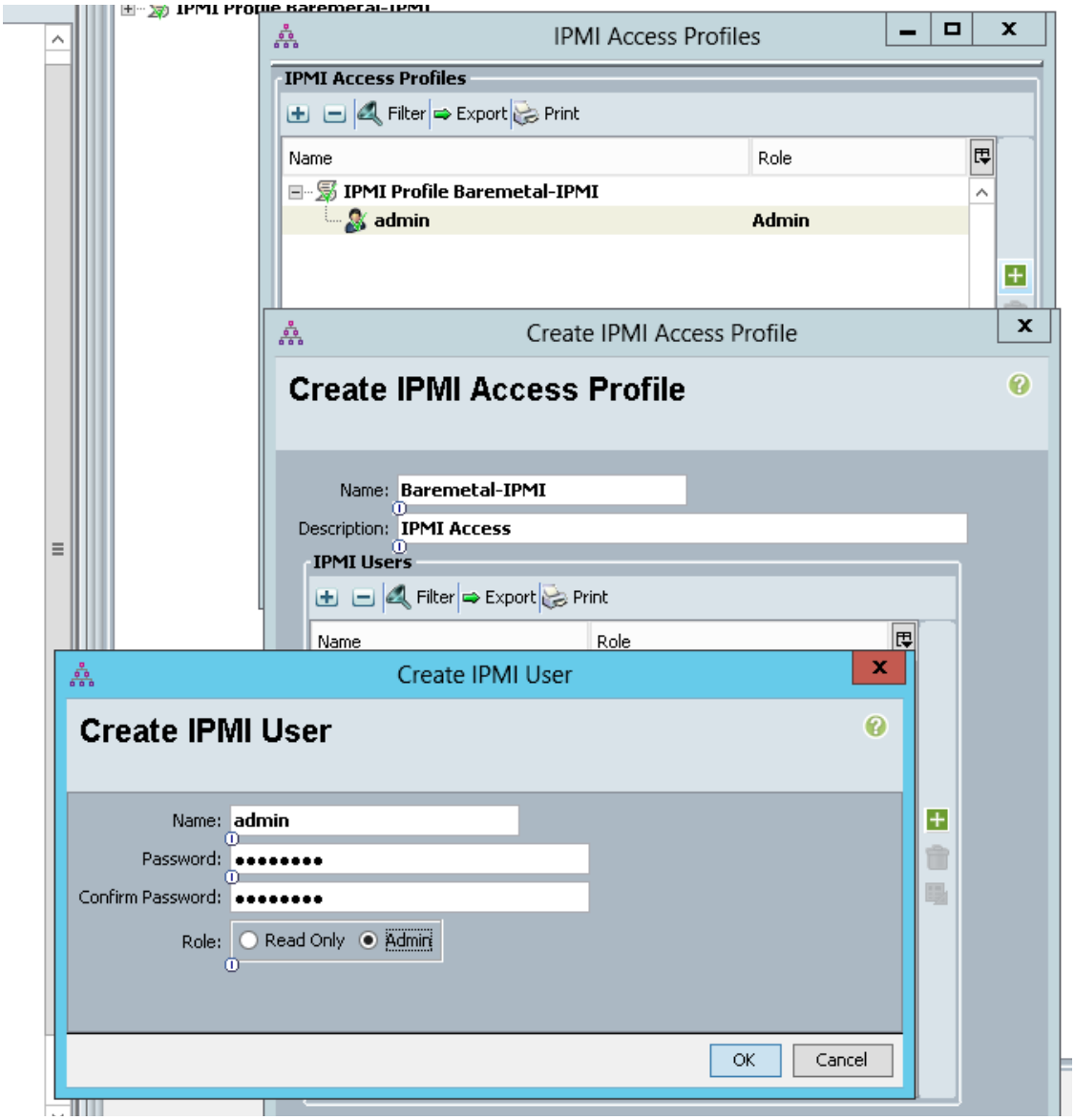
1. 左ペインで、[Policies Servers] タブをクリックします。
2. [Policies] を選択し、[root] を展開して、次に [Sub-Organizations] を展開します。
3. [TenantA] を展開します。
4. [IPMI Access Profile] を右クリックし、[Create IPMI Access Profiles] を選択します。

図 86　IPMI アクセス プロファイルの作成



5. [IPMI Access Profiles] ウィンドウで [Add] をクリックします。
6. [Name] フィールドに **Baremetal-IPMI** と入力します。
7. [Description] フィールドに **IPMI Acess** と入力します。
8. [IPMI Access Profiles] ウィンドウで [Add] をクリックします。
9. [Name] フィールドに admin と入力します。
10. [Password] フィールドに <XXXX> と入力します。
11. [Confirm Password] フィールドに <XXXX> と入力します。
12. [Role] アクセスの [Admin] オプション ボタンを選択します。
13. [OK] をクリックします。

図 87　　アクセス プロファイルでの IPMI ユーザ名およびパスワードの作成



サーバ プール資格情報およびポリシーの作成

サーバ プールは複数のサーバで構成されています。これらのサーバは通常いくつかの特性を共有します。シャーシ内の場所の場合もあり、またはサーバ タイプ、メモリ容量、ローカル ストレージ、CPU のタイプ、またはローカル ドライブ設定などの属性の場合もあります。サーバは手動でサーバ プールに割り当てることが可能です。または、サーバ プール ポリシーおよびサーバ プール ポリシー資格情報を使用して自動で割り当てることもできます。

クラウド サービス オファリングに基づいたコンピュート サービス レベル（費用も含む）を満たすために、UCS ではクラウド管理者が特定の組織で使用される 1 つまたはそれ以上のサーバ プールを指定可能にするサーバ プールを提供します。UCS では、サーバ プール資格情報パラメータを定義して特定のサーバ プールにコンピュート リソースを容易に自動配置することで、お客様のビジネスが成長するための需要に応えることができます。これらのパラメータには、コンピュート ブレードで使用可能なパフォーマンスおよび容量に基づいた物理 CPU およびメモリのタイプなどがあります。

ここでは、メモリ、CPU、およびその他の属性などのクラウド コンピュート オファリングに基づいたポリシー資格情報を使用して 4 つのサーバ プールを作成します。これらはクラウド コンピュート システムで使用可能な場合に、関するサーバ プールに自動的に割り当てられます。

1. Platinum サーバ プール
2. Gold サーバ プール
3. Silver サーバ プール
4. Bronze サーバ プール

この項で説明する手順では、Cisco UCS 環境で Compute-Server-Pool に対して必要なサーバ プール資格情報の設定を詳しく説明します。

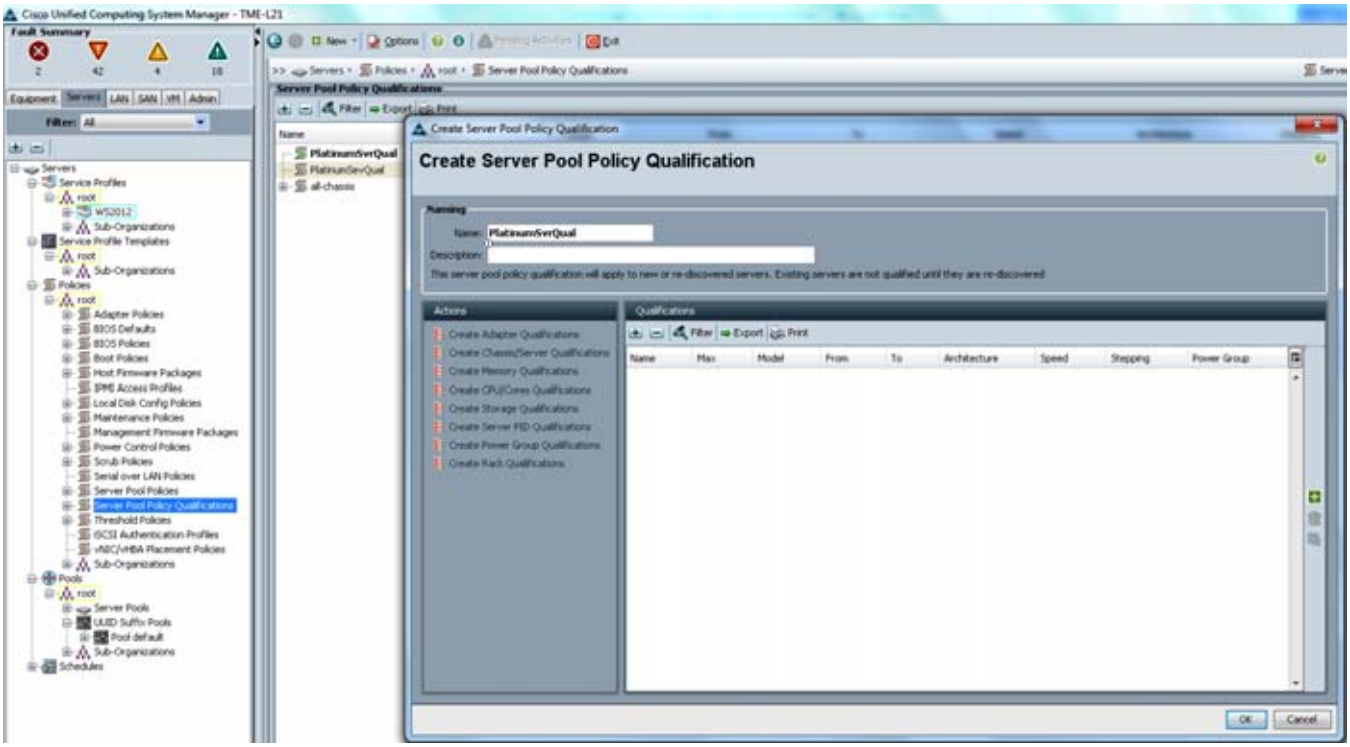
このマニュアルで触れるサーバ プール資格情報は一般的な使用方法に基づいており、クラウド環境でのお客様の特定のコンピュート ニーズを選択するために変更可能です。

Platinum コンピュート サーバ プールおよび資格情報

Cisco UCS Manager にルート ユーザでログインして、組織単位 TenantA を設定します。

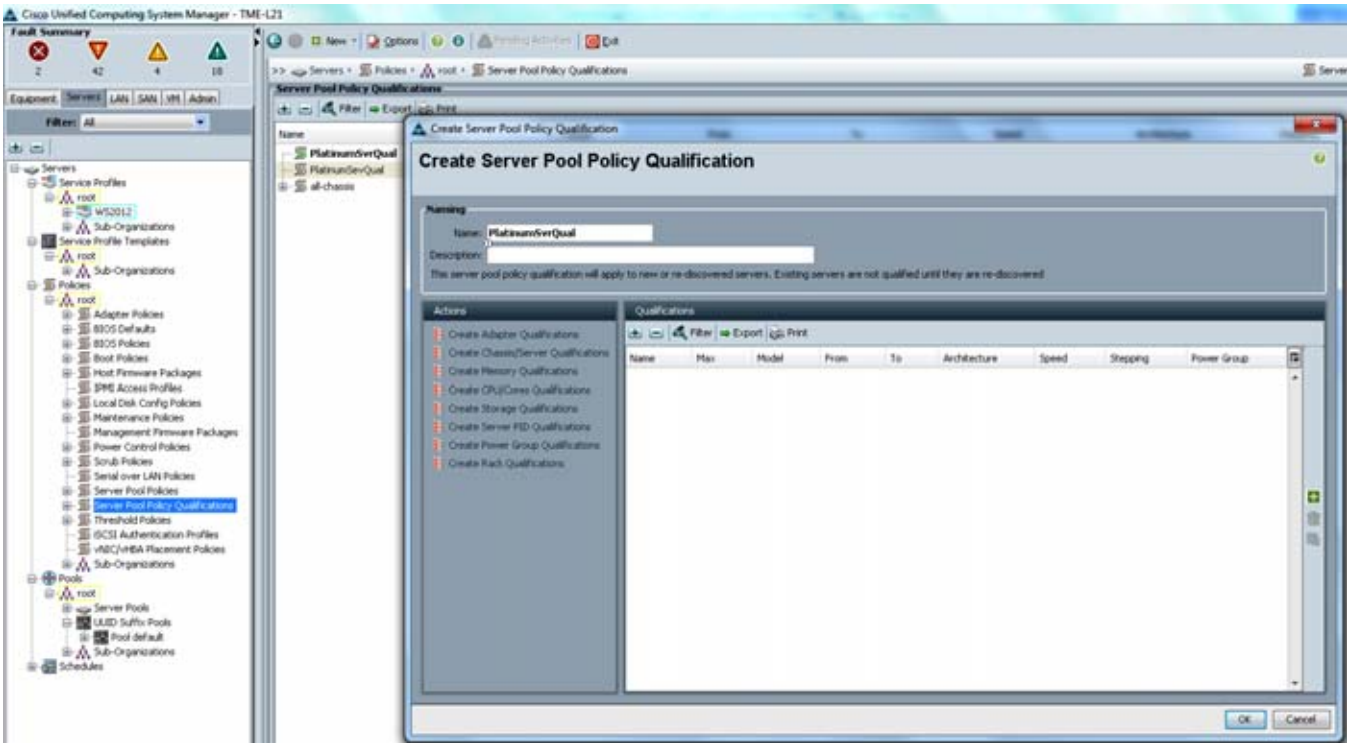
1. 左ペインで、[Servers] タブをクリックします。
2. [Policies] を選択し、[root] を展開します。
3. [Server Pool Policy Qualifications] を右クリックし、[Create Server Pool Policy Qualification] を選択します。

図 88　　サーバ プール ポリシー資格情報の作成



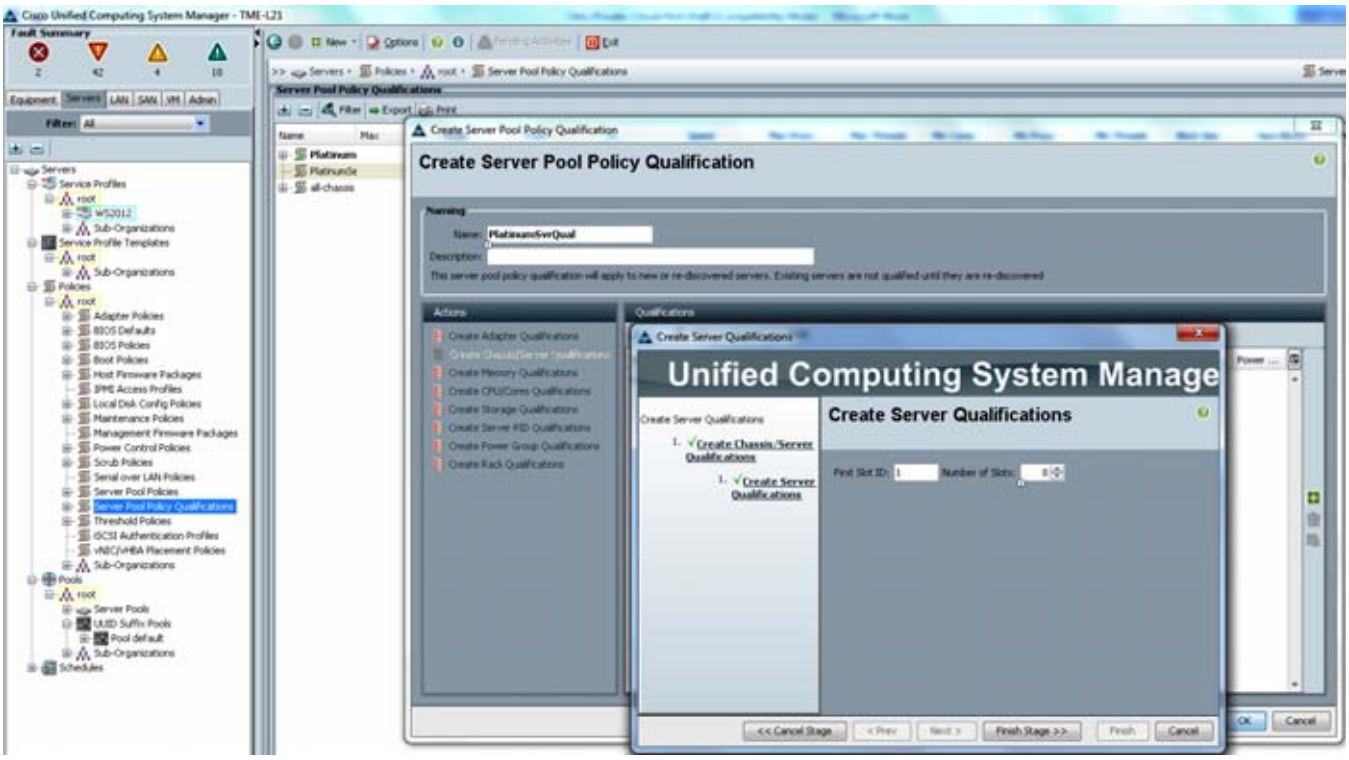
4. サーバ プール ポリシー資格情報の名前を PlatinumSvrQual にします。
5. （任意）説明を入力します。

図 89　　サーバ プール ポリシー資格情報への名前と説明の追加



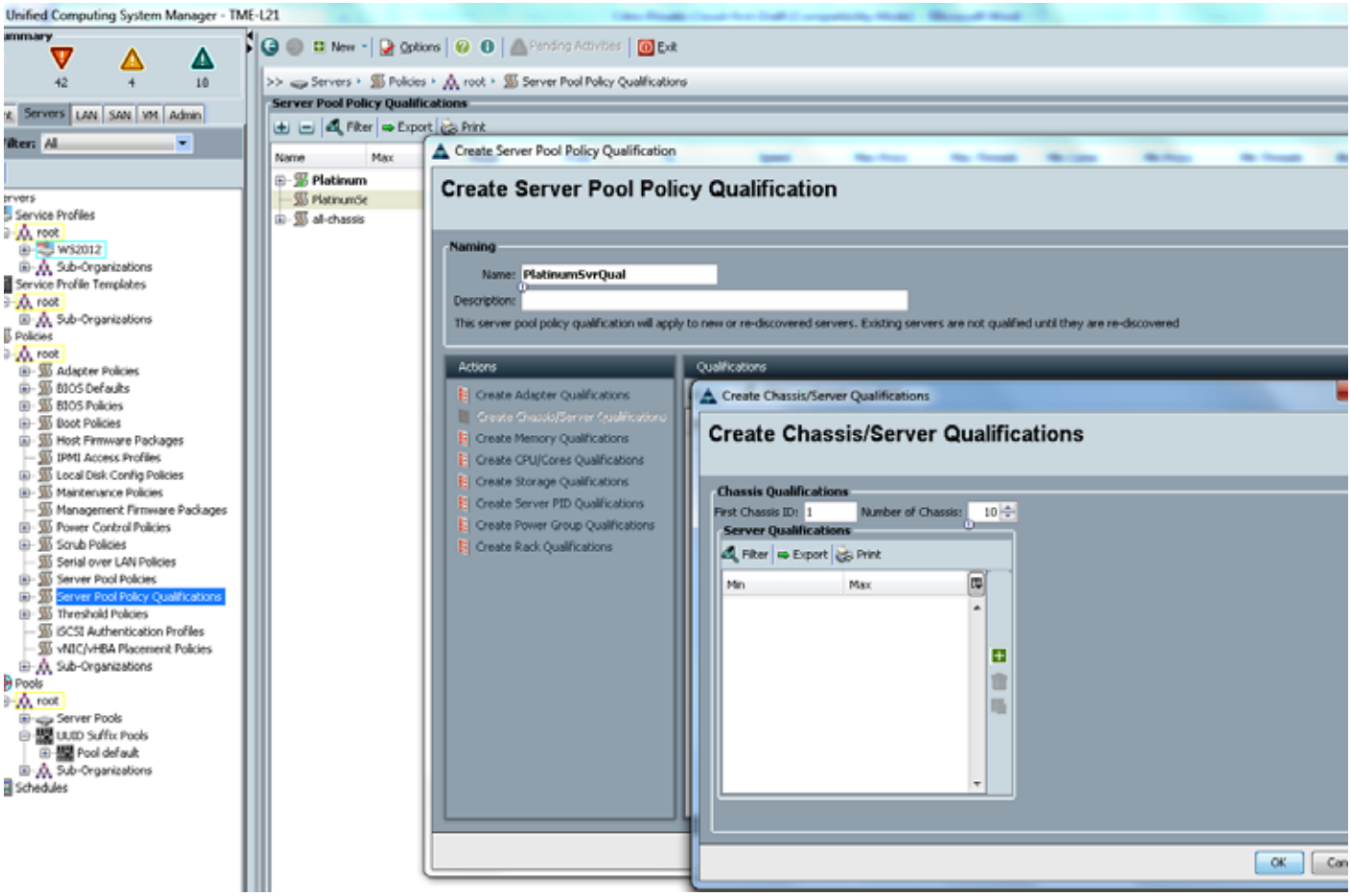
6. [Actions] ペインで、[Create Chassis/Server Qualification] をクリックします。
7. [First Chassis ID] として値 1 を入力し、[Number of chassis] として値 10 を入力します。

図 90　　サーバ資格情報の ID およびスロットの定義



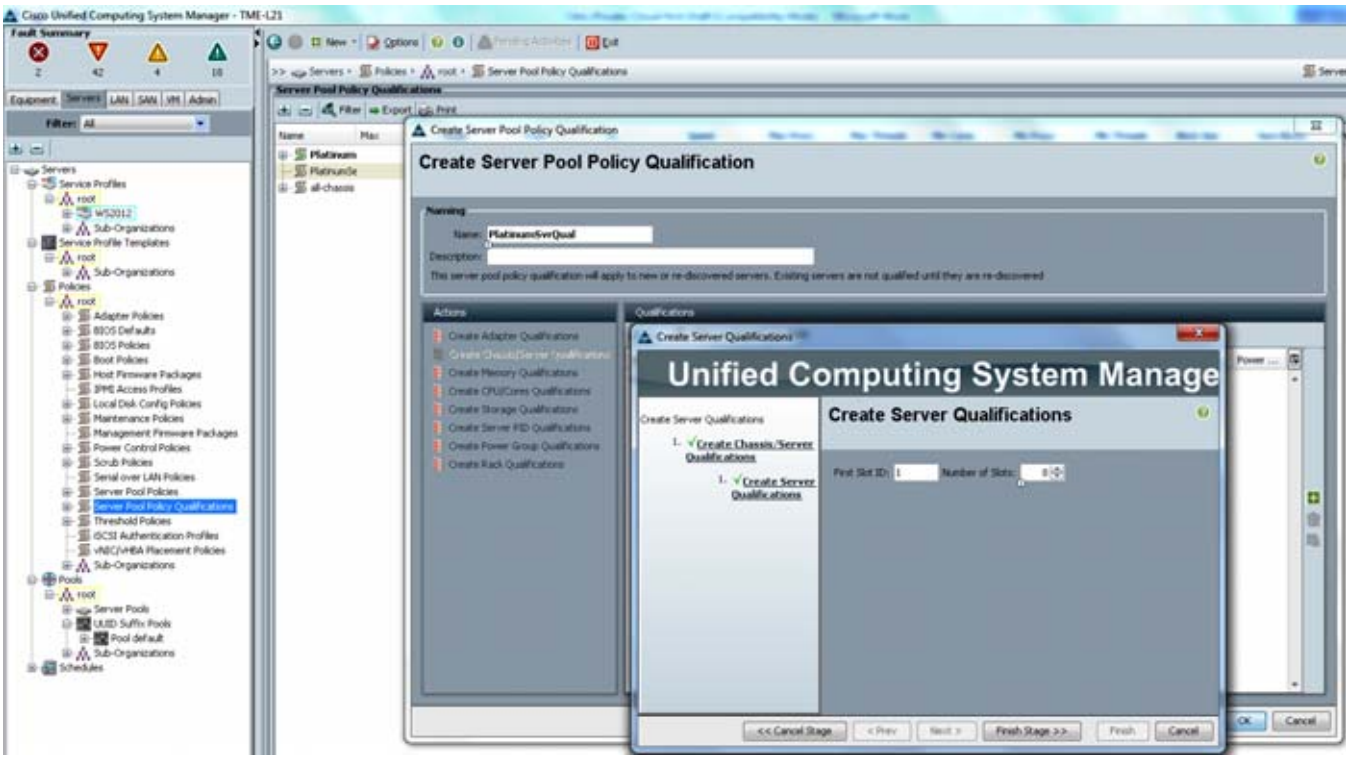
8. [Server Qualifications] の下で [ADD (+)] をクリックします。

図 91　　Platinum サーバへのサーバ資格情報の追加



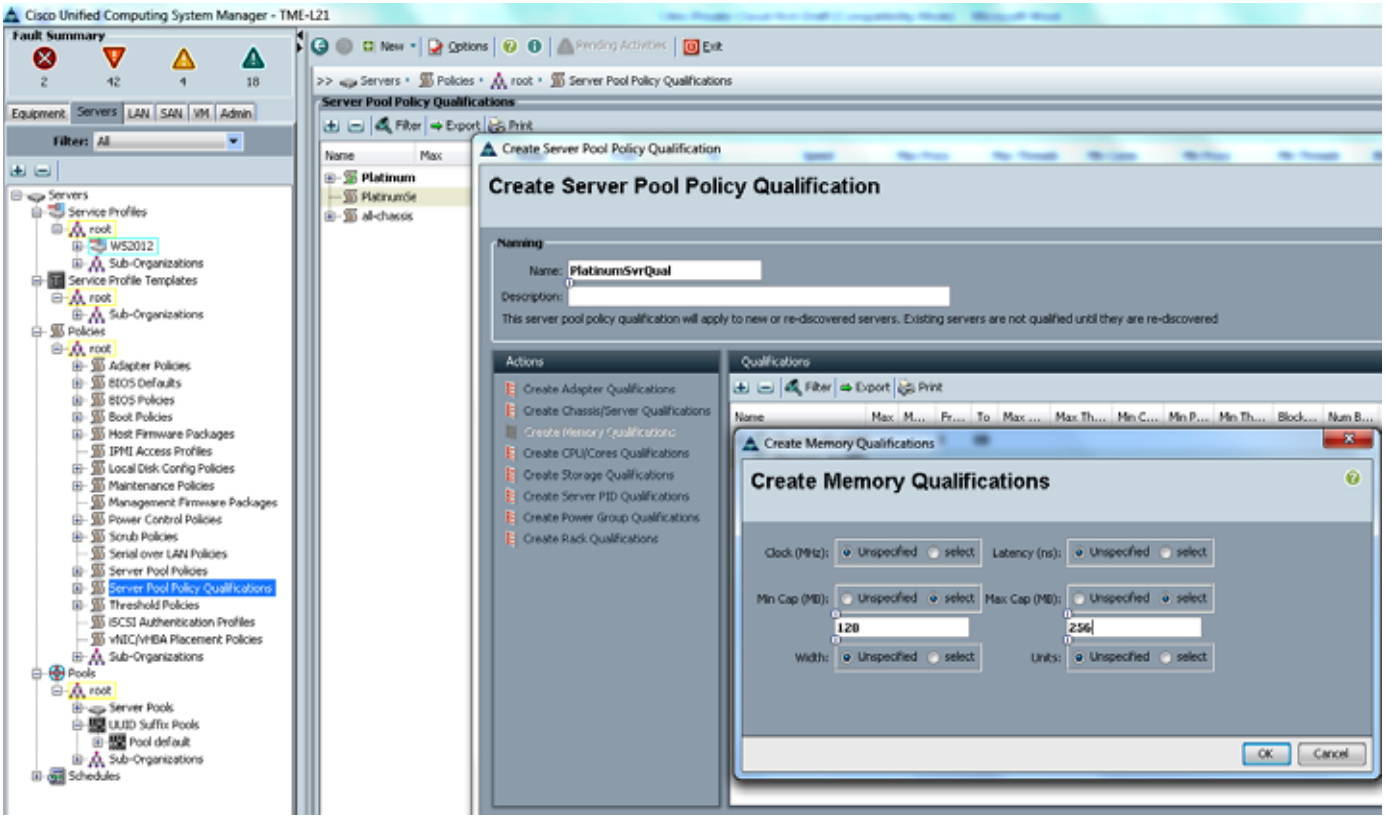
9. [First Slot ID] で値 1 を入力し、[Number of Slots] に 8 を入力します。

図 92　　サーバ資格情報の ID およびスロットの定義



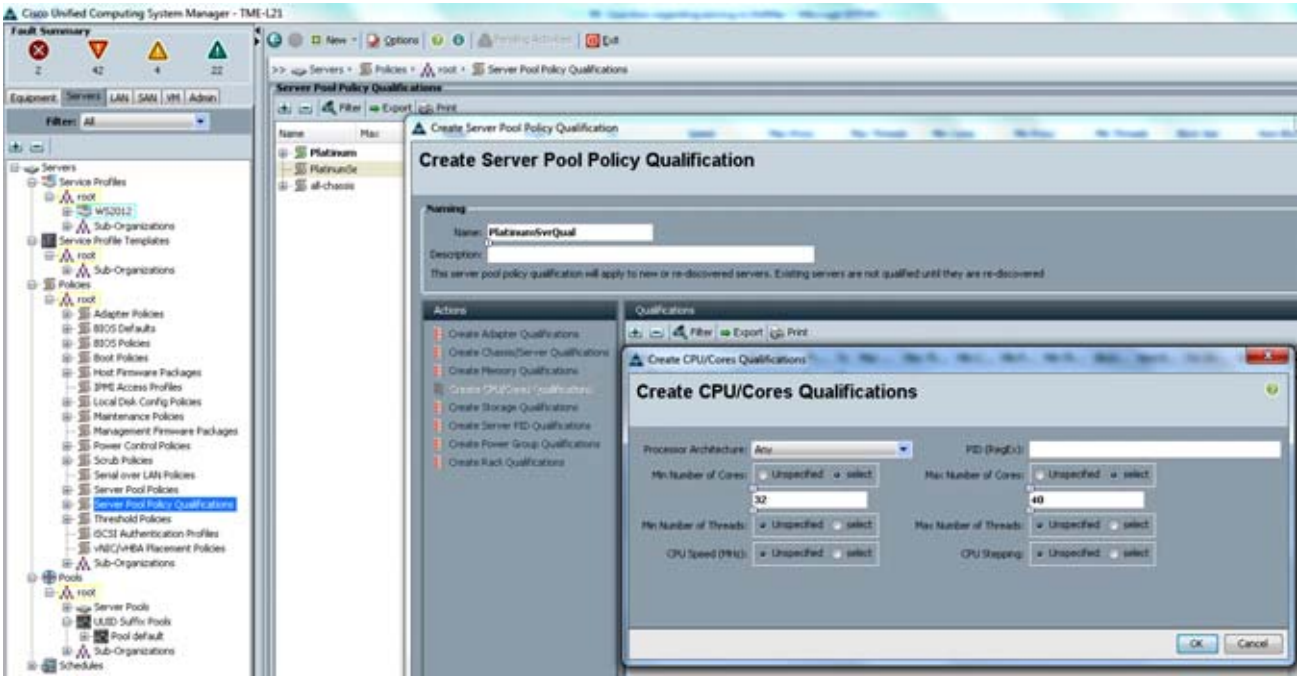
10. [Final Stage] をクリックし、次に [Finish] をクリックします。
11. [Actions] ペインで、[Create Chassis/Server Qualification] をクリックします。
12. [First Chassis ID] フィールドに 1 を入力し、[Number of Chassis] フィールドに 10 を入力します。
13. [Actions] ペインで、[Create Memory Qualification] をクリックします。
14. [Clock (MHz)] フィールドで、[Unspecified] オプション ボタンをクリックします。
15. [Latency (ns)] フィールドで、[Unspecified] オプション ボタンをクリックします。
16. [Min Cap (MB)] フィールドで、[select] オプション ボタンを選択して 128 を入力します。
17. [Max Cap (MB)] フィールドで、[select] オプション ボタンをクリックし 256 を入力します。
18. [Width] フィールドで、[Unspecified] オプション ボタンをクリックします。
19. [Units] フィールドで、[Unspecified] オプション ボタンをクリックします。
20. [OK] をクリックします。

図 93　　メモリ資格情報のパラメータの定義



21. [Actions] ペインで、[Create CPU Qualification] をクリックします。
22. [Min Number of Cores] フィールドで [Select] オプション ボタンをクリックし 32 を入力します。
23. [Max Number of Cores] フィールドで [Select] オプション ボタンをクリックし 40 を入力します。
24. [Processor Architecture] で Any を選択し、[PID (RegEx)] フィールドを空白のまま残します。
25. [Min Number of Threads] フィールドで [Unspecified] オプション ボタンをクリックします。
26. [Max Number of Threads] フィールドで [Unspecified] オプション ボタンをクリックします。
27. [CPU Speed (MHz)] フィールドで [Unspecified] オプション ボタンをクリックします。
28. [CPU Stepping] フィールドで [Unspecified] オプション ボタンをクリックします。
29. [Finish] をクリックします。

図 94　　CPU 資格情報のパラメータの定義

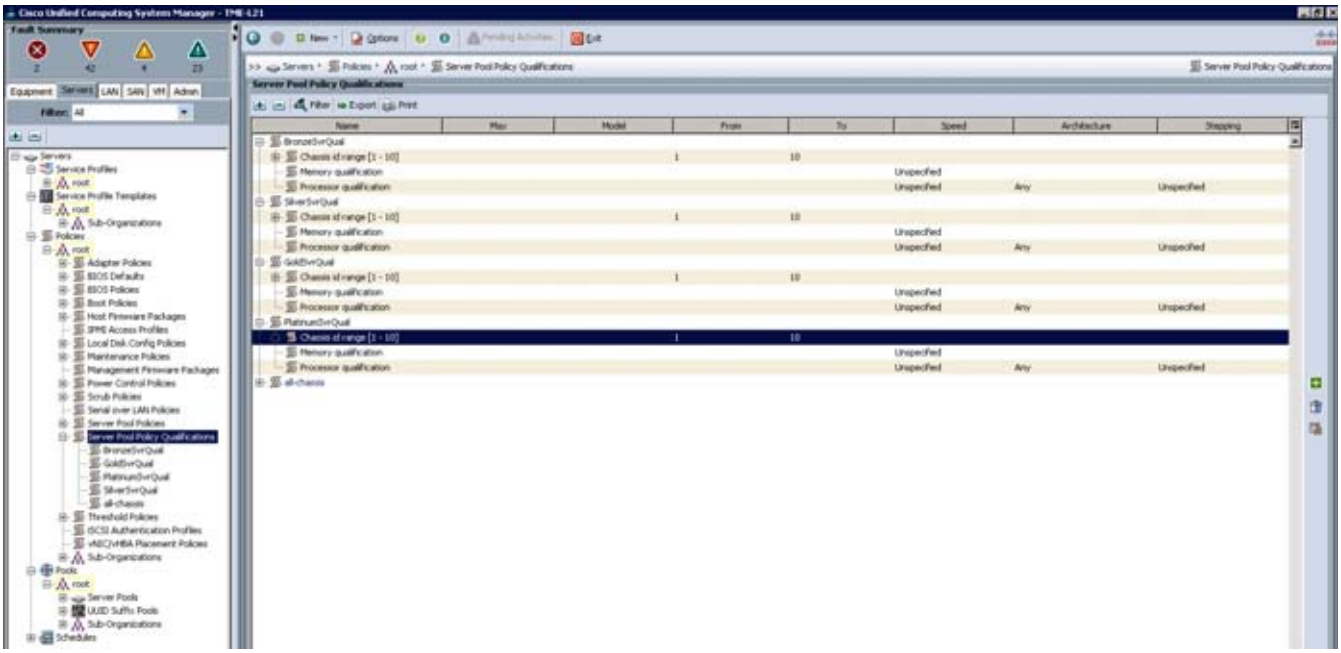


上記で説明した手順に従い、表 15 にリストしたサーバ プール ポリシー資格情報を使用してサーバ プール ポリシー資格情報 Gold-Compute-Server、Silver-Compute-Server、および Bronze-Compute-Server を作成します。

表 15　　すべてのサービス クラスに対するサーバ プール ポリシー資格情報の値

サーバ プール ポリシー資格情報	シャーシ	メモリ	CPU
PlatinumSvrQual	ID の範囲 1 ～ 10 サーバ スロット ID の範囲 1 ～ 8	Min Cap 128 ～ Max Cap 256	Min Number of cores 32 ～ Max Number of cores 40
GoldSvrQual	ID の範囲 1 ～ 10 サーバ スロット ID の範囲 1 ～ 8	Min Cap 64 ～ Max Cap 128	Min Number of cores 32 ～ Max Number of cores 40
SilverSvrQual	ID の範囲 1 ～ 10 サーバ スロット ID の範囲 1 ～ 8	Min Cap 32 ～ Max Cap 64	Min Number of cores 12 ～ Max Number of cores 16
BronzeSvrQual	ID の範囲 1 ～ 10 サーバ スロット ID の範囲 1 ～ 8	Min Cap 16 ～ Max Cap 32	Min Number of cores 12 ～ Max Number of cores 16

図 95　　作成したサーバ プール ポリシー資格情報のサマリー

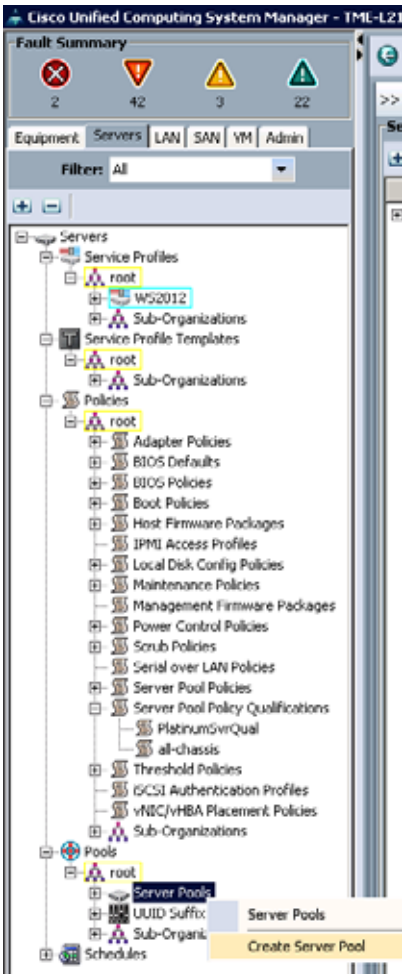


Platinum コンピュート サーバ プール

Cisco UCS Manager にルート ユーザでログインして、組織単位 TenantA に対するサーバ プールを設定します。

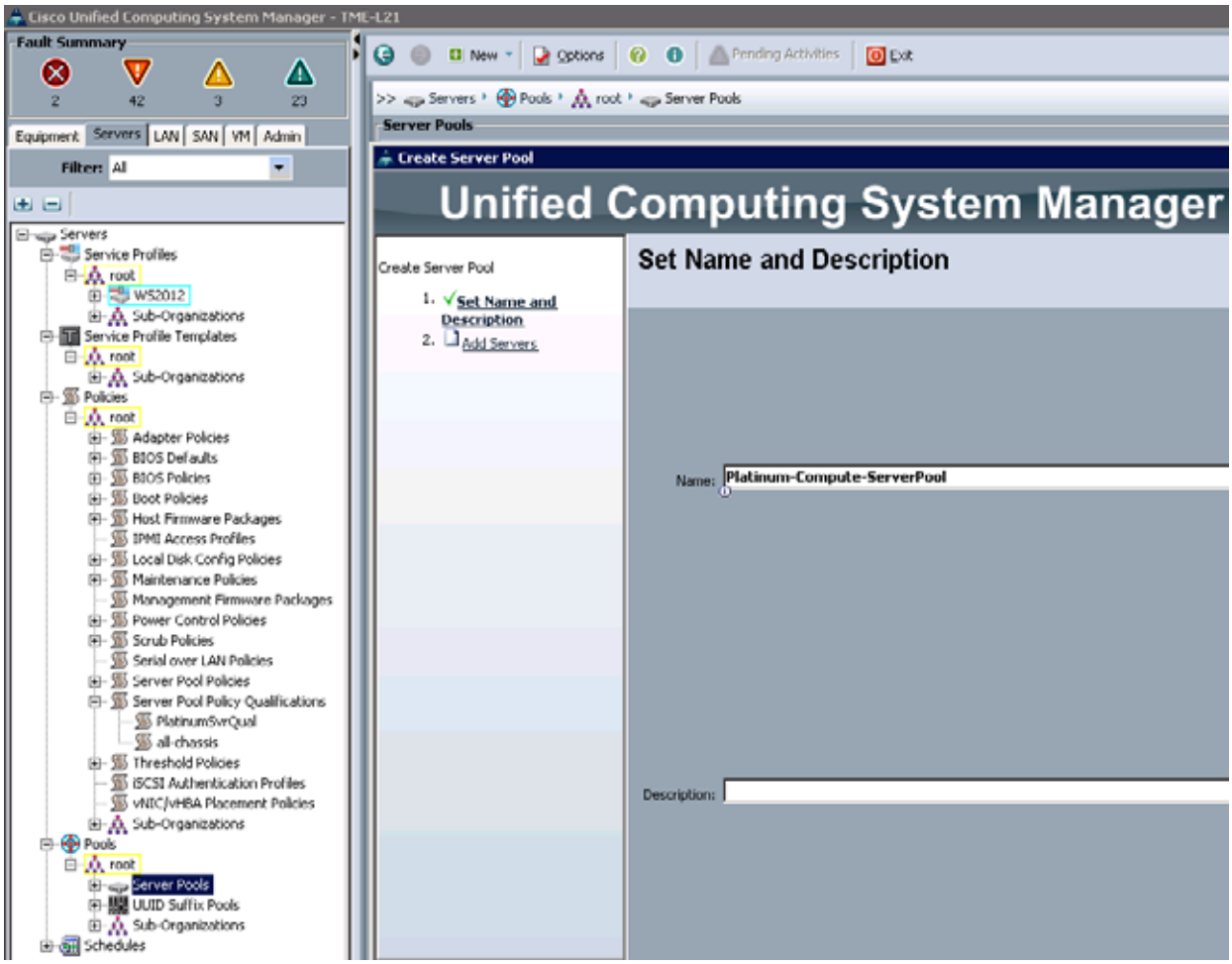
1. 左ペインで、[Servers] タブをクリックします。
2. [Pools] を選択し、[root] を展開します。
3. [Server Pool] を右クリックし、[Create Server Pool] を選択します。

図 96　　サーバ プールの作成



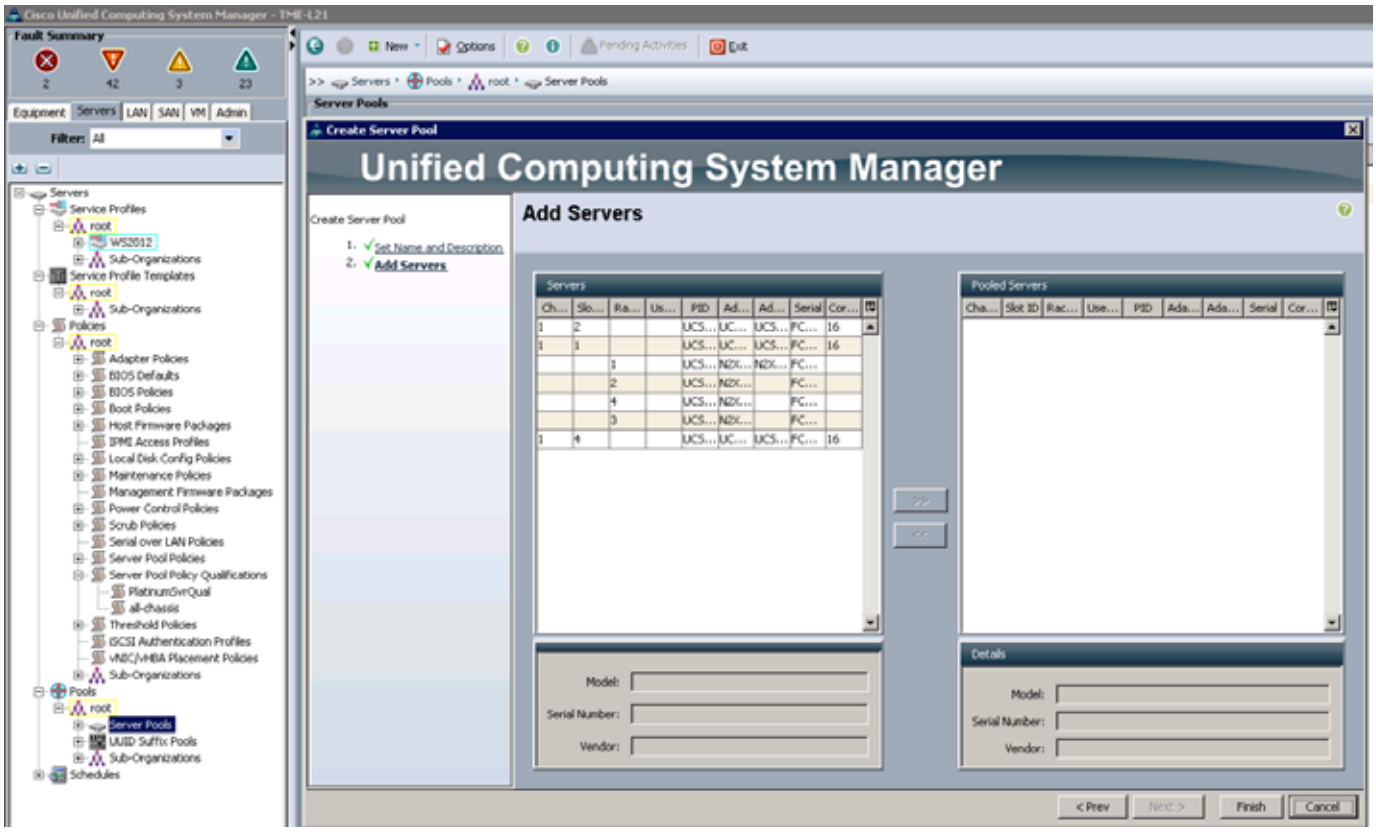
4. [Name] フィールドに Platinum-Compute-ServerPool と入力します。
5. （任意）[Description] フィールドに説明を入力します。

図 97　　サーバ プールの名前および説明の追加



6. [Finish] をクリックします。

図 98　　サーバ プール内のサーバのサマリー

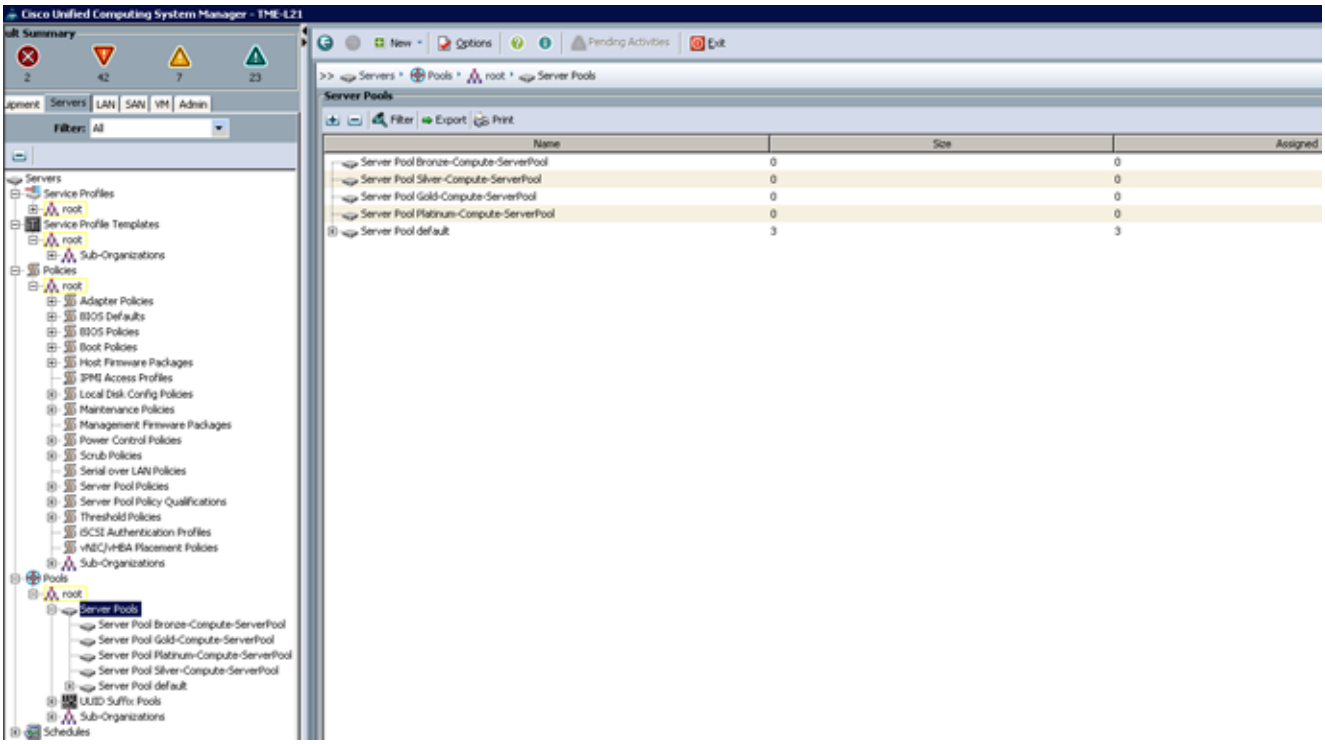


上記で説明した手順に従い、表 16 にリストしたサーバ プール ポリシー資格情報の値を使用してサーバ プール Gold-Compute-ServerPool、Silver-Compute-ServerPool、および Bronze-Compute-ServerPool を作成します。

表 16　　サーバ プールのサーバ プール ポリシー資格情報の値

サーバ プール	ブレード値
Platinum-Compute-ServerPool	1 ～ 8
Gold-Compute-ServerPool	1 ～ 8
Silver-Compute-ServerPool	1 ～ 8
Bronze-Compute-ServerPool	1 ～ 8

図 99　　作成したサーバ プールすべてのサマリー

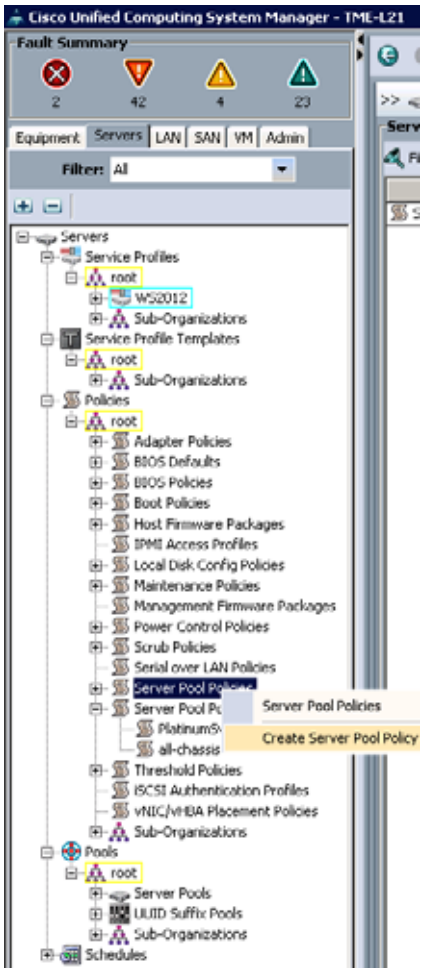


Platinum コンピュート サーバ プール ポリシー

Cisco UCS Manager にルート ユーザでログインして、組織単位 TenantA に対するサーバ プール ポリシーを設定します。

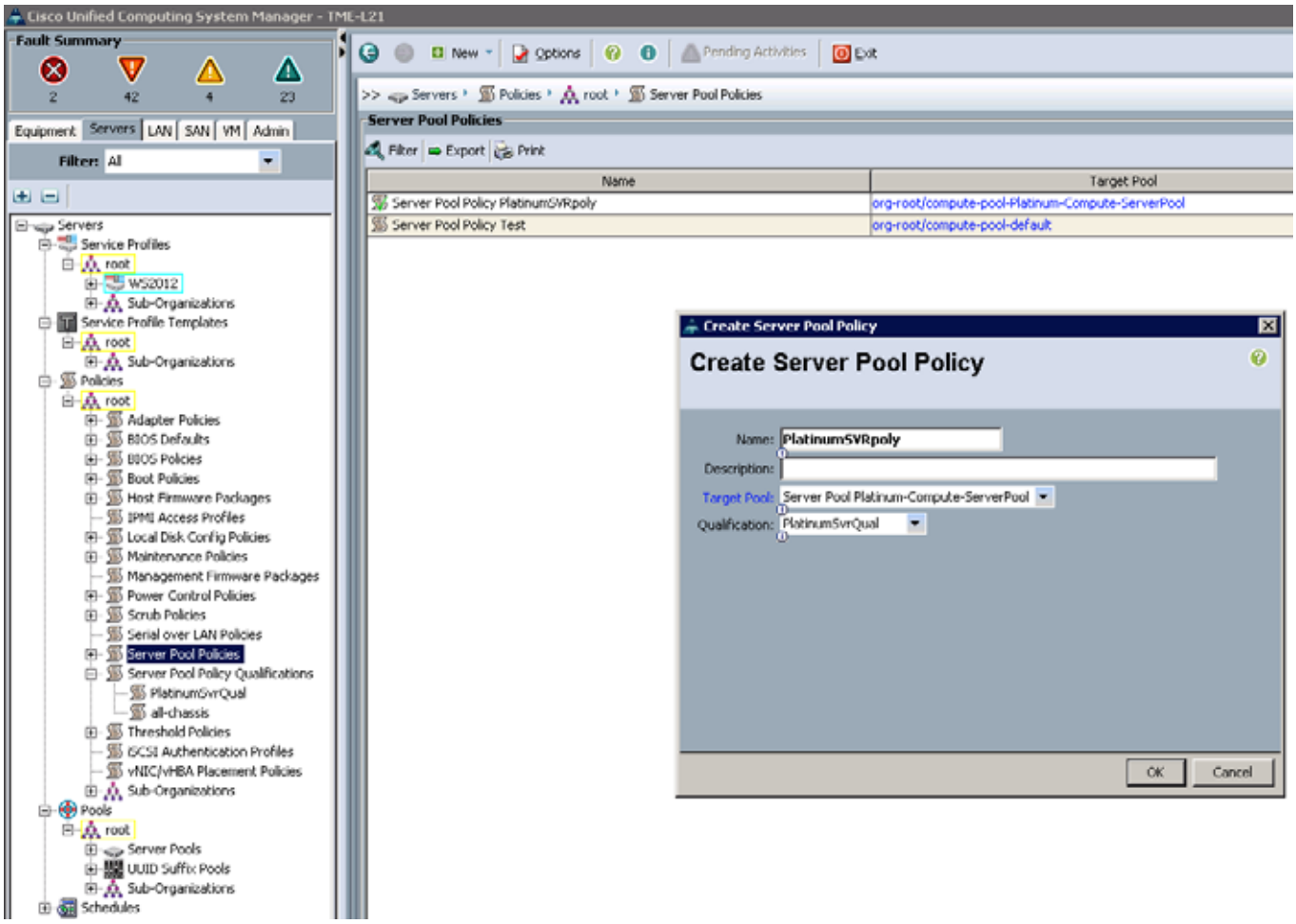
1. 左ペインで、[Servers] タブをクリックします。
2. [Policies] を選択し、[root] を展開します。
3. [Server Pool Policies] を右クリックし、[Create Server Pool Policy] を選択します。

図 100　サーバ プール ポリシーの作成



4. [Name] フィールドに PlatinumSVRPply と入力します。
5. （任意）[Description] フィールドに説明を入力します。
6. [Target Pool] リスト ボックスで、[Server Pool Platinum-Compute-ServerPool]（すでに作成済み）を選択します。
7. [Qualification] リスト ボックスで、[PlatinumSvrQual]（すでに作成済み）を選択します。

図 101　　サーバ プール ポリシー属性の定義

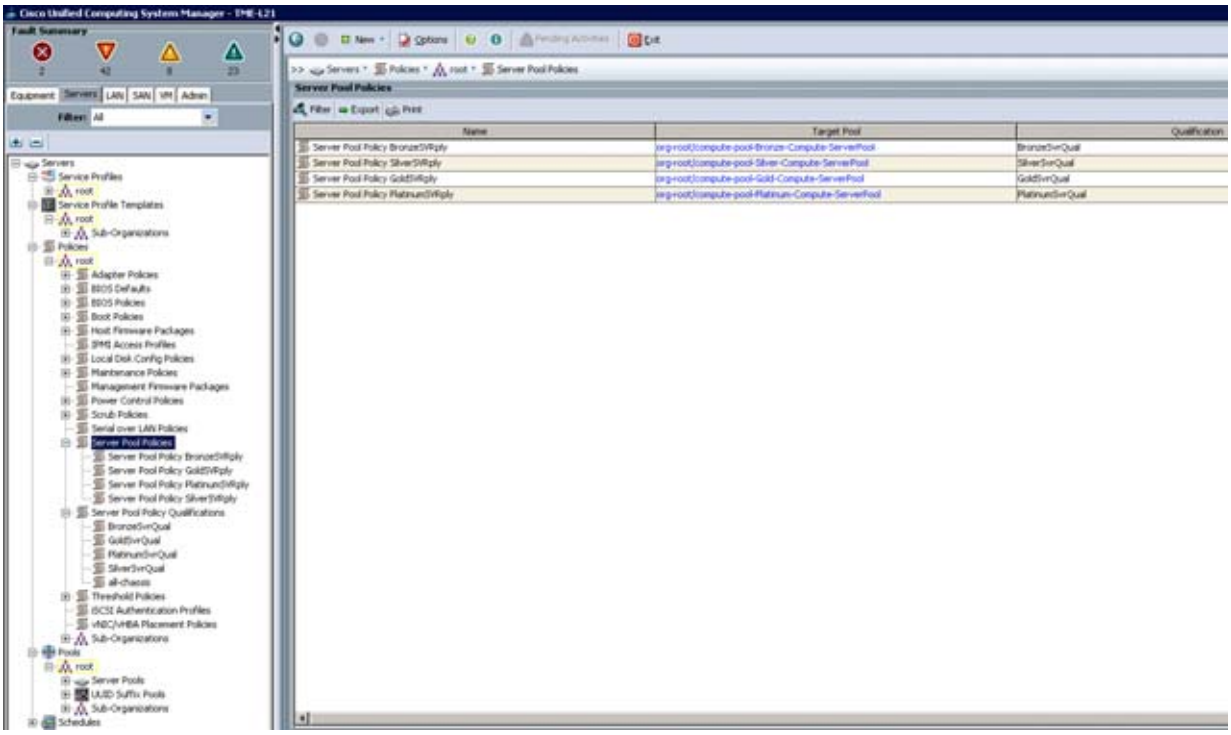


上記で説明した手順に従い、表 17 にリストしたサーバ プール ポリシーを使用してサーバ プール ポリシー Gold-Compute-ServerPool、Silver-Compute-ServerPool、および Bronze-Compute-ServerPool を作成します。

表 17　　サーバ プール ポリシーの値

サーバ プール ポリシー	ターゲット プール	絞り込み
PlatinumSVRply	Server Pool Platinum-Compute-ServerPool	PlatinumSvrQual
GoldSVRply	Server Pool Gold-Compute-ServerPool	GoldSvrQual
SilverSVRply	Server Pool Silver-Compute-ServerPool	SilverSvrQual
BronzeSVRply	Server Pool Bronze-Compute-ServerPool	BronzeSvrQual

図 102　作成したサーバ プール ポリシーすべてのサマリー



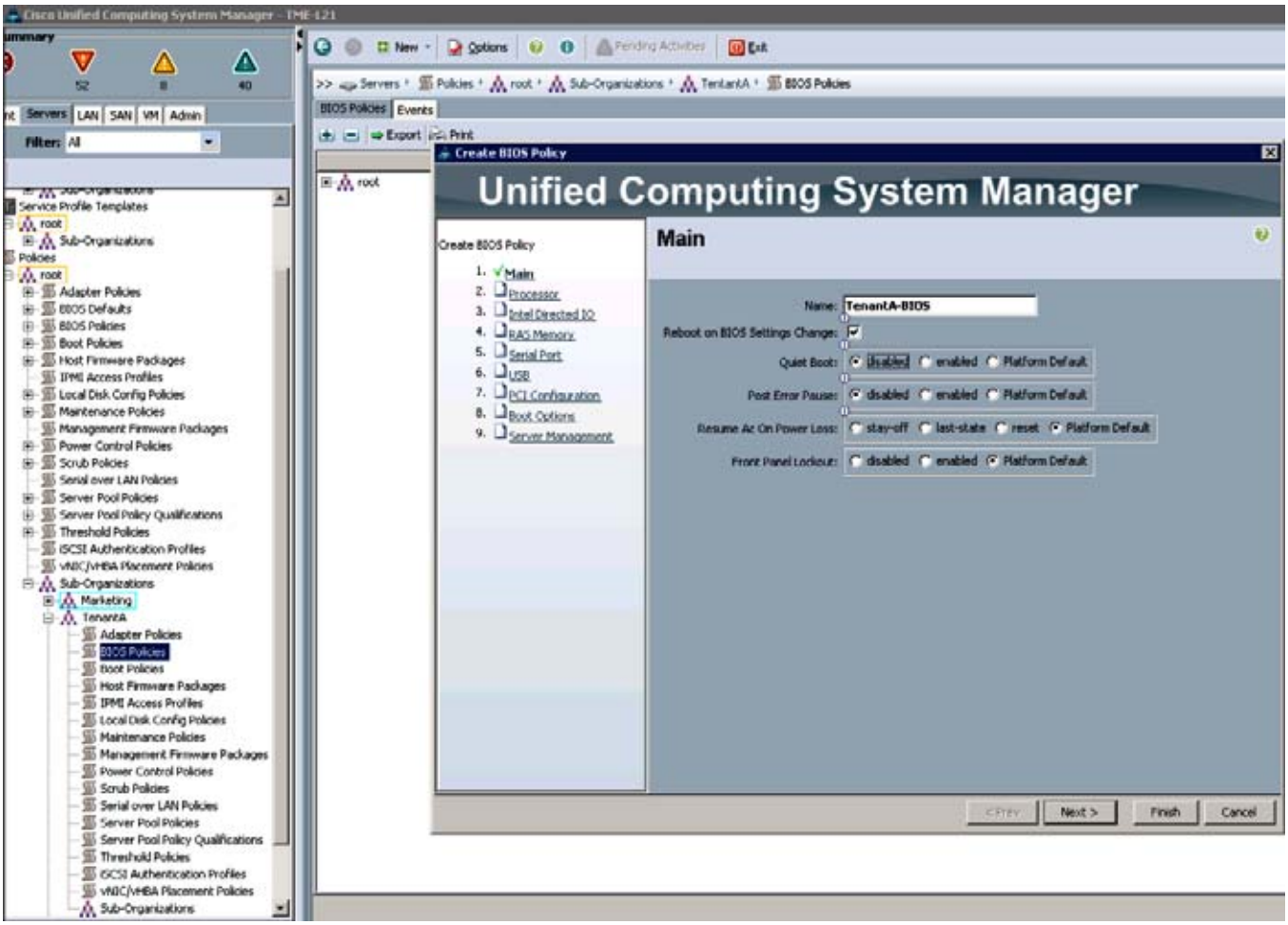
サーバ BIOS ポリシーの作成

以下の手順では、Cisco UCS 環境用のサーバ BIOS ポリシーの作成の詳細を説明します。

組織 Tenant A に対して作成済みのユーザ TenantA-Admin を使用して Cisco UCS Manager にログインします。

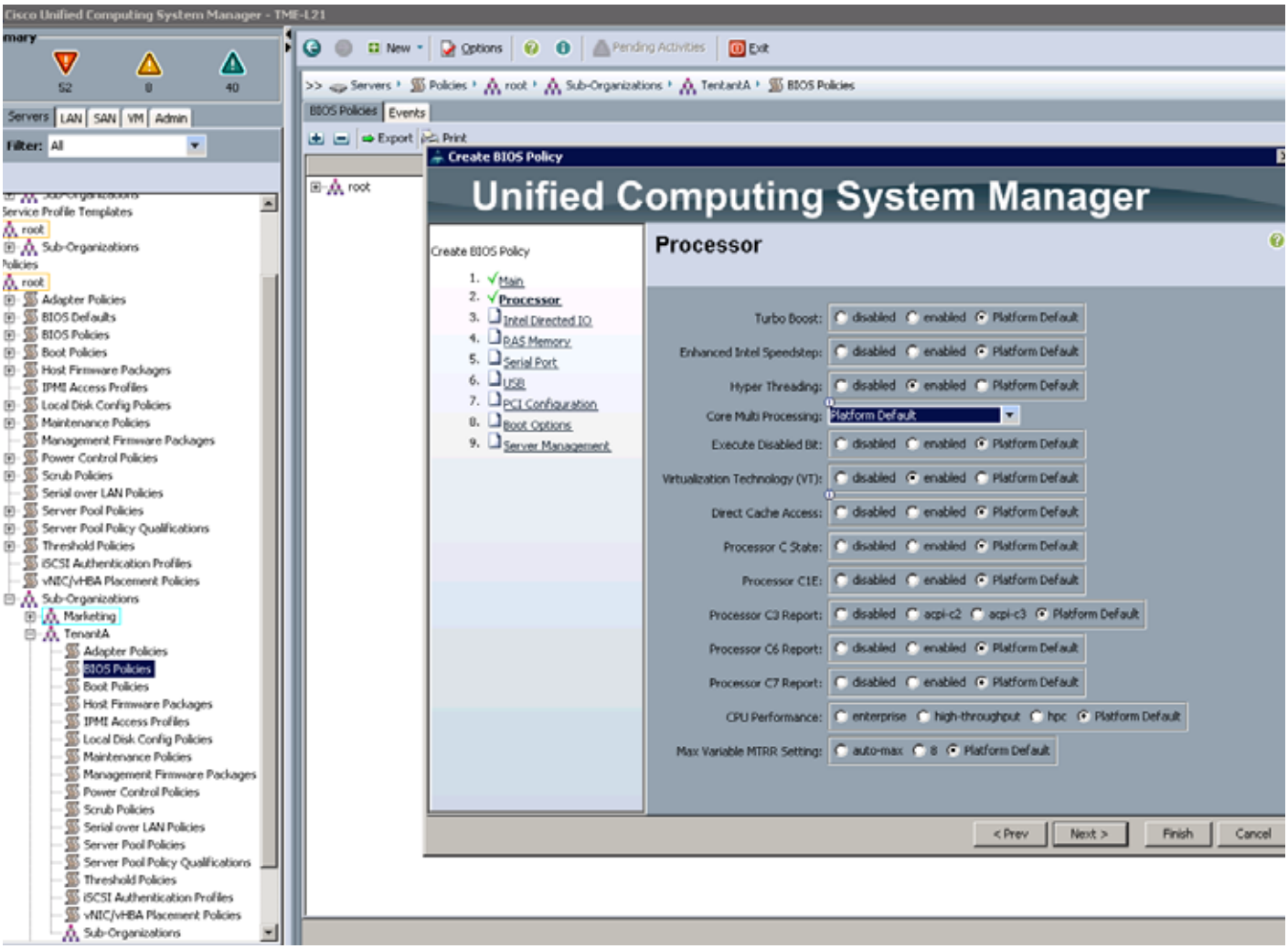
8. [Server] タブをクリックします。
9. [Pools] > [Sub-Organizations] を選択します。
10. [TenantA] を展開し、[BIOS Policies] を選択します。
11. [BIOS Policies] を右クリックして [Create BIOS Policy] を選択します。
12. BIOS ポリシー名として TenantA-BIOS を入力します。
13. [Reboot on BIOS Setting Change] チェック ボックスにチェックを入れます。
14. [Quiet Boot] プロパティを [Disabled] に変更します。

図 103　　BIOS ポリシー属性の定義



15. [Next] をクリックします。
16. [Hyper Threading] で [Enabled] オプション ボタンをクリックします。
17. [Virtualization Technology (VT)] で [Enabled] オプション ボタンをクリックします。
18. デフォルト設定を採用して、[Finish] をクリックします。
19. [OK] をクリックします。

図 104　　プロセッサ属性の設定



サーバ ファームウェア ポリシーの作成

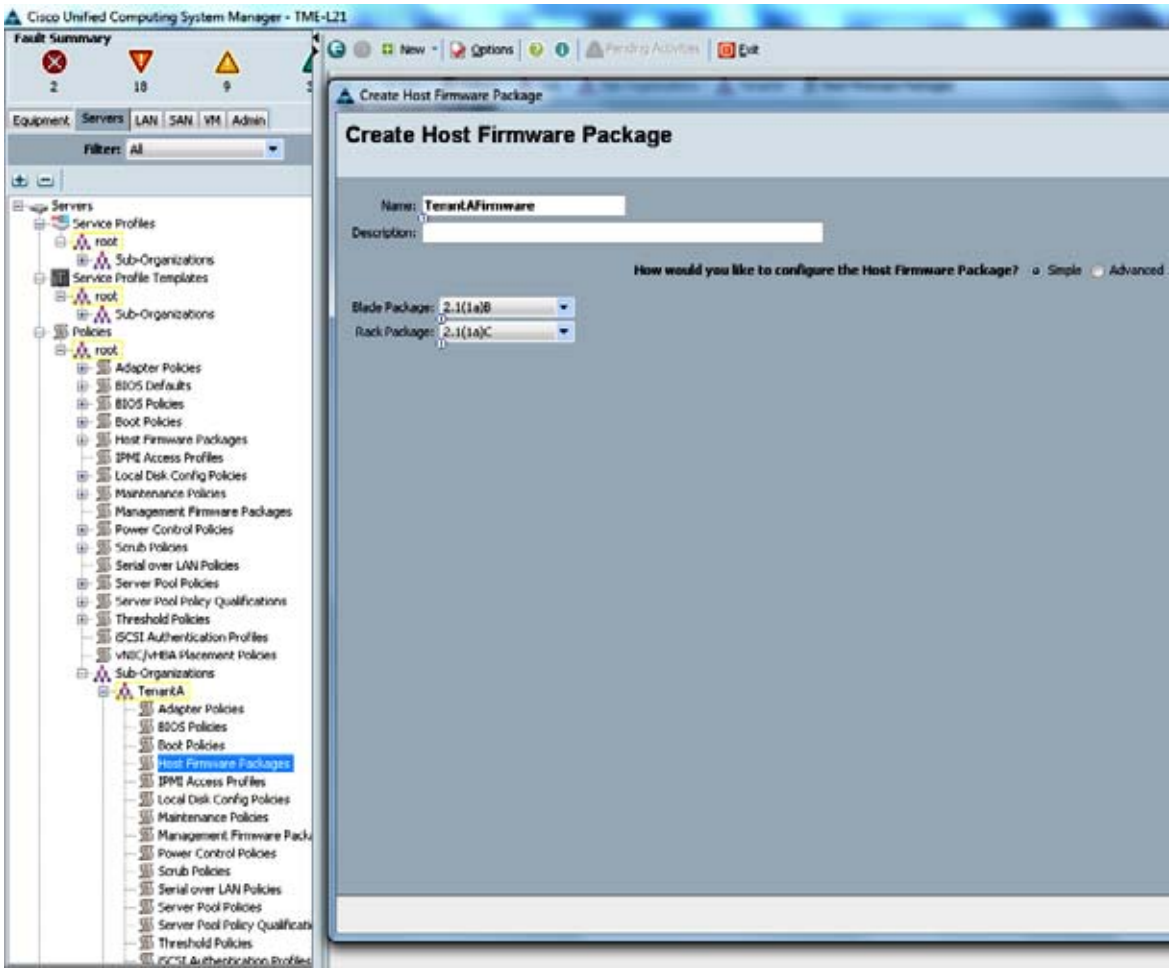
以下の手順では、Cisco UCS 環境用のサーバ BIOS ポリシーの作成の詳細を説明します。

組織 Tenant A に対して作成済みのユーザ TenantA-Admin を使用して Cisco UCS Manager にログインします。

1. [Server] タブをクリックします。
2. [Pools] > [Sub-Organizations] を選択します。
3. [TenantA] を展開し、[Host Firmware Packages] を選択します。
4. [Host Firmware Packages] を右クリックし、[Create] を選択します。
5. BIOS ポリシー名として TenantAFirmware を入力します。
6. [How would you like to configure the Host Firmware Package?] で [Simple] オプション ボタンをクリックします。
7. [Blade Package] および [Rack Package] で最新の Cisco UCS パッケージを選択します。

8. [OK] をクリックします。

図 105　　ホスト ファームウェア パッケージの設定



ローカル ディスク設定ポリシーの作成

以下の手順では、問題となっているサーバにローカル ディスクがない場合に必要となる、Cisco UCS 環境用のローカル ディスク設定の作成について詳しく説明します。

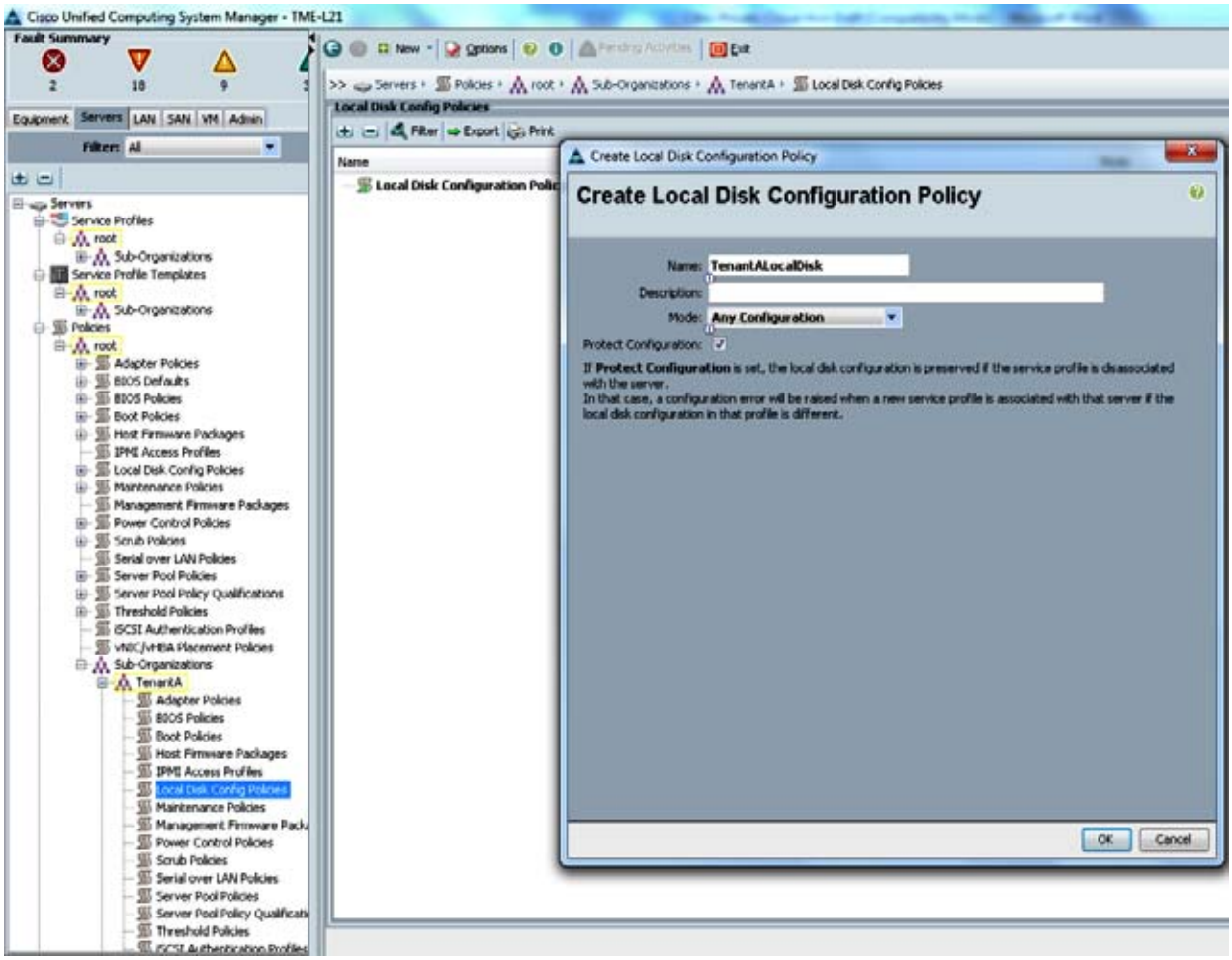
（注）　このポリシーは、ローカル ディスクを含むブレードでは使用しないでください。

組織 Tenant A に対して作成済みのユーザ TenantA-Admin を使用して Cisco UCS Manager にログインします。

1. [Server] タブをクリックします。
2. [Pools] > [Sub-Organizations] を選択します。
3. [TenantA] を展開し、[Local Disk Configuration Policy] を選択します。
4. [Local Disk Configuration Policy] を右クリックし、[Create] を選択します。

5. ローカル ディスク設定ポリシー名として TenantALocalDisk と入力します。
6. [Mode] を [Any Configuration] に変更し、[Protect Configuration] チェック ボックスにチェックを入れます。
7. [OK] をクリックしてホスト ファームウェア パッケージの作成を完了します。

図 106　　ローカル ディスク設定ポリシー プロパティの作成



ブート ポリシーの作成

以下の手順では、Cisco UCS 環境用のブート ポリシーの作成の詳細を説明します。以下の指示は、各ストレージ コントローラの 0c ポートがファブリック A に接続され、各ストレージ コントローラの 0d ポートがファブリック B に接続されている環境に適用します。

（注） このマニュアルでは、2 つのブート ポリシーを作成し、1 つ目は ESXi 5.1 ホスト用、2 つ目は Baremetal RHEL 6.3 ホスト用です。

1 つ目のブート ポリシーは FCoE ターゲットを介して ESXi 5.1 をブートするための SAN Boot オプションを定義します。

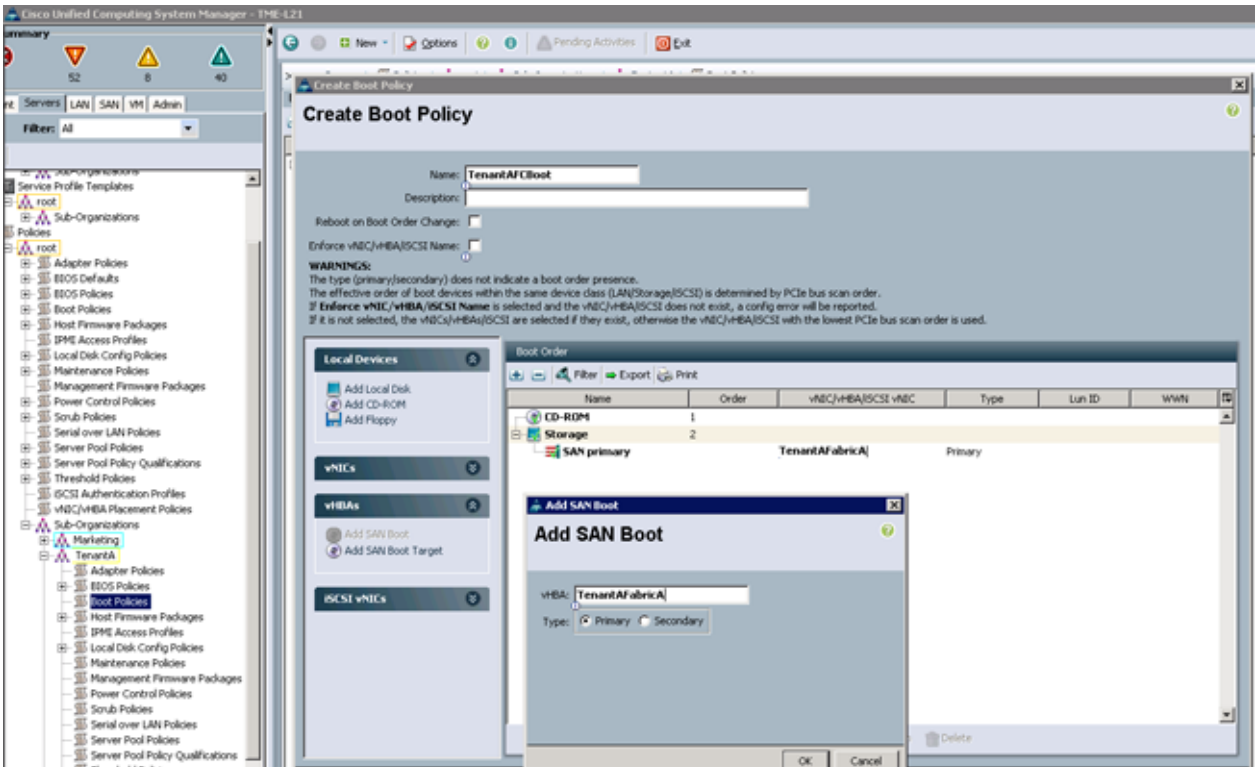
2 つ目のブート ポリシーは FCoE ターゲットを介して Baremetal RHEL 6.3 をブートするための PXE Boot オプションを定義します。

SAN ブート ポリシーは ESXi 5.1 ホスト用です。

組織 Tenant A に対して作成済みのユーザ TenantA-Admin を使用して Cisco UCS Manager にログインします。

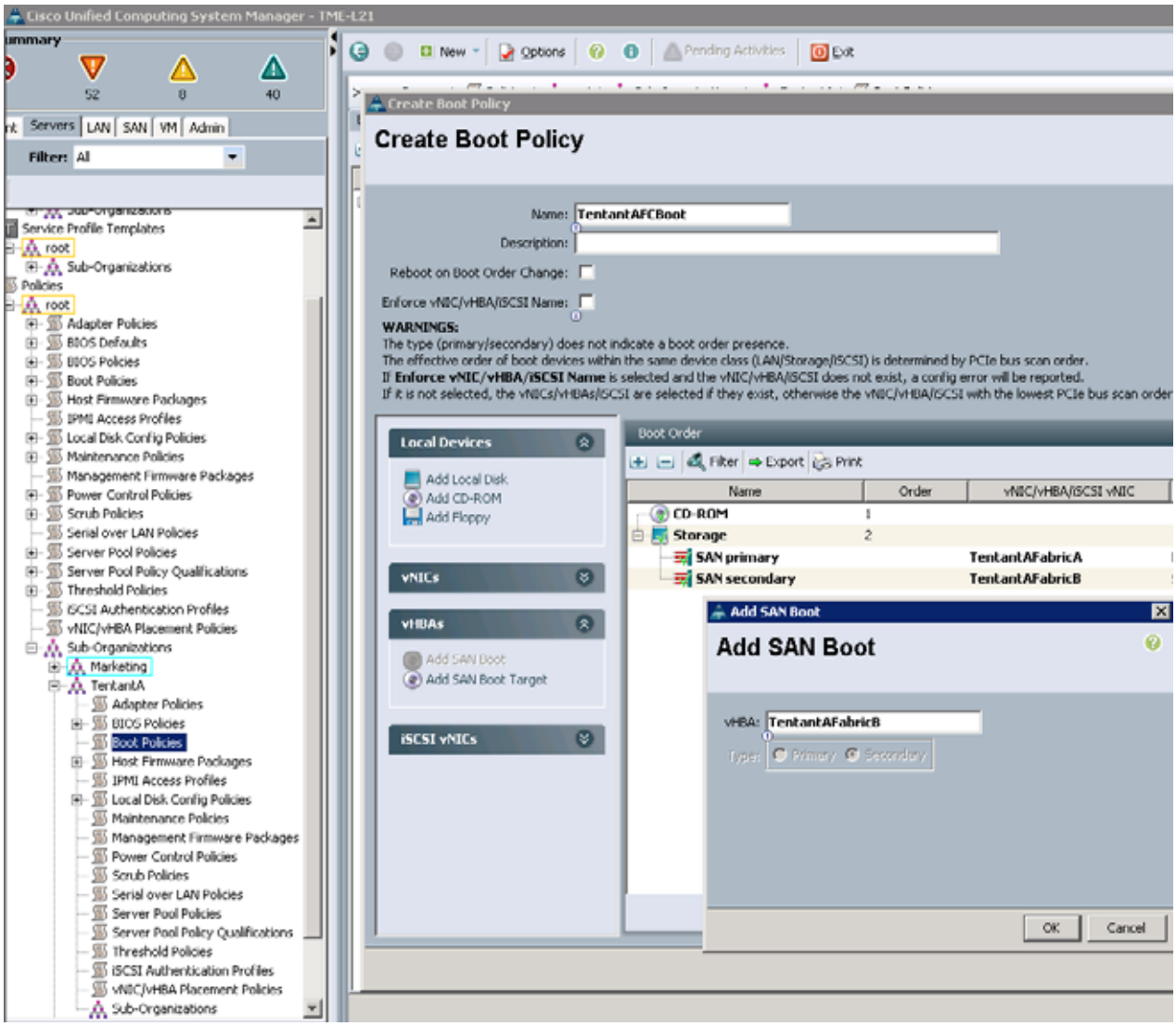
1. [Server] タブをクリックします。
2. [Pools] > [Sub-Organizations] を選択します。
3. [TenantA] を展開し、右ペインの [Policies] タブを選択します。
4. [Boot Policies] サブ タブをクリックします。
5. 右ペインの右端にある [+] 記号をクリックし、ブート ポリシーを作成します。
6. [Name] フィールドに TenantAFCBoot と入力します。
7. （任意）ブート ポリシーの説明を入力します。
8. [Reboot on Boot Order Change] はチェックを入れずそのままにし、[Enforce vNIC/vHBA Name] のチェックを外します。
9. [Local Devices] ドロップダウン リスト メニューを展開し、[Add CD-ROM] を選択します。
10. [vHBAs] ドロップダウン リスト メニューを展開し、[Add SAN Boot] を選択します。
11. [Add SAN Boot] ウィンドウの [vHBA] フィールドに TenantAFabricA と入力します。
12. [Primary] がタイプとして選択されていることを確認します。
13. [OK] をクリックして、SAN ブート イニシエータを追加します。

図 107　　プライマリ SAN ブート内の vHBA 属性の定義



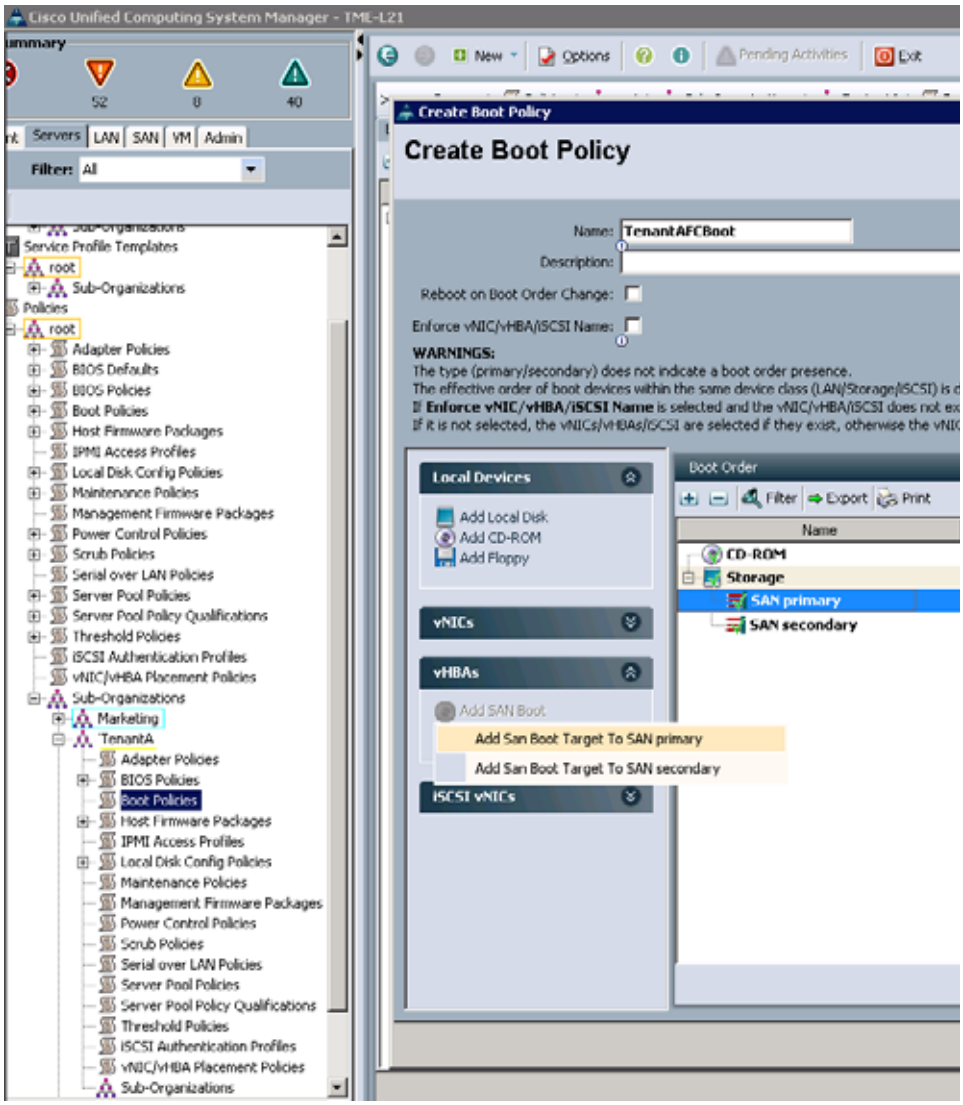
14. セカンダリ FC ブート パスに対する SAN FCboot イニシエータのために [Add SAN Boot] をクリックします。
15. [Add SAN Boot] ウィンドウの [vHBA] フィールドに TenantAFabricB と入力します。
16. [OK] をクリックして、SAN ブート イニシエータを追加します。

図 108　　セカンダリ SAN ブート内の vHBA 属性の定義



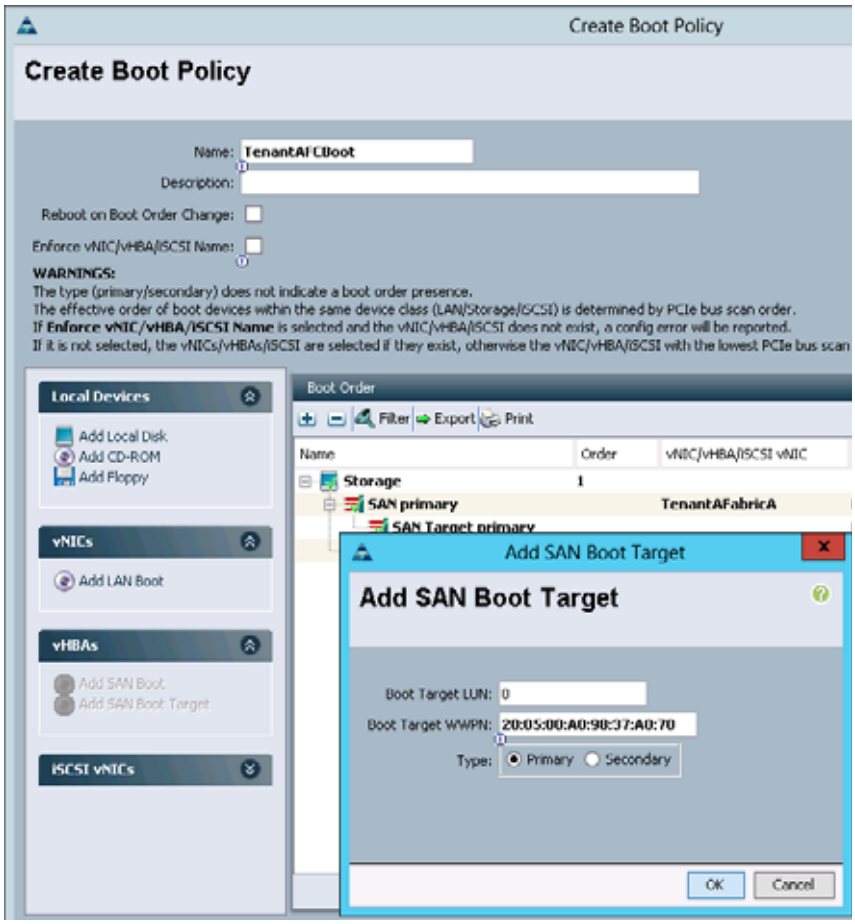
17. 右ペインの [Boot Order] の下で、[Storage] ツリーの下の [SAN Primary] を選択します。
18. [vHBA] ドロップダウン メニューから、[Add SAN Boot] > [Add San Boot Target To SAN Primary] を選択します。

図 109　　SAN ブート ターゲットの追加



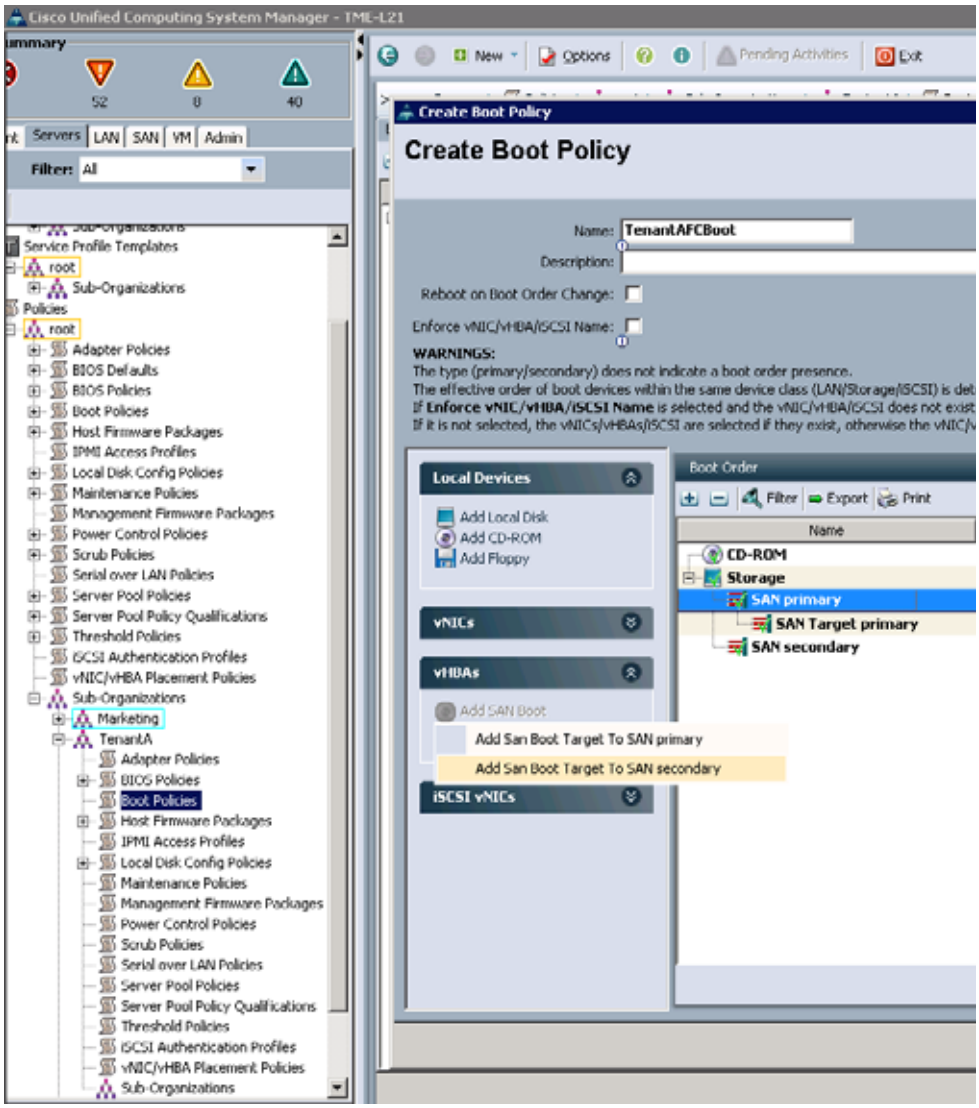
19. [Boot Target LUN] には値 0 を入力します。
20. コントローラ A のプライマリ FC アダプタ インターフェイス 0c の WWPN を入力します。WWPN の情報を得るには、コントローラ A にログインしてコマンド ラインで network interface show コマンドを入力します。
21. FC のノード名ではなく、0c に対する FC ポート名を使用してください。
22. タイプは [Primary] のままにします。
23. [OK] をクリックして、SAN ブート ターゲットを追加します。

図 110　ブート ターゲット LUN および WWPN 値の追加



24. 右ペインの [Boot Order] の下で、[Storage] ツリーの下の [SAN Primary] を選択します。
25. [vHBA] ドロップダウン メニューから、[Add SAN Boot] > [Add San Boot Target to SAN Secondary] を選択します。

図 111　セカンダリ SAN への SAN ブート ターゲットの追加

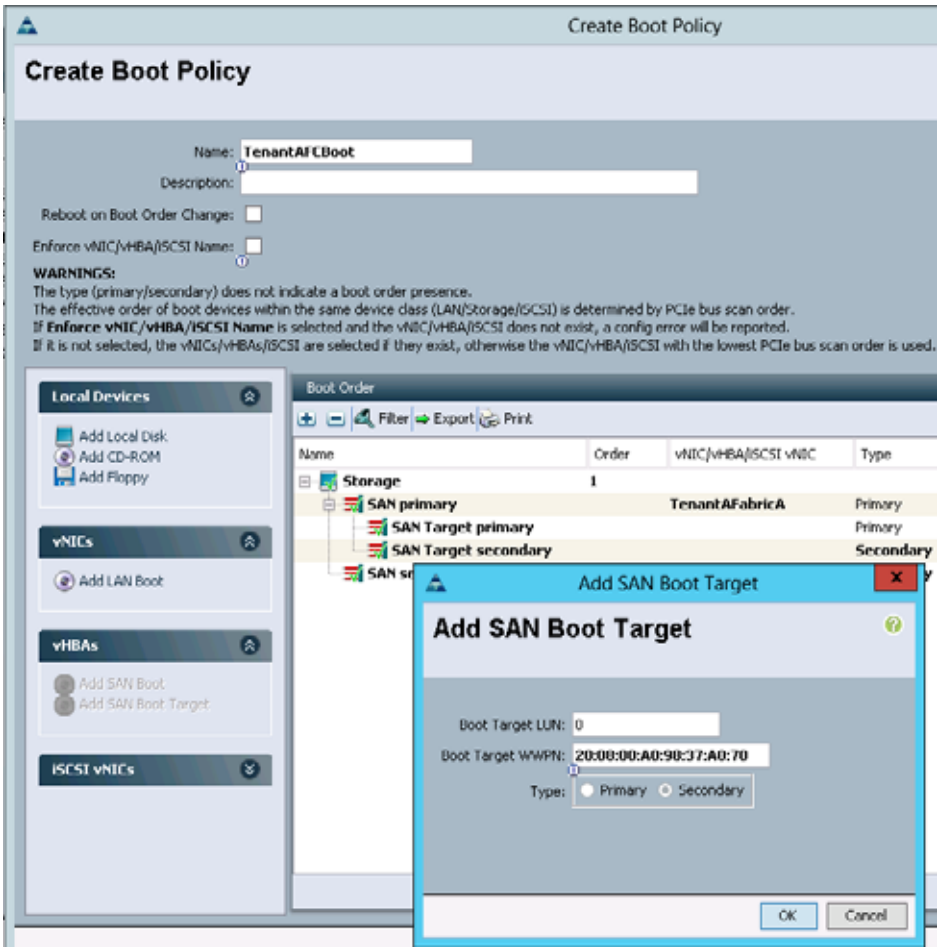


26. [Boot Target LUN] には値 0 を入力します。
27. コントローラ B のプライマリ FC アダプタ インターフェイス 0c の WWPN を入力します。WWPN の情報を取得するには、コントローラ B にログインしてコマンド ラインで network interface show コマンドを入力します。

（注）　FC のノード名ではなく、ポート 0c に対する FC ポート名を使用してください。

28. [OK] をクリックして、SAN ブート ターゲットを追加します。
29. [vHBA] ドロップダウン メニューの下の [Add SAN Boot] を選択します。
30. [Add SAN Boot] ウィンドウの [vHBA] フィールドに TenantAFabricB と入力します。
31. タイプは自動的に [Secondary] に設定され、グレー表示されます。これは正常です。
32. [OK] をクリックして、SAN ブート ターゲットを追加します。

図 112　SAN ブート セカンダリ ターゲット プロパティの定義

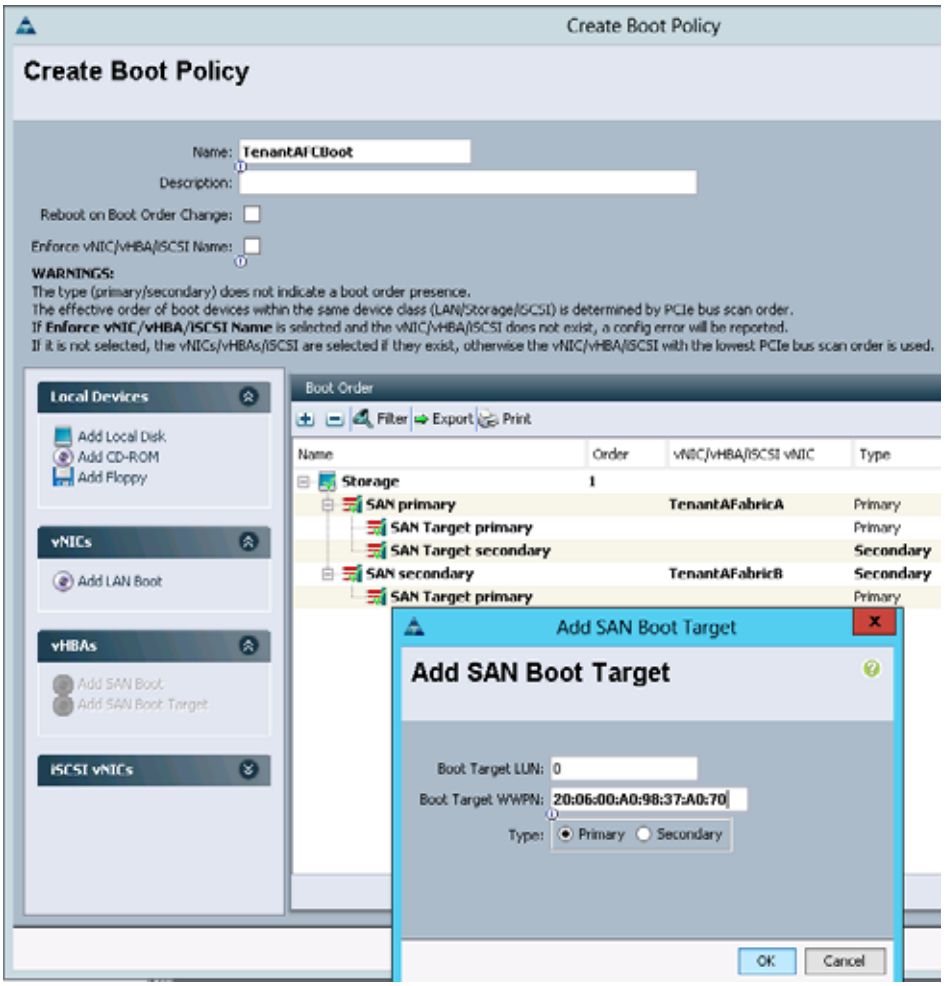


33. 右ペインの [Boot Order] の下で、[Storage] ツリーの下の [SAN Secondary] を選択します。
34. [vHBA] ドロップダウン メニューから、[Add SAN Boot] > [Add San Boot Target To SAN Primary] を選択します。
35. [Boot Target LUN] には値 0 を入力します。
36. コントローラ A のプライマリ FC アダプタ インターフェイス 0c の WWPN を入力します。この情報を得るには、コントローラ A にログインして network interface show コマンドを実行します。

（注）　FC のノード名ではなく、0c に対する FC ポート名を使用してください。

37. タイプは [Primary] のままにします。
38. [OK] をクリックして、SAN ブート ターゲットを追加します。

図 113　　SAN ブート ターゲット プライマリ プロパティの定義

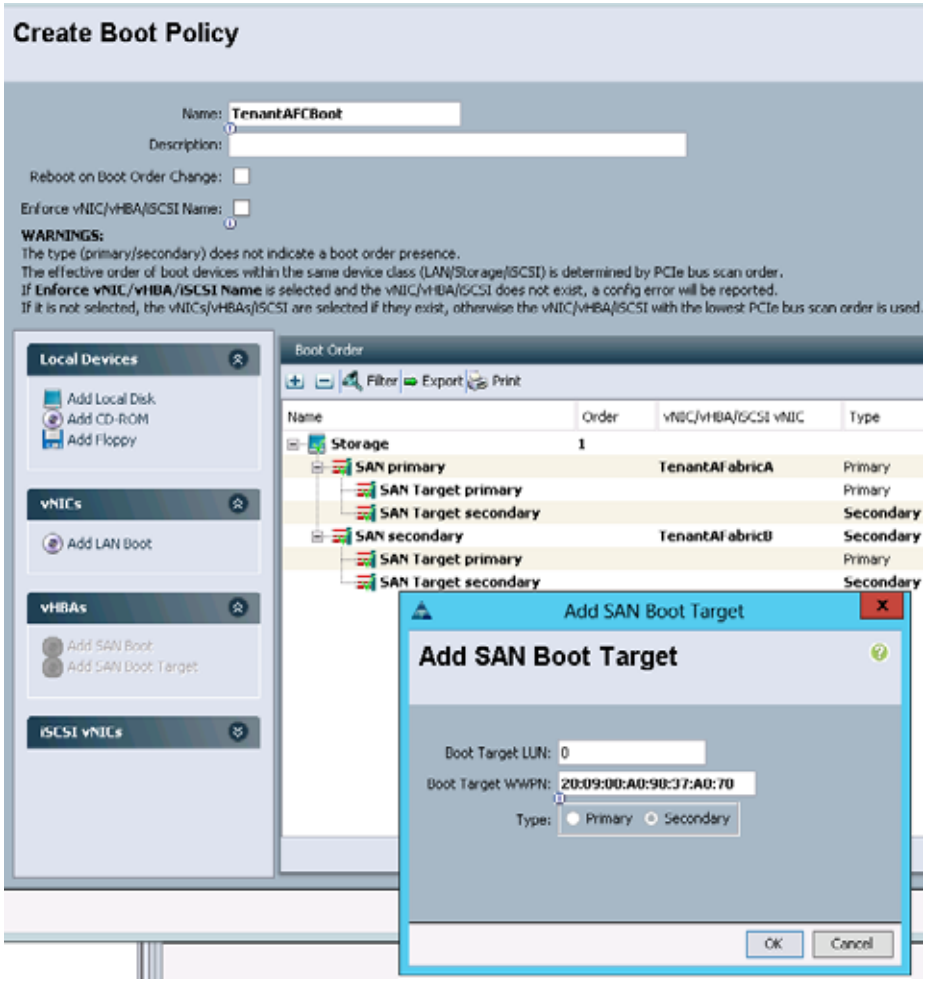


39. 右ペインの [Boot Order] の下で、[Storage] タブの下の [SAN Secondary] を選択します。
40. [vHBA] メニューから、[Add SAN Boot] > [Add San Boot Target To SAN secondary] を選択します。
41. [Boot Target LUN] には値 0 を入力します。
42. コントローラ B のプライマリ FC アダプタ インターフェイス 0c の WWPN を入力します。この情報を得るには、コントローラ B にログインして network interface show コマンドを実行します。

（注）　FC のノード名ではなく、ポート 0c に対する FC ポート名を使用するようにしてください。

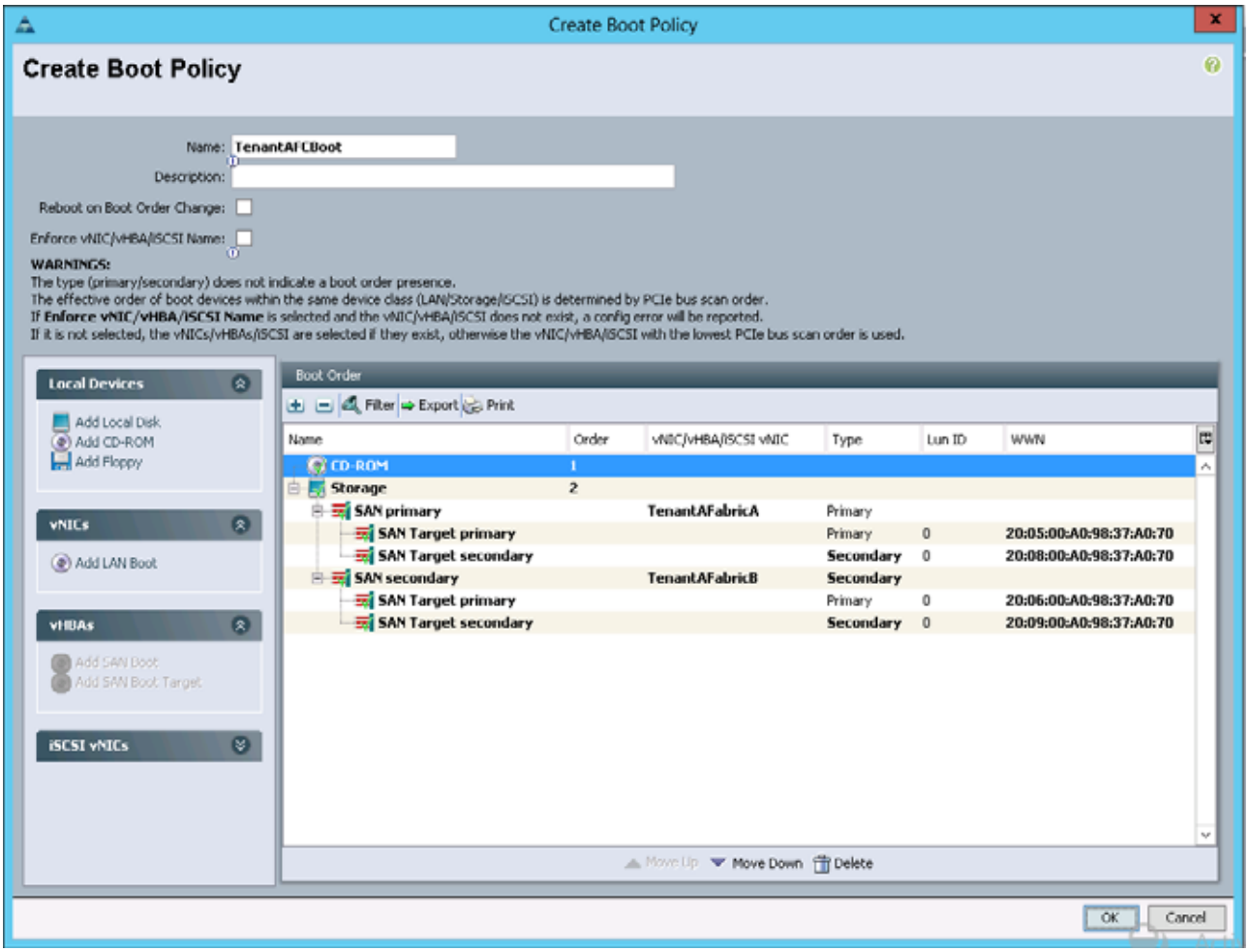
43. [OK] をクリックして、SAN ブート ターゲットを追加します。
44. [vHBA] ドロップダウン メニューの下の [Add SAN Boot] を選択します。
45. 表示される [Add SAN Boot] ウィンドウの [vHBA] フィールドに TenantAFabricB と入力します。
46. タイプは自動的に [Secondary] に設定され、グレー表示されます。
47. [OK] をクリックして、SAN ブート ターゲットを追加します。

図 114　SAN ブート セカンダリ ターゲット プロパティの定義



48. 最後の TenantAFCBoot ポリシーです。

図 115　TenantAFCBpoot SAN ブートポリシー プロパティ

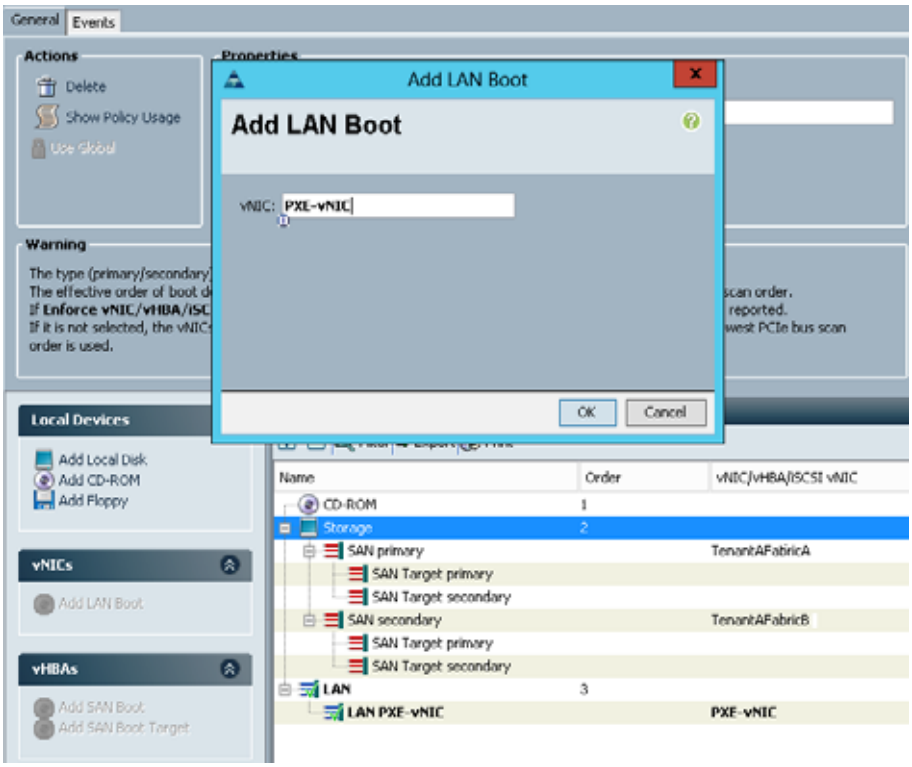


Baremetal RHEL 6.3 ホスト用 PXE ブート ポリシー

PXE ブート ポリシーを設定するには、以下の手順を実行します。

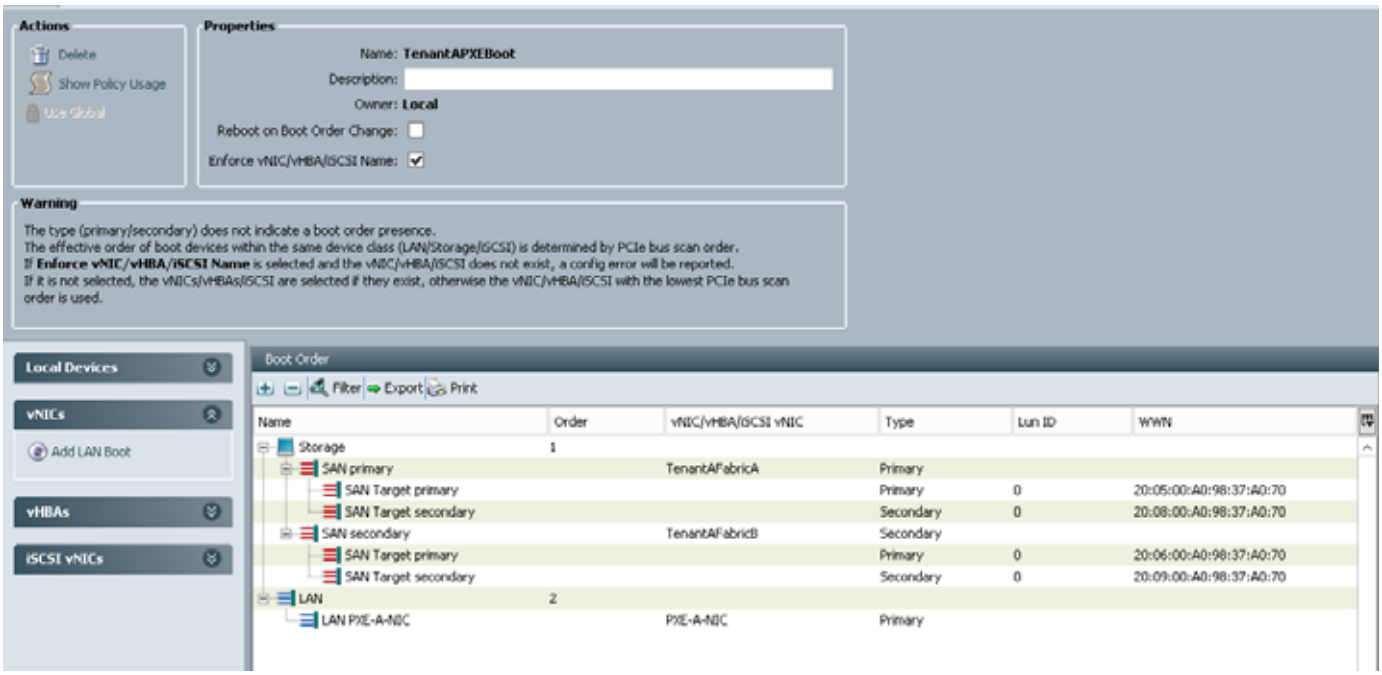
1. 上記の ESXi 5.1 ホスト用の SAN ブート ポリシーで定義した 2 つの vHBA を使用して、SAN ブート ポリシーの TenantA Org 上にブート ポリシー TenantAPXEBoot をプライマリ タイプとセカンダリ タイプで作成します。
2. [Add LAN Boot] オプションで、[vNIC] フィールドに PXE-A-NIC を入力します（PXE-A-NIC スタティック vNIC 名は LAN ブート名（PXE-A-NIC）と一致していることを確認します）。
3. [Enforce vNIC/vHBA/iSCSI Name] チェックボックスにチェックを入れます。

図 116　　FCoE ブート ポリシー プロパティの定義



4. ブート順序で [SAN] を選択し、1 番上に移動します。
5. [Save（保存）] ボタンをクリックします。

図 117　　ブート順序プロパティの定義



ストレージのゾーニング設定

Cisco UCS サービス プロファイルが作成されると（前の手順で）、環境内のインフラストラクチャ ブレードはそれぞれ独自の設定を持ちます。FlexPod 導入を使用して手順を進めるには、各 Cisco UCS ブレードおよび各 NetApp コントローラから固有の情報を収集する必要があります。必要な情報を以下の表に記入してください。

表 18　NetApp コントローラの FC ポートと FC ポート名

NetApp コントローラ	FC ポート	FC ポート名
コントローラ A	0c	50:0a:09:83:8d:93:40:7f
コントローラ B	0c	50:0a:09:83:9d:93:40:7f

（注）　各 NetApp コントローラの CLI で、fcp アダプタを表示するコマンドを入力し、表 19 のリストにある必要な情報を収集します。

表 19　テナント A および B の WWPN の値

Cisco UCS サービス プロファイル名	Fabric-A WWPN	Fabric-B WWPN
TenantA-HostA-Platinum-SLA1	20:00:00:25:b5:01:01:09	20:00:00:25:b5:01:01:08
TenantA-HostB-Platinum-SLA1	20:00:00:25:b5:01:01:07	20:00:00:25:b5:01:01:06

両方のファブリックから WWPN の値を収集するには、Cisco UCS Manager の GUI を起動し以下の手順を実行します。

1. 左ペインで [Servers] タブを選択します。
2. [Servers] > [Service Profiles] > [root] を選択します。
3. [TenantA] をクリックします。
4. 各サービス プロファイルをクリックし、次に右の [Storag] タブをクリックします。
5. 右のウィンドウに表示される、両方のサービス プロファイルの Fabric-A-HBA と Fabric-B-HBA の両方に対する WWPN 情報を記録します。

VSAN の作成、FC ポートの割り当て、FC ポートの起動

以下の手順では、Nexus ネットワーク クラウド環境の UCS と NetApp ストレージで SAN ブートを行うための FC イニシエータおよびターゲット アクセスを提供するために必要なゾーンセットおよびゾーン メンバの設定について詳しく説明します。

（注）　この手順では、Cisco Nexus 5548 と NetApp ストレージ システム間のファイバ チャネル接続をセットアップします。

ゾーンおよびゾーンセットの作成

以下の手順では、すべてのターゲット ポートを使用したプライマリおよびセカンダリのブート パスに対するゾーン メンバおよびゾーンセットの設定を詳しく説明します。

Cisco Nexus 5548 A

各サービス プロファイルに対してストレージ ゾーンおよびゾーンセットを作成するには、Cisco Nexus スイッチにログインし、以下の手順に並んでいる CLI コマンドを入力します。

1. ゾーンを作成します。
2. zone name TenantA-HostA-Plantinum-SLA1 vsan 200 と入力します。
3. member pwwn 20:00:00:25:b5:01:01:01 と入力します。
4. member pwwn 20:05:00:a9:98:37:a0:70 と入力します。
5. member pwwn 20:06:00:a9:98:37:a0:70 と入力します。
6. exit と入力します。
7. zone name TenantA-HostB-Plantinum-SLA1 vsan 200 と入力します。
8. member pwwn 20:00:00:25:b5:01:01:03 と入力します。
9. member pwwn 20:05:00:a9:98:37:a0:70 と入力します。
10. member pwwn 20:06:00:a9:98:37:a0:70 と入力します。
11. exit と入力します。
12. zone name TenantA-BareMetalHostA-Plantinum-SLA1 vsan 200 と入力します。
13. member pwwn 20:00:00:25:b5:04:00:06 と入力します。
14. member pwwn 20:05:00:a9:98:37:a0:70 と入力します。
15. member pwwn 20:06:00:a9:98:37:a0:70 と入力します。
16. exit と入力します。

（注） 最初の Cisco UCS サービス プロファイルのプライマリ パスに対するゾーンを作成したら、ゾーンを整理または管理するゾーンセットを作成します。

17. ゾーンセットを作成し、必要なメンバを追加します。
18. zoneset name TenantA vsan 200 と入力します。
19. member TenantA-HostA-Plantinum-SLA1 と入力します。
20. member TenantA-HostB-Plantinum-SLA2 と入力します。
21. exit と入力します。
22. member TenantA-BareMetalHostA-Plantinum-SLA2 と入力します。
23. exit と入力します。
24. ゾーンセットをアクティブ化します。
25. zoneset activate name TenantA vsan 200 と入力します。
26. exit と入力します。
27. copy run start と入力します。以下はこのコマンドの出力です。

```
N5548-L21-A# sh zoneset vsan 200
zoneset name TenantA vsan 200
```

```
zone name TenantA-HostA-Plantinum-SLA1 vsan 200
  pwwn 20:00:00:25:b5:01:01:01
    pwwn 20:05:00:a9:98:37:a0:70
    pwwn 20:06:00:a9:98:37:a0:70
zone name TenantA-HostB-Plantinum-SLA1 vsan 200
  pwwn 20:00:00:25:b5:01:01:03
    pwwn 20:05:00:a9:98:37:a0:70
    pwwn 20:06:00:a9:98:37:a0:70
zone name TenantA-BareMetalHostA-Plantinum-SLA1 vsan 200
  pwwn 20:00:00:25:b5:04:00:06
    pwwn 20:05:00:a9:98:37:a0:70
    pwwn 20:06:00:a9:98:37:a0:70
```

Cisco Nexus 5548 B

1. 各サーバ プロファイル用にゾーンを作成します。
2. zone name TenantA-HostA-Plantinum-SLA1 vsan 300 と入力します。
3. member pwwn 20:00:00:25:b5:01:01:02 と入力します。
4. member pwwn 20:05:00:a9:98:37:a0:70 と入力します。
5. member pwwn 20:06:00:a9:98:37:a0:70 と入力します。
6. exit と入力します。
7. zone name TenantA-HostB-Plantinum-SLA1 vsan 300 と入力します。
8. member pwwn 20:00:00:25:b5:01:01:04 と入力します。
9. member pwwn 20:05:00:a9:98:37:a0:70 と入力します。
10. member pwwn 20:06:00:a9:98:37:a0:70 と入力します。
11. exit と入力します。
12. zone name TenantA-BareMetalHostA-Plantinum-SLA1 vsan 200 と入力します。
13. member pwwn 20:00:00:25:b5:04:00:05 と入力します。
14. member pwwn 20:05:00:a9:98:37:a0:70 と入力します。
15. member pwwn 20:06:00:a9:98:37:a0:70 と入力します。
16. exit と入力します。

（注） 最初の Cisco UCS サービス プロファイルのプライマリ パスに対するゾーンを作成したら、ゾーンを整理または管理するゾーンセットを作成します。

17. ゾーンセットを作成し、必要なメンバを追加します。
18. zoneset name TenantA vsan <300> と入力します。
19. member TenantA-HostA-Plantinum-SLA1 と入力します。
20. member TenantA-HostB-Plantinum-SLA1 と入力します。
21. exit と入力します。
22. member TenantA-BareMetalHostA-Plantinum-SLA2 と入力します。
23. exit と入力します。
24. ゾーンセットをアクティブ化します。
25. zoneset activate name TenantA vsan <300> と入力します。
26. exit と入力します。

27. copy run start と入力します。以下はこのコマンドの出力です。

```
N5548-L21-A# sh zoneset vsan 10
zoneset name TenantA vsan 10

  zone name TenantA-HostA-Plantinum-SLA1 vsan 300
      pwwn 20:00:00:25:b5:01:01:02
        pwwn 20:05:00:a9:98:37:a0:70
        pwwn 20:06:00:a9:98:37:a0:70
  zone name TenantA-HostB-Plantinum-SLA1 vsan 300
        pwwn 20:00:00:25:b5:01:01:04
        pwwn 20:05:00:a9:98:37:a0:70
        pwwn 20:06:00:a9:98:37:a0:70
  zone name TenantA-BareMetalHostA-Plantinum-SLA1 vsan 200
    pwwn 20:00:00:25:b5:04:00:05
      pwwn 20:05:00:a9:98:37:a0:70
      pwwn 20:06:00:a9:98:37:a0:70
```

Citrix CloudPlatform ホスト定義

ホストとは、ゲストの仮想マシンを実行するためにコンピューティング リソースを提供する単一のコンピュータのようなものです。ハイパーバイザ ソフトウェアは、ゲストの VM を管理するために各ホストにインストールされます。シスコの Cisco UCS Manager は VMware ESXi サーバのコンピューティング、ストレージ、およびネットワーク クラウド インフラストラクチャの設計を理想的に定義します。これらは、クラウド プロバイダーによって定義されるサービスレベル合意書（SLA）に基づくサービスをホストするマルチテナントに必要な機能です。

ホスト定義設計コンポーネントについて説明します。

コンピューティング

コンピューティング定義には CPU、メモリ、および入出力コンポーネントなどがあり、パフォーマンス、動的スケーリング、高可用性、管理性、およびこれらのデータ ポイントに基づくプロビジョニングの面でマルチテナント サービス（アプリケーション）機能をサポートするために必要で、サービス レベルは関連費用で定義されています。

これらのサービス レベルが満たされるように、UCS では動的なスケーリング要求を処理するためにプロビジョニング時間を高速化する Cisco UCS Manager などのさまざまなサービス レベルに対する CPU 速度やメモリ容量定義などの資格情報ポリシーを持つサービス プールを提供します。UCS は、常にシングル ポイント障害が存在しないマルチテナント サービス データ トラフィックを処理する拡張メモリ技術、およびイーサネット チャネルのある 80 G 入出力仮想インターフェイス アダプタを提供し、クラウド環境で高可用性を実現します。

ストレージ

ストレージ定義は、マルチテナント ストレージ要件をサポートするネットワーク スケーラビリティ、データ分離、高可用性、およびパフォーマンスに関与します。これらのデータ ポイントに基づいて、サービス レベルが関連費用とともに定義されます。

ストレージ要件を満たすために、UCS ではマルチテナント クラウド環境でストレージ データ分離を提供するために、仮想論理 SAN を用意しています。高可用性を提供するために、UCS ではすべての物理的 FC ポート障害に対応できる SAN ポート チャネルを提供し、またスケーラビリティを動的に拡張す

ることができます。コンピュート ホスト側では、帯域幅サービス レベル要件に基づいて、各仮想ホスト バス アダプタ（vHBA）のストレージ データが SAN ピン グループを使用して特定の SAN ポート チャネルに固定されます。

ネットワーク

ネットワーク定義は、マルチテナント ストレージ要件をサポートするサービスの品質、高可用性、スケーラビリティ、およびパフォーマンスに関与します。これらのデータ ポイントに基づいて、サービス レベルが関連費用とともに定義されます。

ネットワーク定義を満たすために、UCS ではマルチテナント クラウド環境でネットワーク データ分離を提供するために、仮想ポート チャネルおよび仮想 LAN を用意しています。高可用性を実現するために、UCS ではすべての物理的ポート障害に対応できるイーサネット ポート チャネルを提供し、またスケーラビリティを動的に拡張することができます。コンピュート ホスト側では、帯域幅サービス レベル要件に基づいて、各仮想イーサネット アダプタ（vNIC）のネットワーク データが LAN ピングループを使用して特定の LAN ポート チャネルに固定されます。

サービス プロファイル テンプレートの作成

サービス プロファイルは単一ブレード サーバのシステム設定情報を示しますが、対象にしているブレードの実体を知る必要はありません。プロファイル オブジェクトには、識別情報やネットワーク情報などのサーバの固有情報が含まれています。つまり、プロファイルは一度に単一のブレードと関連付けることができます。コンピュート、ストレージ、ネットワークの各インフラストラクチャ コンポーネントはすべて、UCS サービス プロファイル テンプレートを使用してクラウド ホスト サーバにプロビジョニングされ、設定され、適用されています。

サービス プロファイル テンプレートは単一の管理設定ウィンドウで、すべてのインフラストラクチャ コンポーネントをサーバ プロファイルの形式で複数のクラウド ホストに定義、設定、および適用できます。

サービス レベルに基づいた異なる種類のサービス プロファイル テンプレートの作成手順を以下に示します。これらは、個別のクラウド テナント ホストに適用するサービス プロファイルのインスタンスを作成するために後で使用することができます。

この項では、次の作業を詳しく説明します。

- コンピュート定義
- ネットワーク定義
- ストレージ定義

コンピュート定義

サービス プロファイル テンプレートの作成

この項では、2 つのサービス プロファイル テンプレート、1 つ目はハイパーバイザ ESX ホスト用、2 つ目は Baremtal RHEL オペレーティング システム用の作成について詳しく説明します。

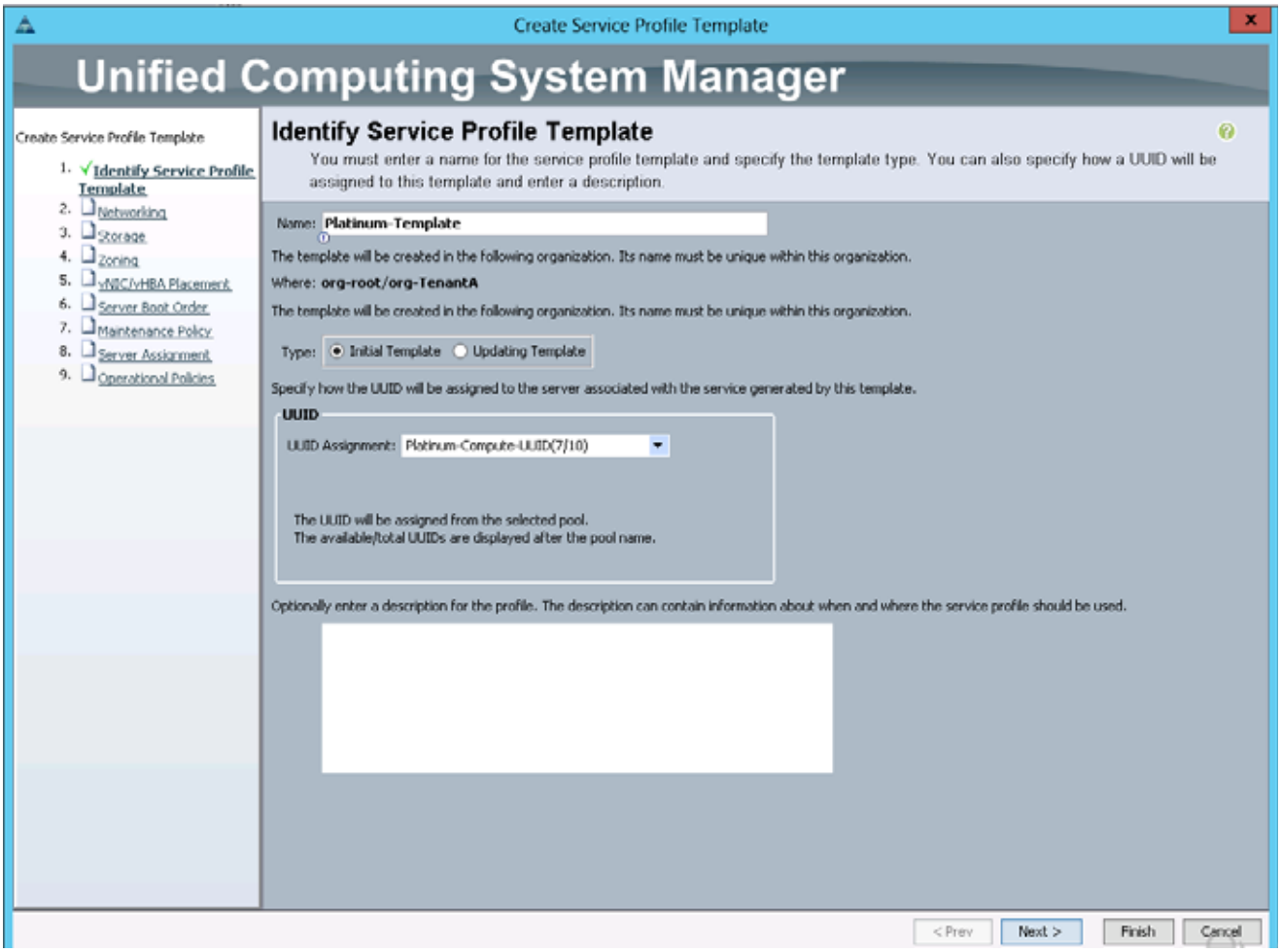
ハイパーバイザ ESX ホスト サービス プロファイル テンプレート

組織 Tenant A に対して作成済みのユーザ TenantA-Admin を使用して Cisco UCS Manager にログインします。

1. 左ペインで、[Servers] タブをクリックします。

2. [Service Profiles] > [Sub-Organizations] を選択します。TenantA を強調表示します。
3. 右ペインの [General] タブ上の [Create Service Profile Templates] を選択します。
4. [Create Service Profile Template] ウィンドウが表示されます。
5. サービス プロファイル テンプレートの名前を Platinum-Template にします。
6. [Initial Template] を選択します。
7. [UUID] セクションで、UUID プールとして [Platinum-Compute-UUID] を選択します。
8. [Next] をクリックして、次のセクションに進みます。

図 118　　サービス プロファイル テンプレートへのユニークな名前の追加



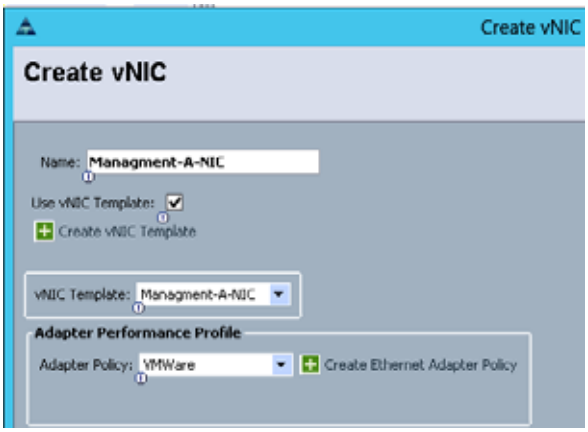
ネットワーク定義

vNIC の作成

1. [Dynamic vNIC Connection Policy] フィールドはデフォルトのままにしておきます。
2. [How would you like to configure LAN connectivity?] で [Expert] を選択します。
3. [Add] アイコンをクリックします（サーバが LAN 接続に使用する vNIC の必要数を指定します）。

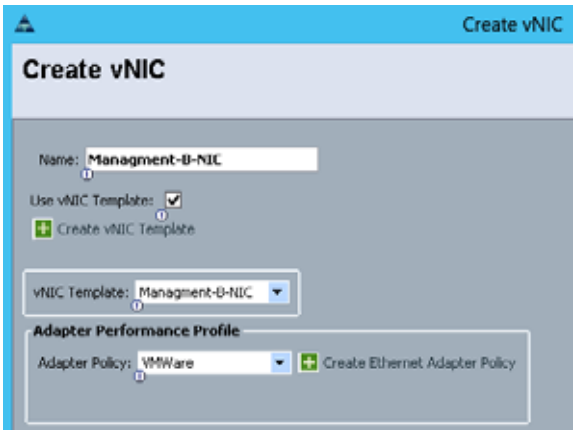
4. [Create vNIC] ウィンドウが開きます。
5. [Name] フィールドに Management-A-NIC と入力します。
6. [Use vNIC Template] チェックボックスを有効にします。
7. [vNIC Template] リスト ボックスの [Management-A-NIC] を選択します。
8. [Adapater Policy] リスト ボックスの [VMWare] を選択します。
9. [OK] をクリックします。

図 119　　管理 A-NIC 用の vNIC プロパティの定義



10. [Add] をクリックします。
11. [Name] フィールドに Management-B-NIC と入力します。
12. [Use vNIC Template] チェックボックスを有効にします。
13. [vNIC Template] リスト ボックスの [Management-B-NIC] を選択します。
14. [Adapater Policy] リスト ボックスの [VMWare] を選択します。
15. [OK] をクリックします。

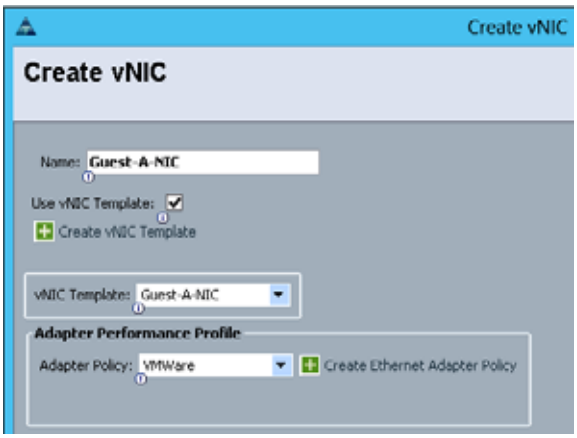
図 120　　管理 B-NIC 用の vNIC プロパティの定義



16. [Add] をクリックします。
17. [Name] フィールドに Guest-A-NIC と入力します。

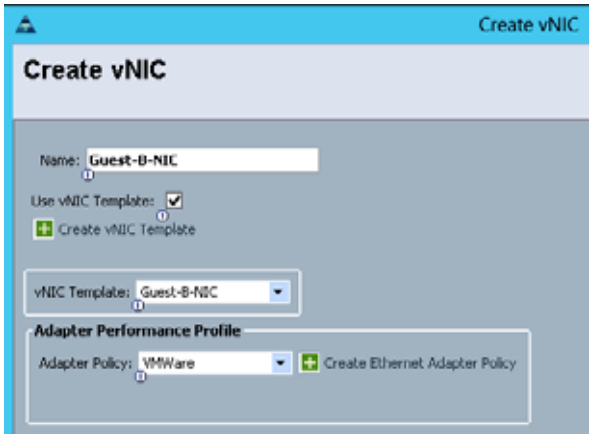
18. [Use vNIC Template] チェックボックスを有効にします。
19. [vNIC Template] リスト ボックスの [Guest-A-NIC] を選択します。
20. [Adapater Policy] リスト ボックスの [VMWare] を選択します。
21. [OK] をクリックします。

図 121　　Guest-A-NIC 用の vNIC プロパティの定義



22. [Add] をクリックします。
23. [Name] フィールドに Guest-A-NIC と入力します。
24. [Use vNIC Template] チェックボックスを有効にします。
25. [vNIC Template] リスト ボックスの [Guest-A-NIC] を選択します。
26. [Adapater Policy] リスト ボックスの [VMWare] を選択します。
27. [OK] をクリックします。

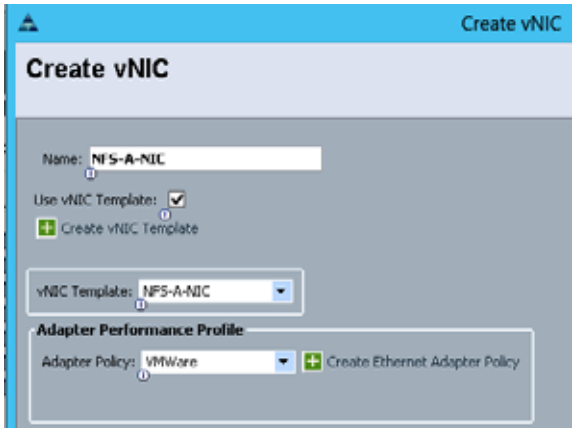
図 122　　Guest-B-NIC 用の vNIC プロパティの定義



28. [Add] をクリックします。
29. [Name] フィールドに NFS-A-NIC と入力します。
30. [Use vNIC Template] チェックボックスを有効にします。
31. [vNIC Template] リスト ボックスの [NFS-A-NIC] を選択します。

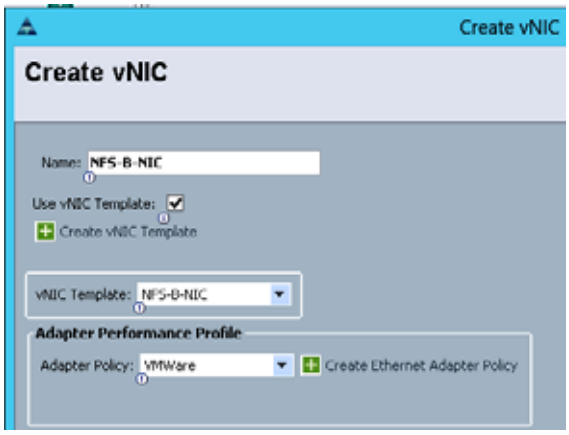
32. [Adapater Policy] リスト ボックスの [VMWare] を選択します。
33. [OK] をクリックします。

図 123　NFS-A-NIC 用の vNIC プロパティの定義



34. [Add] をクリックします。
35. [Name] フィールドに NFS-B-NIC と入力します。
36. [Use vNIC Template] チェックボックスを有効にします。
37. [vNIC Template] リスト ボックスの [NFS-B-NIC] を選択します。
38. [Adapater Policy] リスト ボックスの [VMWare] を選択します。
39. [OK] をクリックします。

図 124　NFS-B-NIC 用の vNIC プロパティの定義



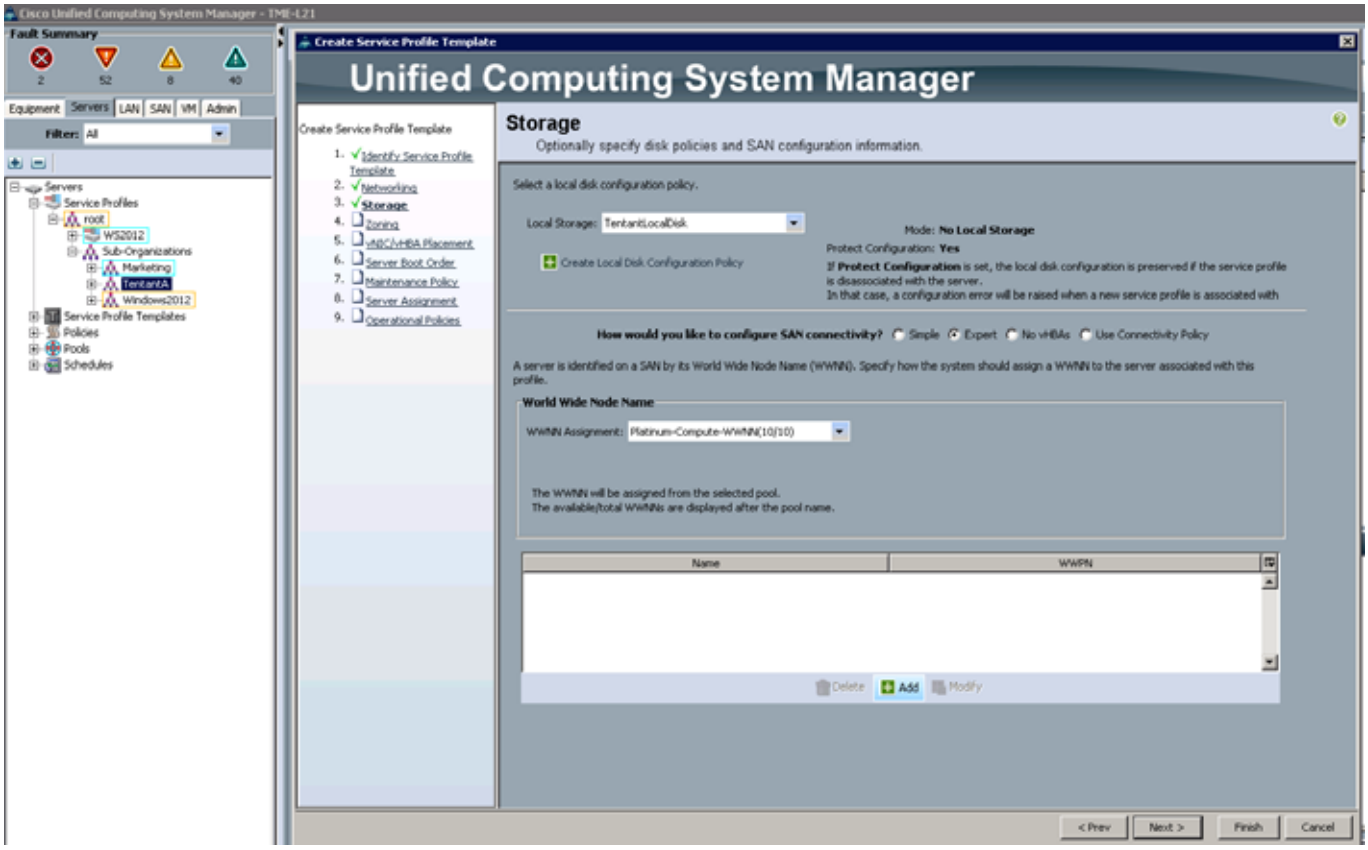
ストレージ定義

vHBA の作成

1. [Local Storage] フィールドで [TenantLocalDisk] を選択します。

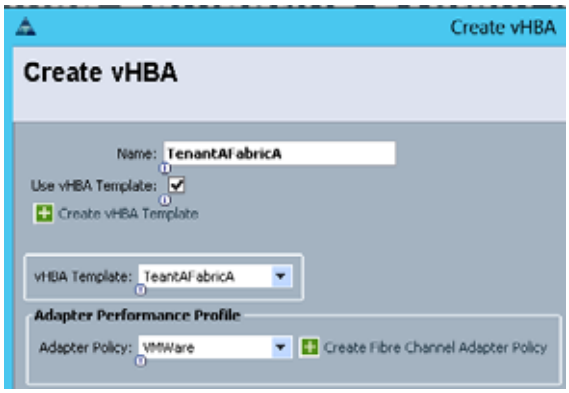
2. [How would you like to configure SAN connectivity] フィールドで定義するために [Expert] をクリックします。
3. [WWNN Assignment] フィールドで、[Platinum-Compute-WWNN] を選択します。

図 125　ディスク プロパティおよび SAN ストレージ プロパティの定義



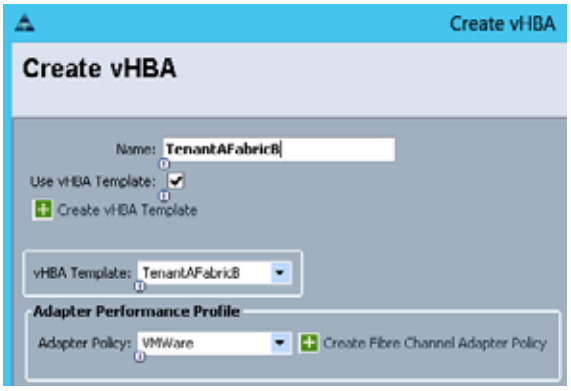
a. [Add] ボタンをクリックして vHBA をテンプレートに追加します。
b. [Name] フィールドに **TenantAFabricA** と入力します。
c. [Use vHBA Template] チェックボックスを有効にします。
d. [vHBA Template] で [TenantAFabricA] を選択します。
e. [Adapater Policy] リスト ボックスの [VMWare] を選択します。
f. [OK] をクリックします。

図 126　Fabric-A-HBA 用の vHBA の値の定義



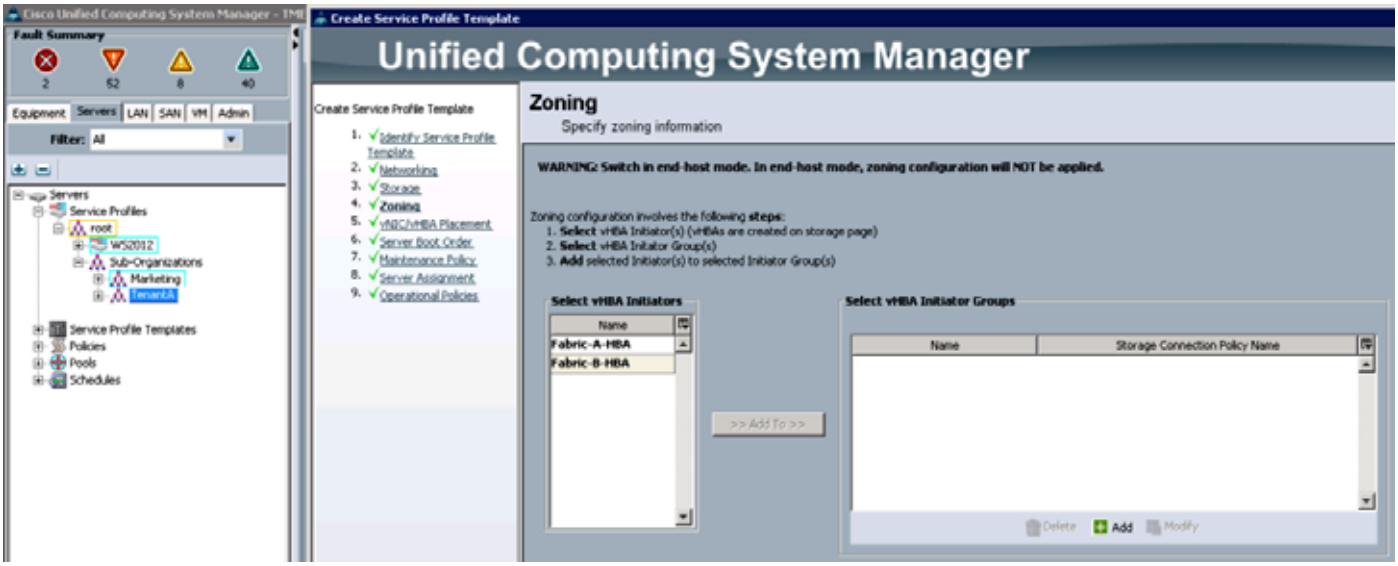
g. [Add] ボタンをクリックして vHBA をテンプレートに追加します。
h. [Name] フィールドに **TenantAFabricB** と入力します。
i. [Use vHBA Template] チェックボックスを有効にします。
j. [vHBA Template] で [TenantAFabricB] を選択します。
k. [Adapater Policy] リスト ボックスの [VMWare] を選択します。
l. [OK] をクリックします。

図 127　Fabric-B-HBA 用の vHBA の値の定義



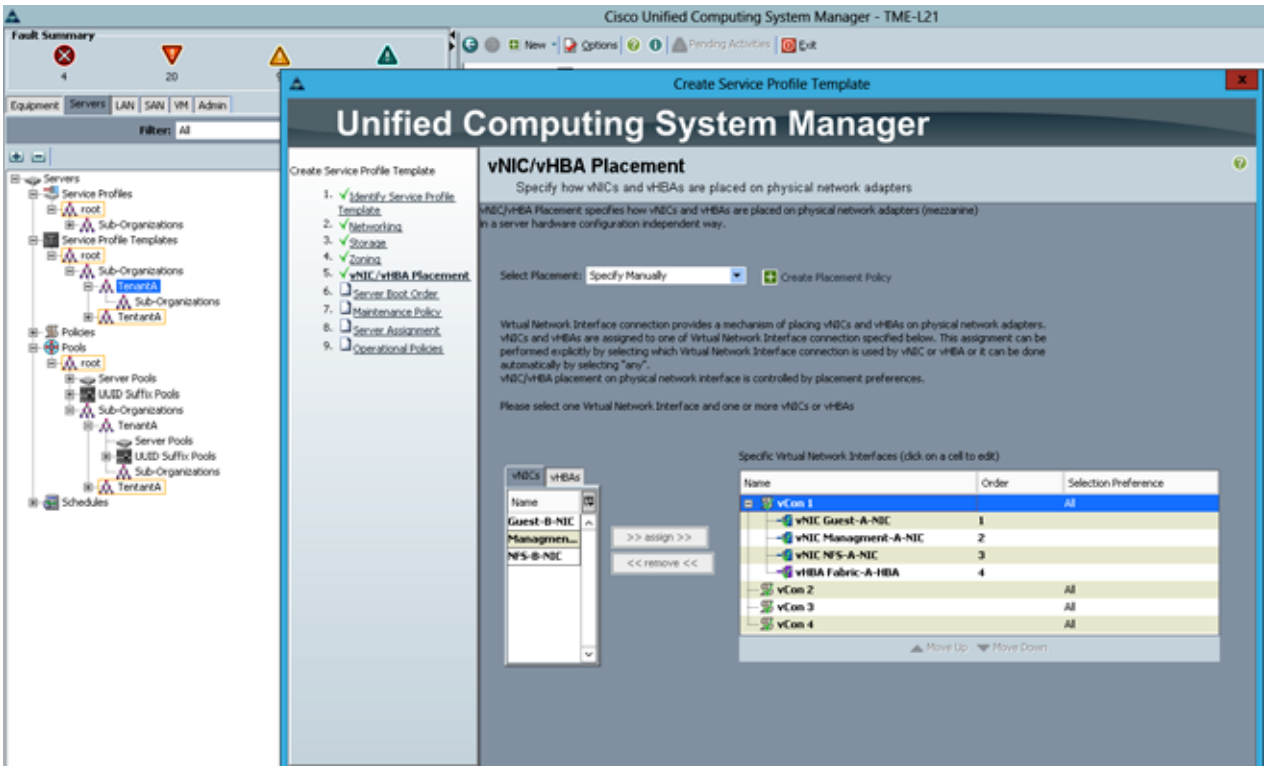
4. [Next] をクリックして、次のセクションに進みます。
5. [Zoning] セクション
   a. デフォルトをすべて採用します。
6. [Next] をクリックします。

図 128　　ゾーニング情報の定義



7. [Next] をクリックして、次のセクションに進みます。
8. [vNIC/vHBA Placement] セクション
   b. [Select Placement] フィールドで手動配置ポリシーを選択します。
   c. [vCon1] を選択し次の順で vNIC を割り当てます。
   - Management-A-NIC
   - Guest-A-NIC
   - NFS-A-NIC
   - Fabric-A-HBA

図 129　　vNIC および vHBA の配置の定義

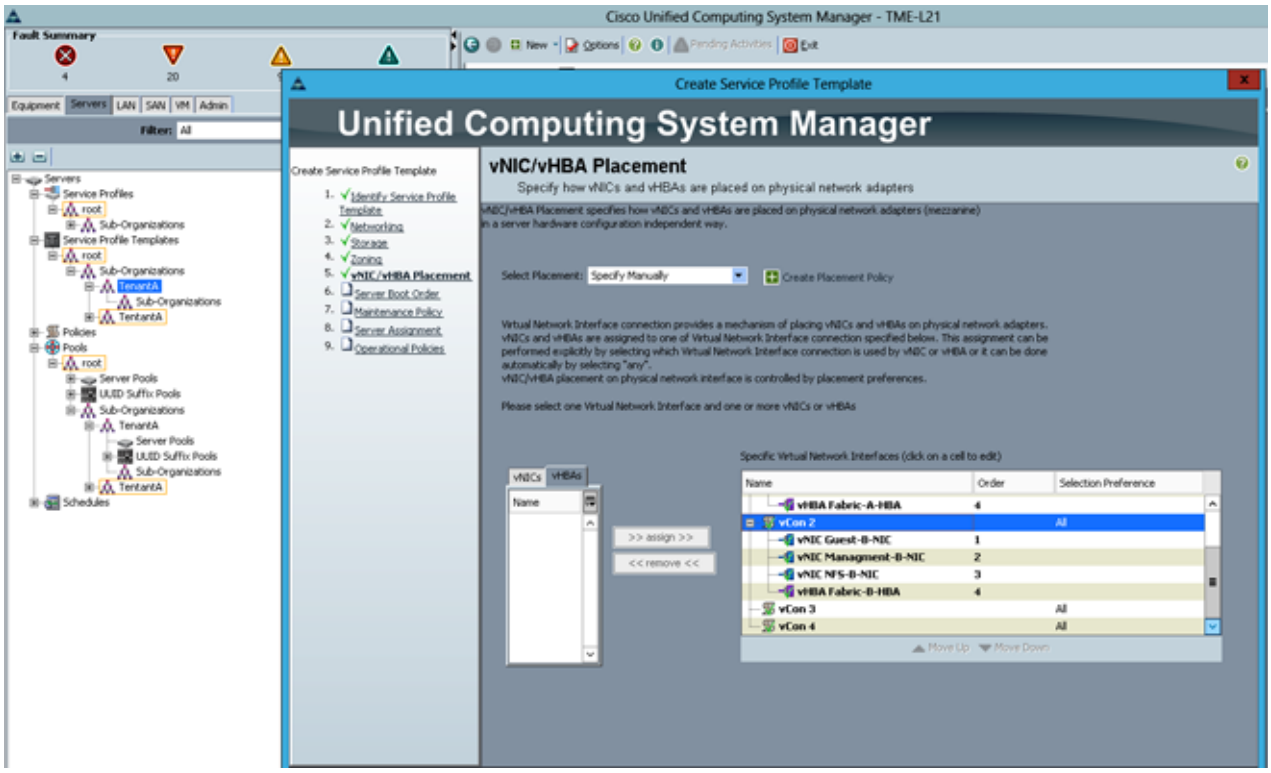


d. [vCon2] を選択し次の順で vNIC を割り当てます。

- Management-B-NIC
- Guest-B-NIC
- NFS-B-NIC
- Fabric-B-HBA

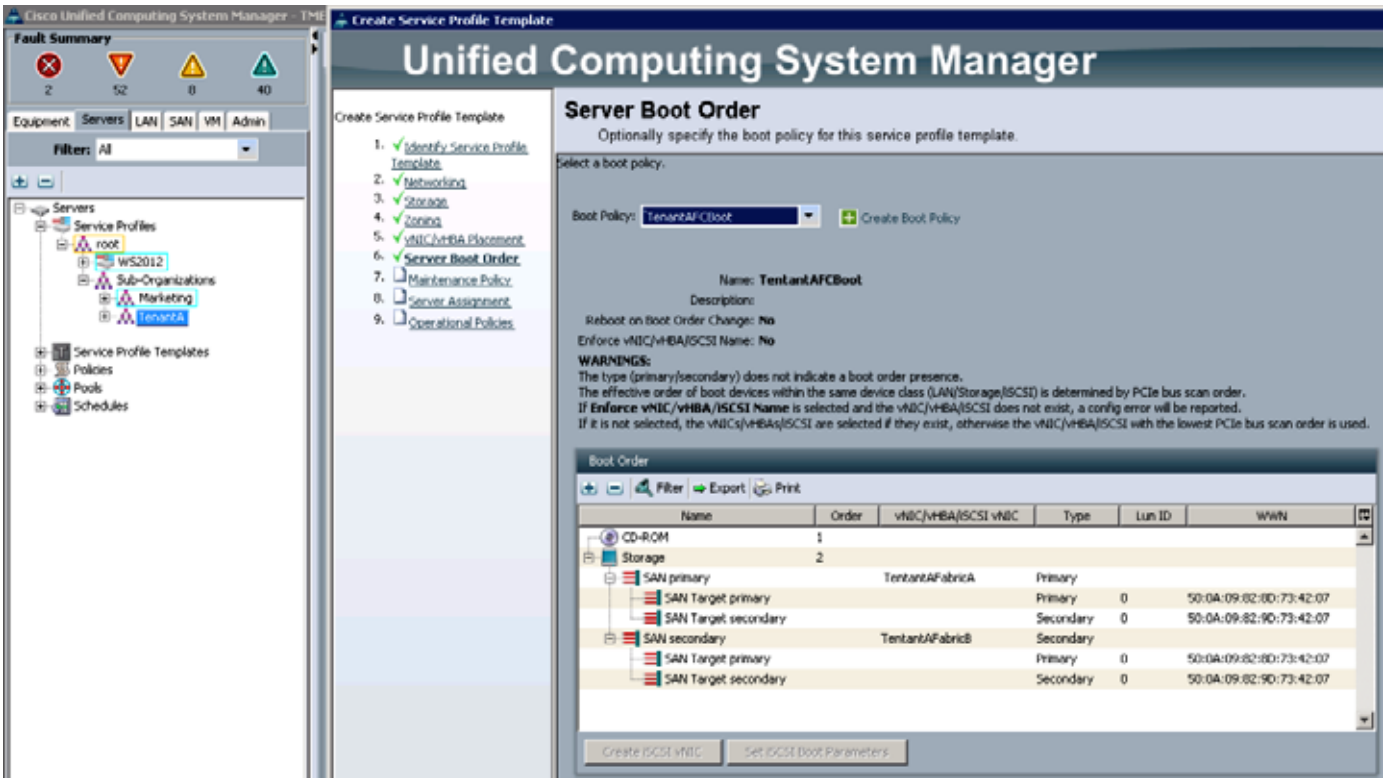
9. [Next] をクリックします。

図 130　　vCon2 への vNIC の割り当て



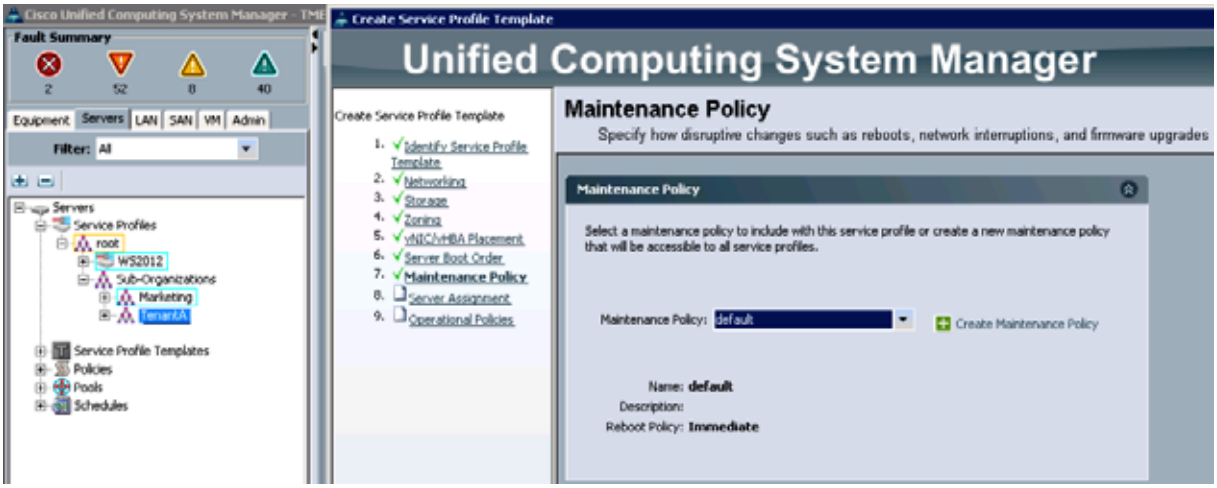
10. [Server Boot Order] セクション
    a. [TenantAFCBoot] ブート ポリシーを選択します。
11. [Next] をクリックします。

図 131　サービス プロファイル テンプレートへの TenantFCBoot ブート ポリシーの適用



12. [Maintenance Policy] セクション
    a. [Maintenance Policy] で [default] を選択します。
13. [Next] をクリックします。

図 132　サービスの中断中にメンテナンス ポリシーに適用されるデフォルト ポリシーの適用



14. [Server Assignment] セクション
    a. [Pool Assignment] で [Platinum-Compute-ServerPool] を選択します。

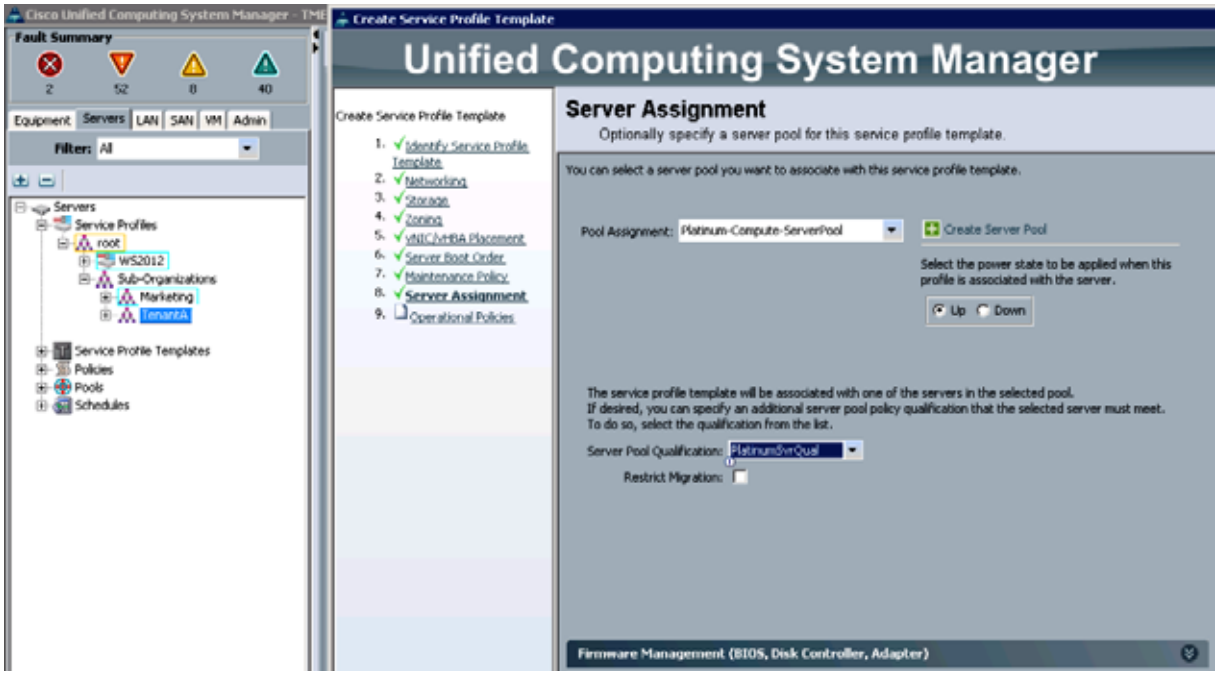
b. [Up] オプション ボタンをクリックして、このプロファイルがサーバに関連付けられたときに適用される電源状態を選択します。

c. [Server Pool Qualification] で [PlatinumSvrQual] を選択します。

d. [Restrict Migration] はチェックしないでください。

15. [Next] をクリックします。

図 133　サービス プロファイルへのサーバ プールの関連付け



16. [Operational Policies] セクション

a. [BIOS Policy] で [TenantA-BIOS] を選択します。

b. [External IPMI Management Configuration] で [default] を選択します。

c. [Management IP Address Policy] で [Platinum-Compute-IP] を選択します。

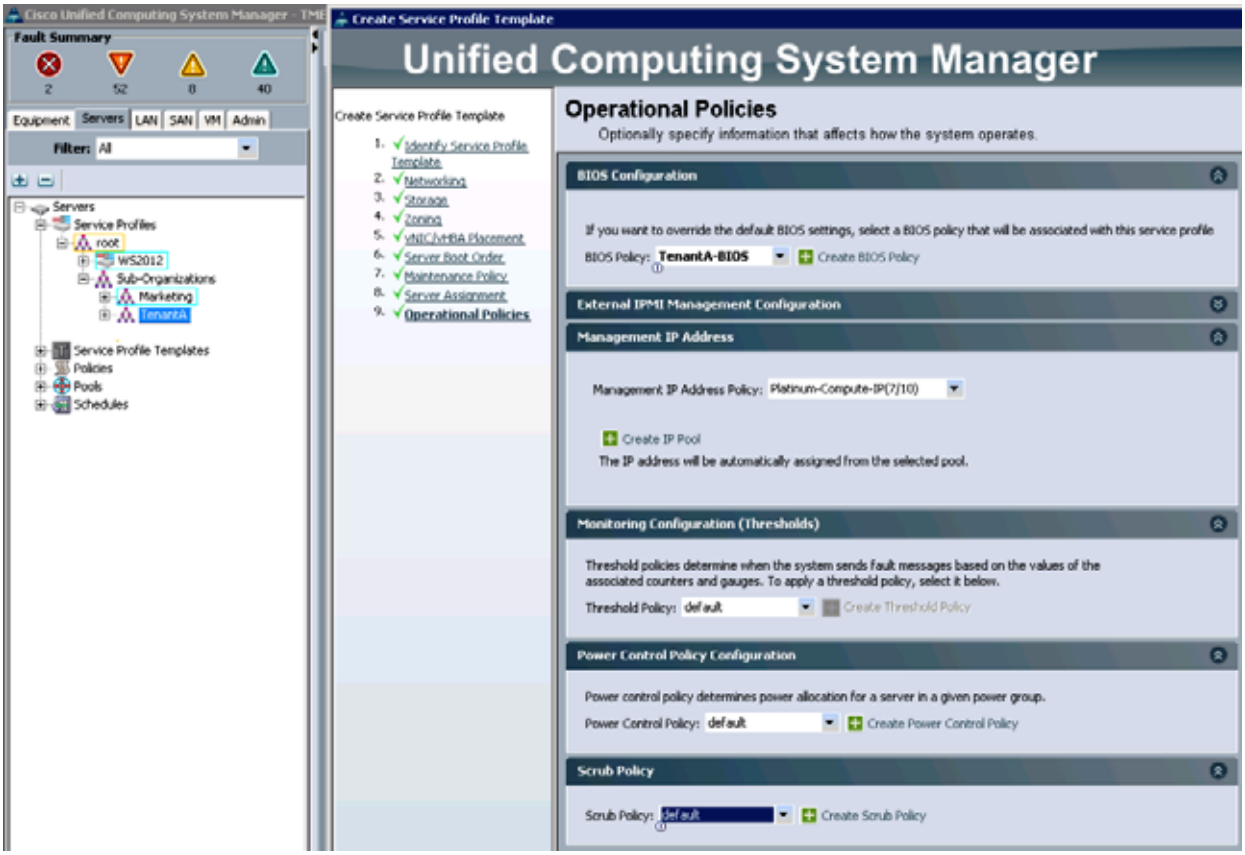
d. [Monitoring Configuration] で [default] を選択します。

e. [Power Control Policy Configuration] で [default] を選択します。

f. [Scrub Policy] で [default] を選択します。

17. [Next] をクリックします。

図 134　運用ポリシーの属性の定義



上記で説明した手順に従い、表 20 および 表 21 にリストしたデータの値を使用して Gold-Template、Silver-Template、および Bronze-Template に対するサービス プロファイル テンプレートを作成します。

表 20　サービス プロファイル テンプレート

名前	タイプ	UUID
Gold-Template	Initial Template	Gold-Compute-UUID
Silver-Template	Initial Template	Silver-Compute-UUID
Bronze-Template	Initial Template	Bronze-Compute-UUID

表 21　ネットワーク設計

ダイナミック vNIC 接続ポリシー	LAN 接続の設定
デフォルトでは Dynamic vNIC ポリシーはなし	エキスパート

表 22 に定義された値によって Gold-Template に対する vNIC を作成します。

表 22　vNIC および Gold サービス クラスに対するそれらのプロパティ

名前	MAC アドレス	ファブリック ID	VLAN ネイティブ VLAN	MTU	PIN グループ	アダプタ ポリシー	ダイナミック vNIC 接続ポリシー	QoS ポリシー	ネットワーク制御ポリシー
Management-A-NIC	Gold-Compute-MAC	A	Management-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Platinum-Net-SLA	デフォルト
Management-B-NIC	Gold-Compute-MAC	B	Management-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Platinum-Net-SLA	デフォルト
Guest-A-NIC	Gold-Compute-MAC	A	Guest-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Gold-Net-SLA	デフォルト
Guest-B-NIC	Gold-Compute-MAC	B	Guest-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Gold-Net-SLA	デフォルト
NFS-A-NIC	Gold-Compute-MAC	A	Guest-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Silver-Net-SLA	デフォルト
NFS-B-NIC	Gold-Compute-MAC	B	Guest-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Silver-Net-SLA	デフォルト

表 23 に定義された値を使用して Silver-Template に対する vNIC を作成します。

表 23　vNIC および Silver サービス クラスに対するそれらのプロパティ

名前	MAC アドレス	ファブリック ID	VLAN ネイティブ VLAN	MTU	PIN グループ	アダプタ ポリシー	ダイナミック vNIC 接続ポリシー	QoS ポリシー	ネットワーク制御ポリシー
Management-A-NIC	Silver-Compute-MAC	A	Management-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Platinum-Net-SLA	デフォルト
Management-B-NIC	Silver-Compute-MAC	B	Management-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Platinum-Net-SLA	デフォルト
Guest-A-NIC	Silver-Compute-MAC	A	Guest-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Gold-Net-SLA	デフォルト
Guest-B-NIC	Silver-Compute-MAC	B	Guest-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Gold-Net-SLA	デフォルト

表 23　vNIC および Silver サービス クラスに対するそれらのプロパティ

NFS-A-NIC	Silver-Compute-MAC	A	Guest-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Silver-Net-SLA	デフォルト
NFS-B-NIC	Silver-Compute-MAC	B	Guest-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Silver-Net-SLA	デフォルト

表 24 に定義された値を使用して Bronze-Template に対する vNIC を作成します。

表 24　vNIC および Bronze クラスに対するそれらのプロパティ

名前	MAC アドレス	ファブリック ID	VLAN ネイティブ VLAN	MTU	PIN グループ	アダプタ ポリシー	ダイナミック vNIC 接続ポリシー	QoS ポリシー	ネットワーク制御ポリシー
Management-A-NIC	Bronze-Compute-MAC	A	Management-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Platinum-Net-SLA	デフォルト
Management-B-NIC	Bronze-Compute-MAC	B	Management-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Platinum-Net-SLA	デフォルト
Guest-A-NIC	Bronze-Compute-MAC	A	Guest-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Gold-Net-SLA	デフォルト
Guest-B-NIC	Bronze-Compute-MAC	B	Guest-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Gold-Net-SLA	デフォルト
NFS-A-NIC	Bronze-Compute-MAC	A	Guest-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Silver-Net-SLA	デフォルト
NFS-B-NIC	Bronze-Compute-MAC	B	Guest-VLAN	9000	Tenant A-Net-PIN	デフォルト	未設定	Silver-Net-SLA	デフォルト

表 25　ストレージ設定

ローカル ストレージ	SAN 接続の設定	WWNN 割り当て
TenantLocalDisk	エキスパート	Gold-Compute-WWNN

表 26　ファブリック A および B の vSAN の値

名前	WWPN	ファブリック ID	VSAN	PIN グループ	永続的なバインディング	最大データ フィールド サイズ	アダプタ ポリシー	QoS ポリシー
Fabric-A-HBA	Gold-Compute-WWPN	A	10	TenantA-SAN-PIN	イネーブル	2048	デフォルト	FC-Net-SLA
Fabric-B-HBA	Gold-Compute-WWPN	B	10	TenantA-SAN-PIN	イネーブル	2048	デフォルト	FC-Net-SLA

表 27　ゾーニングおよび vNIC/vHBA 配置

ゾーニング	vHBA 配置
デフォルト	手動

表 28　vCon1 および vCon2 上の vNIC と vHBA の配置

vCon1	vCon2
Management-A-NIC	Management-B-NIC
Guest-A-NIC	Guest-B-NIC
NFS-A-NIC	NFS-B-NIC
Fabric-A-HBA	Fabric-B-HBA

表 29　サーバ ブート順序ポリシーおよびメンテナンス ポリシーの値

ブート ポリシー	メンテナンス ポリシー
TenantAFC-Boot	デフォルト

表 30　サーバ割り当て

プール割り当て	電源状態	サーバ プールの資格情報	移行を制限
Gold-Compute-ServerPool	Up	GoldSvrQual	チェックを入れない
Silver-Compute-ServerPool	Up	SilverSvrQual	チェックを入れない
Bronze-Compute-ServerPool	Up	BronzeSvrQual	チェックを入れない

表 31　　運用ポリシー

BIOS ポリシー	外部 IPMI 管理	管理 IP アドレス	設定のモニタリング	電源制御ポリシー	スクラブ ポリシー
TenantA-BIOS	デフォルト	Gold-Compute-IP	デフォルト	デフォルト	デフォルト
TenantA-BIOS	デフォルト	Silver-Compute-IP	デフォルト	デフォルト	デフォルト
TenantA-BIOS	デフォルト	Bronze-Compute-IP	デフォルト	デフォルト	デフォルト

Baremetal RHELHost サービス プロファイル テンプレート

この項では、CloudPlatfrom 4.2.1 を使用して RHEL 6.X オペレーティング システムをホストするブレードをプロビジョニングするために定義される Baremetal サービス プロファイル テンプレートの作成について詳しく説明します。

Baremetal as a Service に対しては、サーバ プロファイル テンプレート、プール（UUID、MAC、IP、PWWN、WWNN、およびサーバ）、vNIC テンプレートと vHBA テンプレート、ポリシー（ブート、IPMI、アダプタ、BIOS、ファームウェア）はルート組織に作成される必要があります。

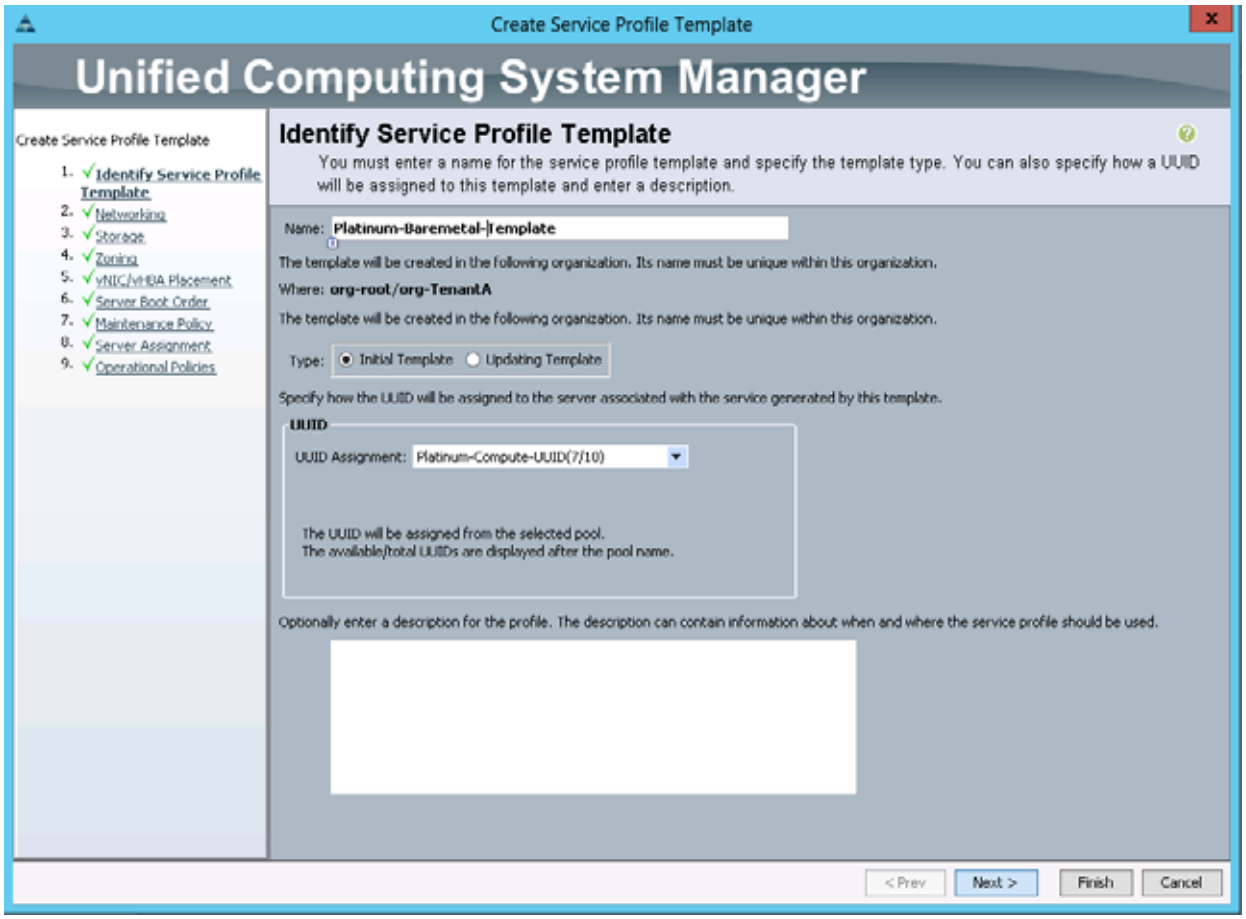
（注）　ここでは、ルート組織に作成されていると思われる以下のプール、ポリシー、vHBA テンプレートの作成手順には触れません。これらの作成手順の詳細については「クラウド コンピュートの設計および導入」の項を参照してください。

1. Platinum-Compute-UUID
2. Baremetal-Disk
3. Platinum-Compute-WWNN
4. Platinum-Compute-WWPN

管理ユーザで Cisco UCS Manager にログインし、以下の手順を実行します。

1. 左ペインで、[Servers] タブをクリックします。
2. [Service Profiles] > [root] を選択します。
3. 右ペインの [General] タブ上の [Create Service Profile Templates] を選択します。
4. [Create Service Profile Template] ウィンドウが表示されます。
5. サービス プロファイル テンプレートの名前を Platinum-Baremetal-Template にします。
6. [Initial Template] を選択します。
7. [UUID] セクションで、UUID プールとして [BarePlatinum-Compute-UUID] を選択します。
8. [Next] をクリックして、次のセクションに進みます。

図 135　サービス プロファイル テンプレートへのユニークな名前の追加

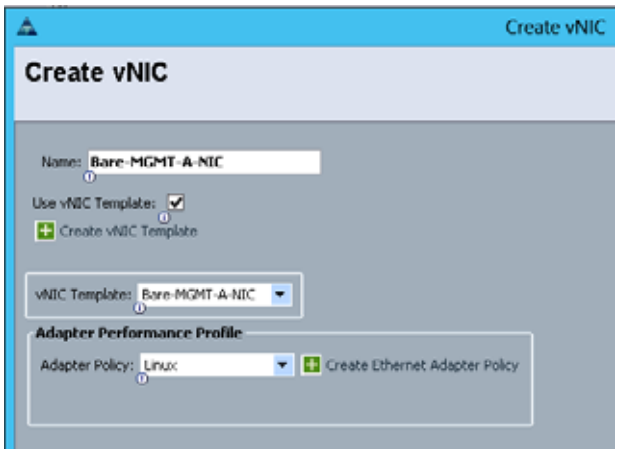


ネットワーク定義

vNIC の作成

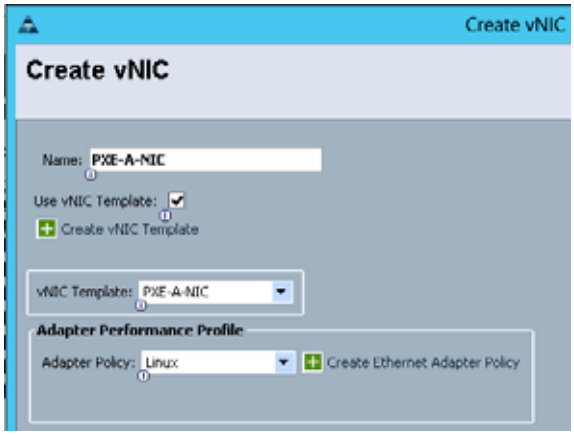
1. [Dynamic vNIC Connection Policy] フィールドはデフォルトのままにしておきます。
2. [How would you like to configure LAN connectivity?] で [Expert] を選択します。
3. [Add] アイコンをクリックします（サーバが LAN 接続に使用する vNIC の必要数を指定します）。
4. [Create vNIC] ウィンドウが開きます。
5. [Name] フィールドに Bare-MGMT-A-NIC と入力します。
6. [Use vNIC Template] チェックボックスを有効にします。
7. [vNIC Template] リスト ボックスの [Bare-MGMT-A-NIC] を選択します。
8. [Adapater Policy] リスト ボックスの [Linux] を選択します。
9. [OK] をクリックします。

図 136　Bare-MGMT-A-NIC 用の vNIC プロパティの定義



10. [Add] をクリックします。
11. [Name] フィールドに PXE-A-NIC と入力します。
12. [Use vNIC Template] チェックボックスを有効にします。
13. [vNIC Template] リスト ボックスの [PXE-A-NIC] を選択します。
14. [Adapater Policy] リスト ボックスの [Linux] を選択します。
15. [OK] をクリックします。

図 137　PXE-A-NIC 用の vNIC プロパティの定義



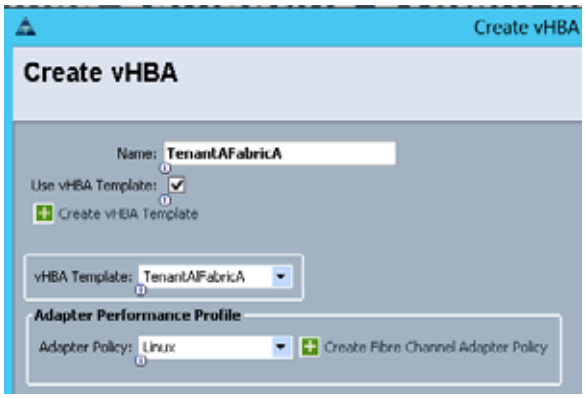
ストレージ定義

vHBA の作成

1. [Local Storage] フィールドで [TenantLocalDisk] を選択します。
2. [How would you like to configure SAN connectivity] フィールドで定義するために [Expert] をクリックします。
3. [WWNN Assignment] フィールドで、[Platinum-Compute-WWNN] を選択します。

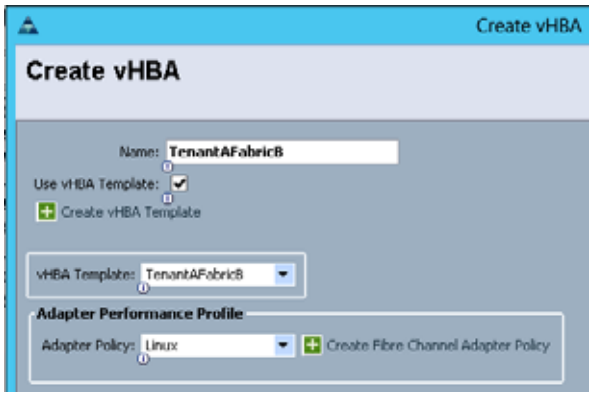
4. [Add] をクリックします。
5. [Name] フィールドに TenantAFabricA と入力します。
6. [Use vHBA Template] チェックボックスを有効にします。
7. [vHBA Template] で [TenantAFabricA] を選択します。
8. [Adapater Policy] で [Linux] を選択します。

図 138　サービス プロファイル テンプレート用の TenantAFabricA vHBA の定義



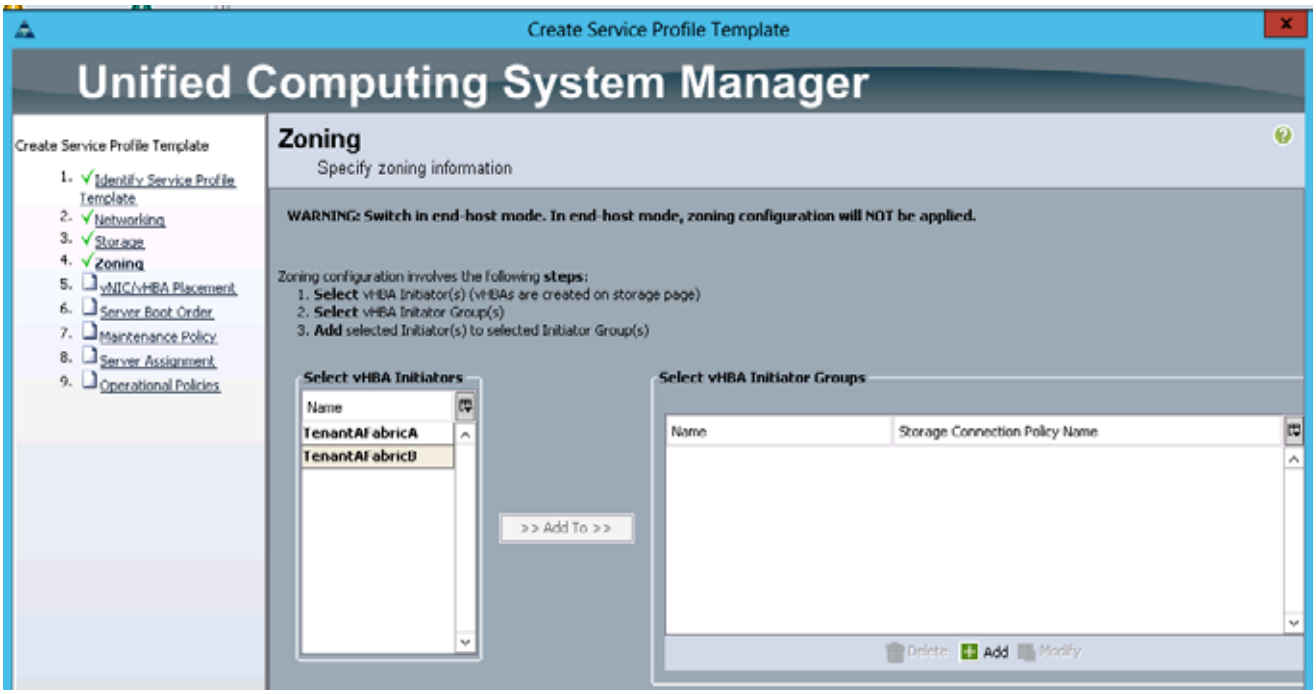
9. [Add] をクリックします。
10. [Name] フィールドに TenantAFabricB と入力します。
11. [Use vHBA Template] チェックボックスを有効にします。
12. [vHBA Template] で [TenantAFabricA] を選択します。
13. [Adapater Policy] で [Linux] を選択します。

図 139　サービス プロファイル テンプレート用の TenantAFabricB vHBA の定義



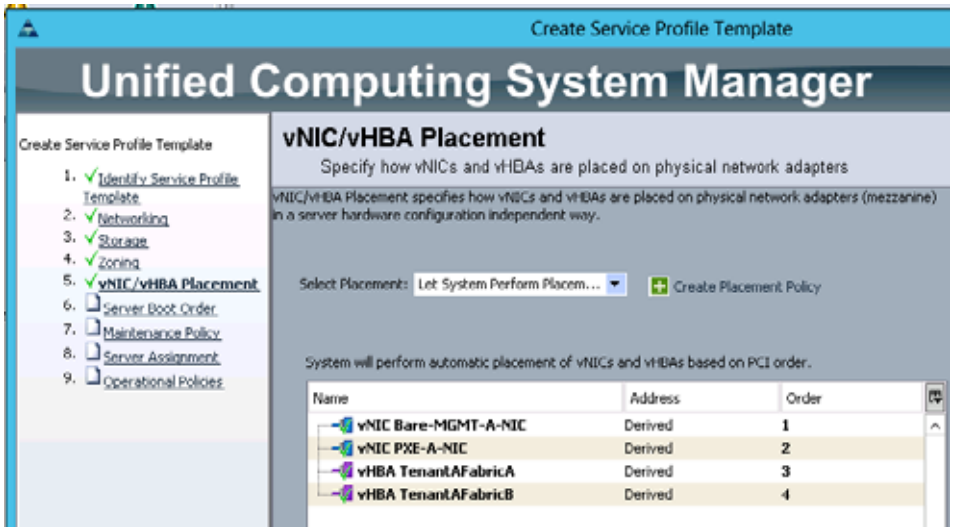
14. [Next] をクリックして、次のセクションに進みます。
15. [Zoning] セクション
    a. デフォルトをすべて採用します。
16. [Next] をクリックします。

図 140　　ゾーニング情報の定義



17. [Next] をクリックして、次のセクションに進みます。
18. [vNIC/vHBA Placement] セクション
    a. [Select Placement] フィールドで [Let System Perform Placement Policy] を選択します。
19. [Next] をクリックします。

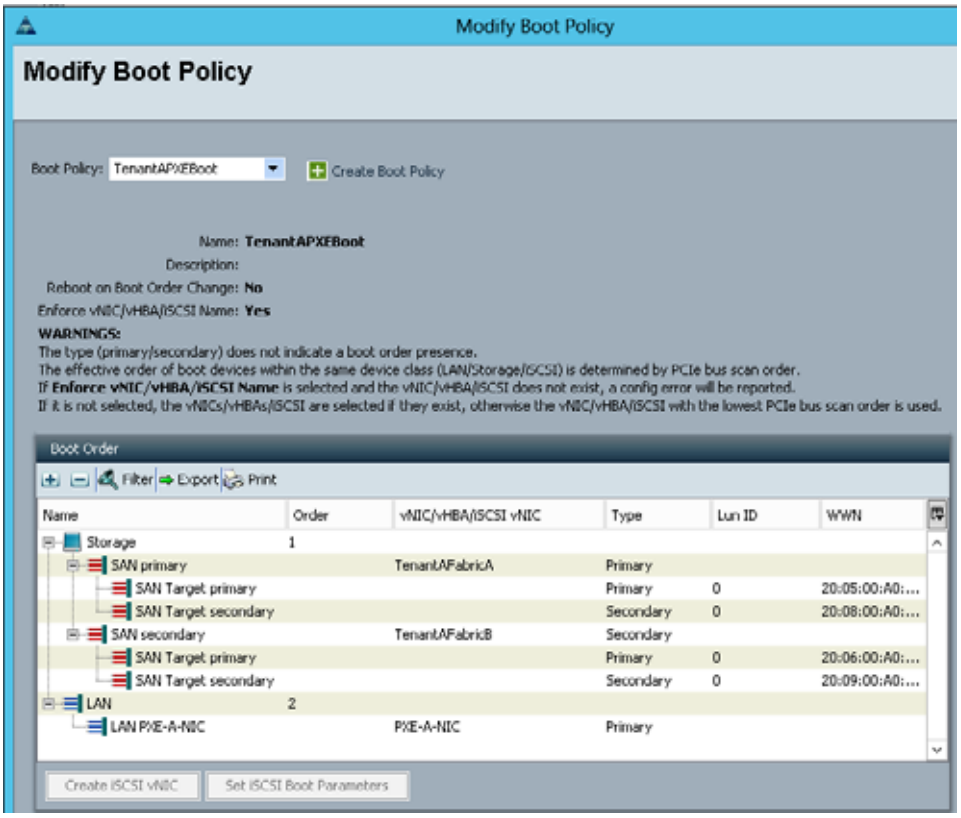
図 141　　vNIC と vHBA の配置の定義



20. [Server Boot Order] セクション
    a. [TenantAPXEBoot] ブート ポリシーを選択します。

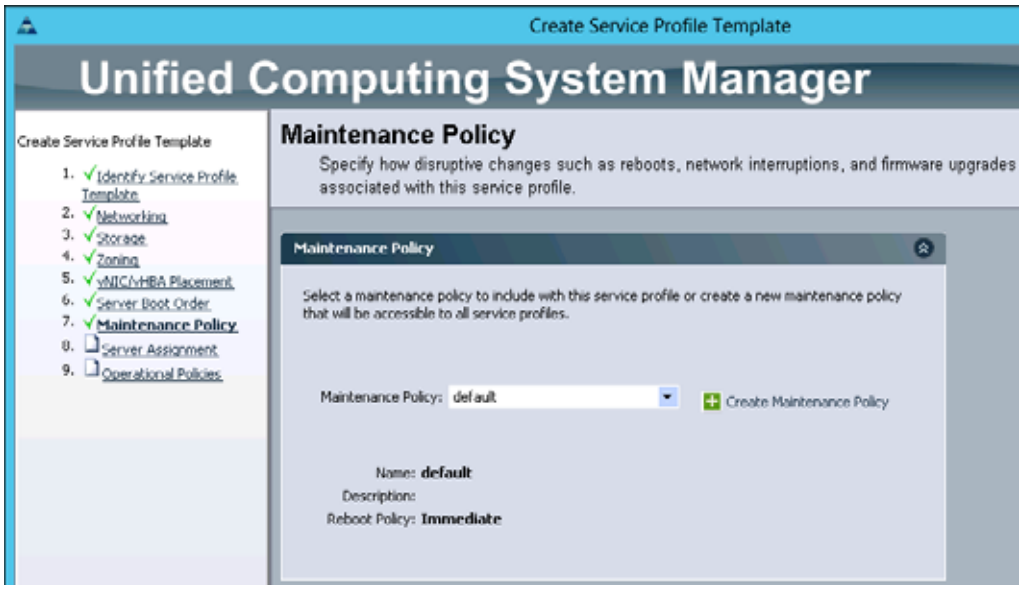
21. [Next] をクリックします。

図 142　サービス プロファイル テンプレートのブート ポリシーの定義



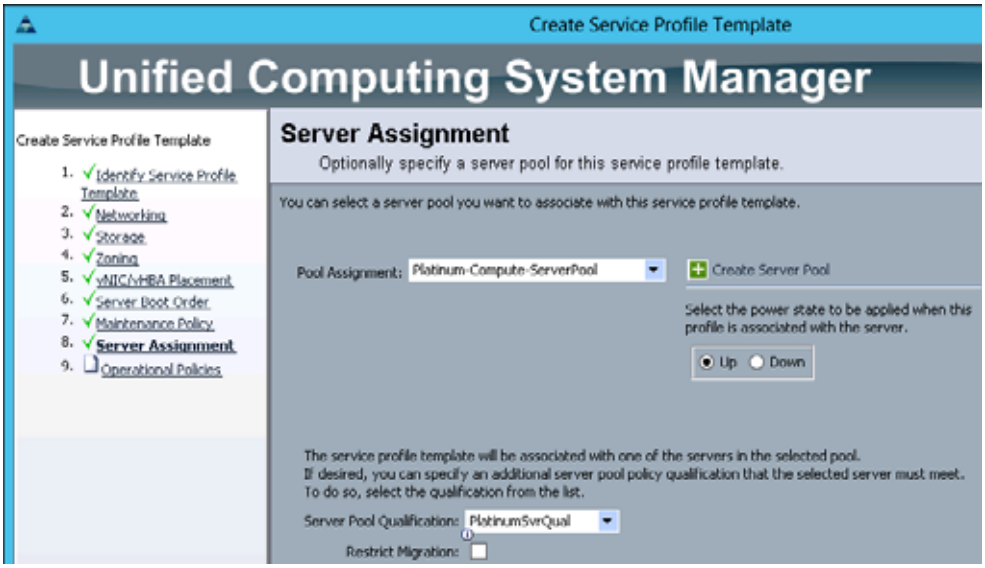
22. [Maintenance Policy] セクション
    a. [default] メンテナンス ポリシーを選択します。
23. [Next] をクリックします。

図 143　サービスの中断中にサーバに適用されるポリシーの定義



24. [Server Assignment] セクション
    a. [Pool Assignment] で [Platinum-Compute-ServerPool] を選択します。
    b. [Up] オプション ボタンをクリックして、このプロファイルがサーバに関連付けられるときに適用される電源状態を選択します。
    c. [Server Pool Qualification] で [PlatinumSvrQual] を選択します。
    d. [Restrict Migration] をチェックしないでください。
25. [Next] をクリックします。

図 144　サービス プロファイルへのサーバ プールの関連付け



26. [Operational Policies] セクション

a. [BIOS Policy] で [TenantA-BIOS] を選択します。
b. [External IPMI Management Configuration] で [BareMetal] を選択します。
c. [Management IP Address Policy] で [Platinum-Compute-IP] を選択します。
d. [Monitoring Configuration] で [default] を選択します。
e. [Power Control Policy Configuration] で [default] を選択します。
f. [Scrub Policy] で [default] を選択します。

27. [Next] をクリックします。

図 145　　運用ポリシーの属性の定義

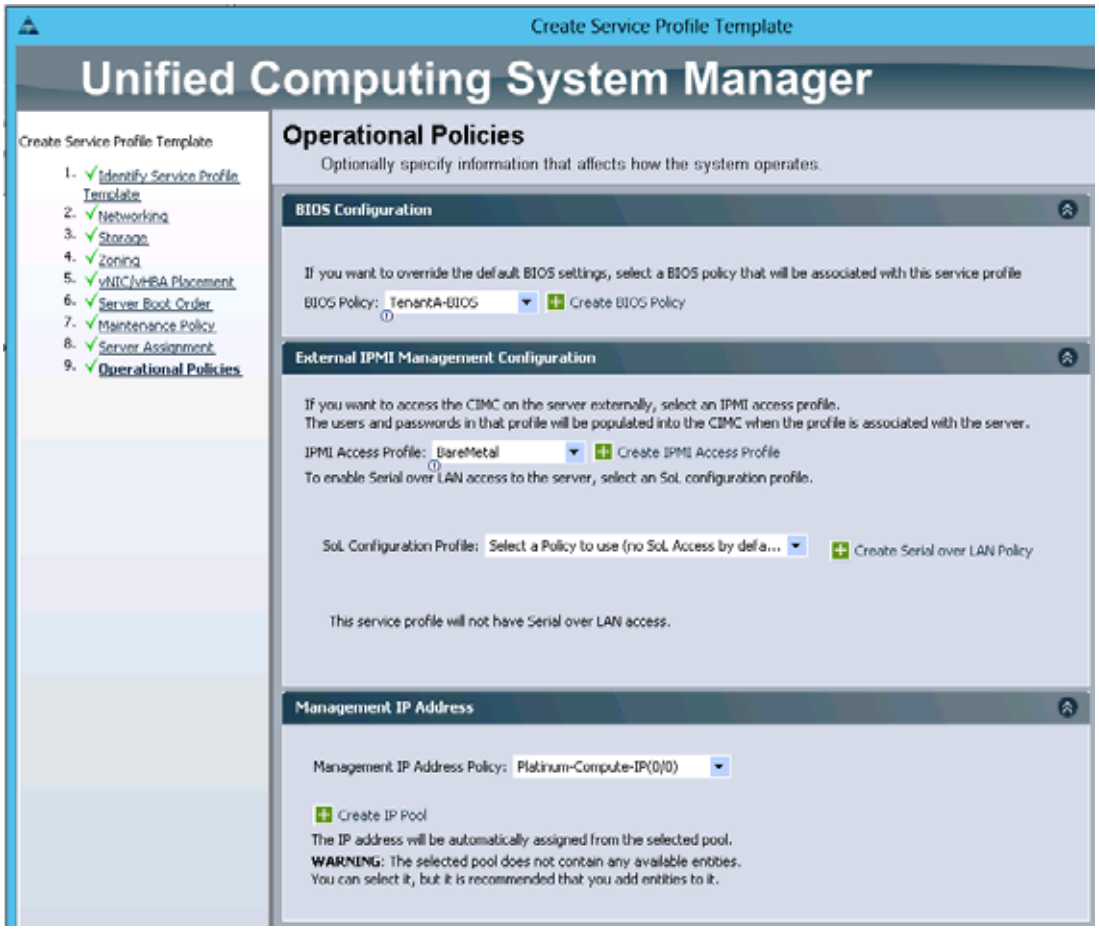
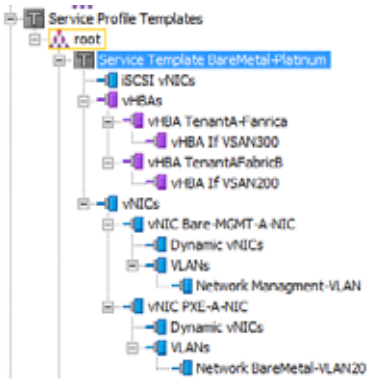


図 146　BareMetal-Platinum サービス プロファイル テンプレートの要約



CloudPlatform ホストの準備

この項では、クラウドベースのサービス レベル定義を使用してクラウド サービスをホストするために、マルチテナントに必要な VMWare ESXi 5.1 Host の準備について説明します。

クラウド ホストの準備は、次のような 3 つのセクションに分割されます。

- ホストの作成
- ホストのインストール
- ホストの設定

ホストの作成

この項では、マルチテナントクラウド環境でクラウド サービスをホストするために必要なサービス レベルの定義に基づいて、クラウド ホストのコンピューティング、ネットワークおよびストレージ インフラストラクチャを作成するために必要な手順の概要を説明します。Cisco UCS は、サービス レベルに基づいて事前に定義されたクラウド ホストのコンピューティング、ネットワークおよびストレージ リソースを含むサービス プロファイル テンプレートを提供します。クラウド サービス レベル合意書を満たす 4 つのサービス プロファイル テンプレートが作成されました。

次の手順は、組織単位 TenantA のサービス プロファイル テンプレート Platinum-Template によって定義されている Platinum サービス レベルに基づいて、クラウド ホストを作成する方法について示しています。

この項では、次のタスクが詳しく説明されます。

- サービス プロファイル テンプレートに基づいたサービス プロファイルの作成
- サーバへのサービス プロファイルの関連付け

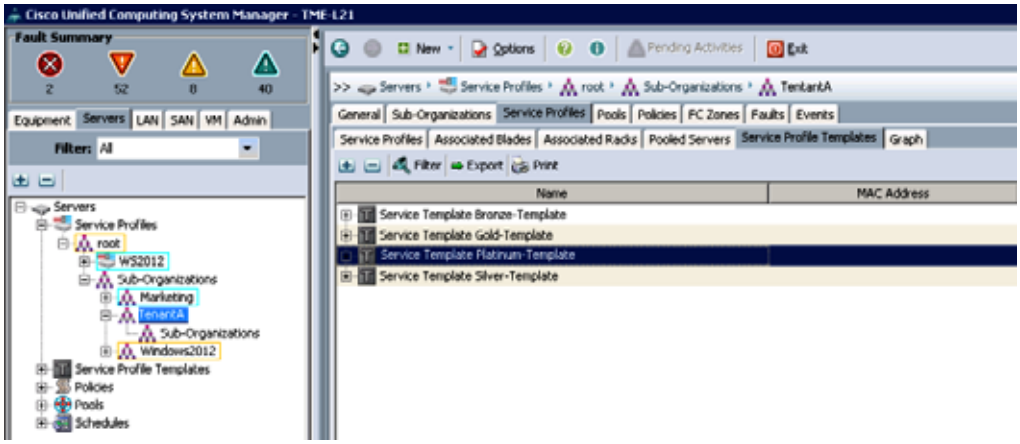
サービス プロファイル テンプレートに基づいたサービス プロファイルの作成

この項では、前述の手順で作成したサービス プロファイル テンプレートに基づいてサービス プロファイルを作成する方法の詳細について説明します。

組織 TenantA に対して以前に作成したユーザ TenantA-Admin を使用して Cisco UCS Manager にログインします。

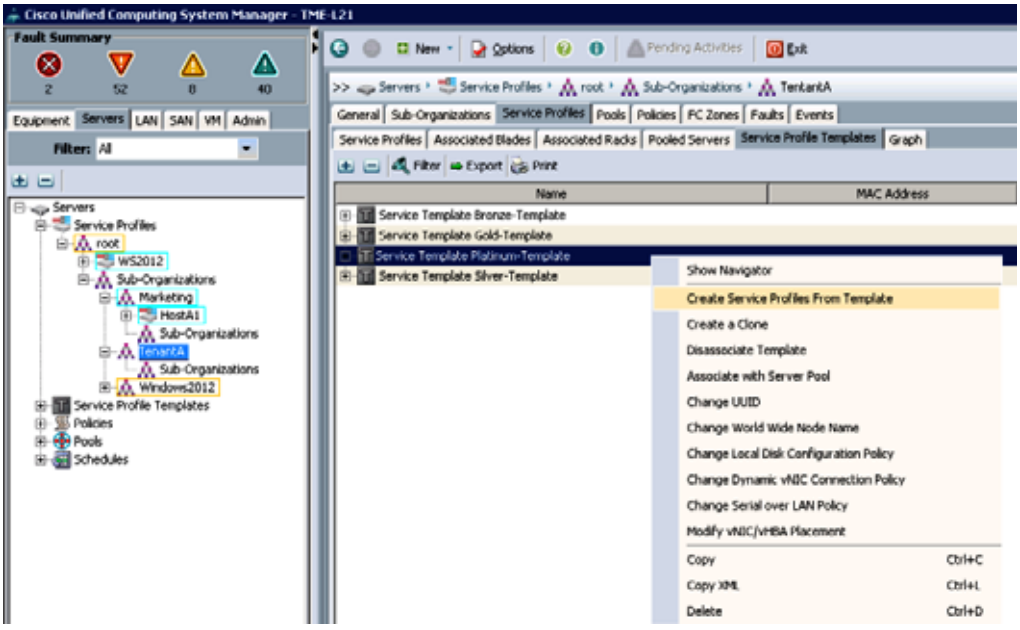
1. 左ペインで [Server] タブをクリックします。
2. [Service Profiles] > [Sub-Organizations] を選択します。[TenantA] を展開します。
3. 右ペインで [Service Profiles] > [Service Profile Template] > [Service Template Platinum-Template] を選択します。

図 147　　サービス プロファイル テンプレートの選択



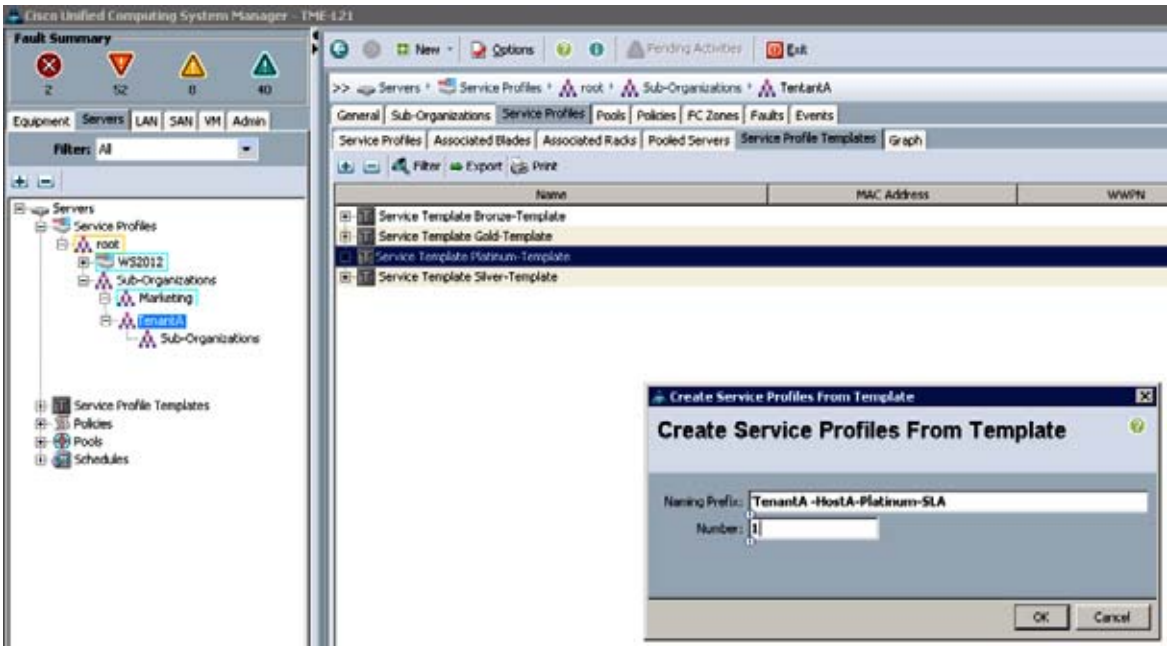
4. [Create Service Profile from Template] を右クリックします。

図 148　　テンプレートからのサービス プロファイルの選択



5. [Naming Prefix] に TenantA-HostA-Platinum-SLA と入力し、作成するサービス プロファイルの数を [Number] テキスト ボックスに入力します。この場合は、1 と入力します。
6. [OK] をクリックします。

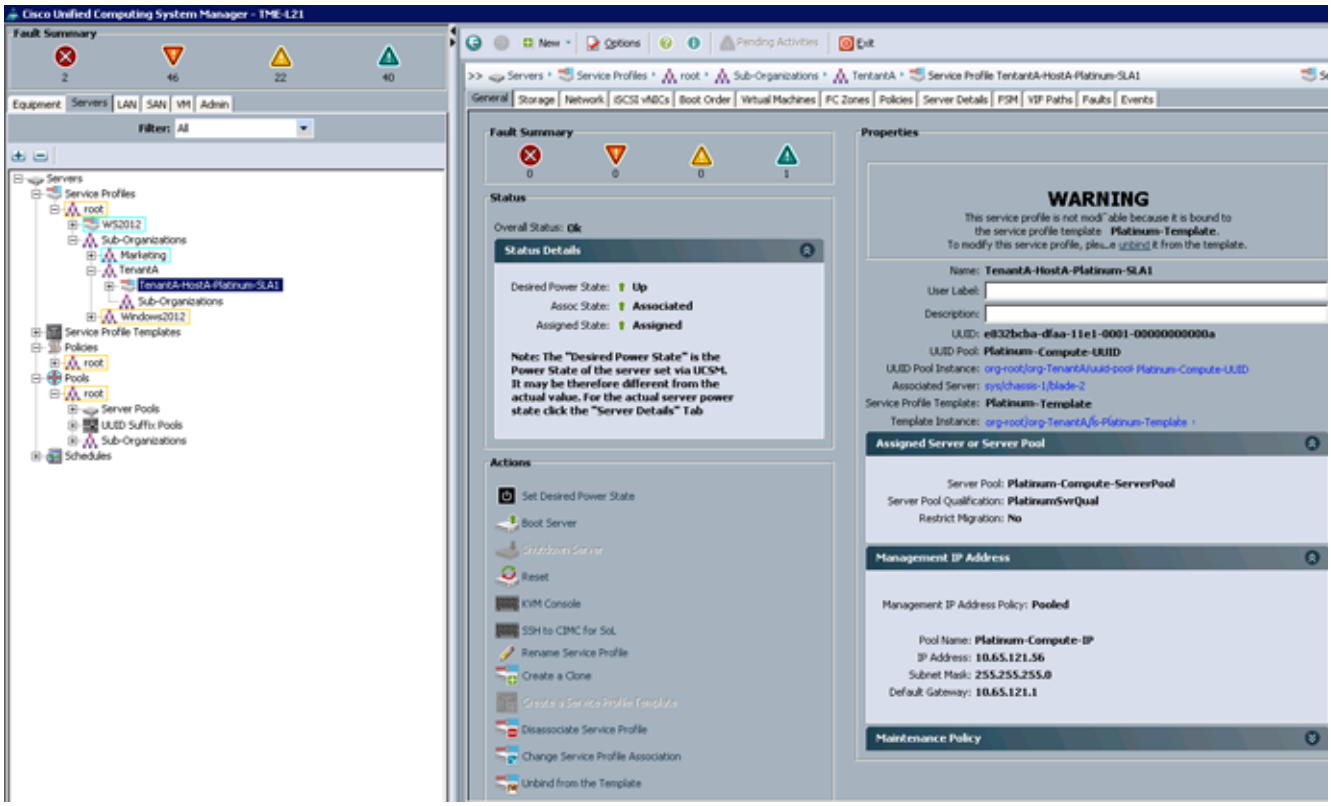
図 149　　プロファイルへの名前と数の追加



サーバへのサービス プロファイルの関連付け

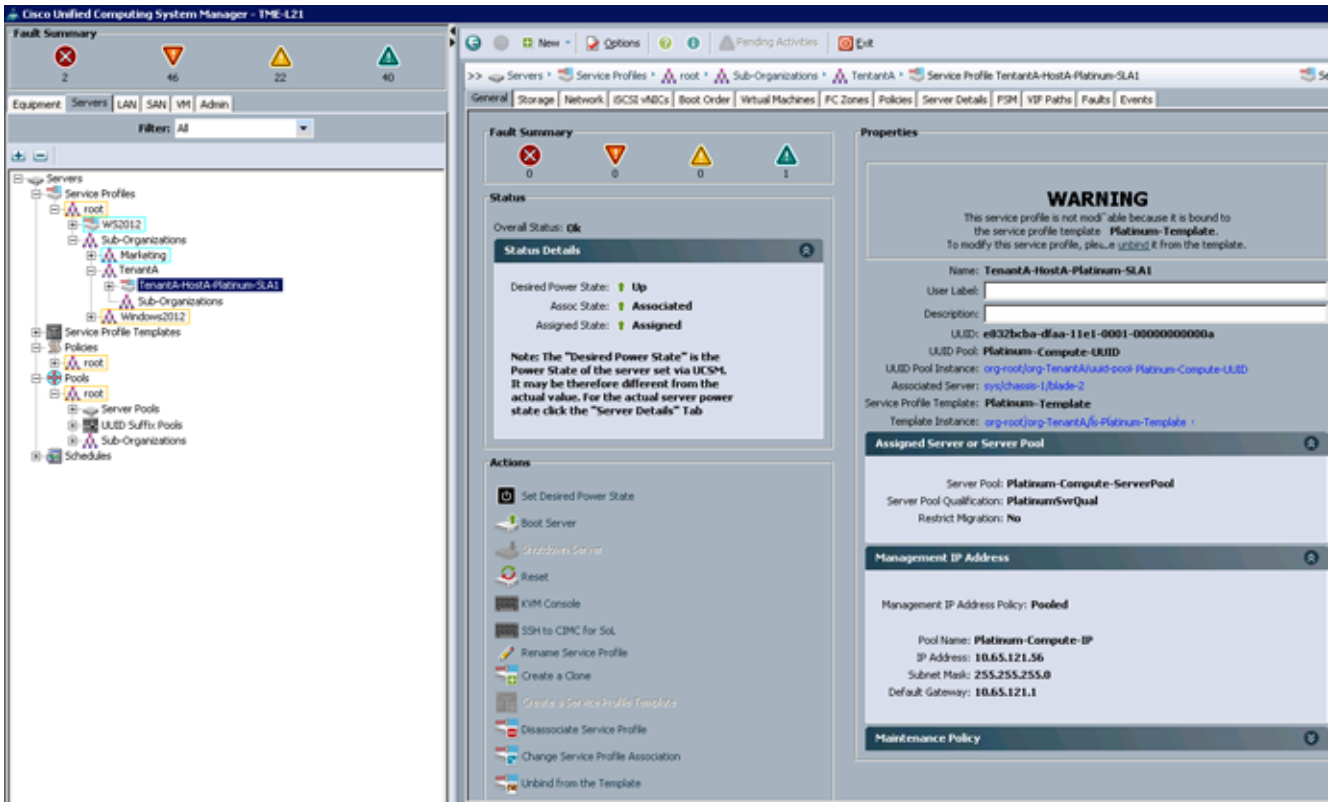
1. [TenantA] の下に新しく作成されたサービス プロファイル TenantA-HostA-Platinum-SLA1 が表示され、関連付けフェーズに存在することになります。

図 150　　サービス プロファイル ステータスの詳細の表示



2. 数分後に、サービス プロファイル TenantA-HostA-Platinum-SLA がサーバ プールで定義された利用可能なブレードに関連付けられます。

図 151　ブレードに関連付けられているサービス プロファイルの確認



ホストのインストール

この項では、クラウド ホスト上に VMware vSphere ESXi 5.1 オペレーティング システムをインストールするために必要な手順について説明します。Cisco UCS は、ブレード上のビデオ出力の Video over IP を表示する KVM コンソールを提供します。Cisco UCS でのサーバ ブレードへの KVM コンソール アクセスは、概念的にブレードへの業界標準の KVM コンソール アクセスに似ています。サーバ プロファイルの関連付けが完了すると、KVM コンソールにアクセスできます。KVM コンソールは、Cisco UCS Manager GUI または KVM の直接接続をエミュレートする KVM Launch Manager からアクセスできるインターフェイスです。

次の手順は、組織単位 TenantA の TenantA-HostA-Platinum-SLA サービス プロファイルを使用して、新しく関連付けられたブレード サーバ上に ESXi 5.1 ハイパーバイザをインストールする方法について示しています。

この項では、次の作業を説明します。

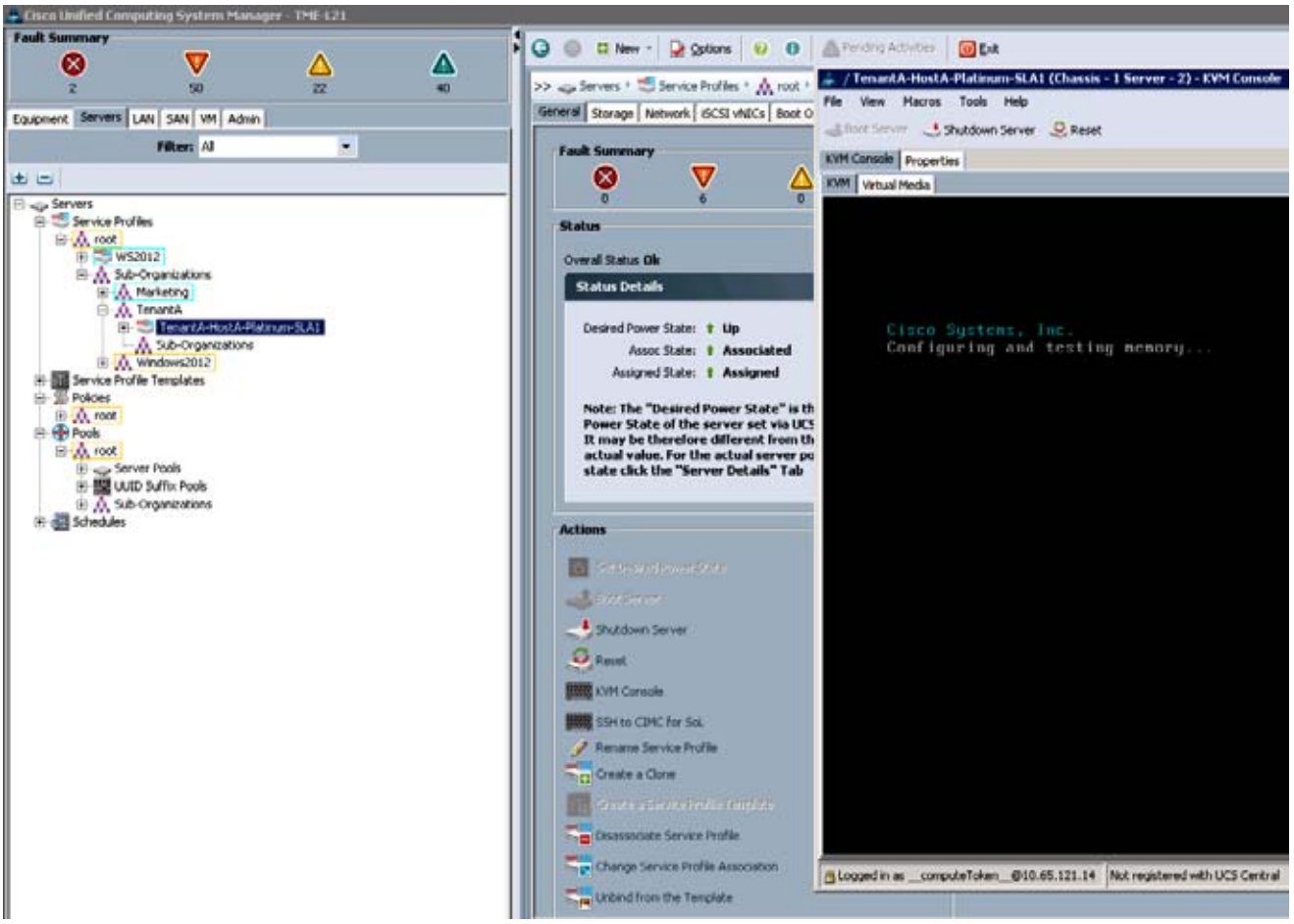
- ブレード サーバの KVM コンソールへの接続
- VMware ESXi 5.1 ハイパーバイザのインストール

組織 TenantA に対して以前に作成したユーザ TenantA-Admin を使用して Cisco UCS Manager にログインします。

1. 左ペインで [Server] タブをクリックします。
2. [Service Profiles] を展開して [Sub-Organizations] を選択します。[TenantA] を展開します。

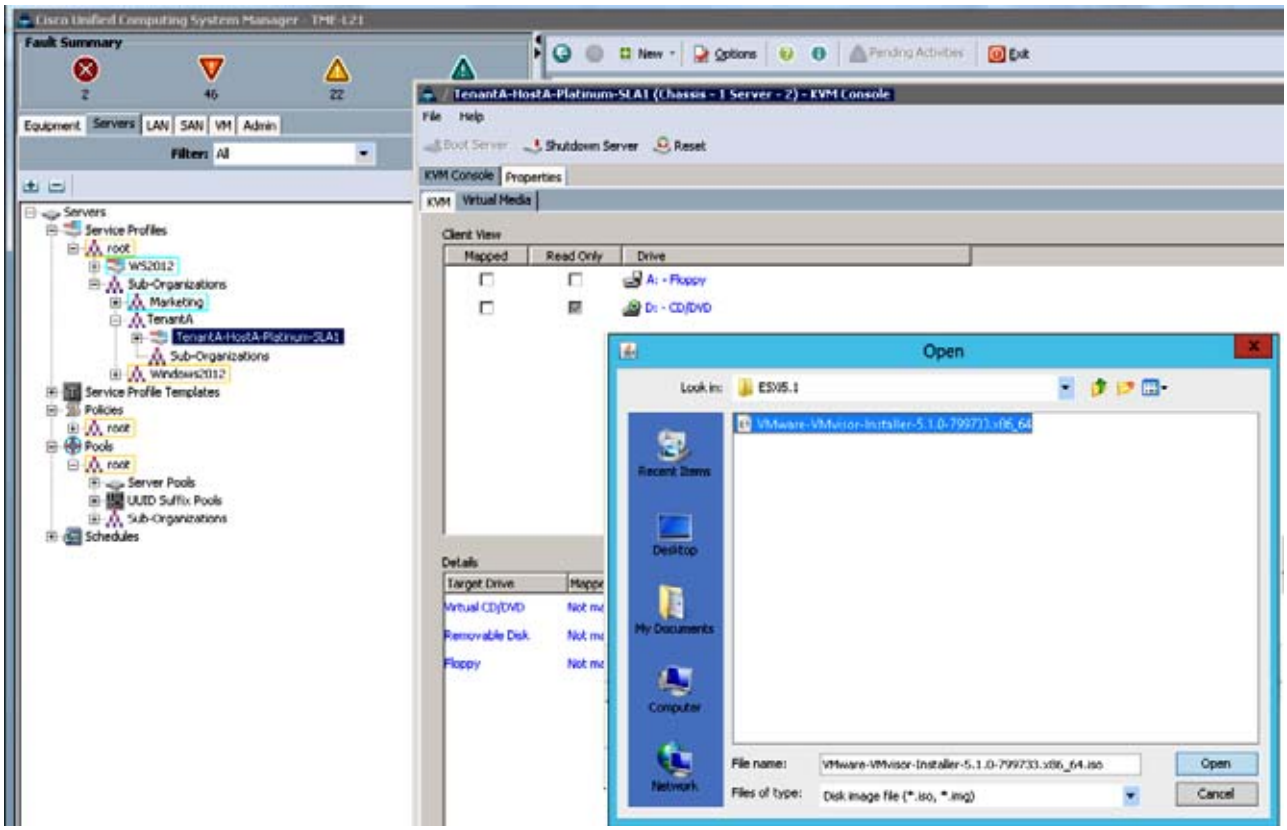
3. [TenantA] を展開します。[Tenant A-HostA-Platinum-SLA1] を選択します。[Actions] の下の右ペインで、[KVM Console] をクリックします。
4. [/TenantA-HostA-Platinum-SAL1 (Chassis -1 server -2) KVM Console] ポップアップ ウィンドウが起動します。

図 152　　KVM コンソールの起動



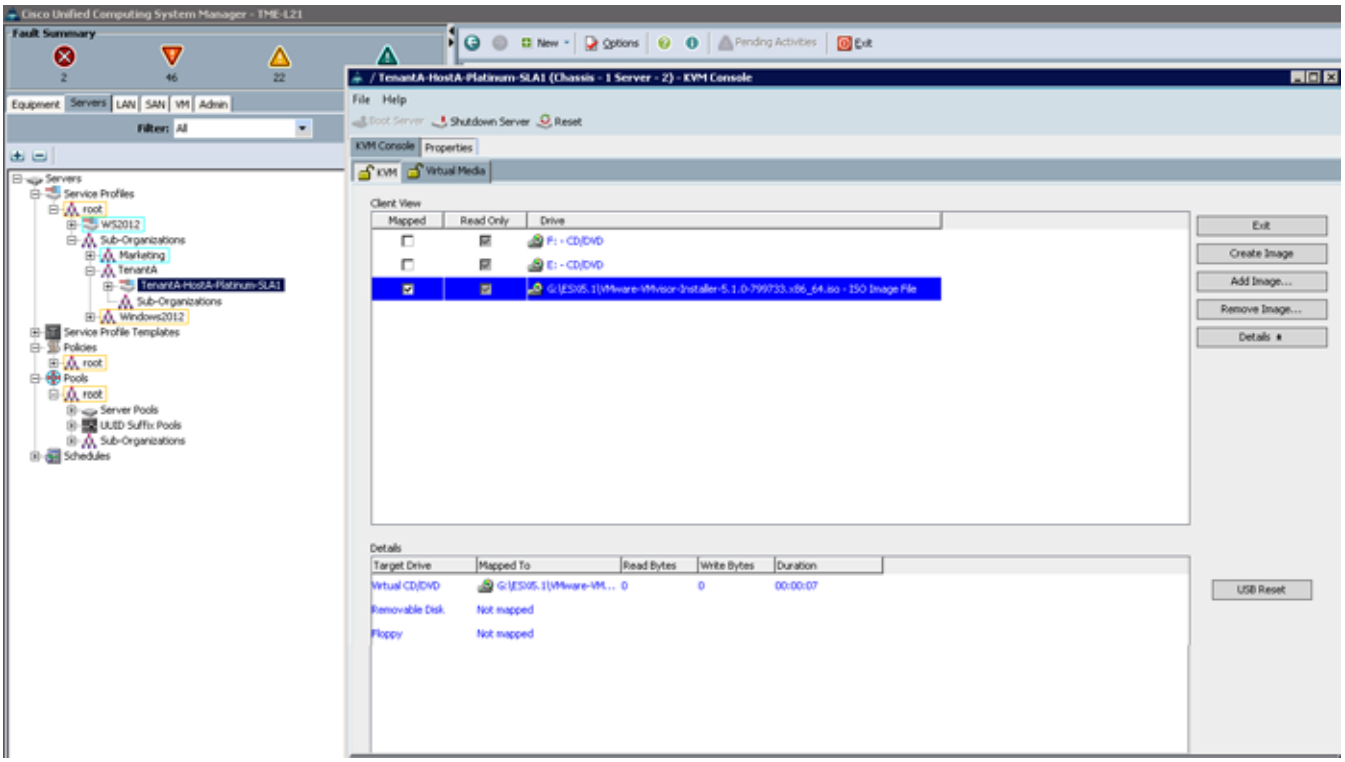
5. [KVM Console] ウィンドウで [Virtual Media] > [Add Image] > [Browse ESX Server 5.1 ISO] イメージを選択します。[Open] をクリックします。

図 153　　VMWare ESXi サーバ イメージの追加



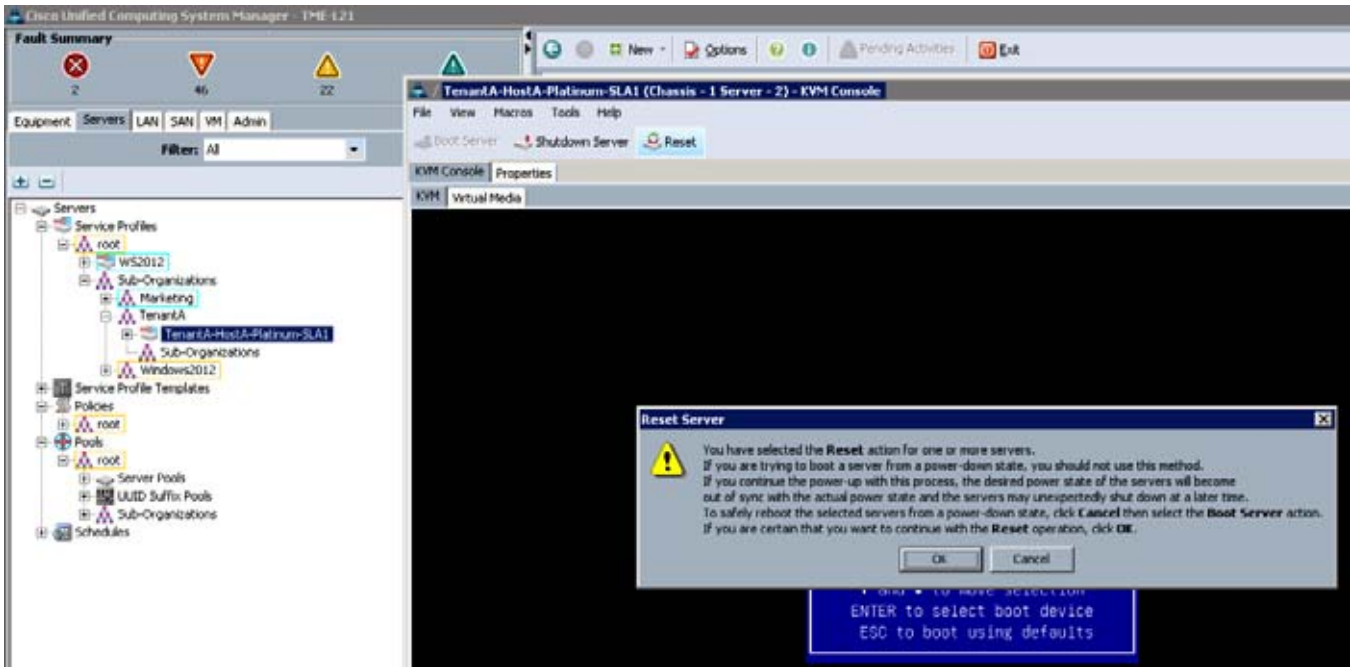
6. [Mapped] チェック ボックスをオンにし、[KVM Console] で [KVM] タブをクリックします。

図 154　　VMWare ESXi イメージの選択



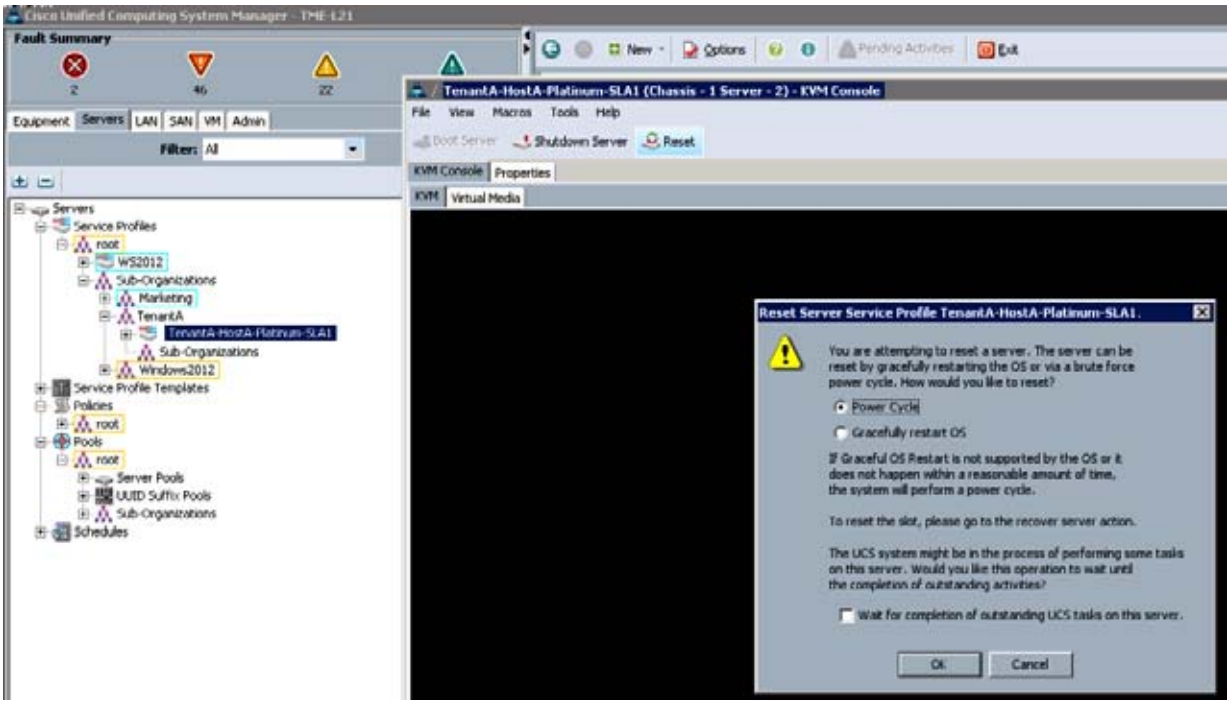
7. [Reset] ボタンをクリックし、[OK] をクリックします。

図 155　　サーバのリセット



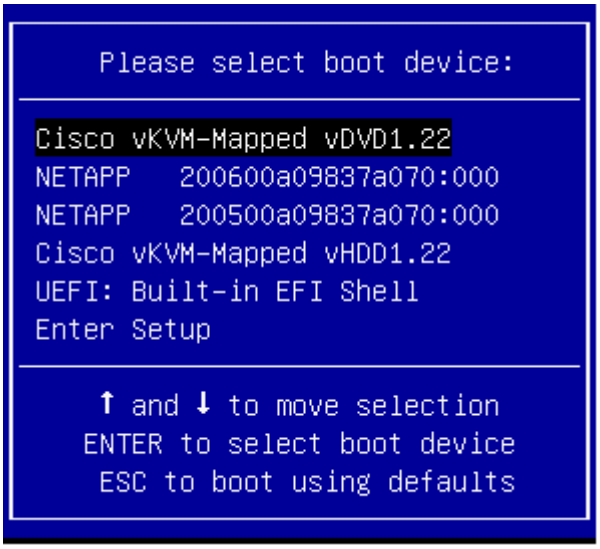
8. [Power Cycle] オプション ボタンをクリックし、[OK] をクリックします。

図 156　　サーバ サービス プロファイルでの電源再投入のリセット



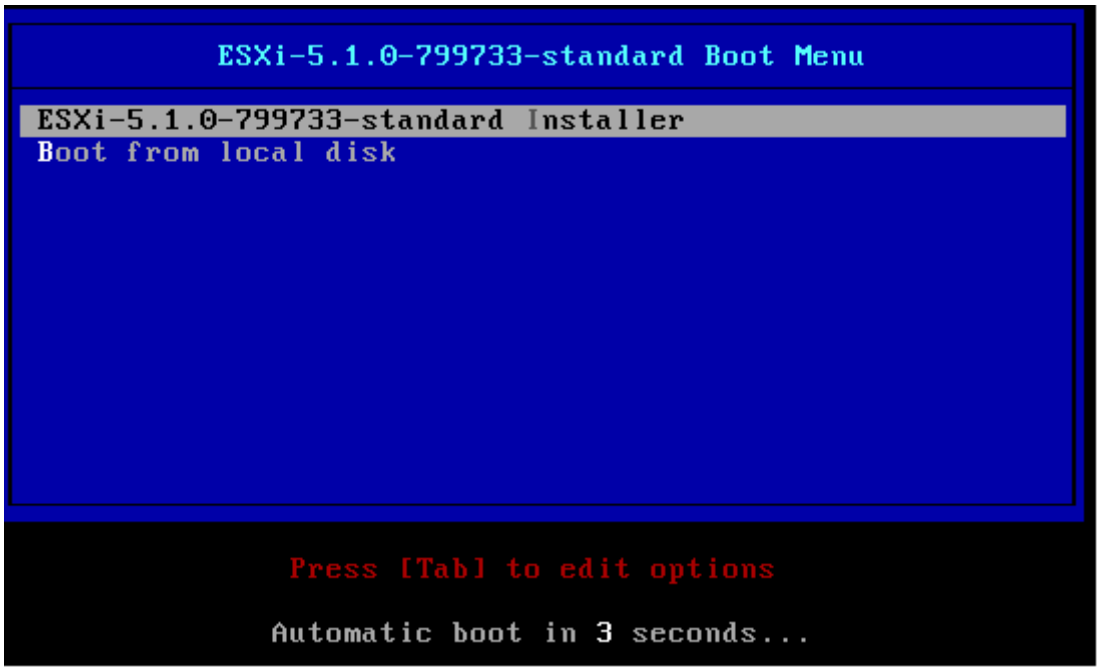
9. ブート メニューで [Cisco Virtual CD/DVD 1.22] オプションを選択し、Enter を押します。

図 157　　ブート デバイスの選択



10. ブート プロンプトで Enter を押します。[VMWare ESXi Server] が起動します。

図 158　VMWare ESXi サーバの起動

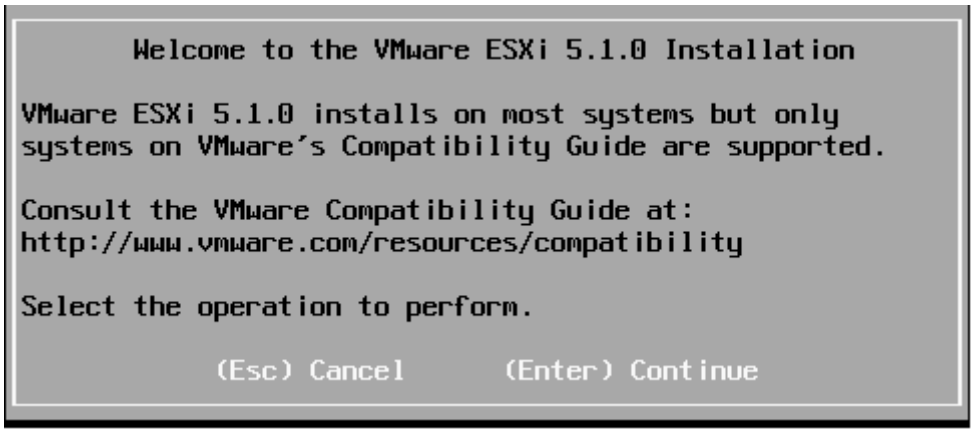


VMWare ESXi サーバのインストール

KVM コンソールで起動された VMWare ESXi サーバをインストールするには、次の手順を実行します。

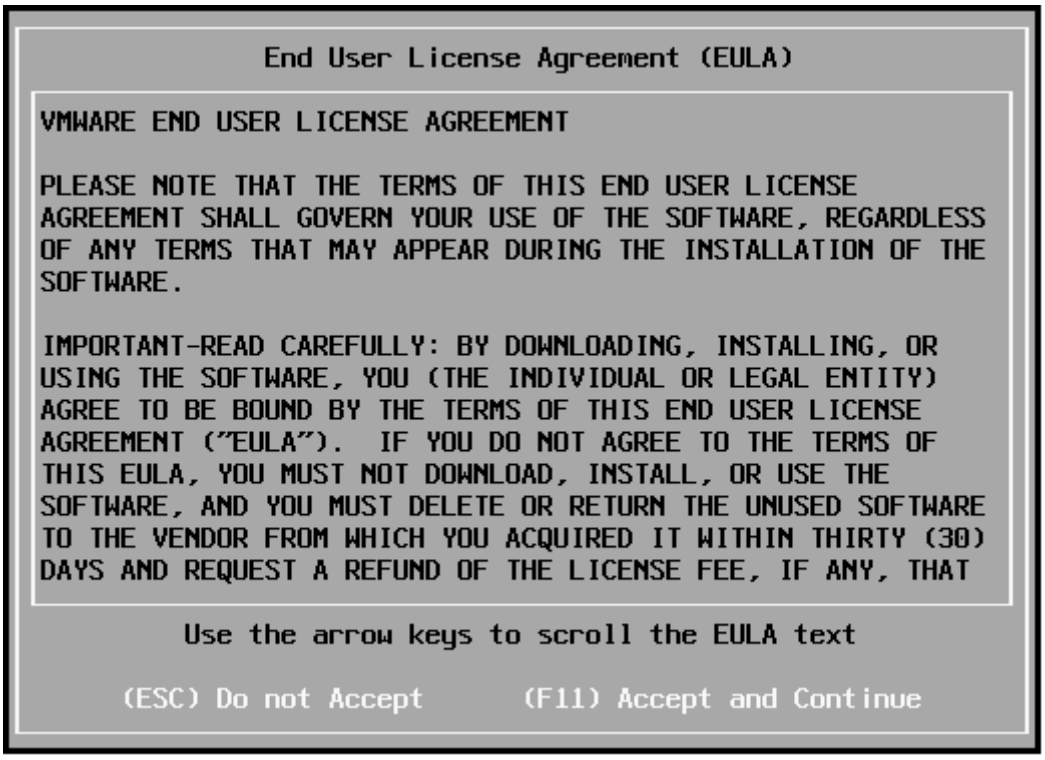
1. VMWare ESXi サーバをインストールします。
2. Enter を押して続行します。

図 159　[Enter] オプションの選択



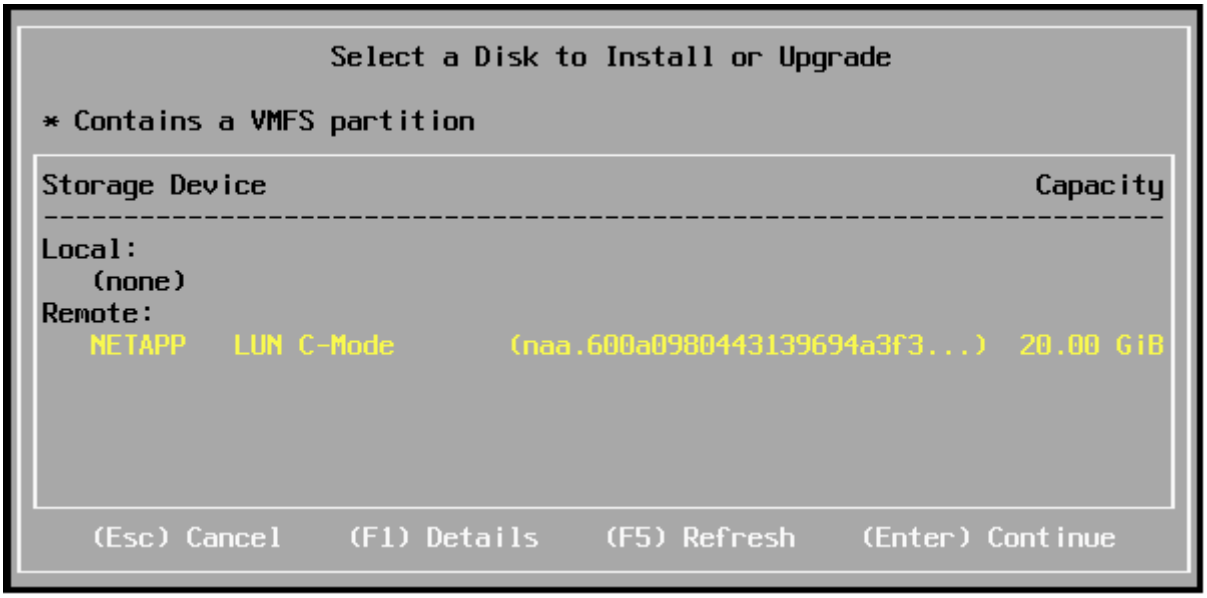
3. 同意して続行するには、[F11] を押します。

図 160　エンド ユーザ ライセンス



4. NetApp LUN C-Mode 20GB を選択します。
5. Enter を押して続行します。

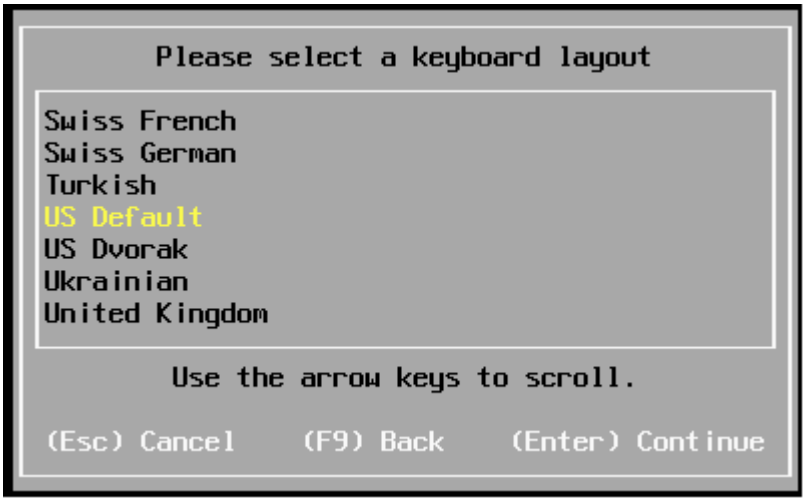
図 161　ディスクの選択



6. [US Default] を選択します。

7. Enter を押して続行します。

図 162　キーボード レイアウトの選択

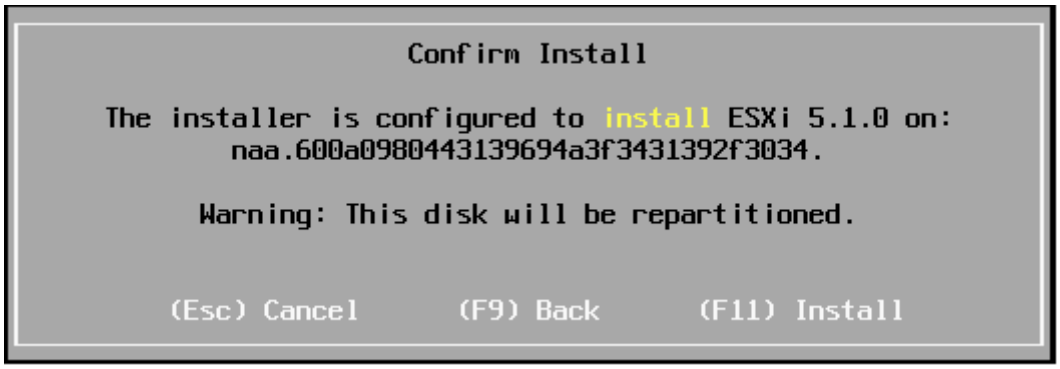


8. パスワードを入力します。
9. Enter を押して続行します。

図 163　パスワードの入力

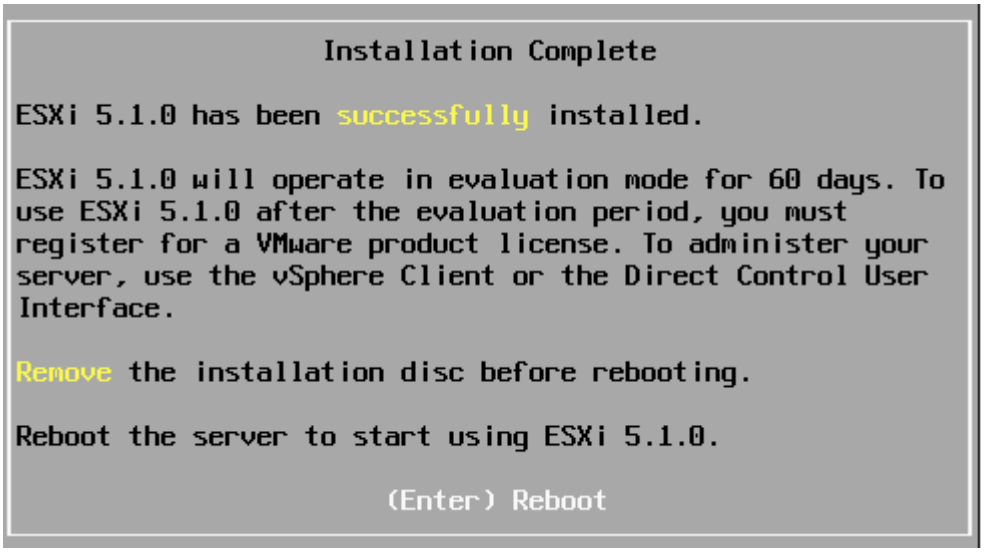
10. F11 を押してインストールを確認します。

図 164　　ESXi をインストールするディスクの定義



11. インストール後にリブートが必要です。VMWare ESXi 5.1 Host のインストール完了情報が表示されます。

図 165　　VMWare ESXi のインストール状態の表示



ホストの設定

この項では、マルチテナント クラウド環境でクラウド サービスをホストするために必要なサービス レベル定義を使用してインストールを完了した後に、クラウド ホスト上で VMWare ESXi 5.1 サーバを設定するために必要な手順の概要を説明します。

ホスト設定は 2 つのタスクに分割されています。

- ネットワーク タスク

  これは、テナント管理、ゲスト、およびプライマリまたはセカンダリ ストレージ（NFS）のネットワーク データ トラフィックのために、ESXi ホスト ネットワーキング インフラストラクチャの設計と設定を定義します。また、物理的および論理的な分離のほか、NIC チーミングおよびロード バランシング機能を使用した高可用性およびロード バランシングを提供します。

- ストレージ タスク

これは、テナントのプライマリ ストレージを作成するために ESXi ホスト ストレージ インフラストラクチャの設計と設定を定義します。これらは、後にクラウドにおけるマルチテナントのゾーンワイドなプライマリ ストレージ インフラストラクチャを定義するために Citrix CloudPlatform によって参照されます。

この項では、次のタスクを詳しく説明します。

- VMWare ESXi ホスト ネットワークの設定
- ファイバ チャネル ストレージ LUN 上の VMFS ベースのデータ ストアの作成

VMWare ESXi ホスト ネットワークの設定

この項では、管理、ゲストおよび NFS ストレージのネットワーク トラフィックのための、VMKernel インターフェイスでの仮想ネットワーク スイッチの設定について詳細に説明します。

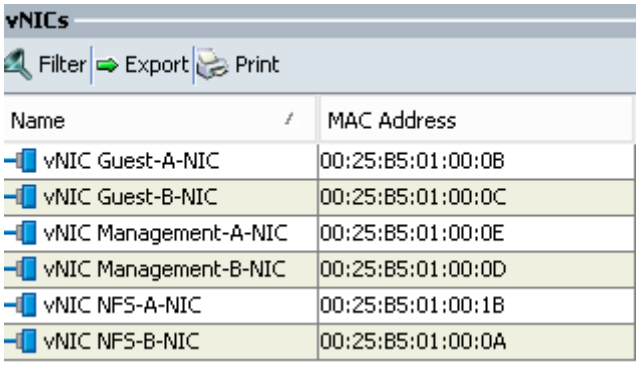
仮想ネットワーク スイッチにアップリンクされた各ネットワーク アダプタは、正しい Cisco UCS 仮想 NIC（vNIC）、つまりサービス プロファイル TenantA-HostA-Platinum-SLA1 で定義された VLAN と一致する必要があります。

表 32 は、UCS vNIC とマッピングしている Citrix ESXi ホスト ネットワーク ボンド イーサネット インターフェイスを示しています。

表 32　　UCS vNIC とマッピングしている ESXi vSwitch NIC インターフェイス

仮想ネットワーク スイッチ（vSwitch）	VNIC イーサネット インターフェイス	UCS サービス プロファイル vNIC
TenantA-Mgmt-Uplink	00:25:B5:01:00:0E	Management–A-NIC 00:25:B5:01:00:0E
	00:25:B5:01:00:0D	Management-B-NIC 00:25:B5:01:00:0D
TenantA-guest-Uplink	00:25:B5:01:00:0B	guest-A-NIC 00:25:B5:01:00:0B
	00:25:B5:01:00:0C	guest-B-NIC 00:25:B5:01:00:0C
TenantA-NFS-Uplink	00:25:B5:01:00:1B	NFS-A-NIC 00:25:B5:01:00:1B
	00:25:B5:01:00:0A	NFS-B-NIC 00:25:B5:01:00:0A

図 166　　Cisco UCS サービス プロファイル vNIC に対応する MAC アドレス



ESXi ホストでの管理ネットワーキングのセットアップ

ホストを管理するためには、VMware ホストごとに管理ネットワークを追加することが必要です。VMware ホストに管理ネットワークを追加するには、各 ESXi ホスト上で次の手順を実行します。

ESXi ホスト TenantA-ESX-HostA-Platinum-SLA1

管理ネットワークにアクセス可能な VM-Host-Infra-01 ESXi ホストを設定するには、次の手順を実行します。

1. サーバの再起動が完了したら、F2 を押してシステムをカスタマイズします。
2. root としてログインし、対応するパスワードを入力します。
3. [Configure the Management Network] オプションを選択して、Enter を押します。
4. [VLAN（Optional）] オプションを選択し、Enter を押します。
5. <<var_mgmt_vlan ID>> 603 を入力し、Enter を押します。

（注） このガイドでは、var_mgmt_vlan ID ラベルとして 603 を入力します。

6. [Configure Management Network] メニューから、[IP Configuration] を選択し、Enter を押します。
7. スペース キーを使用して、[Set Static IP Address] および [Network Configuration] オプションを選択します。
8. 最初の ESXi ホストを管理するための IP アドレスを入力します。<<10.65.121.163>> << var_vm_host_infra_01_ip>>。

（注） このガイドでは、var_vm_host_infra_01_ip ラベルとして 10.65.121.163 を入力します。

9. 最初の ESXi ホストのサブネット マスクを入力します。
10. 最初の ESXi ホストのデフォルトのゲートウェイを入力します。
11. Enter を押して IP の設定の変更を受け入れます。
12. [IPv6 Configuration] オプションを選択し、Enter を押します。
13. スペースバーを使用して、[Enable IPv6] を選択解除し（再起動が必要）、Enter を押します。
14. [DNS Configuration] オプションを選択し、Enter を押します。
15. 最初の ESXi ホストの DNS IP アドレスを入力します。

管理および NFS 仮想スイッチを設定するには、次の手順を実行します。

1. ESXi ホスト <<10.65.121.163 var_vm_host_infra_01_ip>> に対して SSH を実行します。
2. Root および <Password> 資格情報を提供します。
3. サービス プロファイルで定義されている適切なネットワーク アダプタを使用して、仮想スイッチおよびポート グループ <TenantA-Mgmt-Uplink> と <TenantA-NFS-Uplink> を作成します。

```
~ # esxcfg-vswitch -aTenantA-Mgmt-Uplink
~ #esxcfg-vswitch -a TenantA-NFS-Uplink
~ # esxcfg-vswitch TenantA-Mgmt-Uplink -A TenantA-Mgmt-Uplink
~ # esxcfg-vswitch TenantA-Mgmt-Uplink --link=vmnic3
~ # esxcfg-vmknic -a -i 10.65.121.165 -n 255.255.255.0 TenantA-Mgmt-Uplink
~ # esxcfg-vswitch TenantA-NFS-Uplink -A TenantA-NFS-Uplink
~ # esxcfg-vswitch TenantA-NFS-Uplink --link=vmnic2 vmnic5
```

図 167　ESXi vSwitch TenantA-Mgmt-Uplink および TenantA-NFS-Uplink 作成コマンド

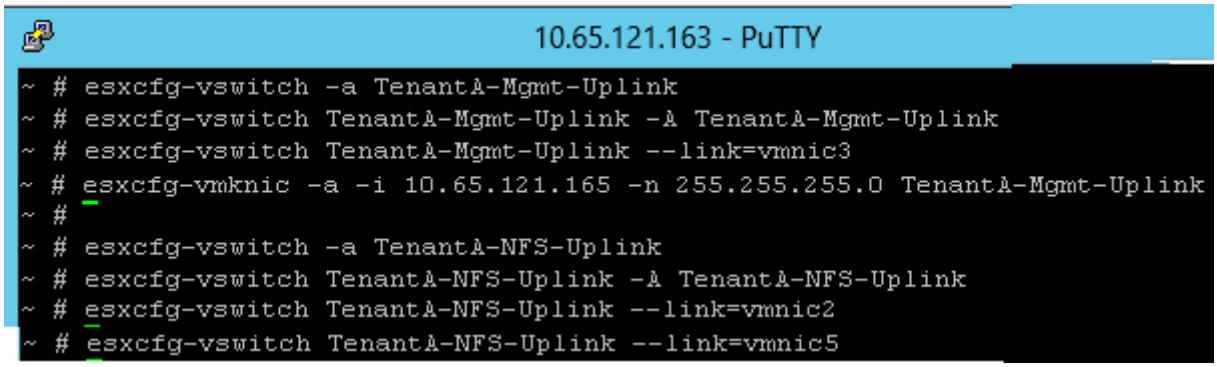
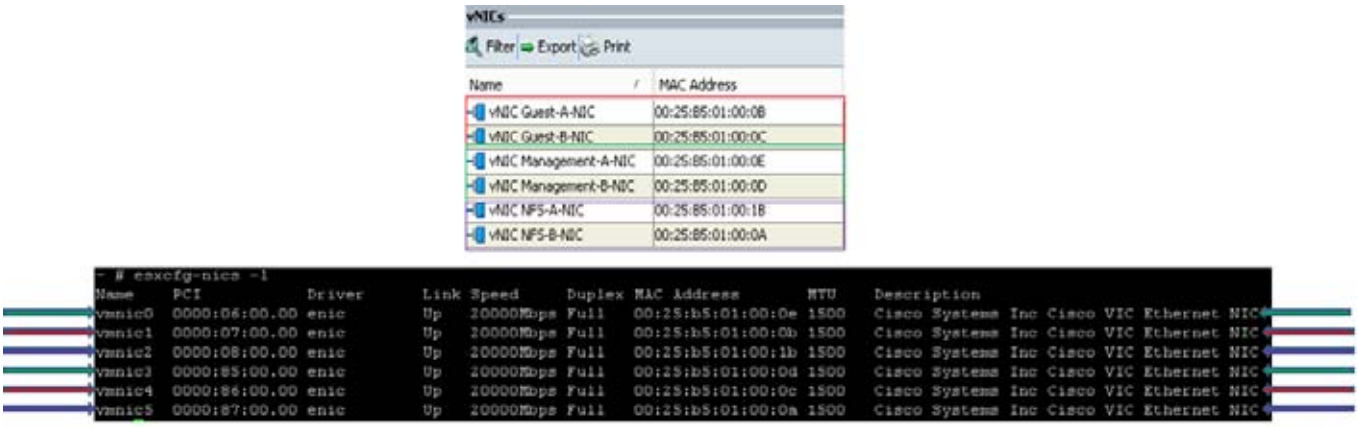


図 168　UCS サービス プロファイル スタティック vNIC とマッピングしている ESXi vSwitch TenantA-Mgmt-Uplink および TenantA-NFS-Uplink Pnic



4. VMware vSphere クライアントおよび vSphere Remote CLI をダウンロードします。
   a. 管理ワークステーションの Web ブラウザを開き、VM-Host-Infra-01 の新しく作成された vmkernel 管理 IP アドレス <10.65.121.165>（TenantA-Mgmt-Uplink ポート グループ）に移動します。
   b. vSphere クライアントと vSphere Remote コマンド ラインの Windows バージョンの両方をダウンロードしてインストールします。
5. VMware vSphere クライアントを使用して VMware ESXi ホストにログインします。
   a. 最後にダウンロードした VMware vSphere クライアントを開き、接続先ホストとして VM-Host-Infra-01 の IP アドレスを入力します。<<10.65.121.165 var_vm_host_infra_01_ip>>。
   b. ユーザに root を入力します。
   c. ルート パスワードを入力します。
   d. [Login] をクリックして接続します。
6. デフォルトの vSwitch0 を削除し、ネットワーク アダプタ vmnic0 を TenantA-Mgmt-Uplink に追加します。
   a. 各 vSphere クライアントから、インベントリのホストを選択します。
   b. [Configuration] タブをクリックします。

c. [Networking] ペインをクリックします。

d. 右ペインで、vSwitch0 の [Remove] をクリックします。

e. [Properties] をクリックします。

f. [Network Adapaters] をクリックします。

g. [Unclaimed Adapaters] の下で、[Add] をクリックし、[vmnic0] を選択します。

h. [Next] をクリックし、再度 [Next] をクリックし、[Finish] をクリックしてネットワーク アダプタを追加します。

7. TenantA-Mgmt-Uplink 仮想スイッチに VMKernel インターフェイスを追加して、vMotion データトラフィックにアクセスします。

a. 各 vSphere クライアントから、インベントリのホストを選択します。

b. [Configuration] タブをクリックします。

c. [Networking] をクリックします。

d. 右ペインで、vTenantA-Mgmt-Uplink の [Properties] をクリックします。

e. [Add] をクリックし、[VMKernel Connection type] オプション ボタンを選択します。

f. [Next] をクリックします。

g. [Network Label] テキスト ボックスに vMotion-VMKernel と入力します。

h. [VLaNID] テキスト ボックスに 192 (vMotion ID) と入力します。

i. [Use this port group for vMotion] チェック ボックスをオンにします。

j. [Use the following IP Setting] オプション ボタンをクリックします。

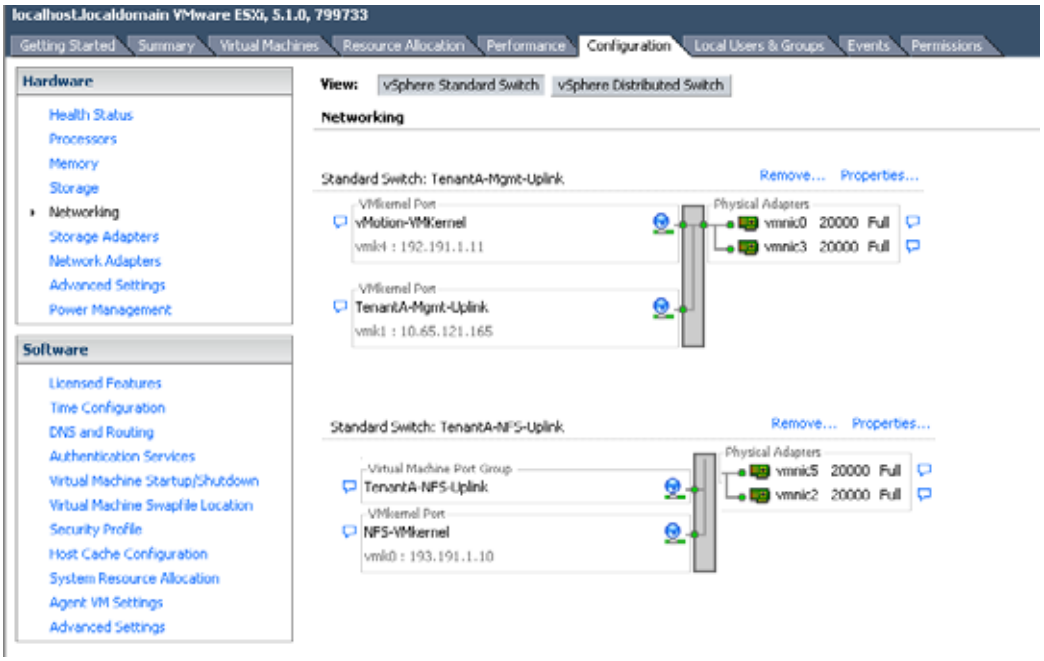
k. [IP Address] テキストボックスに 192.191.1.10 と入力し、[Subnet Mask] に 255.255.255.0 と入力します。

l. デフォルト ゲートウェイ IP アドレスを保持します。

m. [Next] をクリックします。

n. [Finish] をクリックします。

図 169　最終 ESX 仮想スイッチ設定



8. TenantA-NFS-Uplink 仮想スイッチに VMKernel インターフェイスを追加して、NFS データ トラフィックにアクセスします。
   a. 各 vSphere クライアントから、インベントリのホストを選択します。
   b. [Configuration] タブをクリックします。
   c. [Networking] をクリックします。
   d. 右ペインで、vTenantA-NFS-Uplink の [Properties] をクリックします。
   e. [Add] をクリックし、VMKernel 接続タイプ オプション ボタンを選択し、[Next] をクリックします。
   f. [Network Label:] テキスト ボックスに NFS-VMKernel と入力し、[Next] をクリックします。
   g. [Use the following IP Setting] オプション ボタンを選択します。
   h. [IP Address] テキストボックスに 193.191.1.1.10 と入力し、[Subnet Mask] に 255.255.255.0 と入力します。
   i. デフォルト ゲートウェイ IP アドレスを保持し、[Next] をクリックします。
   j. [Finish] をクリックします。
9. Cisco VIC の enic と fnic ドライバの更新されたバージョンをロードするには、各 vSphere クライアントのホストに対して次の手順を実行します。
   a. 各 vSphere クライアントから、インベントリのホストを選択します。
   b. [Summary] タブを選択して、環境の要約を表示します。
   c. [Resources Configuration] タブから、[Storage] を選択します。
   d. [datastore1] を右クリックし、[Browse Datastore] を選択します。
   e. 4 番目のボタンをクリックし、[Upload File] を選択します。
   f. ダウンロードした enic ドライバ バージョンの保存場所に移動し、net-enic-2.1.2.38-1OEM.500.0.0.472560.x86_64.zip を選択します。

g. [Open] をクリックしてファイルを開きます。

h. [Yes] をクリックして .zip ファイルを datastore1 にアップロードします。

i. 4 番目のボタンをクリックし、[Upload File] を選択します。

j. ダウンロードした fnic ドライバ バージョンの保存場所に移動し、scsi-fnic-1.5.0.20-1OEM.500.0.0.472560.x86_64.zip を選択します。

k. [Open] をクリックしてファイルを開きます。

l. [Yes] をクリックして .zip ファイルを datastore1 にアップロードします。

m. 管理ワークステーションから、以前にインストールした VMware vSphere Remote CLI を開きます。

n. コマンド プロンプトで、次のコマンドを実行して各ホスト（enic）を構成します。

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> software vib
install --no-sig-check -d
/vmfs/volumes/datastore1/net-enic-2.1.2.38-1OEM.500.0.0.472560.x86_64.zip
```

o. コマンド プロンプトで、次のコマンドを実行して各ホスト（fnic）を構成します。

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> software vib
install --no-sig-check -d
/vmfs/volumes/datastore1/scsi-fnic-1.5.0.20-1OEM.500.0.0.472560.x86_64.zip
```

p. vSphere クライアントから、インベントリ内の各ホストを右クリックし、[Reboot] を選択します。

q. [Yes] をクリックして続行します。

r. リブートの理由を入力し、[OK] をクリックします。

s. リブートが完了したら、vSphere クライアントを使用して両方のホストに再ログインします。

10. ESXi ホストに仮想イーサネット モジュール（VEM）をインストールするには、次の手順を実行します。

a. Web ブラウザを起動して http://<<var_vsm_mgmt_ip>> に移動します。

b. [cross_cisco-vem-v152-4.2.1.1.2.1.1a.0-3.1.1.vib] ハイパーリンクを右クリックし、[ave target as] を選択します。

c. 管理ワークステーションのデスクトップ上で、ファイルを cross_cisco-vem-v152-4.2.1.1.2.1.1a.0-3.1.1.vib として保存し、All Files と入力します。

d. vCenter に接続されている vSphere クライアントのメイン ウィンドウから、FlexPod Management クラスタの下でリスト内の最初のサーバをクリックします。

e. [Summary] タブをクリックします。

f. 右側のストレージの下で、[infra_datastore_1] を右クリックし、[Browse Datastore] を選択します。

g. ルート フォルダ（/）を選択し、上部にある 3 番目のボタンをクリックしてフォルダを追加します。

h. フォルダに VEM という名前を付け、[OK] をクリックします。

i. 左側で、[VEM] フォルダを選択します。

j. 上部にある 4 番目のボタンをクリックし、[Upload File] を選択します。

k. cross_cisco-vem-v152-4.2.1.1.2.1.1a.0-3.1.1.vib ファイルに移動し、[Open] をクリックします。

l. [Yes] をクリックします。VEM ファイルが、データストアの VEM フォルダに表示されます。

m. VMware vSphere CLI コマンド プロンプトを開きます。

n. VMware vSphere CLI の ESXi ホストごとに、次のコマンドを実行します。

```
esxcli -s <Host Server IP> -u root -p <Root Password> software vib install -v
/vmfs/volumes/infra_datastore_1/VEM/cross_cisco-vem-v152-4.2.1.1.2.1.1a.0-3.1.1.vi
b
```

11. ESX ホスト上の Cisco Nexus 1000V DVS スイッチに TenantA-guest-Uplink VMKernel PortGroup を追加します。

a. vCenter に接続されている VMware vSphere クライアントで、[Home] > [Networking] を選択します。

b. vCenter、データセンター、および Cisco Nexus 1000V のフォルダを展開します。

c. Cisco Nexus 1000V スイッチを選択します。

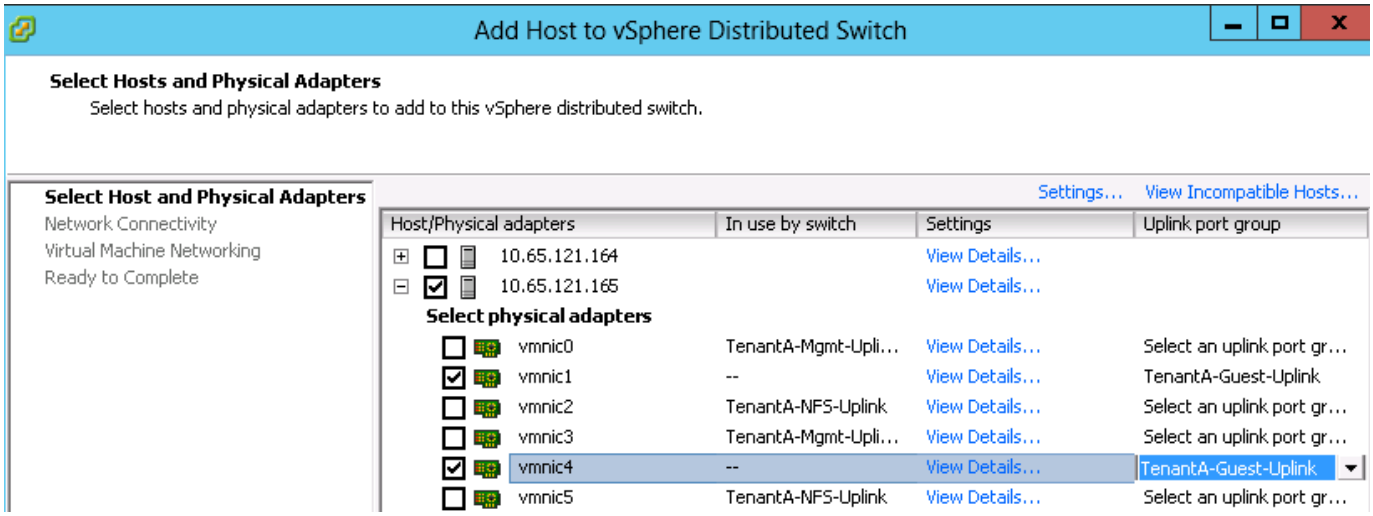
d. vSphere Distributed Switch の [Basic Tasks] の下で、[Add a Host] を選択します。

e. ホスト <var_vm_host_infra_01_ip label> 10.65.121.165 を選択します。

f. vmnic1 と vmnic4 ネットワーク アダプタを選択します。

g. [Uplink port group] リスト ボックスで、TenantA-guest-Uplinkport を選択します。

図 170　　Nexus 1000V DVS Switch へのホスト ネットワーク アダプタの追加

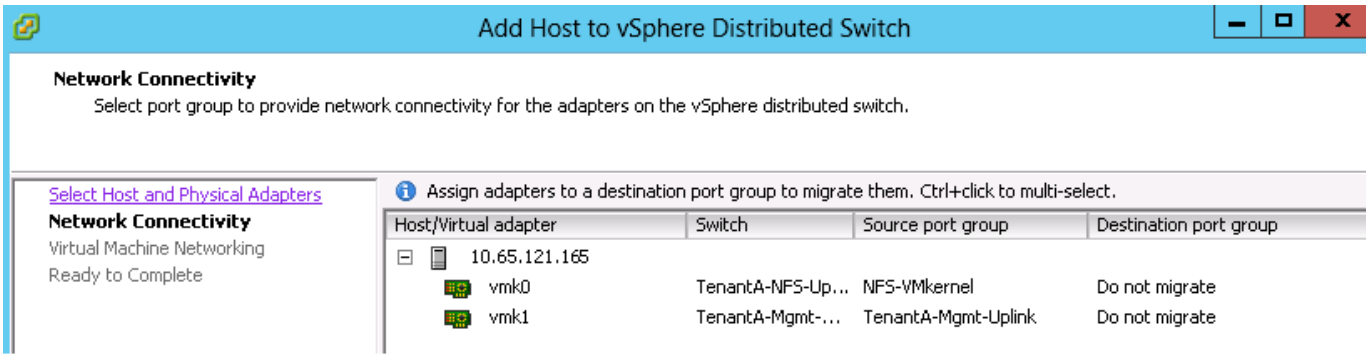


h. [Next] をクリックします。

i. VMKernel アダプタの vmk0 および vmk1 インターフェイスを Nexus 1000V DVS スイッチに移行しないでください。

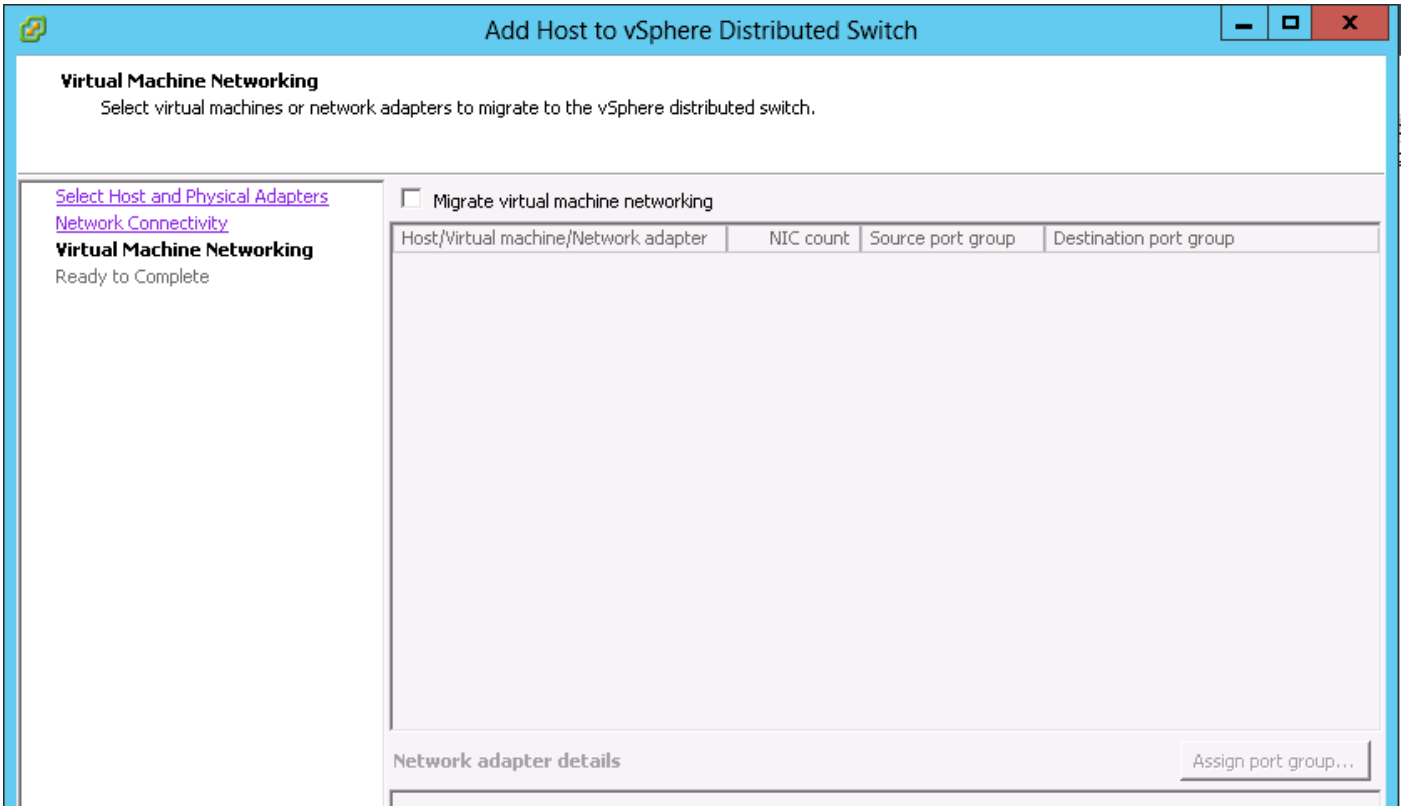
j. [Next] をクリックします。

図 171　　VMKernel インターフェイスを移行しない



k. [Next] をクリックします。

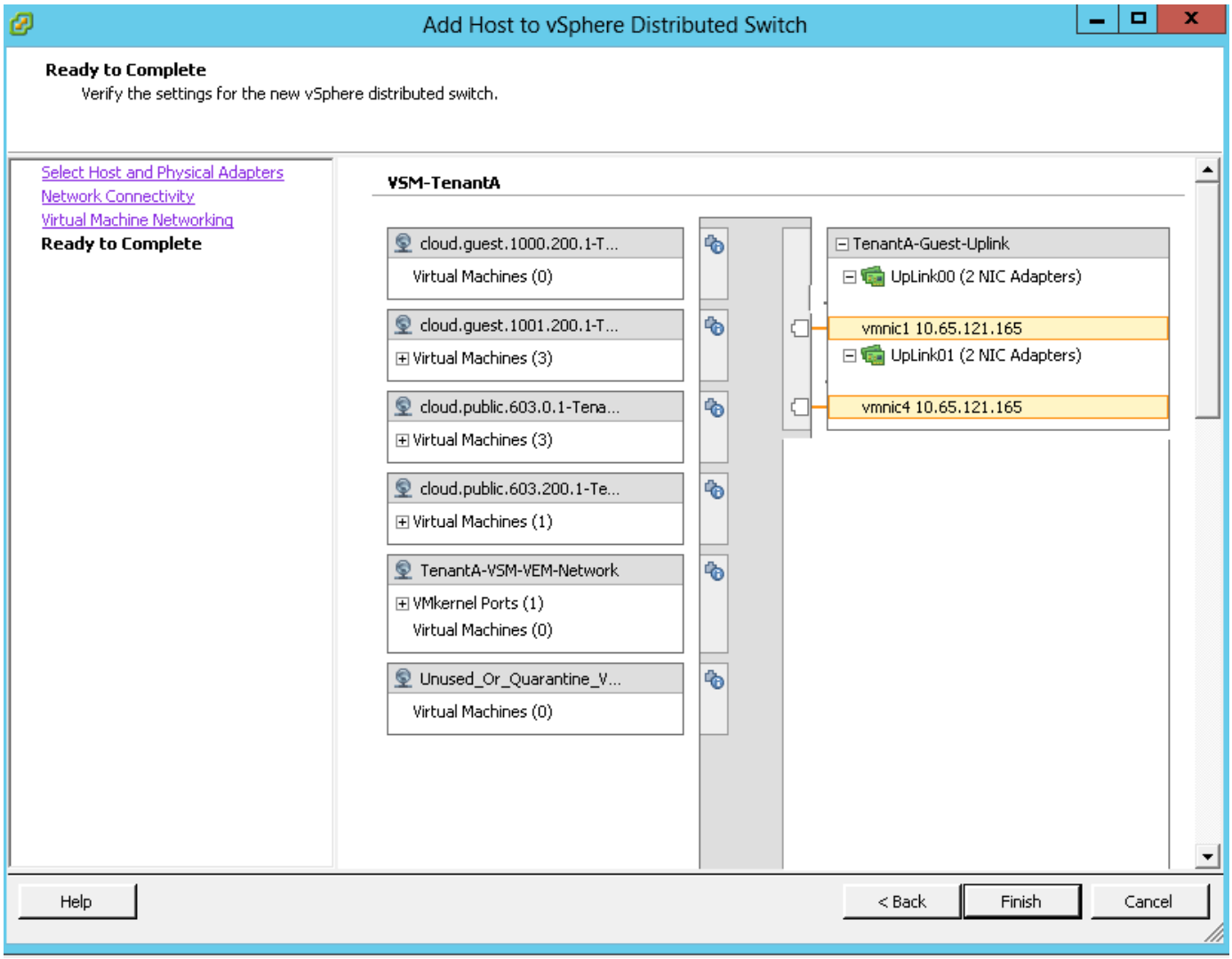
図 172　　移行する仮想マシン ネットワークなし



l. TenantA-guest-Uplink ポート グループの下に 2 つのネットワーク アダプタが一覧表示されていることを確認します。

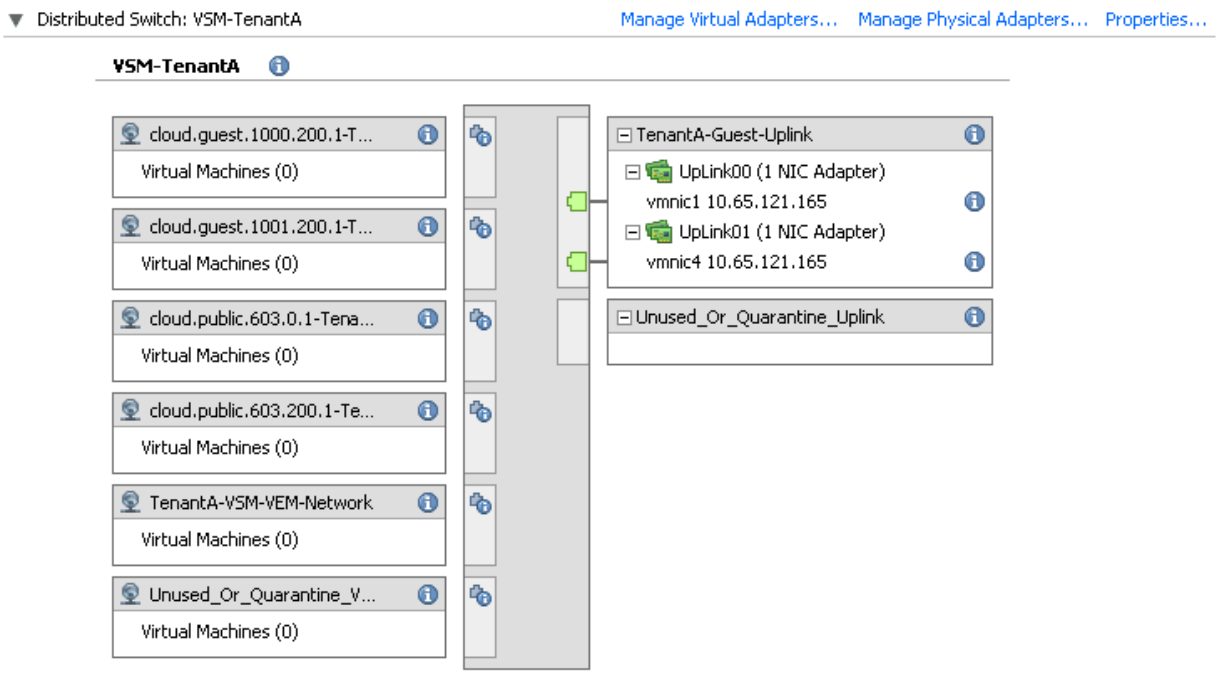
m. [Finish] をクリックします。

図 173　　ネットワーク アダプタの追加



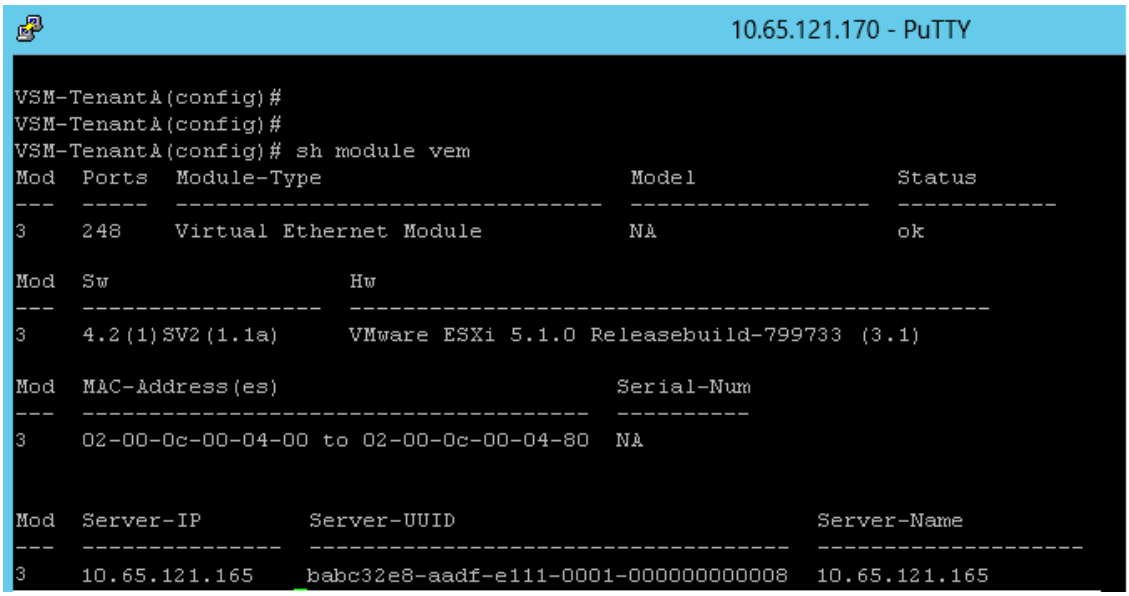
n. 仮想アダプタ リンク ステータスが Up で、ESX ホスト <<10.65.121.165>> が正常に Nexus 1000V DVS スイッチに追加されたことを確認します。

図 174　　Nexus 1000V DVS スイッチの設定



1. テナント ゲストデータ トラフィックにアクセスするために VMKernel インターフェイス Nexus 1000V DVS << VSM-TenantA>> を TenantA-guest-Uplink ポート グループに追加します。
   a. 各 vSphere クライアントから、インベントリのホストを選択します。
   b. [Configuration] タブをクリックします。
   c. [Networking] をクリックします。
   d. 右ペイン ビューで [vSphere Distributed Switch Properties on TenantA-NFS-Uplink] をクリックします。
   e. [Manage Virtual Adapaters] をクリックします。
   f. [Add] をクリックします。
   g. [New Virtual adapater] オプション ボタンをクリックします。
   h. [Next] をクリックします。
   i. VMKernel の仮想アダプタのタイプを選択し、[Next] をクリックします。
   j. リスト ボックスでポート グループ TenantA-VSM-VEM-Network を選択します。
   k. IP アドレス <10.65.121.169>、サブネット マスク <255.255.255.0> を入力し、ゲートウェイ フィールドはデフォルトのままにします。
   l. [Next] をクリックします。
   m. [Finish] をクリックします。
   n. [Close] をクリックします。
2. Nexus 1000V DVS スイッチ <<10.65.121.170>> の VEM モジュールを確認します。
   a. VSM IP アドレス <<10.65.121.70>> に telnet 接続します。
   b. コマンド ラインで show module vem と入力します。

図 175　　Nexus 1000V DVS の VEM モジュール



VMware vSphere 用 NetApp Virtual Storage Console

VSC 4.1 のインストール前の考慮事項

clustered Data ONTAP 8.1.2 を実行するストレージ システム上の VSC には、次のライセンスが必要です。

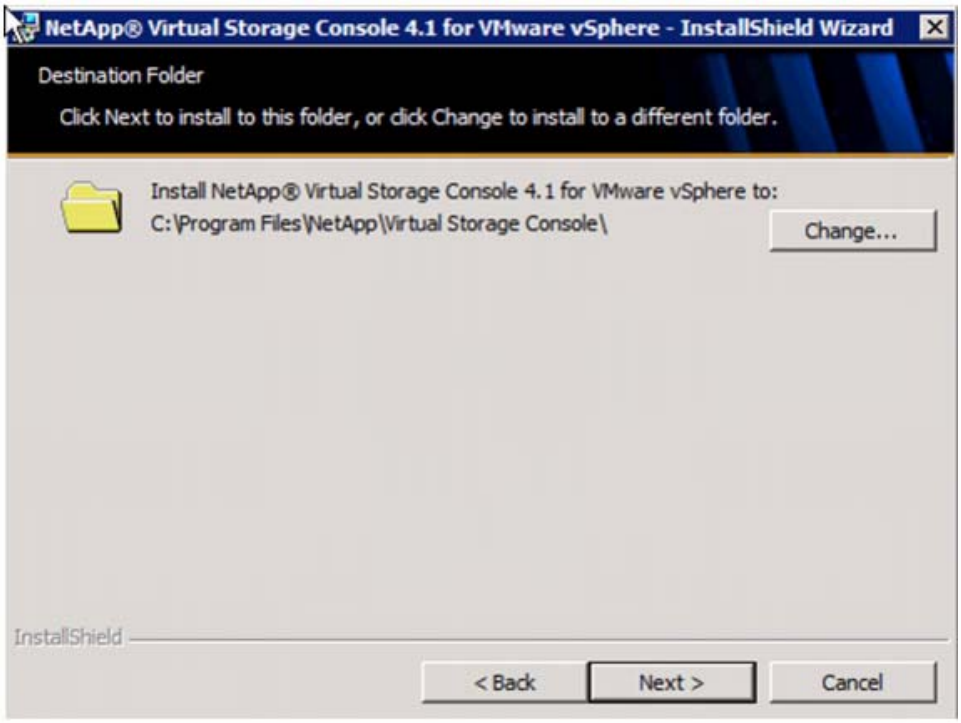
- プロトコル ライセンス（NFS および FCP）
- FlexClone（プロビジョニングおよびクローニングの場合のみ）
- VSC 4.1 をインストールします

VSC 4.1 ソフトウェアをインストールするには、次の手順を実行します。

1. Microsoft SQL サーバ VM の構築に関する項の手順を使用して、4 GB の RAM、2 つの CPU、および <<var_ib-mgmt_vlan_id>> VLAN で 1 つの仮想ネットワーク インターフェイスを持つ OnCommand 仮想マシンおよび VSC を構築します。仮想ネットワーク インターフェイスは VMXNET 3 アダプタにする必要があります。VM を起動して VMware ツールをインストールし、IP アドレスを割り当ててマシンを Active Directory ドメインに参加させます。VM 上に Adobe Flash Player の現在のバージョンをインストールします。VM 上に Windows の更新プログラムをすべてインストールします。
2. FlexPod 管理者ユーザとして VSC および OnCommand VM にログインします。
3. Virtual Storage Console 4.1 の x64 バージョンを次の場所からダウンロードしてください。NetApp サポート サイトの http://support.netapp.com/NOW/cgi-bin/software/?product=Virtual+Storage+Console&platform=VMware+vSphere。
4. ダウンロードしたファイルを右クリックし、[Run As Administrator] を選択します。
5. ユーザ アクセス制御の警告で [Yes] をクリックします。
6. [Installation wizard welcome] ページで、[Next] をクリックします。
7. バックアップおよびリカバリ機能を選択します。

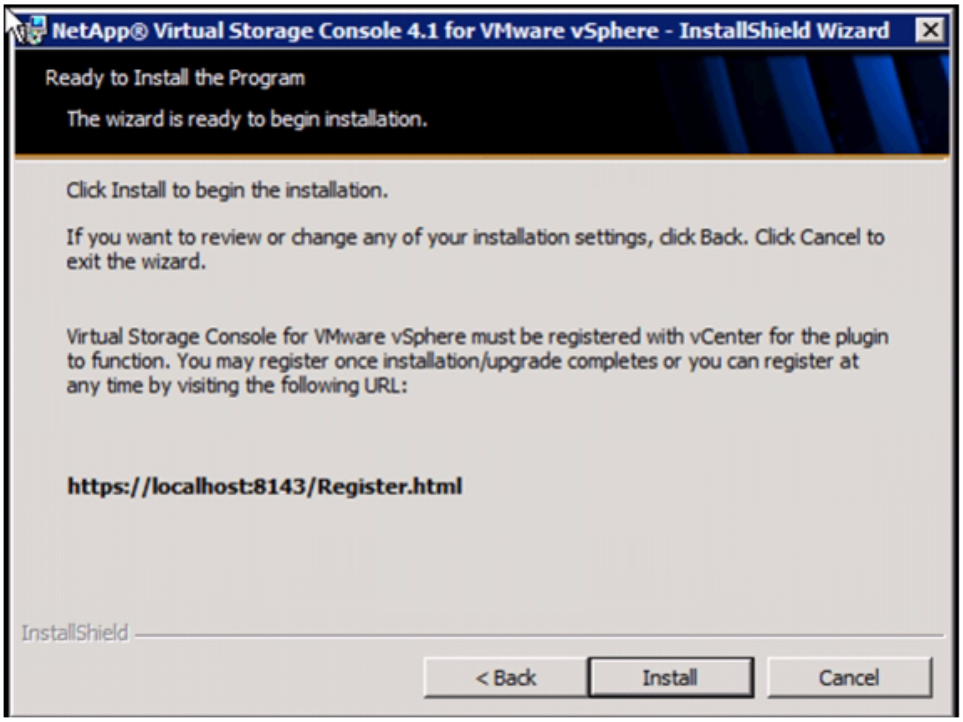
8. [Next] をクリックします。
9. [Next] をクリックしてデフォルトのインストール場所を指定します。

図 176　　VSC のインストール場所



10. [Install] をクリックします。

図 177　　VSC 4.1 をインストールする準備ができました



11. [Finish] をクリックします。

vCenter Server への VSC の登録

vCenter Server に VSC を登録するには、次の手順を実行します。

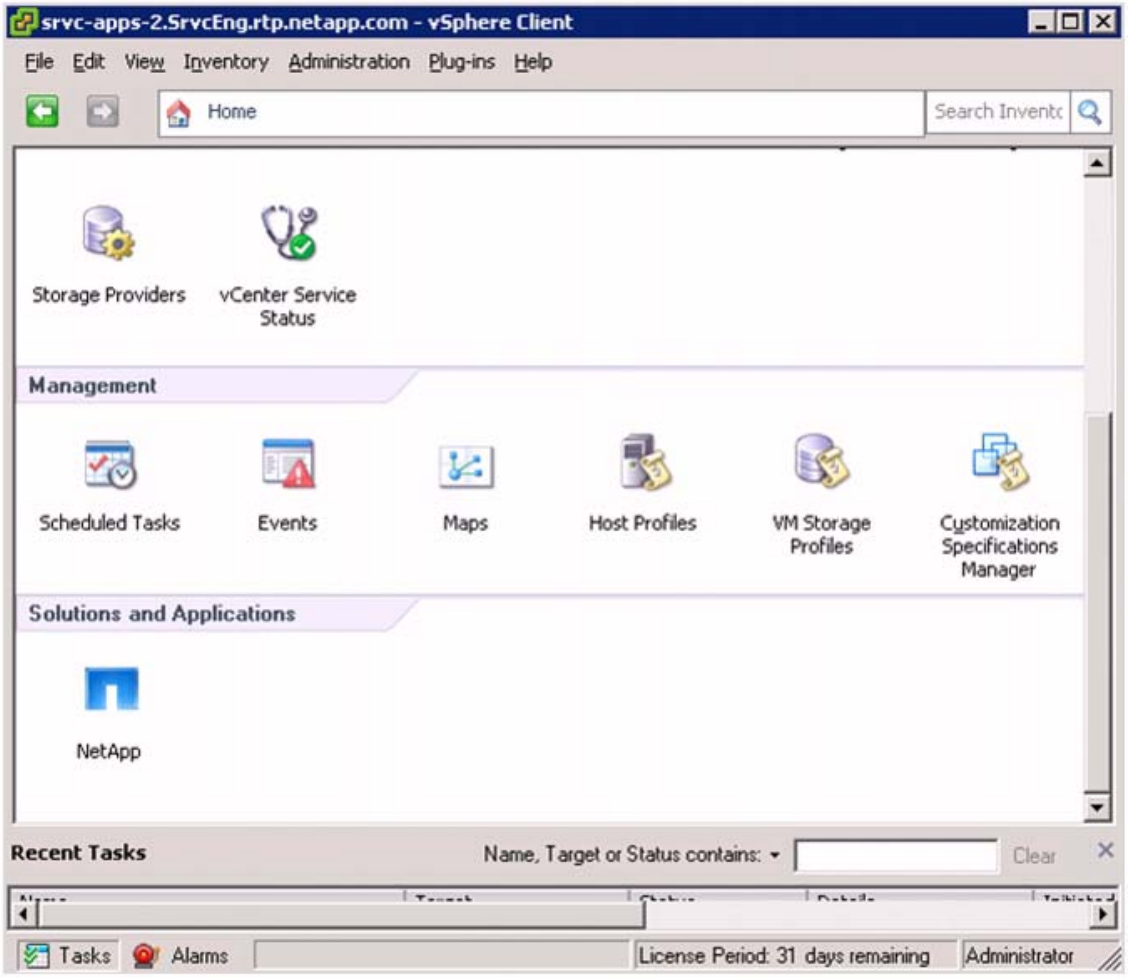
1. インストール フェーズが完了すると、登録 URL のあるブラウザ ウィンドウが自動的に開きます。
2. [Continue to this website（not recommended）] をクリックします。
3. [Plug-in Service Information] セクションで、vCenter Server が VSC サーバにアクセスするために使用するローカル IP アドレスをドロップダウン リストから選択します。
4. [vCenter Server Information] セクションで、vCenter Server のホスト名または IP アドレス、ユーザ名（FlexPod 管理者ユーザ）、およびユーザ パスワードを入力します。
5. [Register] をクリックして、登録を完了します。

ストレージ リソースの検出および追加

モニタリングとホストの設定およびプロビジョニングとクローニング機能のためにストレージ リソースを検出するには、次の手順を実行します。

1. vSphere クライアントを使用して、FlexPod 管理者ユーザとして vCenter Server にログインします。vSphere クライアントがすでに開かれている場合は、それを閉じてから、再度開きます。
2. [vSphere Client] ウィンドウの左側にある [Home] タブをクリックします。
3. [Solutions and Applications] で、[NetApp] をクリックします。

図 178　　ストレージ リソースの追加

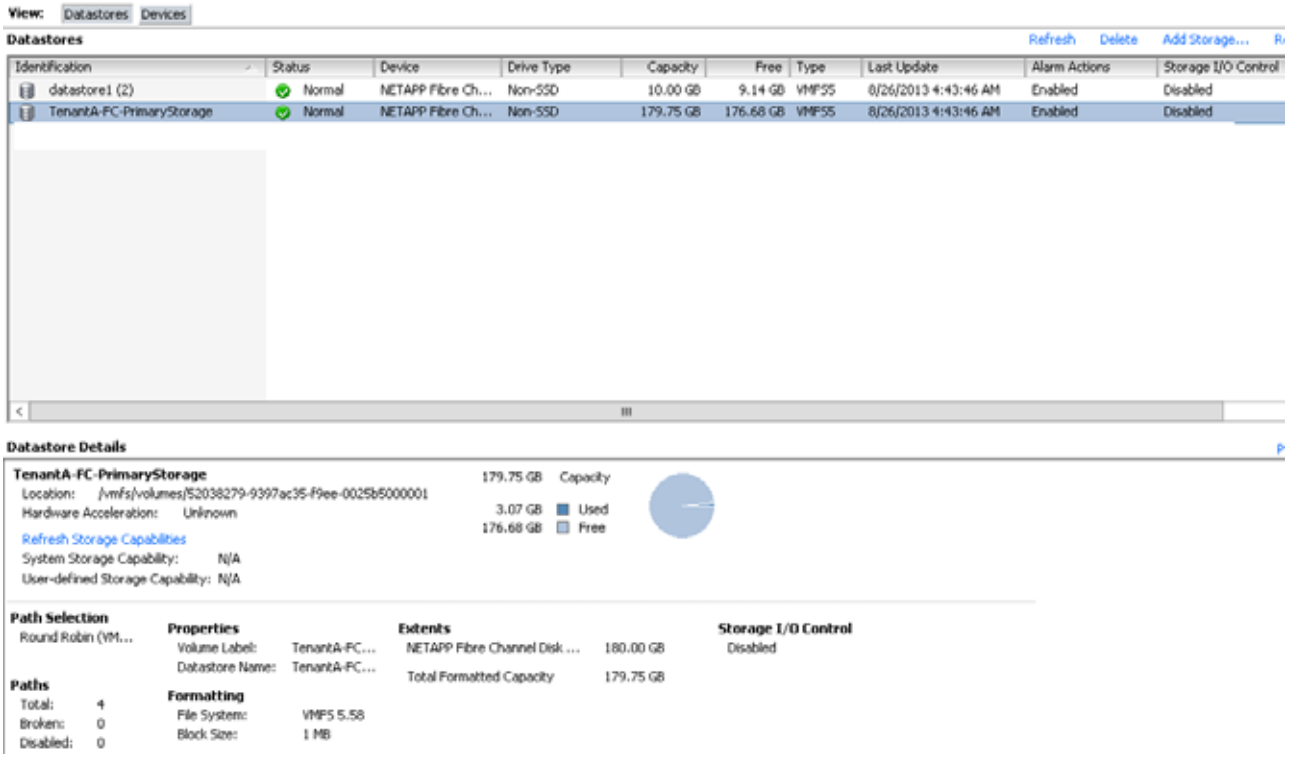


4. セキュリティ証明書の警告が表示されると、[Yes] をクリックします。証明書を表示する場合は、[View Certificatet] をクリックします。
5. デフォルトで選択されていない場合は、ナビゲーション ペインで [Monitoring and Host Configuration] を選択します。
6. 記憶域コントローラのリストで、一覧表示されている最初のコントローラを右クリックし、[Modify Credentials] を選択します。
7. [Management IP address] フィールドにストレージ クラスタの管理 IP アドレスを入力します。ユーザ名に admin を、パスワードに管理者パスワードを入力します。[Use SSL] が選択されていることを確認します。
8. [OK] をクリックします。
9. コントローラ特権を受け入れる場合は、[OK] をクリックします。
10. ストレージ プロビジョニング、ストレージ効率ツール、レポート、およびバックアップとリカバリの詳細については、『VSC Administration Guide』を参照してください。

ファイバ チャネル LUN でのプライマリ ストレージの作成

1. vCenter に接続されている VMware vSphere クライアントで、[Home] > [Hosts and Clusters] を選択します。
2. vCenter、データセンター、および ESX ホスト <var_vm_host_infra_01_ip label > 10.65.121.165 を展開します。
3. [Hardware] で [Storage] をクリックします。
4. [Add Storage] をクリックします。
5. [Disk/LUN] オプション ボタンを選択します。
6. [Next] をクリックします。
7. [NetApp LUN =2] を選択します。
8. [Next] をクリックします。
9. [VMFS-5] オプション ボタンを選択します。
10. [Next] をクリックします。
11. [Next] をクリックしてパーティションを作成します。
12. [Next] をクリックします。
13. TenantA-FC-PrimaryStorage と入力します。
14. [Next] をクリックします。
15. [Maximum available space] オプション ボタンを選択します。
16. [Next] をクリックします。
17. [Finish] をクリックします。
18. [Darastores] の下でデータストア <<TenantA-FC-PrimaryStorage>> が作成されていることを確認します。

図 179　データストア TenantA-FC-PrimaryStorage が NetApp ファイバ チャネル LUN にマップされる



クラウド導入の設計

管理サーバは、ゲスト仮想マシンが実行されるホスト コンピュータを含む 1 つ以上のゾーン（通常はデータセンター）を管理します。クラウド インフラストラクチャの構成は、次のとおりです。

- ゾーン

  通常、1 つのゾーンは単一のデータセンターに相当します。ゾーンは、1 つ以上の Pod およびセカンダリ ストレージから構成されます。

- Pod

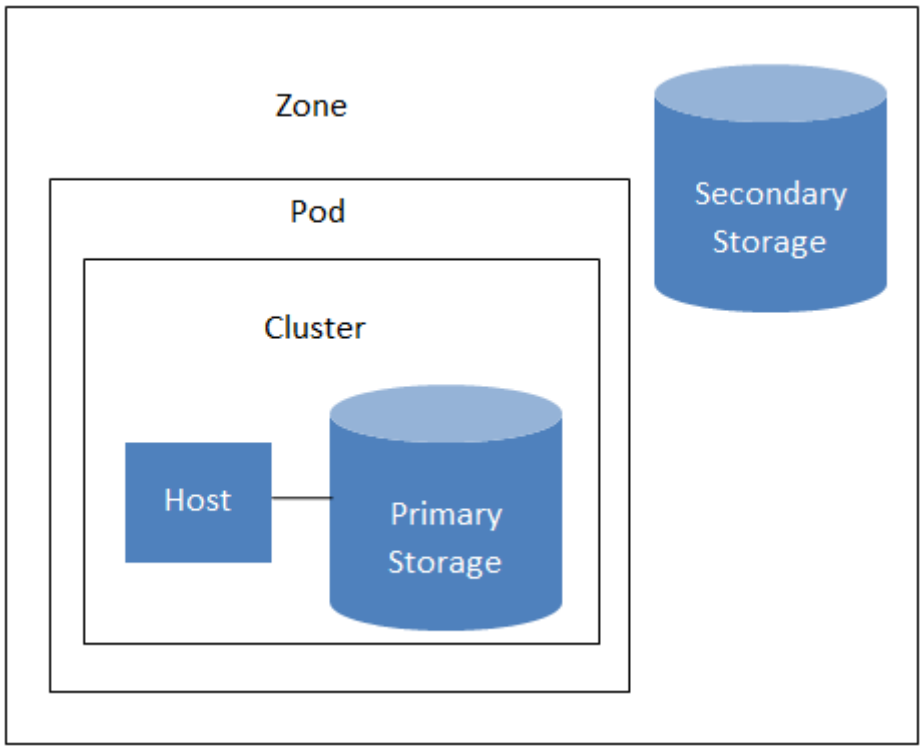
  Pod は通常、レイヤ 2 スイッチおよび 1 つ以上のクラスタを含む 1 個のハードウェアのラックです。

- クラスタ
- クラスタは、1 つ以上のホストおよびプライマリ ストレージから構成されます。
- ホスト

  クラスタ内の単一のコンピューティング ノードです。ホストは、実際のクラウド サービスがゲスト仮想マシンの形式で実行される場所です。

- プライマリ ストレージは、クラスタに関連付けられ、そこにそのクラスタ内のホストで実行されているすべての VM のディスク ボリュームが格納されます。
- セカンダリ ストレージは、ゾーンに関連付けられ、そこにテンプレート、ISO イメージ、およびディスク ボリュームのスナップショットが格納されます。

図 180　CloudPlatfrom クラウド プロビジョニングの論理ビュー



この項では、マルチテナント用にホストされるプライベート クラウドを作成するために必要な Citrix CloudPlatform のコンピューティング、ネットワークおよびストレージ インフラストラクチャ設計の概要を説明します。

CloudPlatform は、サービス クラウド管理プラットフォームとしてマルチハイパーバイザ、マルチテナント、高可用性インフラストラクチャです。また、クラウド インフラストラクチャ統合レイヤを提供し、IaaS コンポーネント（仮想サーバなど）の作成、プロビジョニングおよび設定の自動化を実現します。

さらに、ユーザがクラウドを利用する方法を制御するために、ロール ベースのアクセス機能を提供して、使用率課金、ユーザの自己管理、承認済みの仮想マシン テンプレート ライブラリ、およびセキュリティ コントロールをセットアップします。

クラウド インフラストラクチャを管理および設定するために、Citrix は、パブリック、プライベート、およびハイブリッドのクラウド ネットワークを構築するためコンピューティング リソースをプールするソフトウェア プラットフォームである CloudPlatform を提供します。CloudPlatform は、クラウド インフラストラクチャを構成するネットワーク、ストレージ、およびコンピューティング ノードを管理します。CloudPlatform を使用して、クラウド コンピューティング環境を導入、管理、および設定します。

このマニュアルでは、Citrix CloudPlatform 4.2.1 ソフトウェア バージョンが Cisco B-200 M3 ブレード サーバ上の RHEL 6.0.3 オペレーティング システム上にインストールされます。このマニュアルは、単一ユーザ モードで CloudPlatform 4.2.1 をインストールする手順を説明します。

（注）　障害時にも高可用性をサポートするには、マルチユーザ モードで CloudPlatfrom をインストールすることを推奨します。

以下の表は、管理、NFS および PXE ネットワークにアクセスするために設定されているネットワークインターフェイス、およびそれに対応する IP アドレス（VLAN ID）を示しています。

CloudPlatfrom ホストがインターネットにアクセスでき、ping に応答可能であり、以下の表 33 で定義されているネットワークにアクセスするようにルートが正しく設定されていることを確認します。

表 33　　イーサネット インターフェイスおよび IP アドレス（VLAN ID）の詳細

イーサネット インターフェイス名	IP アドレス（VLAN ID）	ネットワークアクセス
Eth0	<var_vm_host_infra_01_ip_mgnt> 10.65.121.70 (603)	管理アクセス
Eth1	<var_host_infra_01_NFS_ip> 193.191.1.10 (193)	NFS アクセス
Eth2	<var_host_infra-01_PXE_ip> 20.1.1.5 (20)	PXE アクセス

単一ユーザ モードでの CloudPlatfrom のインストール

この項では、単一の管理サーバをインストールする方法および同じノードに MySQL をインストールする方法について説明します。

管理サーバをホストするために RHEL 6.0.3 OS を準備するには、次の手順を実行します。

1. root として OS にログインします。
2. 完全修飾ホスト名であることを確認します。# hostname --fqdn。
3. これにより、「kvm1.lab.example.org」のような完全修飾ホスト名が返されます。完全修飾ホスト名が返されない場合は、/etc/hosts を編集します。
4. デフォルトで SELinux を制限しない（permissive）ように設定します。
5. RHEL または CentOS で、デフォルトで SELinux がインストールされ、有効になります。それを確認するには # rpm -qa | grep selinux 実行します。
6. /etc/selinux/config の SELINUX 変数を permissive に設定します。これにより、システムのリブート後に permissive 設定が維持されます。

```
# vi /etc/selinux/config
```

7. 次に、システムをリブートすることなく、ただちに permissive が開始されるように SELinux を設定します。

```
# setenforce 0
```

8. マシンがインターネットに到達できることを確認します。

```
# ping www.goggle.com
```

9. https://www.citrix.com/English/ss/downloads/ から CloudPlatform 管理サーバをホストにダウンロードします。
10. CloudStack 4.2 一覧で CloudPlatform 4.2.1 を選択します。

（注）　MyCitrix アカウントが必要です。

11. CloudPlatform パッケージをインストールします。CloudStack-VERSION-N-OSVERSION.tar.gz の形式のファイルがあります。ファイルを untar し、そこに含まれる install.sh スクリプトを実行します。次のファイルとディレクトリ名を、使用しているものに置き換えます。

```
# tar xzf CloudStack-VERSION-N-OSVERSION.tar.gz
# cd CloudStack-VERSION-N-OSVERSION
# ./install.sh
```

12. インストーラが準備している間にいくつかのメッセージが表示され、その後に選択肢のリストが表示されます。

```
Choose M to install the Management Server software.
Install the Agent
Install BareMetal Agent
Install the Usage Monitor
Install the CloudPlatform packages installed on this computer
Stop any running CloudPlatform services and remove the CloudPlatform packages from
this computer
Remove the MySQL server (will not remove the MySQL databases)
Quit
```

13. 「Complete!Done.」などのメッセージを待ちます。

14. インストールが終了すると、次のコマンドを実行して重要なサービスを起動します（コマンドは OS によって異なる場合があります）。

```
# service rpcbind start
# service nfs start
# chkconfig nfs on
# chkconfig rpcbind on
```

15. インストールを続行し、データベースを設定します。管理サーバ ノードに MySQL のバージョンがすでにインストールされている場合は、その MySQL のバージョンに応じて、次の選択項目のいずれかを実行します。

    a. MySQL バージョン 5.1.58 以降がすでにインストールされている場合は、ステップ 18 に進みます。

    b. 5.1.58 よりも前のバージョンの MySQL がインストールされている場合は、ステップ 18 に進むか、MySQL をアンインストールするか、ステップ 10 に進んで新しいバージョンをインストールすることができます。

16. CloudPlatfrom 管理サーバをインストールしている同じマシンで、install.sh を再実行します。

```
./install.sh
```

17. 分散リポジトリから MySQL サーバをインストールするには、D を選択します。

```
> D
```

18. MySQL 設定（OS に応じて /etc/my.cnf または /etc/mysql/my.cnf）を編集し、「mysqld」セクションに次の行を挿入します。これらの行は、datadir 行の下に挿入できます。max_connections パラメータは、導入する管理サーバの数に 350 をかけた値にしてください。この例では、1 台の管理サーバを想定しています。

```
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=350
log-bin=mysql-bin
binlog-format = 'ROW'
```

19. MySQL サービスを再起動し、ルート ユーザとして MySQL を起動します。

```
# service mysqld restart
# mysql -u root
```

20. RHEL および CentOS では、デフォルトで MySQL に root パスワードは設定されていません。セキュリティの注意事項として root パスワードを設定することを強くお勧めします。次のコマンドを実行し、専用の任意の root パスワードに置換します。

```
mysql> SET PASSWORD = PASSWORD('password');
```

```
From now on, start MySQL with mysql -p so it will prompt you for the password.
```

21. リモート ユーザにアクセス権限を付与するには、次の手順を実行します。

    a. mysql プロンプトから次のコマンドを実行します。

```
mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' WITH GRANT OPTION;
mysql> exit
```

    b. MySQL サービスを再起動します。

    c. # service mysqld restart

    d. ファイアウォールで MySQL サーバ ポート（3306）を開いて、リモート クライアントが接続できるようにします。

```
# iptables -I INPUT -p tcp --dport 3306 -j ACCEPT
```

22. /etc/sysconfig/iptables ファイルを編集し、INPUT チェーンの先頭に次の行を追加します。

```
-A INPUT -p tcp --dport 3306 -j ACCEPT
```

23. データベースをセットアップします。次のコマンドで、DBA アクティビティを実行するデータベース上にクラウド ユーザを作成します。

    a. dbpassword に、クラウド ユーザに割り当てるパスワードを指定します。パスワードを指定しないことも選択できます。

    b. deploy-as に、データベースを展開するユーザのユーザ名とパスワードを指定します。次のコマンドでは、ルート ユーザがデータベースを展開し、クラウド ユーザを作成していることが想定されています。

    c. （任意）encryption_type では、ファイルまたは Web を使用して、データベース暗号パスワードを渡すために使用する技術を示します。デフォルト：file。

    d. （任意）management_server_key では、CloudPlatform プロパティ ファイルで機密パラメータを暗号化するために使用するデフォルト キーを置換します。デフォルト：password。これをよりセキュアな値に置き換えることを強く推奨します。

    e. （任意）database_key では、CloudPlatform データベースで機密パラメータを暗号化するために使用するデフォルト キーを置換します。デフォルト：password。これをよりセキュアな値に置き換えることを強く推奨します。

```
# cloud-setup-databases cloud:<dbpassword>@localhost --deploy-as=root:<password>
-e <encryption_type> -m <management_server_key> -k <database_key>
```

24. 管理サーバと同じマシン上で KVM ハイパーバイザを実行している場合は、/etc/sudoers を編集し、次の行を追加します。

```
Defaults:cloud !requiretty
```

25. データベースが設定されたので、管理サーバ用の OS の設定を完了することができます。このコマンドは、iptables、sudoers をセットアップし、管理サーバを起動します。

```
# cloud-setup-management
```

26. システム VM テンプレートを準備します。

    a. セカンダリ ストレージは、CloudPlatform システム VM に使用するテンプレートでシードする必要があります。

    b. 管理サーバ上で、次の cloud-install-sys-tmplt コマンドを 1 つ以上実行して、システム VM テンプレートを取得して圧縮解除します。エンド ユーザがこのゾーンで実行すると予想されるハイパーバイザ タイプごとにコマンドを実行します。

    c. 管理サーバ上の NetApp NFS 共有を /TenantADataSecNFS というマウント ポイント名でマウントします。

    d. データベースをセットアップしたときに CloudPlatform データベース暗号化タイプを「web」に設定した場合、パラメータ -s <management-server-secret-key> を使用する必要があります。このプロセスには、ローカル ファイル システム上に約 5 GB の空き容量が必要で、実行するたびに最大 30 分が必要です。

vSphere の場合：

```
# /usr/share/cloudstack-common/scripts/storage/secondary/cloud-install-sys-tmplt -m
/export/TenantADataSecNFSVol -u
http://download.cloud.com/templates/4.2.1/systemvmtemplate-4.2.1-vh7.ova -h vmware -o
<<var_vm_host_infra_01_ip_mgnt> 10.65.121.70 -r admin -d xxxxxx -F
```

クラウドで Baremetal as a Service を実行するには、BareMetal Agent を準備し、CloudPlatfrom 4.2.1 用に RHEL Linux オペレーティング システム上で PXE を設定します。

（注） このマニュアルでは、CloudPlatfrom 4.2.1 がインストールされている同じシステムを使用しました。

1. RHEL 6.X に root としてログインし、PXE、DHCP、TFTP および NFS パッケージをダウンロードしてインストールします。
2. CloudPlafrom のインストール セクションに示されているように、CloudPlatform-VERSION-N-OSVERSION.tar.gz は、準備している CloudPlatfrom 4.2.1 インストールの一部としてすでにダウンロードされ、untar されています。
3. BareMetal Agent をインストールするには、抽出された CloudPlatfrom 4.2.1 ディレクトリにある install.sh スクリプトを実行します。

```
[root@PXE CloudPlatform-4.2.1.1-rhel6.3]# ./install.sh
Setting up the temporary repository...
Cleaning Yum cache...
Loaded plugins: product-id, refresh-packagekit, security, subscription-manager
Updating certificate-based repositories.
Unable to read consumer identity
Cleaning repos: cloud-temp
0 metadata files removed
Welcome to the CloudPlatform Installer.  What would you like to do?
 NOTE: For installing KVM agent, please setup EPEL<http://fedoraproject.org/wiki/EPEL>
yum repo first;
  For installing CloudPlatform on RHEL6.x, please setup distribution yum repo either
from ISO or from your registeration account.
  3.We detect you already have MySql server installed, you can bypass mysql install
chapter in CloudPlatform installation guide.
        Or you can use E) to remove current mysql then re-run install.sh selecting D)
to reinstall if you think existing MySql server has some trouble.
        For MySql downloaded from community, the script may not be able to detect it.
    A) Install the Agent
    B) Install BareMetal Agent
    S) Install the Usage Monitor
    U) Upgrade the CloudPlatform packages installed on this computer
    R) Stop any running CloudPlatform services and remove the CloudPlatform packages
from this computer
    E) Remove the MySQL server (will not remove the MySQL databases)
    Q) Quit
Type B option to install BareMetal Agent
> B
Installing the BareMetal Agent...
Loaded plugins: product-id, refresh-packagekit, security, subscription-manager
Updating certificate-based repositories.
Unable to read consumer identity
cloud-temp
| 1.3 kB     00:00 ...
cloud-temp/primary
| 2.5 kB     00:00 ...
cloud-temp
7/7
Setting up Install Process
Package cloudstack-baremetal-agent-4.2.1.0-2.el6.x86_64 already installed and latest
version
```

```
Nothing to do
Done
```

e. BareMetal Agent のインストール後に BareMetal セットアップ スクリプトを実行します。TFTP ルート ディレクトリを書き留めてください。

```
[root@PXE CloudPlatform-4.2.1.1-rhel6.4]# cloudstack-setup-baremetal
Checking is root
[ OK ]
Checking tftp-server
[ OK ]
Checking syslinux
[ OK ]
Checking xinetd
[ OK ]
Checking chkconfig
[ OK ]
Checking dhcp
[ OK ]
Executing 'chkconfig --level 345 tftp on'
[ OK ]
Executing 'chkconfig --level 345 xinetd on'
[ OK ]
Executing 'chkconfig --level 345 dhcpd on'
[ OK ]
Executing '/etc/init.d/xinetd restart'
[ OK ]
Detected iptables is running, need to open tftp port 69
Executing 'iptables -I INPUT 1 -p udp --dport 69 -j ACCEPT'
[OK]
Executing '/etc/init.d/iptables save'
[ OK]
Executing 'cp -f /usr/share/syslinux/pxelinux.0 /export'
[ OK ]
Setup BareMetal PXE server successfully
TFTP root directory is: /export
```

f. NFS 設定ファイル /etc/exports を設定します。BareMetal Host が PXE イメージにアクセスするために /export（TFTP ルート）および /var/www/html/RHEL63（http ルート）ディレクトリが NFS でエクスポートされることを確認します。

```
[root@PXE ~]# cat /etc/exports
/export *(rw,async,no_root_squash)
/var/www/html/RHEL63 *(rw,async,no_root_squash)
```

g. NFS サーバ上で NFS が実行されていることを確認します。

```
[root@PXE ~]# vi /export/RHEL63.ks
[root@PXE ~]# rpcinfo -p
   program vers proto   port  service
    100000    4   tcp    111  portmapper
    100024    1   udp    662  status
    100011    1   udp    875  rquotad
    100005    1   udp    892  mountd
    100003    2   tcp   2049  nfs
```

h. RHEL 6.0.3 オペレーティング システム ISO イメージから PXE ファイルの pxelinux.0、pxelinux.cfg および RHEL63.ks（キックスタート イメージ）を共有ディレクトリ /export（TFTP ルート ディレクトリ）にダウンロードします。

```
[root@PXE export]# ll
total 112
drwxr-xr-x.  2 root root  4096 Oct 11 04:52 pxeimages
-rw-r--r--.  1 root root 26828 Oct 22 04:16 pxelinux.0
- drwxr-xr-x.  2 root root  4096 Oct 22 04:55 pxelinux.cfg
-rwxr-xr-x.  1 root root  1478 Oct 22 04:56 RHEL63.ks
```

i. DHCPD サービスが開始され、サーバ上で実行されていることを確認します。DHCPD サービスを実行するために、DHCPD.conf ファイルのサンプルを作成できます。

```
[root@PXE export]# service dhcpd status
dhcpd (pid  7306) is running...
```

ファイルのサンプル

```
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#   see 'man 5 dhcpd.conf'
ignore client-updates;
authoritative;
allow booting;
allow bootp;
subnet 10.65.121.0 netmask 255.255.255.0
{
 option routers          10.65.121.1;
          option subnet-mask      255.255.0.0;
           option broadcast-address 10.65.121.255;
            option time-offset      -18000;
            default-lease-time      21600;
             max-lease-time  43200;
 }
```

j. ISO を共有ディレクトリ /export/RHEL6-3 に抽出することによって、RHEL 6.3 OS イメージをコピーします。

```
[root@PXE RHEL6-3]# ls
EFI                        RELEASE-NOTES-es-ES.html  RELEASE-NOTES-si-LK.html
EULA                       RELEASE-NOTES-fr-FR.html  RELEASE-NOTES-ta-IN.html
GPL                        RELEASE-NOTES-gu-IN.html  RELEASE-NOTES-te-IN.html
HighAvailability           RELEASE-NOTES-hi-IN.html  RELEASE-NOTES-zh-CN.html
images                     RELEASE-NOTES-it-IT.html  RELEASE-NOTES-zh-TW.html
isolinux                   RELEASE-NOTES-ja-JP.html  repodata
LoadBalancer               RELEASE-NOTES-kn-IN.html  ResilientStorage
media.repo                 RELEASE-NOTES-ko-KR.html  RPM-GPG-KEY-redhat-beta
Packages                   RELEASE-NOTES-ml-IN.html  RPM-GPG-KEY-redhat-release
README                     RELEASE-NOTES-mr-IN.html  ScalableFileSystem
RELEASE-NOTES-as-IN.html   RELEASE-NOTES-or-IN.html  Server
RELEASE-NOTES-bn-IN.html   RELEASE-NOTES-pa-IN.html  TRANS.TBL
RELEASE-NOTES-de-DE.html   RELEASE-NOTES-pt-BR.html
RELEASE-NOTES-en-US.html   RELEASE-NOTES-ru-RU.html
```

k. CloudPlatfrom Agent が RHEL 6.3 キックスタート、カーネルおよび initrd ファイルにアクセスして PXE ブートを実行できるようにするために、http と tftp サーバを開始および設定します。

```
[root@PXE RHEL63]# service httpd start
Starting httpd:
[root@PXE export]# service xinetd status
xinetd (pid  3748) is running...
```

4. BareMetal Host PXE をサポートするための、RHEL 6.3 キックスタート イメージ、initrd.img および vmlinuz カーネル ファイルへのリンクが作成されている /var/www/html/RHEL63 の下にソフトリンクのパスを作成します。

```
[root@PXE RHEL63]#ln -s /export/RHEL6-3/images/pxeboot/initrd.img initrd.img
[root@PXE RHEL63]#ln -s /export/RHEL63.ks RHEL63.ks
[root@PXE RHEL63]#ln -s /export/RHEL63.ks RHEL6-3/images/pxebooy/vmlinuz vmlinuz
[root@PXE RHEL63]# ll
total 1780
lrwxrwxrwx. 1 root root      41 Oct 21 05:45 initrd.img ->
/export/RHEL6-3/images/pxeboot/initrd.img
lrwxrwxrwx. 1 root root      17 Oct 21 07:11 RHEL63.ks -> /export/RHEL63.ks
lrwxrwxrwx. 1 root root      38 Oct 17 02:52 vmlinuz ->
/export/RHEL6-3/images/pxeboot/vmlinuz
```

l. RHEL 6.3 キックスタート イメージ ファイルの NGS インストール メディア オプションを、NFS IP アドレスおよび RHEL 6.3 OS イメージを使用して設定します。

（注） このマニュアルでは、PXE ブートにアクセスするために **Eth2 (20.1.1.5) VLAN 20** PXE ネットワークを作成し、RHEL 6.3 オペレーティング システム インストール ファイル、キックスタート、initrd およびカーネル ファイルを格納する NFS エクスポート パス **/export** を使用しています。

RHEL キックスタート イメージ ファイルのサンプル

```
[root@PXE export]# cat RHEL63.ks
#platform=x86, AMD64, or Intel EM64T
#version=DEVEL
# Firewall configuration
firewall --disabled
# Install OS instead of upgrade
install
# Use NFS installation media
nfs --server=20.1.1.5 --dir=/export/RHEL6-3
# Root password
rootpw --iscrypted $1$rWDxD1lu$iQJek3Co0ivKUEhl68CmA/
# System authorization information
auth  --useshadow  --passalgo=nbv12345
# Use graphical install
graphical
# Run the Setup Agent on first boot
firstboot --enable
# System keyboard
keyboard us
# System language
lang en_US
# Driver Disk
#driverdisk
--source=nfs:20.1.1.50:/var/www/html/RHEL63/dd-fnic-rhel6.3-1.6.0.5.iso
#driverdisk
--source=nfs:192.85.0.2:/home/Delmar-MR1-Driver/RHEL6.3/enic-2.1.1.41-rhel6u3-dd.i
so
# SELinux configuration
selinux --disabled
# Installation logging level
logging --level=info
# Reboot after installation
#reboot
# System timezone
timezone  Asia/Kolkata
# Network information
network  --bootproto=dhcp --device=eth0 --onboot=yes --activate
#network  --bootproto=dhcp --device=eth2 --onboot=yes --activate
# System bootloader configuration
#bootloader --location=mbr
# Clear the Master Boot Record
#zerombr
# Partition clearing information
#clearpart --none
# Disk partitioning information
#part /boot --fstype="ext4" --size=100
#part swap --fstype="swap" --size=2048
#part / --fstype="ext4" --grow --size=1
%packages
@base
@network-file-system-client
@network-tools
```

```
@server-platform
%end
install
#xconfig --defaultdesktop=GNOME --depth=8 --resolution=800x600
```

CloudPlatfrom の高度な設計

Citrix クラウド設計は、次のタスクに分割されています。

1. ゾーンの作成
2. ネットワークの定義
3. Pod の追加
4. クラスタの追加
5. ホストの追加
6. ストレージの定義

ゾーンの作成

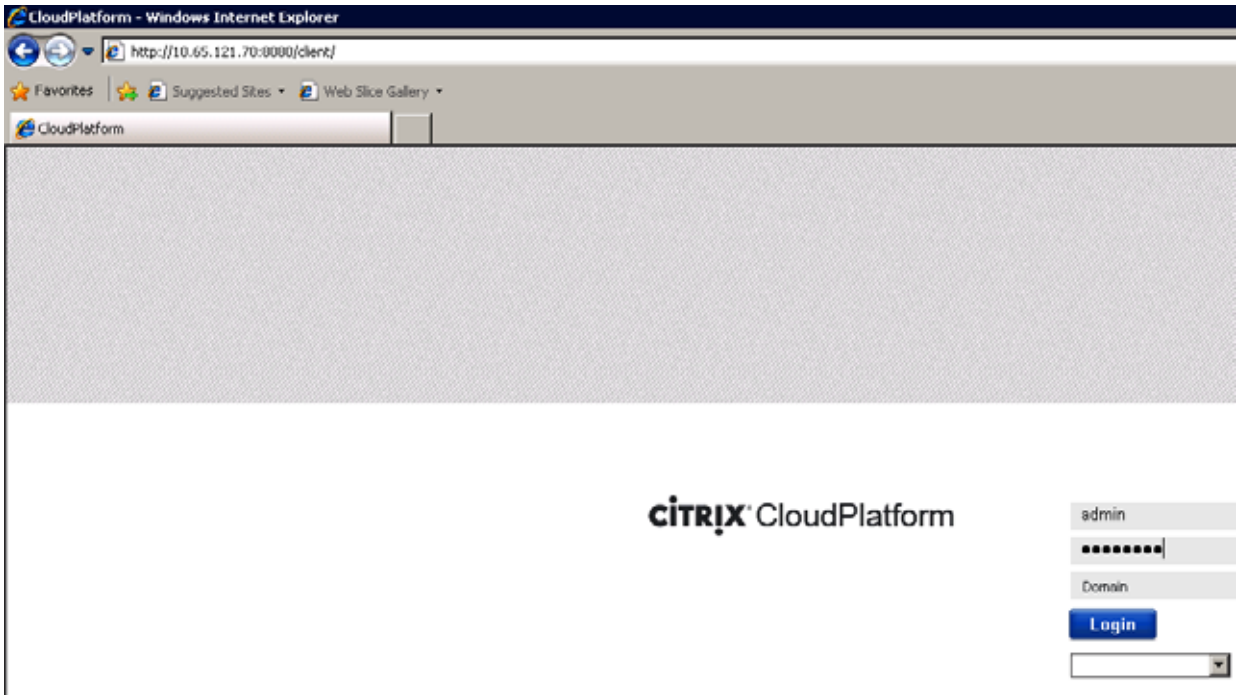
ゾーンは、CloudPlatform 導入における最大の組織単位です。ゾーンは通常単一のデータセンターに対応しますが、データセンター内に複数のゾーンを持つことが許容されます。クラウドのコンピューティング、ネットワークおよびストレージ インフラストラクチャをゾーンに編成する利点は、物理的な分離および冗長性を実現できることです。

真のマルチ テナント クラウド サービスを提供するために、CPU、メモリ、ネットワークおよびストレージなどの仮想マシン リソースをホストする テナント クラウド インフラストラクチャのコンピューティング、ストレージおよびネットワークを、ゾーン、Pod、クラスタおよびホストを作成することによって、隔離された異なる論理的パーティションに細かくグループ分けすることができます。

クラウド サービスをホストするために Citrix CloudPlatform アプリケーションを使用してゾーンを作成するには、ユーザ資格情報を使用して CloudPlatform にログインし、次の手順を実行します。

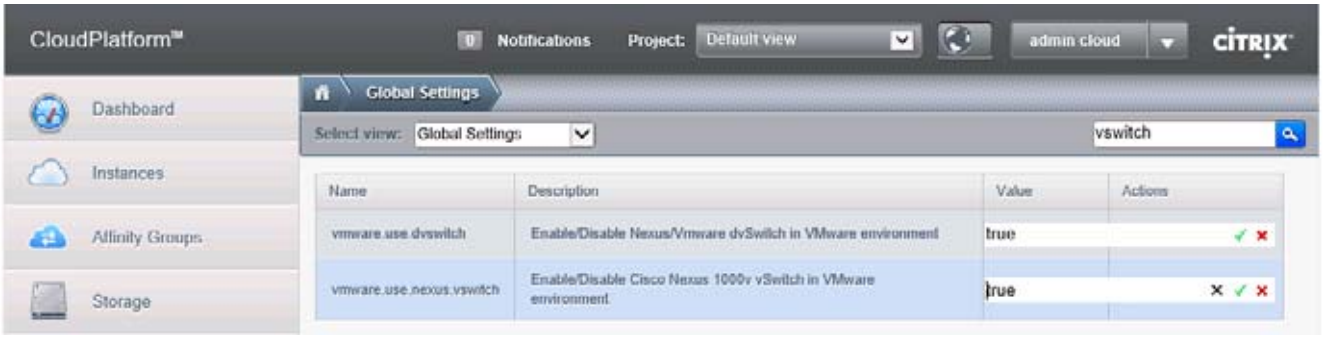
1. Web ブラウザで URL http://10.65.121.70:8080/client/ を指定して、CloudPlatfrom 4.2.1 管理サーバの IP アドレスにアクセスします。
2. ユーザ名 <root>、パスワード <XXXXXX>、およびドメインを入力します。
3. [Login] をクリックします。

図 181　　Citrix CloudPlatform へのログイン



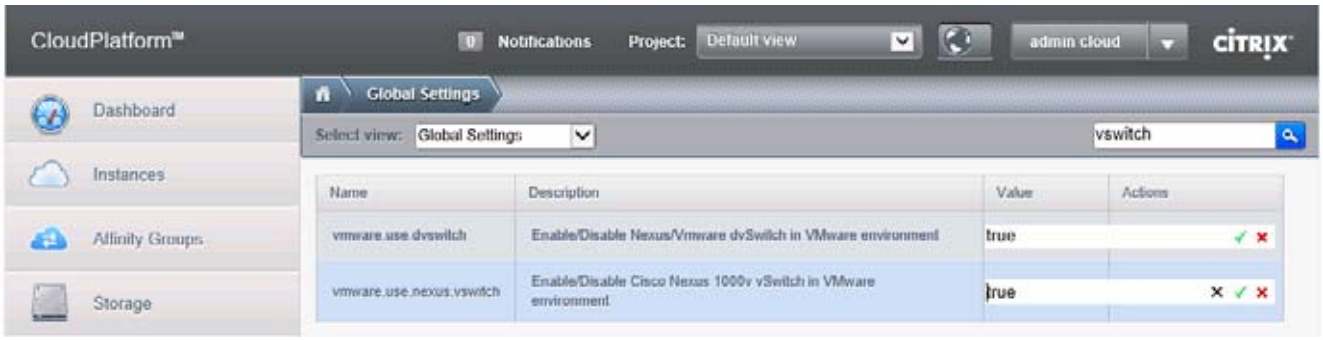
4. [Agree] をクリックして、エンド ユーザ ライセンス契約を確認します。
5. [I have used CloudPlatform before, skip this guide] ボタンをクリックします。
6. 左ペインで、[Infrastructure] をクリックします。これにより、現在設定されていない CloudPlatform 環境が表示されます。

図 182　　インフラストラクチャ ページの表示



7. TenantA 仮想マシン ネットワーク アクセスを処理するには、CloudPlafrom 4.2.1 で vmware use nexus vswitch DVS を有効にします。左ペインで、[Global Settings] をクリックします。[Select View] ボックスに [Global Settings] が選択された右ペインで、[Search] ボックスに vSwitch と入力します。
8. Enter を押します。
9. [VMWare.use.dvswitch] で [Value] を [True] に変更します。
10. [VMWare.use.nexus.vswitch] で [Value] を [True] に変更します。
11. Enter を押します。

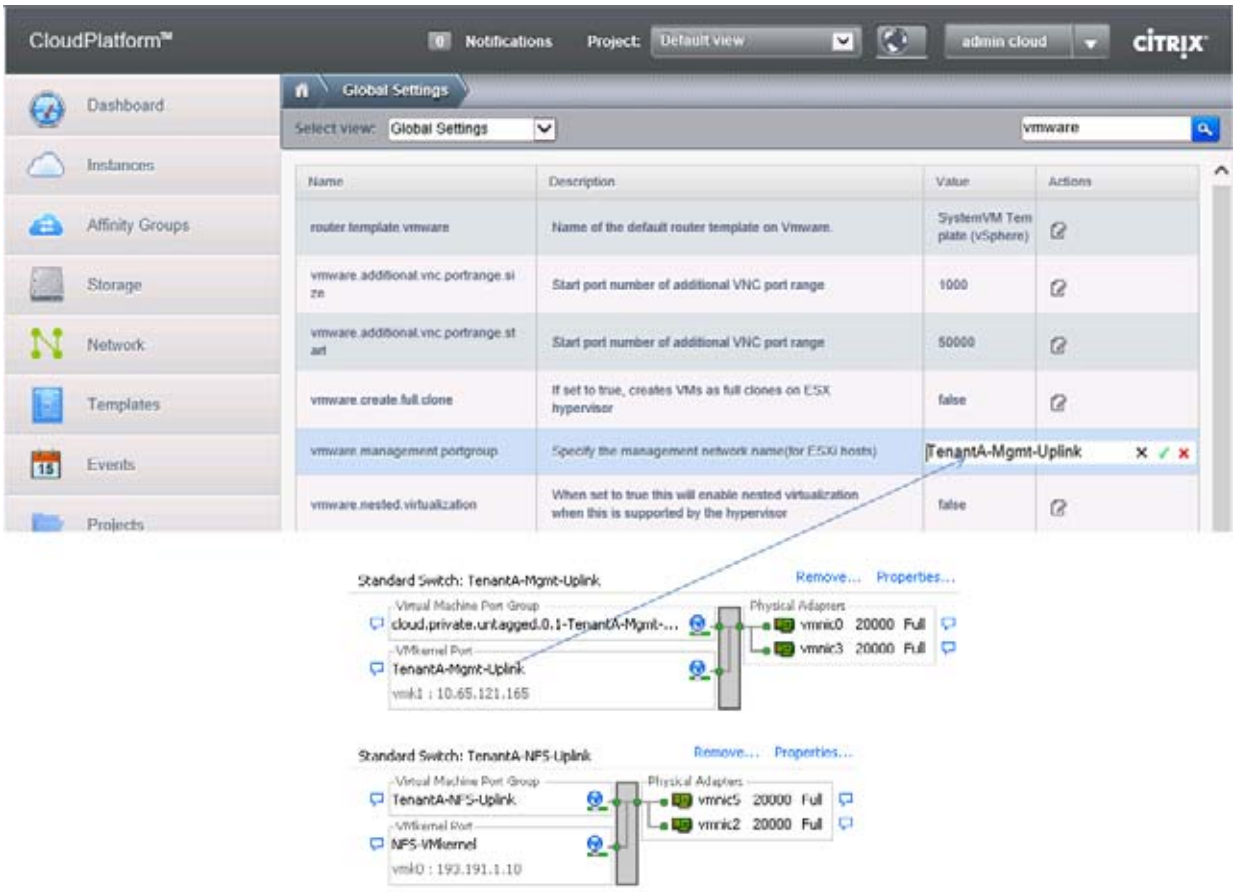
図 183　[Global Setting] で [Value] を [True] に変更します。



12. 検索ボックスに vmware と入力します。
13. Enter を押します。
14. [vmware.managment.portgroup] で [Value] を [TenantA-Mgmt-Uplink] に変更します。
15. Enter を押します。
16. 10.65.121.70 に対して SSH を実行して、CONSOLE で cloudstack 管理サービスを再起動します。

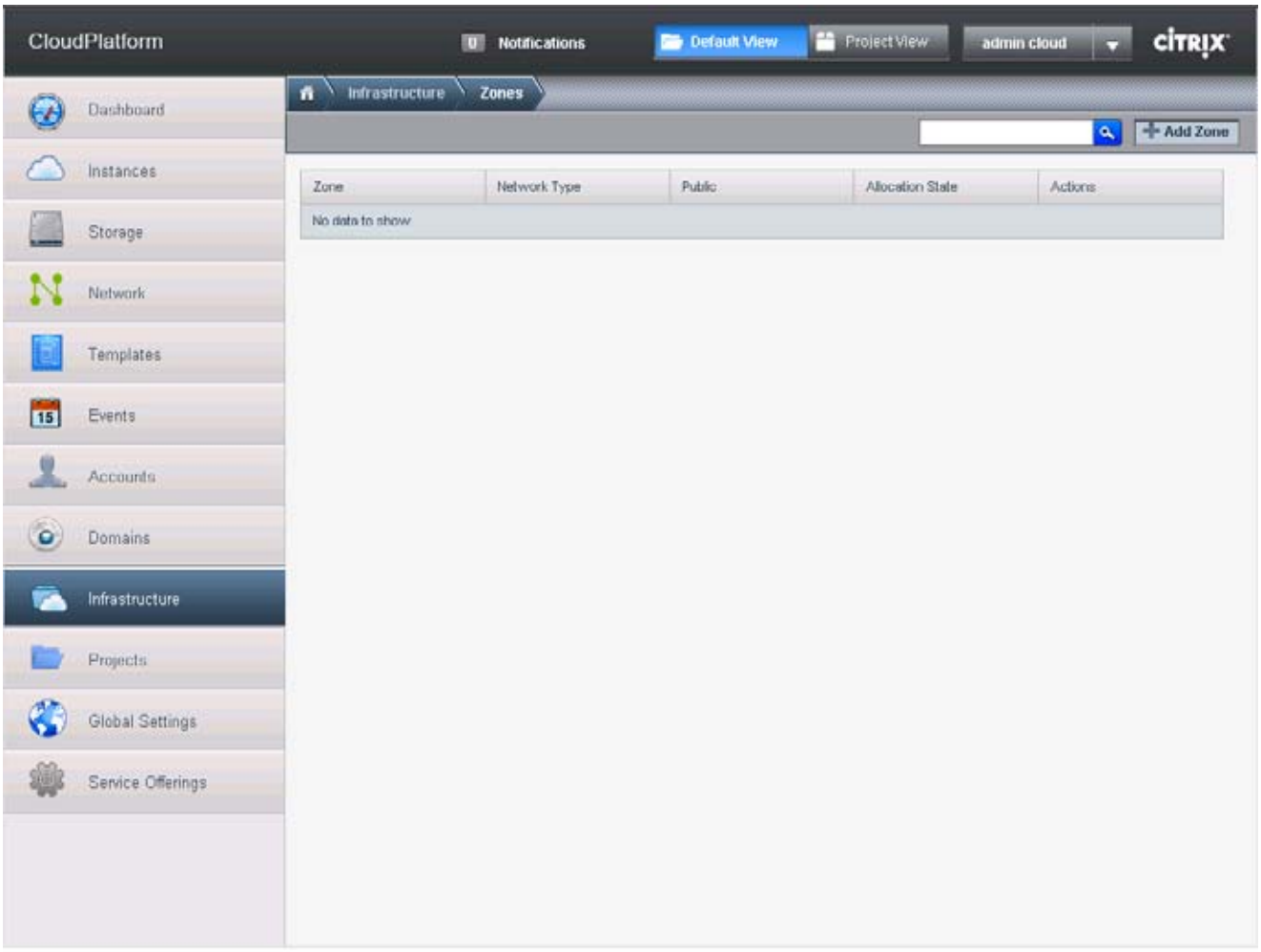
```
[root@cloudstack CloudPlatform-UCS-for-cisco-4.2.1.1-5-rhel6.3]# service
cloudstack-management status
Stopping cloudstack-management:                [  OK  ]
Starting cloudstack-management:                  [  OK  ]
```

図 184　[Global Setting] で [Value] を [TenantA-Mgmt-Uplink] に変更します。



17. ユーザ名およびパスワードを入力して、CloudPlatfrom 4.2.1 管理サーバにログインします。
18. 左ペインで [Infrastructure] をクリックし、右ペインの [Zones] タイルの下で**すべてを表示**します。
19. マルチテナントを提供するためにテナントのゾーンを作成するには、右ペインの右上隅にある [+ Add Zone] をクリックします。

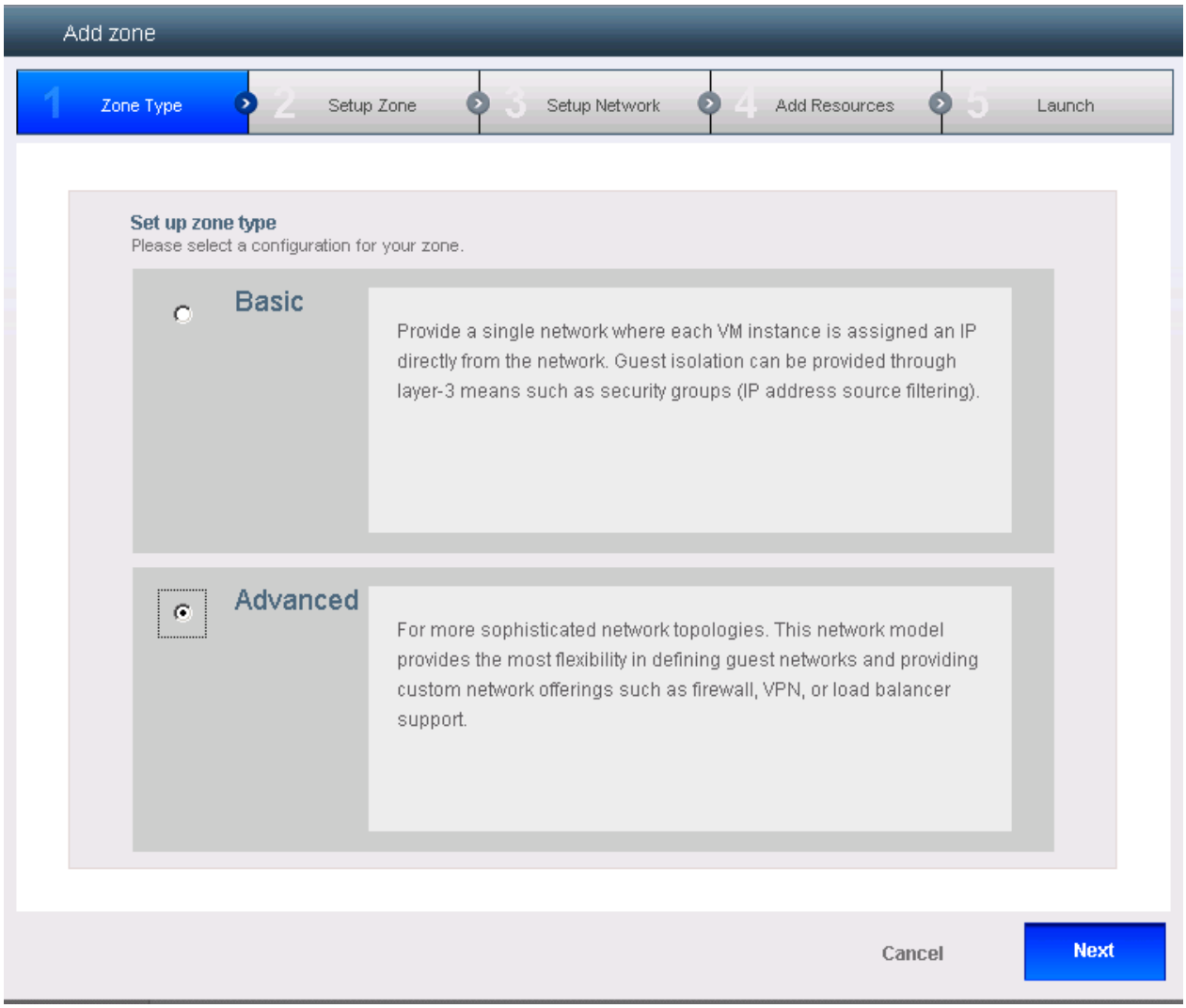
図 185　　インフラストラクチャにおけるすべてのゾーンの表示



20. [Advanced zone type] オプション ボタンをクリックします。

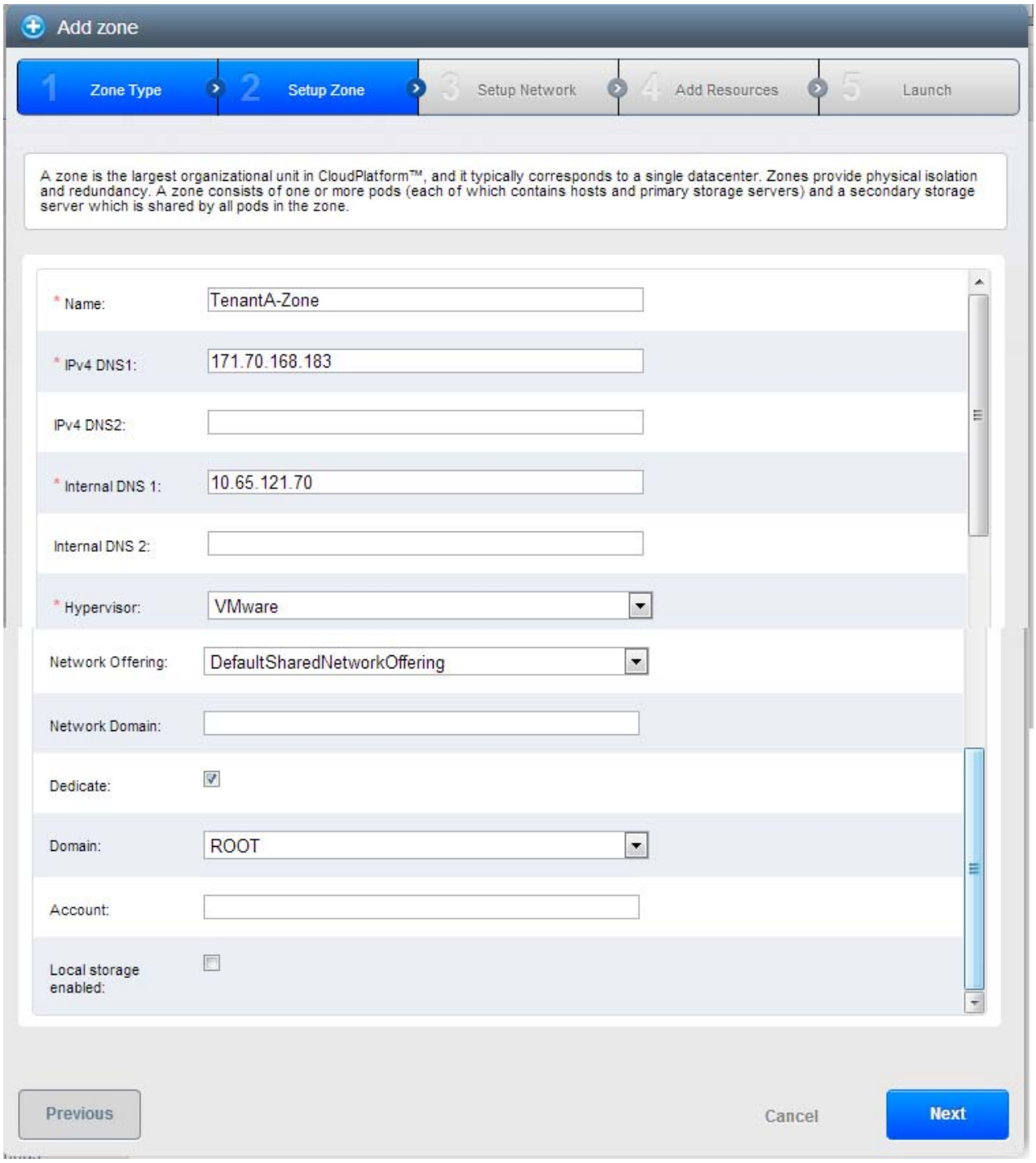
21. [Next] をクリックします。

図 186　　ゾーンの設定の定義



22. [Name] フィールドに TenantA-Zone と入力します。
23. パブリック インターネットにアクセスするために、[DNS1] フィールドに 171.70.168.183 と入力します。
24. [Internal DNS 1] フィールドに CloudPlatfrom 管理サーバ上で実行している 10.65.121.70 を入力します。
25. [Hypervisor] で、リスト ボックスから [VMware] を選択します。
26. [guest CIDR] フィールドに 10.1.1.0/24 を入力します。これは、CloudPlatfrom 4.2.1 のルータ システム VM で実行している DHCP サーバによって、Pod 内部の仮想マシン通信に割り当てられます。
27. [Public] チェックボックスをオフにします。
28. [Local Storage Enabled] チェックボックスをオフにします。
29. [Next] をクリックします。

図 187　　ゾーン属性の定義



ネットワークの定義

ゾーン定義後の次のステップは、クラウド ネットワークを設計し、定義することです。ネットワークの定義には、ベーシックとアドバンスドという 2 つのタイプがあります。ベーシック ネットワーキングでは 1 つのゾーンに物理ネットワークが 1 つだけ存在できますが、アドバンスド ネットワークでは 1 つのゾーンに複数の物理ネットワークが存在できます。各物理ネットワークは 1 つ以上のトラフィック タイプを伝送でき、CloudPlatform では各ネットワークによって伝送するネットワーク トラフィックのタイプを定義できます。このソリューション設計では、アドバンスド ネットワーキングを実装します。

3 つのタイプのトラフィックが定義されており、それぞれは仮想スイッチおよび対応するイーサネットと、ESXi ホストで定義されたポート グループ名を使用して伝送されます。

- 管理トラフィック

  管理トラフィックは、内部リソースが互いに通信するときに CloudPlatform 内で生成されます。これには、ホスト、システム VM（CloudPlatform がクラウドでさまざまなタスクを実行するために使用する VM）、および、CloudPlatform 管理サーバと直接通信するその他のコンポーネント間の通信が含まれます。

  管理トラフィックにアクセスするために、個別の ESX 仮想スイッチ <<TenantA-Mgmt-Uplink>> および VMKernel ポート グループ <<TenantA-Mgmt-Uplink>> が、適切なネットワーク アクセスを持つ対応するネットワーク アダプタによって作成され、vCenter ホストによって管理されている ESXi 5.1 ホスト上で QoS 定義が作成されます。

- ゲスト プライベート トラフィック

  ゲスト プライベート トラフィックは、VM を実行しているエンド ユーザによって使用および生成されます。ゲスト ネットワークは、VM がネットワーク経由で互いに通信するときに発生します。ゲスト パブリック トラフィックは、クラウド内の VM がインターネットにアクセスするときに生成されます。このために、パブリックにアクセス可能な IP を割り当てる必要があります。エンド ユーザは、CloudPlatform UI を使用して IP を取得して、ゲスト ネットワークとパブリック ネットワーク間で NAT を実装することができます。

  ゲストのパブリックとプライベート トラフィックにアクセスするために、Cisco Nexus 1000V DVS スイッチ <<VSM-TenantA>> および VMKernel ポート グループ <<TenantA-guest-Uplink>> が、適切なネットワーク アクセスおよび QoS 定義を持つ対応するネットワーク アダプタによって作成されます。

- ストレージ トラフィック

  ストレージ トラフィックは、セカンダリ ストレージ VM とセカンダリ ストレージ サーバ間で送信される VM テンプレートおよびスナップショットに使用されます。CloudPlatform は、ストレージ ネットワーク トラフィックに対してストレージ NIC という名前の個別のネットワーク インターフェイス コントローラ（NIC）を使用します。常に広帯域幅ネットワークで動作するストレージ NIC を使用すると、テンプレートとスナップショットをすばやくコピーすることができます。

  ストレージ NFS トラフィックにアクセスするために、個別の ESX 仮想スイッチ <<TenantA-NFS-Uplink>> および VMKernel ポート グループ <<TenantA-NFS-Uplink>> が、適切なネットワーク アクセスおよび QoS 定義を持つ対応するネットワーク アダプタによって作成されます。

表 34　　ネットワーク タイプと情報

ネットワーク タイプ	ESX vSwitch / Cisco Nexus 1000V DVS	タグ
管理	TenantA-Mgmt-Uplink	TenantA-Mgmt-Uplink

表 34　　ネットワーク タイプと情報

ゲスト	TenantA-guest-Uplink	TenantA-guest-Uplink
セカンダリ ストレージ	TenantA-NFS-Uplink	TenantA-NFS-Uplink

クラウド サービスをホストするために TenantA マルチテナントに専用の Citrix CloudPlatform アプリケーションを使用して、ゾーンのアドバンスド ネットワークを設定するには、次の手順を実行します。

1. ゲストのパブリックとプライベート トラフィック タイプ アイコンを [Physical Network 2] にドラッグします。

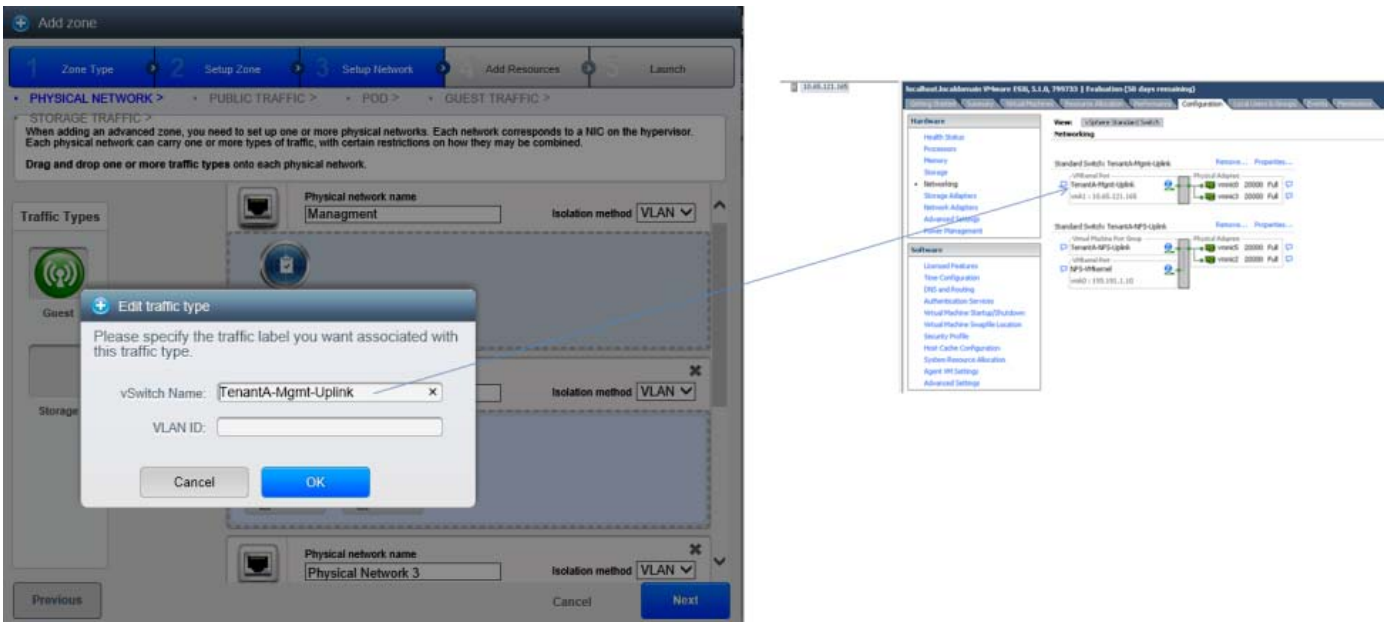
図 188　　ゾーンのアドバンスド ネットワーキング設定の定義

2. ストレージ トラフィック タイプ アイコンを [Physical Network 3] にドラッグします。

図 189　　物理ネットワークへのトラフィック タイプの追加

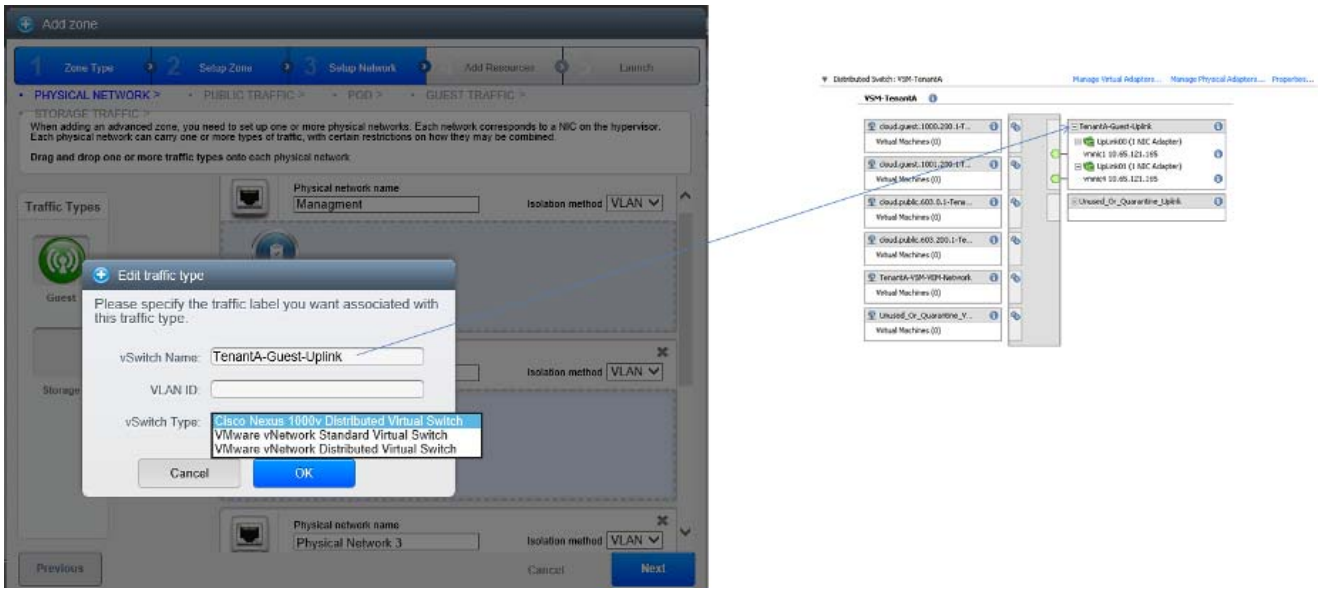
3. 物理ネットワーク Network 1 の名前を <Management> に変更します。
4. [Edit] をクリックし、CloudPlatfrom トラフィック ラベル フィールドに <TenantA-Mgmt-Uplink> と入力します。VLAN ID では、タグなし VLAN の場合は空白のままにします。
5. [Isolation method] リスト ボックスで [VLAN] を選択します。
6. [OK] をクリックします。

図 190　　管理ネットワークでのトラフィック タイプのラベル付け



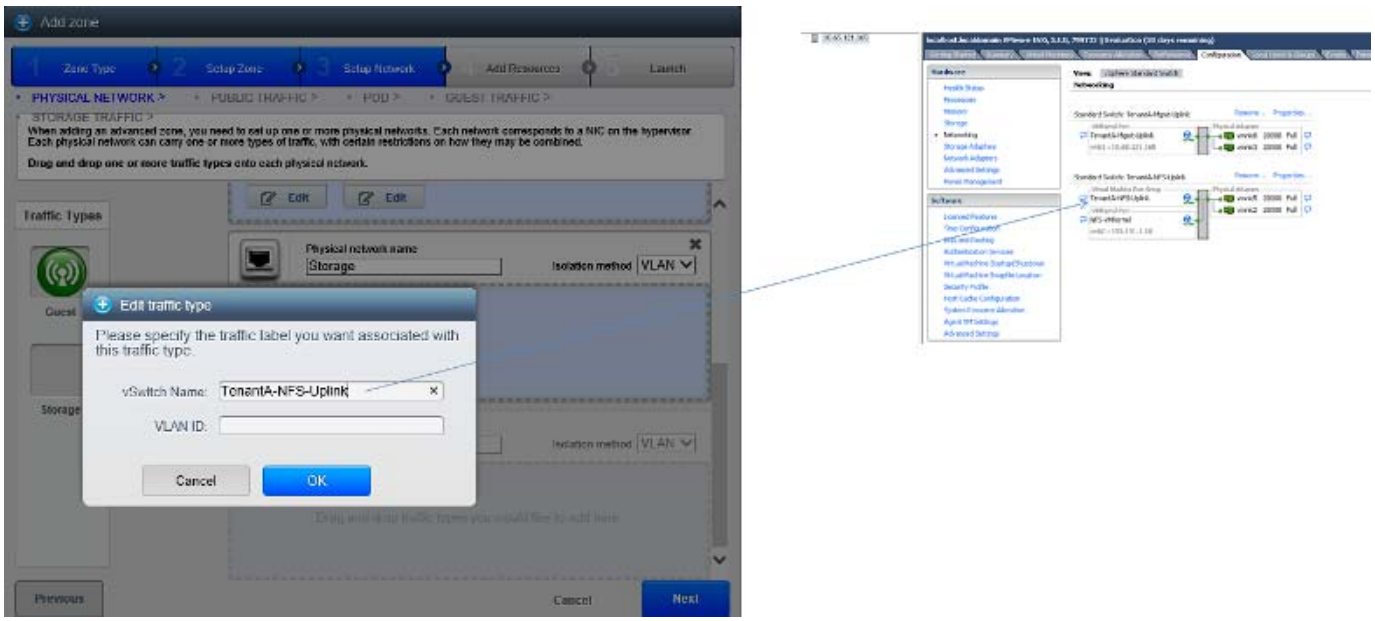
7. 物理ネットワーク Network 2 の名前を <guest> に変更します。
8. [Public Edit] をクリックし、CloudPlatfrom トラフィック ラベル フィールドに <TenantA-guest-Uplink> と入力します。VLAN ID では、タグなし VLAN の場合は空白のままにします。
9. [Private Edit] をクリックし、CloudPlatfrom トラフィック ラベル フィールドに <TenantA-guest-Uplink> と入力します。VLAN ID では、タグなし VLAN の場合は空白のままにします。
10. [Isolation method] リスト ボックスで [VLAN] を選択します。
11. [OK] をクリックします。

図 191　ゲスト ネットワークのトラフィック タイプのラベル付け



12. 物理ネットワーク Network 3 の名前を <Storage> に変更します。
13. [Public Edit] をクリックし、CloudPlatfrom トラフィック ラベル フィールドに <TenantA-NFS-Uplink> と入力します。VLAN ID では、タグなし VLAN の場合は空白のままにします。
14. [Isolation method] リスト ボックスで [VLAN] を選択します。
15. [OK] をクリックします。

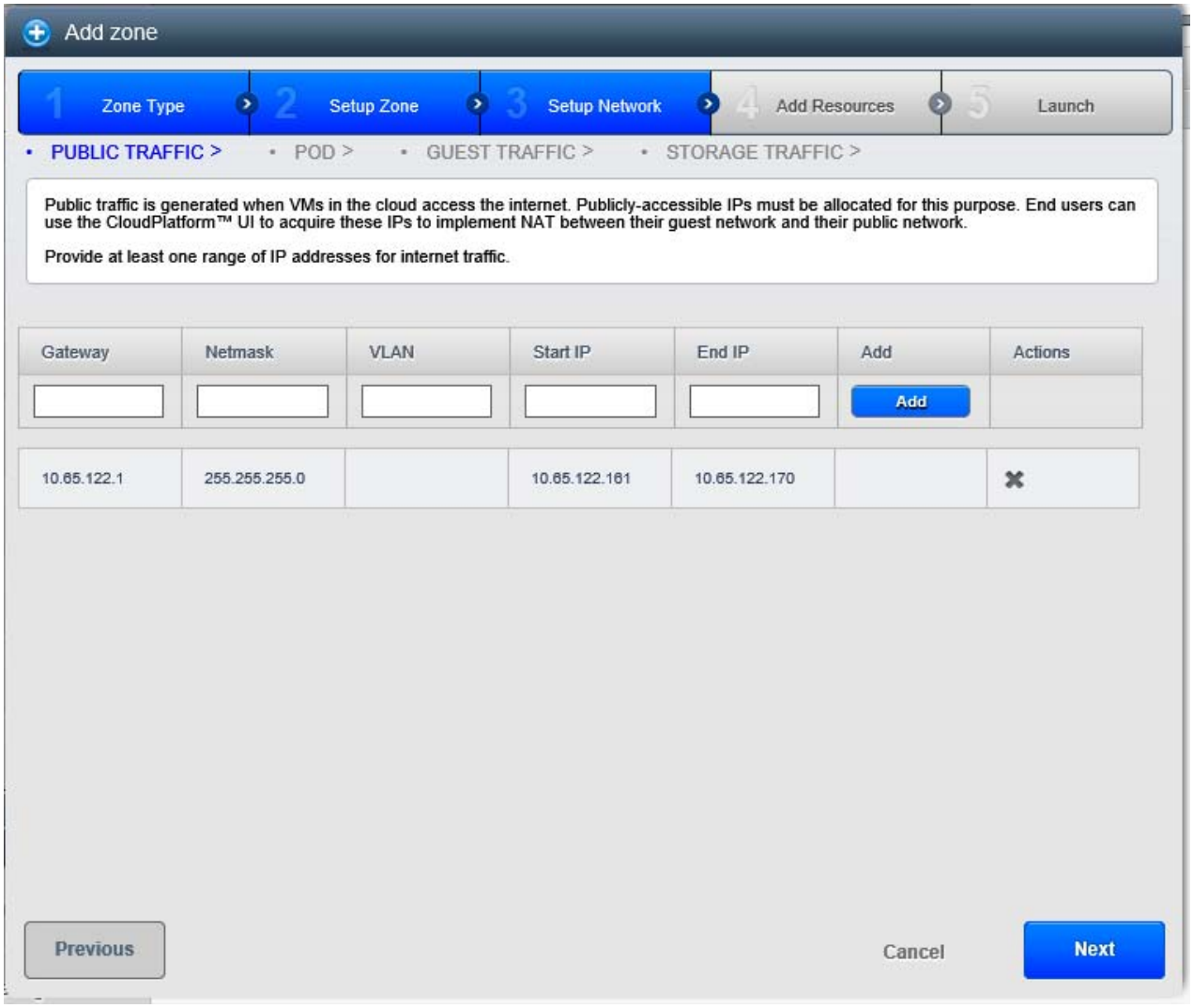
図 192　ストレージのトラフィック タイプのラベル付け



16. [VM Public TRAFFIC] で、次の IP ネットワークの詳細を入力します。
17. [Gateway] フィールドに 10.65.122.1 と入力します。

18. [Network] フィールドに 255.255.255.0 と入力します。
19. [VLAN] は空白のままにします（UCS タグ VLAN 603）。
20. [Start IP] に 10.65.122.161 と入力します。
21. [End IP] に 10.65.122.170 と入力します。
22. [ADD] ボタンをクリックします。
23. [Next] をクリックします。

図 193　　VM パブリック トラフィック ネットワークの詳細の定義



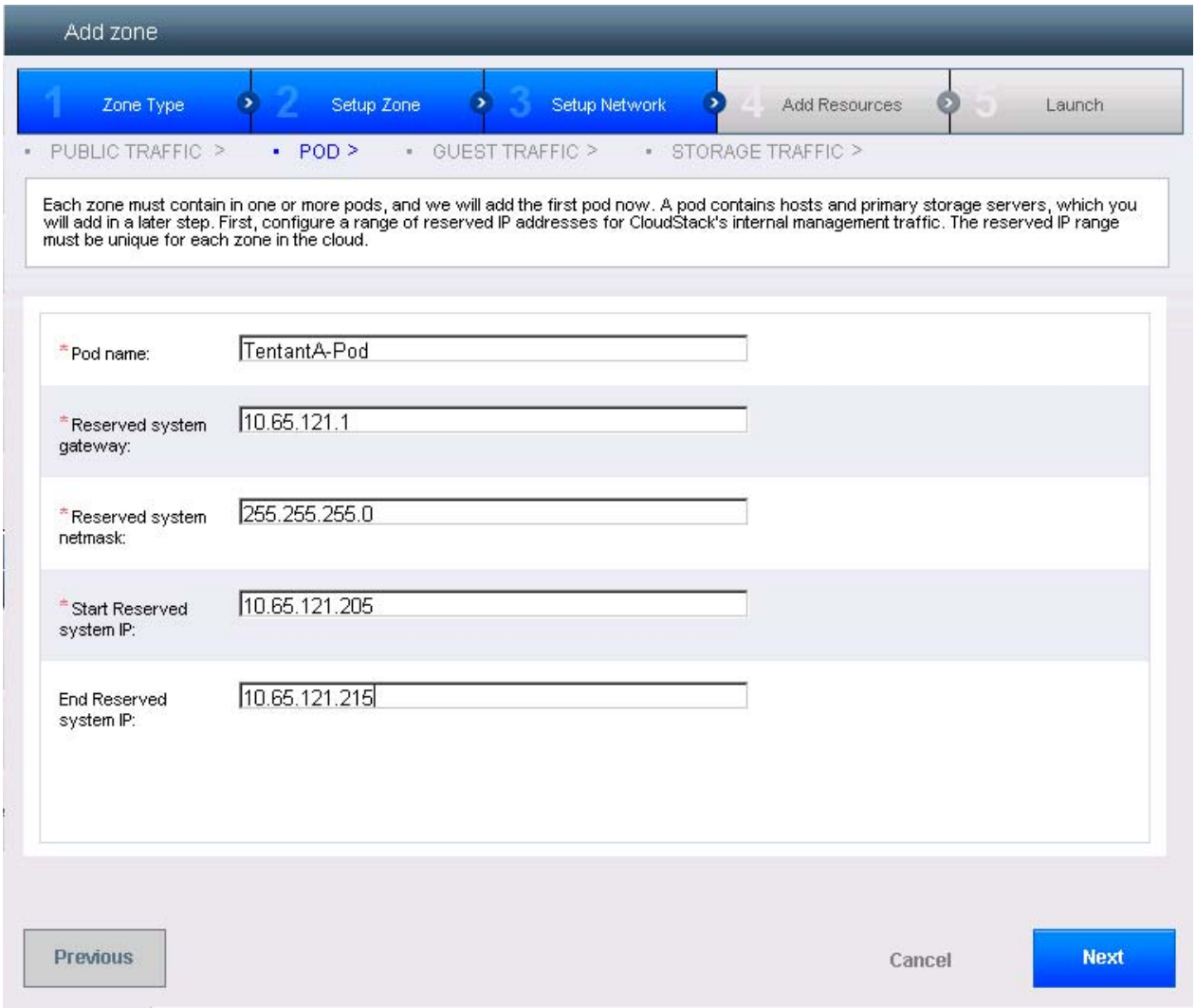
Pod の追加

Pod は、CloudPlatform 導入における 2 番目に大きな組織単位です。Pod はゾーン内に含まれています。各ゾーンは 1 つ以上の Pod を含むことができます。Pod は、ホストの 1 つ以上のクラスタおよび 1 つ以上のプライマリ ストレージ サーバから構成されます。

クラウド サービスをホストするために TenantA マルチテナントに専用の Citrix CloudPlatform アプリケーションを使用して、ゾーンのアドバンスド ネットワーク設定に Pod ネットワークを追加するには、次の手順を実行します。

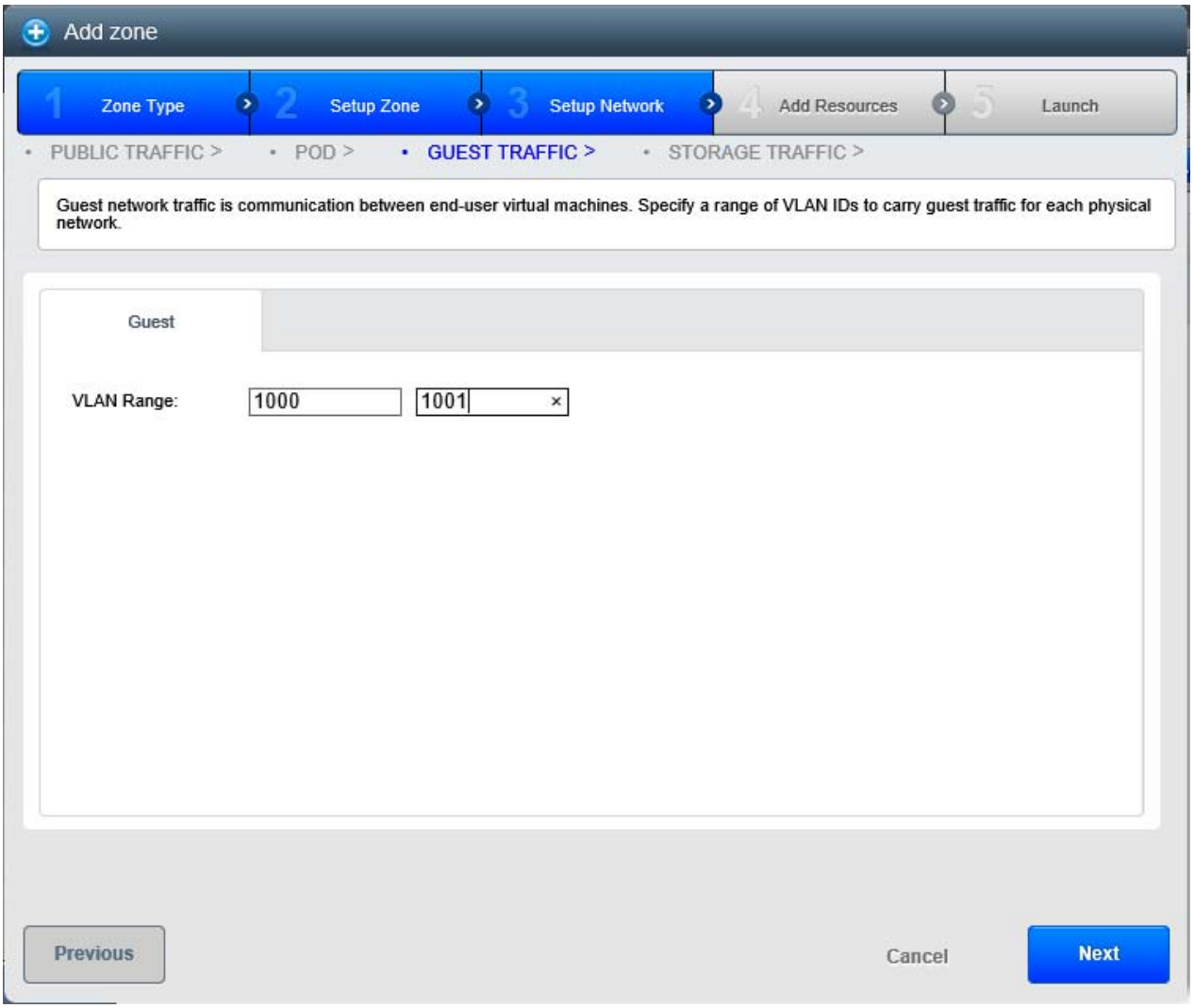
1. [Pod Name] フィールドに TenantA-Pod と入力します。
2. [Reserved System Gateway] フィールドに <Pod_VLAN_603_Gateway>10.65.121.1 と入力します。
3. [Reserved System netmask] フィールドに 255.255.255.0 と入力します。
4. [Start Reserved system IP] フィールドに 10.65.121.205 と入力します。
5. [End Reserved system IP] フィールドに 10.65.121.215 と入力します。
6. [Next] をクリックします。

図 194　　ゾーンへの Pod の追加



7. [Guest] の [VLAN Range] フィールドに 1000 ～ 1001 と入力します。
8. [Next] をクリックします。

図 195　　ゲストの VLAN 範囲の設定

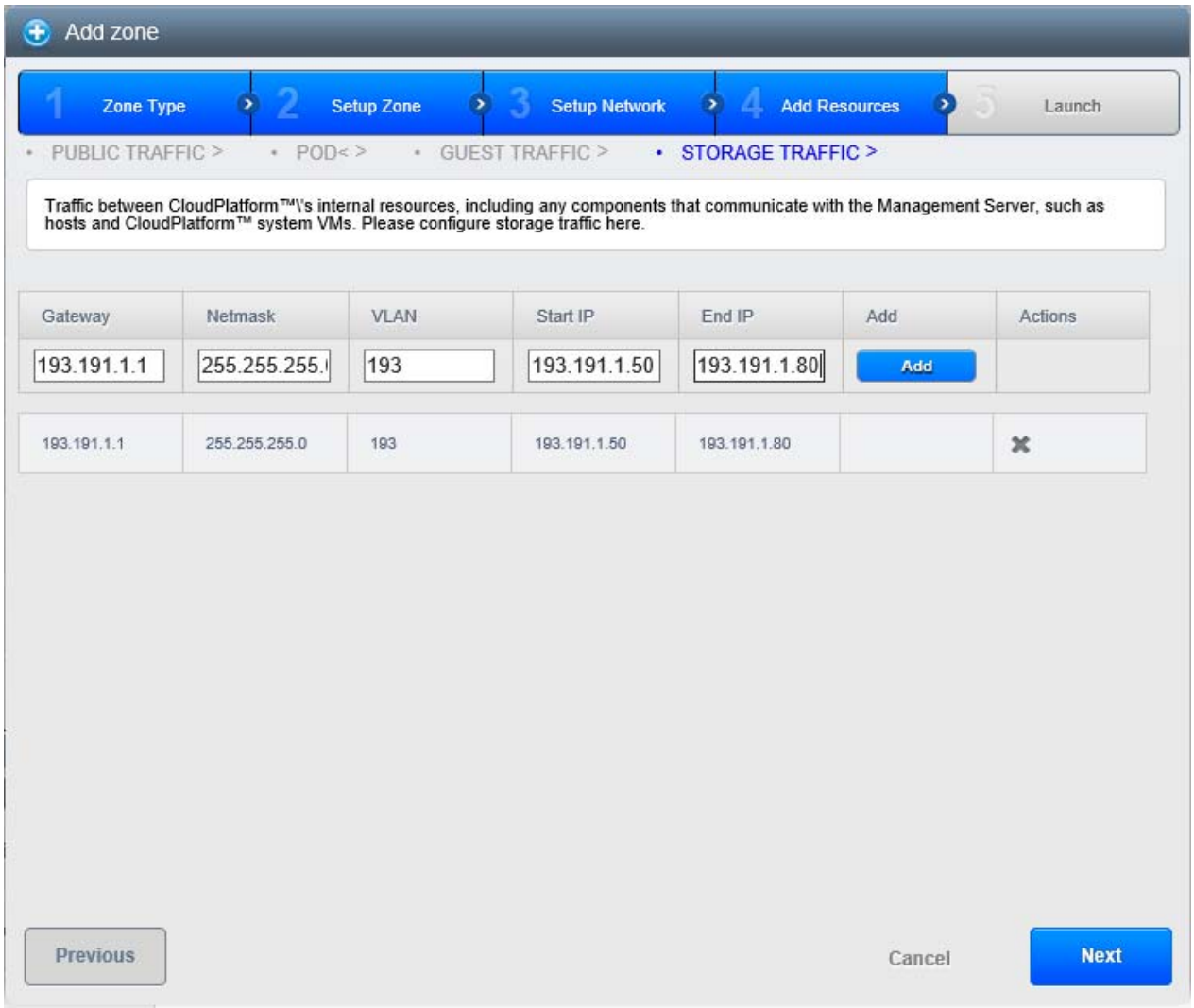


ストレージ トラフィックの追加

クラウド サービスをホストするために TenantA マルチテナントに専用の Citrix CloudPlatform アプリケーションを使用して、ゾーンのアドバンスド ネットワーク設定にストレージ ネットワークを追加するには、次の手順を実行します。

1. [Gateway] フィールドに <Storage_NFS_VLAN_Gateway>193.191.1.1 と入力します。
2. [Netmask] フィールドに 255.255.255.0 と入力します。
3. [VLAN] フィールドに 193 と入力します。
4. [Start IP] フィールドに 193.191.1.50 と入力します。
5. [End IP] フィールドに 193.191.1.80 と入力します。
6. [Add] をクリックします。
7. [Next] をクリックします。

図 196　　ストレージ トラフィック設定の定義



クラスタの追加

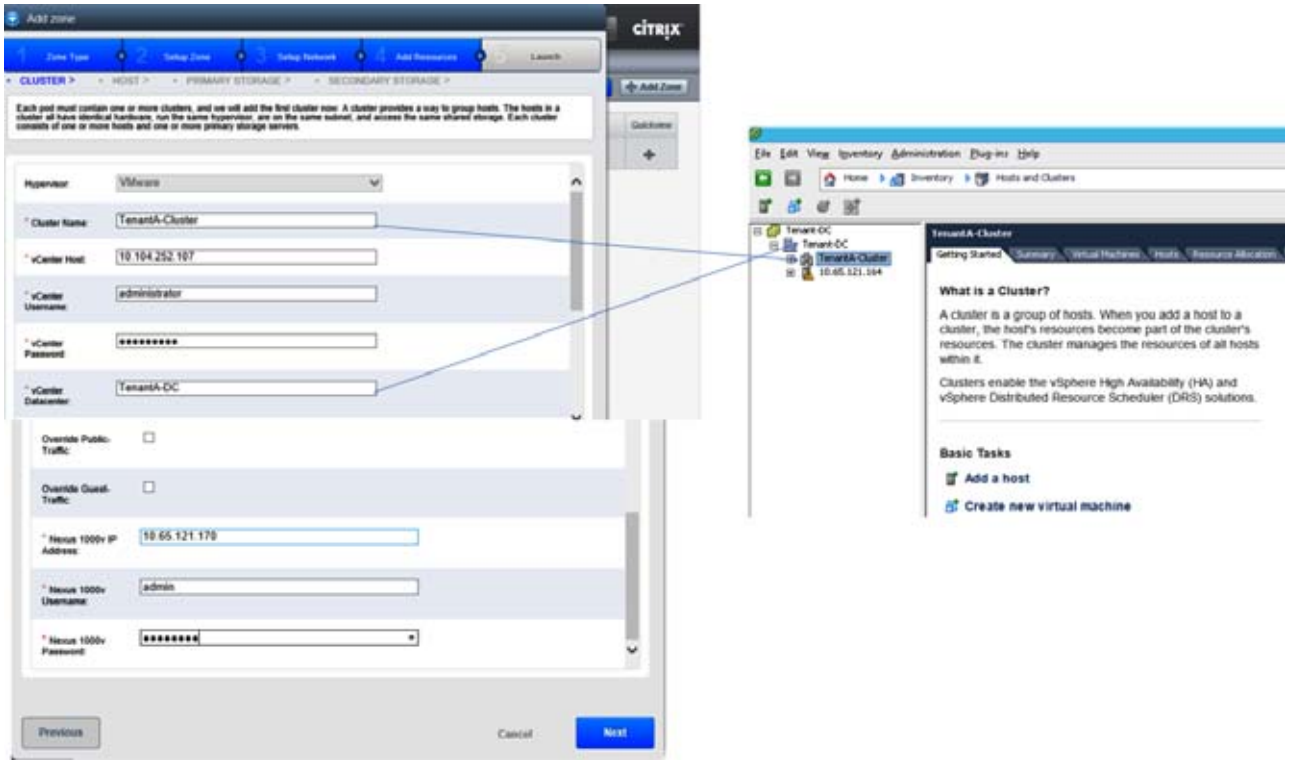
クラスタはホストをグループ化する方法を提供します。具体的にここでは、vCenter で事前に設定された一連の VMware クラスタを含むクラスタを使用します。定義によると、クラスタのすべてのホスト部分は同じハードウェアを持ち、同じハイパーバイザを実行し、同じサブネット上に存在し、同じ共有プライマリ ストレージにアクセスする必要があります。仮想マシン（VM）のインスタンスは、ユーザへのサービスを中断することなく、1 つのホストから別のホストにライブマイグレーションすることができます。

クラスタは、CloudPlatform 導入における 3 番目に大きな組織単位です。クラスタは Pod 内に含まれ、Pod はゾーン内に含まれています。クラスタのサイズは基盤となるハイパーバイザによって制限されていますが、ほとんどの場合 CloudPlatform ではより小さいサイズを推奨します。クラスタは、1 つ以上のホストおよび 1 つ以上のプライマリ ストレージ サーバから構成されます。

Citrix CloudPlatform を使用して、ゾーンに TenantA のクラスタを追加するには、次の手順を実行します。

1. [Cluster Name] フィールドに <TenantA-Cluster> と入力します。
2. [vCenter Host] に <vCenter_IP_Address>10.104.252.107 と入力します。
3. [vCenter Username] に <administrator> と入力します。
4. [vCenter Password] に <xxxxx> と入力します。
5. [vCenter Datacenter Name] に <Tenant-DC> と入力します。vCenter データセンター名が命名規則に従っていることを確認します。
6. [Override Public] および [Guest Traffic] チェックボックスをオフにします。
7. [Nexus 1000V IP Address] に <VSM_IP_Address>10.65.121.170 と入力します。
8. [Nexus 1000V Username] に <admin> と入力します。
9. [Nexus 1000V Password] に <xxxx> と入力します。
10. [Next] をクリックします。

図 197　　ゾーンへのクラスタの追加



ホストの追加

ホストは、ゲスト仮想マシンを実行するコンピューティング リソースを提供します。各ホストにはハイパーバイザ ソフトウェアがインストールされ、ゲスト VM を管理します。ここでのホストは ESXi サーバです。ホストは、CloudPlatform 導入における最小の組織単位です。ホストはクラスタ内に含まれ、クラスタは Pod 内に含まれ、Pod はゾーン内に含まれています。

最初のゾーン作成中に、CloudPlatfrom は VMware vCenter と自動的に同期して、vCenter クラスタの一部であるホストを自動的に追加します。

後にゾーン内のホストを追加または変更するために、CloudPlatfrom では、「クラウド インフラストラクチャ設計」の項で説明されているようにホストを手動で追加および削除することができます。

ストレージの定義

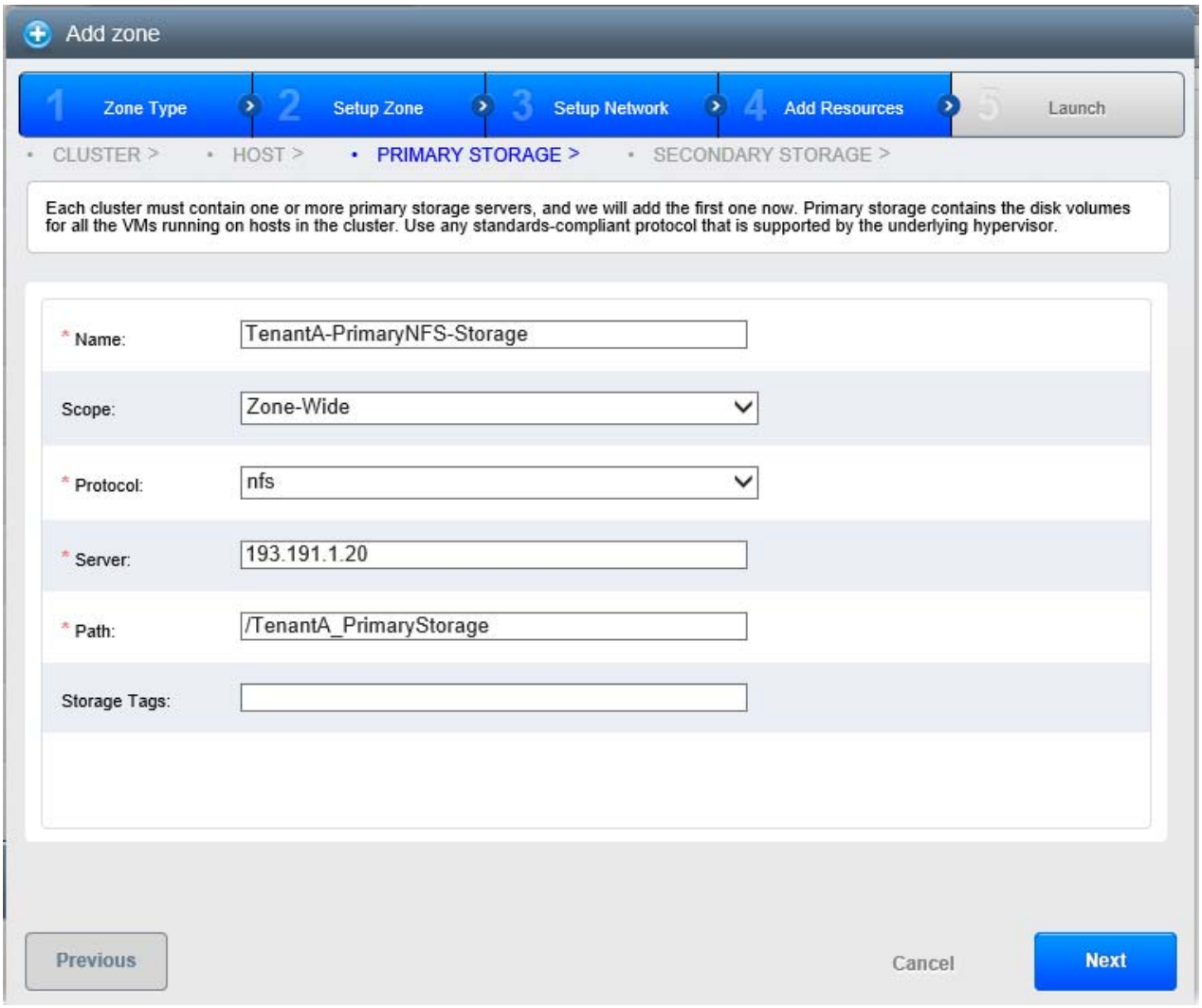
プライマリ ストレージ

CloudPlatfrom では、ゾーン ワイド ベース上でプライマリ ストレージを定義できます。プライマリ ストレージは、クラスタに関連付けられ、そのクラスタ内のホストで実行されているすべての VM のオペレーティング システムおよびデータのディスク ボリュームが格納されます。プライマリ ストレージは、ファイルまたはブロック ベースのプロトコルを使用して VM データを格納します。

クラウド サービスをホストするために TenantA マルチテナントに専用の Citrix CloudPlatform アプリケーションを使用して、ゾーンのプライマリ ストレージを追加するには、次の手順を実行します。

1. [Name] フィールドに <TenantA-PrimaryNFS-Storage> と入力します。
2. [Scope] フィールドに Zone-Wide と入力します。
3. [Protocol] リスト ボックスで [nfs] を選択します。
4. [Server] フィールドに <NetApp_NFS_LIF_IP_Address>193.191.1.20 と入力します。
5. [Path] フィールドに </TenantA_PrimaryStorage> と入力します。
6. [Next] をクリックします。

図 198　　プライマリ ストレージ プロパティの定義



セカンダリ ストレージ

セカンダリ ストレージはゾーンに関連付けられており、OS イメージに使用される VM テンプレートを格納します。OS イメージは、VM をブートするために使用でき、インストールされているアプリケーションなどの追加の設定情報を含むことができます。また、オペレーティング システムのデータまたはブート可能なメディアを含む OS イメージまたはディスク イメージを格納する ISO リポジトリを提供します。ストレージ VM ディスク ボリューム スナップショットは、データ リカバリまたは新しいテンプレートの作成に使用できる VM データの保存されたコピーを格納します。

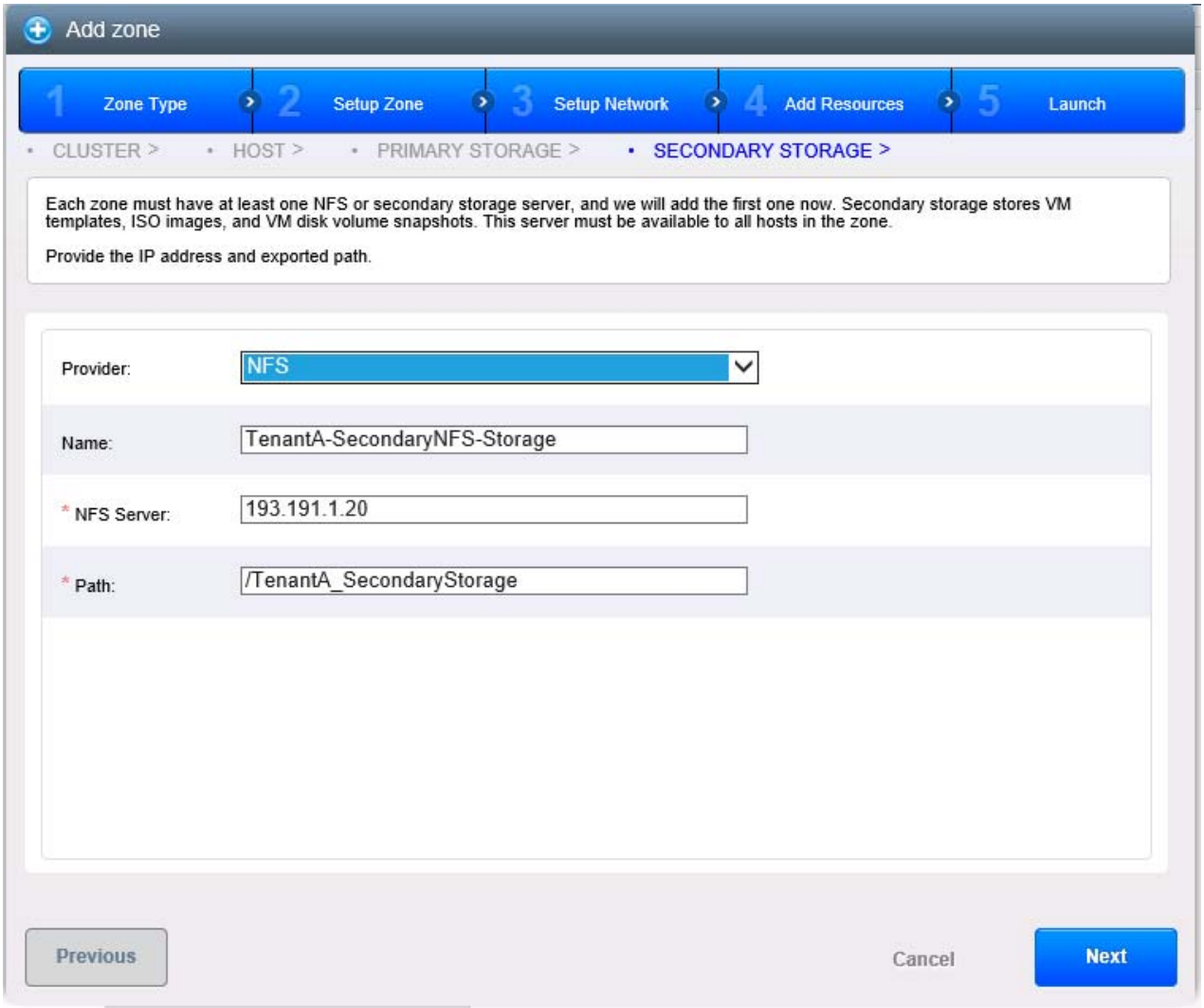
セカンダリ ストレージ内の項目は、ゾーン内のすべてのホストで使用できます。

クラウド サービスをホストするために TenantA マルチテナントに専用の Citrix CloudPlatform アプリケーションを使用して、ゾーンのセカンダリ ストレージを追加するには、次の手順を実行します。

1. [Provider] フィールドに <NFS> と入力します。
2. [Name] フィールドに </TenantA_SecondaryNFS-Storage> と入力します。
3. [NFS Server] フィールドに <NetApp_NFS_LIF_IP_Address>193.191.1.20 と入力します。

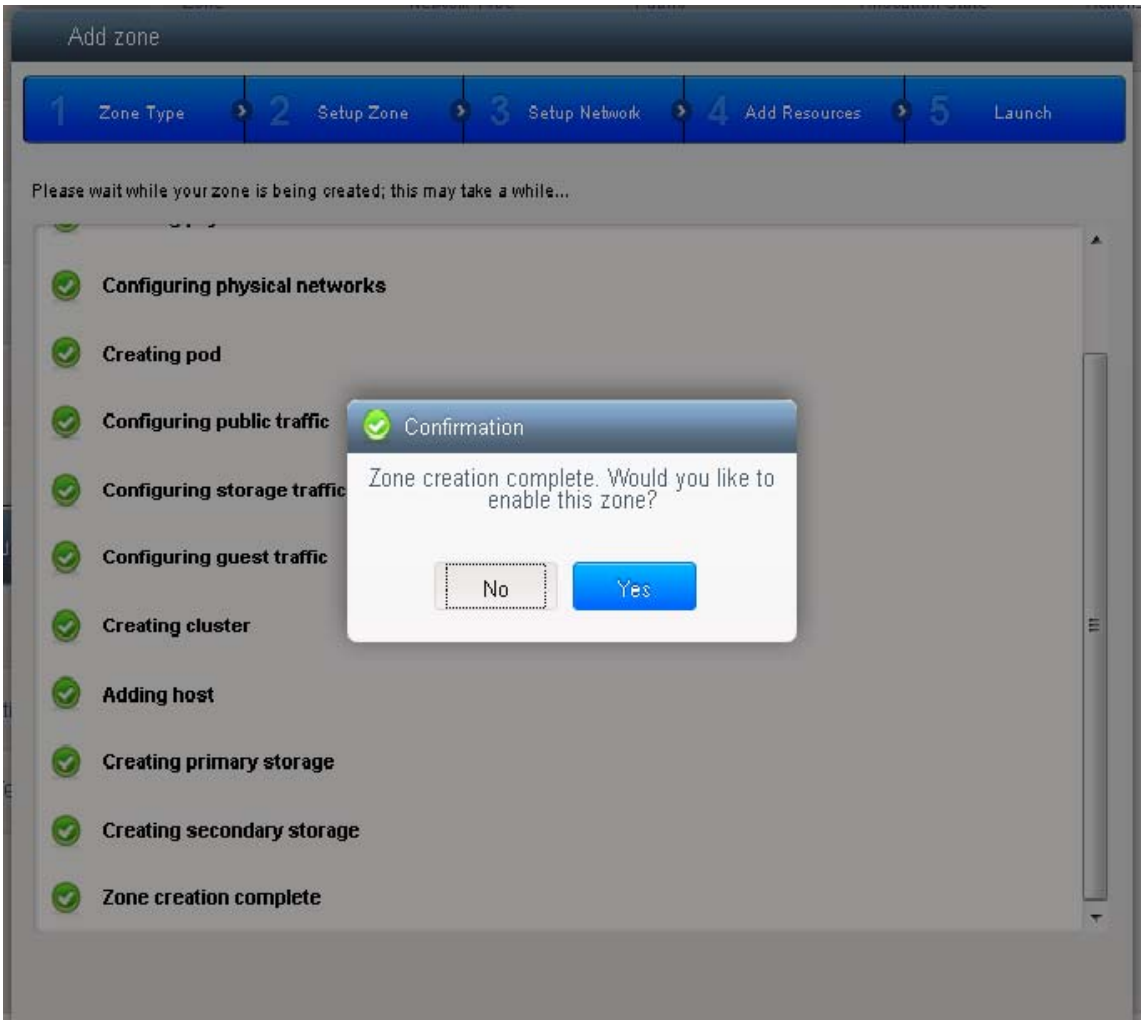
4. [Path] フィールドに </TenantA_SecondaryStorage> と入力します。
5. [Next] をクリックします。

図 199　　セカンダリ ストレージの名前とパスの定義



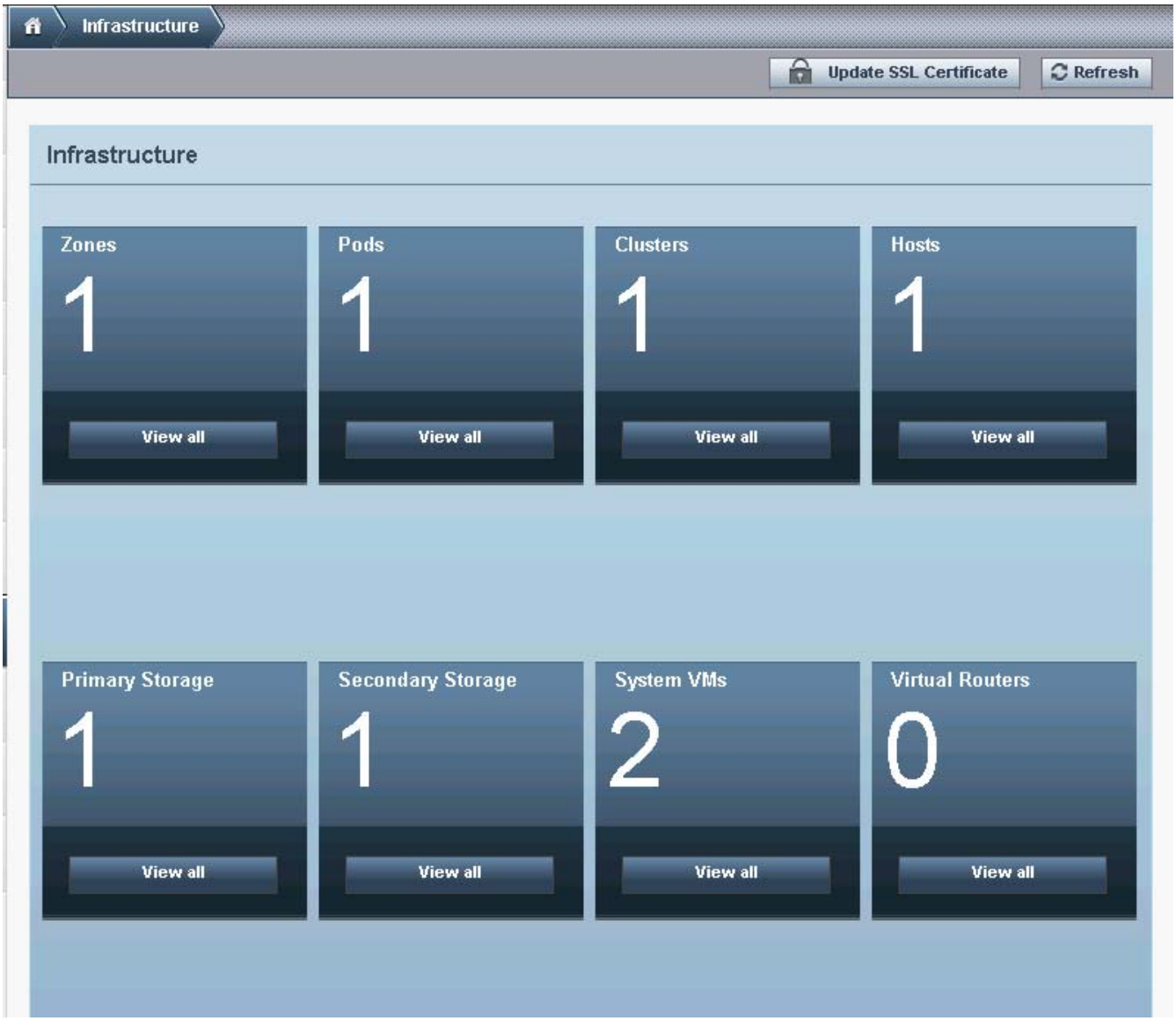
（注）　ゾーンが作成されたら、「Zone is ready to launch; proceed to the next step」というメッセージを含むウィンドウが表示されます。[Launch Zone] ボタンをクリックすると、ゾーンの有効化を確認するウィンドウが起動されます。[Yes] をクリックし、ゾーンを有効化します。

図 200　　ゾーンの有効化



（注）　ゾーンで定義されたすべてのコンポーネントを表示するクラウド インフラストラクチャ ウィンドウが表示されます。

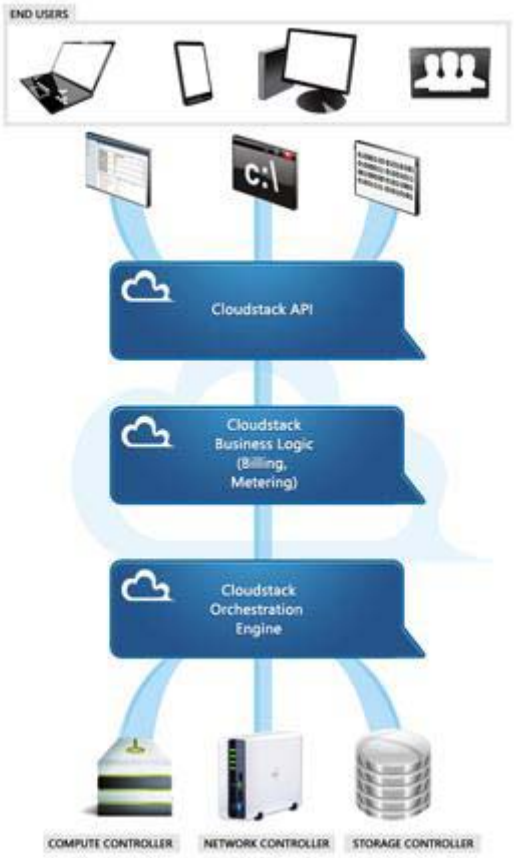
図 201　　ゾーンおよび他のコンポーネントの表示



クラウド インフラストラクチャ設計

この項では、クラウド サービスをホストするために複数のテナントに提供される Citrix CloudPlatform インフラストラクチャ オファリングおよびサービス レベルの概要を説明します。インフラストラクチャ オファリングには、テナントへの共有モデルで提供されるコンピューティング、ネットワークおよびストレージ リソースが含まれます。QoS に基づいたコストで、これらのリソースにサービス レベルを提供します。

図 202　CloudPlatform インフラストラクチャ設計



Citrix CloudPlatform、Cisco UCS および NetApp ストレージは、完全に統合されたクラウドのマルチテナントのソリューションを使用して、サービス レベル定義に基づいてプロビジョニング、設定および導入されるクラウド インフラストラクチャ リソースを提供します。この項では、次のインフラストラクチャ オファリングを Citrix Cloud Platform で有効化、設定および導入します。

- クラウド コンピューティング
- クラウド ストレージ
- クラウド ネットワーク

クラウド コンピューティング

Cisco UCS システムは、サービス プロファイル テンプレートとサービス プロファイル、および CPU とメモリの要件に基づくコンピューティング サーバ プールとサーバ プール資格情報ポリシー定義を提供します。これはサービス カタログのサービス レベル コスト定義に関連する場合があります。これらの SLA 定義は、サーバ プール資格情報定義を定義することによって、コンピューティング上でマップできます。Cisco UCS システムは、コンピューティング リソースを正しいサービス プロファイルに自動的に割り当て、サーバをそれぞれのサーバ プールに配置します。Cisco UCS は、コンピューティング、ネットワークおよびストレージの定義をホスト上で設定するための単一のウィンドウを提供するサービス プロファイル テンプレートとサービス プロファイルを提供します。それらは、サーバ プールを使用して、マルチテナント クラウドの要件をプロビジョニングするために取得されます。

CloudPlatfrom は、Cisco UCS Manager API を呼び出してコンピューティング操作を実行するプラグインを使用して、Cisco Unified Computing System 上でクラウド コンピューティングを管理、設定および導入する管理ウィンドウの単一のペインを提供します。Cisco UCS Manager プラグインが CloudPlatrorm に登録されると、クラウド管理者は、すばやくプロビジョニングし、サービス プロファイルを関連する B シリーズ ブレードに関連付けて、ESXi ハイパーバイザ OS サーバをインストールできます。

vSphere のホスト管理は、vCenter と CloudPlatform 管理者 UI の組み合わせで行われます。CloudPlatform には、データセンターで定義された VMware vCenter クラスタの一部である CloudPlatform クラスタに追加されたすべてのホストが必要です。複数ホストのクラスタでは、vMotion 移行などの機能が可能です。CloudPlafrom では、内部的に vCenter API を呼び出して、クラスタの VM 部分で vMotion 操作を実行する VM 移行操作を実行できます。VM vMotion を実行するには、共有 FC または NFS ストレージが必要です。

サービス レベル定義に基づく Citrix CloudPlatform は、高可用性、オン デマンド リソース、パフォーマンス、および容量をサポートするために、ゾーン内に複数のクラスタを定義できます。表 35 は、TenantA ゾーンに作成できるクラスタ定義の 4 つのサンプルを示しています。

表 35　　すべてのサービス レベルのクラスタ定義での CloudPlatform ホスト

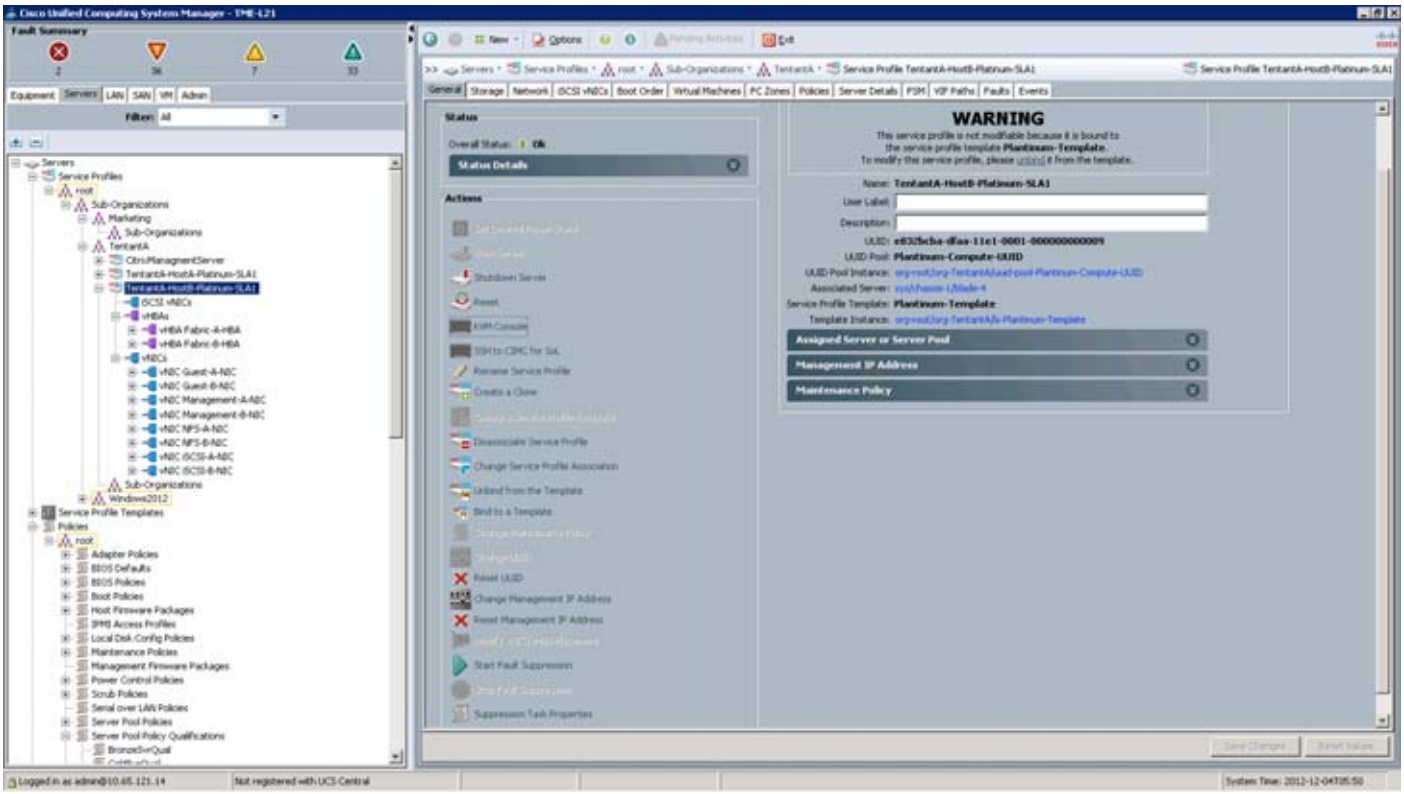
クラスタ名	ホスト リソース	UCS サービス プロファイル テンプレート	コンピューティング資格情報 最小～最大
TenantA-Platinum-Cluster	最高の CPU & メモリ パフォーマンス ハイ アベイラビリティ	Platinum-Template	32 ～ 40 CPU コア 128 ～ 256 GB メモリ
TenantA-Gold-Cluster	2 番目に高い CPU とメモリ パフォーマンス ハイ アベイラビリティ	Gold-Template	32 ～ 40 CPU コア 64 ～ 128 GB メモリ
TenantA-Silver-Cluster	3 番目に高い CPU とメモリ パフォーマンス ハイ アベイラビリティ	Silver-Template	12 ～ 16 CPU コア 32 ～ 64 GB メモリ
TenantA-Bronze-Cluster	4 番目に高い CPU とメモリ パフォーマンス ハイ アベイラビリティ	Bronze-Template	12 ～ 16 CPU コア 16 ～ 32 GB メモリ

このマニュアルでは、高可用性を実現するために 2 つの ESXi ホスト TenantA-HostA と TenantA-HostB ESXi を含む vCenter データセンター TenantA-DC の VMware クラスタ TenantA-Cluster 部分が追加され、Citrix CloudPlatform を使用して仮想マシンを割り当てるコンピュート オファリングを定義します。次の手順は、クラウド サービスをホストするために TenantA マルチテナントに専用の Citrix CloudPlatform アプリケーションを使用して仮想マシンを割り当てて、CPU、メモリ、ネットワーク、ホスト、および高可用性の定義を使用してコンピュート オファリングを作成する方法を示しています。

2 番目のホストの TenantA-HostB 上に ESXi サーバを導入するには、CloudPlatform ホストの準備に関する項を参照し、サービス レベルによるコンピューティング、ネットワークおよびストレージ インフラストラクチャ定義を含む Platinum-Template に基づいてサービス プロファイルを作成する方法を確認してください。

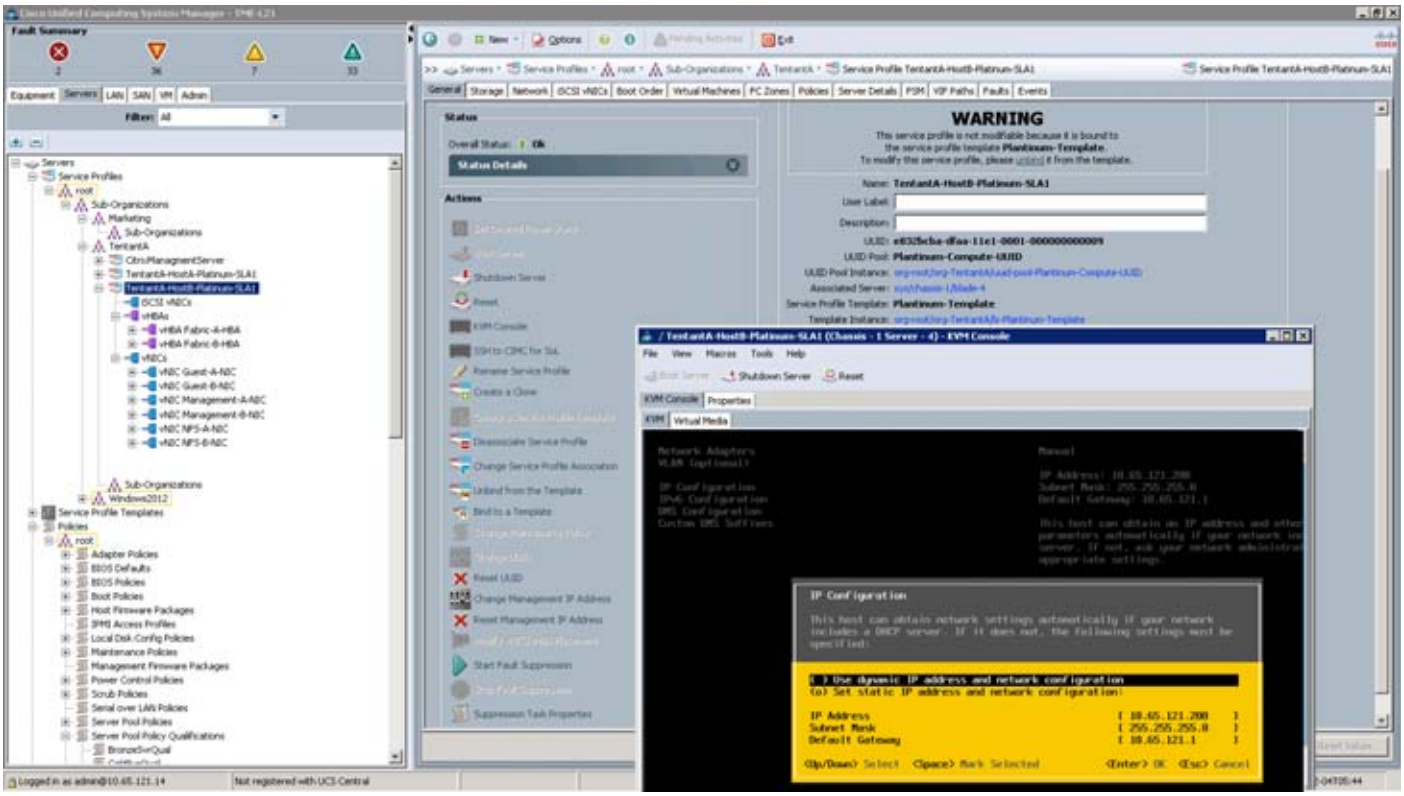
組織 TenantA に対して以前に作成したユーザ TenantA-Admin を使用して Cisco UCS Manager にログインします。

図 203　テナント A のサービス プロファイルの表示



1. 左ペインで [Server] タブをクリックします。
2. [Service Profiles] > [Sub-Organizations] を選択します。[TenantA] を展開します。
3. 「CloudPlatfrom ホストの準備」の項で示された手順を実行して、サービス プロファイル <TenantA-HostB-Platinum-SLA2> を作成します。
4. サービス プロファイル [<TenantA-HostB-Platinum-SLA2>] をクリックします。
5. 右ペインで、[KVM Console] をクリックします。

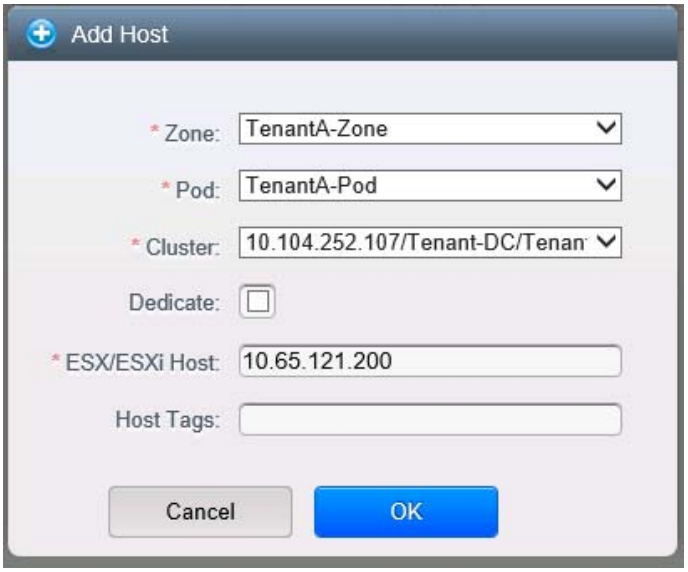
図 204　　ESXi サーバのステータスの表示



6. vCenter データセンター <Tenant-DC> の一部である vCenter クラスタ <TenantA-Cluster> に ESXi ホスト <10.65.121.200> を追加します。CloudPlatfrom は、[Hosts] タブで ESXi ホスト <10.65.121.200> を自動的に検出します。
   a. vCenter に接続されている VMware vSphere クライアントで、[Home] > [Host and Clusters] を選択します。
   b. vCenter、データセンター <Tenant-DC>、およびクラスタ <TenantA-Cluster> を展開します。
   c. [Basic Tasks] で [Add a host] をクリックします。
   d. [Host] テキスト ボックスに <10.65.121.200> と入力し、[Username] テキスト ボックスに <root>、[Password] に <xxxx> を入力し、[Next] をクリックします。
   e. [Yes] をクリックし、セキュリティ アラートを確認します。
   f. [Host summary] で [Next] をクリックします。
   g. [Assign a new license key to host] オプション ボタンをクリックします。
   h. [Next] をクリックします。
   i. [Enable Lockdown Mode] をオフにします。
   j. [Next] をクリックします。
   k. [Finish] をクリックします。
7. クラスタ <TenantA-Cluster> が vCenter のデータセンター <Tenant-DC> に追加されたら、CloudPlatfrom の [Hosts] タブで ESXi ホスト <10.65.121.200> を追加します。
   a. ユーザ名とパスワードを使って CloudPlatfrom にログインします。
   b. [Infrastructure] タブをクリックします。

c. 左ペインで [Hosts] をクリックします。
d. [Add Host] をクリックします。
e. [Zone] リスト ボックスで [TenantA-Zone] を選択します。
f. [Pod] リスト ボックスで [Tenant-Pod] を選択します。
g. [Cluster] リスト ボックスで [<10.104.252.107/Tenant-DC/TenantA-Cluster>] を選択します。
h. [ESX/ESXi Host Name] フィールドに <10.65.121.200> と入力します。
i. [OK] をクリックします。

図 205　CloudPlatfrom での 2 番目のクラスタ ホストの追加



8. vCenter および CloudPlatfrom に <10.65.121.200> が追加されたことを確認します。

図 206　VMWare vCenter データセンターおよびクラスタの設定

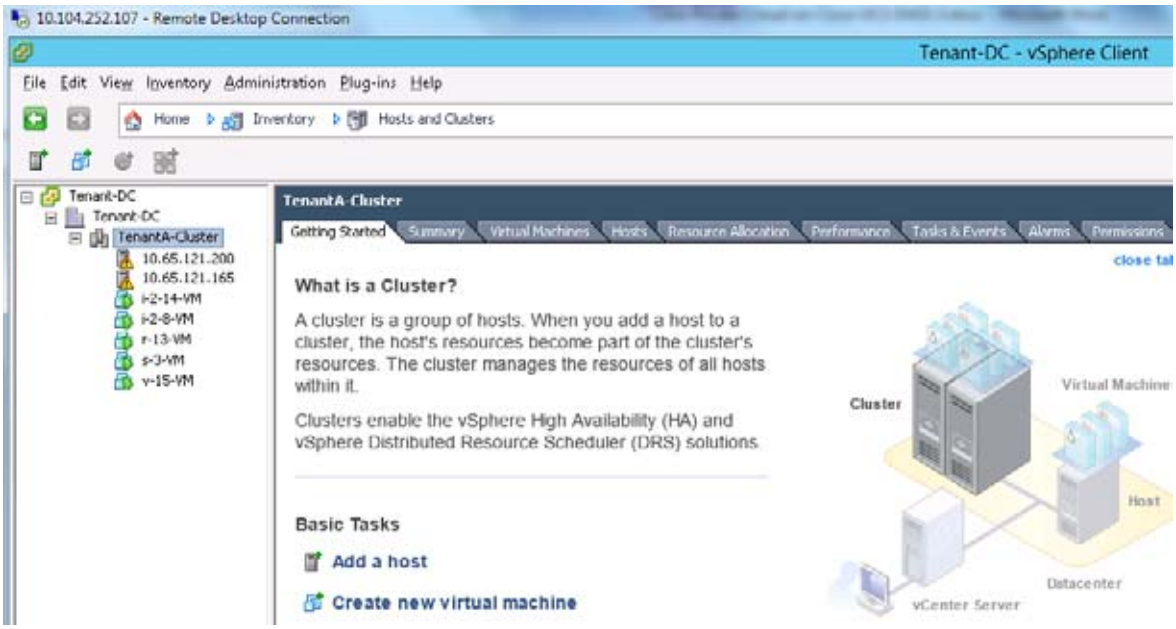
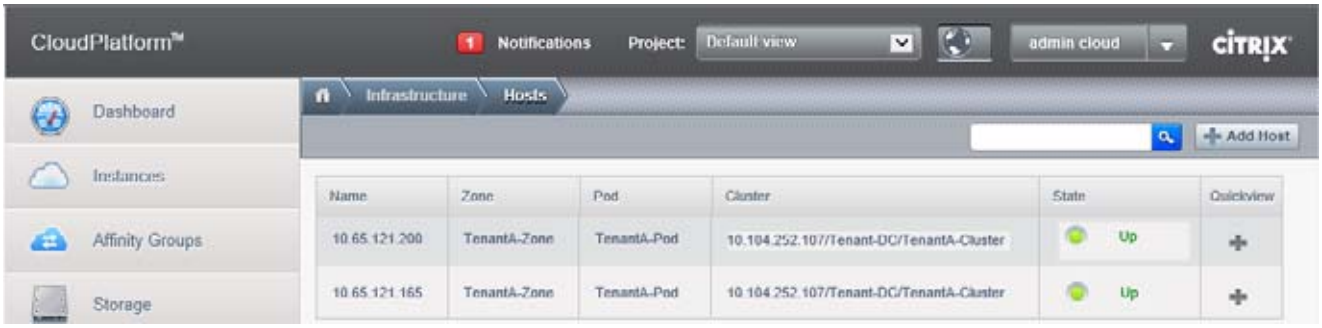


図 207　ESXi クラスタ ホストを表示する CloudPlatfrom ホスト



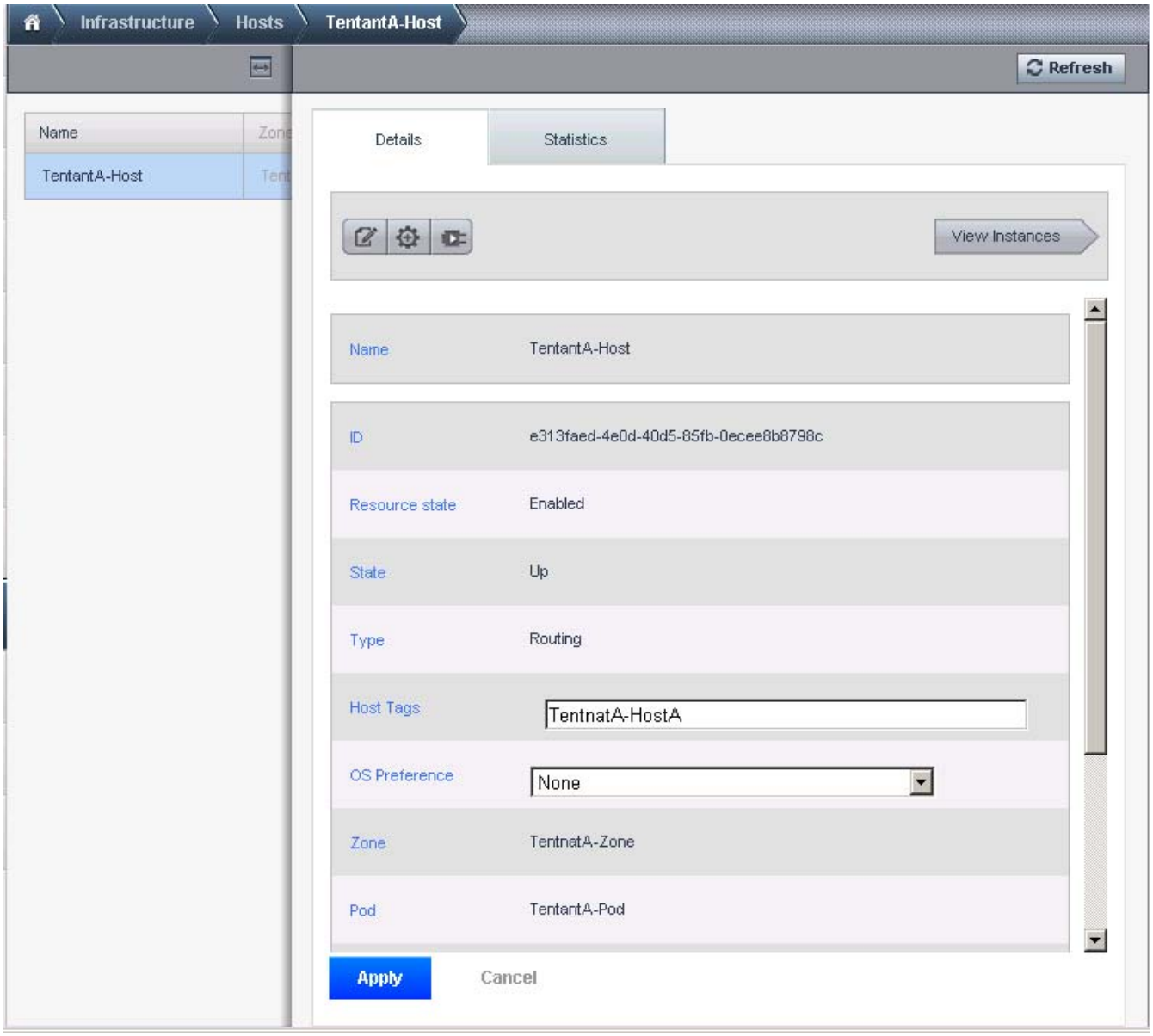
タグの定義

タグとは、プライマリ ストレージ、ディスク オファリング、またはコンピュート オファリングに関連付けられているテキスト文字列属性です。タグを使用すると、管理者はクラウド サービス オファリングに関する追加情報を提供でき、それらはコンピュート、サービス、およびディスク オファリングに配置されているタグと一致します。CloudPlatform では、仮想マシン ホストの配置およびプライマリ ストレージ上でデータ ディスクを割り当てるために、コンピュート、サービス、およびディスク オファリングに必要なタグを定義することができます。

ホスト タグ

1. [TenantA-HostA] をクリックします。
2. [Edit] アイコンをクリックします。
3. [Host Tags] フィールドに TenantA-HostA 名を入力します。
4. [Apply] をクリックします。

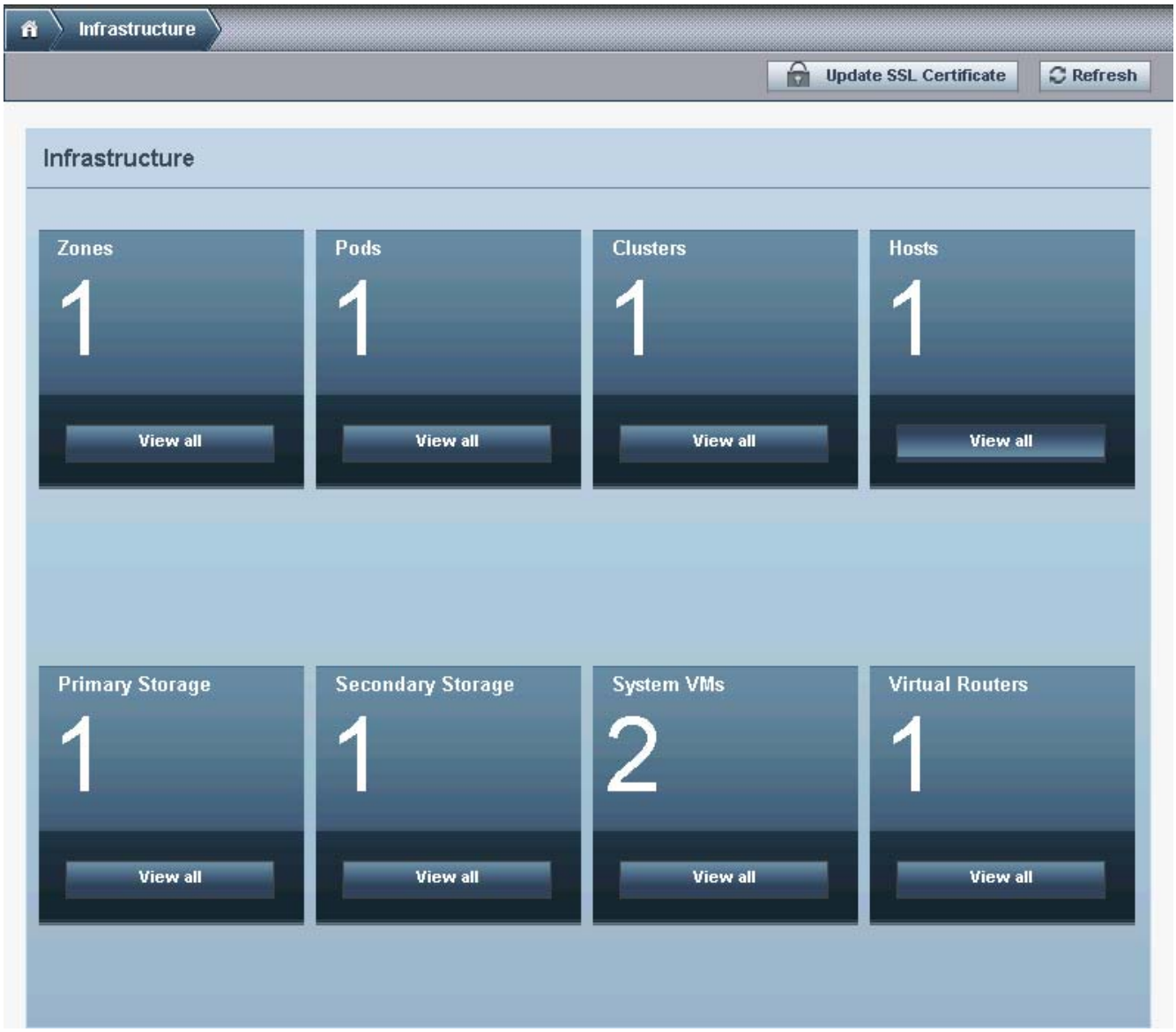
図 208　　ホストへのタグの追加



ストレージ タグ

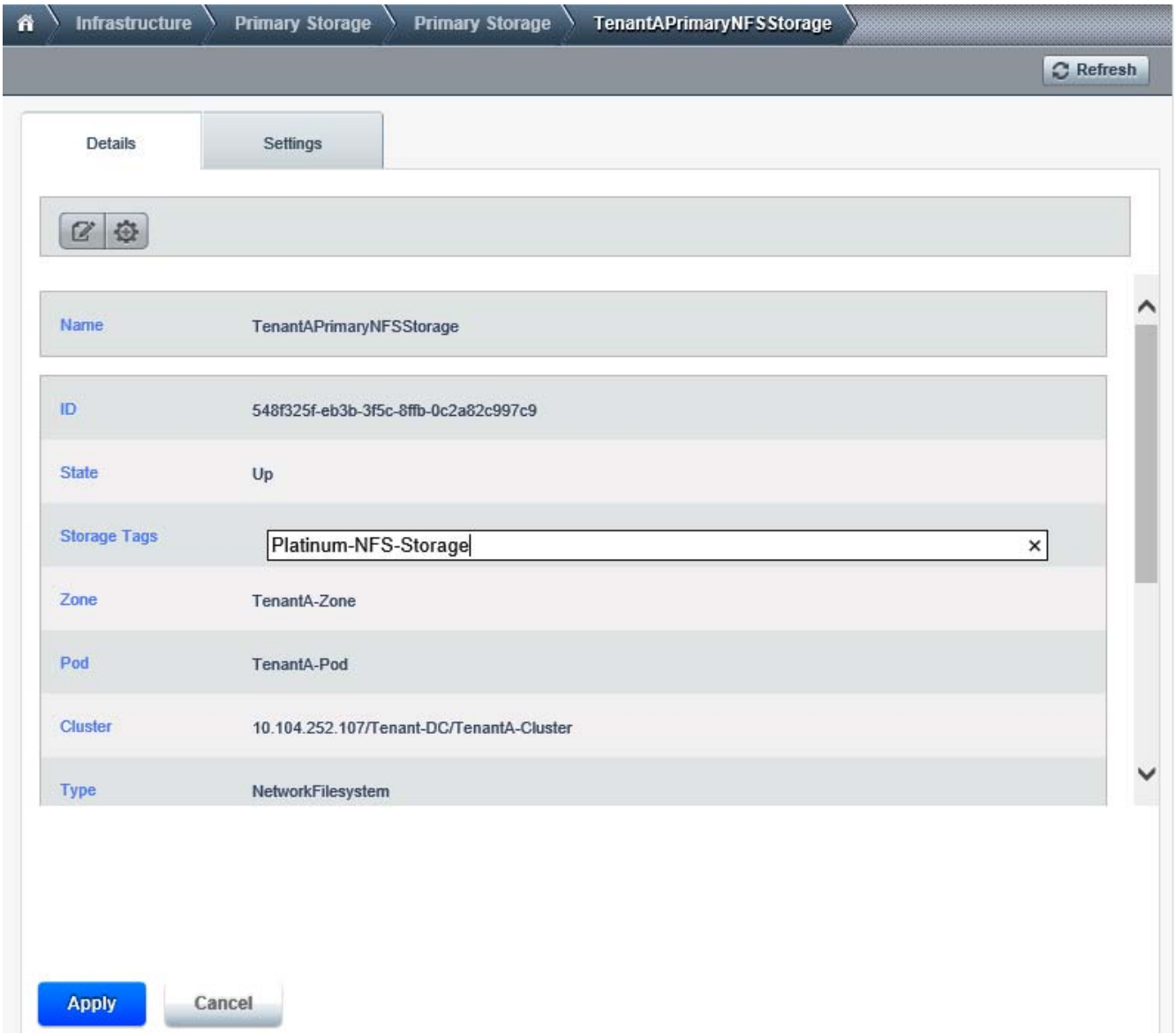
1. [Infrastructure] タブをクリックします。
2. 右ペインで [Primary Storage] をクリックします。

図 209　　プライマリ ストレージの選択



3. [TenantAPlatinumNFSStorage] をクリックします。
4. [Edit] アイコンをクリックします。
5. [Storage Tags] フィールドに **Platinum-NFS-Storage** と入力します。
6. [Apply] をクリックします。

図 210　　ストレージへのタグの適用



提供サービス

サービス オファリングは、CPU のコア数と速度、メモリ、およびディスク サイズなどの仮想ハードウェア機能をまとめたものです。CloudPlatform 管理者はさまざまなオファリングを設定でき、次にエンド ユーザがコンピューティング、ネットワーク、およびストレージ リソースを持つ新しい仮想マシンを作成するときに、使用可能なオファリングから選択します。

CloudPlatform はサービス オファリングをコンピュート オファリングとディスク オファリングに分けます。

コンピュート オファリングは次を指定します。

- ゲスト CPU
- ゲスト RAM

- ホスト タグ
- ストレージ タグ
- ネットワーク速度

ディスク オファリングは次を指定します。

- ディスク サイズ
- ストレージ タグ

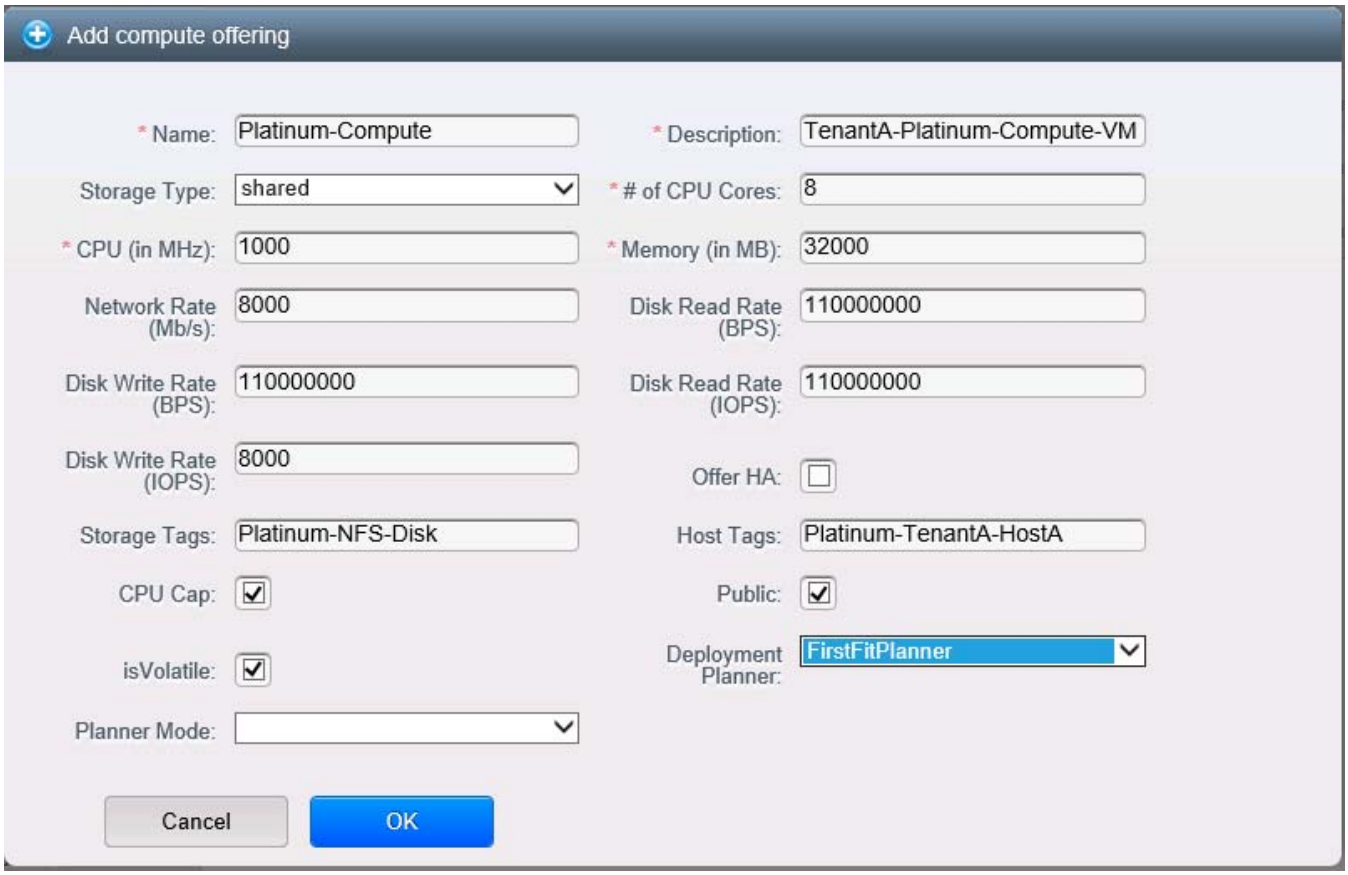
コンピュート オファリングの定義

1. [Service Offering] タブをクリックします。

図 211　　コンピュート オファリングの表示

2. [Select Offering] リスト ボックスで [Compute Offering] を選択します。
3. [Add compute offering] ボタンをクリックします。
4. [Name] フィールドに Platinum-Compute と入力します。
5. [Description] フィールドに TenantA-Platinum-Compute VM と入力します。
6. [Storage Type] リスト ボックスで [shared] を選択します。
7. [No of CPU Cores] フィールドに 16 と入力します。
8. [CPU] フィールドに 2 GHz を入力します。
9. [Memory] フィールドに 32 GB を入力します。
10. [Network ratek] フィールドに 8 G を入力します。
11. [Offer HA] チェックボックスをオンにします。
12. [Storage Tags] に Platinum-NFS-Disk と入力します。
13. [Host Tags] に TenantA-HostA と入力します。
14. [CPU Cap] チェックボックスをオンにします。
15. [OK] をクリックします。

図 212　コンピュート オファリング属性の表示



サービス レベル定義に基づいて Citrix CloudPlatform は、テナントの仮想マシンが高可用性、オン デマンド リソース、パフォーマンスおよび容量をサポートできるように、ゾーンで複数のコンピュート オファリングを定義してプロビジョニングできます。表 36 は、TenantA ゾーンに作成できる 4 つのコンピュート オファリングの定義を示しています。

表 36　4 つのサービス クラスのコンピュート オファリングの定義

コンピュート オファリング	VM CPU コア数および MHz	メモリ	ネットワーク速度	ディスクの読み取り/書き込み IOPS/ レート	ストレージ/ホスト タグ
Platinum-Compute	8 コア 2 GHz	32 GB	8GB	110000000	Platinum-Storage TenantA-Platinum-Host
Gold-Compute	6 コア 2 GHz	16 GB	6 GB	810000000	Gold-Storage TenantA-Gold-Host
Silver-Compute	4 コア 1 GHz	8 GB	4 GB	540000000	Silver-Storage TenantA-Silver-Host
Bronze-Compute	2 コア 1 GHz	4 GB	2 Gb	270000000	Bronze-Storage TenantA-Bronze-Host

クラウド ストレージ

この項では、クラウド上でマルチテナント データをホストするサービス レベル定義に基づくストレージ設計について説明します。記憶域は、NetApp ストレージ システムによってサービス レベル コストに基づいてプロビジョニングされ、プライマリ ストレージとして CloudPlatform アプリケーションに提供されます。プライマリ ストレージは、ゲスト仮想マシンがマルチテナントをホストするためにオペレーティング システムやデータ ファイルを格納するストレージを定義および設定することを許可します。

プライマリ ストレージは、クラスタに関連付けられ、ゾーンの一部であるそのクラスタ内のホストで実行されているすべての VM の OS およびディスク ボリュームが格納されます。これらのプライマリ ストレージへは、ファイバ チャネル、NFS または iSCSI プロトコルでアクセスできます。

サービス レベル定義に基づく Citrix CloudPlatform は、ゾーンで複数のプライマリ ストレージを定義し、これらの定義を使用して高可用性、オン デマンド リソース、パフォーマンスおよび容量をサポートします。表 37 に一覧表示されているこれらの定義は、TenantA ゾーンのクラスタで作成できる 3 つのプライマリ ストレージ定義を示しています。

表 37　　サービス クラスのプライマリ ストレージ定義

クラスタ名	プライマリ ストレージ（プロトコル）
TenantA-Platinum-Cluster	TenantA-FC-PrimaryStorage（ファイバ チャネル） TenantA-PrimaryNFS-Storage（NFS）
TenantA-Gold-Cluster	TenantA-Gold-FC-Storage（ファイバ チャネル） TenantA-Gold-NFS-Storage（NFS）
TenantA-Silver-Cluster	TenantA-Silver-FC-Storage（ファイバ チャネル） TenantA-Silver-NFS-Storage（NFS）
TenantA-Bronze-Cluster	TenantA-Bronze-FC-Storage（ファイバ チャネル） TenantA-Bronze-NFS-Storage（NFS）

このマニュアルでは、CloudPlatform を使用して TenantA-Platinum-Cluster に TenantA-Platinum-Storage、TenantA-Platinum-NFS-Storage および TenantA-Platinum-FC--Storage プライマリ ストレージを作成して、データ ディスクを仮想マシンに割り当てます。

次の手順は、クラウド サービスをホストするために TenantA マルチテナントに専用の Citrix CloudPlatform アプリケーションを使用してデータ ディスクを仮想マシンに割り当てて、ファイバ チャネルおよび NFS 上にプライマリ ストレージを作成する方法を示しています。

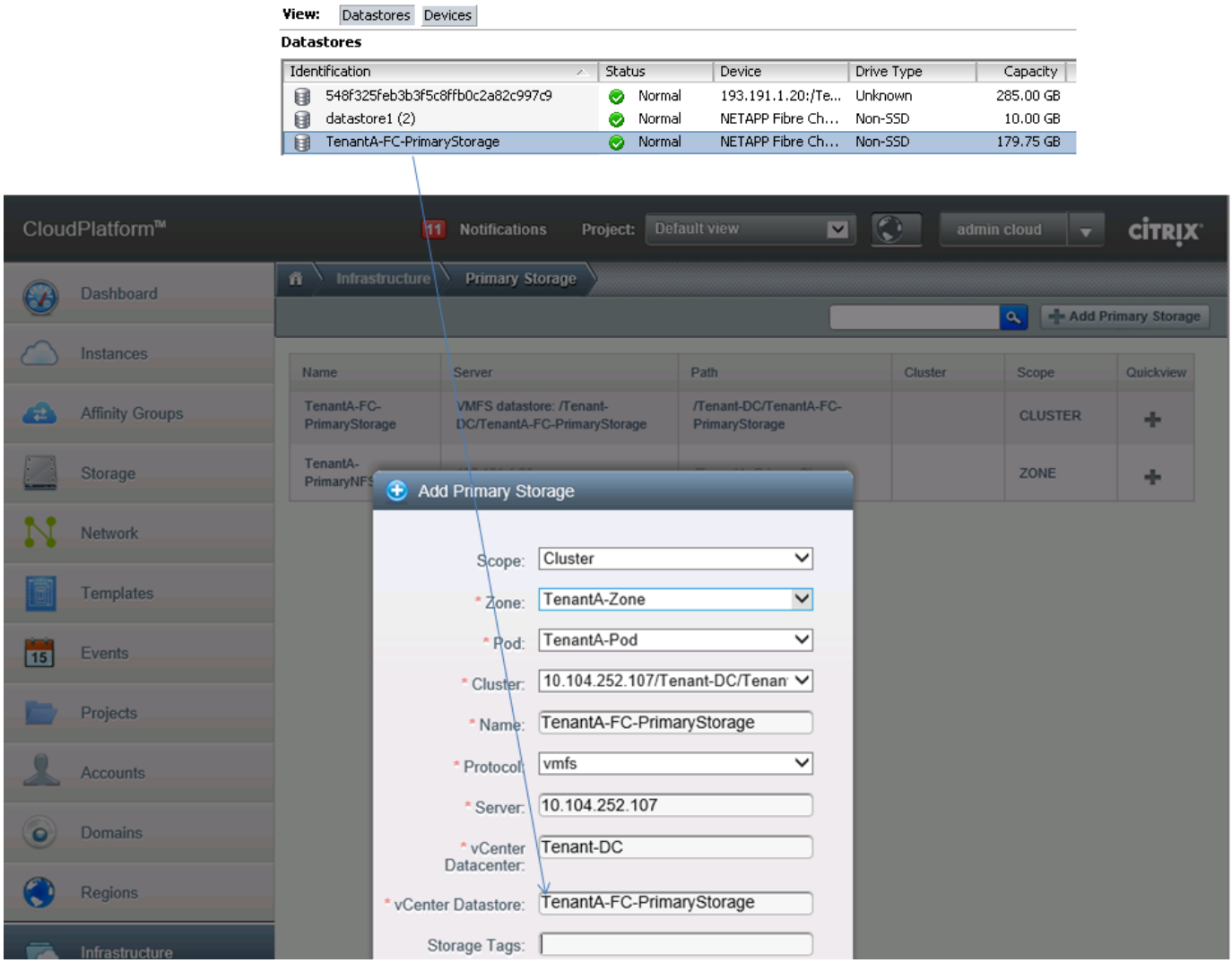
ユーザ資格情報を使用して CloudPlatform にログインして、TenantA ゾーンのプライマリ ストレージを設定します。

FC プライマリ ストレージの追加

1. [Add Primary Storage] ボタンをクリックします。
2. [Scope] リスト ボックスで [Cluster] を選択します。
3. [Zone] リスト ボックスで [TenantA-Zone] を選択します。
4. [Pod] リスト ボックスで [TenantA-Pod] を選択します。

5. [<vCenter_IP_Address>10.104.252.107/Tenant-DC-/TenantA-Cluster] を選択します。
6. [Name] フィールドに TenantA-FC-PrimaryStorage と入力します。
7. [Protocol] リスト ボックスで [vmfs] を選択します。
8. [Server] フィールドに <vCenter_IP_Address>10.104.252.107 と入力します。
9. [vCenter Datacenter] に Tenant-DC と入力します。
10. [vCenter Datastore] に TenantA-FC-PrimaryStorage と入力します。
11. [OK] をクリックします。

図 213　　FC プライマリ ストレージ情報の定義

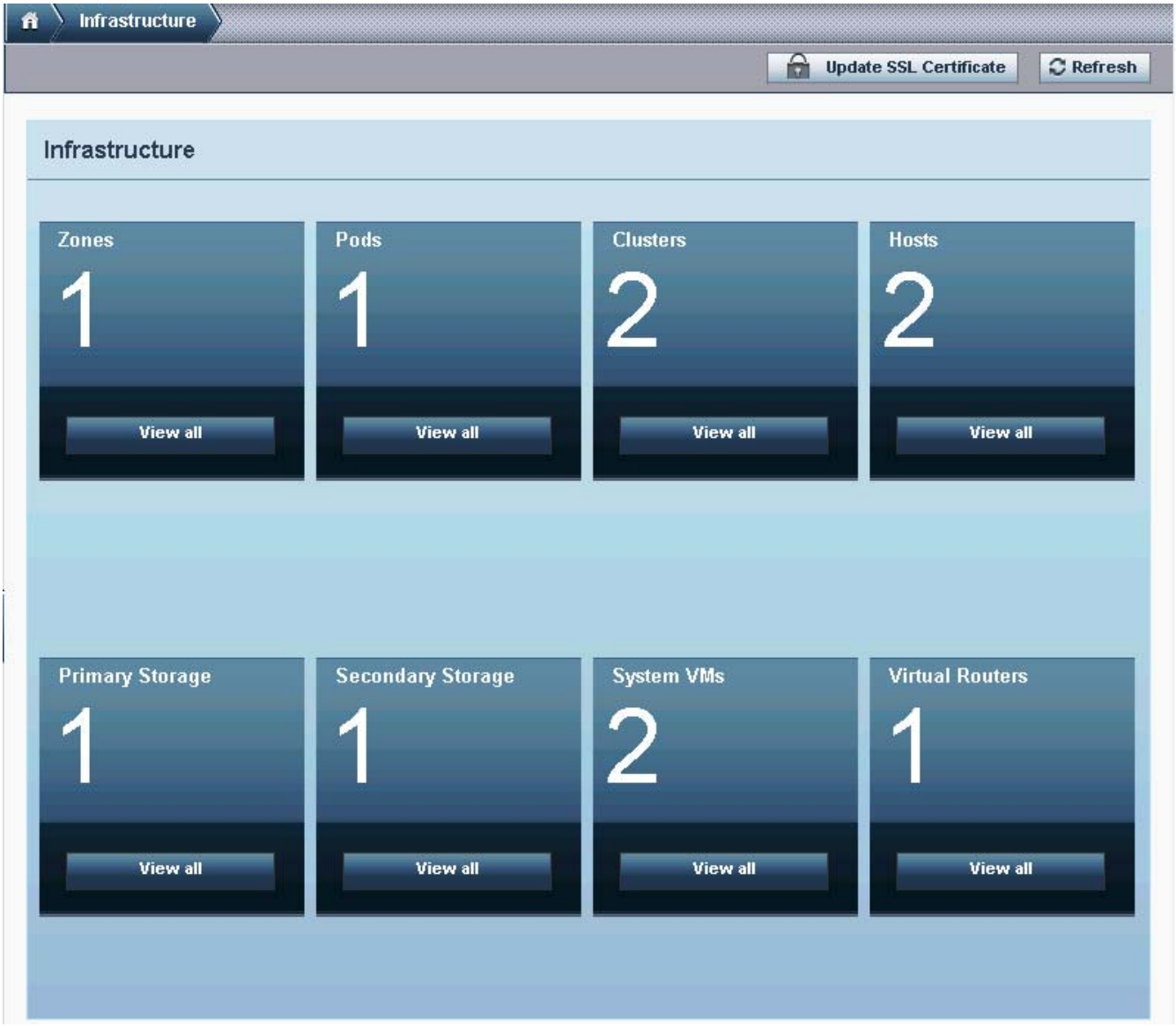


NFS プライマリ ストレージの追加

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。

3. 左ペインで [Infrastructure] タブをクリックします。
4. 右ペインの [Primary Storage] で [View All] をクリックします。

図 214　　プライマリ ストレージの表示



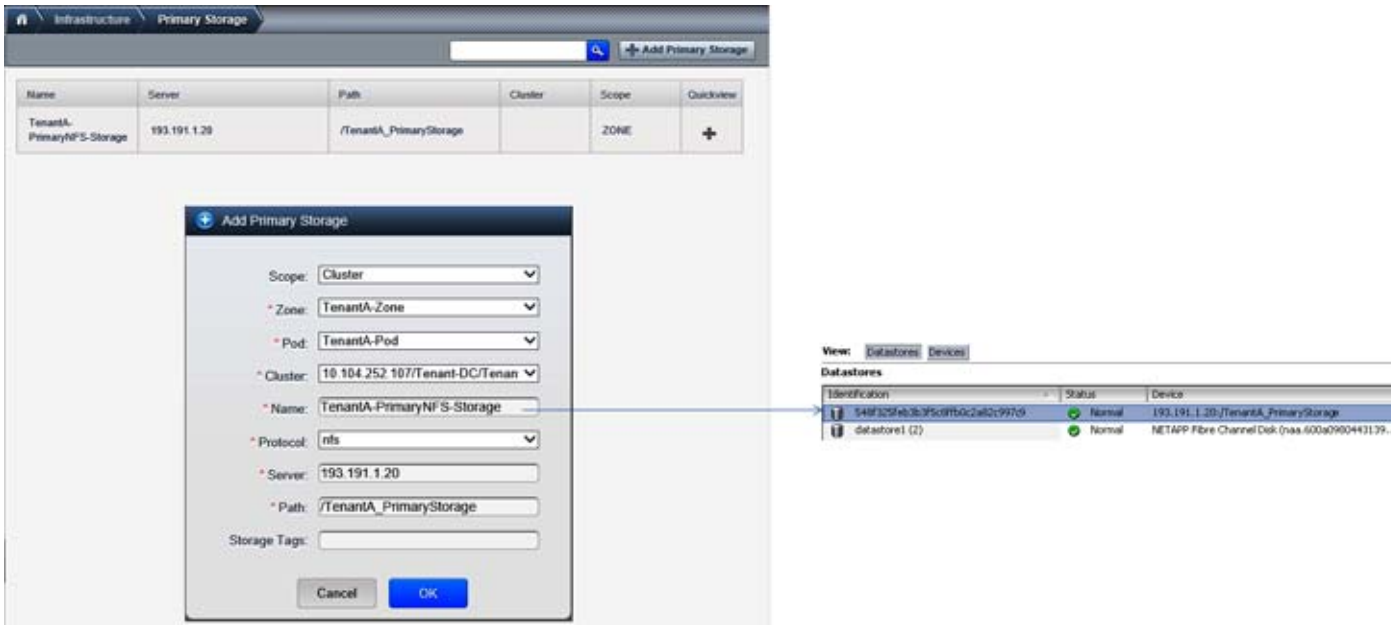
NFS プライマリ ストレージの追加

1. [Add Primary Storage] をクリックします。
2. [Scope] リスト ボックスで [Cluster] を選択します。
3. [Zone] リスト ボックスで [TenantA-Zone] を選択します。
4. [Pod] リスト ボックスで [TenantA-Pod] を選択します。
5. [<vCenter_IP_Address>10.104.252.107/Tenant-DC-/TenantA-Cluster] を選択します。

6. [Name] フィールドに TenantA-PrimaryNFS-Storage と入力します。
7. [Protocol] リスト ボックスで [nfs] を選択します。
8. [Server] フィールドに <NetApp_NFS_LIF_IP_Address>193.191.1.20 と入力します。
9. [Path] に /TenantA_PrimaryStorage と入力します。
10. [OK] をクリックします。

CloudPlatfrom での NFS プライマリ ストレージの追加に成功すると、対応する NFS データストアが、データセンター内の VMWare クラスタの ESX ホスト部分で自動的に設定されます。

図 215　　NFS プライマリ ストレージ情報の定義



クラウド ストレージ ボリューム

プライマリ ストレージで作成されたサービス レベル定義に基づいてテナント仮想マシンへのデータ ストレージ アクセスを提供するために、CloudPlatform ではボリューム、つまり特定の VM に追加のデータ ディスクを提供できるストレージの単位を実装しています。CloudPlatform では、ボリュームをゲスト VM が使用可能なストレージの単位と定義します。

データ ディスクは追加のストレージを備えています（「/opt」または「D:」など）。すべての VM はルート ディスクを持ち、VM はオプションとしてデータ ディスクも持つことができます。エンド ユーザは、複数のデータ ディスクをゲスト VM にマウントできます。ユーザは、クラウド管理者によって作成されたディスク オファリングからデータ ディスクを選択します。

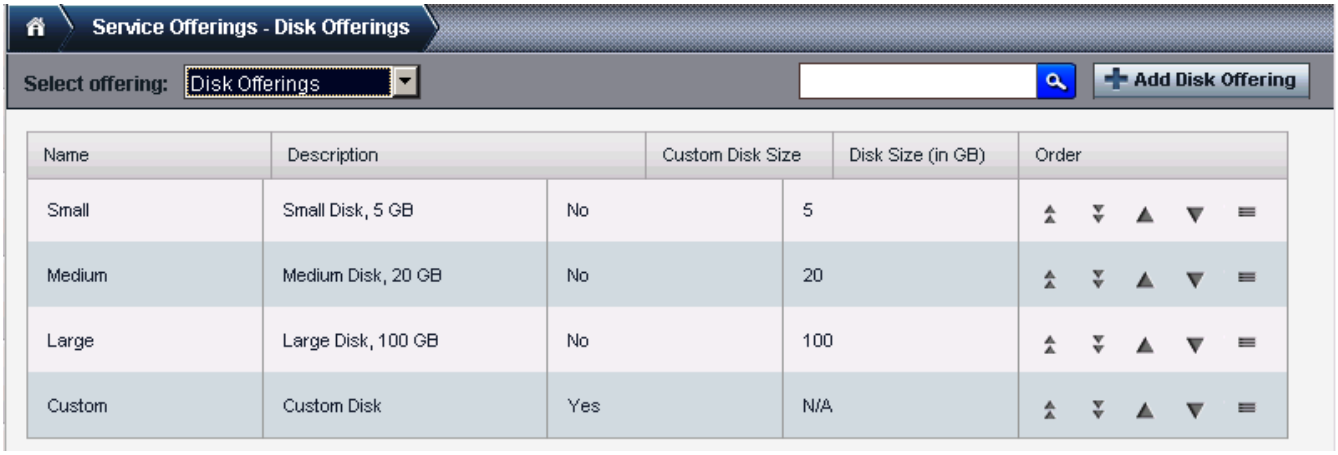
ユーザ資格情報を使用して CloudPlatform にログインして、TenantA ゾーンのプライマリ ストレージを設定します。

ディスク オファリングの定義

1. [Service Offering] タブをクリックします。

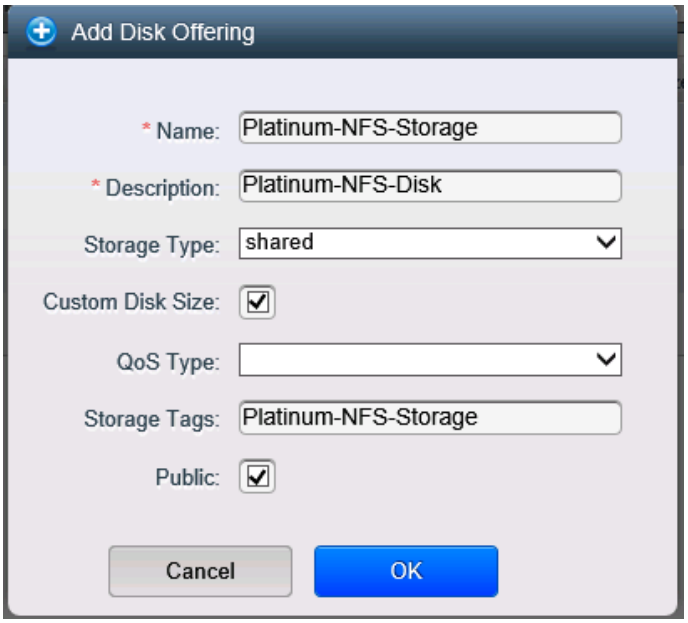
2. [Select Offering] リスト ボックスで [Offering] を選択します。
3. [Add Disk Offering] ボタンをクリックします。

図 216　　ディスク オファリングの選択



4. [Name] フィールドに Platinum-NFS-Storage と入力します。
5. [Description] フィールドに Platinum-NFS-Disk と入力します。
6. [Storage Type] リスト ボックスで [shared] を選択します。
7. [Custom Tags] チェックボックスをオンにします。
8. [QoS Type] を空白のままにします。
9. [Storage Tags] に Platinum-NFS-Storage と入力します。
10. [Public] チェックボックスをオンにします。
11. [OK] をクリックします。

図 217　　ディスク オファリング情報の定義



サービス レベル定義に基づいて Citrix CloudPlatform は、てテナントの仮想マシンが高可用性、オンデマンド リソース、パフォーマンス、および容量をサポートできるように、ゾーン内に複数のディスク オファリングを定義してプロビジョニングできます。表 38 は、TenantA ゾーンに作成できる 4 つのディスク オファリングの定義を示しています。

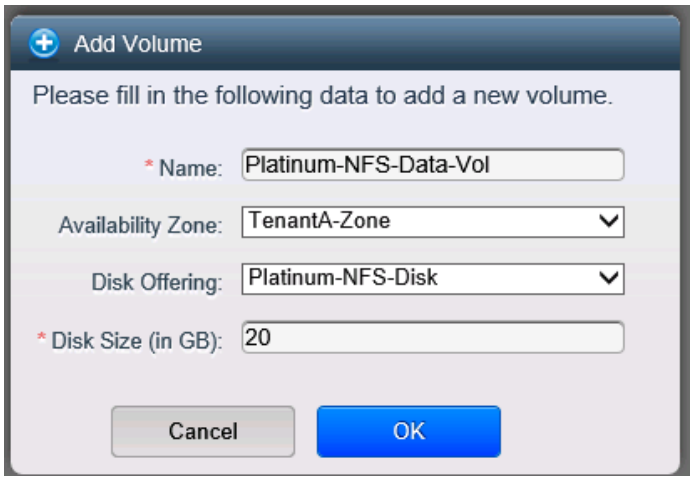
表 38　　すべてのサービス クラスのディスク オファリングの定義

ディスク オファリング	ストレージ タグ
Platinum-Storage-Disk	Platinum-NFS-Storage
Gold-Storage-Disk	Gold-NFS-Storage
Silver-Storage-Disk	Silver-NFS-Storage
Bronze-Storage-Disk	Bronze-NFS-Storage

ストレージ ボリュームの作成

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. 左側ペインで [Storage] タブをクリックします。
4. 右ペインで、[Add Volume] をクリックします。
5. [Name] フィールドに Platinum-NFS-Data-Vol と入力します。
6. [Availability Zone] リスト ボックスで [TenantA-Zone] を選択します。
7. [Disk Offering] リスト ボックスで [Platinum-NFS-Disk] を選択します。
8. [Disk Size] フィールドに 20 の値を入力します。

図 218　　ボリューム データの定義



サービス レベル定義に基づく Citrix CloudPlatform は、ゾーン内のディスク オファリング要件に基づいて複数のボリュームを定義し、これらの定義を用いて高可用性、オン デマンド リソース、パフォーマンス、および容量をサポートします。表 39 は、TenantA ゾーンの仮想マシンにデータ ディスクを割り当てるために作成可能な 4 つのボリューム定義を示しています。

表 39　　ディスク オファリングに基づくボリューム定義

ボリューム名	ディスク オファリング
Platinum-NFS-Data-Vol	Platinum-NFS-Disk
Gold-NFS-Data-Vol	Gold-NFS-Disk
Silver-NFS-Data-Vol	Silver-NFS-Disk
Bronze-NFS-Data-Vol	Bronze-NFS-Disk

クラウド ネットワーク

ネットワークの分離を実現し、特定のテナント ネットワークのサービス レベル定義に基づいてカスタム ネットワーク サービスを提供するために、CloudPlatform は、アドバンスド ゾーン ネットワーク トラフィック タイプ、およびゾーン ベースで適用できるネットワーク オファリングを実装します。

このマニュアルでは、ゾーンは、複数の物理ネットワークが 1 つ以上のトラフィック タイプを伝送できるアドバンスド ゾーン ネットワーキングを使用するように設定されており、管理者はネットワークによって伝送されるネットワーク トラフィックのタイプについて CloudPlatform で定義する必要があります。アドバンスド ゾーンのトラフィック タイプを次に示します。

- Guest

  エンドユーザが VM を実行すると、ゲスト トラフィックが生成されます。ゲスト VM は、ゲスト ネットワークと呼ばれるネットワークを介して互いに通信します。このネットワークを分離、または共有できます。分離ゲスト ネットワークでは、管理者は CloudPlatform アカウントのネットワークごとに分離を実現するために VLAN 範囲を予約する必要があります（VLAN の数が多くなる可能性があります）。共有ゲスト ネットワークでは、すべてのゲスト VM が単一のネットワークを共有します。

- 管理

  CloudPlatform の内部リソースが互いに通信すると、管理トラフィックが生成されます。これには、ホスト、システム VM（CloudPlatform がクラウドでさまざまなタスクを実行するために使用する VM）、および、CloudPlatform 管理サーバと直接通信するその他のコンポーネント間の通信が含まれます。使用するシステム VM の IP 範囲を設定する必要があります。

- パブリック

  このトラフィックはクラウド上の VM がインターネットにアクセスする際に生成されます。このために、パブリックにアクセス可能な IP を割り当てる必要があります。エンド ユーザは、CloudPlatform UI を使用して IP を取得して、ゲスト ネットワークとパブリック ネットワーク間で NAT を実装することができます。

- ストレージ

  このトラフィックは VM テンプレートおよびスナップショットなどで、セカンダリ ストレージ VM とセカンダリ ストレージ サーバ間で送信されます。CloudPlatform は、ストレージ ネットワーク トラフィックに対してストレージ NIC という名前の個別のネットワーク インターフェイス コントローラ（NIC）を使用します。

（注） Cisco UCS Compute System で異なる物理ネットワーク デバイスに対してこれらのネットワーク トラフィック タイプを設計および設定する方法の詳細については、CloudPlatform ホストの準備および導入に関する項を参照してください。

ネットワーク オファリング

CloudPlatform 管理者は、CloudPlatform で提供されるデフォルトのネットワーク オファリングに加えて、任意の数のカスタム ネットワーク オファリングを作成できます。複数のカスタム ネットワーク オファリングを作成することによって、クラウドは単一のマルチテナント物理ネットワーク上で異なるクラスのサービスを提供するように装備され、これにより、サービス レベル コスト定義に基づくさまざまなレベルのサービスも保証されます。

例：次の 2 つのテナントがある場合を想定しています。テナント A はその Web サイト用に単純なファイアウォールを必要としますが、テナント B は Web サーバ ファームを実行していて、スケーラブルなファイアウォール ソリューション、ロード バランシング ソリューション、およびデータベース バックエンドにアクセスするための代替ネットワークが必要です。

このマニュアルでは、ゾーンのアドバンスド ネットワークの設定中に定義されるデフォルトの分離ネットワーク オファリングを使用します。サービス レベル定義およびネットワーク提供サービスに基づいて、Citrix CloudPlatform はゾーンで複数のネットワークを定義できます。

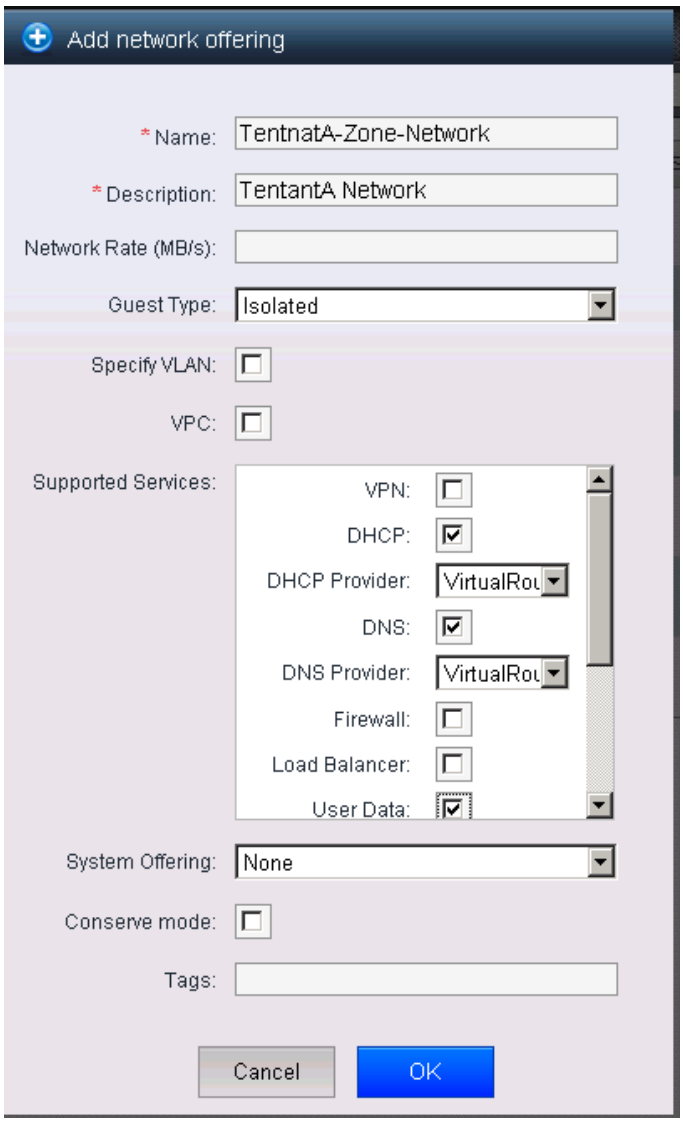
ユーザ資格情報を使用して CloudPlatform にログインして、TenantA ゾーンのプライマリ ストレージを設定します。

ネットワーク オファリングの作成

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Service Offering] タブをクリックします。
4. [Select Offering] リスト ボックスで [Network Offering] を選択します。
5. [Add network offering] をクリックします。
6. [Name] フィールドに TenantA-Zone-Network と入力します。

7. [Description] フィールドに TenantA Network と入力します。
8. [Guest Traffic] リスト ボックスで [Isolated] を選択します。
9. [Required Services] リスト ボックスで [DHCP]、[DNS]、[UserData] チェック ボックスをオンにします。
10. [OK] をクリックします。

図 219　　ネットワーク オファリング プロパティの定義

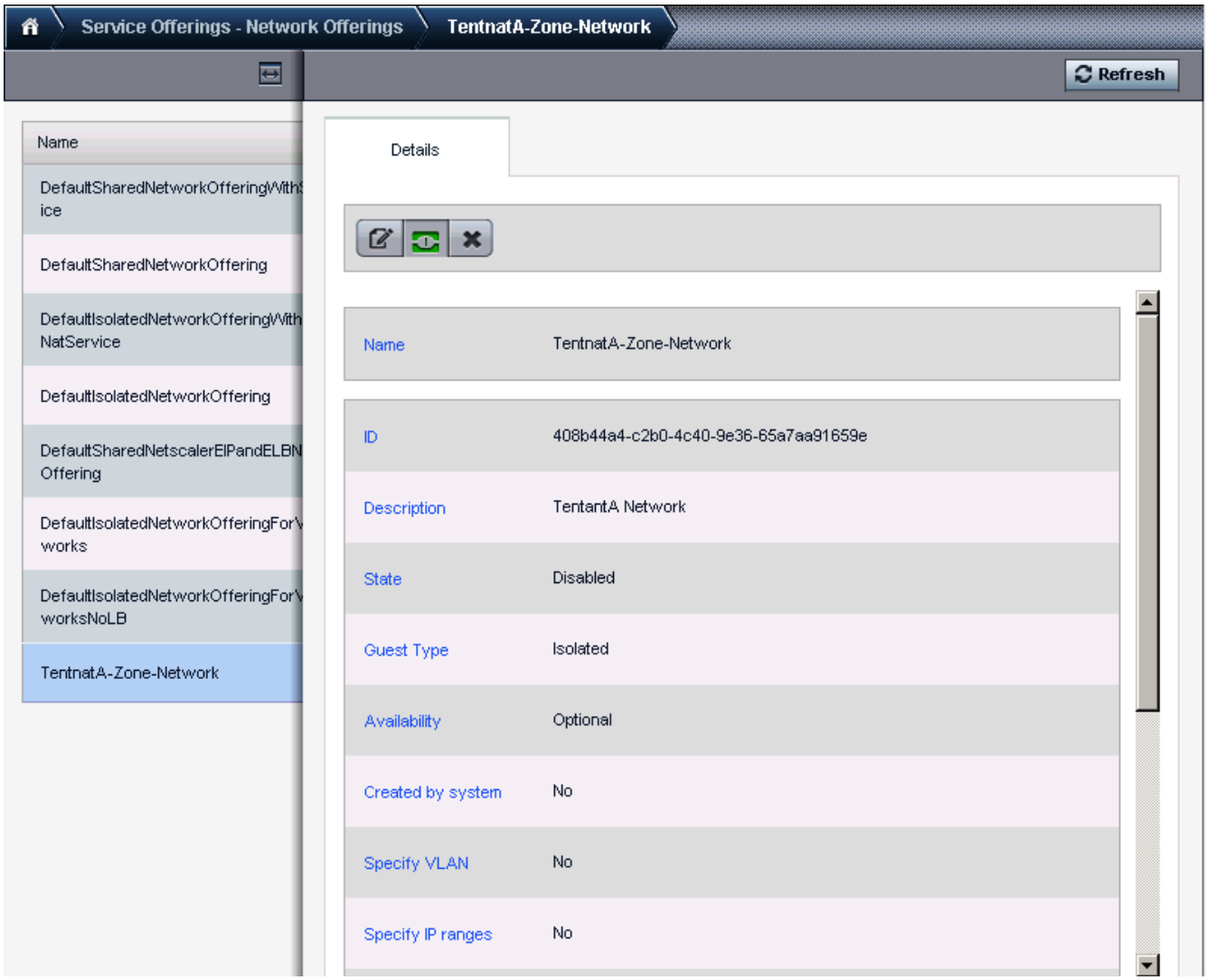


11. [TenantA-Zone-Network] オプション ボタンをクリックすると、無効になります。

図 220　ネットワーク オファリング ステータスの表示

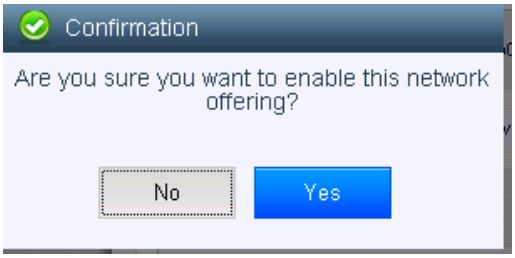
12. [Enable] アイコンをクリックします。

図 221　TenantA ゾーン ネットワークの有効化



13. [OK] をクリックします。

図 222　ネットワーク オファリングの有効化の確認



仮想マシンの設定と管理

CloudPlatform では、管理者はクラウド内で実行しているすべてのゲスト VM のライフ サイクルを完全に制御できます。CloudPlatform は、いくつかのゲスト管理操作をエンド ユーザおよび管理者に提供します。VM を停止、開始、リブート、および破棄できます。

この項では、共有クラウド インフラストラクチャ上のマルチテナント仮想マシンをプロビジョニングするために従う仮想マシン（VM）ライフ サイクル管理設計プロセスについて説明します。Citrix CloudPlatform から提供される VM 管理機能には、ライブ スナップショット、チェックポイント、移行、バックアップ、および削除が含まれます。

仮想マシンのライフ サイクルの管理に関連するタスクは、次のとおりです。

- VM インフラストラクチャ
- VM へのオペレーティング システムのインストール
- VM の設定
- VM のバックアップおよび復元
- VM の移行
- VM の削除

VM インフラストラクチャ

この項では、定義済みのサービス レベル コストに基づいて、マルチテナントに専用の仮想マシンのコンピューティング、ネットワーク、およびストレージ インフラストラクチャを作成する方法について説明します。コンピューティング、ネットワーク、およびストレージのクラウド要件に関する初期クラウド インフラストラクチャ設計は、前の項で定義されています。

ここでは、CloudPlatform を使用して Windows 2008 R2 ISO イメージを追加し、プラチナ レベルのコンピューティング、ネットワークおよびストレージのクラウド インフラストラクチャの仮想マシンを作成します。

ユーザ資格情報を使用して CloudPlatform にログインして、TenantA ゾーンの ISO イメージを作成します。

CloudPaltfrom がダウンロードする Windows 2008 R2 ISO が配置されている HTTP の追加

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. 検索タイプ secstorage.allowed.internal.sites で [Global Setting] タブをクリックします。
4. secstorage.allowed.internal.sites で <<Var_HTTP_Server>> 10.65.121.70 と入力します。
5. CloudPlatfrom サービスを再起動します。

ISO イメージの追加

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Templates] タブをクリックします。
4. [Select view] リスト ボックスで [ISO] を選択します。

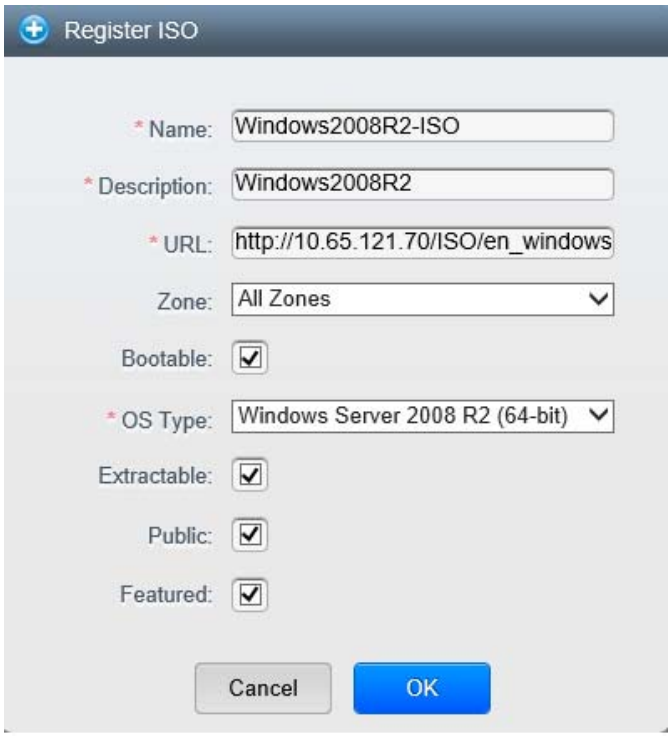
図 223　　ISO テンプレートの表示

5. [Register ISO] をクリックします。
6. [Name] フィールドに Windows2008R2-ISO と入力します。
7. [Description] フィールドに Windows2008R2 と入力します。
8. [URL] フィールドに http://10.65.121.70/ISO/en_windows_server_2008_r2_standard_enterprise_datacenter_and_web_with_sp1_x64_dvd_617601.iso と入力します。

（注）　HTTP サーバがセットアップされ、/etc/www/html パスの下に Windows 2008 R2 ISO イメージを格納されていることを確認します。

9. [Zone] リスト ボックスで [TenantA-Zone] を選択します。
10. [Bootable] チェックボックスをオンにします。
11. [OS Type] リスト ボックスで [Windows 2008 R2（64-bit）] を選択します。
12. [Extractable] チェックボックスをオンにします。
13. [Public] チェックボックスをオンにします。
14. [Featured] チェックボックスをオンにします。
15. [OK] をクリックします。

図 224　　ISO プロパティの登録



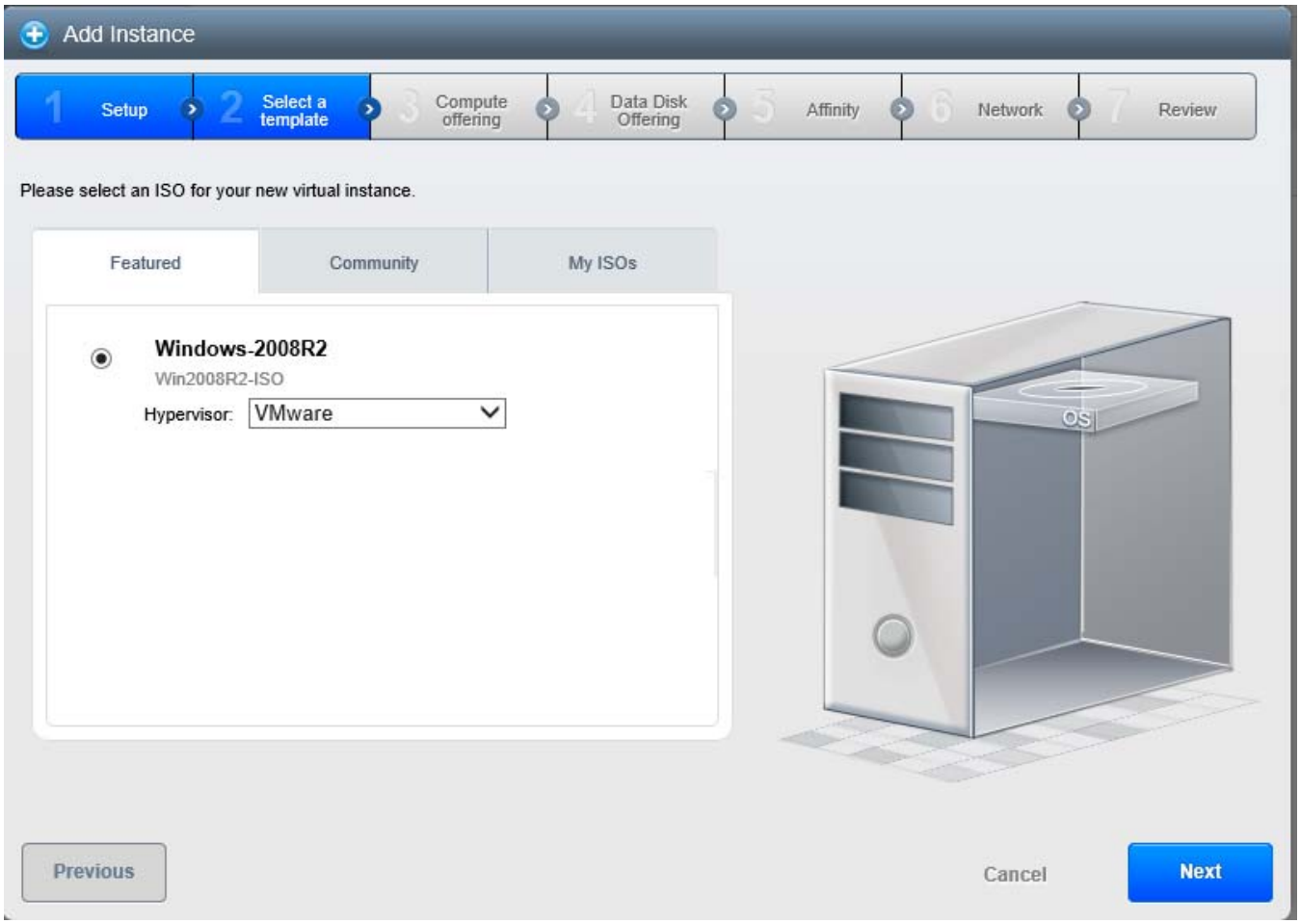
VM の作成

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Instance] タブをクリックします。
4. [Select view] リスト ボックスで [ISO] を選択します。
5. [Add Instance] をクリックします。
6. [Zone] リスト ボックスで [TenantA-Zone] を選択します。
7. [ISO] オプション ボタンを選択します。
8. [Next] をクリックします。

図 225　　インスタンスの名前とイメージの定義

9. [Windows-2008R2 Image] オプション ボタンをクリックします。
10. [Hypervisor] リスト ボックスで [ESXiServer] を選択します。
11. [Next] をクリックします。

図 226　　インスタンスのハイパーバイザの定義

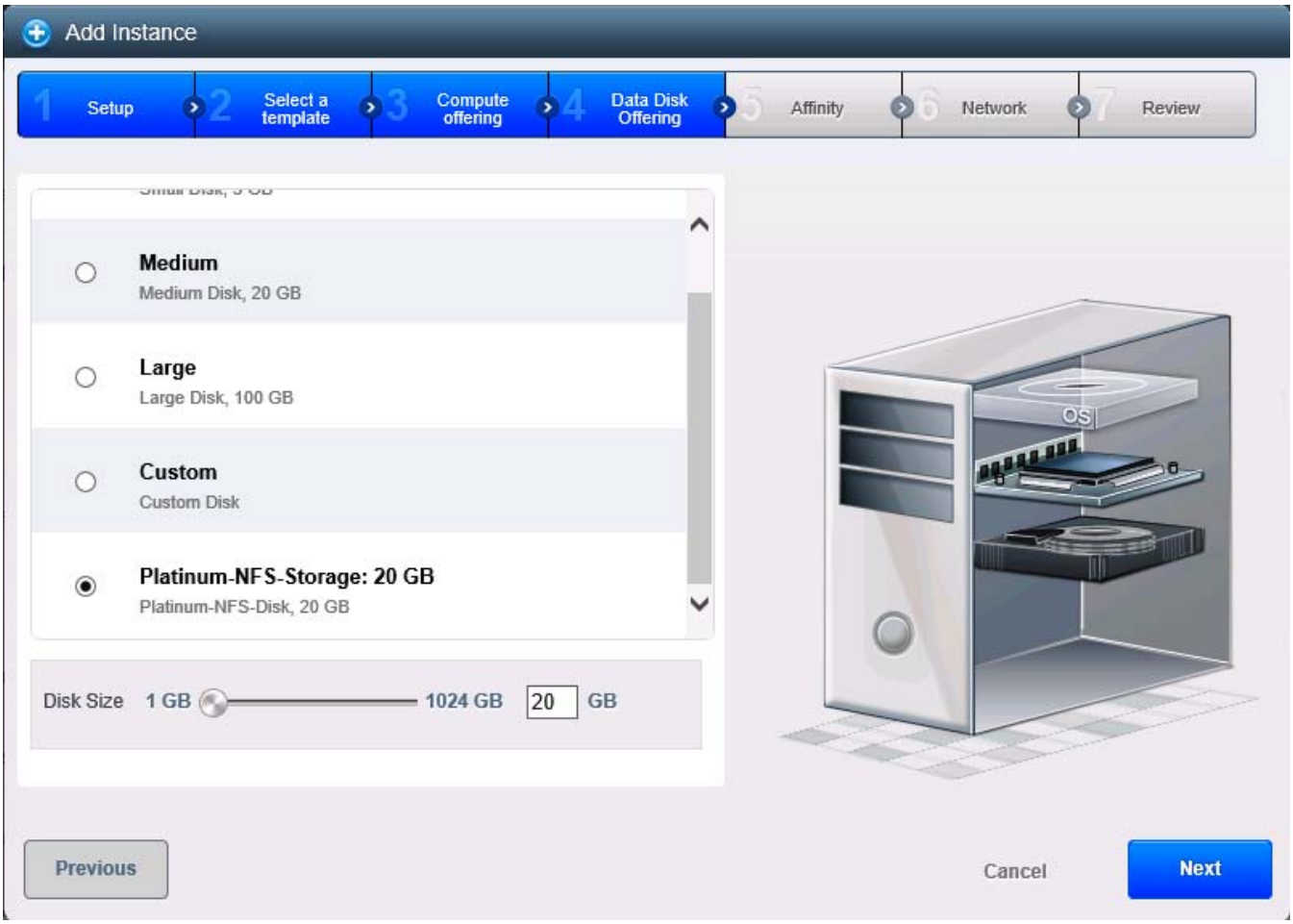


12. [Platinum-Compute] を選択します。
13. [Next] をクリックします。

図 227　　インスタンスのコンピュート オファリングの定義

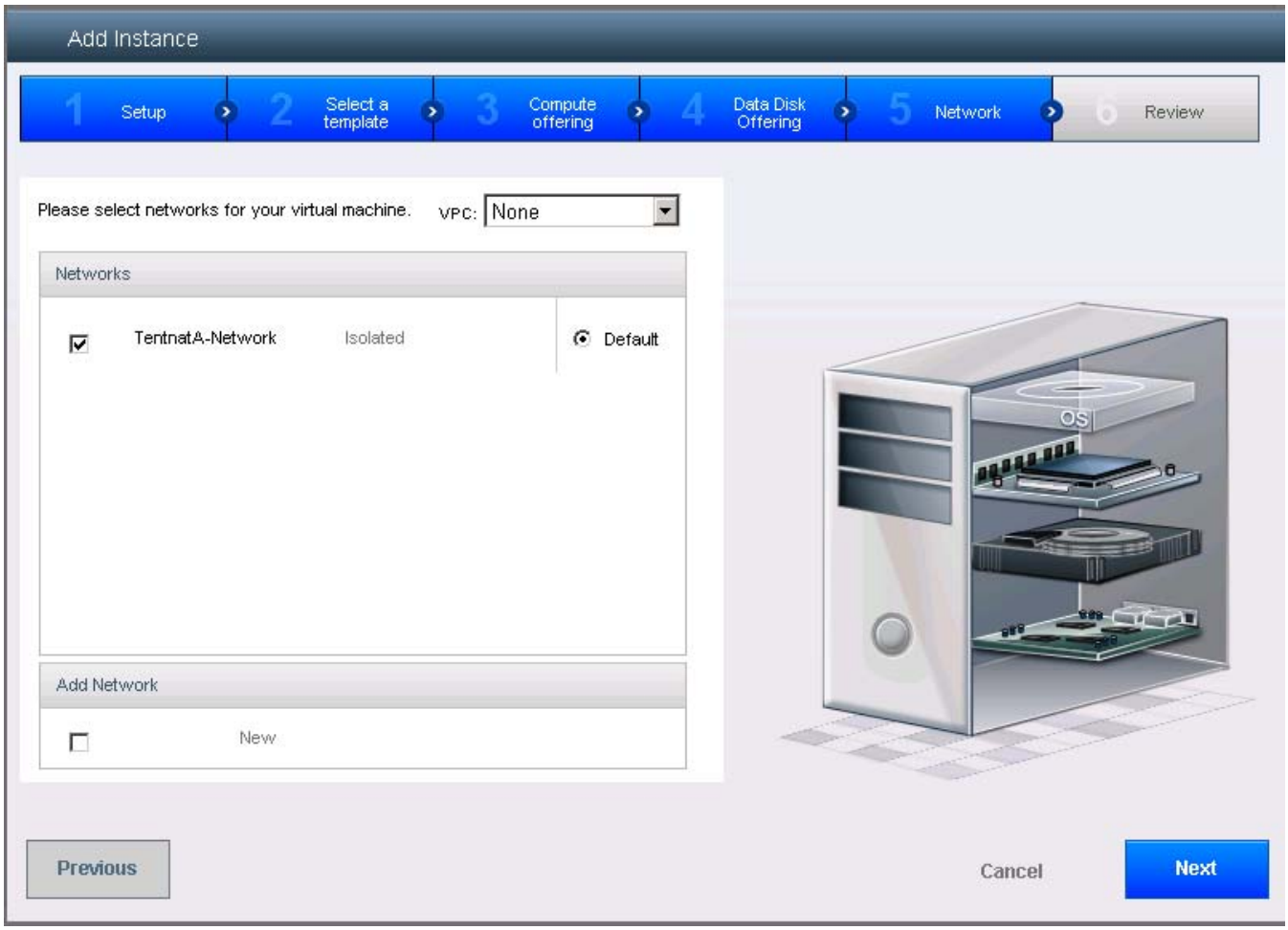
14. [Platinum-NFS-Storage-Disk] を選択します。
15. [Disk Size] フィールドに 20 GB の値を入力します。
16. [Next] をクリックします。

図 228　　ディスク オファリングとサイズの選択



17. [Network] で、[TdenantA-Network] および [Default] チェックボックスをオンにします。
18. [Next] をクリックします。

図 229　　仮想マシンのネットワークの選択



19. VM の [Name] フィールドに TenantA-Platinum-VM1 と入力します。
20. [Launch VM] をクリックします。

図 230　　仮想インスタンス情報の確認

オペレーティング システムのインストール

この項では、データをホストするマルチテナントに専用のコンピューティング、ネットワークおよびストレージ インフラストラクチャをプロビジョニングした後で、仮想マシン上にゲスト オペレーティング システムをインストールする方法について説明します。

ここでは、CloudPlatform を使用して、プラチナ レベルのコンピューティング、ネットワーク、およびストレージのクラウド インフラストラクチャによって新しく作成された TenantA-Platinum-VM1 仮想マシン上に RHEL 6.2 ゲスト オペレーティング システムをインストールします。

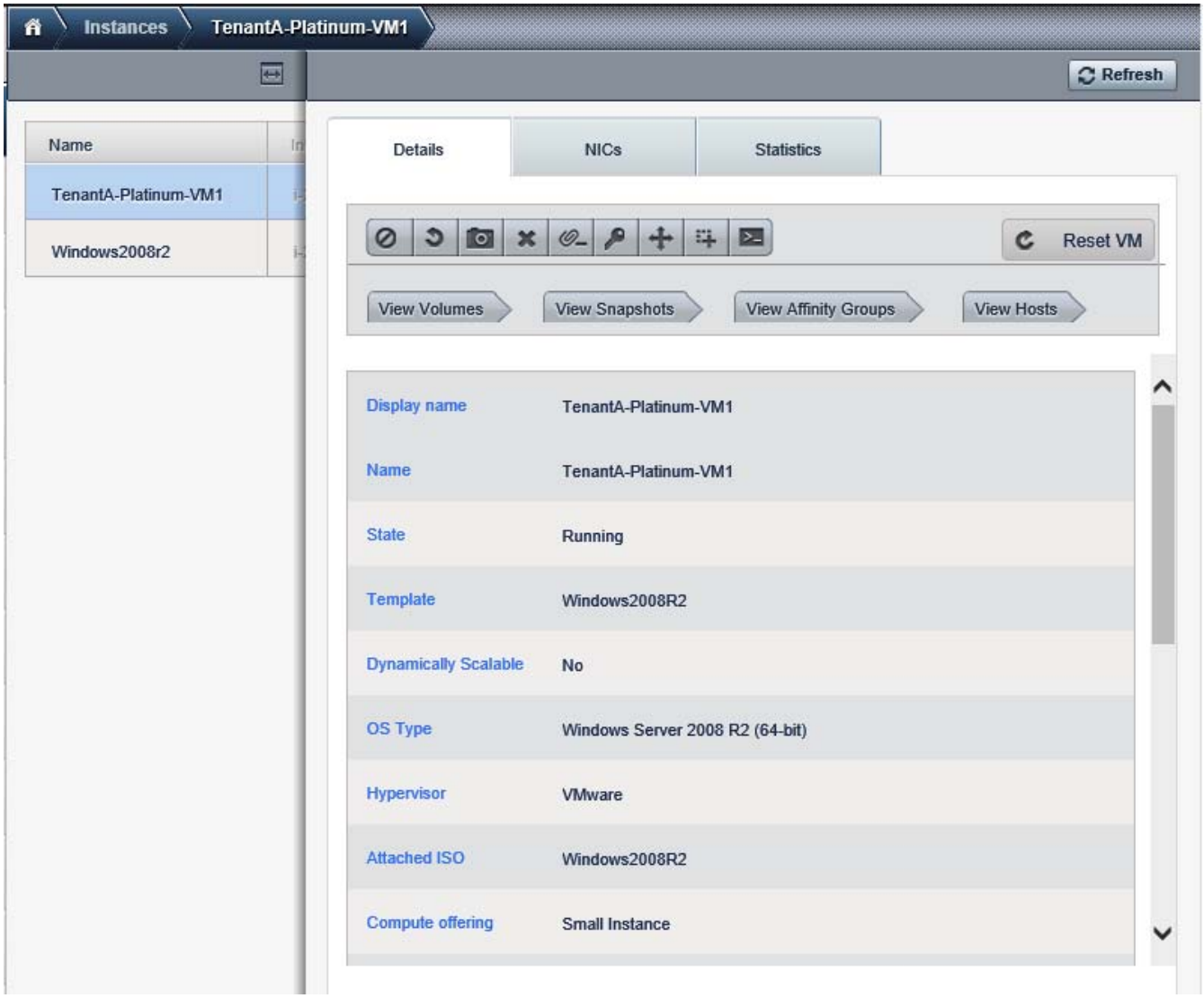
ユーザ資格情報を使用して CloudPlatform にログインして、TenantA ゾーンの ISO イメージを作成します。

Windows OS のインストール

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Instances] タブをクリックします。

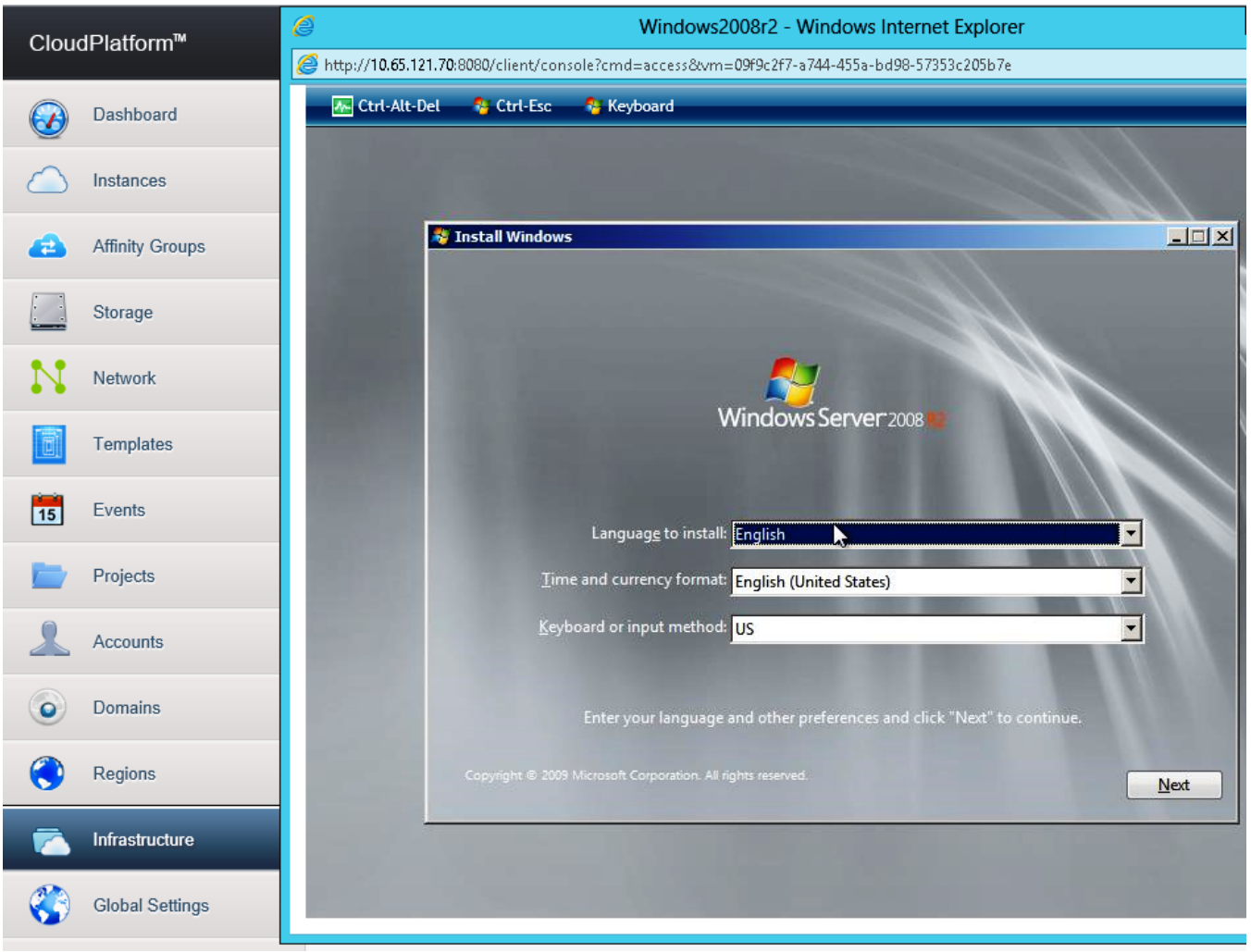
4. [Display name] で [TenantA-Platinum-VM1] をクリックします。
5. [View Console] アイコンをクリックします。

図 231　　VM 詳細の表示



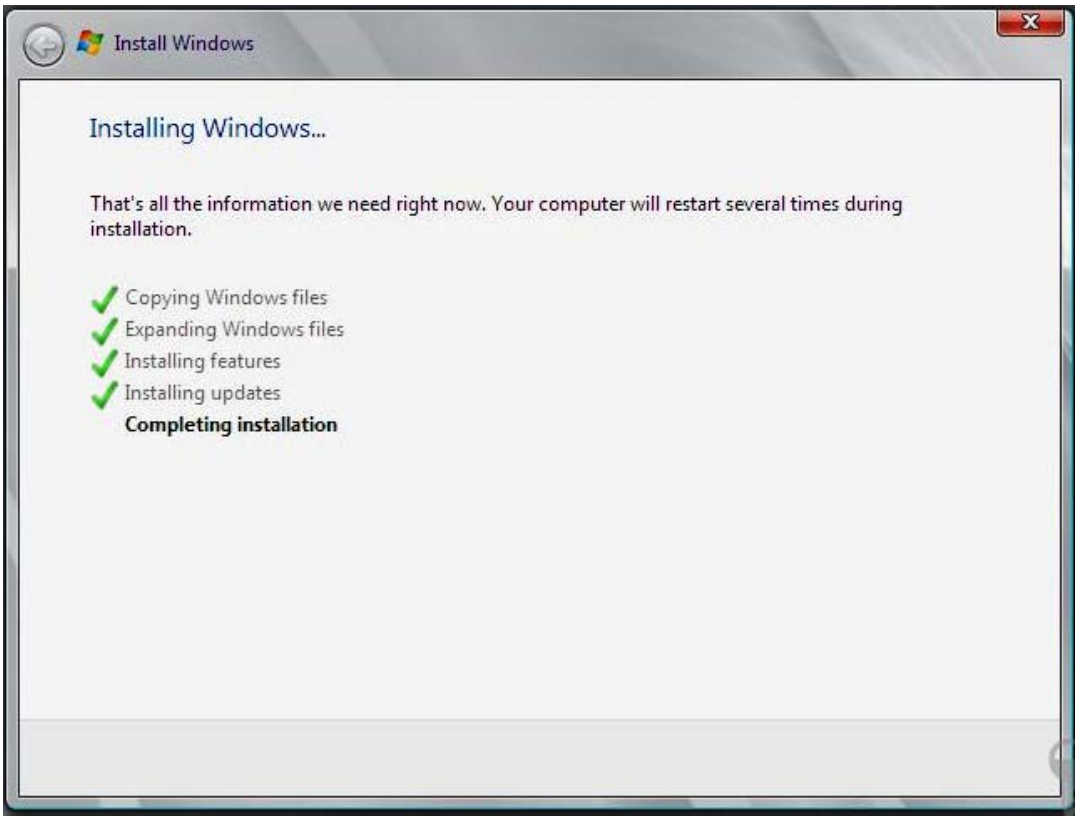
6. [Console] ボタンをクリックして、Windows OS のインストールのために起動します。

図 232　　VM の起動



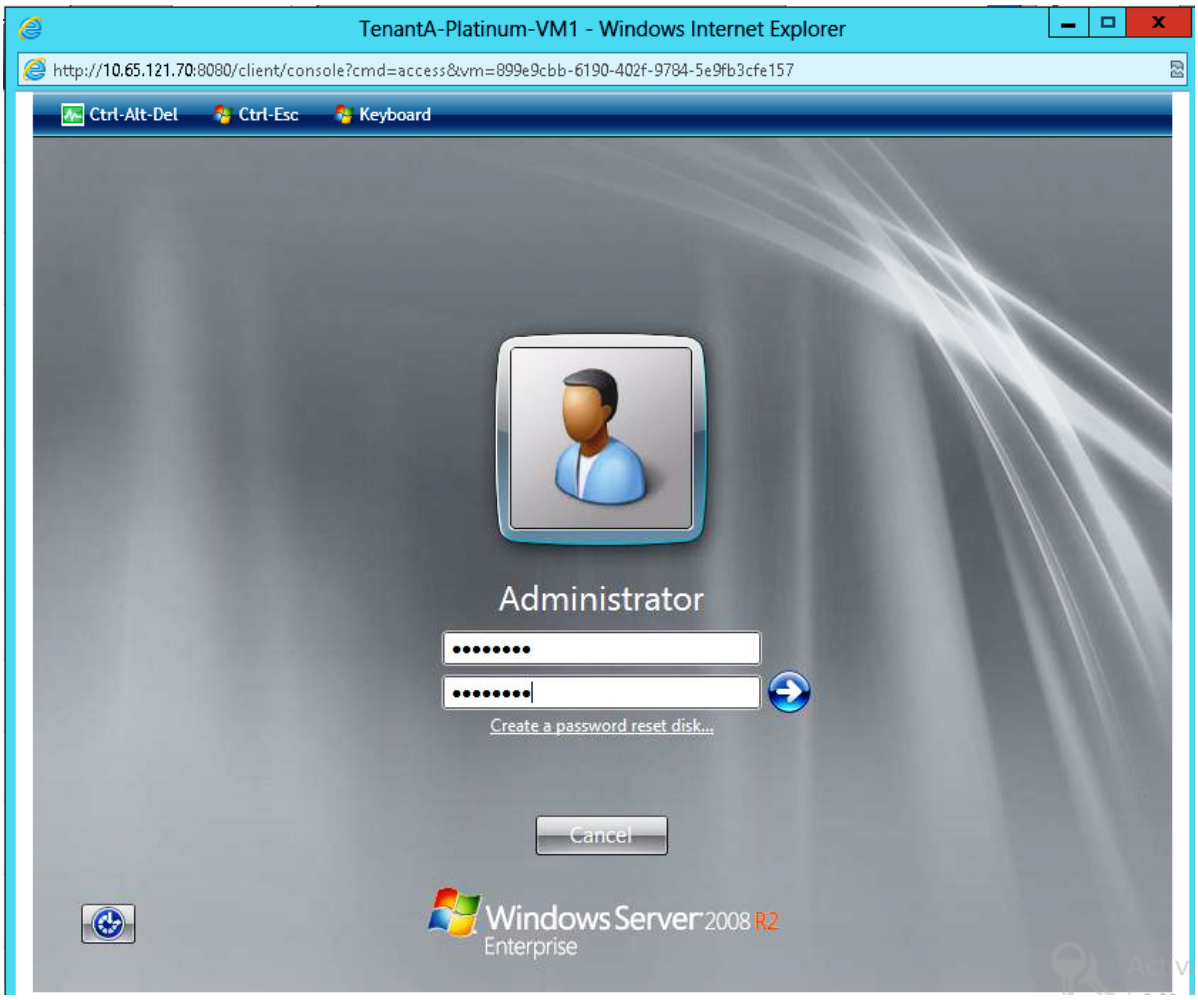
7. [Language to install] で [English] をクリックし、[English (United States)] を選択し、[Keyboard or input method] で [US] を選択します。
8. [Next] ボタンをクリックします。
9. [Install Now] ボタンをクリックします。
10. [Windows Server 2008 R2 Enterprise (Full Installation)] OS タイプを選択します。
11. [Next] ボタンをクリックします。
12. [Accept license] チェックボックスをオンにします。
13. [Next] ボタンをクリックします。
14. [Custom Installation] 方法をクリックします。
15. [Next] ボタンをクリックします。
16. [Disk0] を選択します。
17. [Next] をクリックして OS をインストールします。

図 233　Windows 2008 R2 OS の VM へのインストールの完了



18. パスワード <xxxxx> およびパスワードの確認 <xxxxx> を入力します。

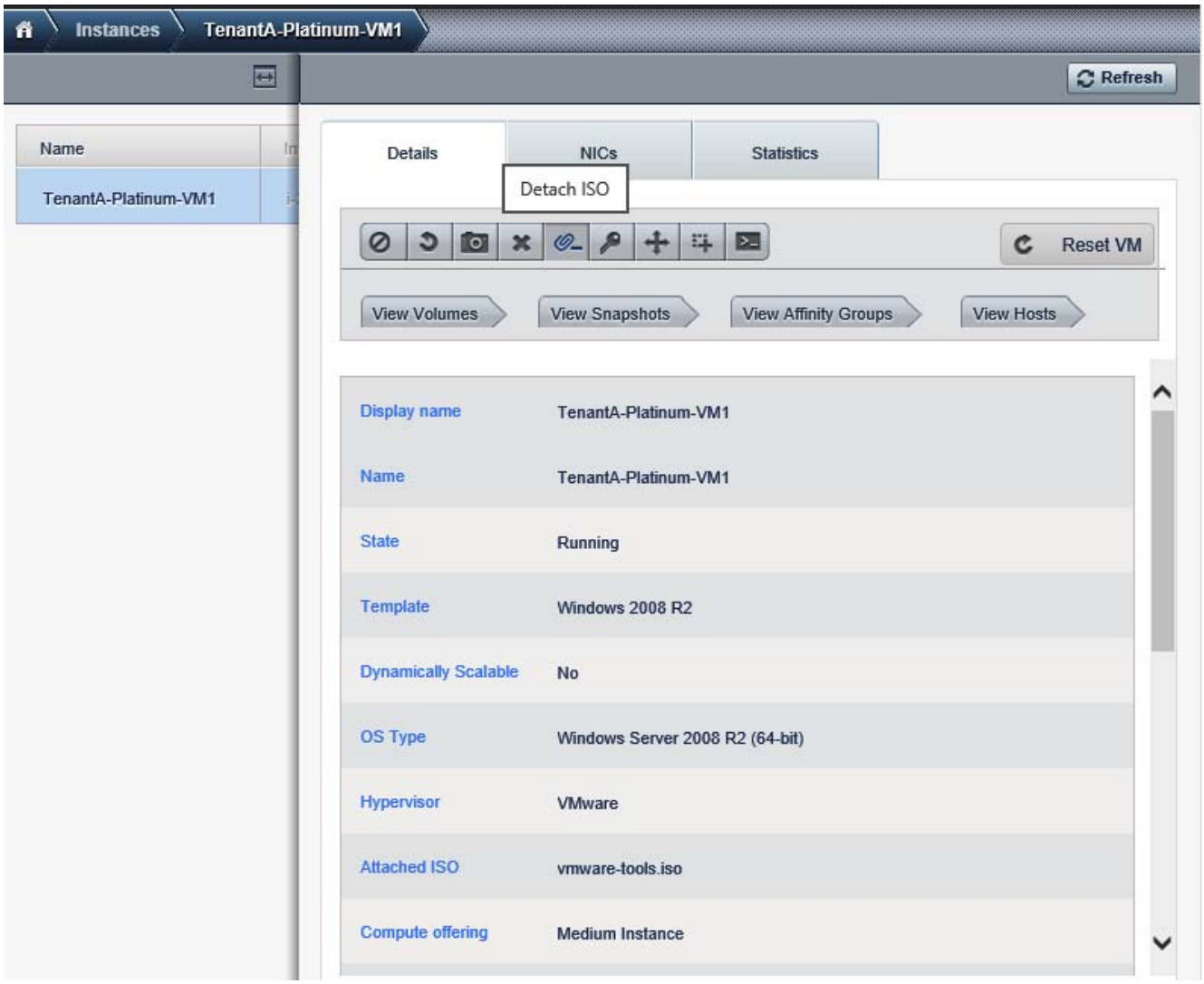
図 234　　VM へのログイン



TenantA-Platinum-VM1 での ISO の解除

1. [Instance] タブをクリックします。
2. [Detach ISO] アイコンをクリックします。

図 235　　ISO イメージの解除



3. 確認ウィンドウで、[Yes] をクリックします。

VM の設定

この項では、ESXi PV ドライバを使用してパブリック ネットワークにアクセスし、外部データ ディスクをプロビジョニングして、テナントにホストするデータ情報を格納するための、仮想マシン クラウド ネットワーク アドレス変換（NAT）ついて説明します。

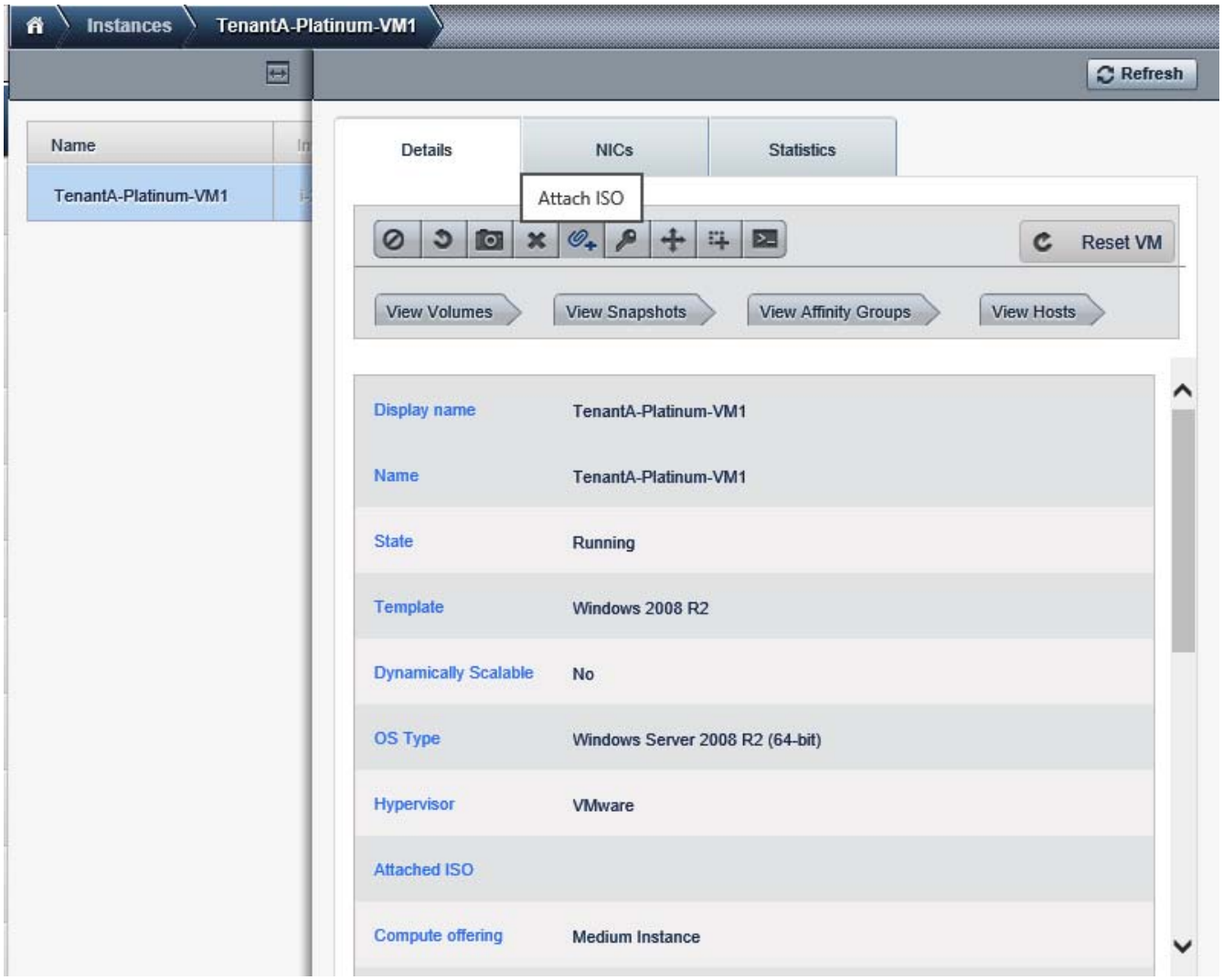
ここでは、CloudPlatform を使用して ESXi PV ドライバをインストールし、データ ディスクをプロビジョニングし、新しく作成された仮想マシン TenantA-Platinum-VM1 にアタッチし、次にパブリック アクセスから仮想マシンにアクセスするためにソース NAT を設定します。

ユーザ資格情報を使用して CloudPlatform にログインして、TenantA ゾーンの仮想マシンに ESXi PV ドライバをインストールします。

ESXi PV ドライバのインストール

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Instances] タブをクリックします。
4. [Attach ISO] アイコンをクリックします。

図 236　　ISO のアタッチ

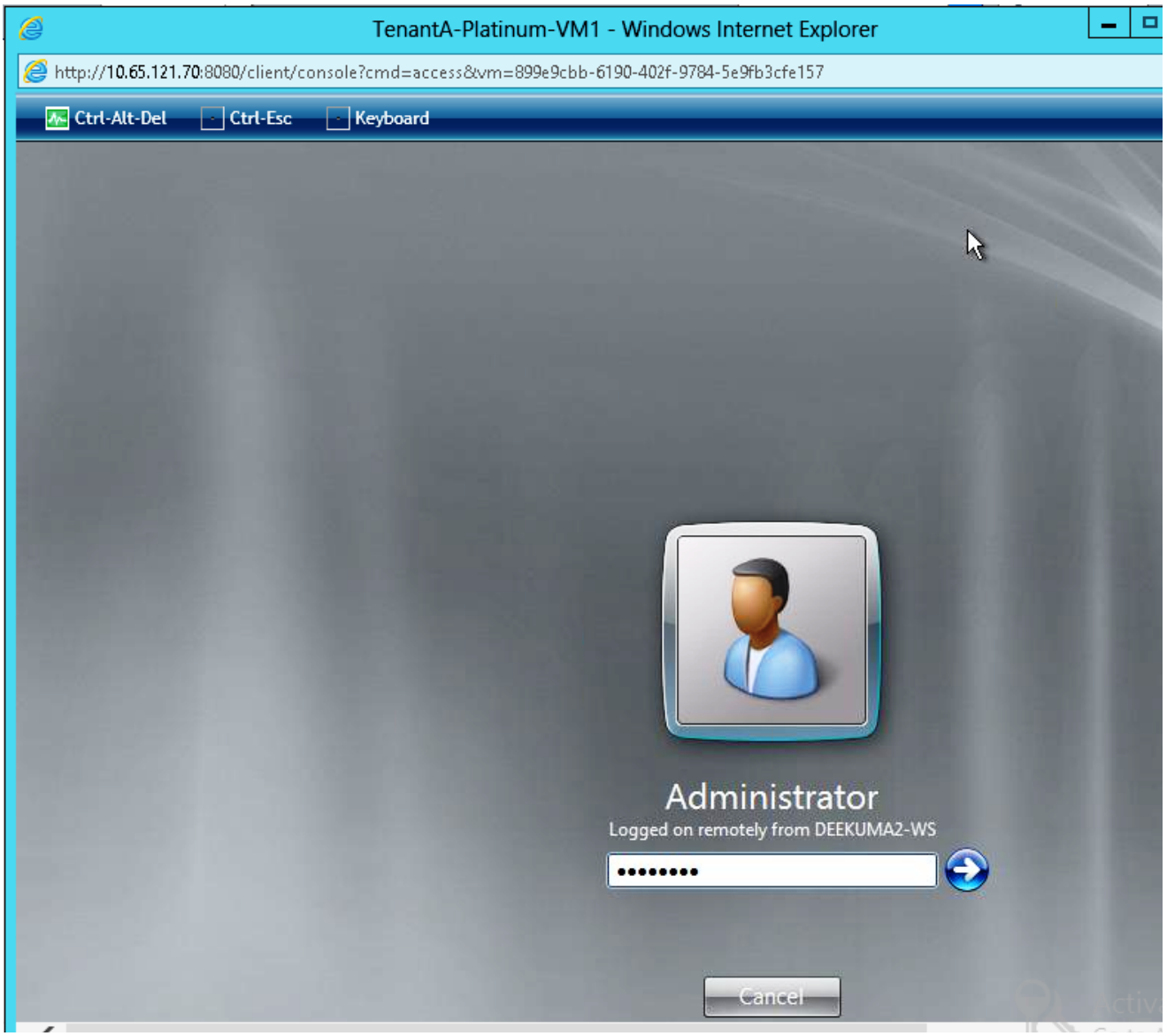


5. [ISO] リスト ボックスから [VMware Tools Installer ISO] を選択します。
6. [OK] をクリックします。

図 237　　ISO の選択

7. VM CONSOLE を起動し、<TenantA-Platinum-VM1> にログインします。
8. ユーザ名 <Root> およびパスワード <XXXXXX> を入力します。

図 238　　VM へのログイン



9. [Run setup64.exe installer] をクリックします。
10. [Next] をクリックします。
11. [Complete] オプション ボタンをクリックします。
12. [Install] をクリックします。
13. [Finish] をクリックします。
14. [Yes] をクリックしてリブートします。

ユーザ資格情報を使用して CloudPlatform にログインして、TenantA ゾーンの VM NAT を設定します。

パブリック アクセスから VM にアクセスするための NAT のソーシング

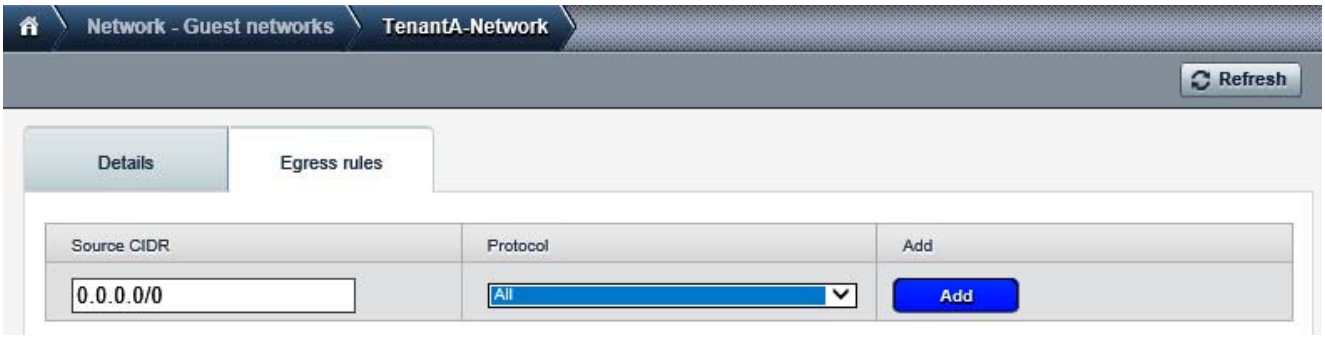
1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。

2. [Login] をクリックします。
3. [Network] タブをクリックします。

図 239　　ゲスト ネットワークの表示

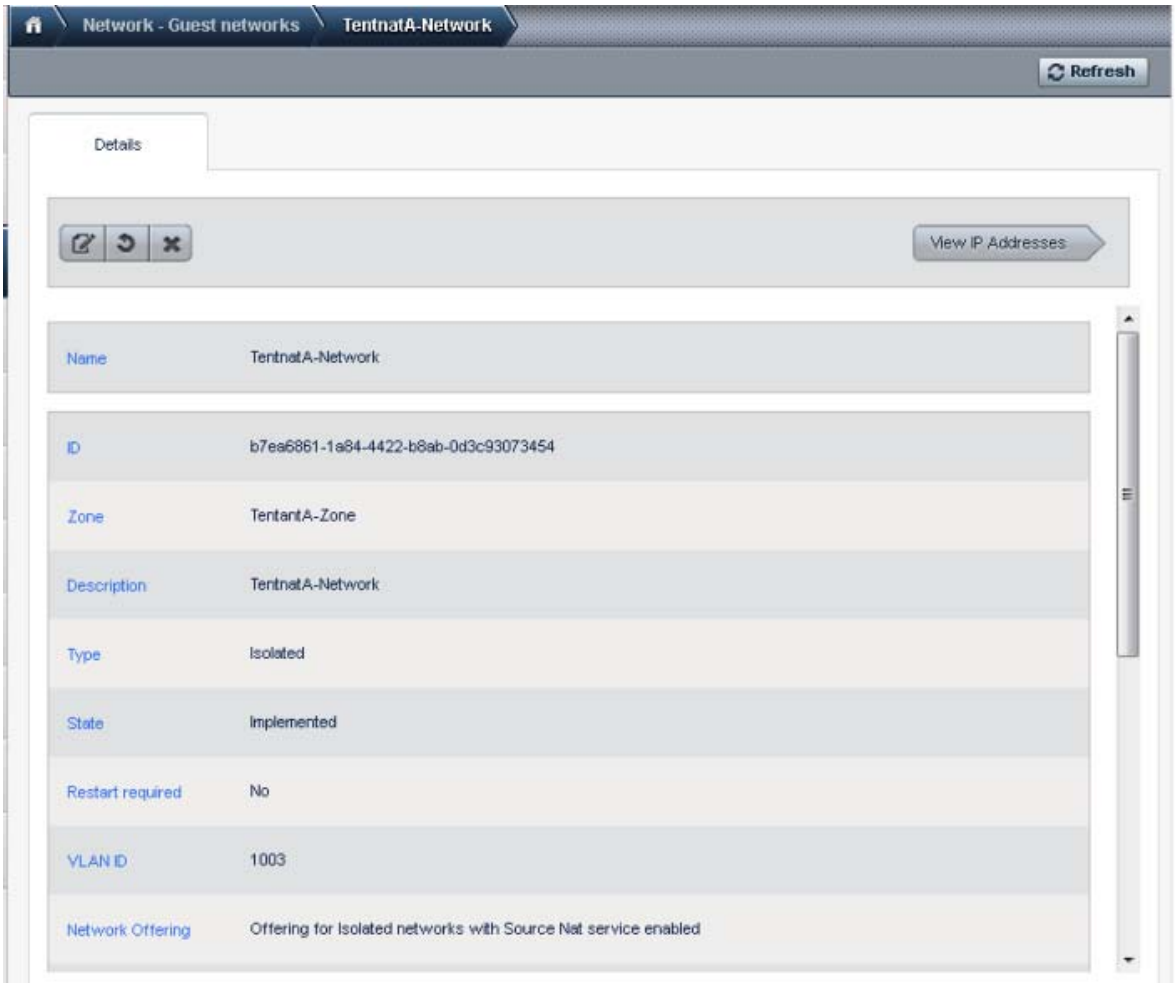
4. [TenantA-Network] タブをクリックします。
5. [Egress rules] をクリックします。
6. [Source CIDR] で 0.0.0.0/0 と入力し、[Protocol] リスト ボックスで [All] を選択します。
7. [ADD] ボタンをクリックします。

図 240　　ゲスト ネットワークの出力規則の表示



8. [TenantA-Network] タブをクリックします。
9. [View IP Address] をクリックします。

図 241　　ネットワーク詳細の表示

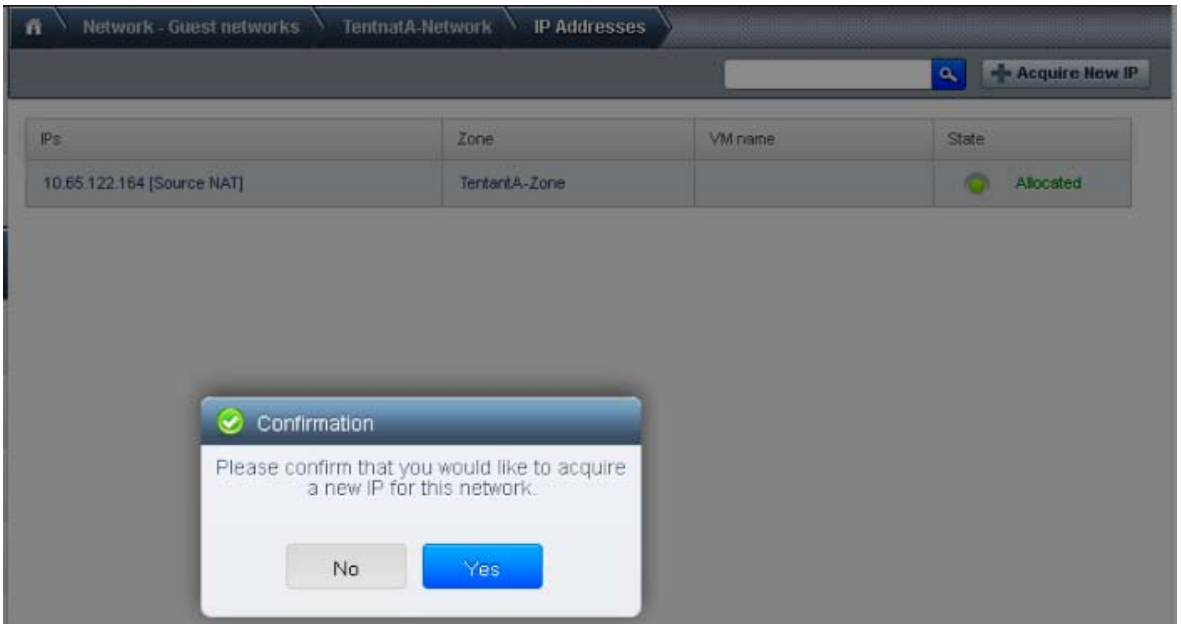


10. [+Acquire New IP] ボタンをクリックします。

図 242　　ゲスト ネットワークの IP アドレスの表示

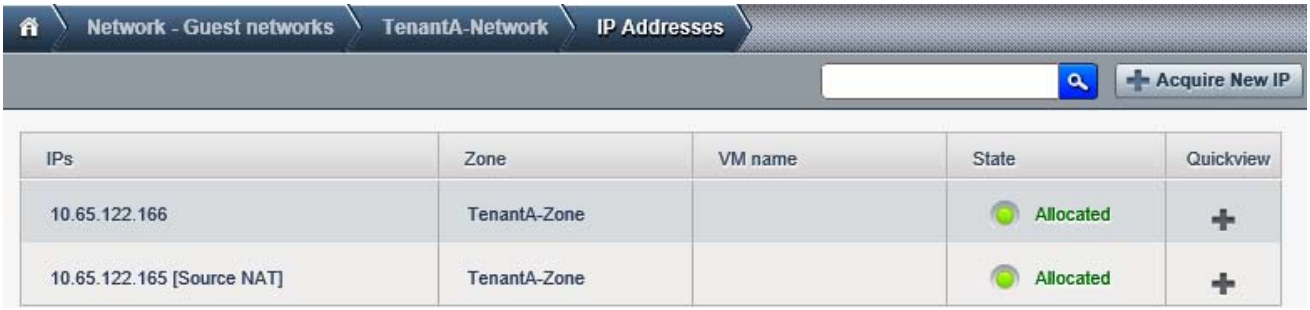
11. [Yes] ボタンをクリックします。

図 243　　IP アドレスの確認



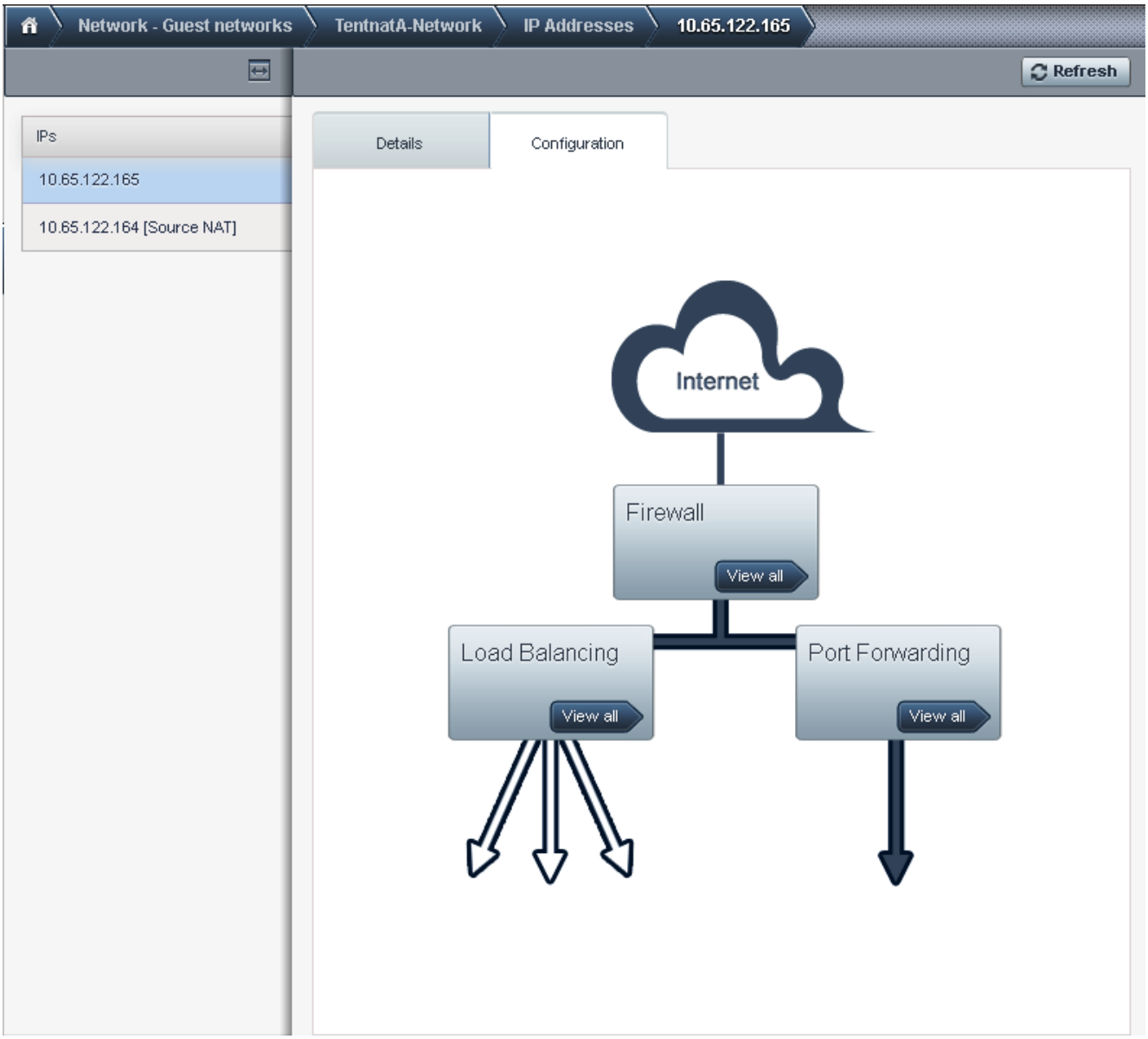
12. IP アドレス <10.65.122.166> がパブリック IP アドレスとして割り当てられます。

図 244　　IP アドレスの表示



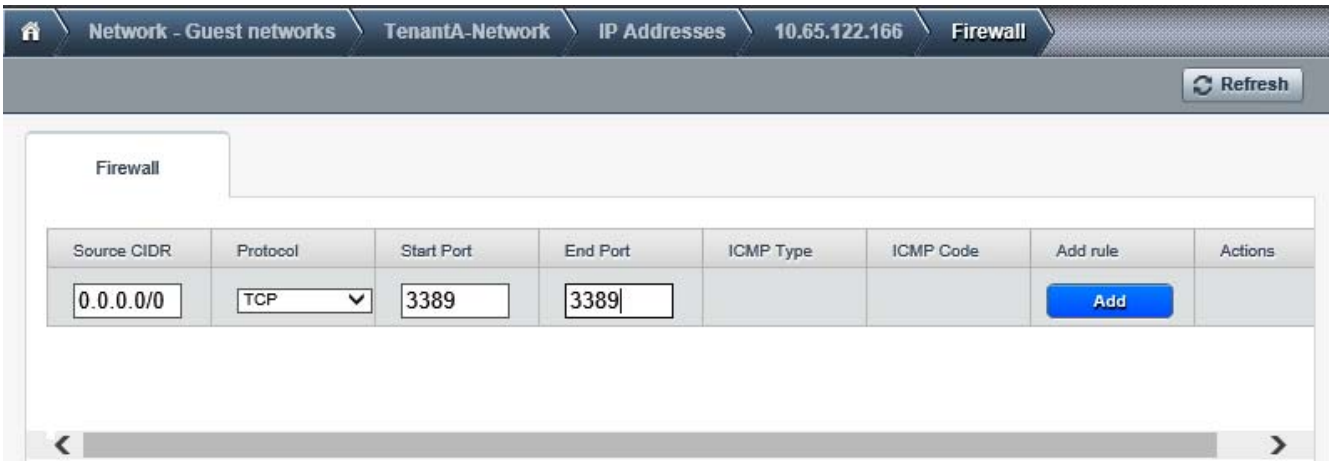
13. IP アドレス <10.65.122.166> をクリックします。
14. [Configuration] タブをクリックします。

図 245　　構成フロー図の表示



15. [Firewall] タブをクリックします。
16. [Source CIDR] フィールドに <0.0.0.0/0> と入力します。
17. [TCP] プロトコル リスト値を選択します。
18. [Start Port] フィールドに 3389（RDP）と入力します。
19. [End Port] フィールドに 3389（RDP）と入力します。
20. [ADD] ボタンをクリックします。

図 246　ファイアウォール設定の定義



21. フロー図で [Port Forwarding] をクリックします。

図 247　ポート フォワーディング オプションの選択

22. [Private Port] フィールドに 3389 と入力します。
23. [Public Port] フィールドに 3389 と入力します。
24. [Protocol] リスト ボックスで [TCP] を選択します。

図 248　ポート フォワーディング設定の定義

25. [Add] をクリックします。
26. [TenantA-Platinum-VM1] の [Select] オプション ボタンをクリックします。
27. [Apply] をクリックします。

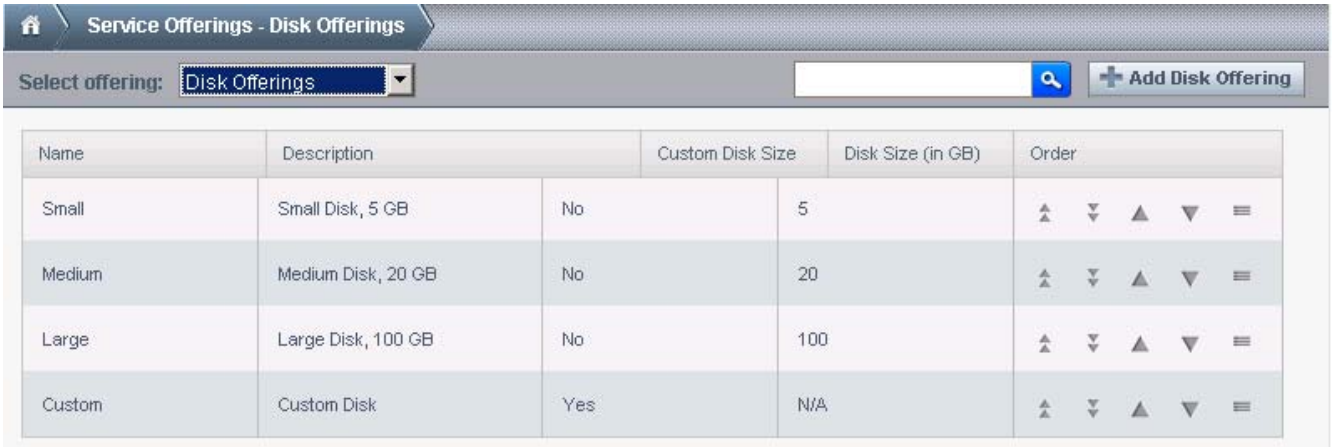
図 249　　VM の追加

TenantA ゾーンの VM データ ディスクを設定するには、CloudPlatform にログインします。

TenantA-Platinum-VM1 へのデータ ディスクのアタッチ

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Service Offerings] タブをクリックします。
4. [Select Offering] リスト ボックスで [Disk Offering g] を選択します。

図 250　　ディスク オファリングの表示



5. [Name] フィールドに Platinum-NFS-Storage と入力します。
6. [Description] フィールドに Platinum-NFS-Disk と入力します。
7. [Storage Type] リスト ボックスで [shared] を選択します。
8. [Custom Tags] チェックボックスをオンにします。
9. [QoS Type] では選択しません。
10. [Storage Tags] に Platinum-NFS-Storage と入力します。
11. [Public] チェックボックスをオンにします。
12. [OK] をクリックします。

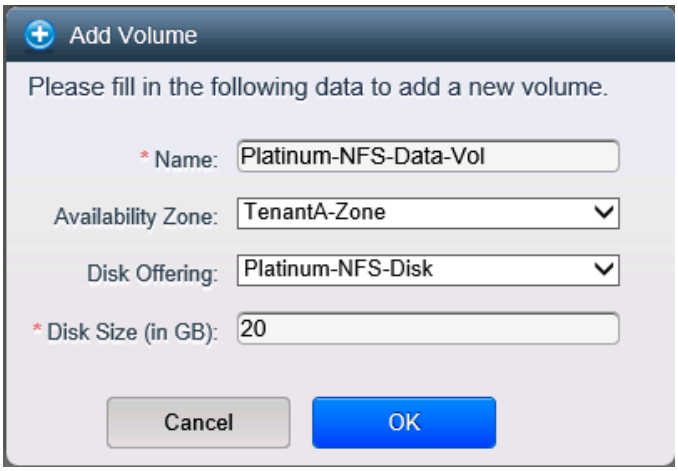
図 251　　ディスク オファリング情報の定義

13. [Storage] タブをクリックします。
14. [Select view] リスト ボックスで [Volumes] を選択します。

図 252　　ストレージ ボリュームの表示

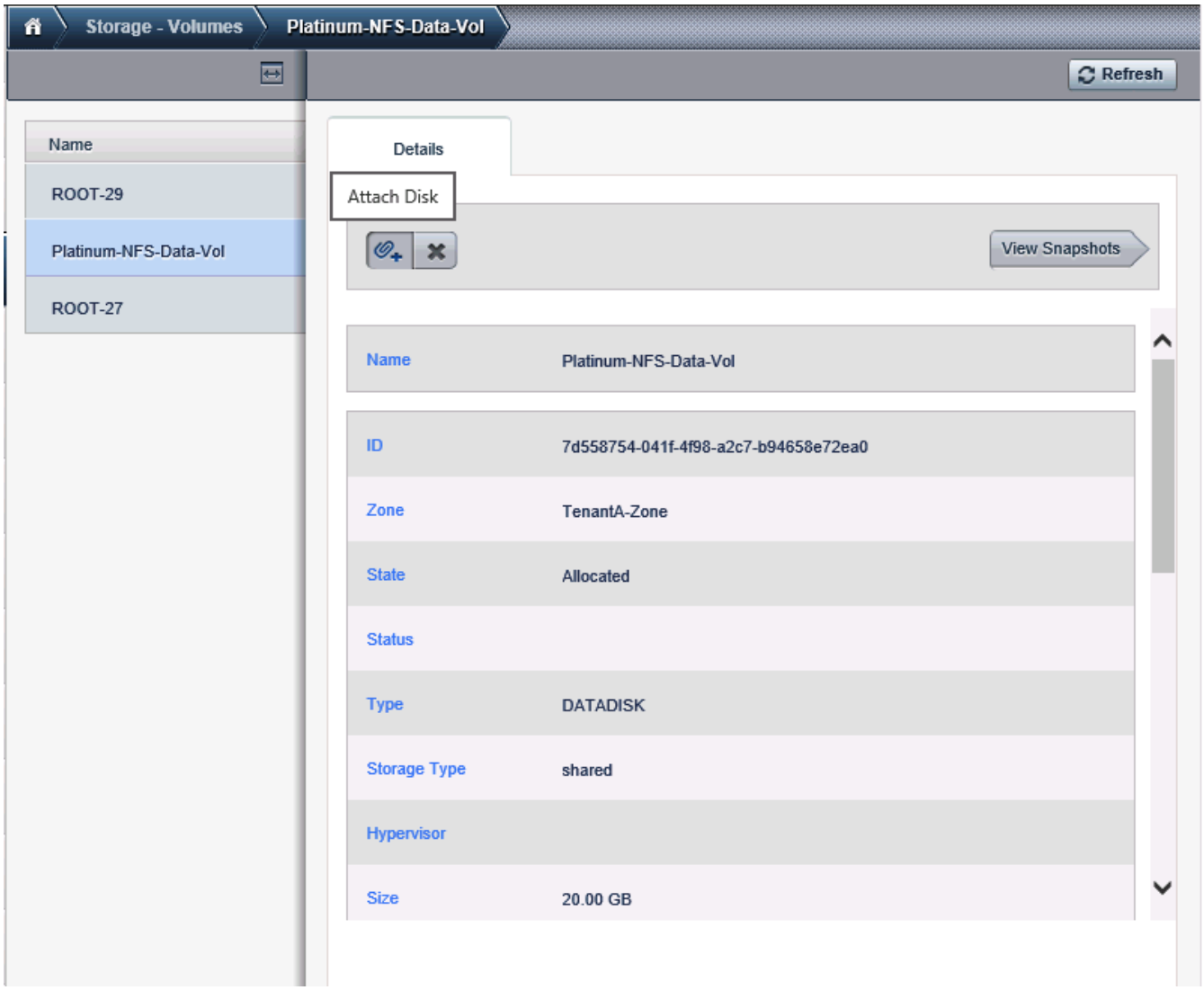
15. [Add Volume] ボタンをクリックします。
16. [Select view] リスト ボックスで [Volumes] を選択します。
17. Platinum-NFS-Data-Vol と入力します。
18. [Availability Zone] リスト ボックスで [<TenantA-Zone>] を選択します。
19. [Disk Offering] リスト ボックスで [Platinum-NFS-Disk] を選択します。
20. [Disk Size（in GB）] フィールドに 20 を入力します。

図 253　　ボリューム情報の定義



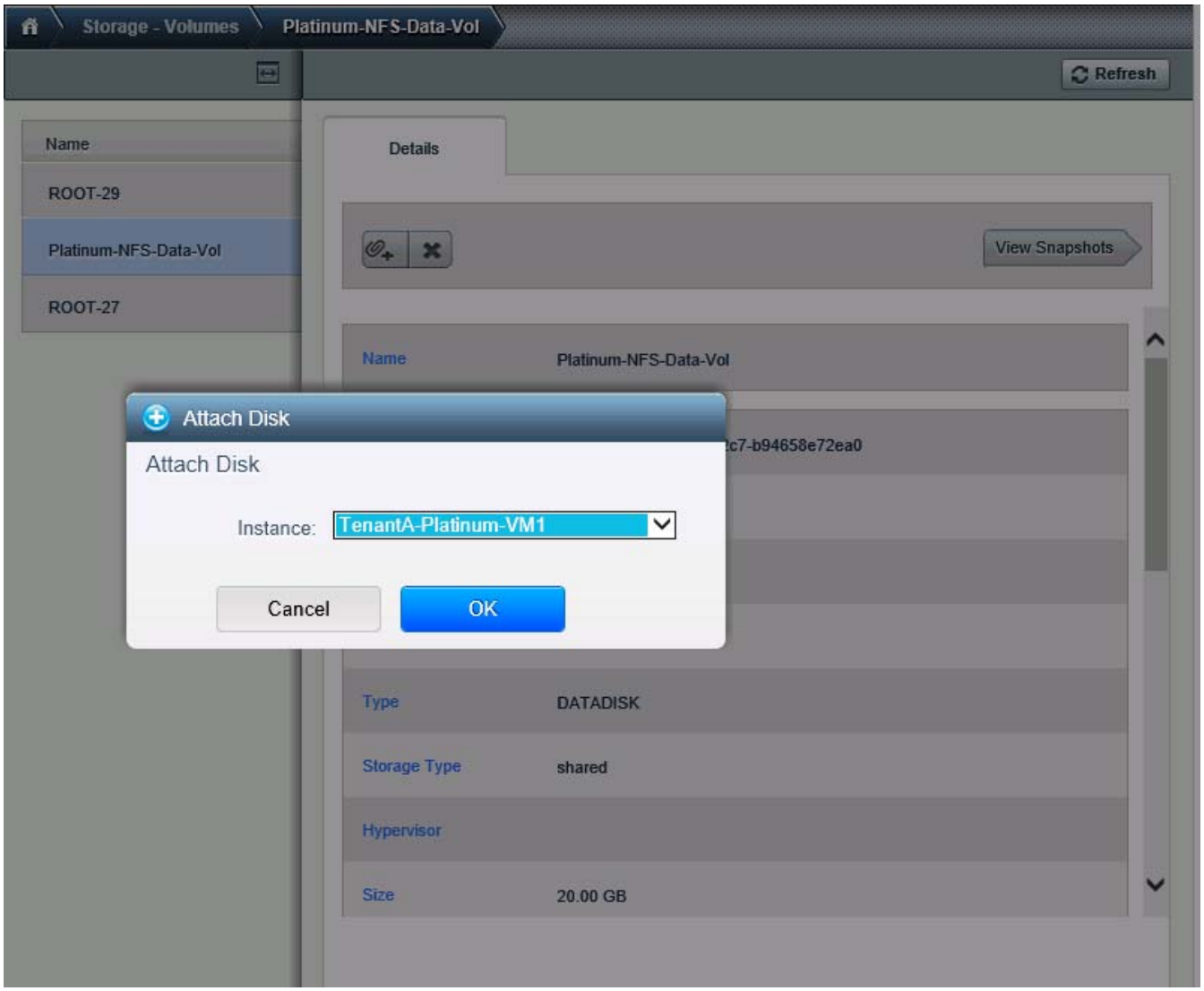
21. [<Platinum-NFS-Data-VOL>] をクリックします。
22. [Attach Disk] アイコンをクリックします。

図 254　　データ ディスクの詳細の表示



23. [Instance] リスト ボックスで [<TenantA-Platinum-VM1>] を選択します。
24. [OK] をクリックします。

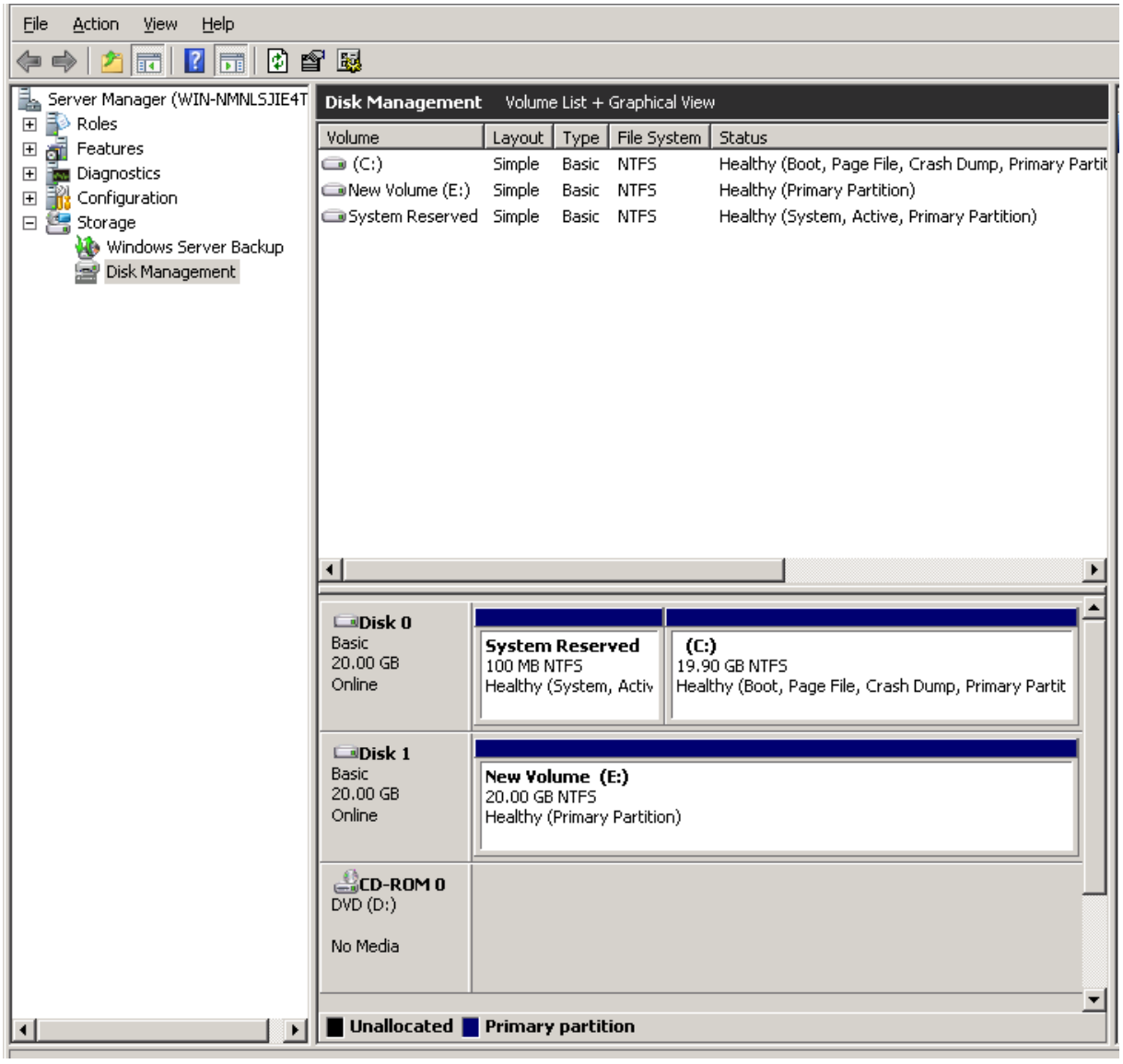
図 255　　ディスクへのインスタンスのアタッチ



25. リモートで TenantA-Platinum-VM1 <10.65.122.166> に接続します（IP 取得）。
26. <administrator> とパスワード <xxxxxxxxx> を使用してログインします。
27. [Server Manager] を開きます。
28. [Storage Under Disk Management] をクリックします。
29. [Disk 1 Initilize and Online Disk] を右クリックします。
30. [Create simple volume] を選択します。
31. [Next] をクリックします。
32. 割り当てるドライブ（E）を選択します。
33. [Next] をクリックします。
34. デフォルトのオプションを選択します。
35. [Next] をクリックします。

36. [Finish] をクリックします。

図 256　　アタッチされたディスクの情報を表示する Windows VM



VM のバックアップおよび復元

この項では、クラウドで提供されるサービス レベルに基づいて仮想マシンのバックアップおよび復元ポリシーを設定する方法について説明します。CloudPlatform では、ディスク ボリュームのスナップショットをとることによって VM OS およびデータ ディスクのバックアップを実行します。スナップショットは、OS およびデータ情報が保存されている仮想マシン ディスクを、特定の時点でキャプチャしたものです。

- バックアップの方法

VM のバックアップを行うには 2 つの方法があります。最初の方法は手動で、クラウド管理者はディスク ボリュームのバックアップを手動で実行する必要があります。2 番目の方法は自動で、定期的なスナップショット ポリシーを設定して、時間、日、週および月の単位および保持数に基づいてバックアップ時間をスケジュールすることができます。要件に従って複数のバックアップ ポリシーを定義できます。

- 復元の方法

  スナップショットの復元を実行するには 2 つの方法があります。最初の方法は、スナップショットのボリュームを作成して、スナップショットをディスクの形式でインスタンス VM にアタッチします。2 番目の方法は、テンプレートを作成して、バックアップ VM にアクセスします。

（注） 最初の方法を使用してデータ ディスクのスナップショット復元を作成し、2 番目の方法を使用してルート ディスク（オペレーティング システム）のスナップショット復元を作成することを推奨します。

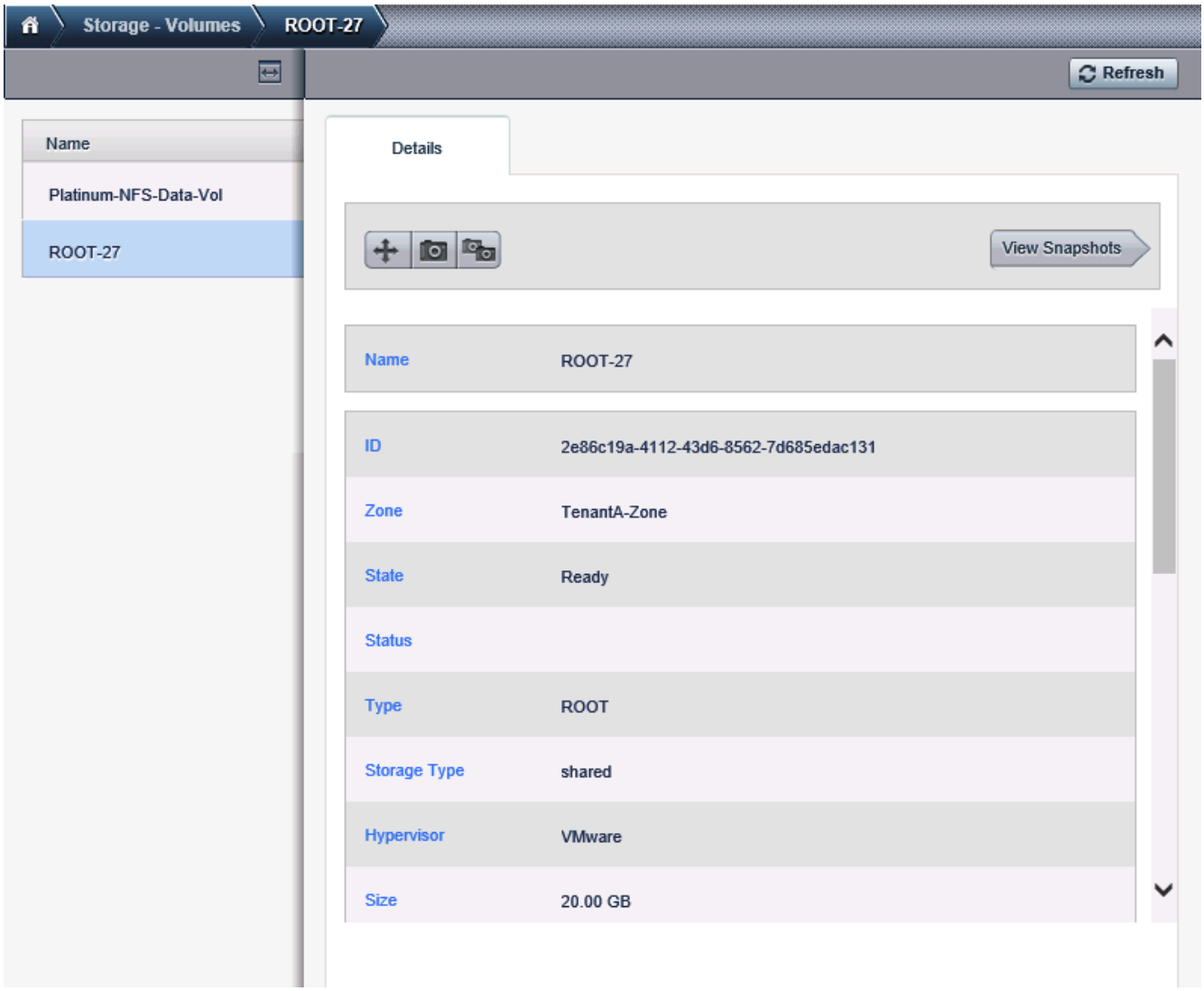
ここでは、CloudPlatform を使用して TenantA-Platinum-VM1 ルートの手動バックアップ、および Platinum-NFS-Data-Vol データ ディスクの自動バックアップを作成し、テンプレートでルート ディスクを、ボリューム方法でデータ ディスクを回復します。

ユーザ資格情報を使用して CloudPlatform にログインして、TenantA ゾーンで TenantA-Platinum-VM1 の手動および自動バックアップを作成します。

手動バックアップ

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Storage] タブをクリックします。

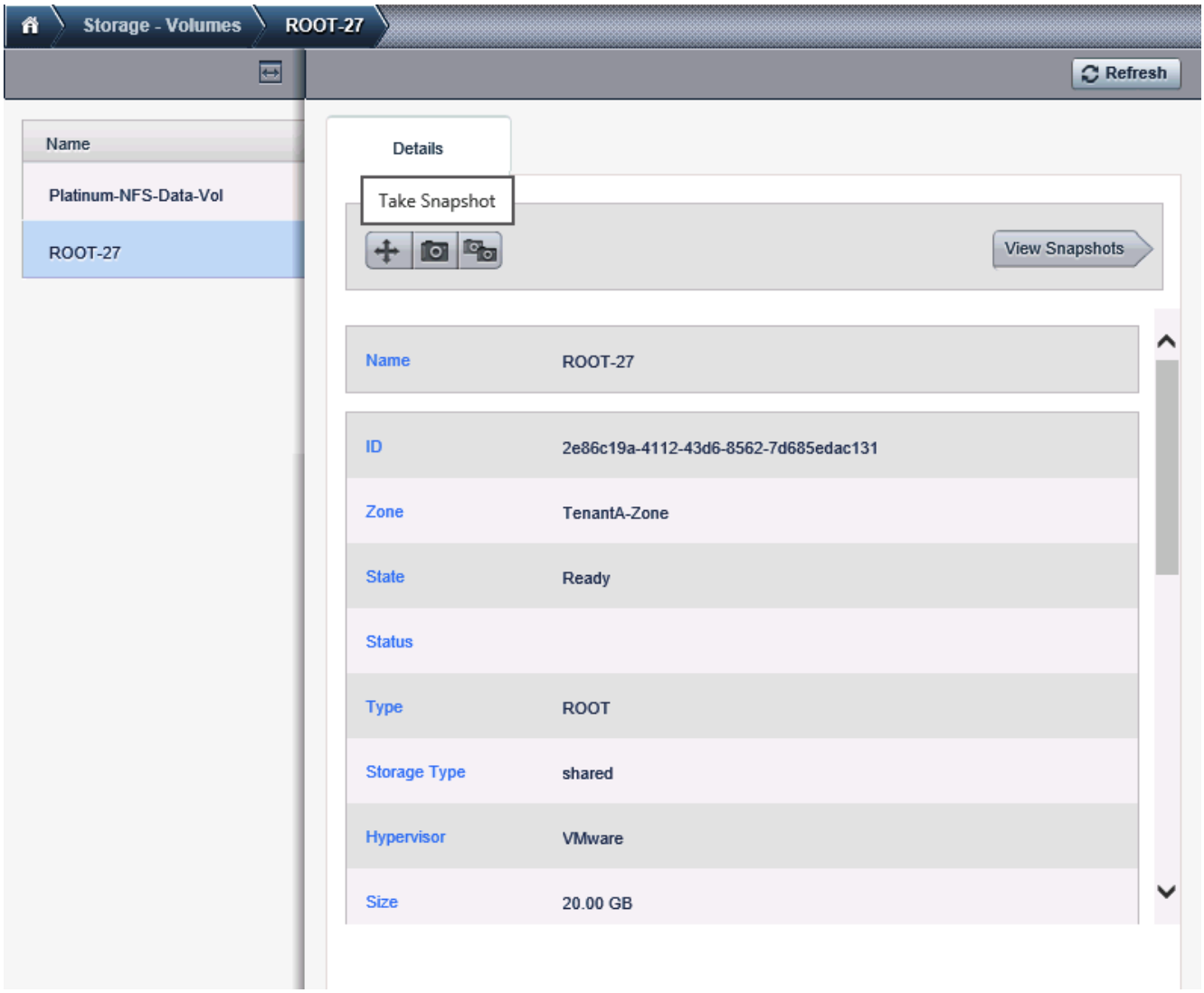
図 257　　ストレージ ボリューム データの表示



4. 右ペインの [Name] で [Root-27] をクリックします。
5. TenantA-Platinum-VM1 ルート ディスク（オペレーティング システム）の手動バックアップを行います。
6. 単一カメラの [Take Snapshot] アイコンをクリックします。

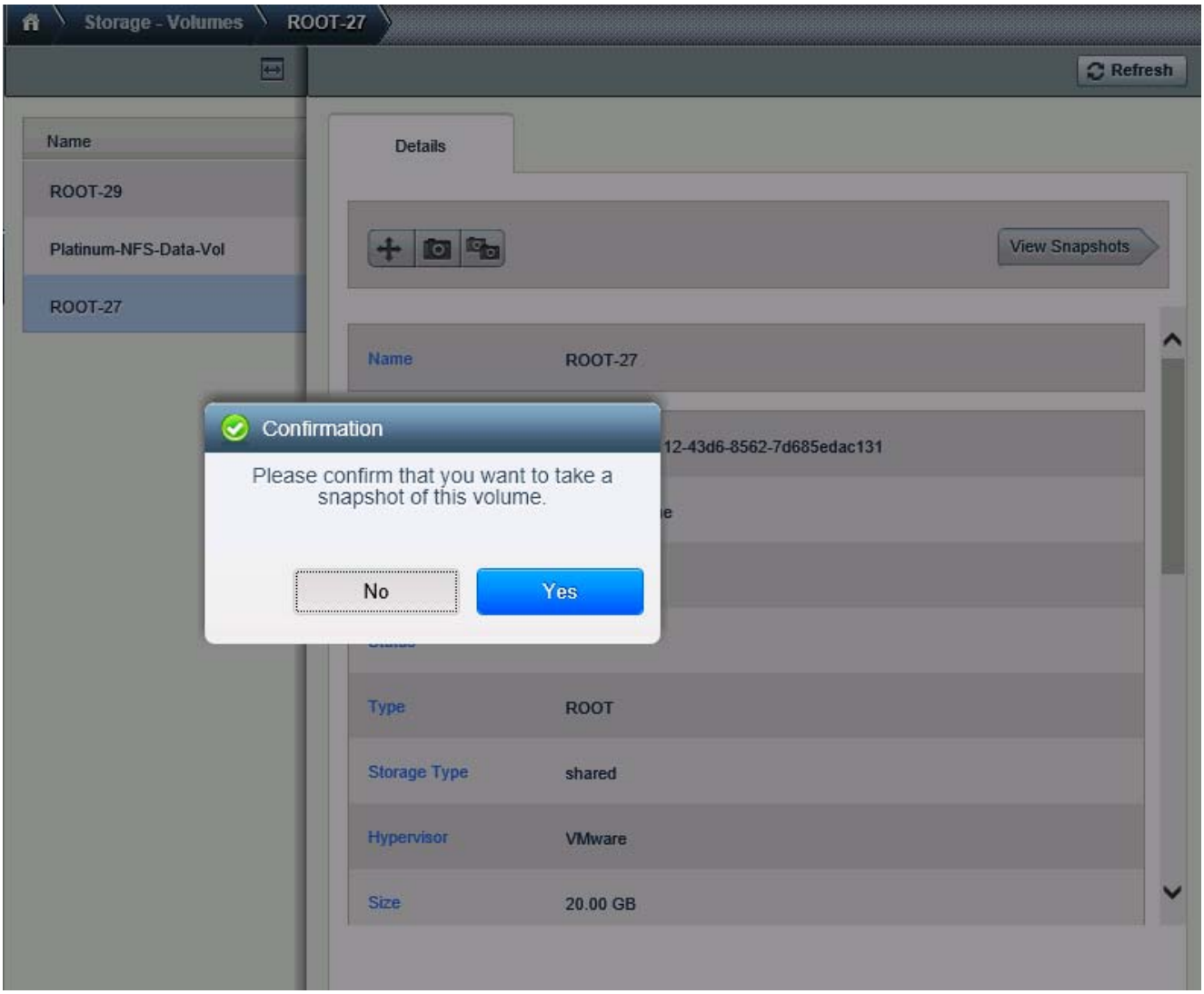
（注）　ESXi ハイパーバイザ ホストで一貫したスナップショットのコピーがとれるように仮想マシンの電源がオフになっていることを確認します。

図 258　　ストレージ ボリュームのスナップショットの表示



7. 確認のために [Yes] をクリックします。

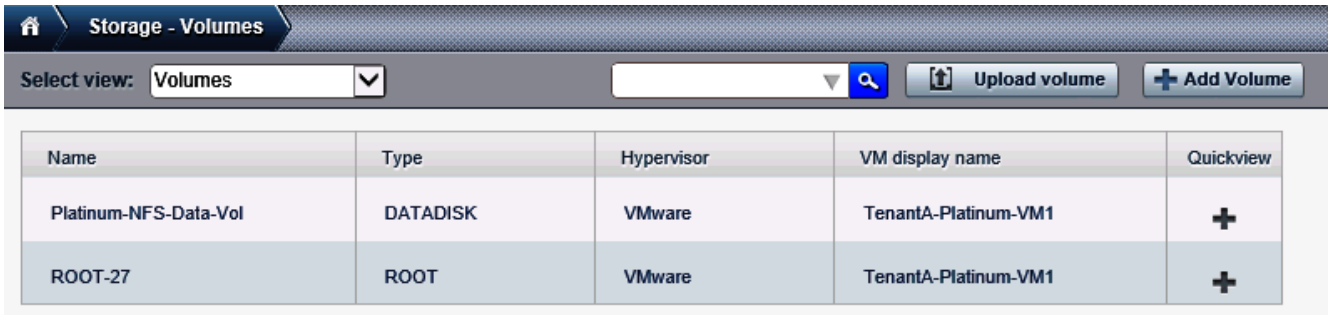
図 259　　スナップショットの取得



自動バックアップ

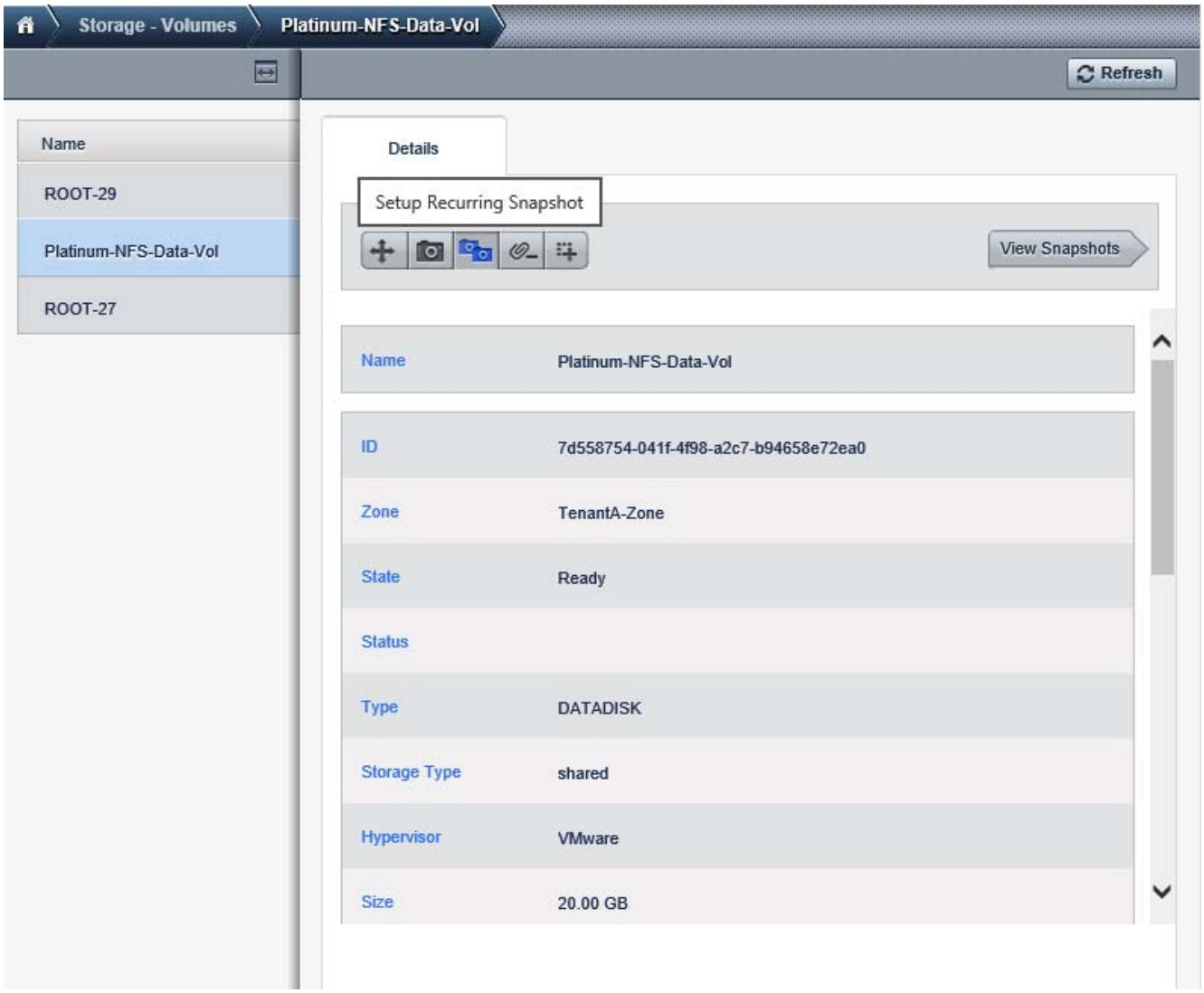
1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Storage] タブをクリックします。

図 260　　ストレージ ボリュームの表示



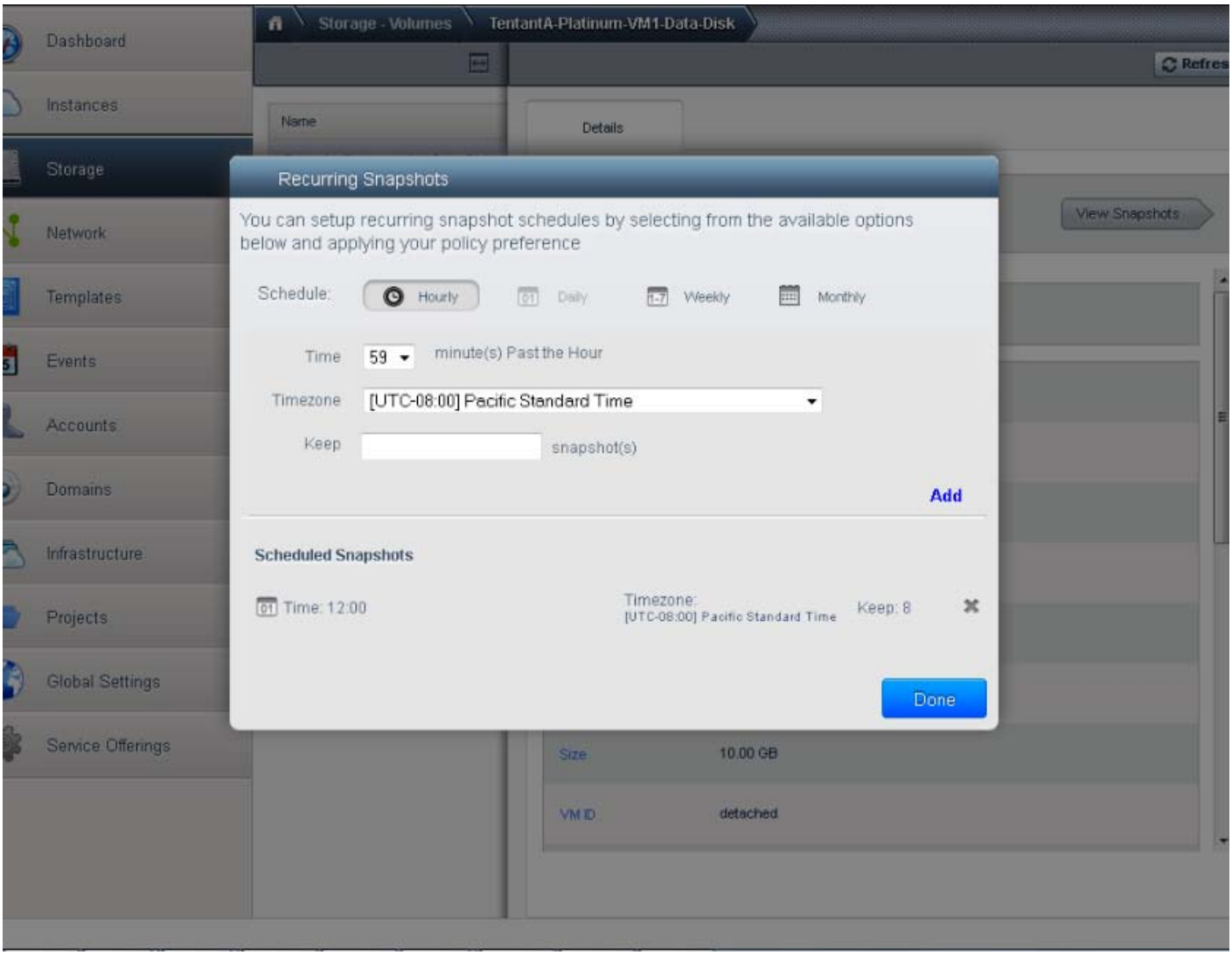
4. 右ペインの [Name] で [Platinum-NFS-Data-Vol] をクリックします。
5. （TenantA-Platinum-VM1 データ ディスクのバックアップは毎日深夜 0 時に実行され、バックアップ データは 2 週間保持されます）。
6. 2 つのカメラの [Recurring Snapshot] アイコンをクリックします。

図 261　　定期的なスナップショット機能のセットアップ



7. [Schedule] フィールドで [Daily] ボタンをクリックします。
8. [Time] リスト ボックスで [12 Hour 00 minutes] と [PM] を選択します。
9. [Timezone] リスト ボックスで [Pacific Standard Time] を選択します。
10. [Keep] フィールドに 8 の値を入力します。
11. [Add] をクリックします。
12. [Done] をクリックします。

図 262　　定期的スナップショットのスケジュールの定義



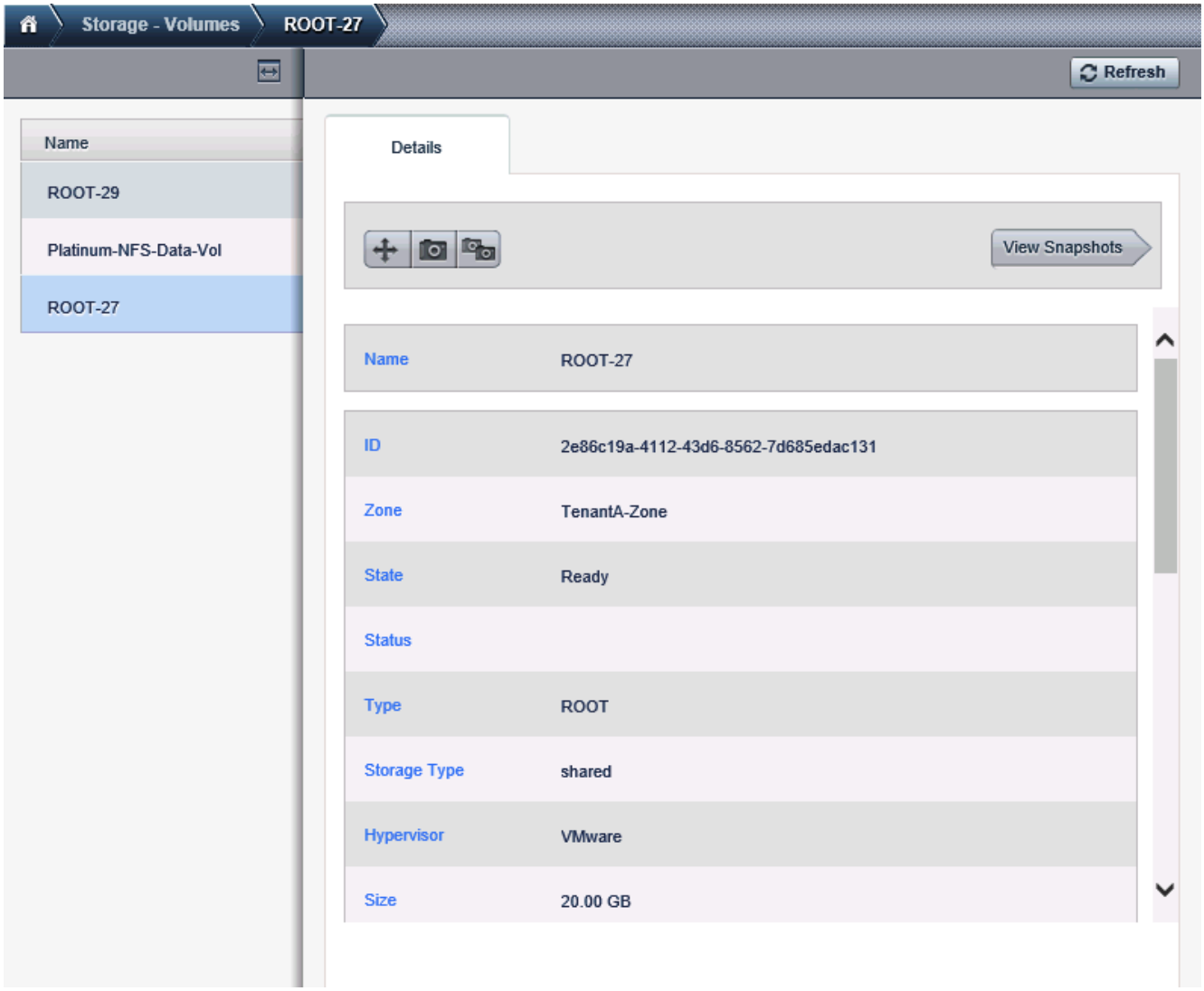
テンプレート ベースのスナップショットの復元

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Storage] タブをクリックします。

図 263　ストレージ ボリュームの表示

4. [Storage-Volumes] で [Root-27] をクリックします。
5. [View Snapshots] をクリックします。

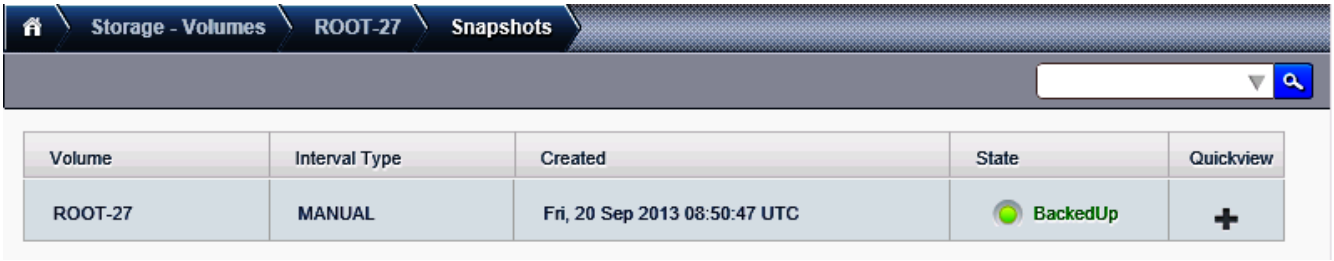
図 264　スナップショット詳細の表示



6. [Root-27 Snapshot] をクリックします。

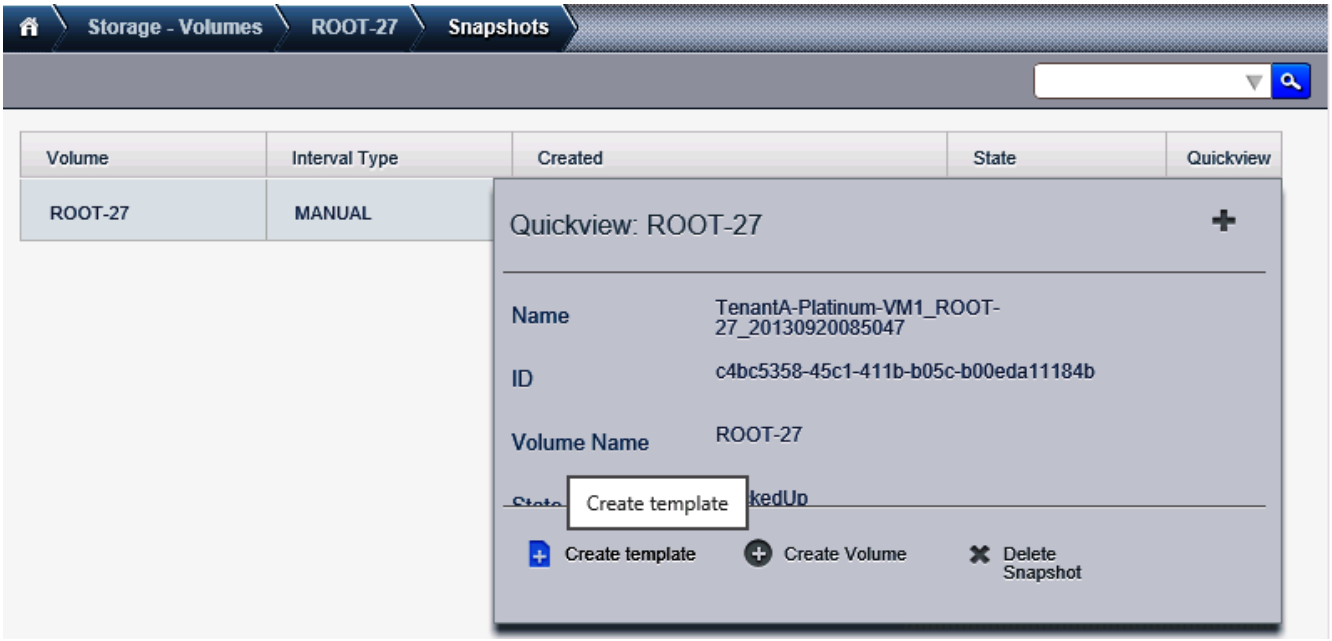
7. [View Snapshots] をクリックします。

図 265　スナップショット ステータスの表示



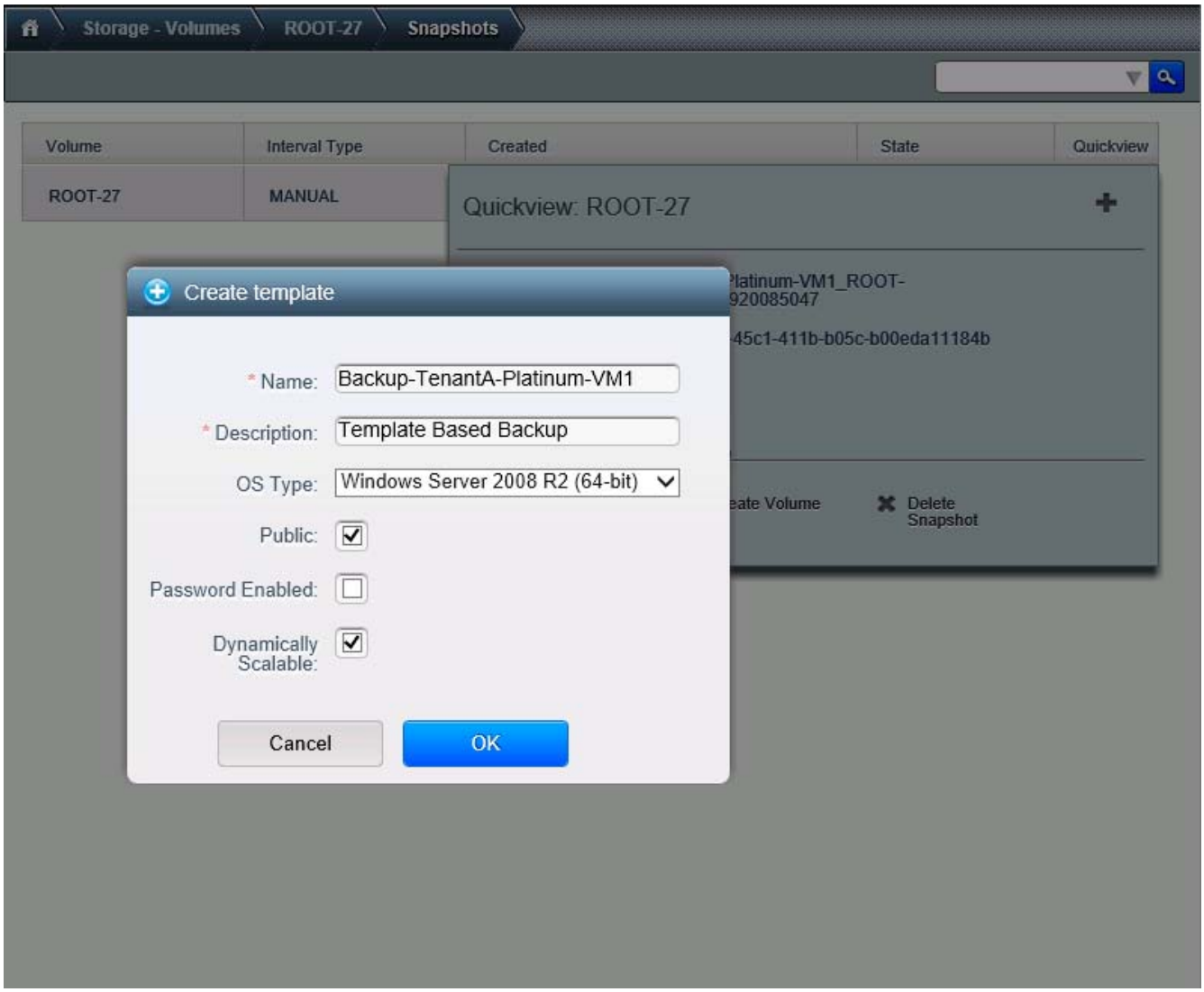
8. + 記号付きの [Create Template] アイコンをクリックします。

図 266　新しいテンプレートの作成



9. + 記号付きの [Create Template] アイコンをクリックします。
10. Backup-TenantA-Platinum-VM1 と入力します。
11. Template based Restore と入力します。
12. [OS Type] リスト ボックスで [Windows 2008 R2（64-bit）] を選択します。
13. [Public] チェックボックスをオンにします。
14. [Password Enabled] チェック ボックスはオンにしないでください。

図 267　　テンプレート プロパティの定義

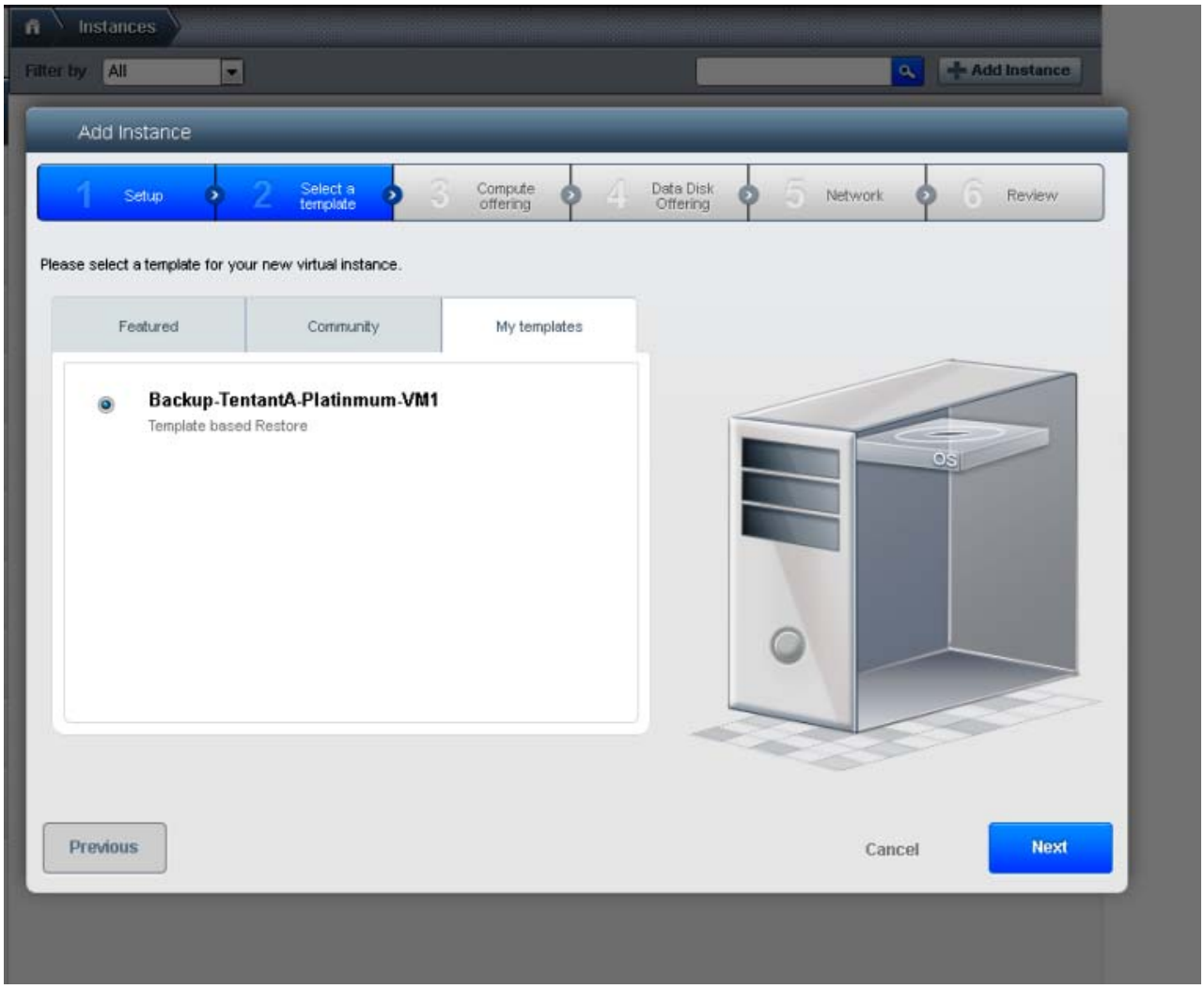


15. [Instances] タブをクリックします。
16. 右ペインで、[Add Instance] ボタンをクリックします。
17. [Zone] リスト ボックスで [TenantA-Zone] を選択します。
18. [Template] オプション ボタンをクリックします。
19. [Next] をクリックします。

図 268　テンプレートに対するゾーンの選択

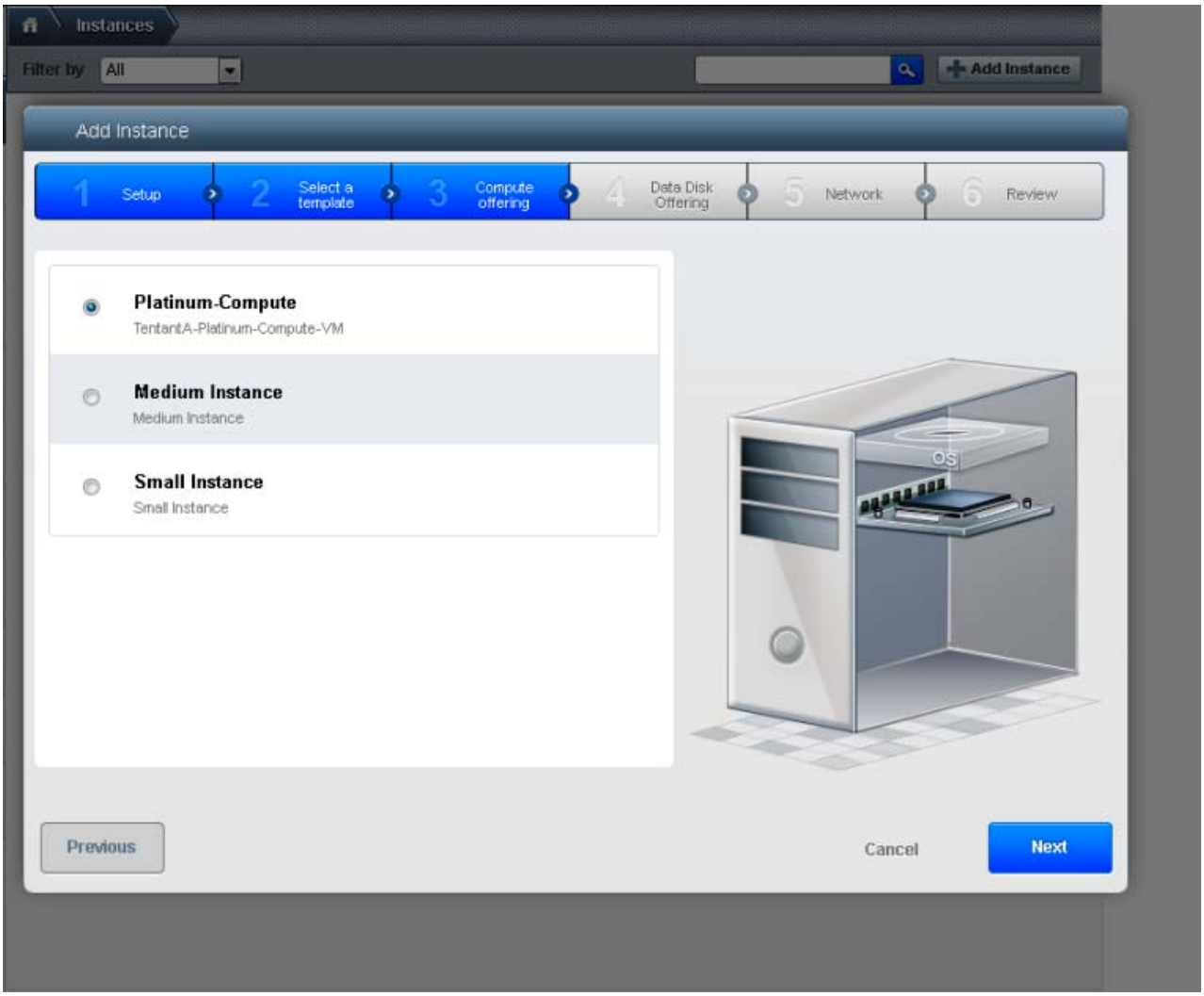
20. [My Templates] をクリックします。
21. [Backup-TenantA-Platinum-VM1] オプション ボタンをクリックします。
22. [Next] をクリックします。

図 269　　仮想インターフェイスのテンプレートの選択



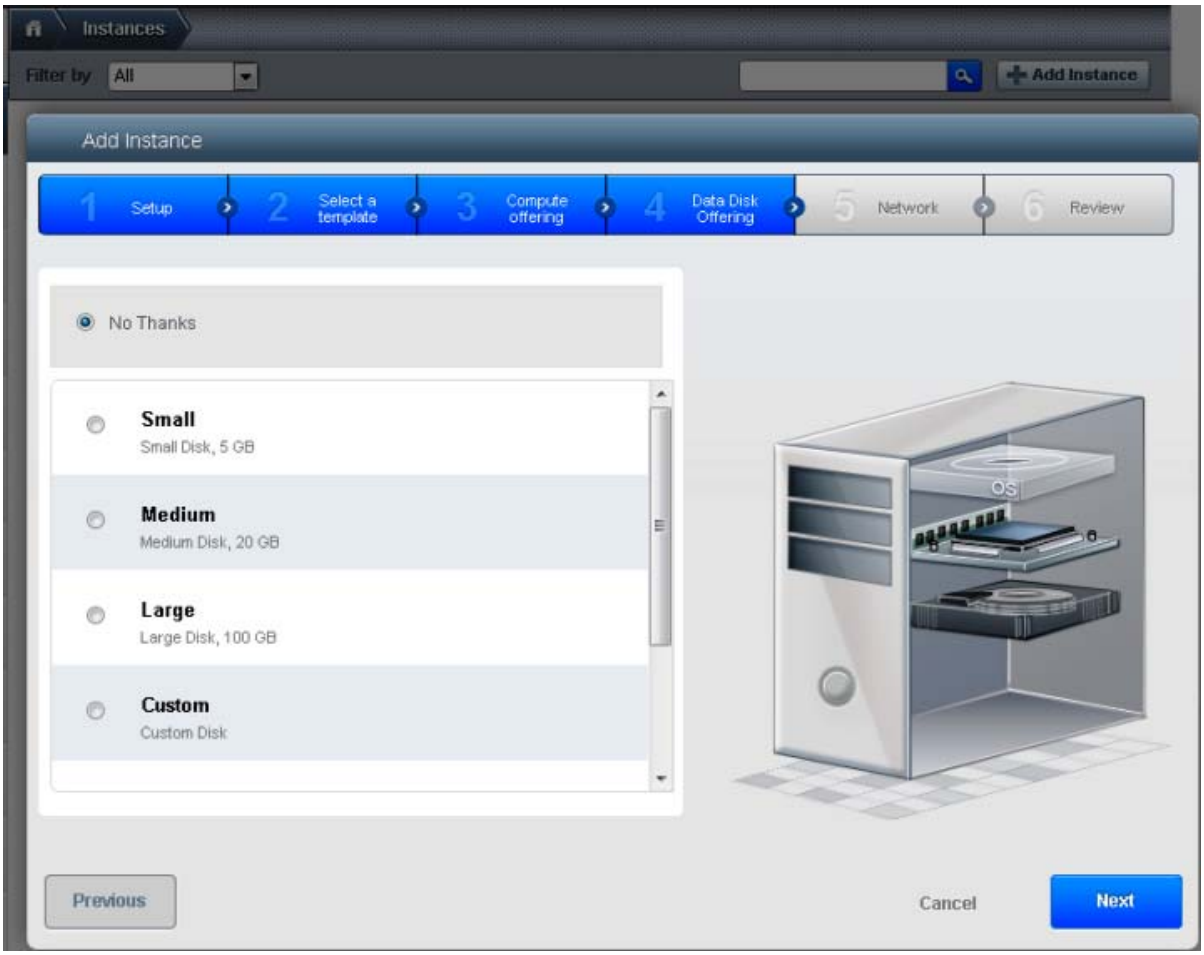
23. [Platinum-Compute] オプション ボタンをクリックします。
24. [Next] をクリックします。

図 270　　コンピュート オファリングの選択



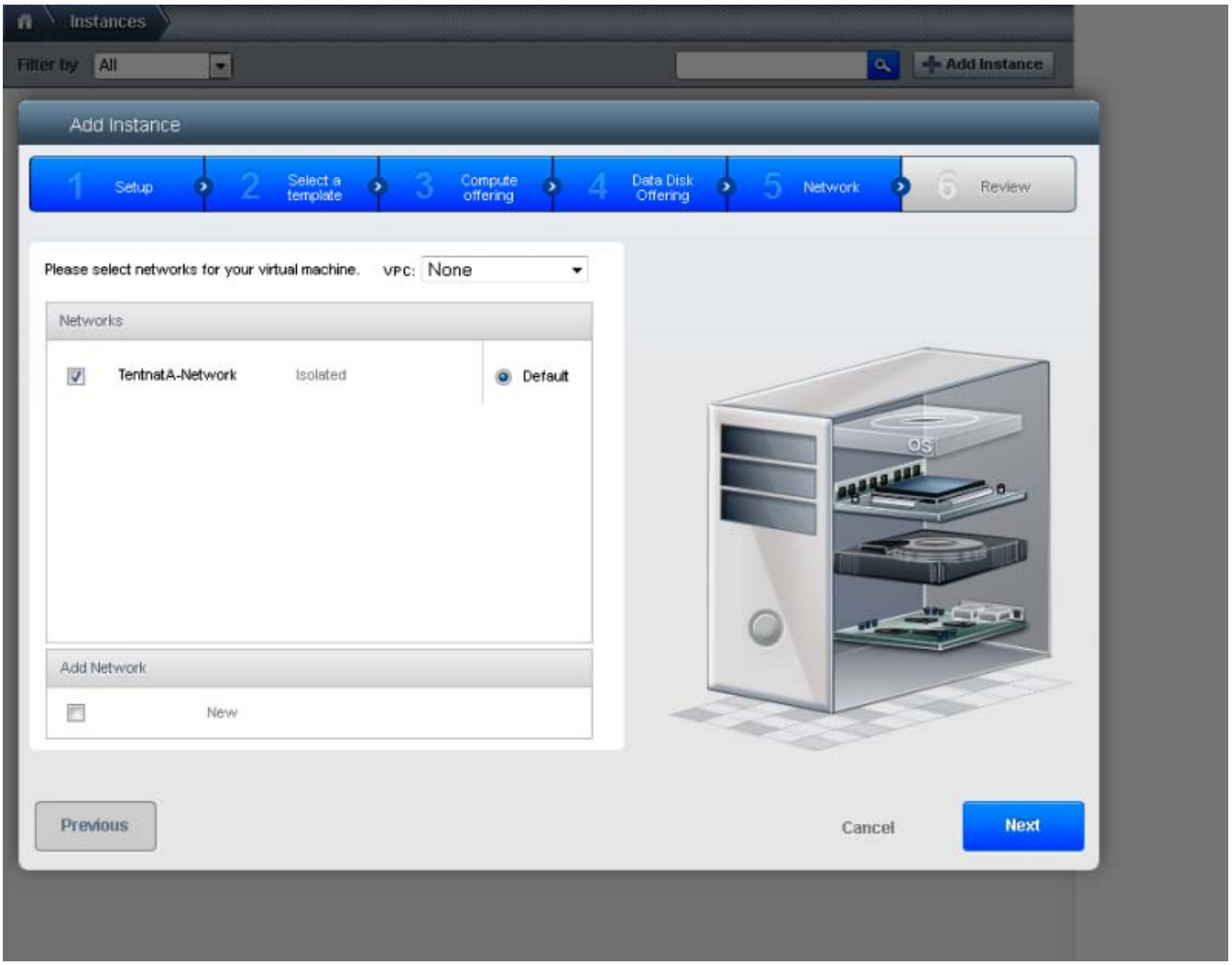
25. [No Thanks] オプション ボタンをクリックします。
26. [Next] をクリックします。

図 271　　ディスク オファリングの不選択



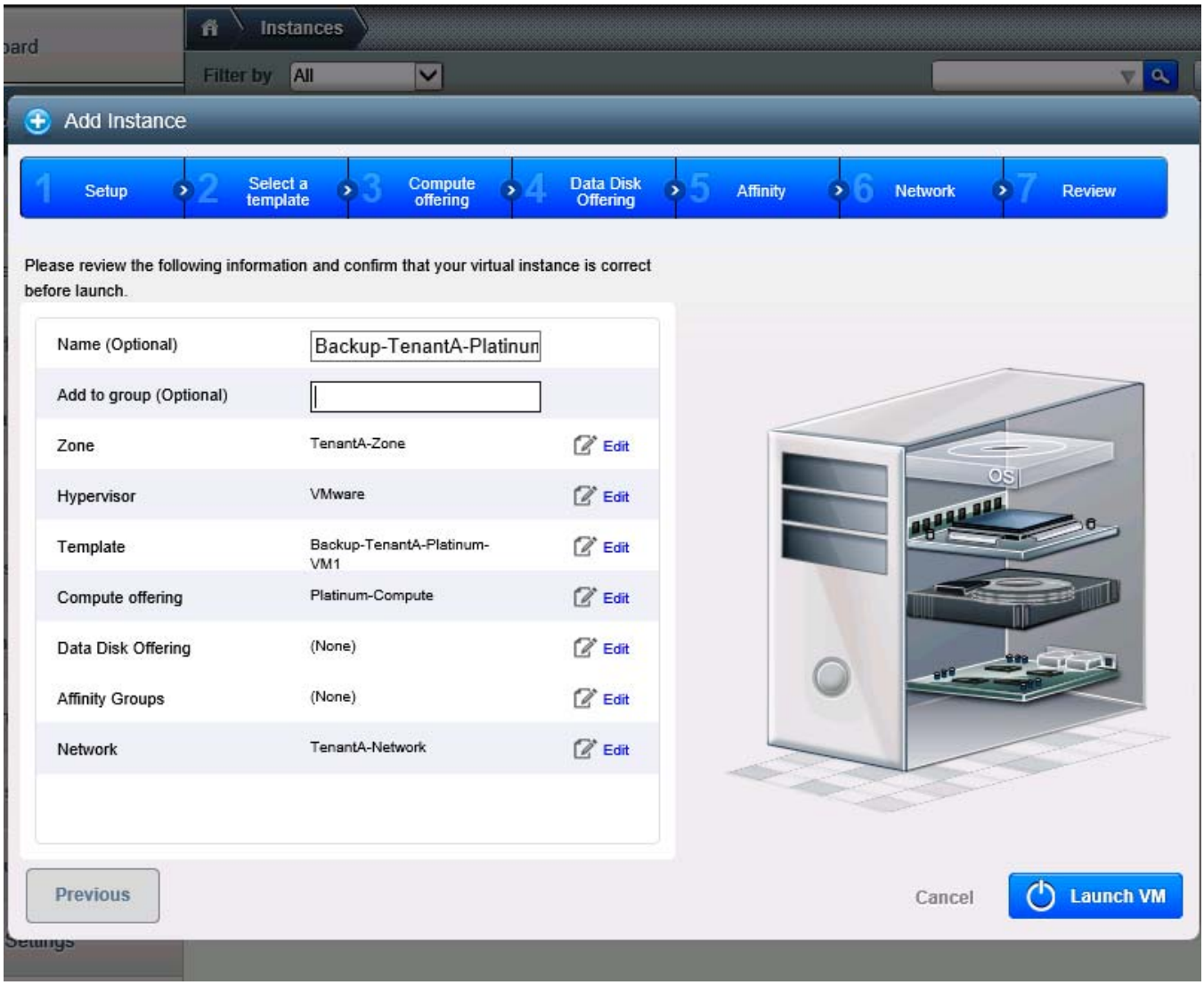
27. [TenantA-Network] チェックボックスをオンにし、[Default] オプション ボタンをクリックします。
28. [Next] をクリックします。

図 272　　VM のディスク ネットワークの選択



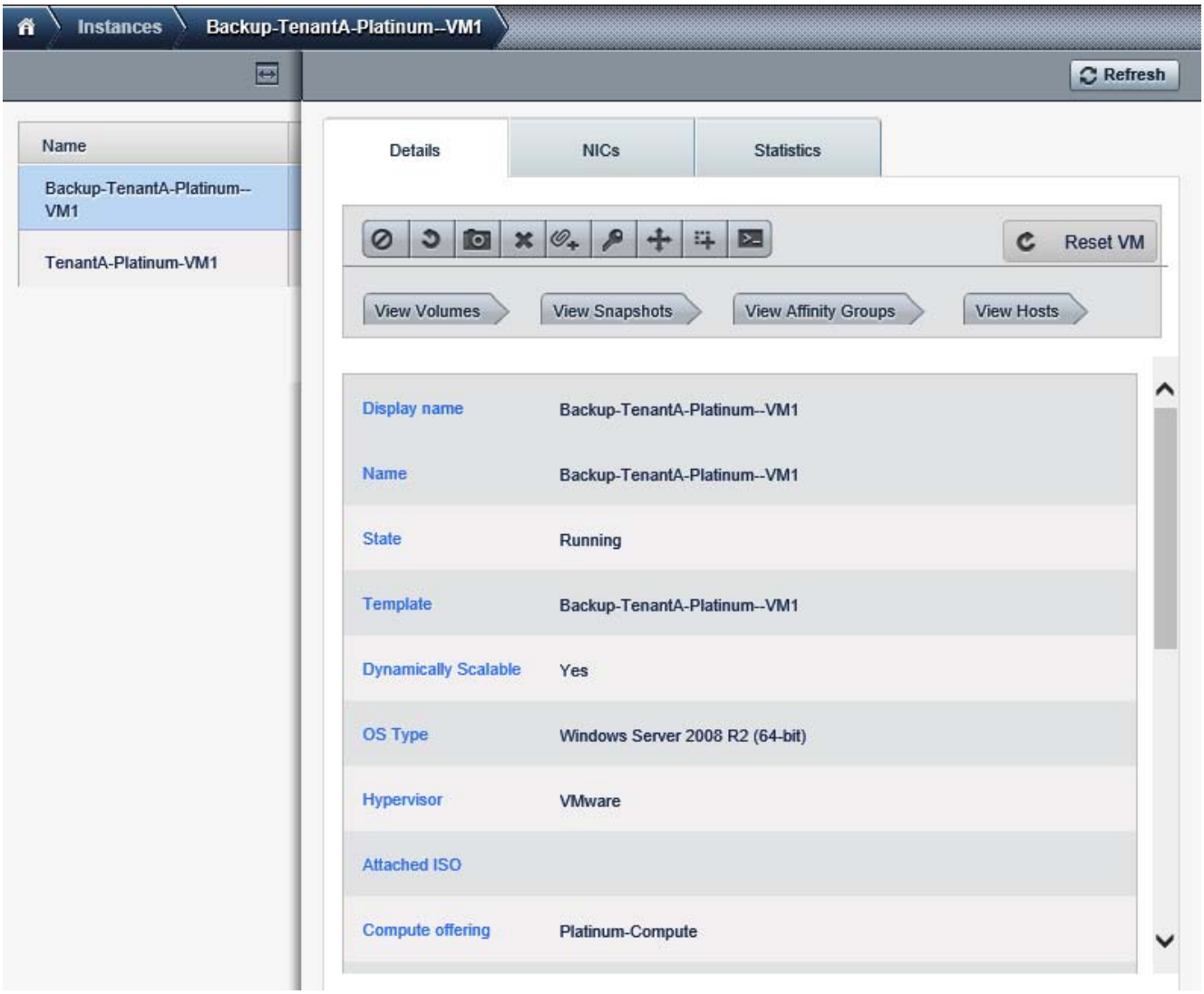
29. [Name（Optional）] フィールドに Backup-TenantA-Platinum-VM1 と入力します。
30. [Launch VM] をクリックします。

図 273　　仮想インスタンス情報の確認



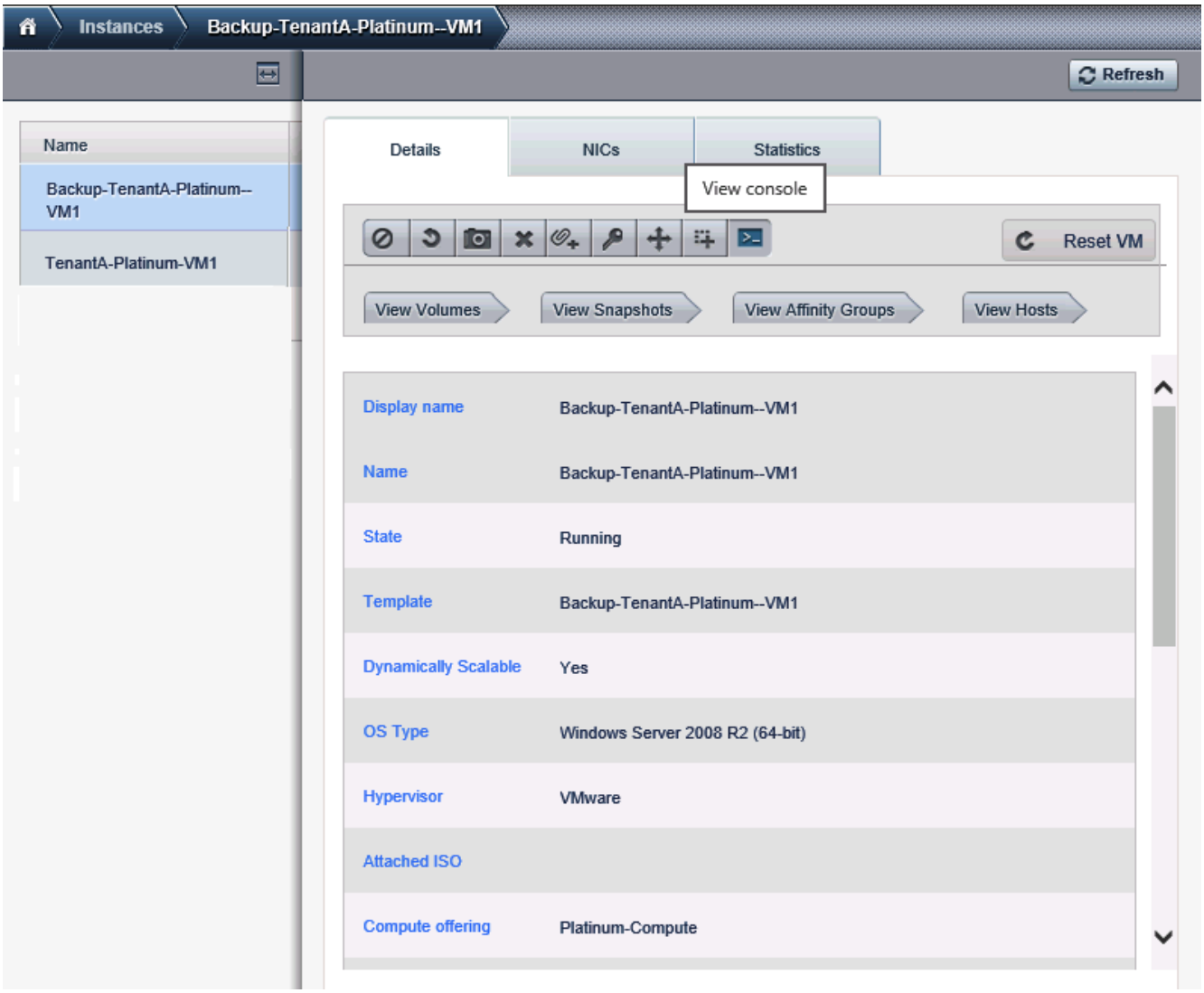
31. [Instances] タブをクリックします。
32. [Backup-TenantA-Platinum-VM1] をクリックします。

図 274　　バックアップ VM の選択



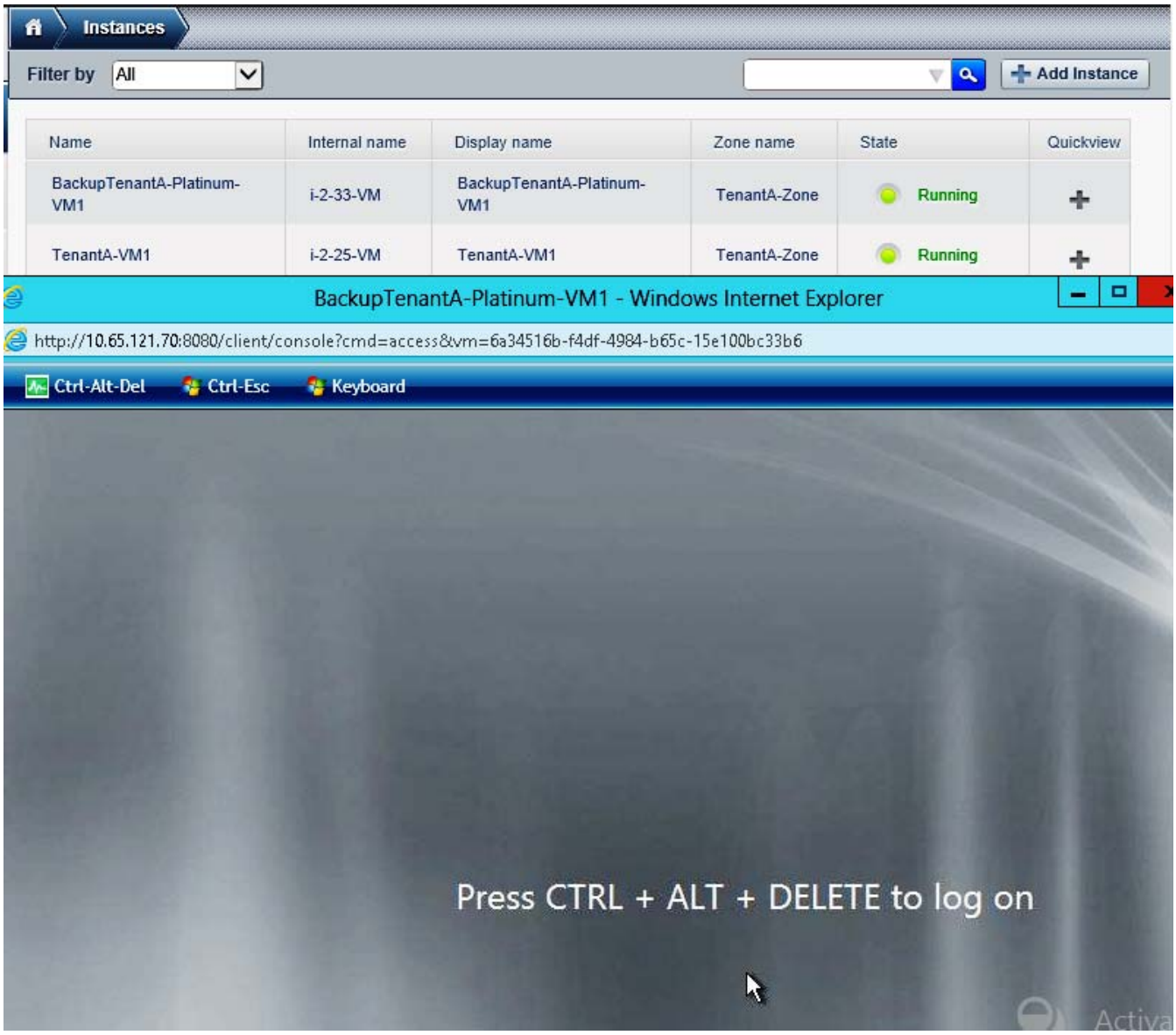
33. [View Console] をクリックします。

図 275　　バックアップ VM の詳細の表示



34. ユーザ名 <administrator> とパスワード<XXXXX> を入力し、ログインします。
35. 注：Password は、VM に設定されている親インスタンスと同じです。

図 276　　VM へのログイン



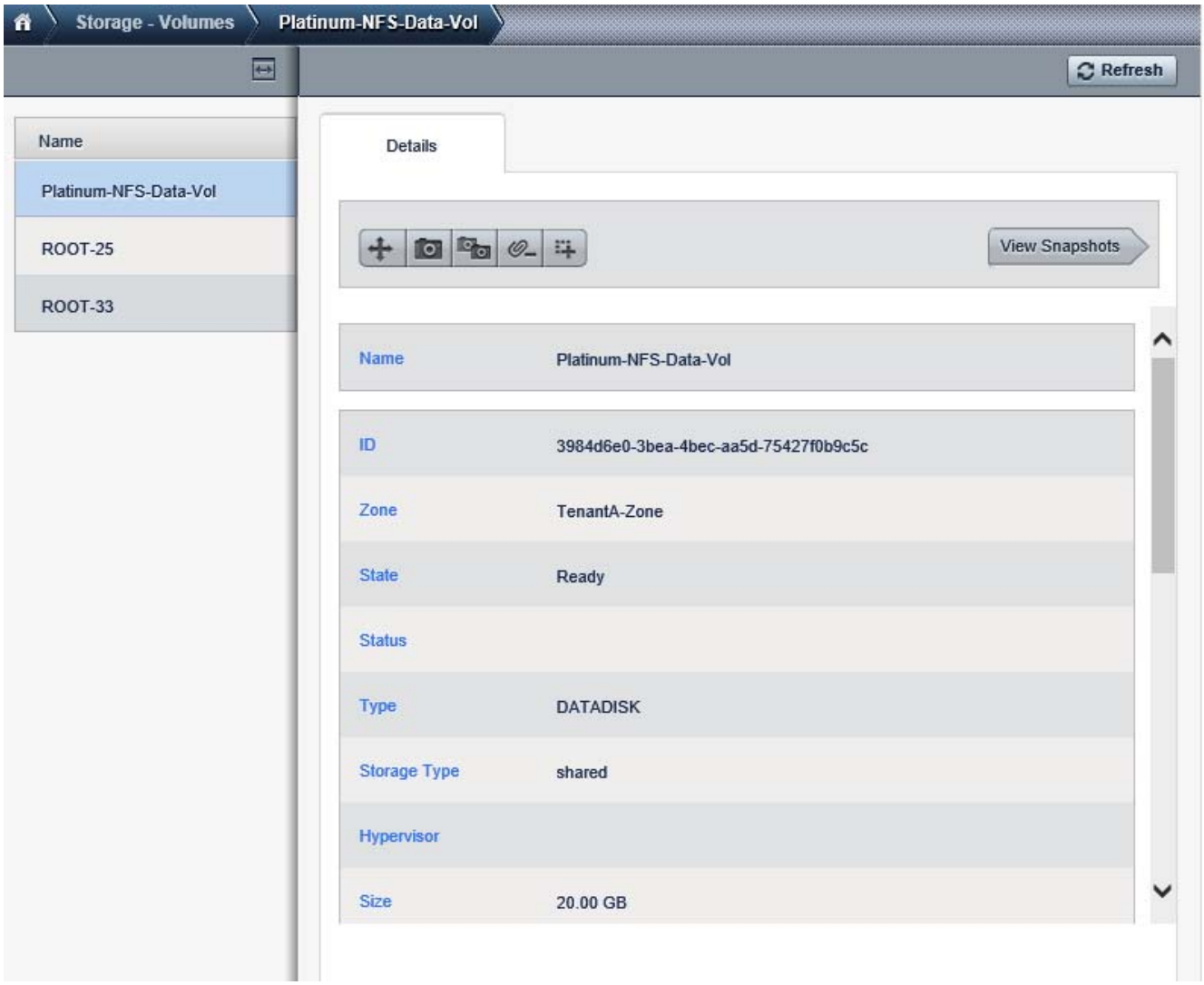
ボリューム ベースのスナップショットの復元

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Storage] タブをクリックします。
4. [Select view] リスト ボックスで [Volumes] を選択します。

図 277　　ストレージ ボリュームの表示

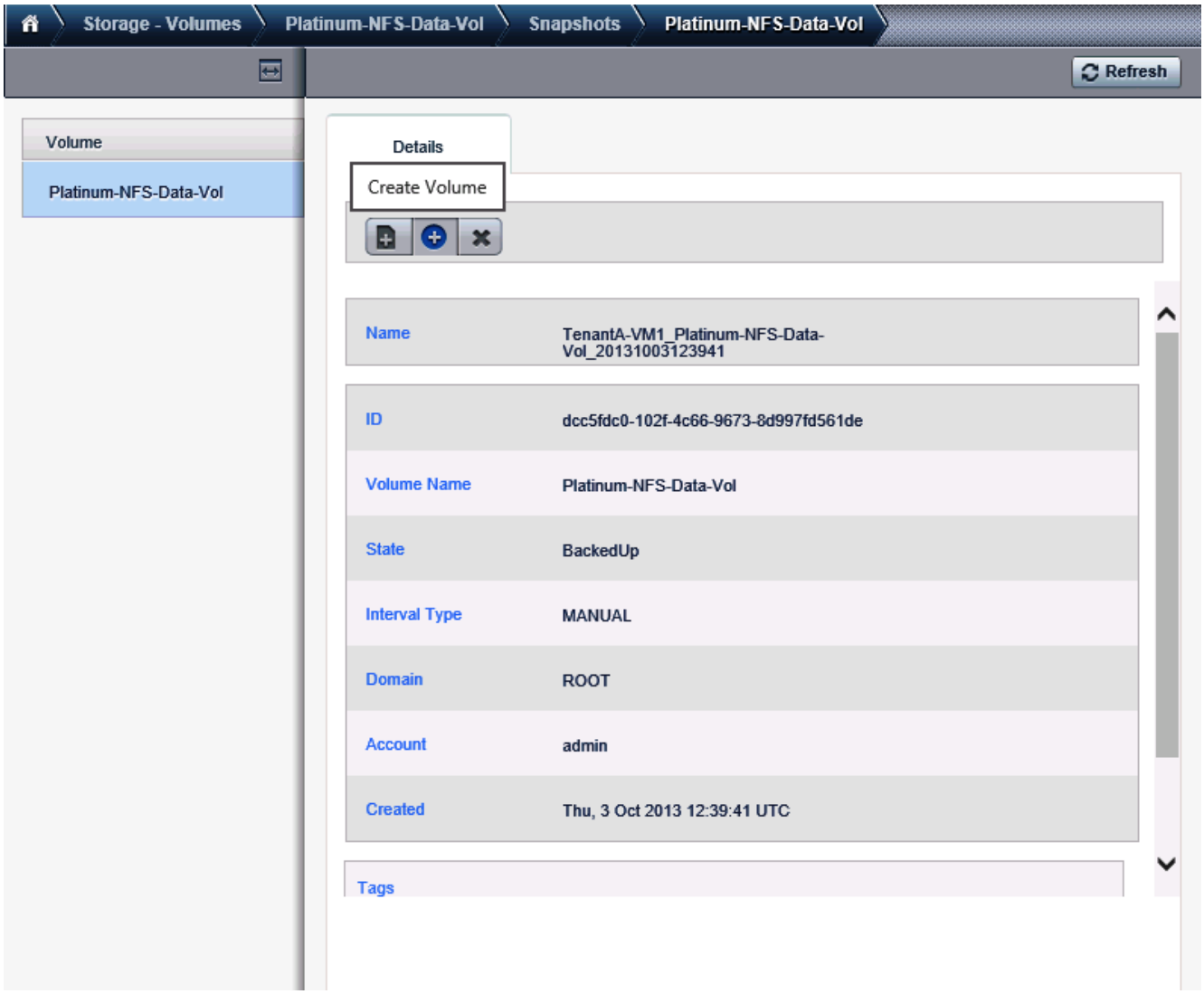
5. [TenantA-Platinum-Data-Disk Volume] をクリックします。
6. [View Snapshots] をクリックします。

図 278　　仮想データ ディスクのスナップショットの表示



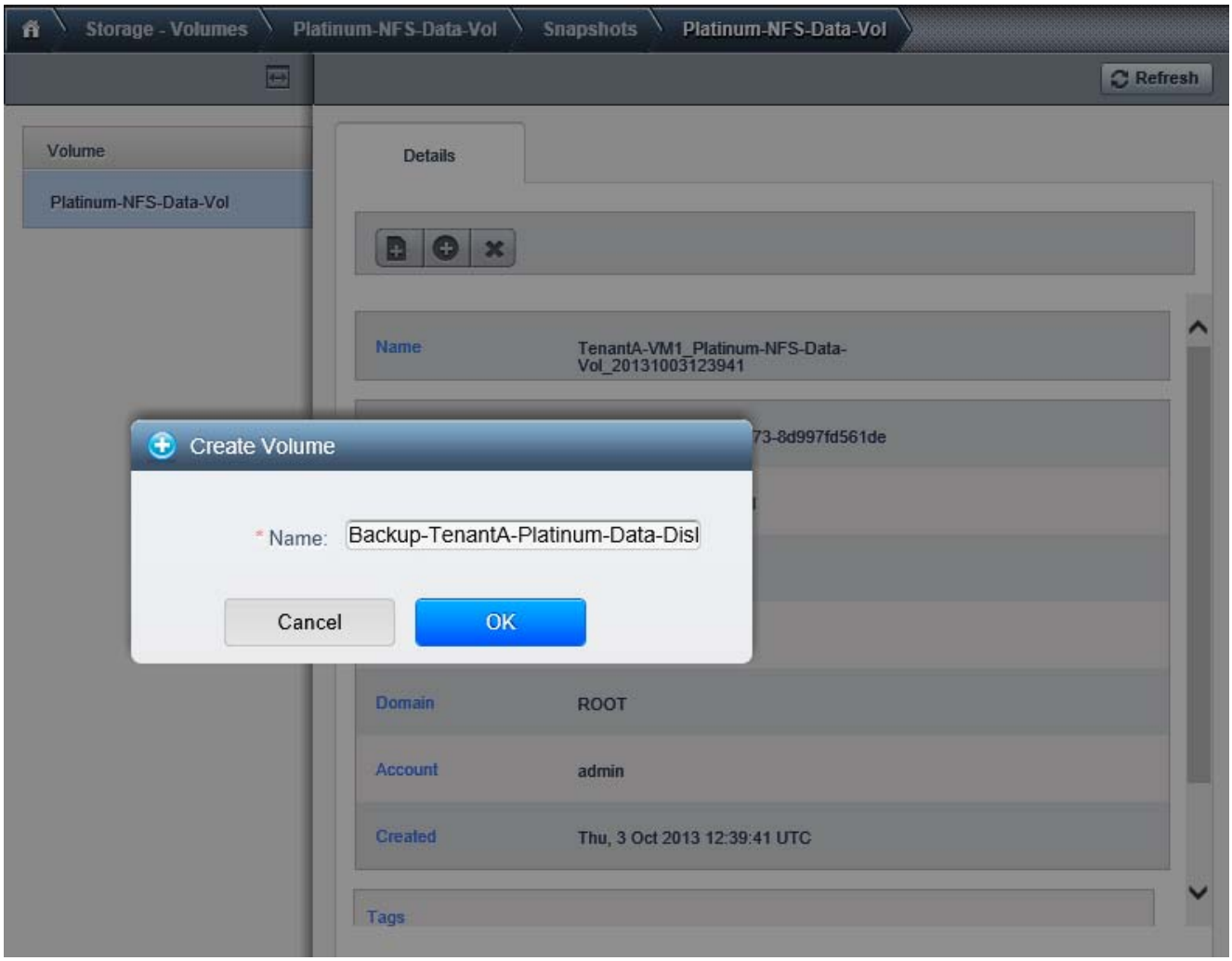
7. [TenantA-Platinum-Data-Disk Volume] をクリックします。
8. [View Snapshots] をクリックします。
9. [Create Volume] アイコンをクリックします。

図 279　　ボリュームの作成



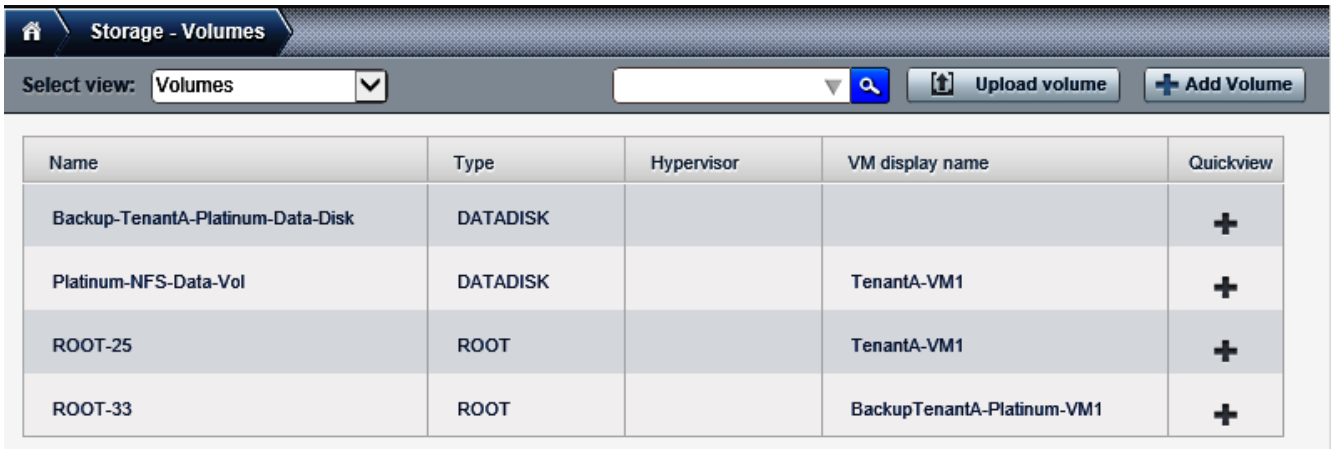
10. [Name] フィールドに <Backup-TenantA-Platinum-Data-Disk> と入力します。
11. [OK] をクリックします。

図 280　　ボリュームの名前の追加



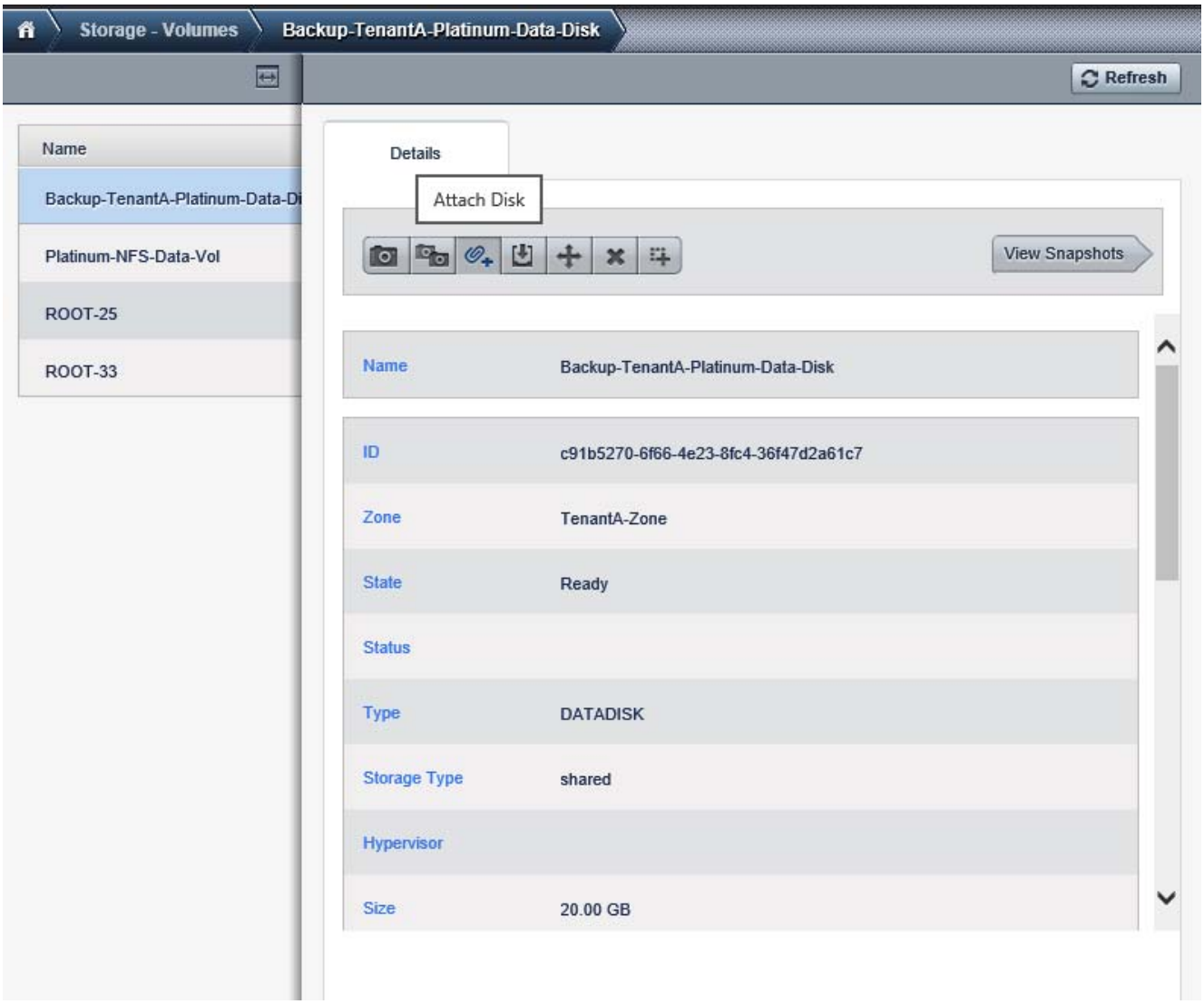
12. [Storage] タブをクリックします。
13. [Backup-TenantA-Platinum-Data-Disk] をクリックします。

図 281　　ストレージ ボリュームの表示



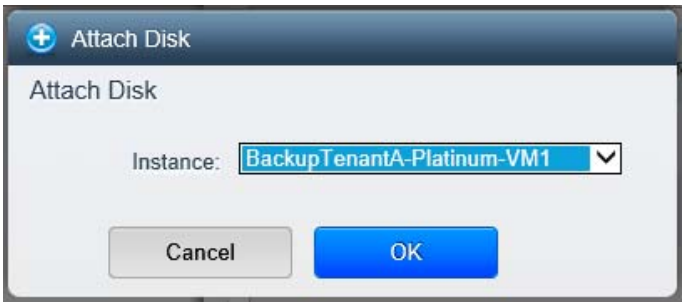
14. [Attach Disk] アイコンをクリックします。

図 282　　ディスクのアタッチ



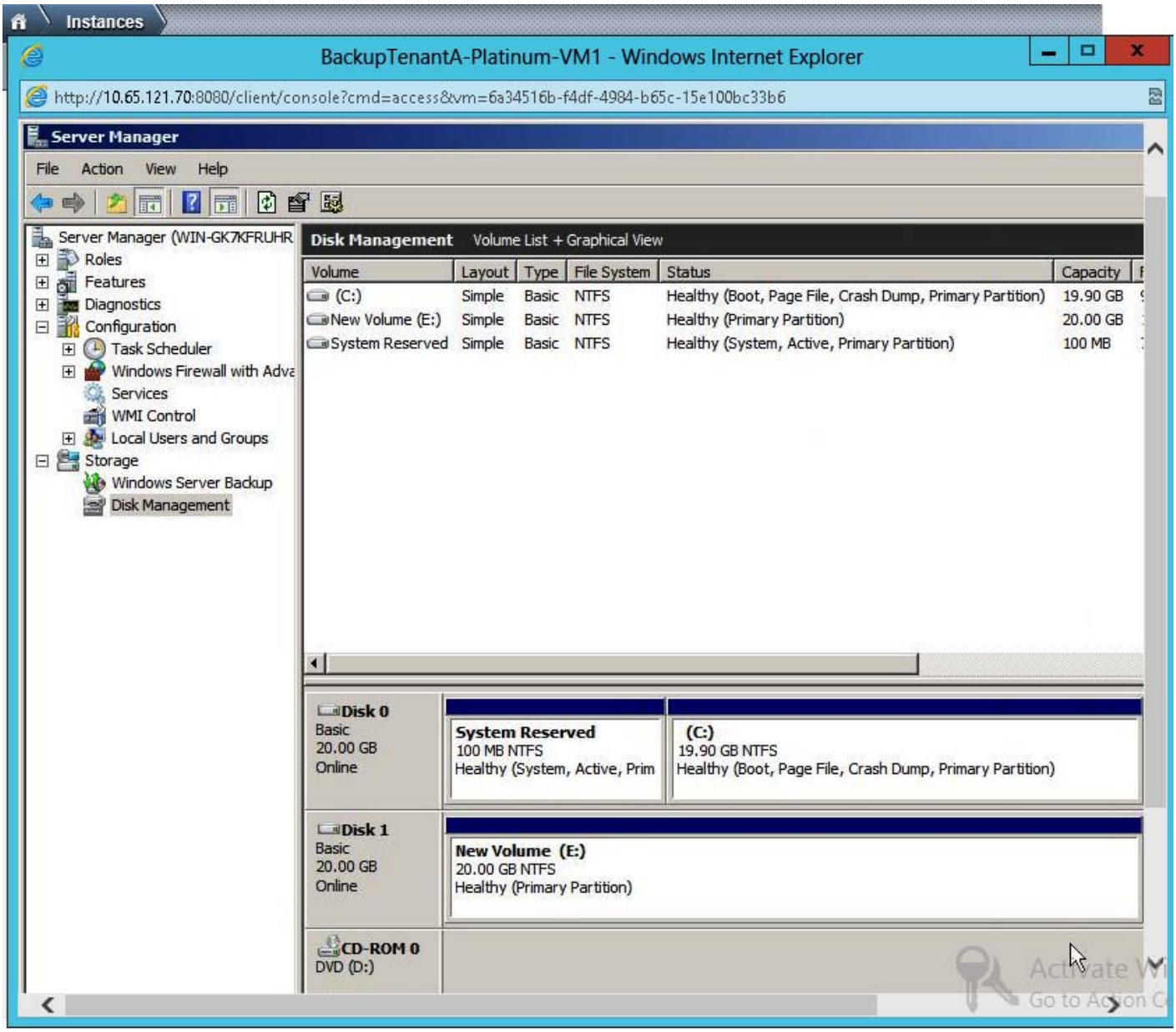
15. [Instance] リスト ボックスで [Backup-TenantA-Platinum-VM1] を選択します。
16. [OK] をクリックします。

図 283　　インスタンスへのディスクの選択



17. [Instance] リスト ボックスで [Backup-TenantA-Platinum-VM1] を選択します。
18. [View Console] をクリックします。
19. ユーザ名 <Administrator> およびパスワード <XXXXX> を入力します。
20. [Disk Management] からオンラインの [Disk1] にアクセスします。

図 284　　オンライン スナップで復元されたディスク



VM の移行

この項では、ユーザへのサービスを中断することなく、あるホストから別のホストに VM を手動で移動するのに必要な設定手順について説明します。これはライブ マイグレーションと呼ばれ、次の条件の下で行うことができます。

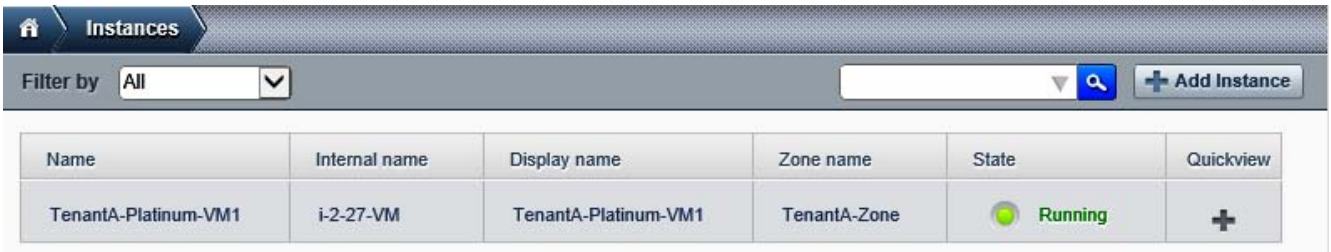
- ルート管理者がログインしている。ドメイン管理者とユーザは VM のライブ マイグレーションを実行できない。
- VM が実行されている。停止した VM のライブ マイグレーションは実行できない。
- 宛先ホストが、元のホストと同じクラスタ内にある。
- VM がローカル ディスク ストレージを使用することはできない。
- 宛先ホストに十分な空き容量がある。十分な空き容量がない場合は、メモリが使用できるようになるまで VM は「移行中」状態になる。

（注） ここでは、クラウド ホスト TenantA-HostA 上の VM インスタンス TenantA-Platinum-VM1 を TenantA-HostB に移行します。

ユーザ資格情報を使用して CloudPlatform にログインして、TenantA-Platinum-VM1 を TenantA-HostB に手動でライブ マイグレーションします。

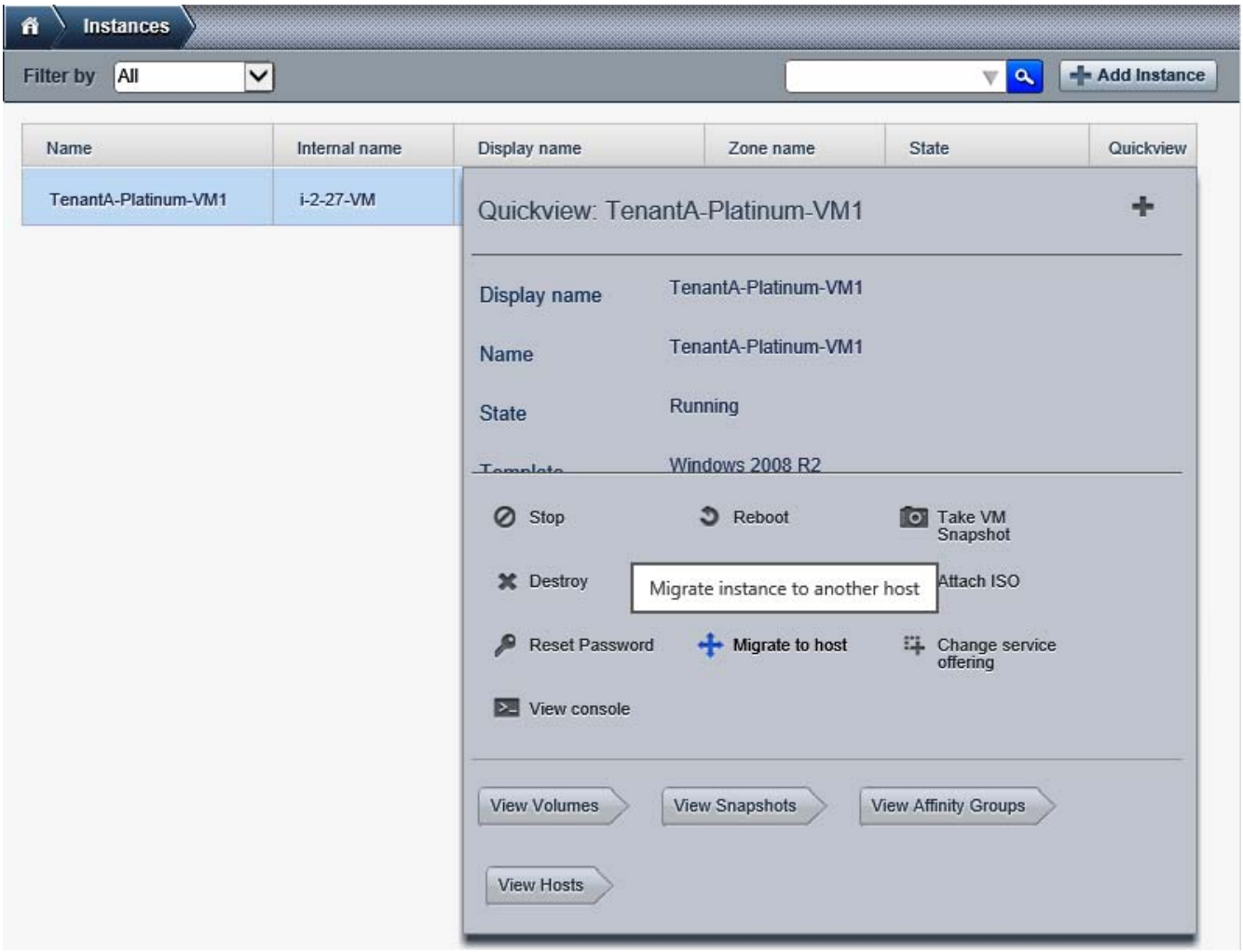
1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Instance] タブをクリックします。
4. [TenantA-Platinum-VM1] をクリックします。

図 285　テナント A プラチナ ホストの選択



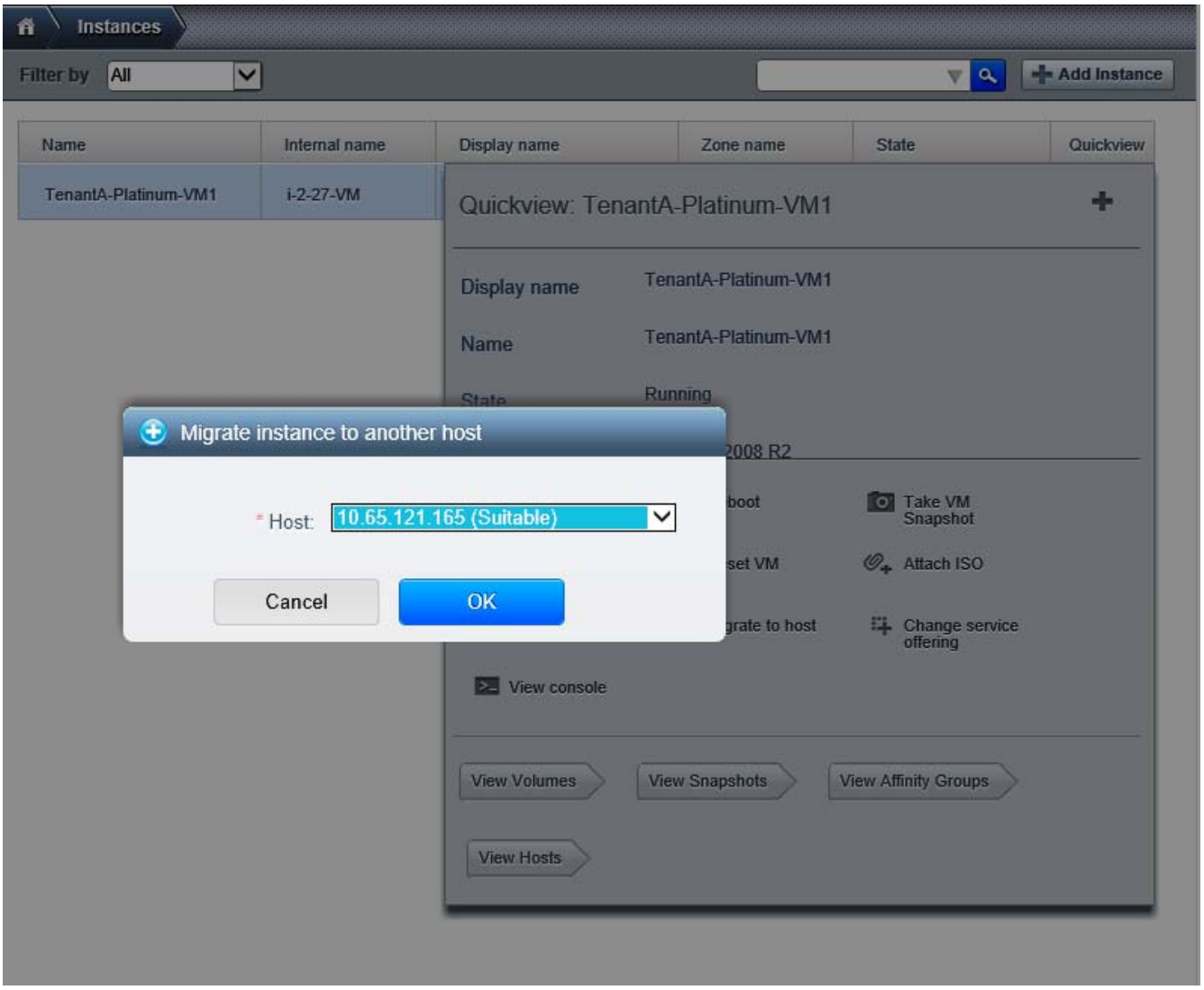
5. [migrate instance to another host] ボタンをクリックします。

図 286　　インスタンスの移行



6. [Host] リスト ボックスで [10.65.121.165 (TenantA-HostB)] を選択します。
7. [OK] をクリックします。

図 287　　移行の宛先ホストの選択



8. VM 移行タスクが完了しました。

図 288　　移行の完了

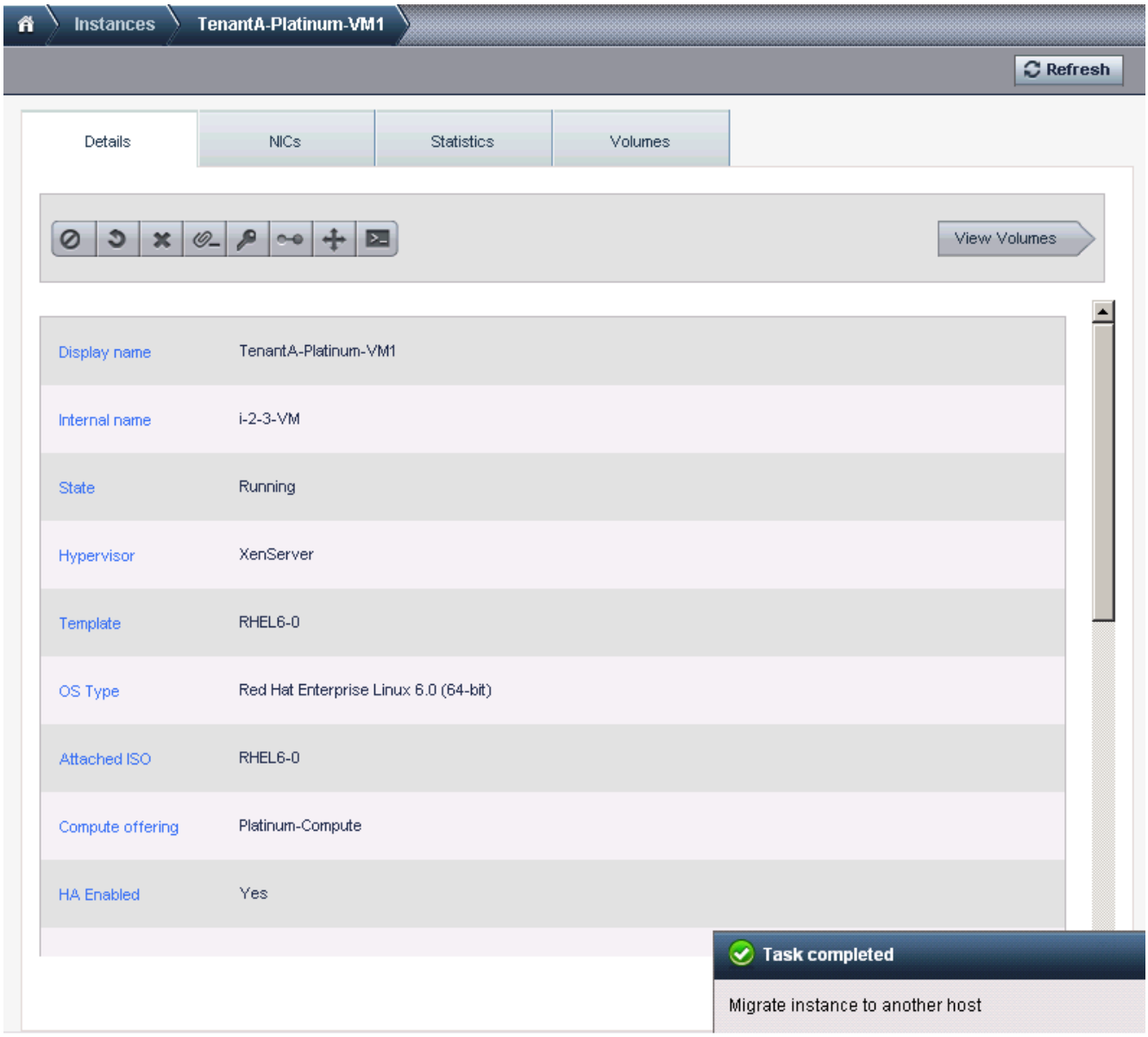
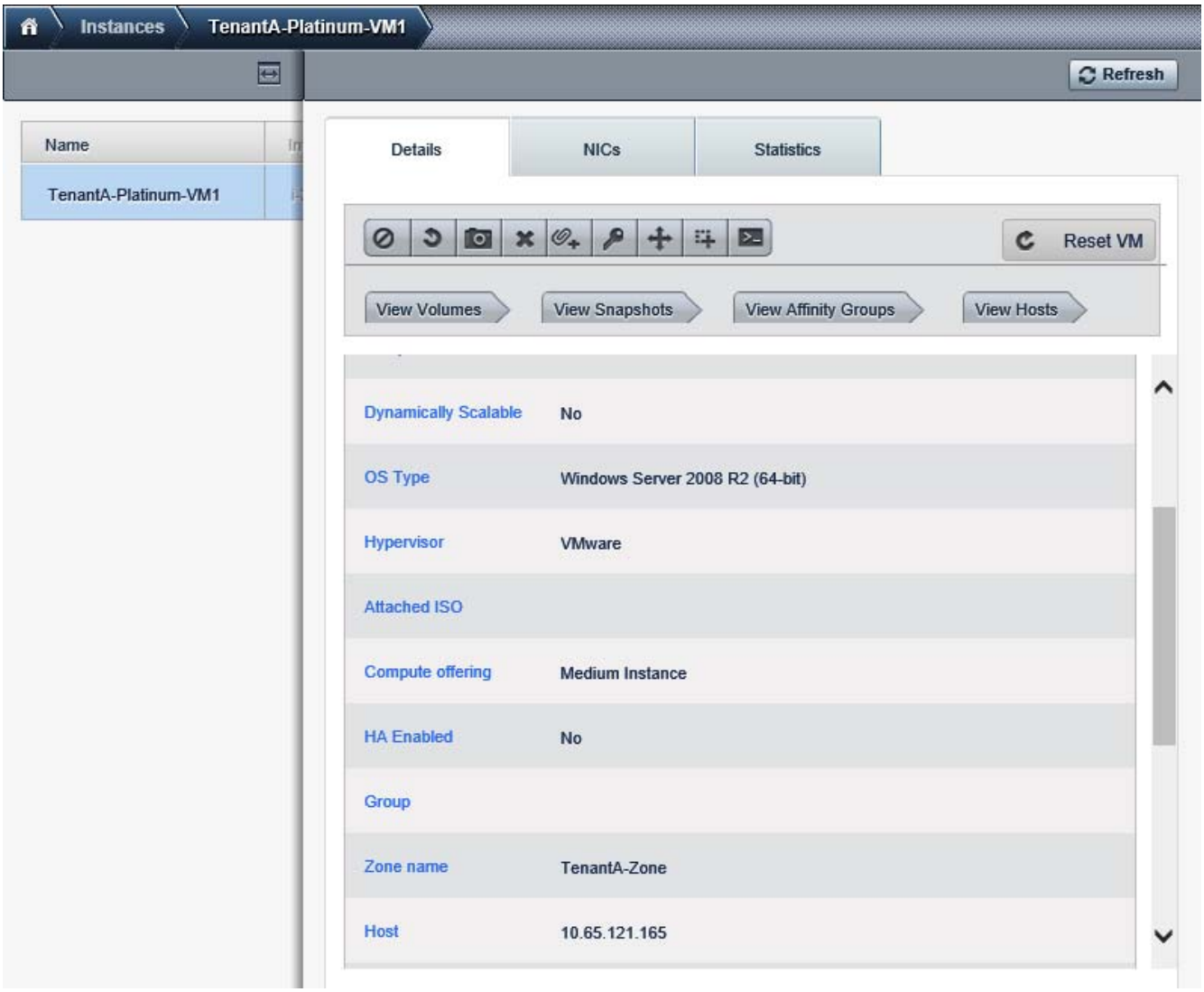

Instances
TenantA-Platinum-VM1
Refresh
Details
NICs
Statistics
Volumes
View Volumes
Display name
TenantA-Platinum-VM1
Internal name
i-2-3-VM
State
Running
Hypervisor
XenServer
Template
RHEL6-0
OS Type
Red Hat Enterprise Linux 6.0 (64-bit)
Attached ISO
RHEL6-0
Compute offering
Platinum-Compute
HA Enabled
Yes
Task completed
Migrate instance to another host

図 289　　VM 移行の要約



VM ストレージの移行

この項では、メンテナンス モードまたはロード バランシング モードに入るために仮想マシン ストレージを、プライマリ ストレージから別のプライマリ ストレージに手動で移動する際に必要な設定手順について説明します。ストレージの移行が実行できるのは停止したインスタンスだけなので、VM インスタンスにディスクをアタッチしないでください。

（注）　現在の CloudPlatfrom 4.2.1.1 バージョンでは、GUI を使用した、ゾーン内の同じクラスでの仮想マシンストレージの移行はサポートされていませんが、API を呼び出すことによってこれを実現できます。

これを実現するには、VM に対してターゲット ホストを、VM の各ボリュームに対してターゲット ストレージを指定して API「migrateVirtualMachineWithVolume」を使用します。

次に例を示します。

```
command=migrateVirtualMachineWithVolume&hostid=<TARGET_HOST>&virtualmachineid=<V
M_IN_QUESTION>&migrateto[<I>].volume=<VOLUME_ID>&migrateto[<I>].pool=<TARGET_POOL
_ID>
<TARGET_HOST> - UUID of target host for the VM to be relocated to. This host can
be within or out of cluster.
<VM_IN_QUESTION> - UUID of VM which need to be migrated out of the current
storage pool.
<VOLUME_ID> - UUID of volume of the VM
<TARGET_POOL_ID> - UUID of target primary storage pool. This pool can belong to
current cluster or other cluster)
```

VM の削除

この項では、再利用のためにコンピューティング、ネットワークおよびストレージ リソースを解放してクラウド プールに戻すクラウド管理者が、メンテナンス作業の一部として仮想マシンをクリーンアップするために実行する手順について説明します。

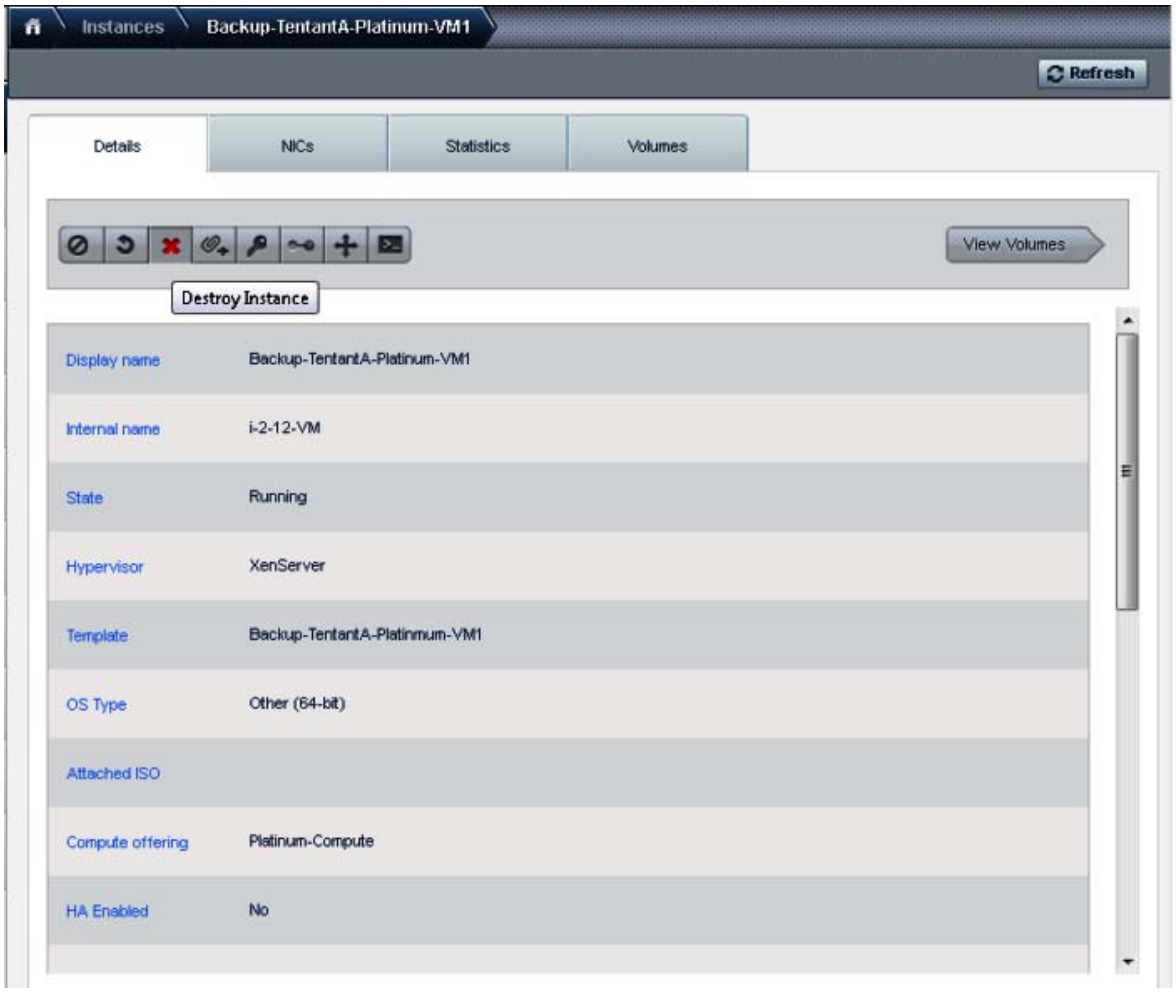
仮想マシンが破棄されると、仮想マシンによって使用されたすべてのリソースはシステムによって回収されます。これには、仮想マシンの IP アドレスが含まれます。

（注） ここでは、CloudPlatform を使用して Backup-TenantA-Platinum-VM1 を削除します。

ユーザ資格情報を使用して CloudPlatform にログインして、TenantA ゾーンで TenantA-Platinum-VM1 の手動および自動バックアップを作成します。

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. 検索タイプ secstorage.allowed.internal.sites で [Global Setting] タブをクリックします。
4. secstorage.allowed.internal.sites で <<Var_HTTP_Server>> 10.65.121.705 と入力します。
5. CloudPlatfrom サービスを再起動します。

図 290　バックアップをチェックするためのインスタンスの破棄



Baremetal ホスト クラウド構成の設計

この項では、プライベート クラウド環境で提供することができるサービス オファリングとしての Citrix CloudPlatform 4.2.1 BareMetal ホストの概要を説明します。複数のテナントは物理計算上で LINUX ベースのオペレーティング システムをインストールしてパフォーマンスとセキュリティの要件のあるワーク ロードを実行し、CloudPlatfrom 4.2.1 はこれらの BareMetal ホストのマルチ化傾向およびライフ サイクル管理を実現します。

CloudPlatform 4.2.1 は、基本ゾーンの Baremetal ホスト上で RPM ベースの Linux オペレーティング システムをインストールする方法としてキックスタートをサポートします。キックスタート ファイルと対応する OS インストール ISO が用意されている限り、ユーザは CloudPlatform で管理される Baremetal ホストをプロビジョニングできます。

キックスタート インストールでは、OS のインストール中に手動による介入はありません。スクリプトとしてテキスト ファイルを使用し、インストールを自動化します。キックスタート ファイルには、オペレーティング システムをインストールするときに表示されるすべてのユーザ入力プロンプトへの応答が含まれています。キックスタート インストールを使用すると、多数のホストへのオペレーティング システム ソフトウェアのインストールを自動的に行うことができます。

キックスタート Baremetal インストールの制限事項

1. アドバンスド ゾーンでの使用はサポートされていません。基本ゾーンでのみ使用してください。
2. CloudPlatform ストレージのコンセプト：プライマリ ストレージ、セカンダリ ストレージ、ボリューム、スナップショット。
3. システム VM：SSVM、CPVM、VR。
4. テンプレートのコピーまたはテンプレートのダウンロード
5. VM の移行。
6. 複数の NIC。
7. ホストを割り当て用のホスト タグの使用、サービス オファリングの容量（CPU、メモリ）の指定。
8. 停止された VM（ホスト上で実行されている OS）は、一番最近に起動されたホスト上でのみ開始できます。

Citrix BaremetalCloud 設計は、次のタスクに分割されています。

1. ネットワーク オファリングおよびコンピュート オファリングの定義。
2. ゾーンの定義。
3. ネットワークの定義。
4. Pod の追加
5. クラスタの追加。
6. ホストの追加。
7. Baremetal ホストの導入。

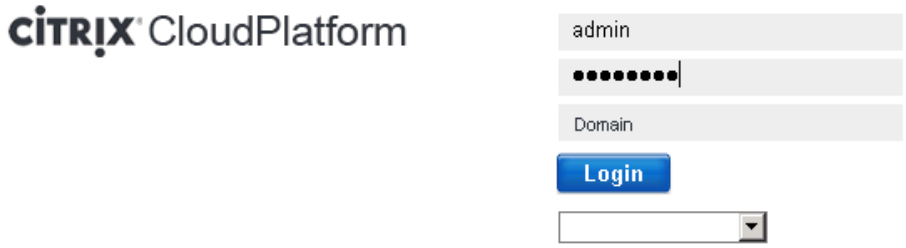
ネットワーク オファリングおよびコンピュート オファリングの定義

ゾーンは、CloudPlatform 導入における最大の組織単位です。ゾーンは通常単一のデータセンターに対応しますが、データセンター内に複数のゾーンを持つことが許容されます。クラウドのコンピューティング、ネットワークおよびストレージ インフラストラクチャをゾーンに編成する利点は、物理的な分離および冗長性を実現できることです。

クラウド サービスをホストする TenantA マルチテナントに専用の Citrix CloudPlatform アプリケーションを使用してゾーンを作成するには、ユーザ資格情報を使用して CloudPlatform にログインし、次の手順を実行します。

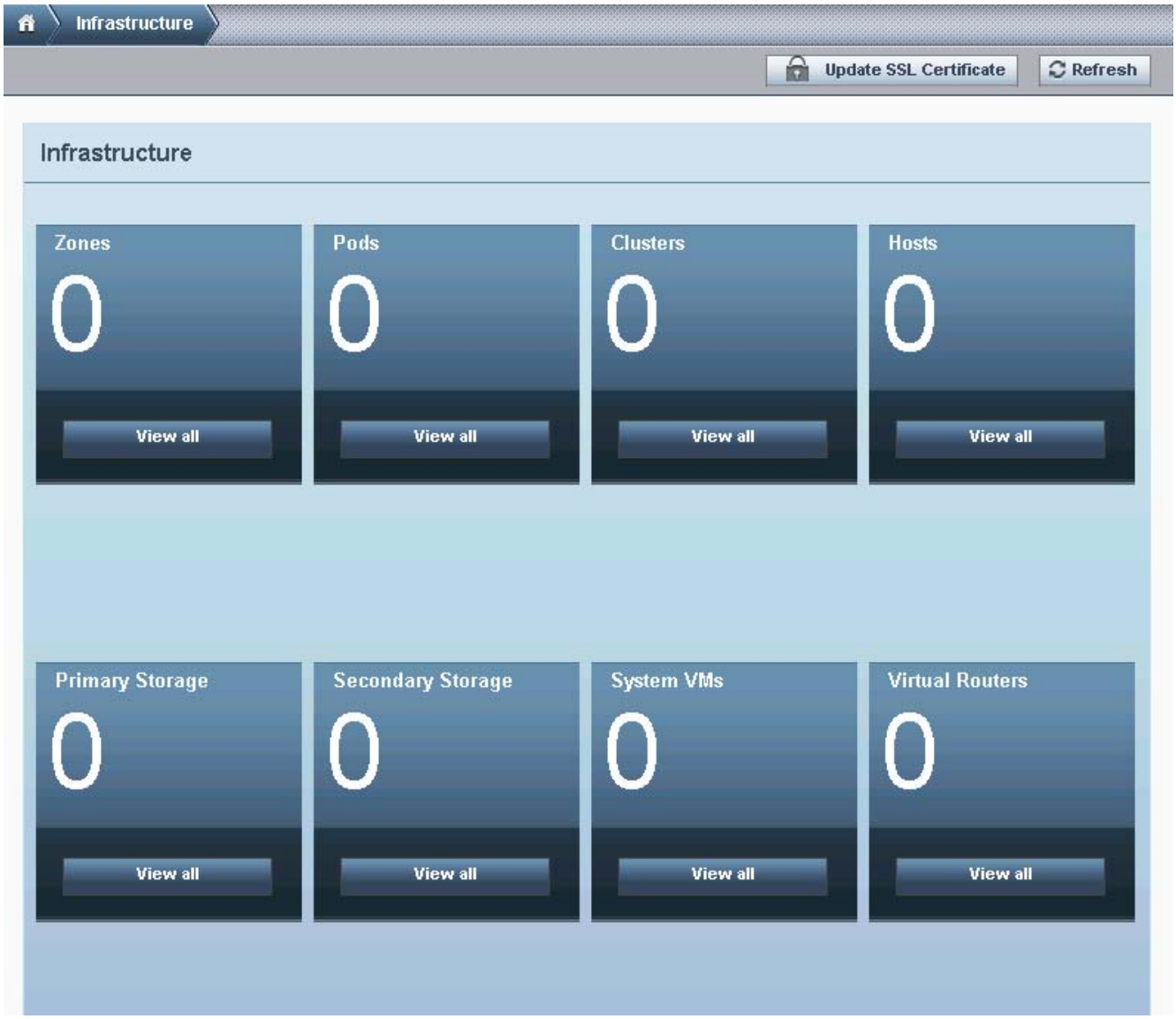
1. ユーザ名 <root>、パスワード <XXXXXX>、およびドメインを入力します。
2. [Login] をクリックします。

図 291　Citrix CloudPlatform へのログイン



3. [Agree] をクリックして、エンド ユーザ ライセンス契約を確認します。
4. [I have used CloudPlatform before, skip this guide] ボタンをクリックします。
5. 左ペインで、[Infrastructure] タブをクリックします。

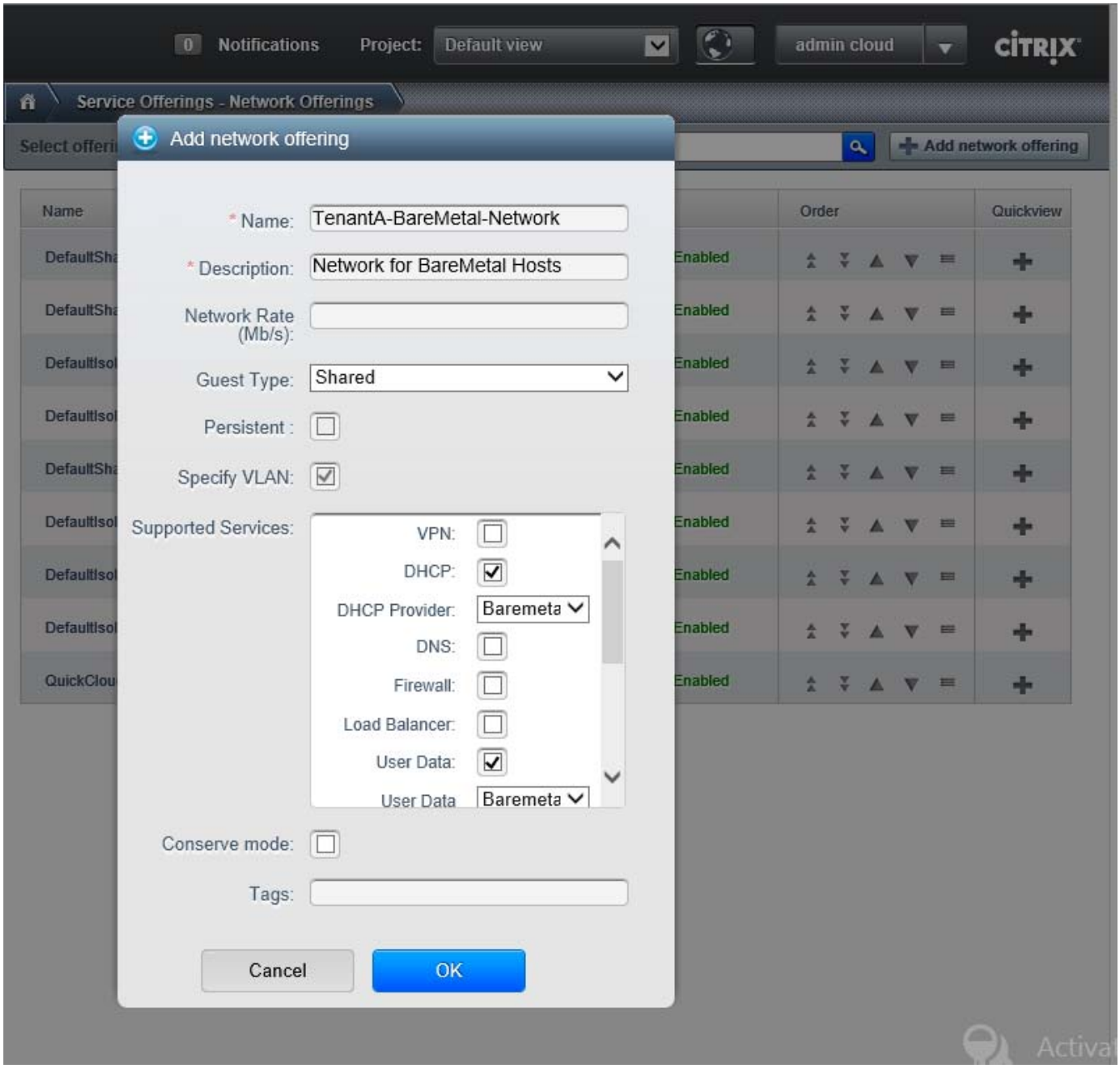
図 292　　インフラストラクチャ ページの表示



6. 左ペインで、[Service Offerings] をクリックします。
7. 右ペインの [Select Offering] リスト ボックスで、[Network Offering] を選択します。
8. [Add network offering] をクリックします。
9. [Name] フィールドに TenantA-BareMetal-Network と入力します。
10. [Description] フィールドに Network for BareMetal Hosts と入力します。
11. [Guest Type] リスト ボックスで [Shared] を選択します。
12. [Specify VLAN] チェックボックスをオンにします。
13. [Supported Services] で、[DHCP] チェックボックスをオンにします。
14. [DHCP Provider] リスト ボックスで [BaremetalDhcpProvider] を選択します。
15. [UserData] チェックボックスをオンにします。

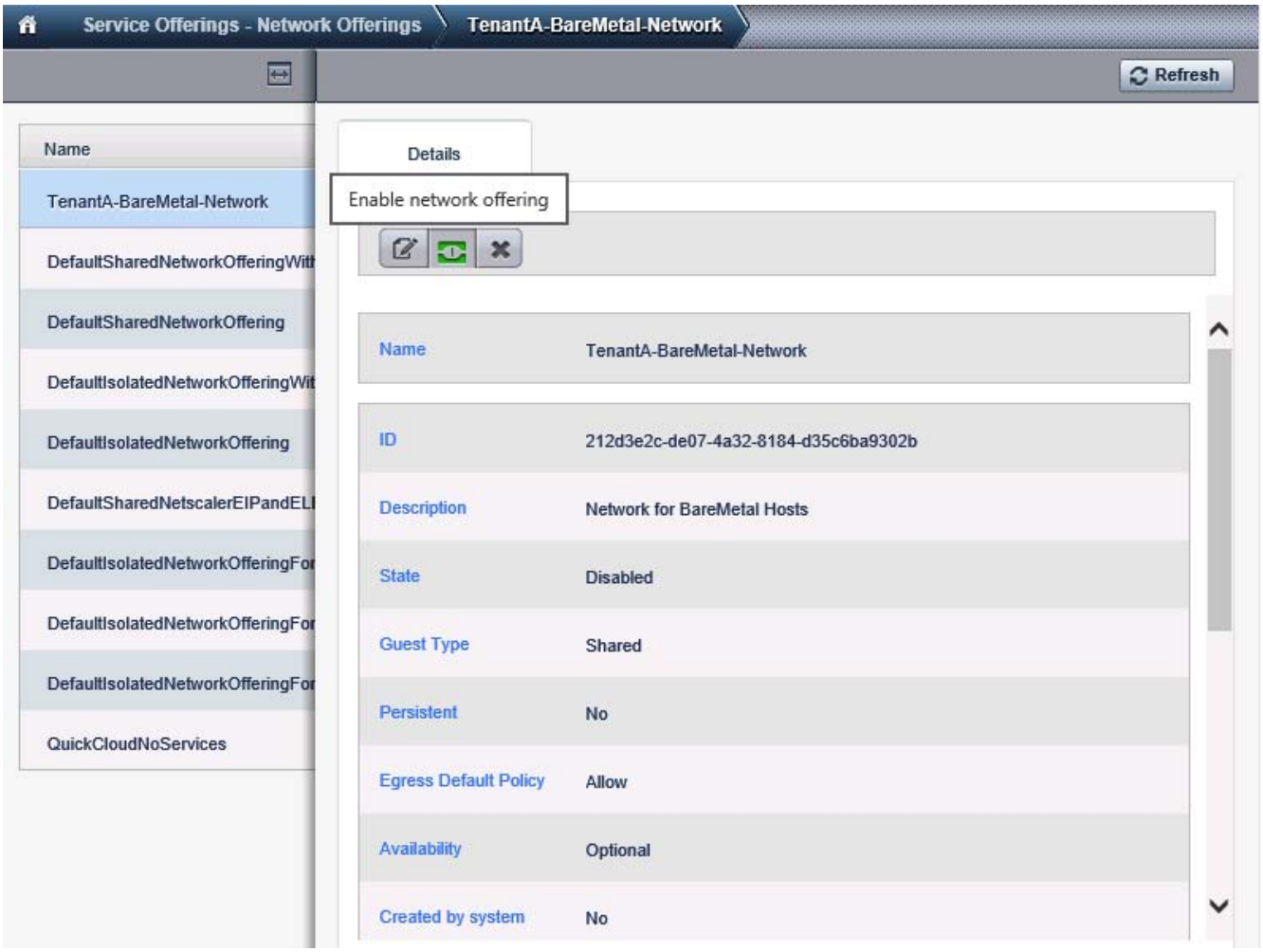
16. [User Data Provider] リスト ボックスで [BaremetalUserdataProvider] を選択します。
17. [BaremetalPxeService] チェックボックスをオンにします。
18. [OK] をクリックします。

図 293　Baremetal ネットワーク オファリングの設定



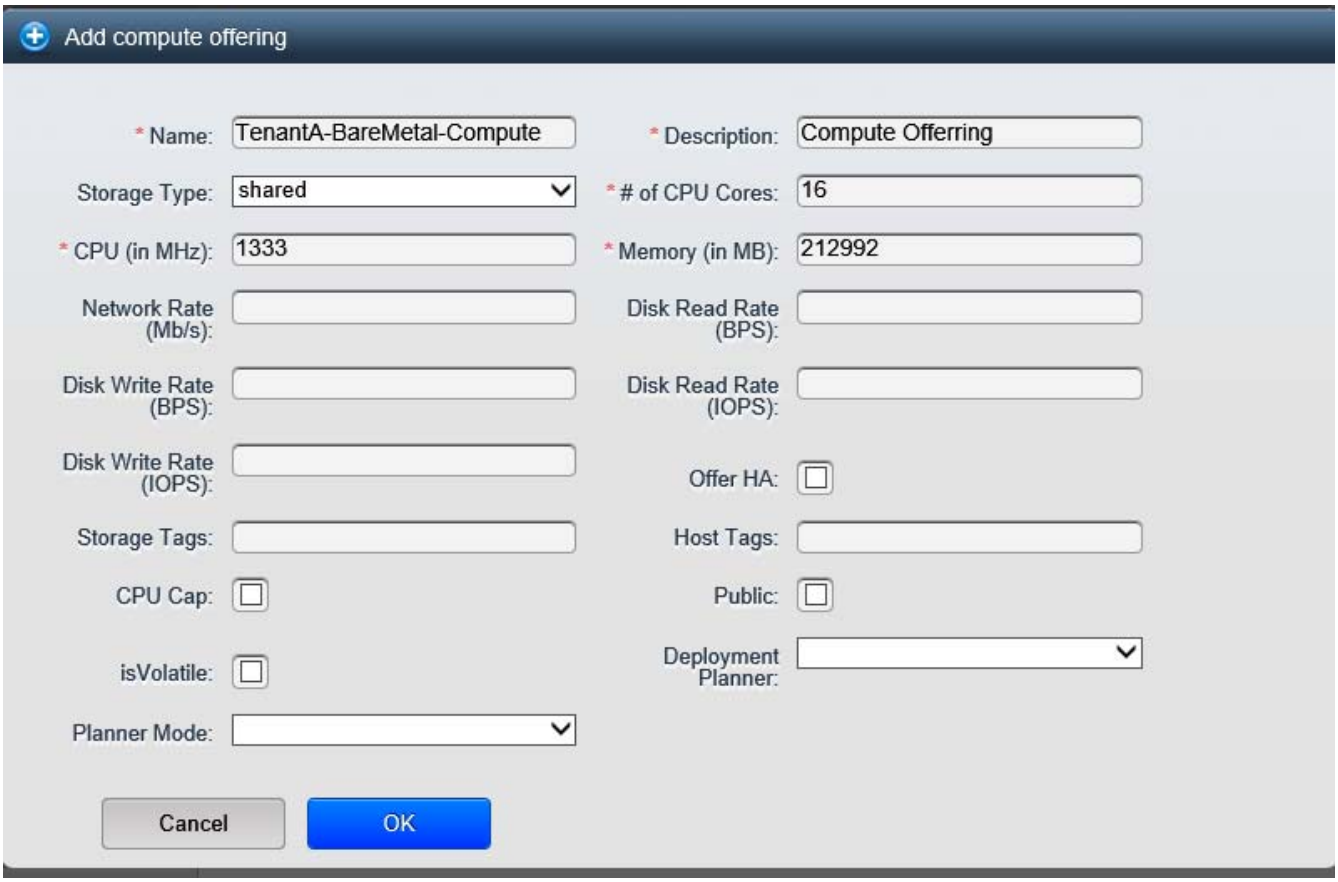
19. [TenantA-BareMetal-Network] および [Enable Network] を選択します。

図 294　TenantA-BareMetal-Network オファリングの有効化



20. 左ペインで、[Service Offerings] をクリックします。
21. 右ペインの [Select Offering] リスト ボックスで、[Compute Offering] を選択します。
22. [Add Compute offering] をクリックします。
23. [Name] フィールドに TenantA-BareMetal-Compute と入力します。
24. [Description] フィールドに Compute Offering と入力します。
25. [Storage Type] フィールドに Shared と入力します。
26. [CPU Cores] フィールドに <Physical_Blade_CPU_Core> 16 と入力します。
27. [CPU Mhz] フィールドに <Physical_Blade_CPU_Mhz> 1333 と入力します。
28. [Memory (MB)] フィールドに <Physical_Blade_Memory> 212992 と入力します。
29. [OK] をクリックします。

図 295　Baremetal コンピュート オファリングの設定



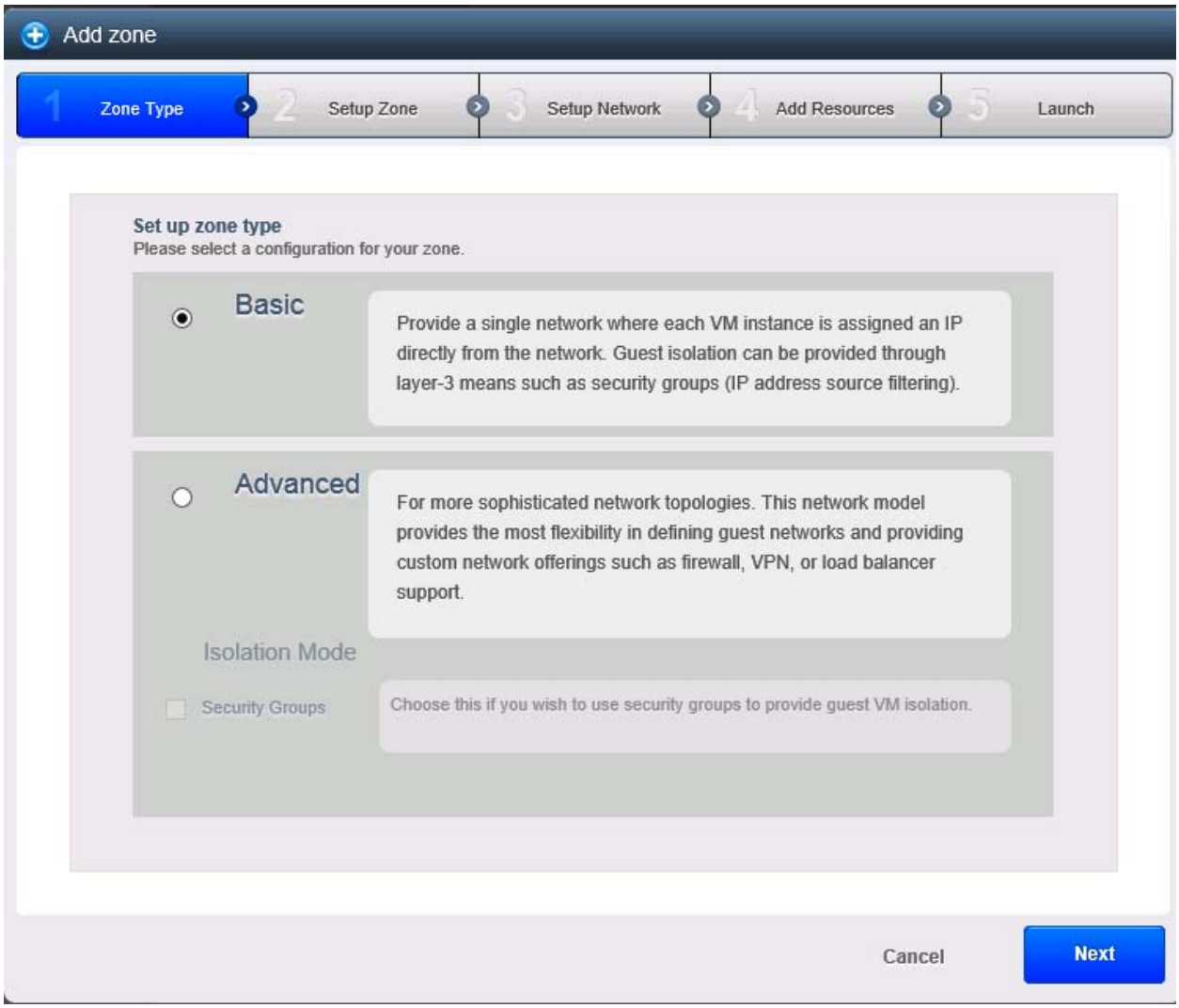
ゾーンの定義

1. 左ペインで [Infrastructure] タブが選択された状態で、右ペインの [Zones] で [View all] をクリックします。
2. [+ Add Zone] をクリックします。

図 296　インフラストラクチャ ページの表示

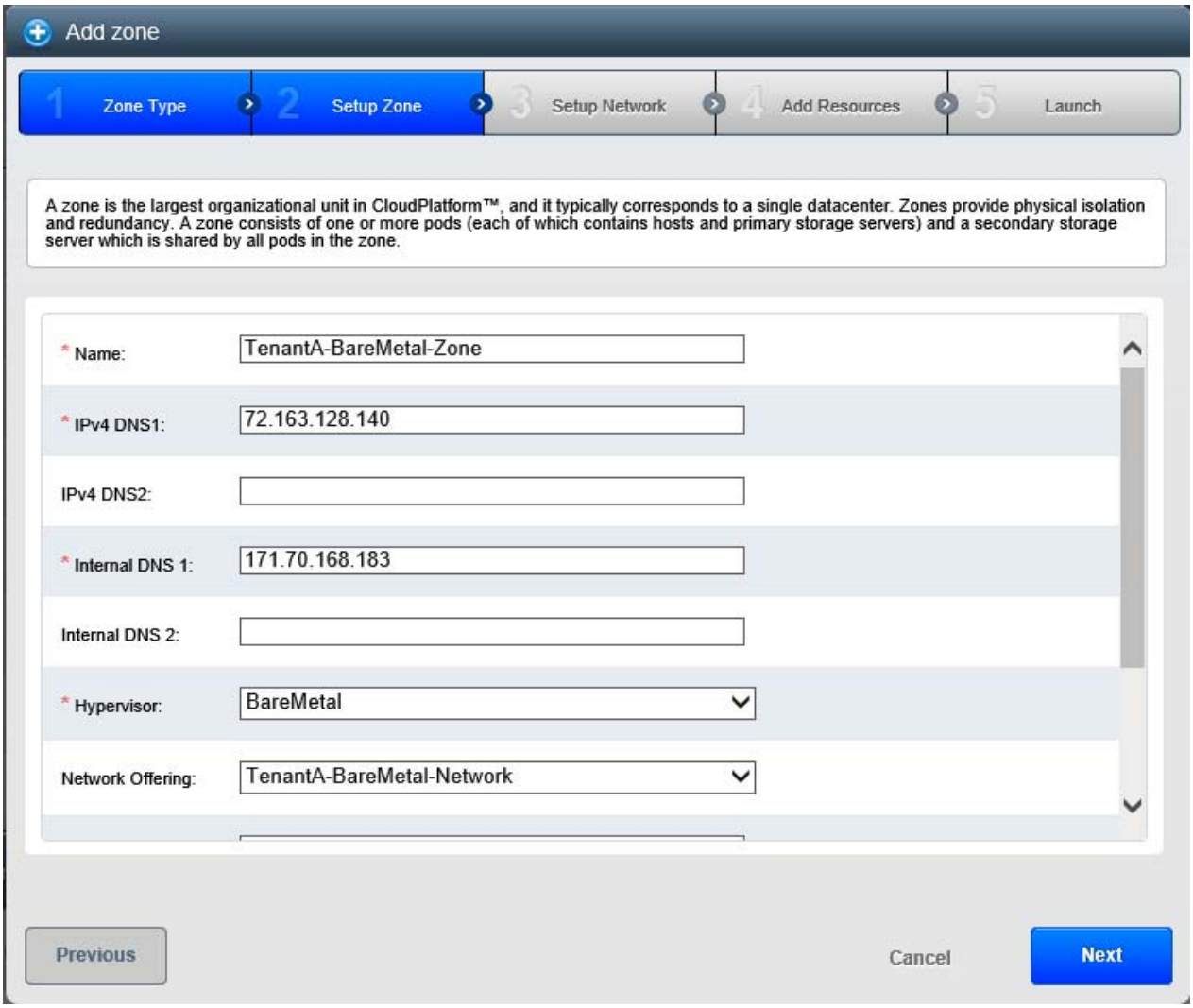
3. [Basic zone type] オプション ボタンをクリックします。
4. [Next] をクリックします。

図 297　　基本ゾーン設定の定義



5. [Name] フィールドに TenantA-BareMetal-Zone と入力します。
6. [DNS1] フィールドに <Public_DNS_IP_Address>72.163.128.140 と入力します。
7. [Internal DNS 1] フィールドに 171.70.168.183 と入力します。
8. [Hypervisor] で、リスト ボックスから [BareMetal] を選択します。
9. [Network Offering] で、TenantA-BareMetal-Network を選択します。
10. [Next] をクリックします。

図 298　　ゾーン属性の定義



ネットワークの定義

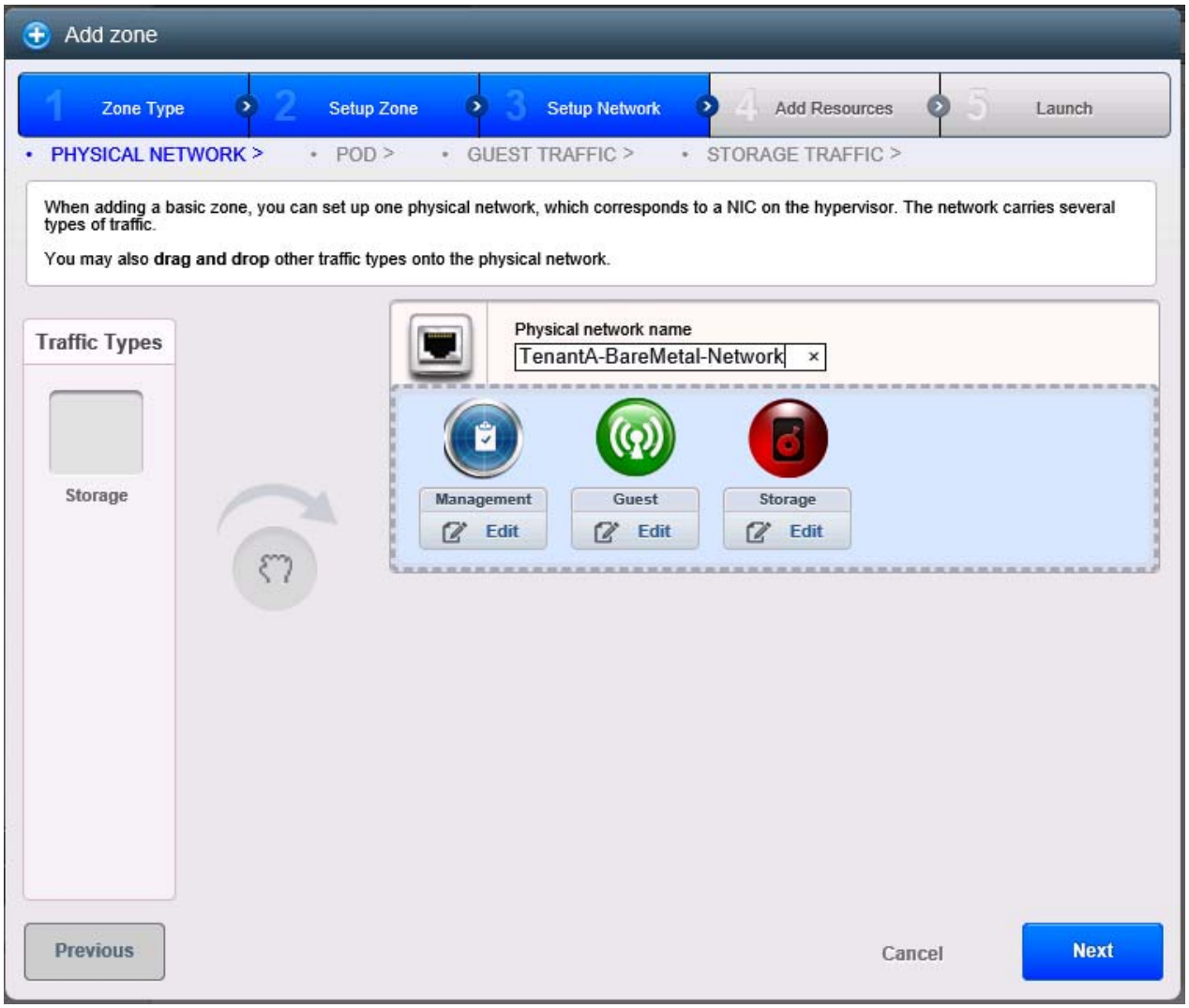
ゾーン定義後の次のステップは、クラウド ネットワークを設計および定義することです。Baremetal ホストは、ベーシック ネットワークをサポートするゾーンにのみ追加できるので、このソリューション設計はベーシック ネットワーキングを実装します。ゲストおよび管理トラフィック タイプを伝送する 1 つの物理ネットワークがゾーンで定義されます。

- 管理トラフィック：内部リソースが互いに通信するときに CloudPlatform 内で生成されます。これにはホスト間の通信が含まれます。
- ゲスト プライベート トラフィック：Baremetal ホストによって使用および生成されます。ゲスト ネットワークは、Baremetal ホストがネットワーク経由で互いに通信するときに発生します。

クラウド サービスをホストする TenantA-BareMetal マルチテナントに専用の Citrix CloudPlatform アプリケーションを使用して、ゾーンのベーシック ネットワークを設定するには、次の手順を実行します。

1. ゲストのパブリックとプライベート トラフィック タイプ アイコンおよびストレージ タイプ アイコンを [Physical Network 2] にドラッグします。
2. [Physical network name] フィールドで、物理ネットワーク Network 1 の名前を TenantA-BareMetal-Network に変更します。
3. [Next] をクリックします。

図 299　　ゾーンのベーシック ネットワーキング設定の定義



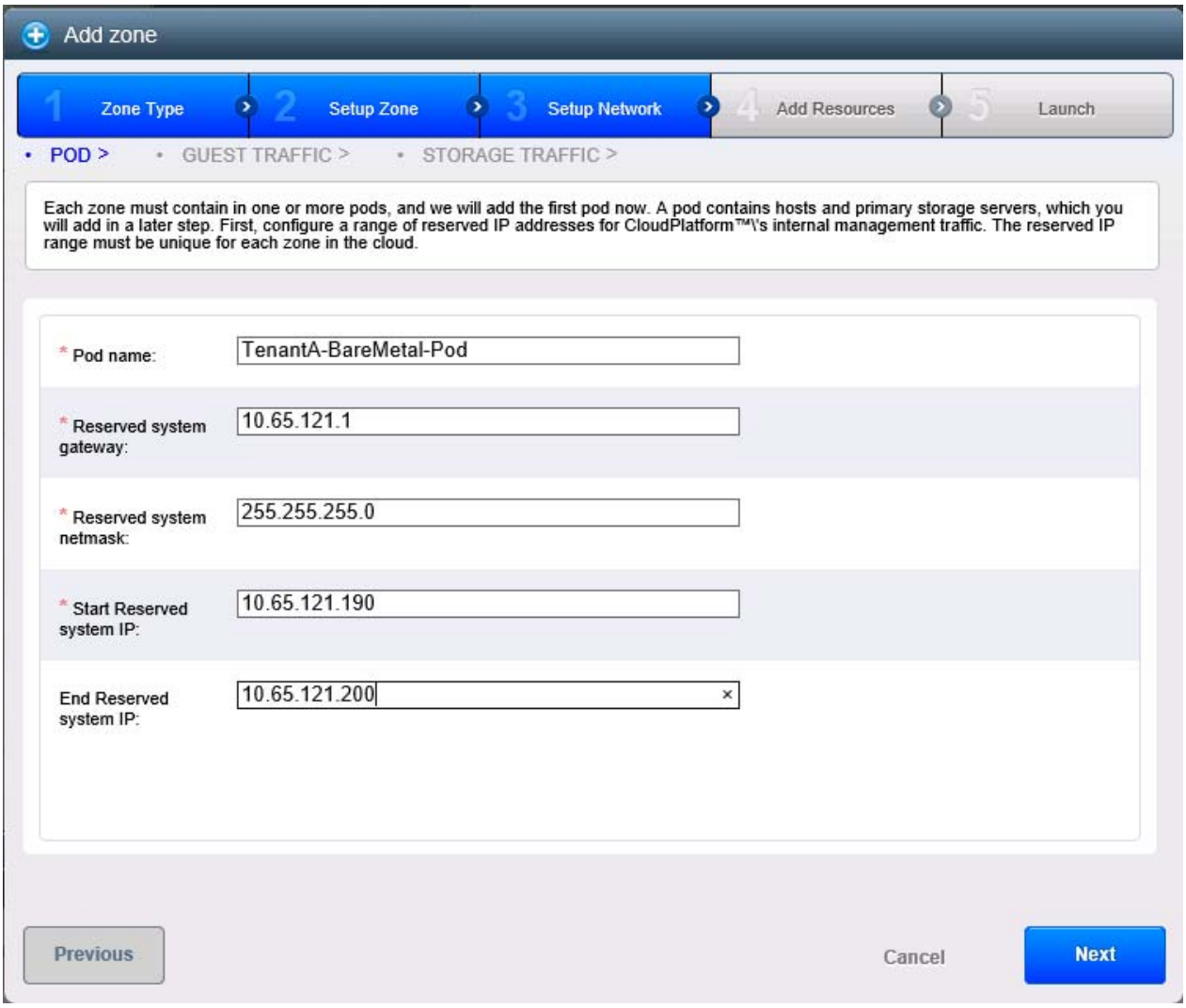
Pod の追加

Pod は、CloudPlatform 導入における 2 番目に大きな組織単位です。Pod はゾーン内に含まれています。各ゾーンは 1 つ以上の Pod を含むことができます。Pod は、ホストの 1 つ以上のクラスタおよび 1 つ以上のプライマリ ストレージ サーバから構成されます。

クラウド サービスをホストする TenantA-BareMetal マルチテナントに専用の Citrix CloudPlatform アプリケーションを使用して、ゾーンのアドバンスド ネットワーク設定に Pod ネットワークを追加するには、次の手順を実行します。

1. [Name] フィールドに TenantA-BareMetal-Pod と入力します。
2. [Reserved System Gateway] フィールドに <Management_VLAN_602_GW_IP_Address>10.65.121.1 と入力します。
3. [Reserved System netmask] フィールドに 255.255.255.0 と入力します。
4. [Start Reserved system IP] フィールドに 10.65.121.190 と入力します。
5. [End Reserved system IP] フィールドに 10.65.121.200 と入力します。
6. [Next] をクリックします。

図 300　　ゾーンへの Pod の追加

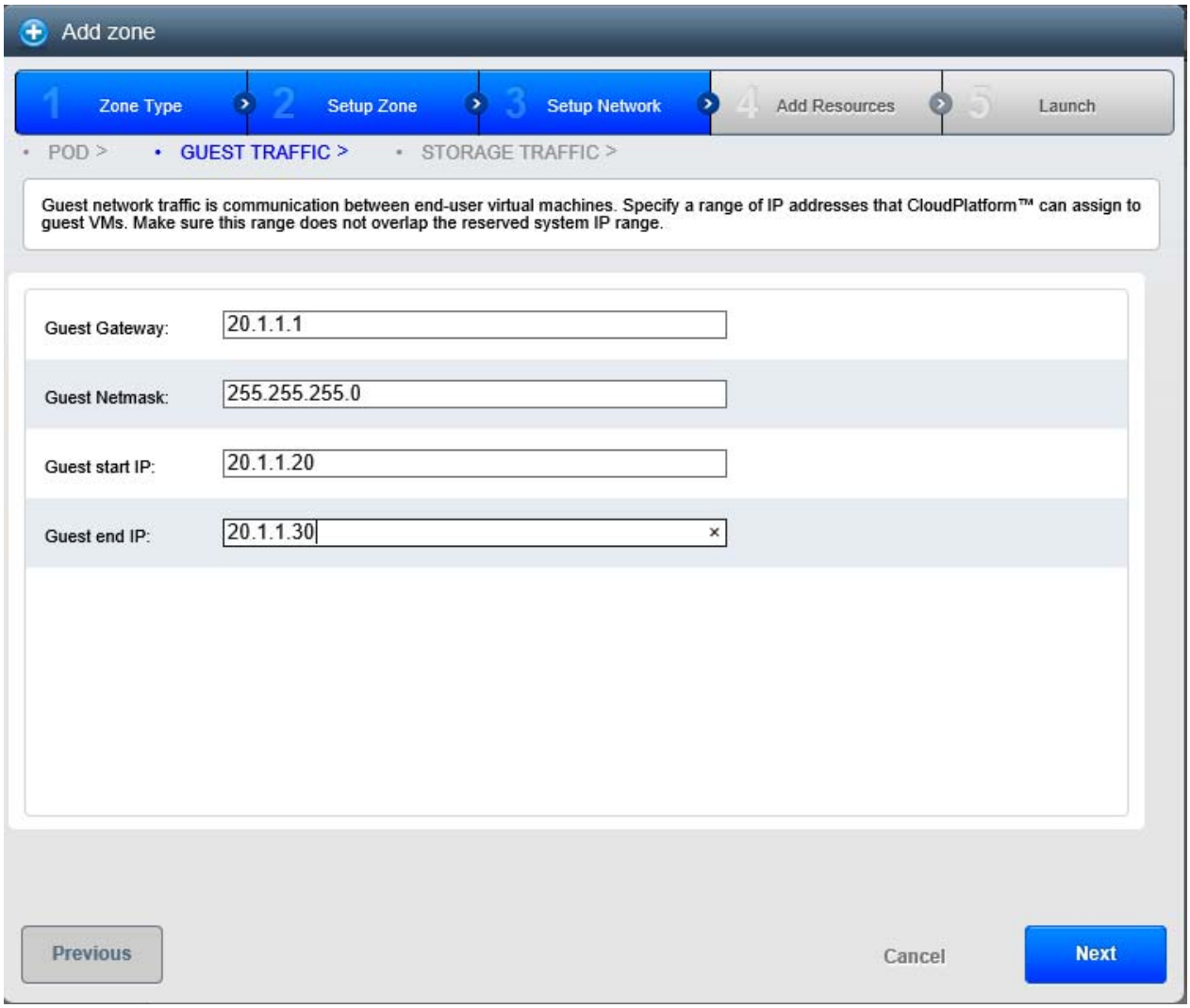


ゲスト トラフィックの追加

クラウド サービスをホストする TenantA-BareMetal マルチテナントに専用の Citrix CloudPlatform アプリケーションを使用して、ゾーンのベーシック ネットワーク設定にゲスト ネットワークを追加するには、次の手順を実行します。

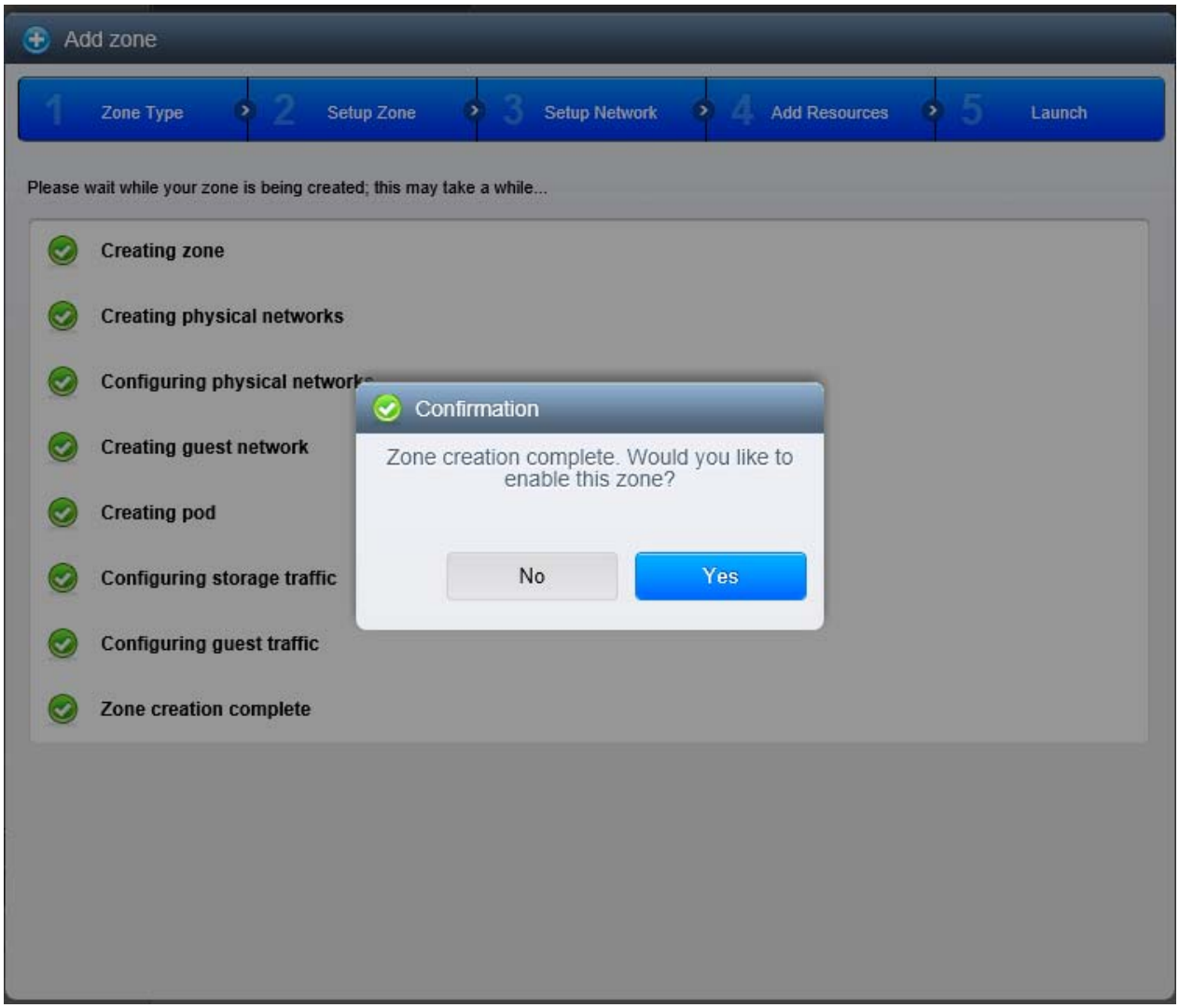
1. [Gateway] フィールドに <guest_VLAN20_GW_IP_Address>20.1.1.1 と入力します。
2. [Netmask] フィールドに 255.255.255.0 と入力します。
3. [Start IP] フィールドに 20.1.1.20 と入力します。
4. [End IP] フィールドに 20.1.1.30 と入力します。
5. [Next] をクリックします。

図 301　　ゲストの VLAN 範囲の設定



6. ゾーンの作成に対して [Yes] をクリックします。

図 302　　ソーンの作成の確認



Cisco UCS Manager プラグインの追加

ベア メタル ホストとして使用するために Cisco UCS サーバ ブレードを CloudPlatform にプロビジョニングできます。UCS 統合型インフラストラクチャのプログラマビリティ、および、CloudPlatform のクラウド アーキテクチャの知識と調整能力を活用することで、クラウドを簡単に拡張できるようにするためです。CloudPlatform は UCS 環境やサーバ プロファイルなどを自動的に把握するので、CloudPlatform 管理者は Cisco UCS 上にベア メタルを導入できます。

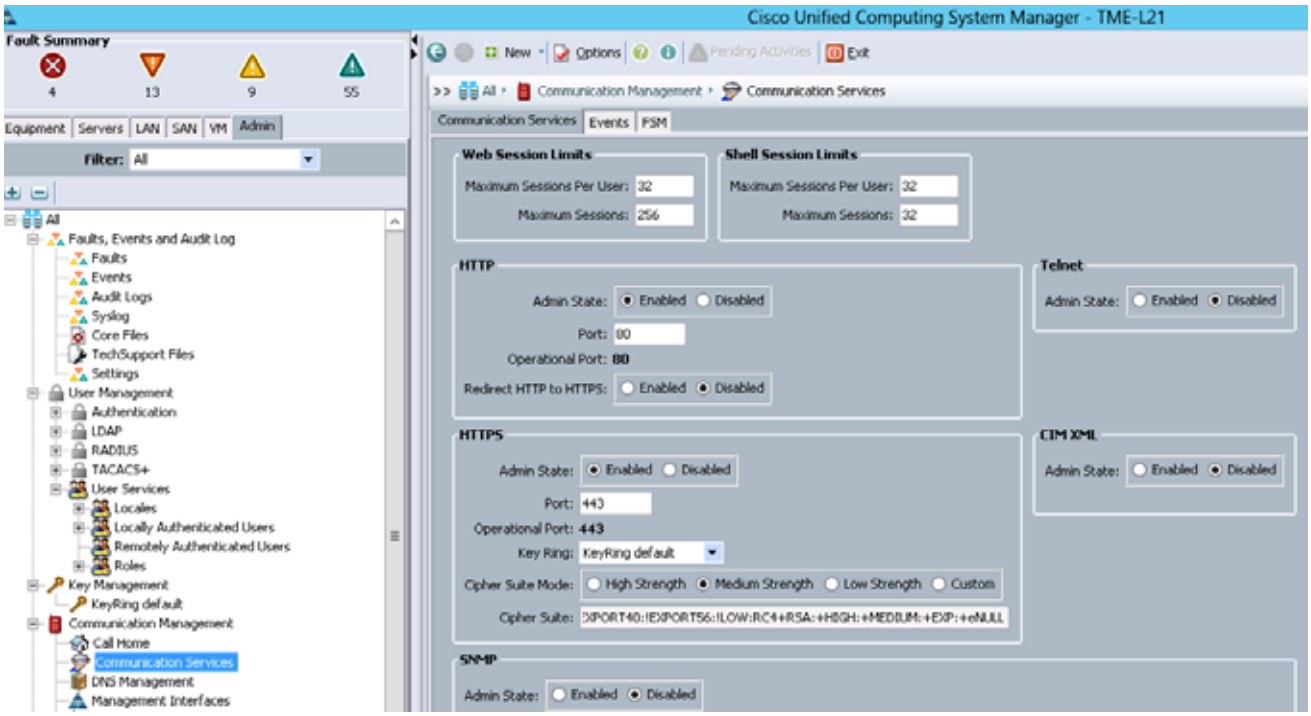
ここでは、Cisco UCS Manager プラグインを使用して Cisco UCS Manager を CloudPlatfrom に登録します。ハードウェア インベントリを実行して、使用可能なブレードとそのステータス（サービス プロファイルの関連付け / 関連付け解除）を表示します。

CloudPlatfrom 管理者は、空き（関連付けなし）のブレードを選択し、Cisco UCS Manager によってすでに定義されているサービス プロファイル テンプレートに基づいてサービス プロファイルを作成できます。CloudPlatfrom 管理者は、Cisco UCS Manager API 呼び出しをトリガーし、サービス プロファイル テンプレート関連付けブレードに基づいてサービス プロファイルを作成します。

ブレードの関連付けに成功すると、CloudPlatfrom は、PXE のブートを使用して RHEL 6.3 オペレーティング システムをインストールすることで、Baremetal as a Service のプロビジョニングを実行します。

1. CloudPlatfrom は Cisco UCS Manager にアクセスするために HTTP および HTTPS プロトコルを有効にする必要があるので、Cisco UCS Manager 通信サービスの [HTTP Admin State] が **<enabled>** に、[Redirect HTTP to HTTPS] が **<disabled>** になっていることを確認します。

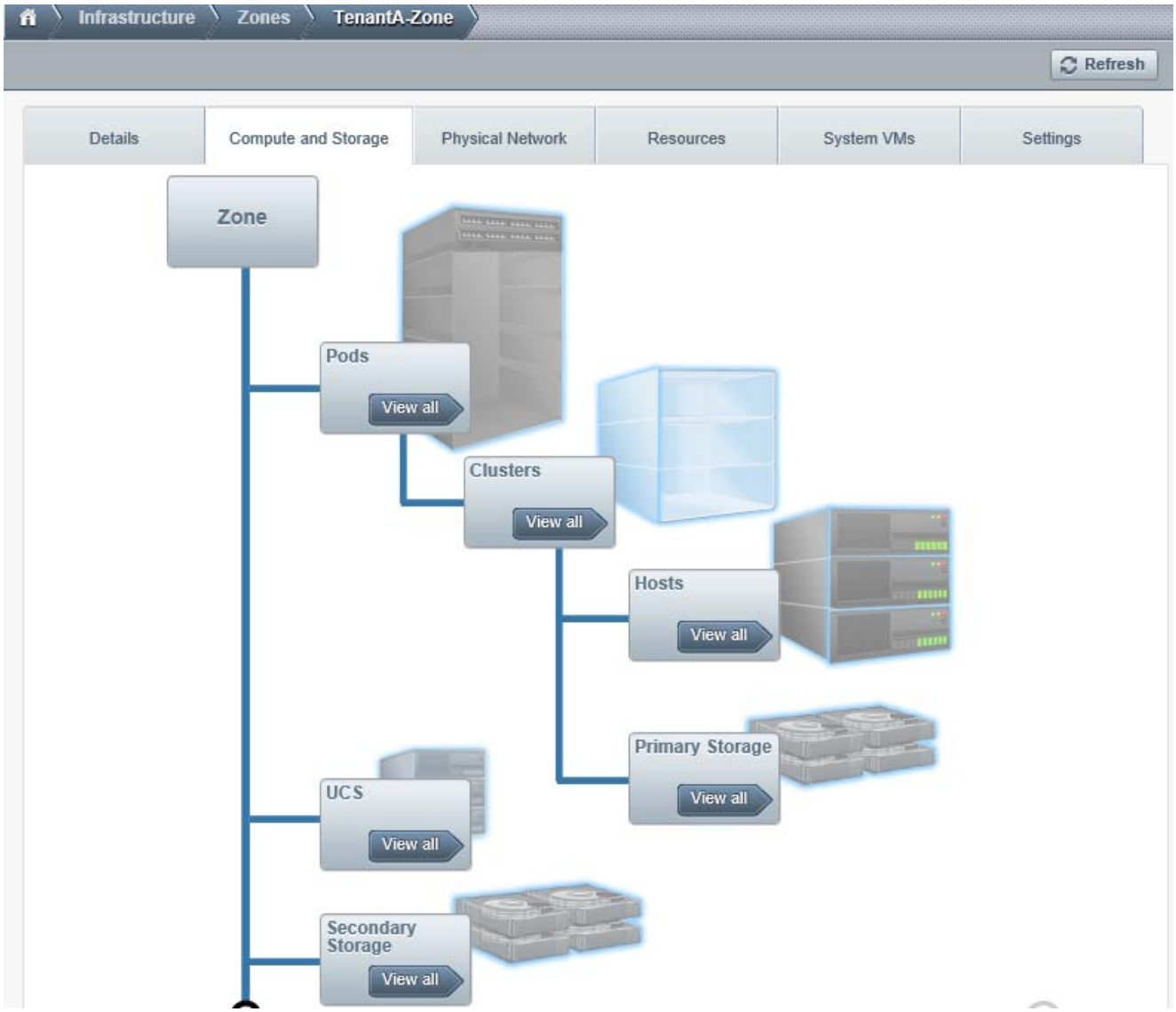
図 303　　Cisco UCS Manager 通信サービスの HTTP 設定の詳細



ユーザ資格情報を使用して CloudPlatform にログインして、TenantA-BareMetal-Zone ゾーンで Cisco UCS Manager プラグインを設定します。

1. [Login] をクリックします。
2. 左ペインで [Infrastructure] タブをクリックします。
3. [Zones] の [View All] をクリックします。
4. [<TenatA-BareMetal-Zone> Zone] をクリックします。
5. [Compute and Storage] をクリックします。
6. [UCS View All] をクリックします。

図 304　　Cisco UCS Manager の追加の詳細

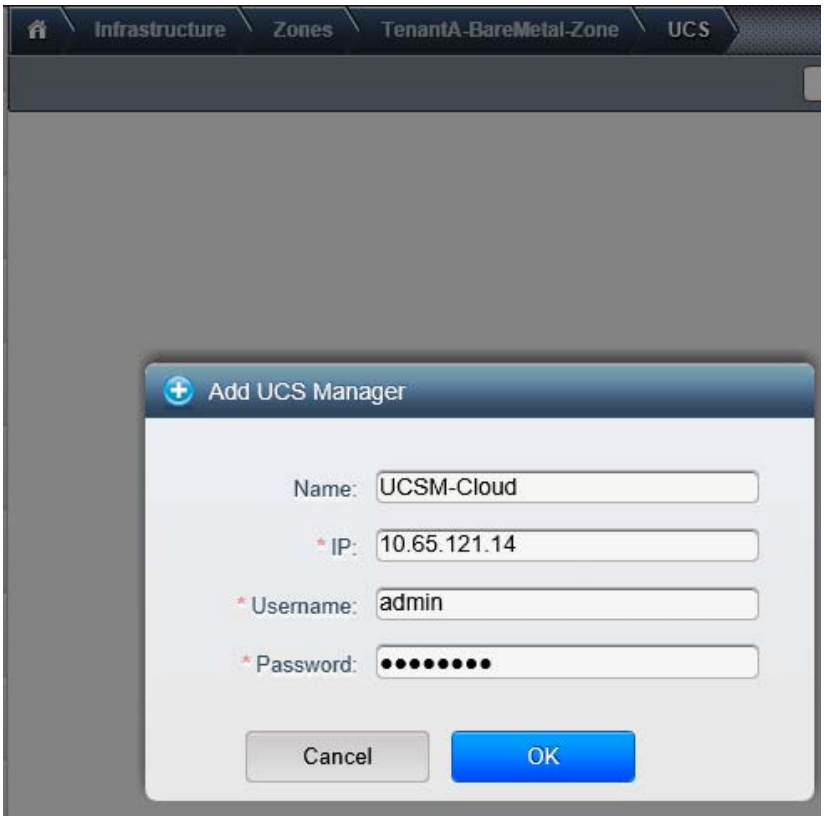


7. [Add Cisco UCS Manager] をクリックします。
8. [Name] に <Cisco UCS Manager-Cloud> と入力します。
9. [URL] に UCS クラスタの IP アドレス **<10.65.121.14>** を入力します。

（注）　IP アドレスのみ入力します。

10. [UserName] に <admin> と入力します。
11. [Password] に <xxxxx> と入力します。
12. [OK] をクリックします。

図 305　Cisco UCS Manager プラグインの設定の表示



13. [Cisco UCS Manager-Cloud] を選択します。

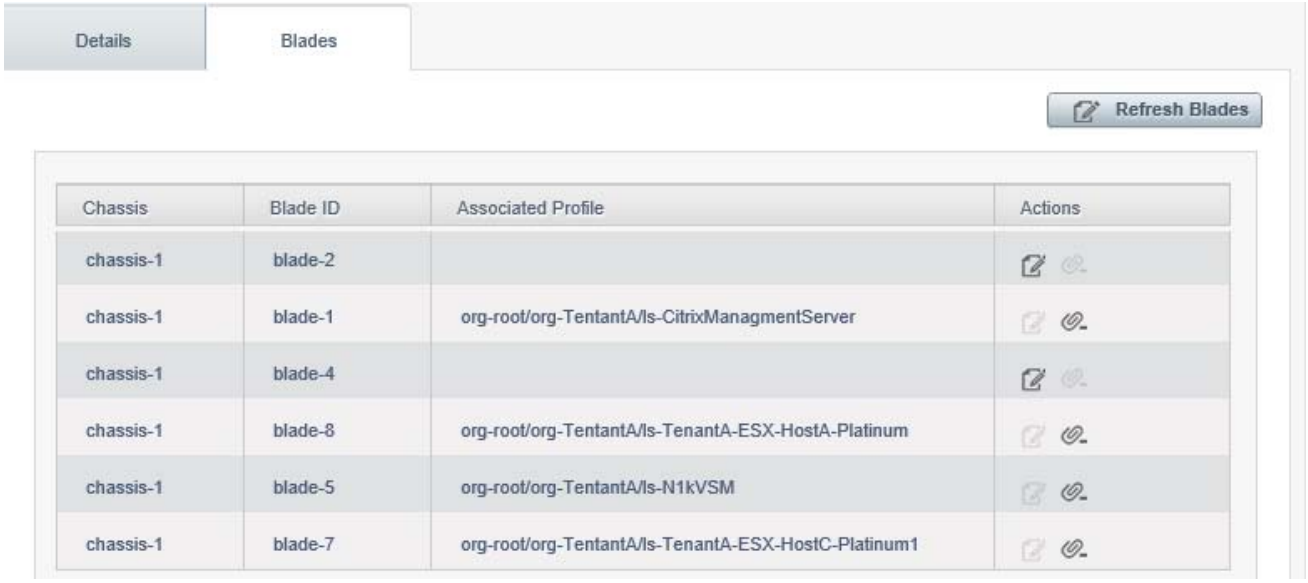
図 306　Cisco UCS Manager プラグインへのアクセス

14. [Blades] をクリックします。

15. 現在の CloudPlatfrom 4.2.1 は、Baremetal ホストをプロビジョニングするために、サービス プロファイルに関連付けられている、またはサービス プロファイルとの関連付けに使用できる、すべてのブレードを表示します。CloudPlatfrom 4.2.1 では、Cisco UCS Manager で作成されたサービス プロファイル テンプレートを使用して取得されるサービス プロファイルを作成することで、使用可能なブレードを自由に関連付けることができます。

（注） 現在の CloudPlatfrom 4.2.1 バージョンでは、Cisco UCS Manager プラグインを使用する場合、Cisco UCS Manager の Root Org で作成されたサービス プロファイル テンプレートから取得されるサービス プロファイルにのみブレードを関連付けることができるので、CloudPlatfrom Manager に公開するには Cisco UCS Manager プラグインの Root Org でサービス プロファイル テンプレートを作成したことを確認してください。また、Baremetal プロビジョニングを開始する前にブレードをリフレッシュすることを推奨します。

図 307　使用可能な物理ブレードのインベントリを表示する Cisco UCS Manager



16. [Blade-2] の [Action] で、[Associate Profile to Blade] をクリックします。

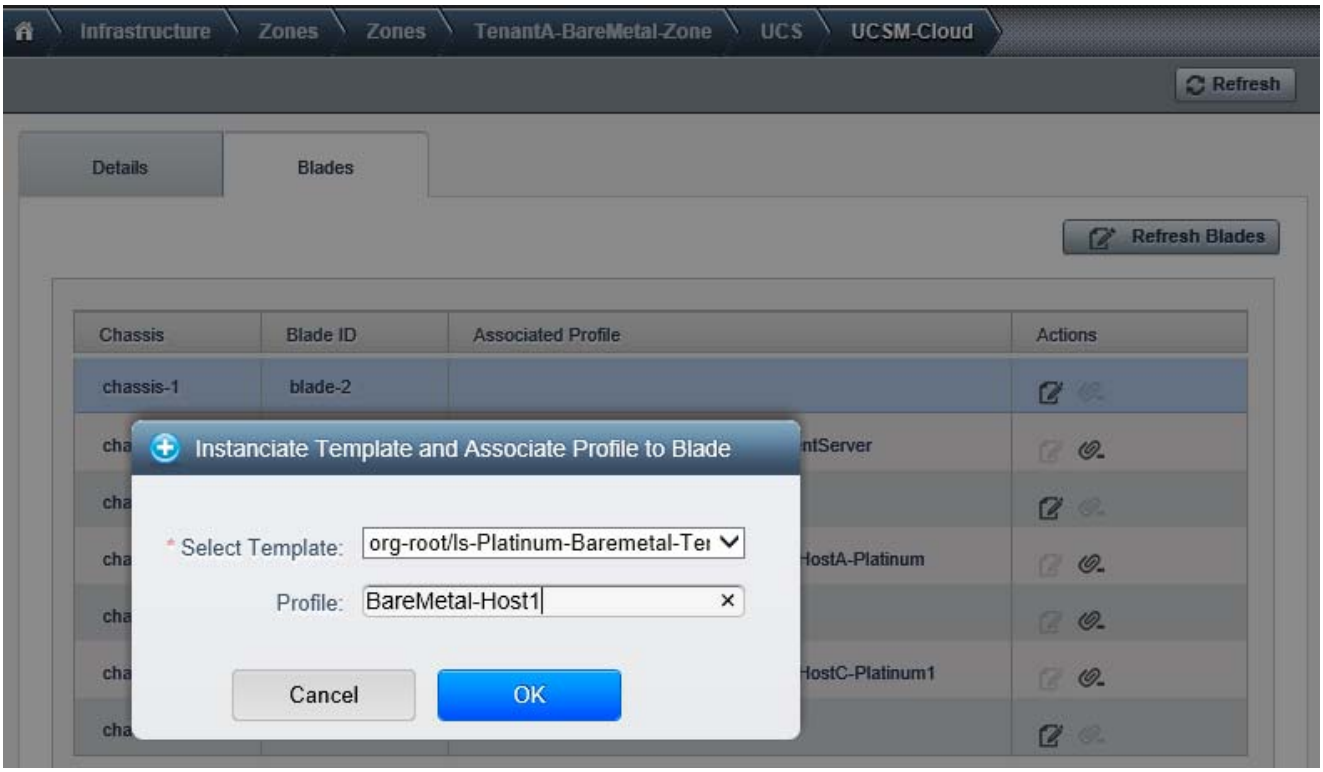
図 308　blade -2 を選択して Cisco UCS Manager のサービス プロファイルに関連付ける

17. [Select Template] リスト ボックスで [Platinum-Baremetal-Template] を選択します。

18. [Profile Name] フィールドに **BareMetal-Host1** と入力します。

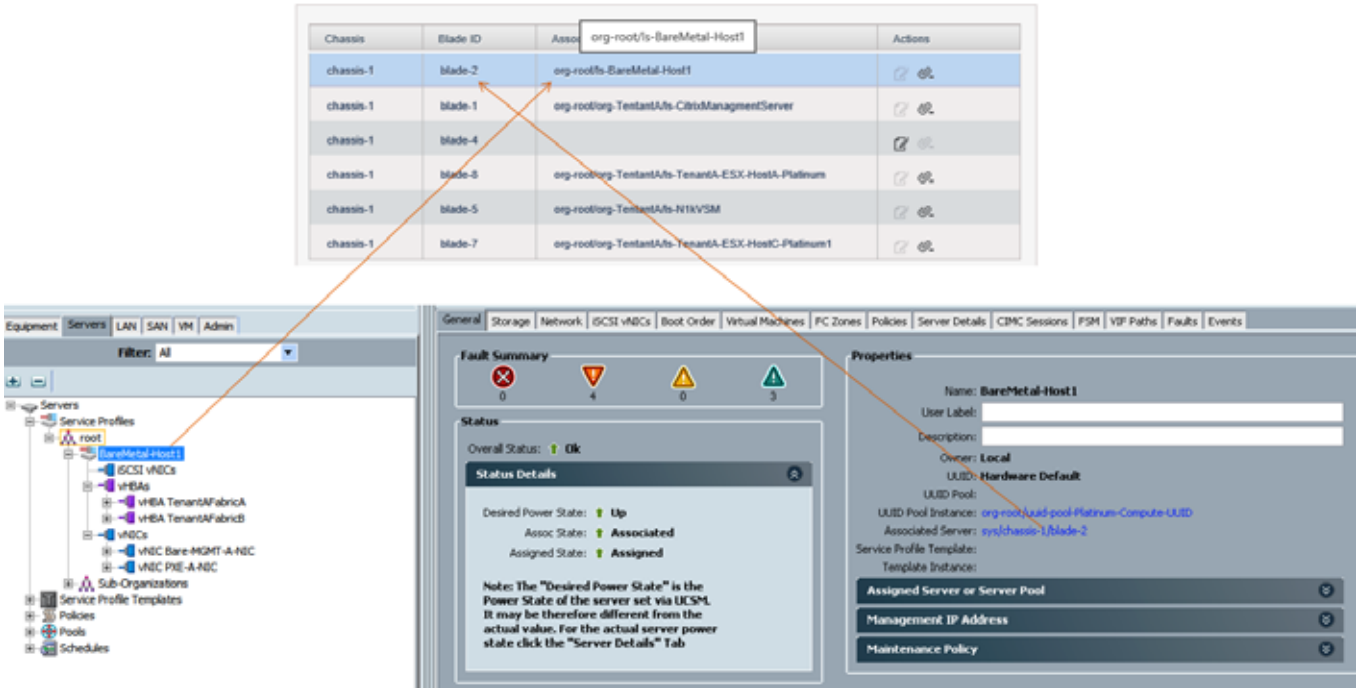
19. [OK] をクリックします。

図 309　blade-2 に関連付けるために Platinum-Baremetal-Template を選択して BareMetal-Host1 サービス プロファイルを作成する



20. 図 310 は、サービス プロファイル BareMetal-Host1 を Blade 2 に関連付けた後の、Cisco UCS Manager と CloudPlatfrom のマッピング設定を示しています。

図 310　blade-2 に関連付けられた BareMetal-Host1 サービス プロファイルを表示する Cisco UCS Manager と CloudPlatfrom



クラスタの追加

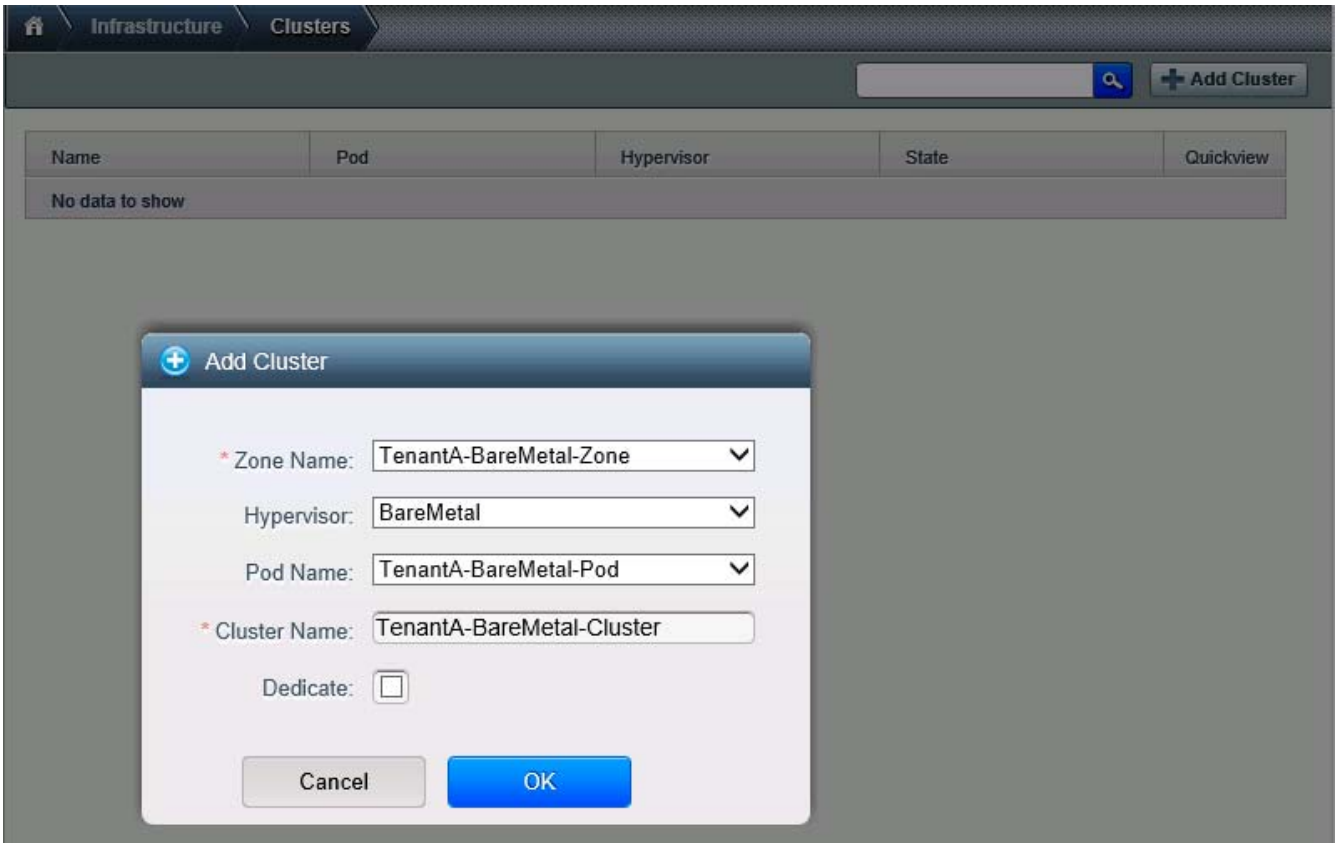
クラスタはホストをグループ化する方法を提供します。具体的にはここで、クラスタの Baremetal ホスト部分のセットを含むクラスタを使用します。クラスタ内のホストはすべて、同じハードウェアを持ち、同じ Baremetal オペレーティング システムを実行し、同じサブネット上に存在し、同じ共有プライマリ ストレージにアクセスします。

クラスタは、CloudPlatform 導入における 3 番目に大きな組織単位です。クラスタは Pod 内に含まれ、Pod はゾーン内に含まれています。クラスタのサイズは基盤となるハイパーバイザによって制限されていますが、ほとんどの場合 CloudPlatform ではより小さいサイズを推奨します。クラスタは、1 つ以上のホストおよび 1 つ以上のプライマリ ストレージ サーバから構成されます。

クラウド サービスをホストするために TenantA マルチテナントに専用の Citrix CloudPlatform アプリケーションを使用して、ゾーンにクラスタを追加するには、次の手順を実行します。

1. [Zone Name] リスト ボックスで [<TenantA-BareMetal-Zone>] を選択します。
2. [Hypervisor] リスト ボックスで [<BareMetal>] を選択します。
3. [Pod Name] リスト ボックスで [<TenantA-BareMetal-Pod>] を選択します。
4. [Cluster Name] フィールドに <TenantA-BareMetal-Cluster> と入力します。
5. [Next] をクリックします。

図 311　　ゾーンへのクラスタの追加



ホストの追加

ホストは、Baremetal オペレーティング システムを実行するコンピューティング リソースを提供します。各ホストには Baremetal Linux ベースの OS がインストールされ、アプリケーションを管理します。ここにあるホストは RHEL 6.3 ベースのサーバです。ホストは、CloudPlatform 導入における最小の組織単位です。ホストはクラスタ内に含まれ、クラスタは Pod 内に含まれ、Pod はゾーン内に含まれています。

クラウド サービスをホストする TenantA-BareMetal マルチテナントに専用の Citrix CloudPlatform アプリケーションを使用して、クラスタにホストを追加するには、次の手順を実行します。

1. [Zone Name] リスト ボックスで [<TenantA-BareMetal-Zone>] を選択します。
2. [Pod Name] リスト ボックスで [<TenantA-BareMetal-Pod>] を選択します。
3. [Cluster Name] フィールドに <TenantA-BareMetal-Cluster> と入力します。
4. [Host Name] フィールドに <UCS-IPMI-IP-Address> 10.65.121.57 と入力します。

（注）　[Host Name] の IP アドレスは、Cisco UCS Manager によって物理ブレードに割り当てられた CIMC IP アドレスで、Baremetal ホストとしてゾーンに追加されています。

5. [Username] フィールドに <admin> と入力します。

（注） admin ユーザ名は、Baremetal ホストのブレード部分に関連付けられたサービス プロファイルに適用されている、Cisco UCS Manager の IMPI ポリシーで作成されます。

6. [Password] フィールドに <XXXX> と入力します。

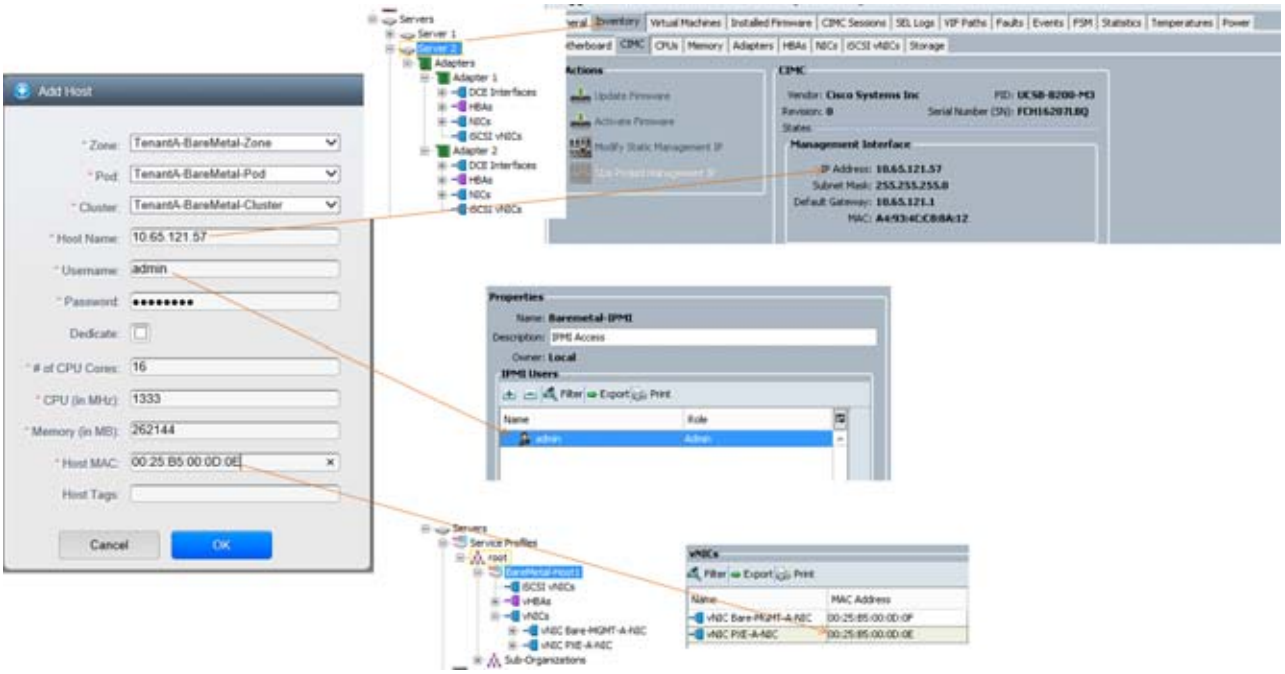
（注） パスワードは、Baremetal ホストのブレード部分に関連付けられたサービス プロファイルに適用されている、Cisco UCS Manager の IMPI ポリシーで作成されます。

7. [Dedicate] チェックボックスをオフにします。
8. [CPU Cores] フィールドに <Physical_Blade_CPU_Core> 16 と入力します。
9. [CPU (in MHz)] フィールドに <Physical_Blade_CPU_Mhz> 1333 と入力します。
10. [Memory (MB)] フィールドに <Physical_Blade_Memory> 262144 と入力します。
11. [Host MAC] フィールドに <00:25:b5:00:0D:0E> と入力します。

（注） The MAC Address < 00:25:b5:00:0D:0E > は、PXE のブート操作を処理する、サービス プロファイルの静的 vNIC に割り当てられます。

12. [OK] をクリックします。

図 312　　ゾーンへのホストの追加



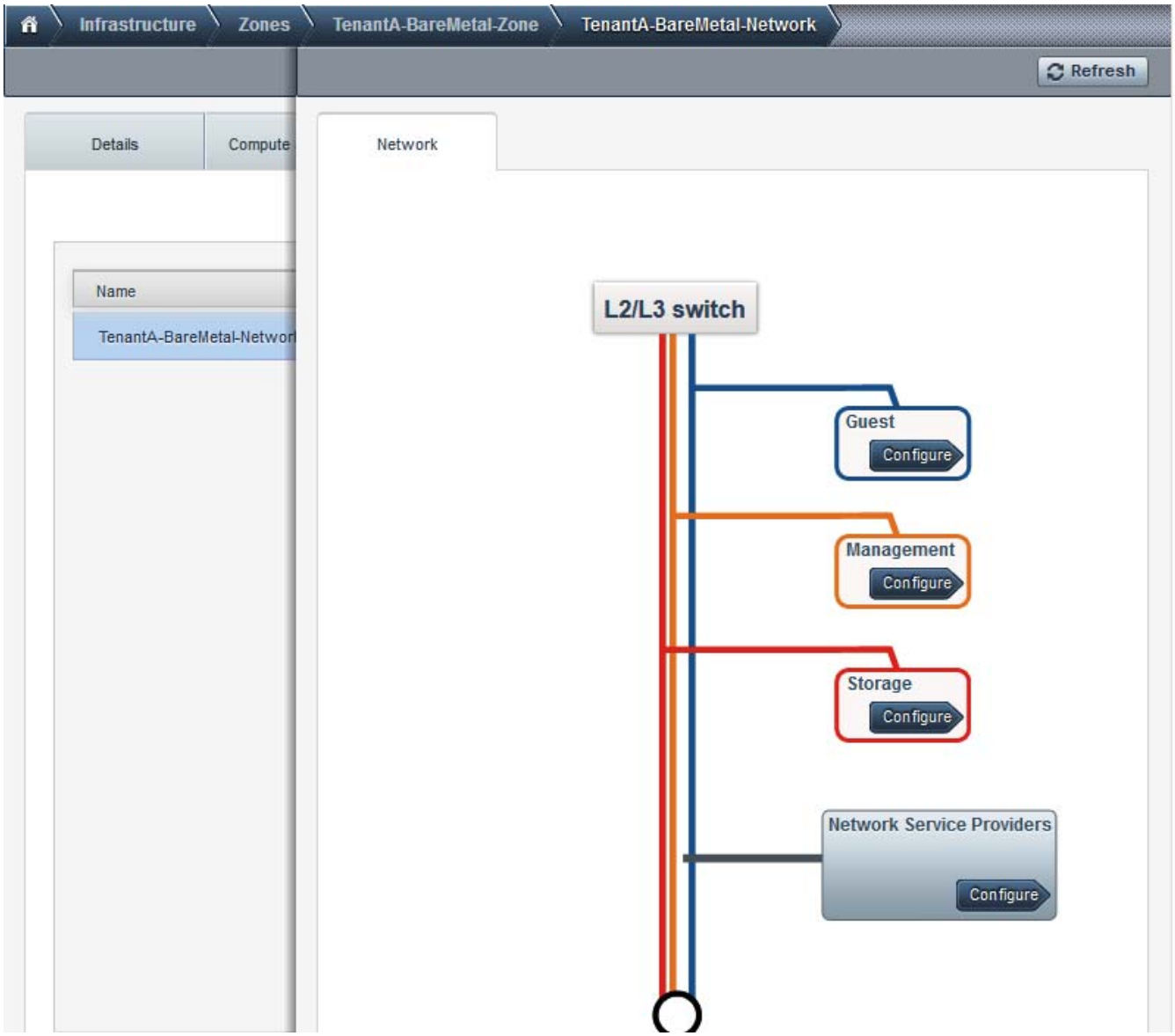
PXE および DHCP サーバの追加

物理サーバに対するオペレーティング システムの Baremetal ホスト PXE インストールをサポートするには、CloudPlatfrom 4.2.1 でアクセスする外部 PXE および DHCP サーバが必要です。PXE および DHCP のセットアップと設定については、クラウドの導入に関する項で参照できます。

ユーザ資格情報を使用して CloudPlatform にログインして、TenantA-BareMetal-Zone ゾーンで PXE および DHCP サーバを作成します。

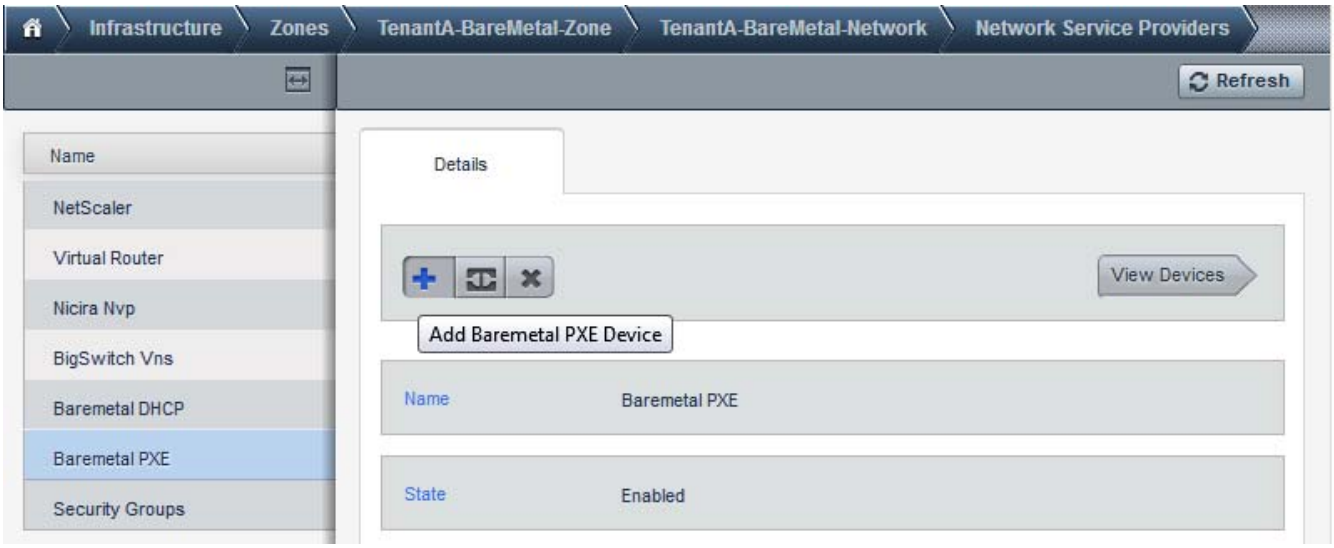
1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Infrastructure] タブをクリックします。
4. [Zones View all] をクリックします。
5. [TenantA-BareMetal-Zone] をクリックします。
6. [Physical Network] をクリックします。
7. [TenantA-BareMetal-Network] をクリックします。
8. [Configure Network Service Providers] をクリックします。

図 313　　DHCP および PXE サーバ設定の詳細



9. [Baremetal PXE] タブをクリックします。
10. [+ ADD] アイコンをクリックして Baremetal PXE デバイスを追加します。

図 314　Baremetal PXE サーバ設定の追加の詳細



11. [URL] フィールドに <BaremetalAgent_PXE_Server_IP_Address> http://20.1.1.5 と入力します。

（注） IP アドレス 20.1.1.5 が、CloudPlatfrom 4.2.1 Baremetal エージェントおよび PXE サービスが設定されているサーバに割り当てられます。

12. [Username] フィールドに <root> と入力します。

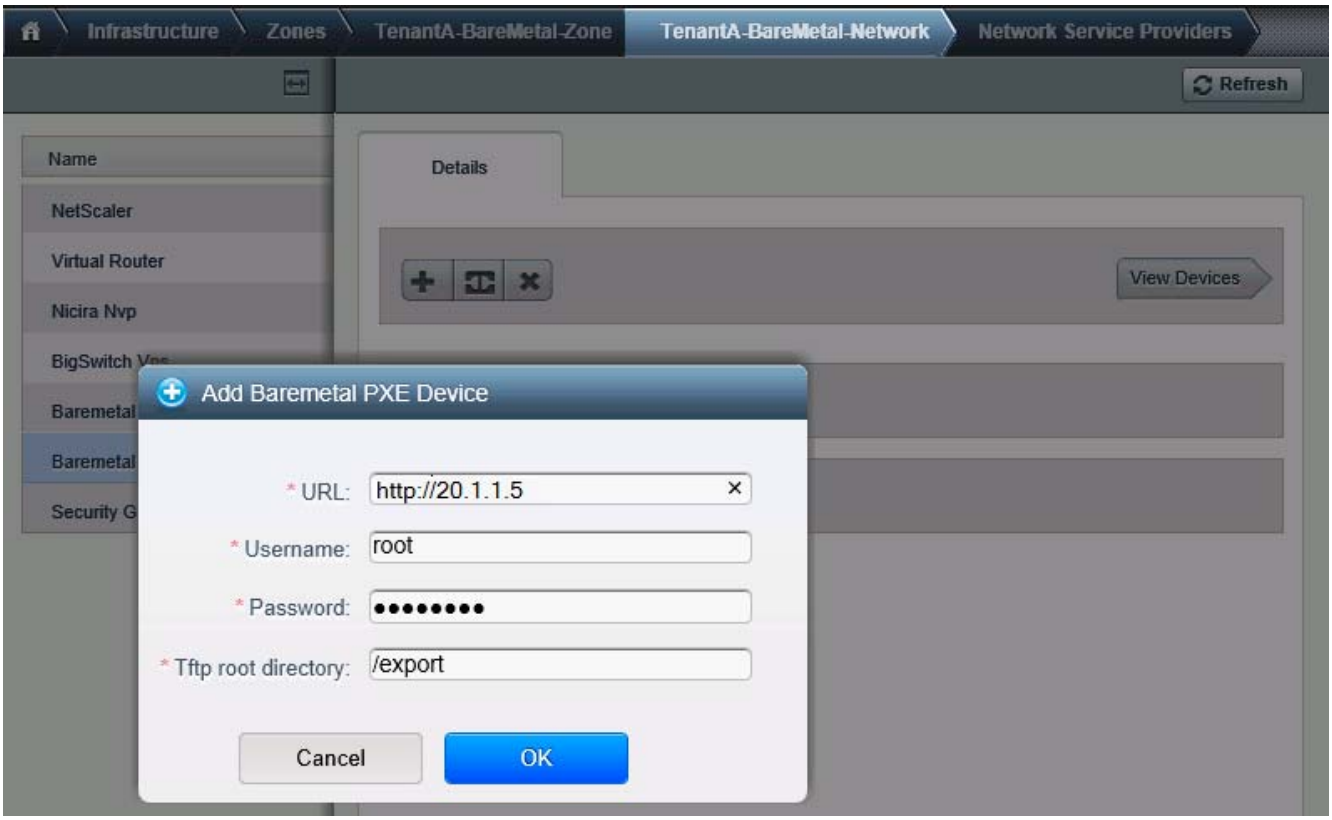
13. [Password] フィールドに <XXXXX> と入力します。

14. [Tftp root directory] に **</export>** と入力します。

（注） /export パスは、PXE および Baremetal OS イメージ ファイルが保存され、NFS エクスポートされる場所です。詳細については、クラウドの導入に関する項を参照してください。

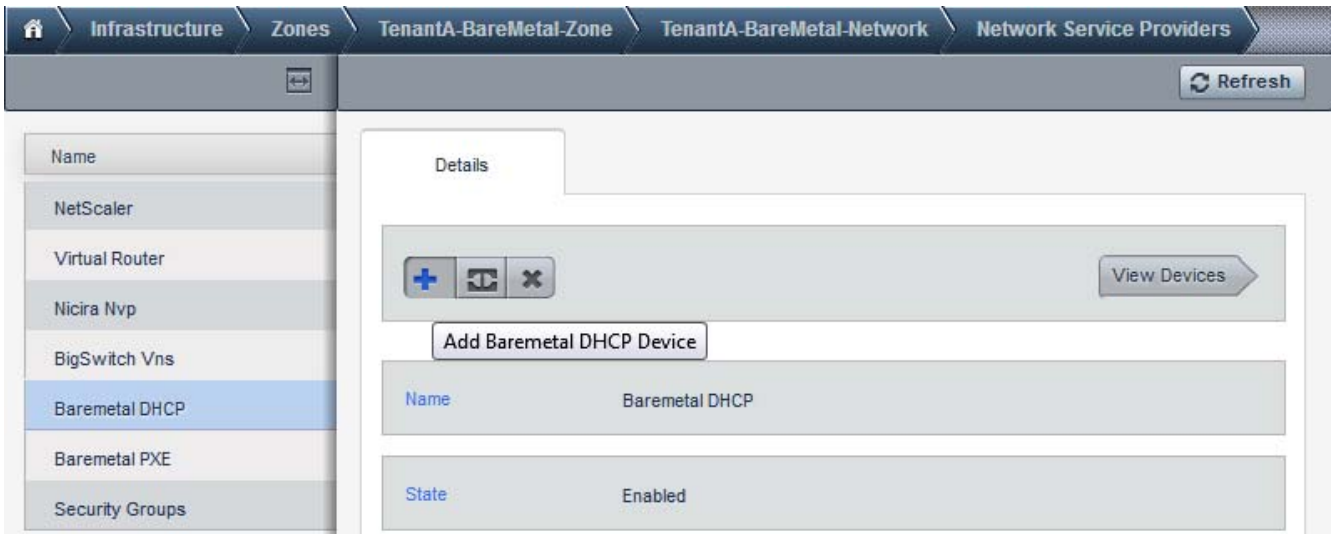
15. [OK] をクリックします。

図 315　Baremetal PXE サーバおよびパス設定の追加の詳細



16. [Baremetal DHCP] タブをクリックします。
17. [+ ADD] アイコンをクリックして Baremetal DHCP デバイスを追加します。

図 316　Baremetal DHCP サーバ設定の追加の詳細

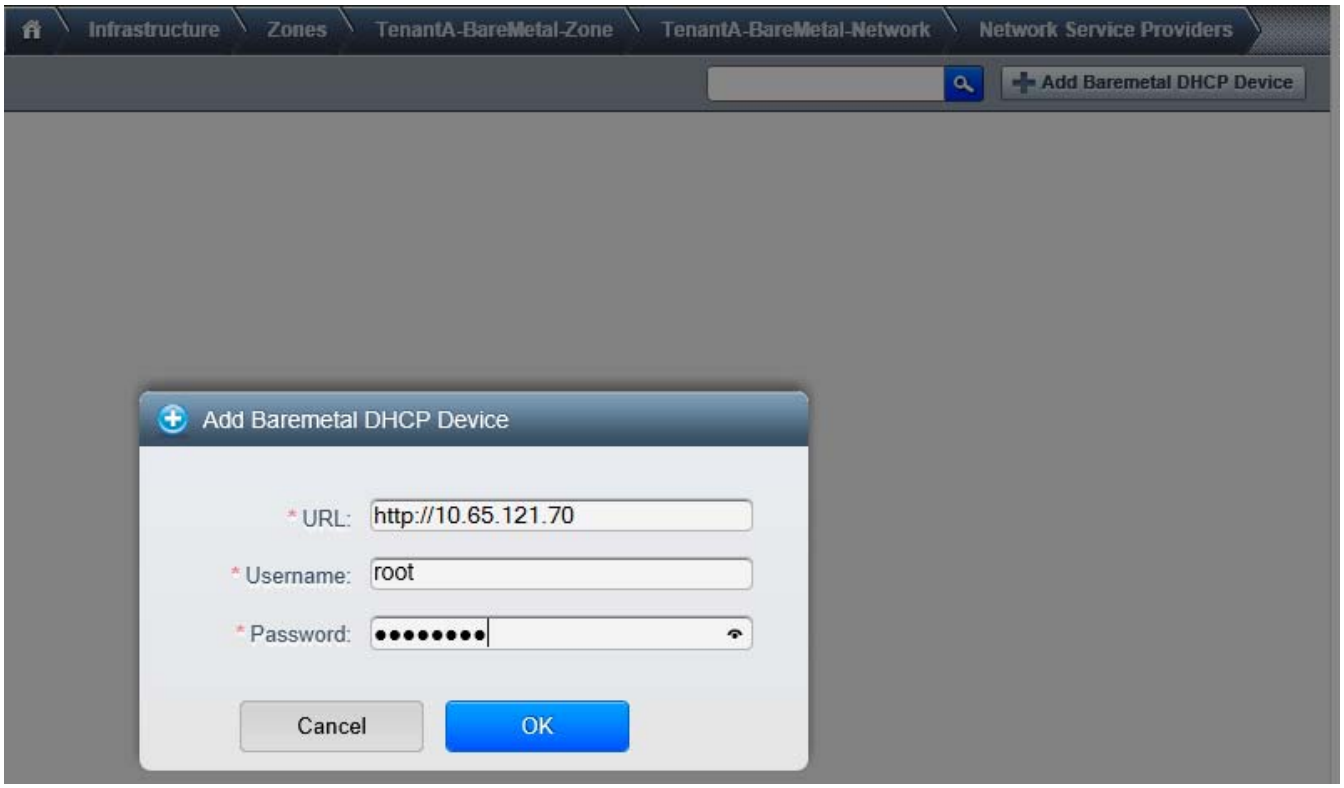


18. [URL] フィールドに <CloudPlatfrom_Management_IP_Address> http://10.65.121.70 と入力します。

（注） IP アドレス 10.65.121.70 が、DHCP サービスが設定されているサーバに割り当てられます。詳細については、クラウドの導入に関する項を参照してください。

19. [Username] フィールドに <**root**> と入力します。
20. [Password] フィールドに <**XXXXX**> と入力します。
21. [OK] をクリックします。

図 317　　DHCP サーバ設定の詳細



Baremetal ホストの導入

この項では、Baremetal ホスト テンプレートを Linux オペレーティング システムの PXE イメージに登録し、コンピュートおよびネットワーク オファリングを使用して Baremetal インスタンスを作成する方法について説明します。

ベア メタル ホストは次のオペレーティング システムを実行できます。CentOS 5.5、CentOS 6.2、CentOS 6.3、Fedora 17、RedHat 6.1 ～ 6.3 および Ubuntu12.04。

ここでは、FCoE NetApp クラスタ ターゲットに PXE 方法を使用して新しく作成された Baremetal インスタンス BareMetal-Host1 上に RHEL 6.3 オペレーティング システムをインストールします。

ユーザ資格情報を使用して CloudPlatform にログインして、TenantA ゾーンの ISO イメージを作成します。

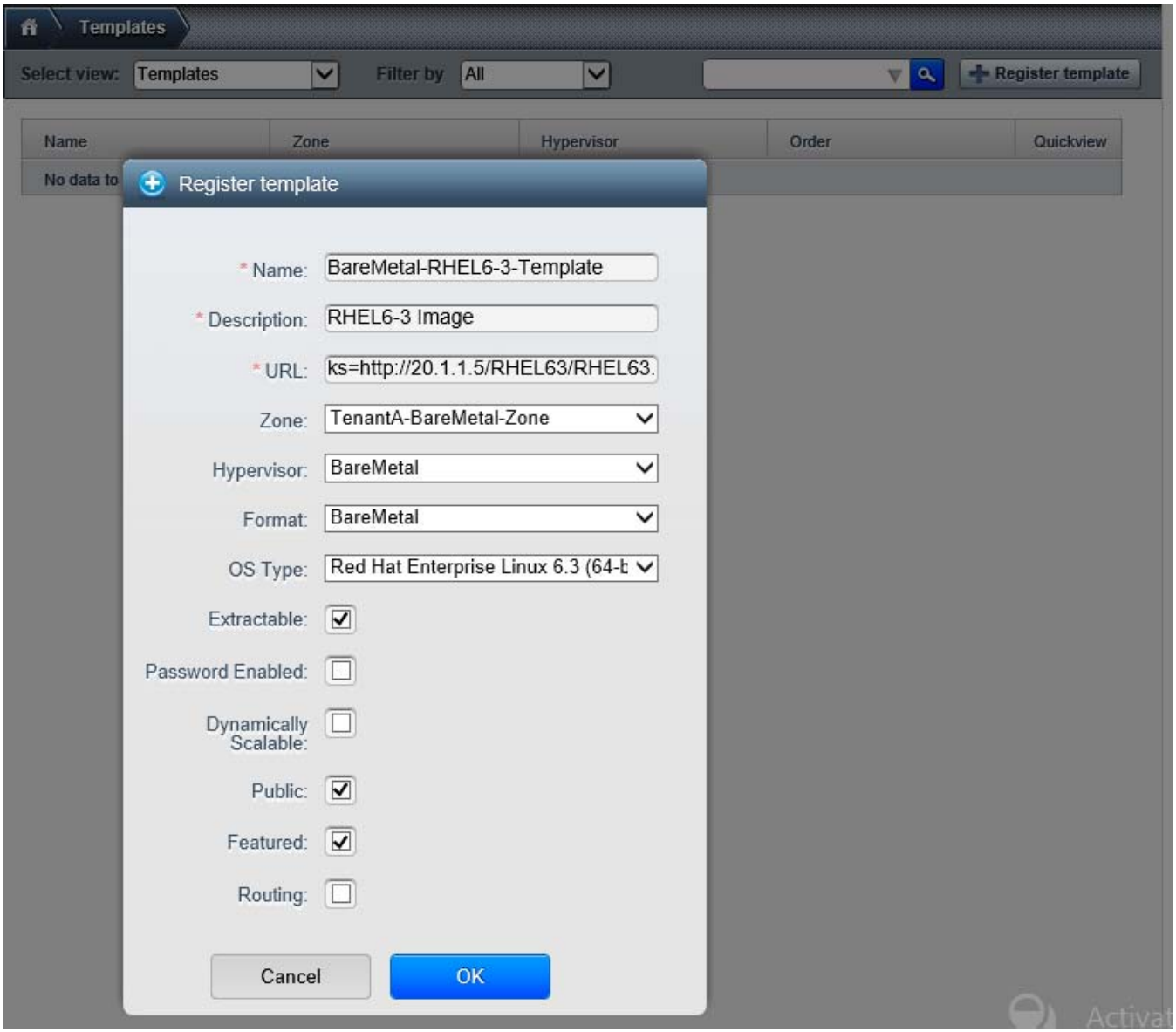
1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。

2. [Login] をクリックします。
3. [Template] タブをクリックします。
4. [Select view] リスト ボックスで [Templates] を選択します。
5. [Register template] をクリックします。
6. [Name] フィールドに **BareMetal-RHEL6-3-Template** と入力します。
7. [Description] フィールドに **RHEL6-3 Image** と入力します。
8. [URL] にパス ks=http://20.1.1.5/RHEL63/RHEL63.ks;kernel=20.1.1.5:/var/www/html/RHEL63/vmlinuz;initrd=20.1.1.5:/var/www/html/RHEL63/initrd.img を入力します。

（注） RHEL6-3 のキックスタート、カーネルおよび initrd ファイルの正しいパスを入力したことを確認します。これらのファイルが保存されているディレクトリ /export と /var/www/html/RHEL63 は NFS エクスポートされています。詳細については、クラウドの導入に関する項を参照してください。

9. [Zone] リスト ボックスで [TenantA-BareMetal-Zone] を選択します。
10. [Hypervisor] リスト ボックスで [BareMetal] を選択します。
11. [Format] リスト ボックスで [BareMetal] を選択します。
12. [OS Type] リスト ボックスで [Red Hat Enterprise Linux 6.3（64 bit）] を選択します。
13. [Extractable] チェックボックスをオンにします。
14. [Public] チェックボックスをオンにします。
15. [Featured] チェックボックスをオンにします。
16. [OK] をクリックします。

図 318　Baremetal テンプレート詳細の表示

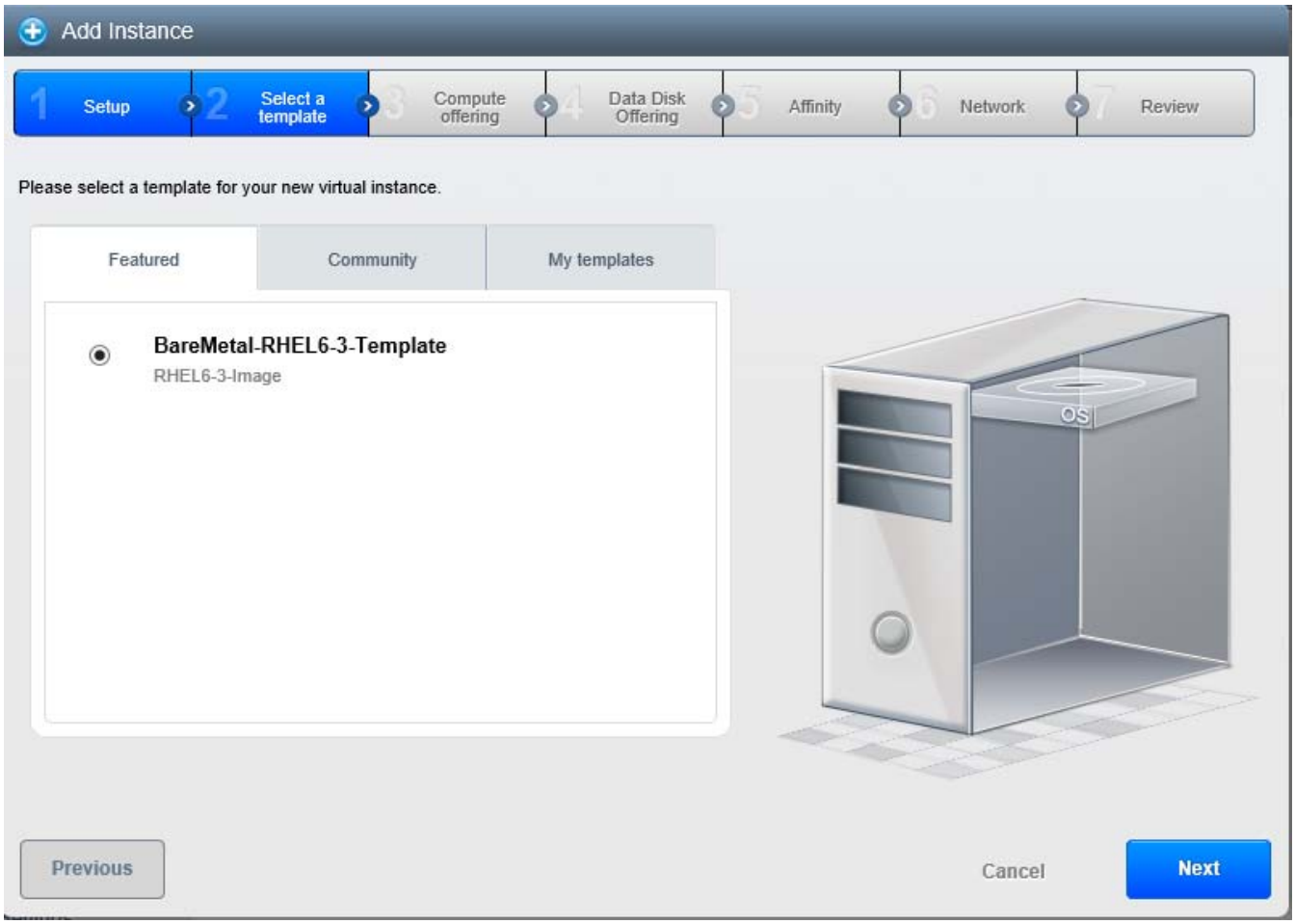


17. [Instances] タブをクリックします。
18. [Add Instance] をクリックします。
19. [Zone] リスト ボックスで [TenantA-BareMetal-Zone] を選択します。
20. [Template] オプション ボタンを選択します。
21. [Next] をクリックします。

図 319　テンプレートの選択

22. [Name] フィールドに **BareMetal-RHEL6-3-Template** と入力します。
23. [Description] フィールドに **RHEL6-3 Image** と入力します。
24. [template] で [BareMetal-RHEL6-3Template] を選択します。
25. [Next] をクリックします。

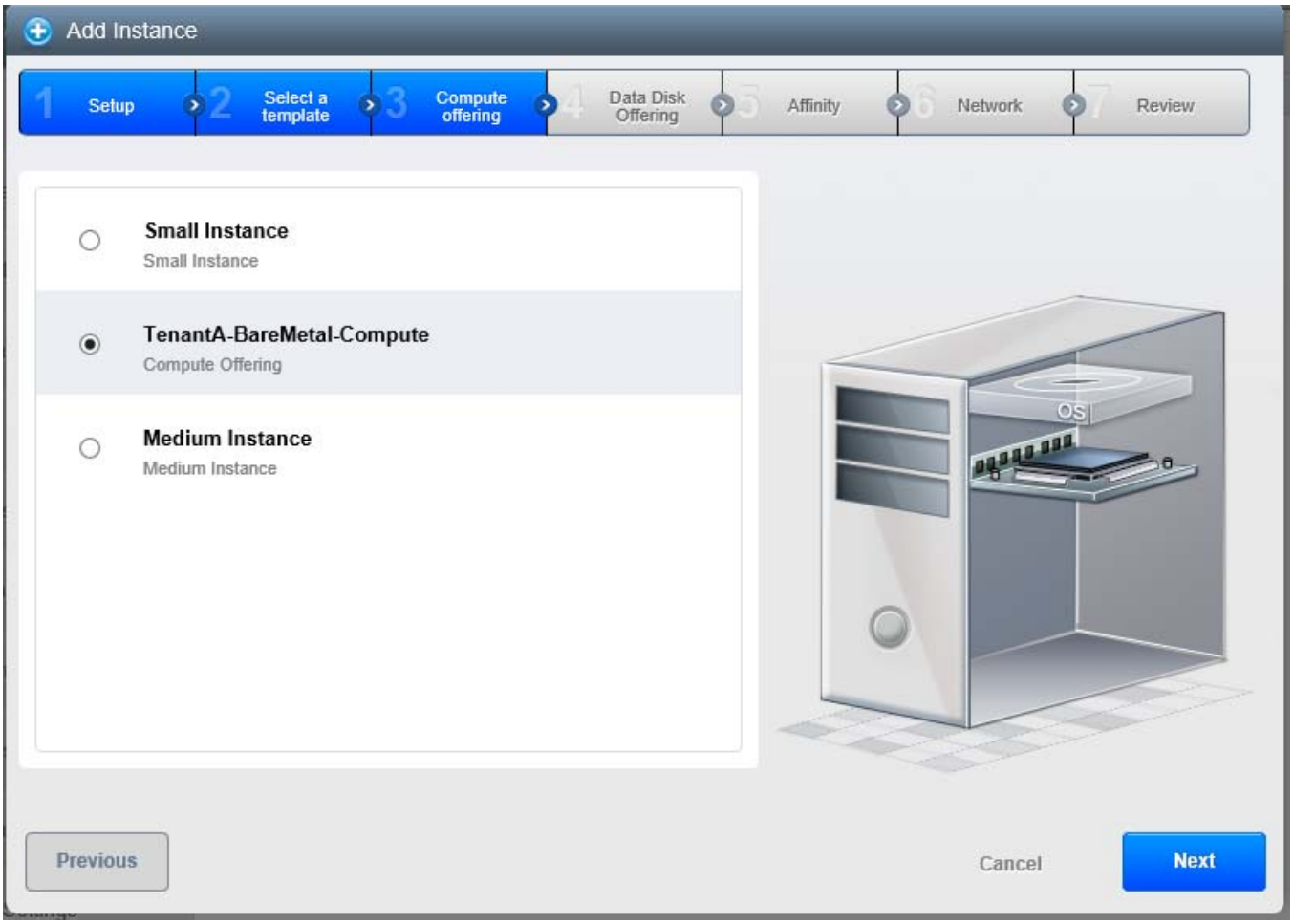
図 320　テンプレート イメージの選択



26. [Compute offering] で [TenantA-BareMetal-Compute] を選択します。

27. [Next] をクリックします。

図 321　　コンピュート オファリングの選択

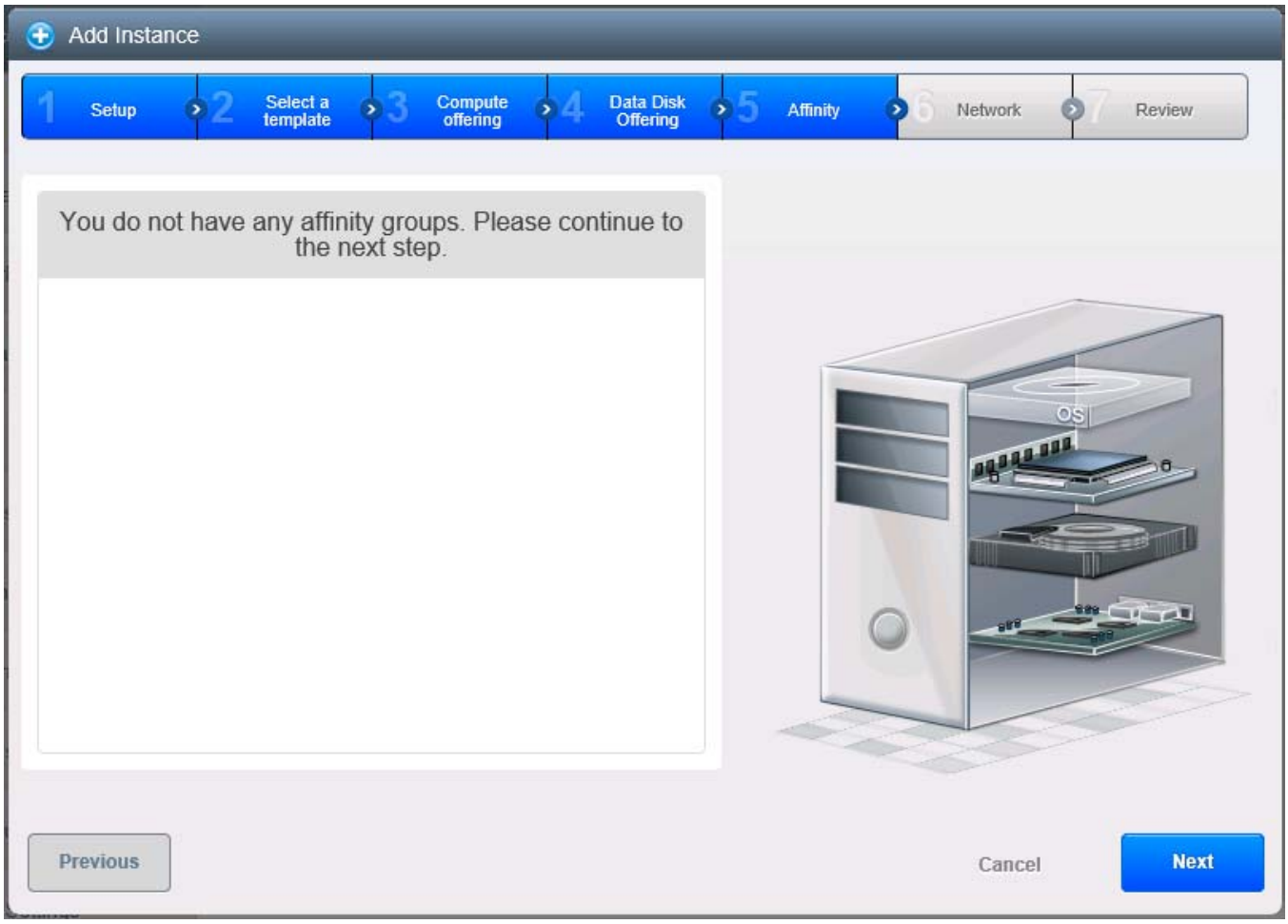


28. [Data Disk offering] で [Medium] を選択します。
29. [Next] をクリックします。

図 322　　ディスク オファリングの選択

30. [Next] をクリックします。

図 323　　設定されたアフィニティ ルールなし

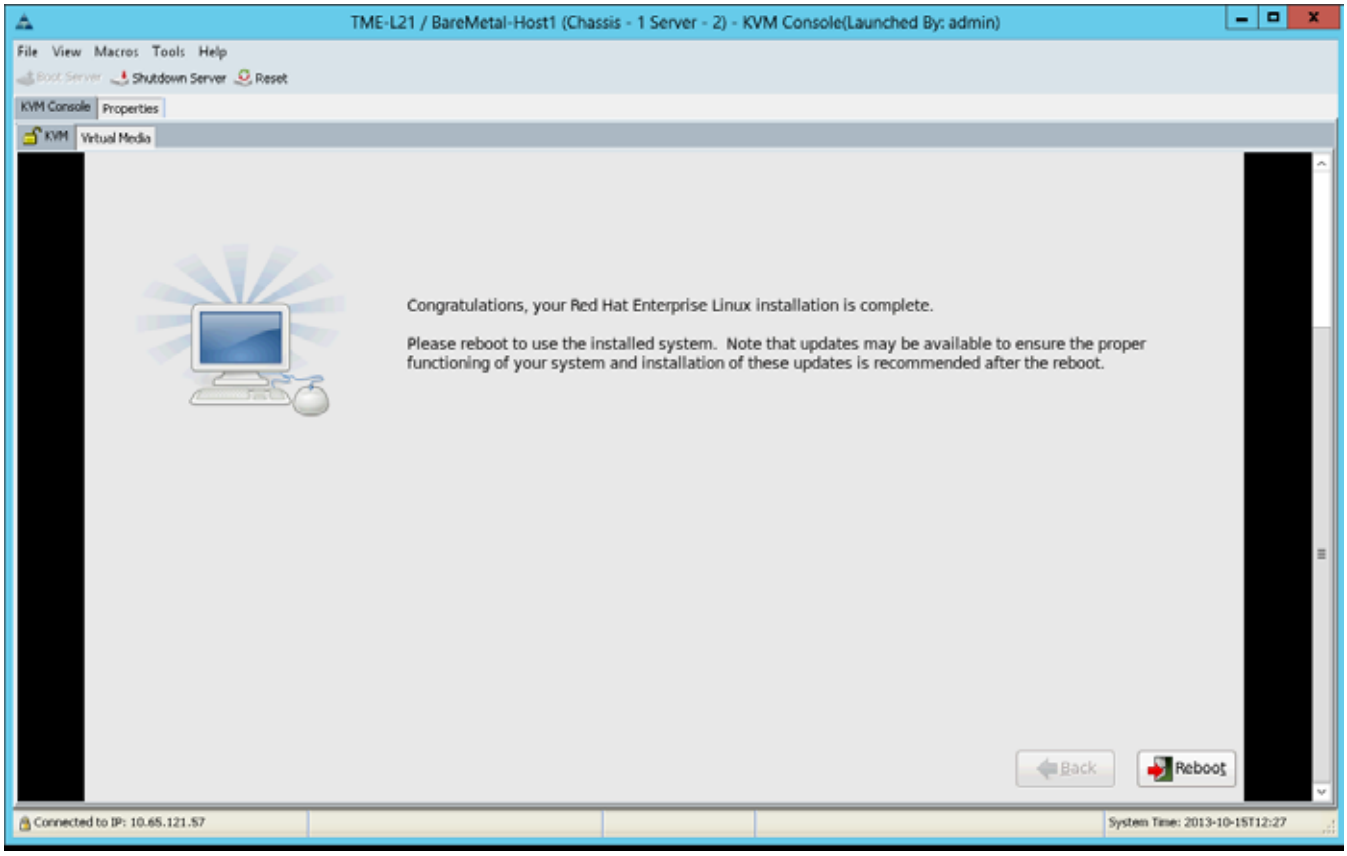


31. [Next] をクリックします。

図 324　　設定されたネットワークなし

32. [Reboot] をクリックします。
33. ホスト **BareMetal-Host1** 上での PXE ブート後の最終画面

図 325　　インスタンスの最終設定



Baremetal ブレードのプロビジョニング解除

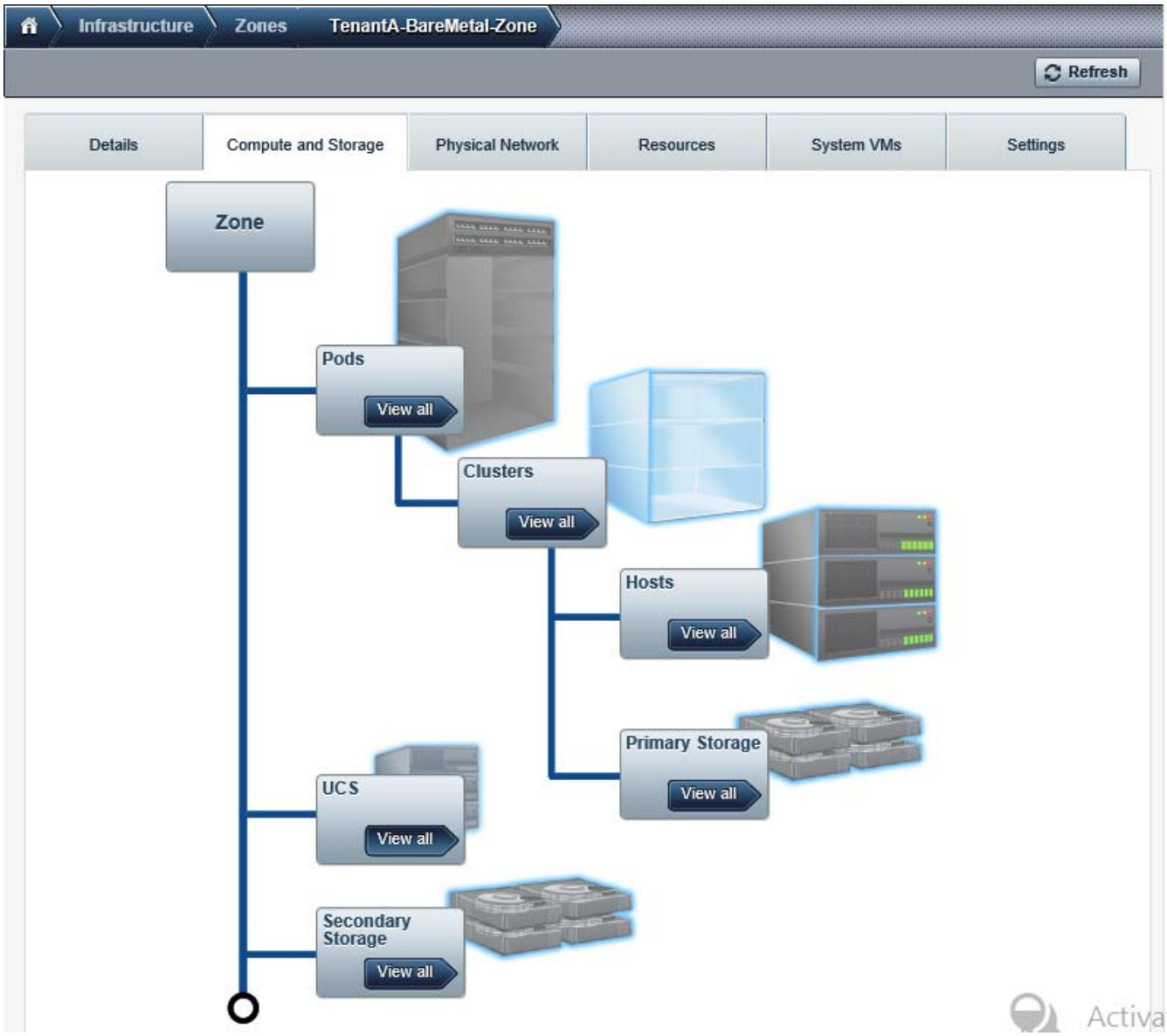
この項では、再利用のためにコンピューティング、ネットワークおよびストレージ リソースを解放してクラウド プールに戻すため、メンテナンス作業の一部として Baremetal インスタンスをクリーンアップするためにクラウド管理者が実行する手順について説明します。このプロセスの一部として、Cisco UCS Manager はブレード上でサービス プロファイルの関連付けを解除し、サービス プロファイルを削除します。

（注）　ここでは、CloudPlatform を使用して BareMetal-Host1 の関連付けを解除します。

ユーザ資格情報を使用して CloudPlatform にログインして、TenantA-BareMetal-Zone ゾーンで BareMetal-Host1 インスタンスを削除します。

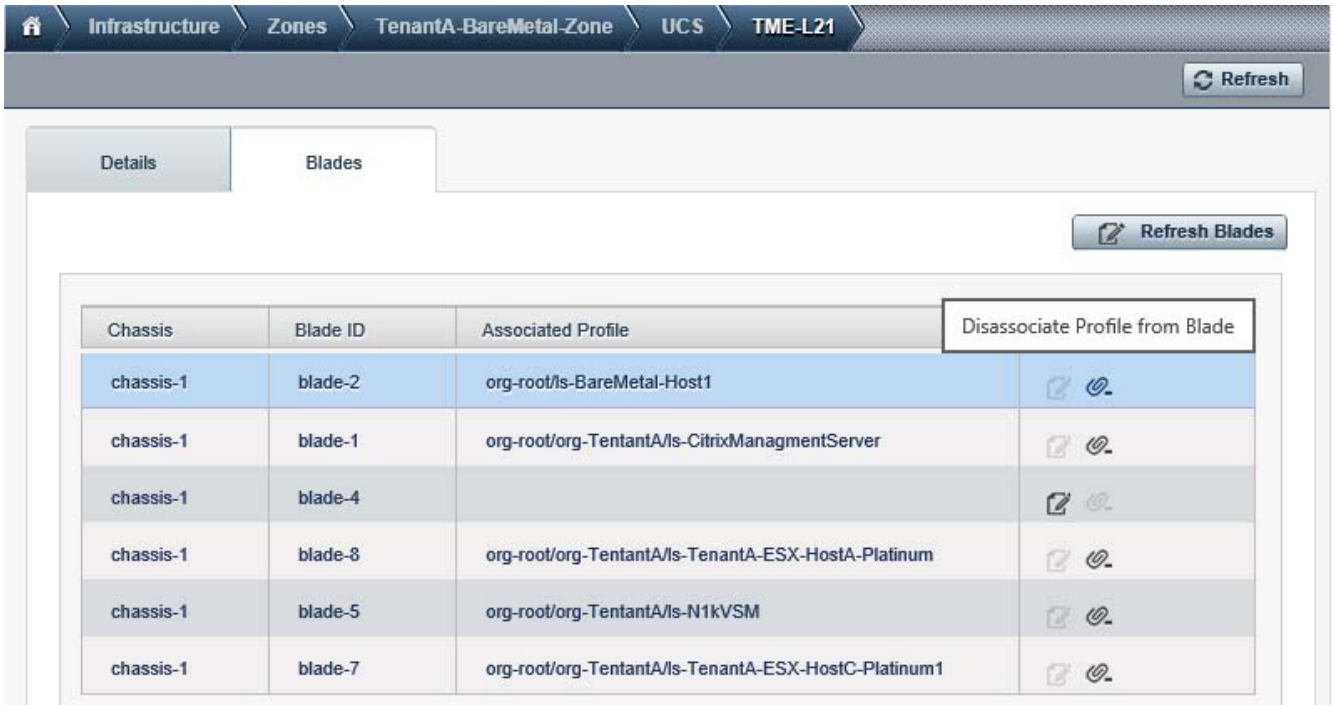
1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Infrastructure] タブをクリックします。
4. [Zones] をクリックし、[TenantA-BareMetal-Zone] をクリックします。
5. [UCS View All] をクリックします。

図 326　　Cisco UCS プラグインへのアクセス



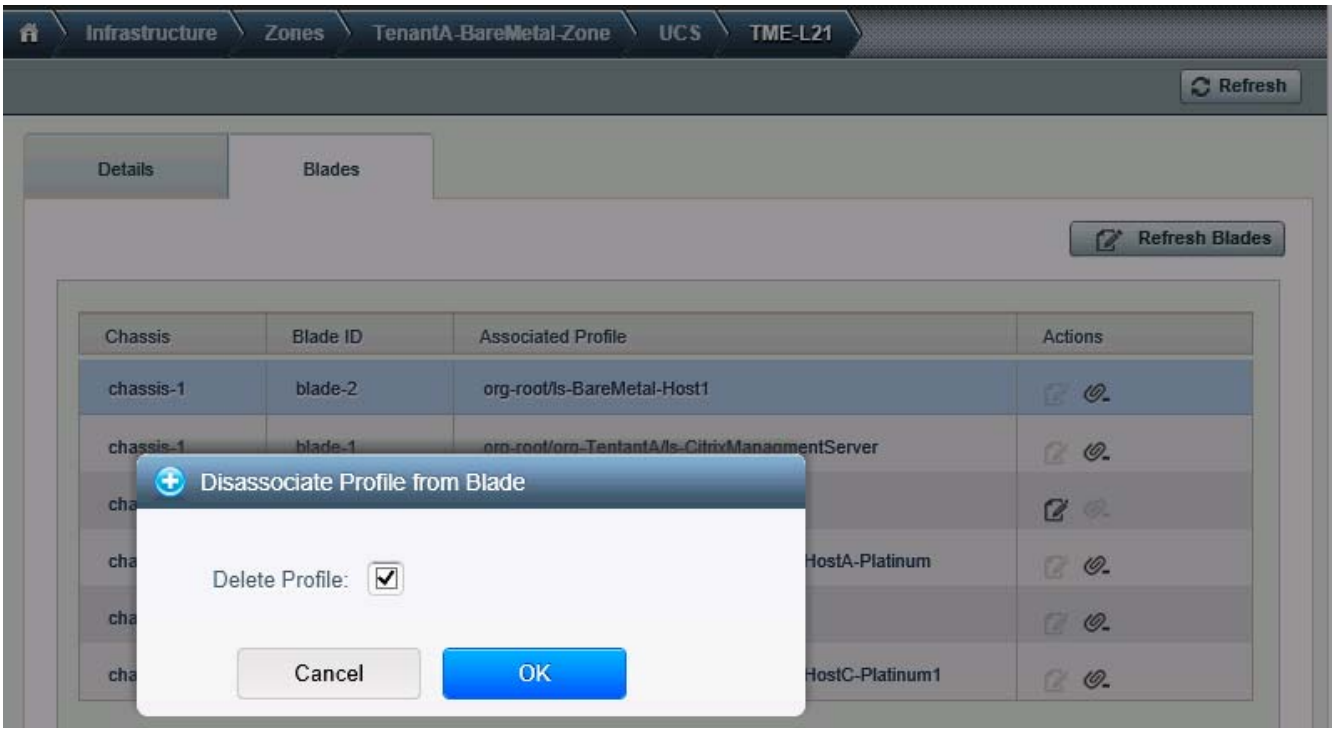
6. [TME-L21] をクリックし、[Blades] をクリックします。
7. [chassis-1] の [blade-2] で [Disassociate Profile from Blade] アイコンをクリックします。

図 327　Cisco UCS プラグインで BareMetal-Host1 サービス プロファイルから関連付けを解除する chassis-1 上の blade-2 を選択する



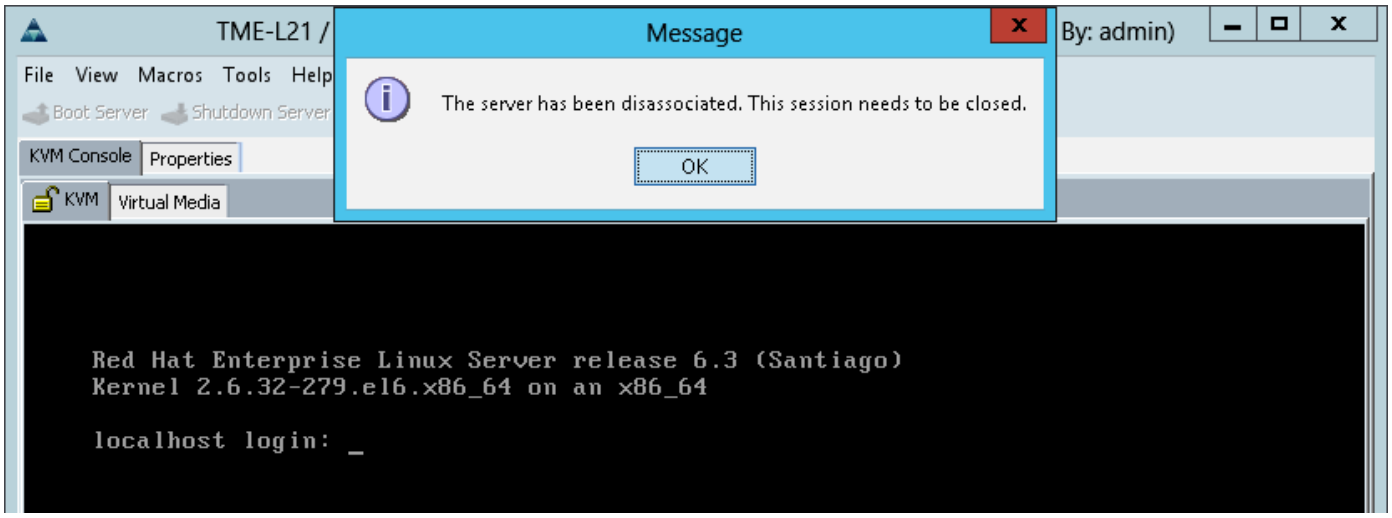
8. [Delete Profile] チェック ボックスを有効にします（このオプションがは Cisco UCS Manager 上のサービス プロファイルを削除します）。
9. [OK] をクリックします。

図 328　サービス プロファイル BareMetal-Host1 を削除するために [Delete Profile] チェック ボックスを有効にする



10. サービス プロファイル BareMetal-Host1 と blade-2 の関連付けが解除され、Cisco UCS Manager で削除されます。

図 329　blade-2 で関連付けが解除され、削除されたサービス プロファイル BareMetal-Host1



Baremetal インスタンスのライフ サイクル管理

この項では、再利用のためにコンピューティング、ネットワークおよびストレージ リソースを解放してクラウド プールに戻すための、メンテナンス作業の一部として Baremetal インスタンスのライフ サイクル管理を可能にするためにクラウド管理者が実行する手順について説明します。

CloudPlatfrom 4.2.1.1 は、Baremetal ホストの一部である、Cisco UCS ブレード サーバ上で実行されている RHEL オペレーティング システムを開始、リブート、および破棄するために、IPMI インターフェイスを使用して Cisco UCS Manager API コールを呼び出します。

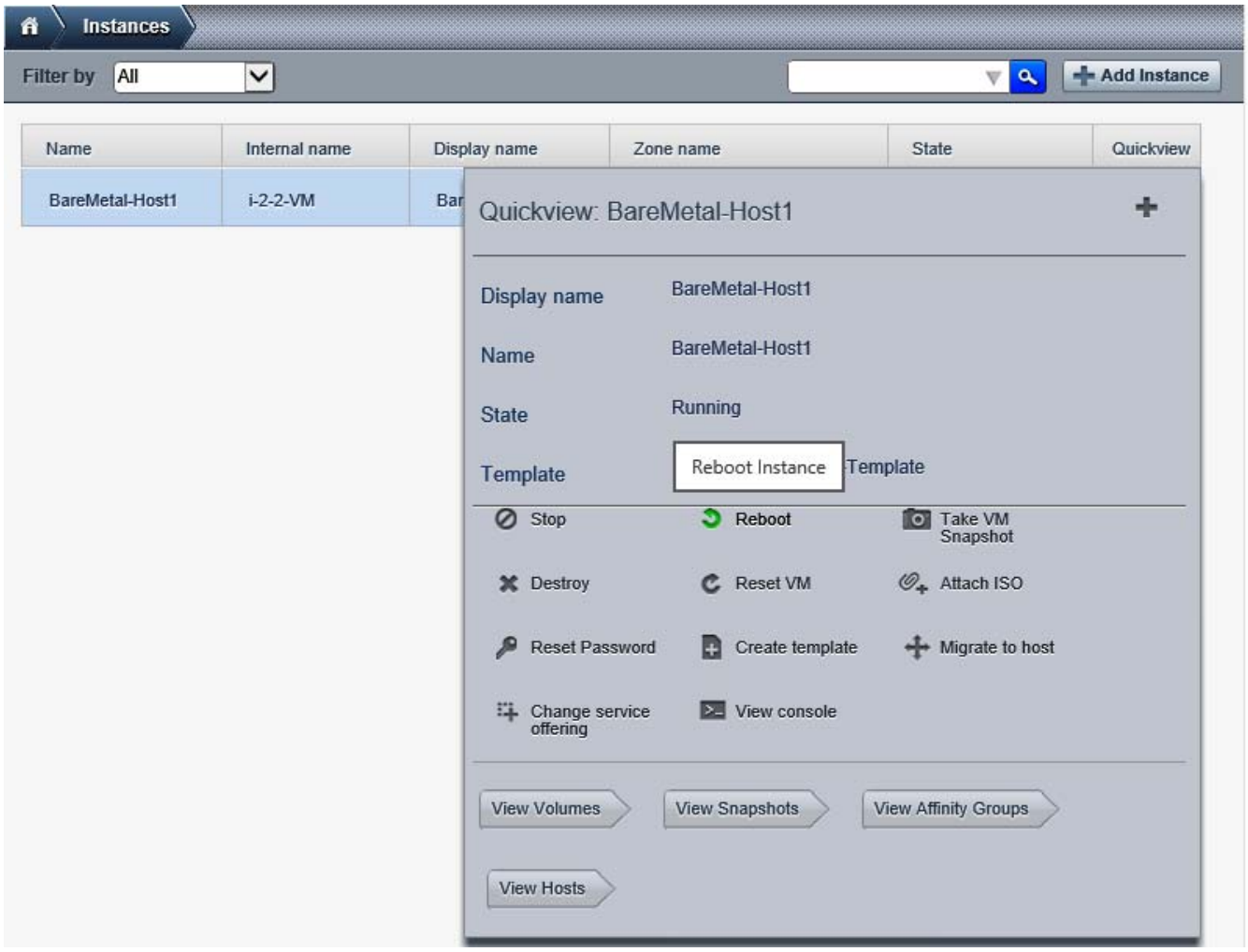
Baremetal インスタンスのリブート

ここでは、CloudPlatform を使用して BareMetal-Host1 インスタンスをリブートします。

ユーザ資格情報を使用して CloudPlatform にログインして、TenantA-BareMetal-Zone ゾーンで BareMetal-Host1 インスタンスをリブートします。

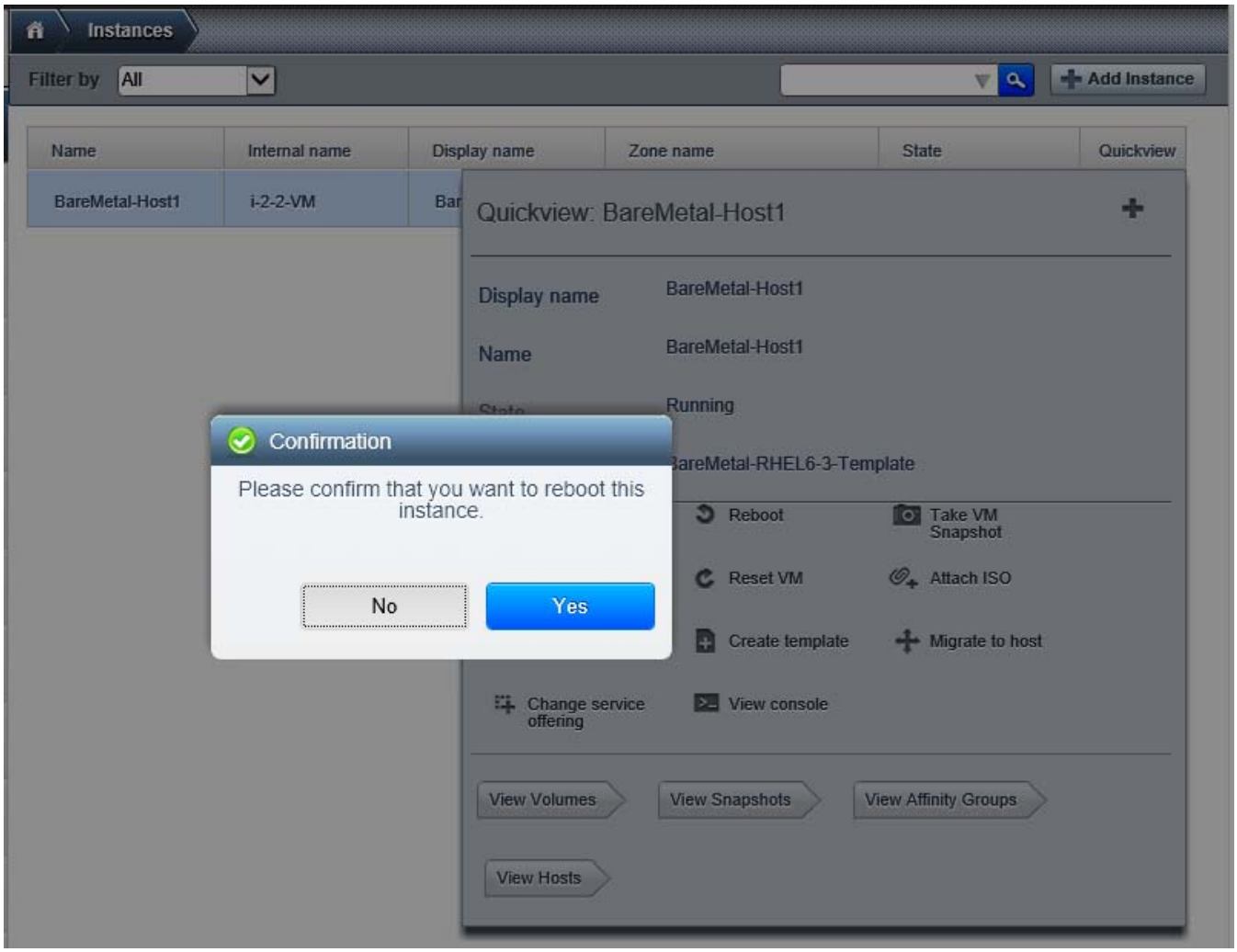
1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Instances] タブをクリックします。
4. [BareMetal-Host1] の [Quickview] アイコンをクリックします。
5. [Reboot] をクリックします。

図 330 BareMetal-Host1 インスタンスのリブート



6. [Yes] をクリックし、インスタンスを確認します。

図 331　BareMetal-Host1 インスタンスのリブートの確認



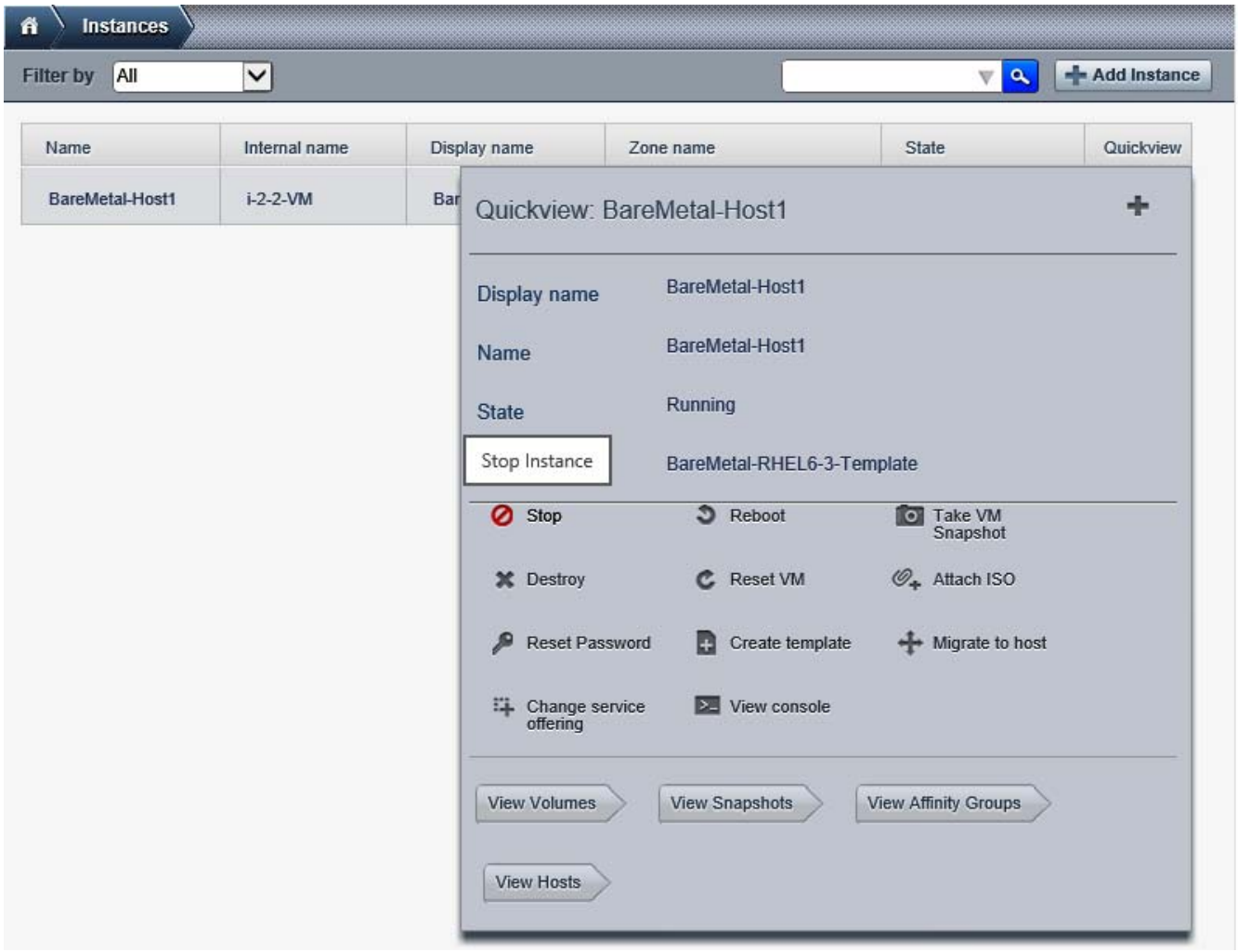
Baremetal インスタンスの停止と起動

（注）　ここでは、CloudPlatform を使用して BareMetal-Host1 インスタンスを停止および起動します。

ユーザ資格情報を使用して CloudPlatform にログインして、TenantA-BareMetal-Zone ゾーンで BareMetal-Host1 インスタンスをリブートします。

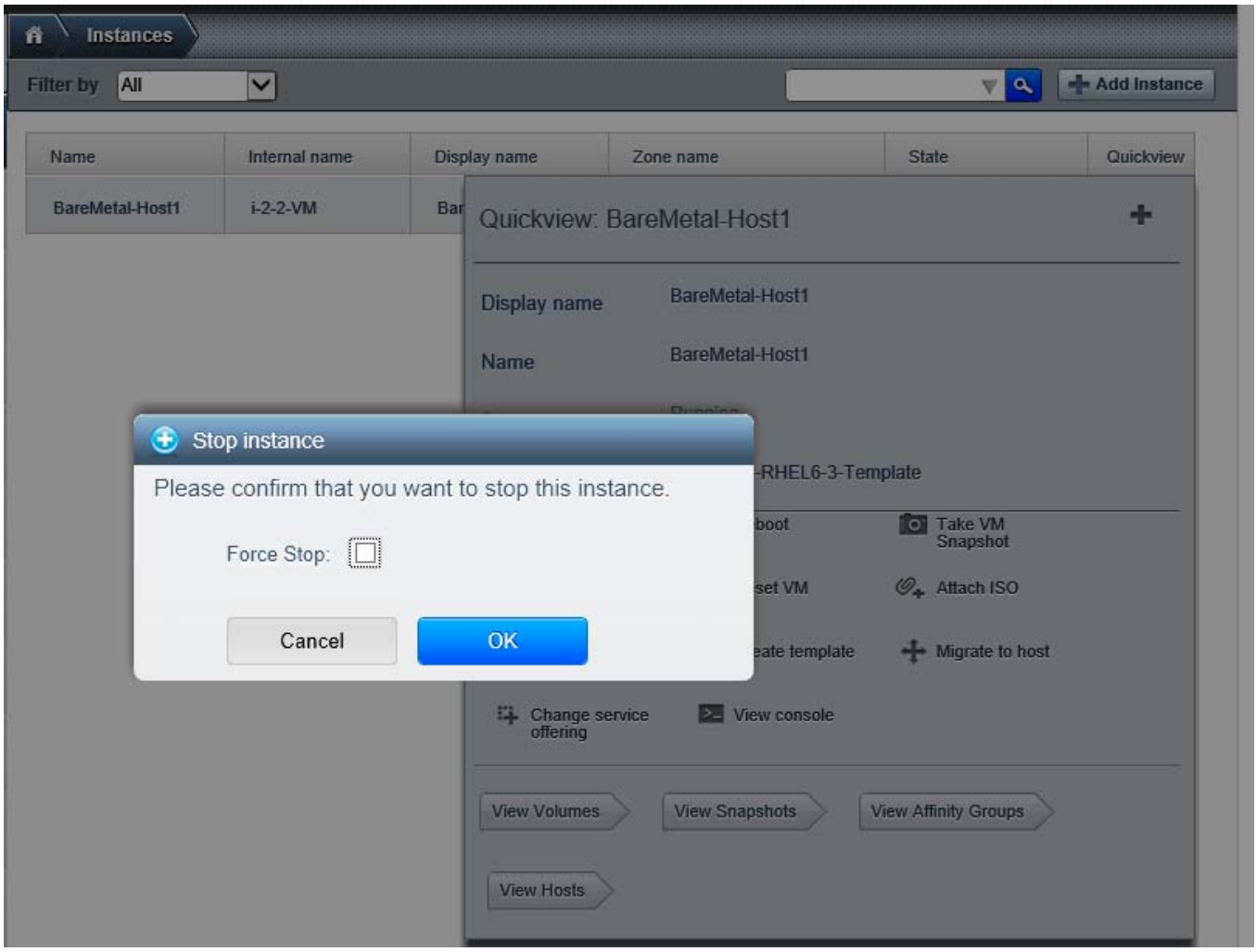
1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Instances] タブをクリックします。
4. [BareMetal-Host1] の [Quickview] アイコンをクリックします。
5. [Stop] をクリックします。

図 332　BareMetal-Host1 インスタンスの停止



6. [Yes] をクリックし、インスタンスの停止を確認します。
7. [Force Stop] インスタンスをオフにします。

図 333 BareMetal-Host1 インスタンスの停止の確認

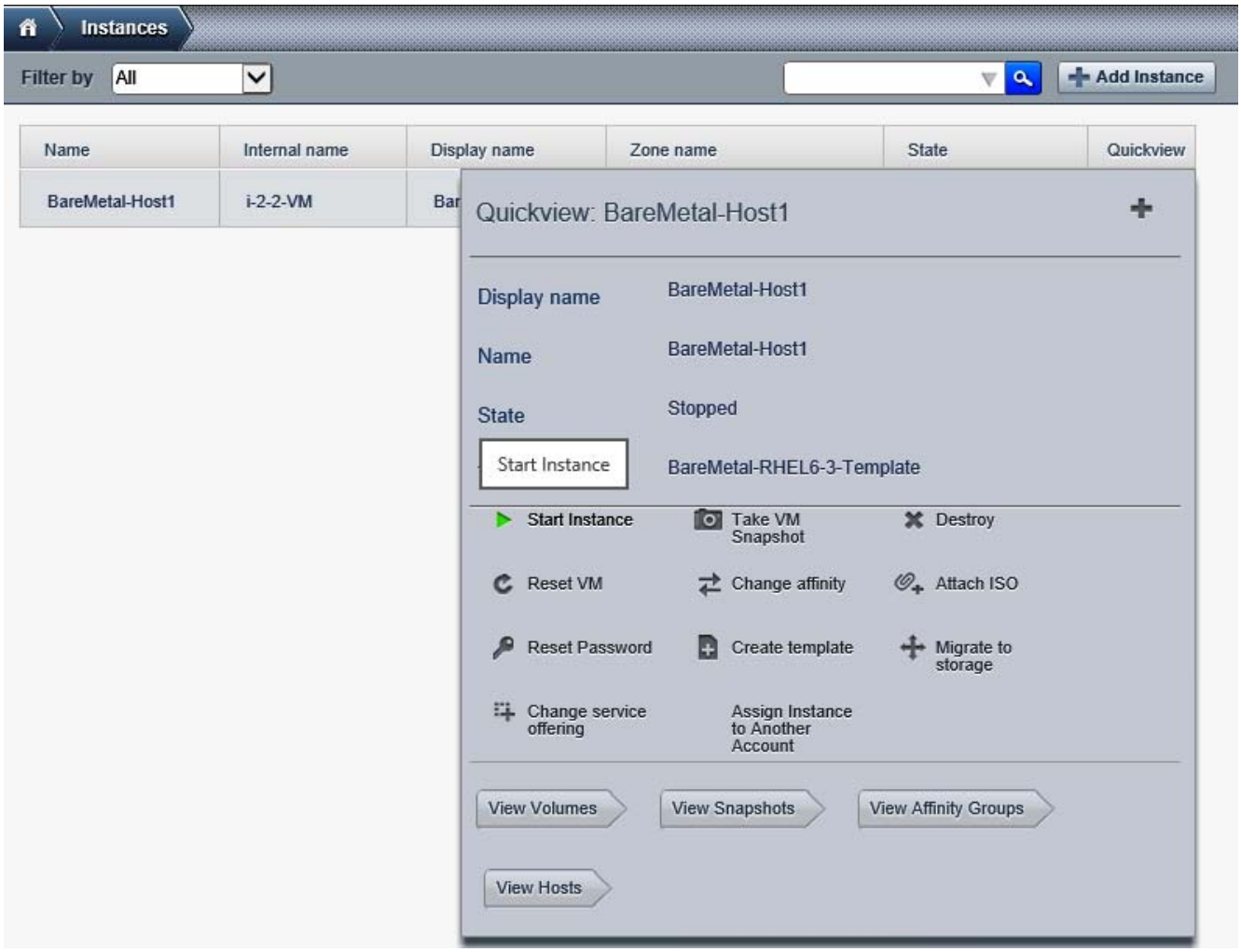


8. インスタンス ステータスを停止します。

図 334 BareMetal-Host1 インスタンスのステータスの停止

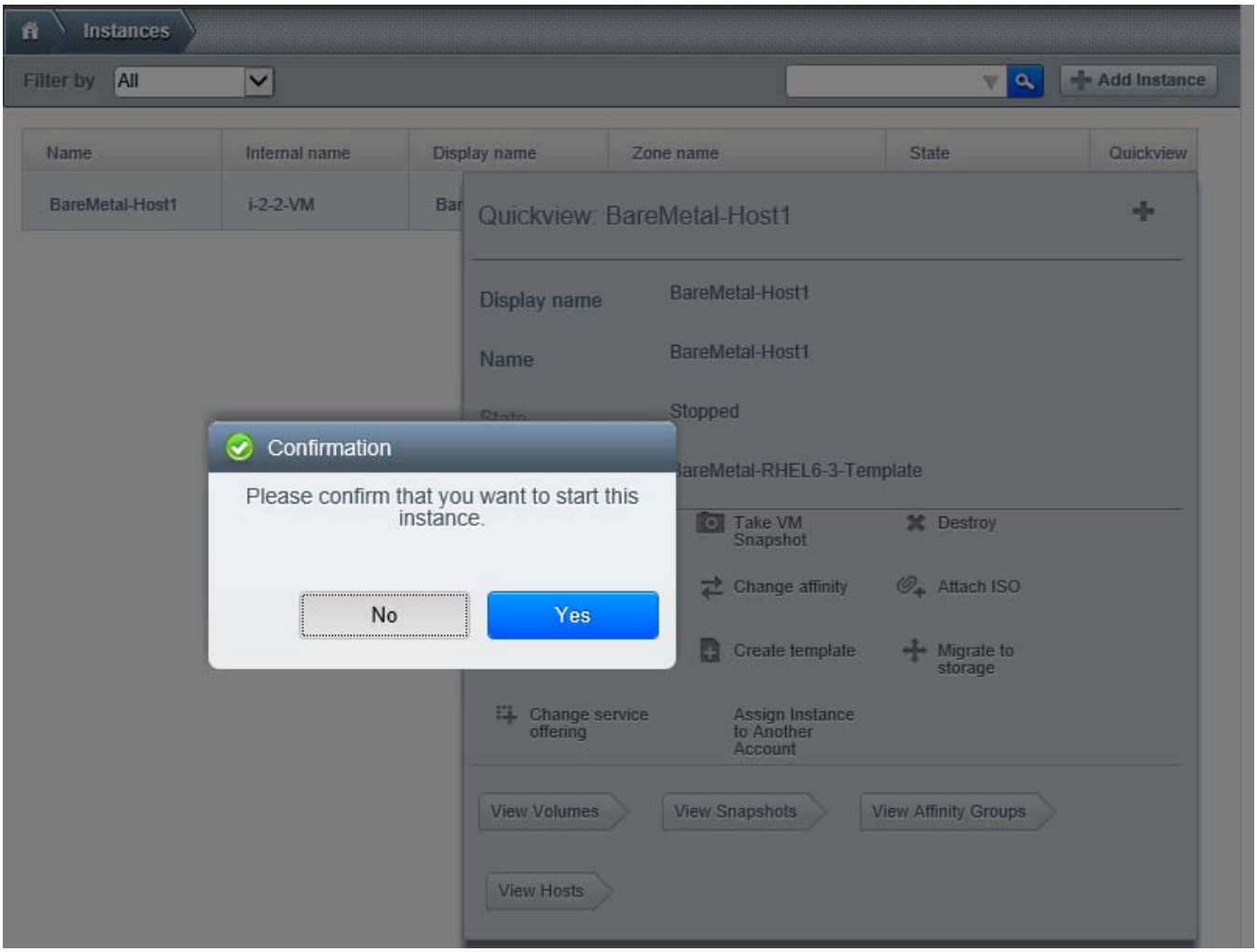
9. [Instances] タブをクリックします。
10. [BareMetal-Host1] の [Quickview] アイコンをクリックします。
11. [Start instance] をクリックします。

図 335　BareMetal-Host1 インスタンスの開始



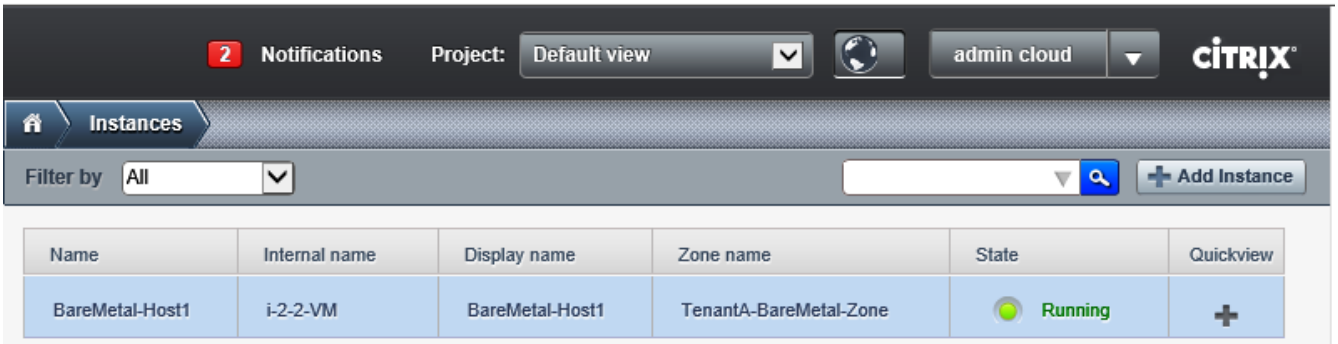
12. [Yes] をクリックし、インスタンスの開始を確認します。

図 336　BareMetal-Host1 インスタンスの開始の確認



13. インスタンスの開始後に BareMetal ステータスが [Running] になります。

図 337　インスタンスの開始後の BareMetal-Host1 の実行ステータス



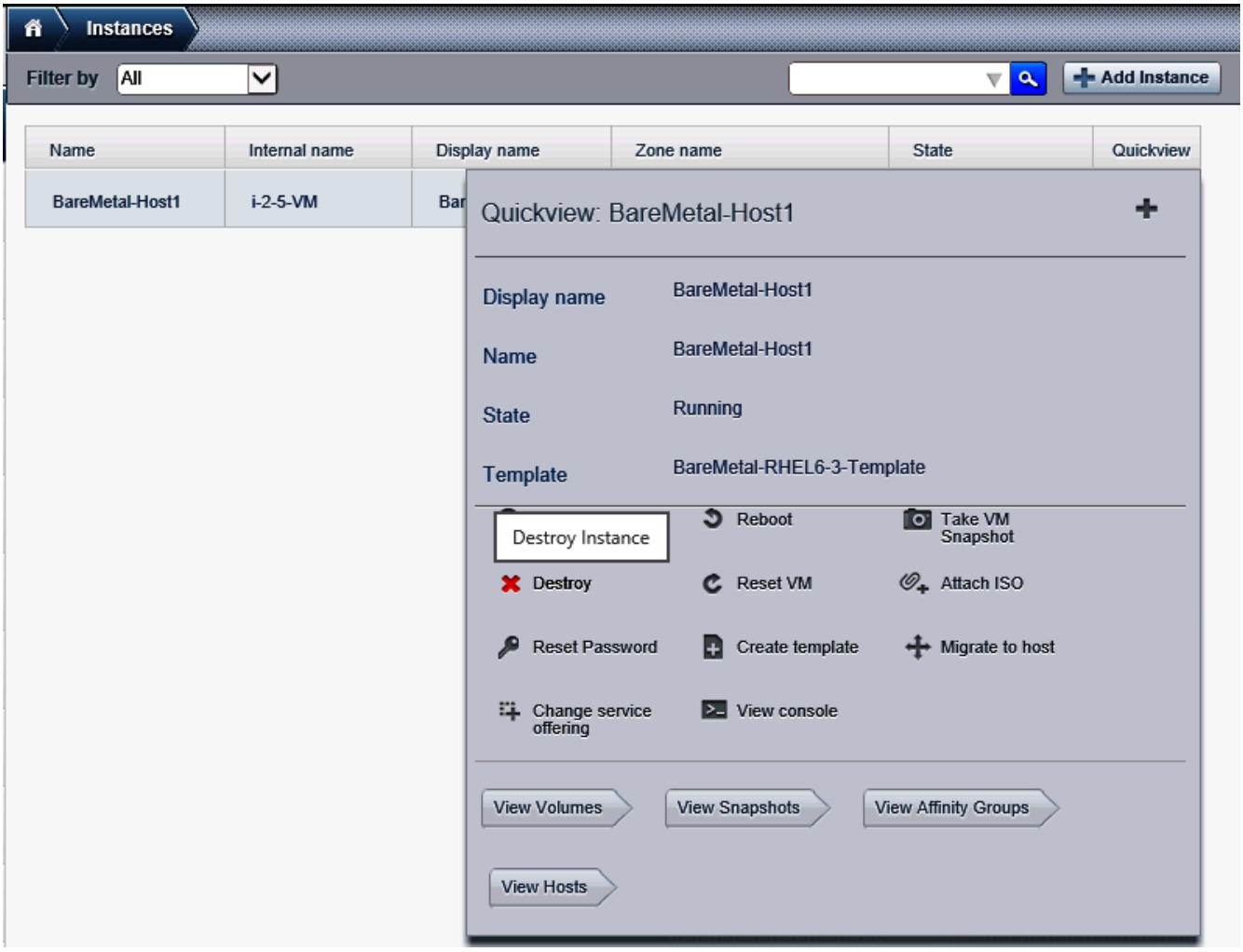
Baremetal インスタンスの破棄と復元

ここでは、CloudPlatform を使用して BareMetal-Host1 インスタンスを破棄および復元します。

ユーザ資格情報を使用して CloudPlatform にログインして、TenantA-BareMetal-Zone ゾーンで BareMetal-Host1 インスタンスを破棄します。

1. ユーザ名 <root> およびパスワード <XXXXXX> およびドメインを入力します。
2. [Login] をクリックします。
3. [Instances] タブをクリックします。
4. [BareMetal-Host1] の [Quickview] アイコンをクリックします。
5. [Destory] をクリックします。

図 338　　BareMetal-Host1 インスタンスの破棄

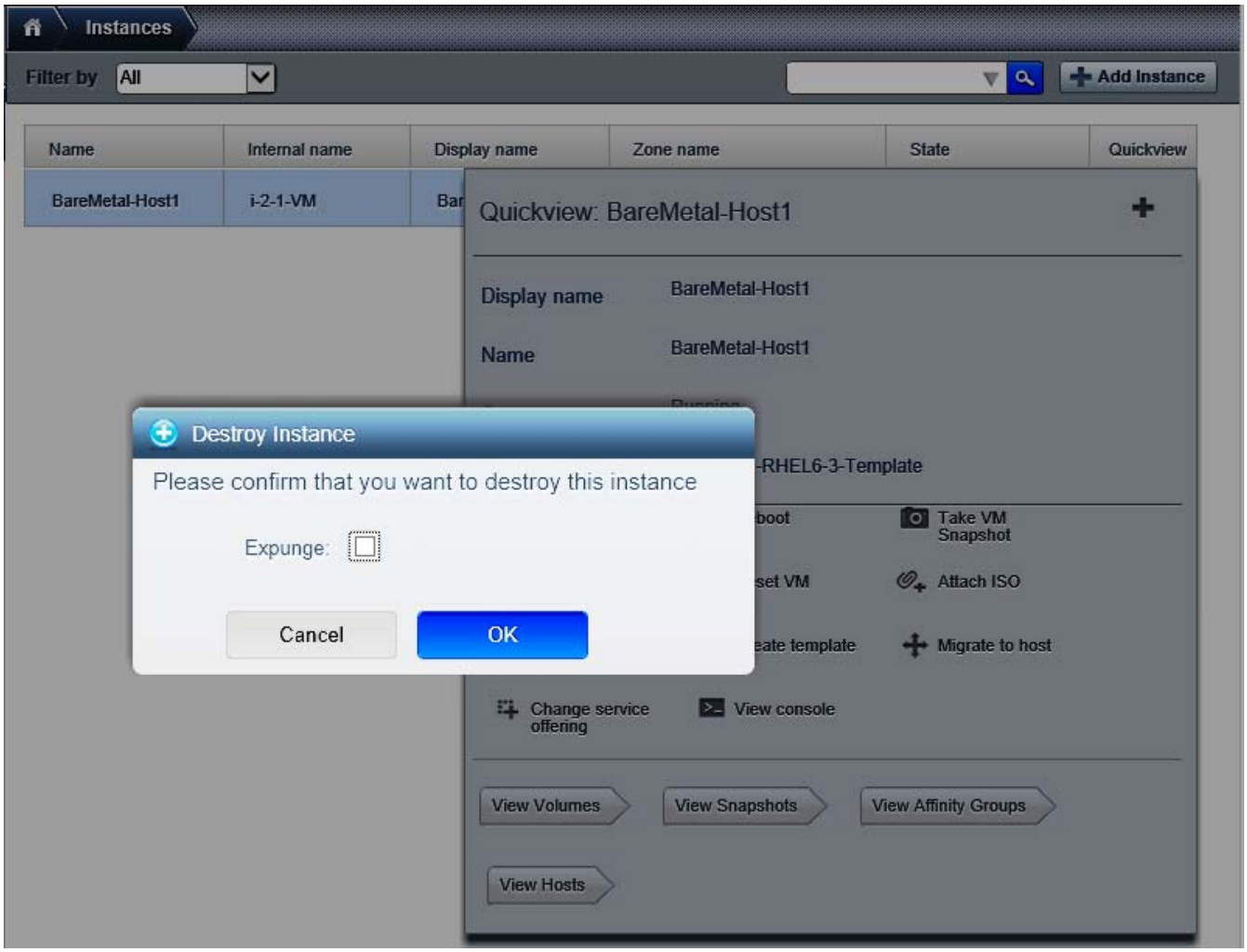


6. [OK] をクリックして破棄を確定します。
7. [Expunge] チェックボックスをオフにします。

（注） [Expunge] がオフの場合、BareMetal-Host1 インスタンスを後で復元できます。

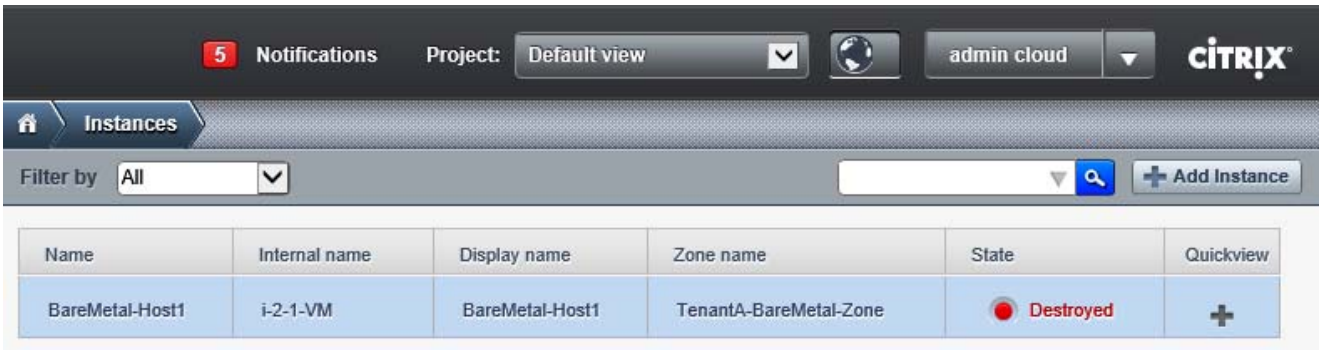
（注） [Expunge] がオンの場合、BareMetal-Host1 インスタンスが削除されて、復元できません。

図 339 BareMetal-Host1 インスタンスの破棄の確認



8. インスタンス BareMetal-Host1 が破棄されました。

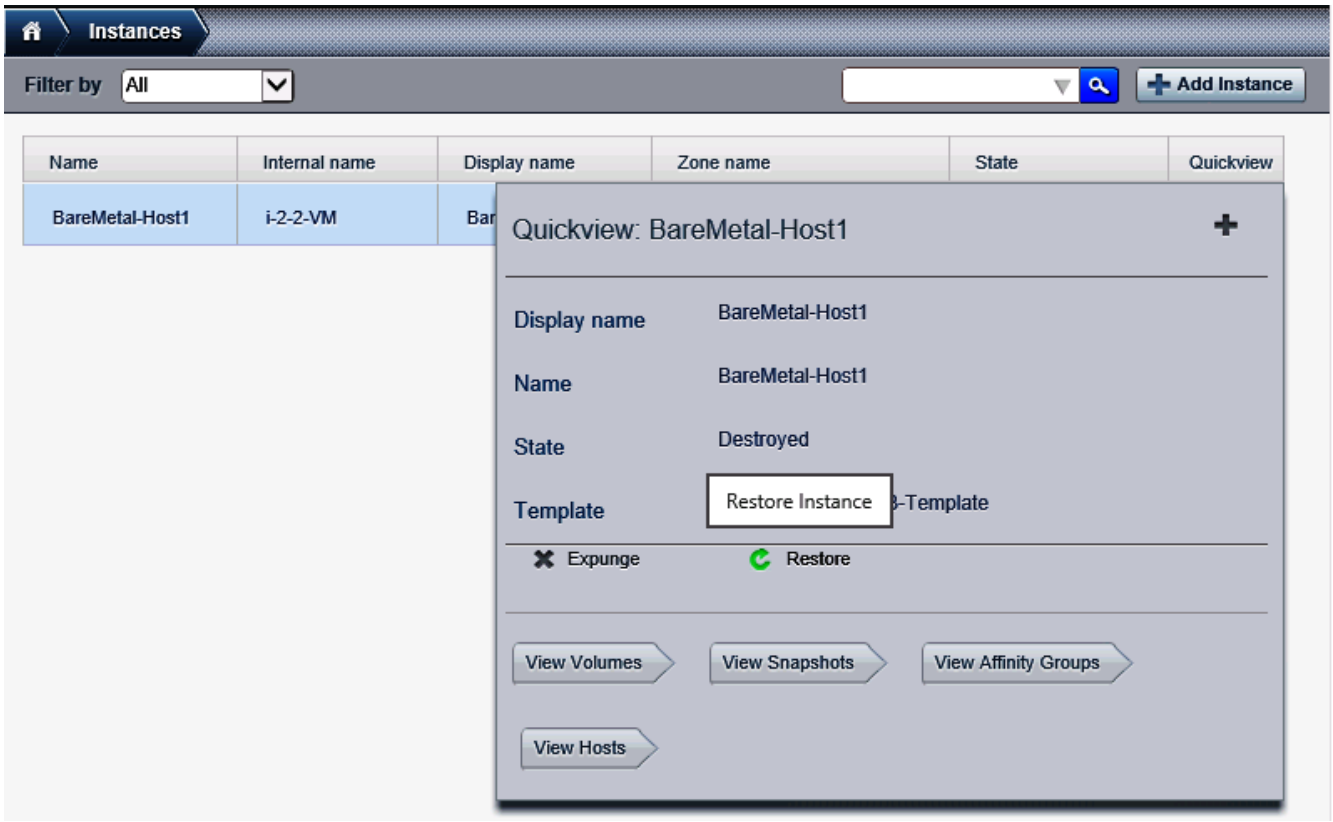
図 340　BareMetal-Host1 インスタンスの破棄



[Restore]

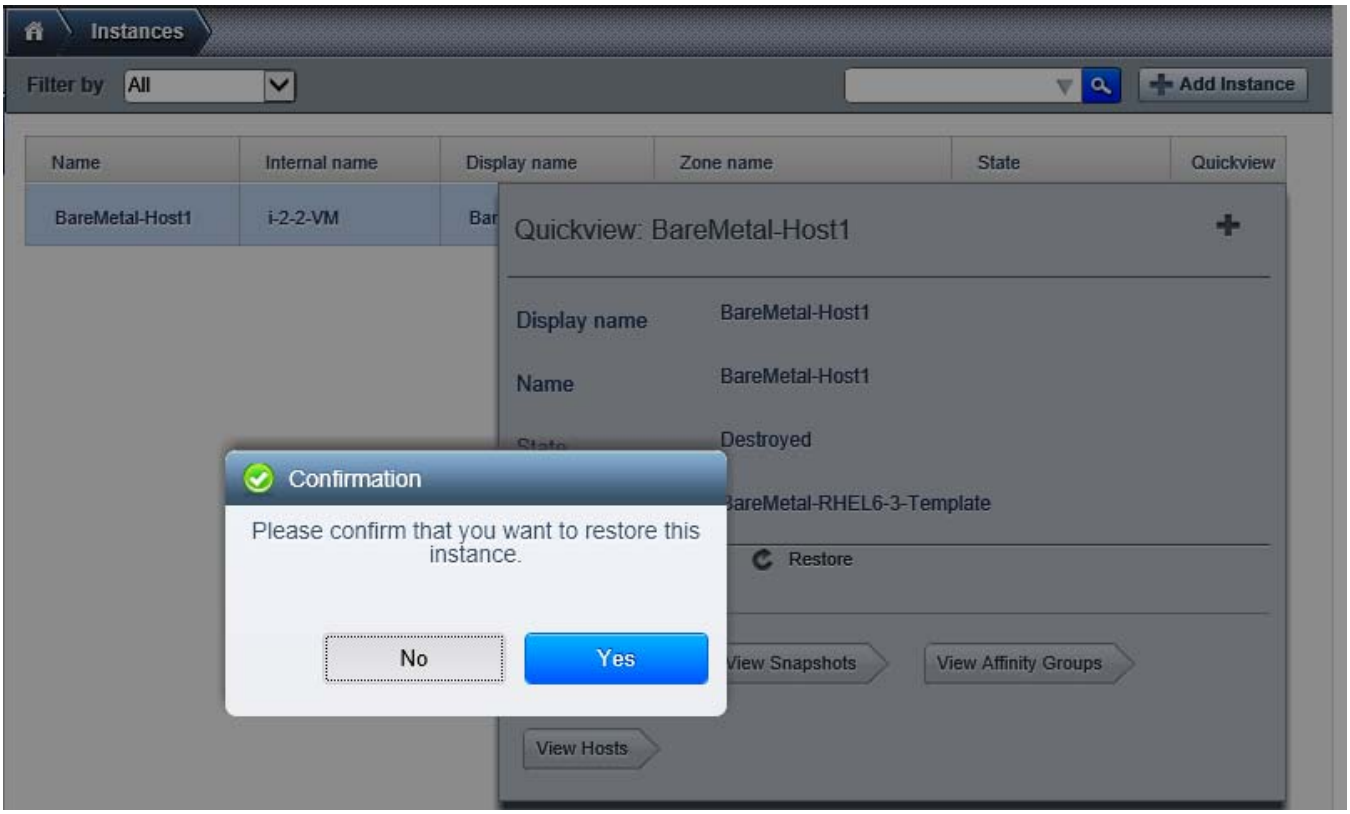
1. [Instances] タブをクリックします。
2. [BareMetal-Host1] の [Quickview] アイコンをクリックします。
3. [Restore] をクリックします。

図 341　BareMetal-Host1 インスタンスの復元



4. [Yes] をクリックして BareMetal-Host1 での復元を確認します。

図 342　BareMetal-Host1 インスタンスの復元の確認

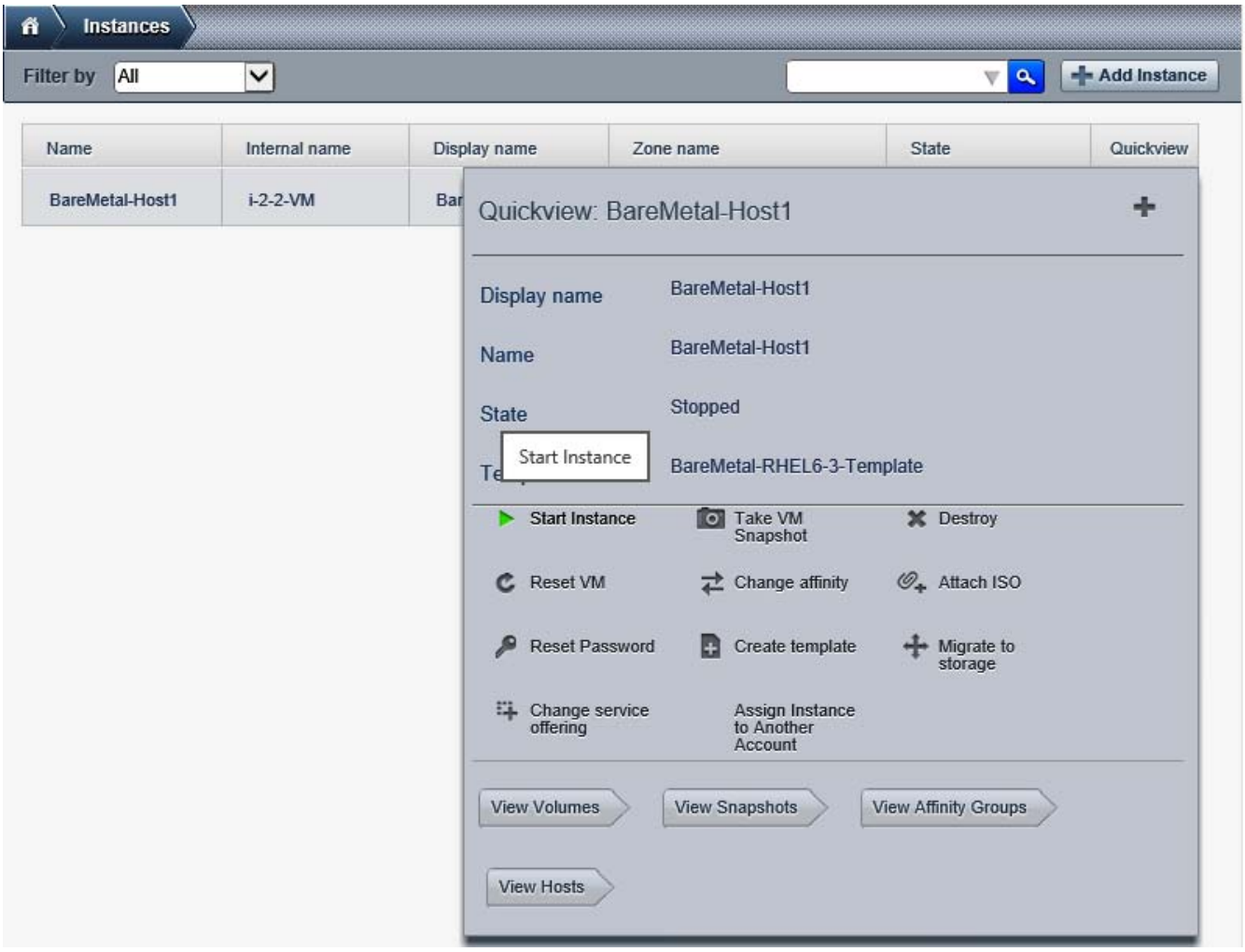


5. 停止されたインスタンスの [BareMetal-Host1] をクリックします。

図 343　停止された BareMetal-Host1 インスタンス

6. 停止されたインスタンスの [BareMetal-Host1] をクリックします。
7. [Quickview] アイコンをクリックします。
8. [Start Instance] をクリックします。

図 344　BareMetal-Host1 インスタンスの起動



9. インスタンスの復元後に BareMetal ステータスが [Running] になります。

図 345　インスタンスの復元後の BareMetal-Host1 の実行ステータス

まとめ

シスコと Citrix は、両社とも優れたクラウド ソリューションをグローバルなクライアントに提供することに真剣に取り組んでいます。両社の製品は、簡素化された物理および仮想インフラストラクチャ管理によってクラウドベースのサービスを柔軟かつ迅速に提供することができます。大手企業の多くは、シスコと Citrix のオファリングの組み合わせを選択し、Cisco UCS と Citrix CloudPlatform を利用して、堅固でスケーラブルな企業クラウドを構築しています。このマニュアルのリファレンス アーキテクチャでは、インフラストラクチャとソフトウェア設定のベスト プラクティスを提供することで、これらの製品の導入をさらに簡略化します。

参照

ここで示すドキュメントには、Citrix プライベート クラウドおよび NetApp ストレージ システムを Cisco UCS B シリーズ サーバ上に実装する方法に関連する追加情報が記載されています。

- 『Cisco Nexus QoS Switch Configuration Guide』:『Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide』
- 『Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide, Release 5.0(3)N2(1)』
- 『Citrix CloudPlatform Installation and configuration Guides』
- 『Cisco UCS System Hardware and Software Interoperability Matrix』
- 『NetApp Storage Deployment Guide』

©2008 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)
この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

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/