Cisco Virtual Network Management Center GUI コンフィギュレーション ガイド リリース 2.0

初版：2012 年 08 月 17 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number: OL-26494-01-J

【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。

目 次

はじめに

この「はじめに」は、次の項で構成されています。

対象読者

このガイドは、次の 1 つ以上に責任と専門知識を持つデータセンター管理者を主な対象にしています。

- サーバ管理
- ストレージ管理
- ネットワーク管理
- ネットワーク セキュリティ

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
第 1 章	概要	Cisco Virtual Network Management Center（VNMC）の概要について説明します。

章	タイトル	説明
第 2 章	VNMC GUI の概要	VNMC UI の概要について説明します。
第 3 章	プライマリ認証の設定	LDAP プロバイダーの設定方法およびプライマリ認証サービスの選択方法について説明します。
第 4 章	RBAC の設定	ユーザ ロケール、ユーザ ロール、ローカル認証のユーザ アカウントを含むロールベース アクセス コントロールの設定方法ついて説明します。 ユーザ セッションのモニタ方法についても説明します。
第 5 章	トラスト ポイントの設定	トラスト ポイントの設定方法について説明します。
第 6 章	VNMC プロファイルの設定	VNMC ポリシーおよびプロファイルの設定方法について説明します。
第 7 章	VNMC Manager の設定	VM Manager の設定方法について説明します。
第 8 章	テナントの設定	テナント、データセンター、アプリケーション、および階層の設定方法について説明します。
第 9 章	サービス ポリシーおよびプロファイルの設定	サービス ポリシーおよびポリシー セットの設定方法、ポリシーの確認方法、コンピュート ファイアウォールおよびエッジ ファイアウォールのセキュリティ ポリシーの設定方法、およびプロファイルのファイアウォールへの適用方法について説明します。
第 10 章	デバイス ポリシーおよびプロファイルの設定	デバイス ポリシーおよびデバイス プロファイルの設定方法、およびデバイス ポリシーをプロファイルと関連付ける方法について説明します。
第 11 章	管理対象リソースの設定	コンピュート ファイアウォール、エッジ ファイアウォール、プールなど管理対象リソースの設定方法について説明します。
第 12 章	管理操作の設定	バックアップ操作、エクスポート操作、およびインポート操作を設定する方法について説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	用途
太字フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
イタリック体	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、イタリック体フォントで示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。 string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string と見なされます。
`courier` フォント	システムが表示するターミナル セッションおよび情報表示は、`courier` フォントで示しています。
太字の `courier` フォント	ユーザが入力する情報は、**太字の `courier`** フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注）「注釈」です。

ヒント「問題解決に役立つ情報」です。

⚠ **注意** 「要注意」の意味です。 機器の損傷またはデータ損失を予防するための注意事項が記述されています。

関連資料

Cisco Virtual Network Management Center

次の Cisco Virtual Network Management Center マニュアルは、Cisco.com の次の URL で入手できます。

http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html

- 『*Cisco Virtual Network Management Center 2.0 Documentation Overview*』
- 『*Cisco Virtual Network Management Center 2.0 Release Notes*』
- 『*Cisco Virtual Network Management Center 2.0 Quick Start Guide*』
- *Cisco Virtual Network Management Center 2.0 CLI* コンフィギュレーション ガイド
- 『*Cisco Virtual Network Management Center 2.0 GUI Configuration Guide*』
- 『*Cisco Virtual Network Management Center 2.0 XML API Reference Guide*』
- 『*Open Source Used in Cisco Virtual Network Management Center 2.0*』

Cisco ASA 1000V に関するマニュアル

Cisco Adaptive Security Appliance（ASA）のマニュアルは、Cisco.com の次の URL で入手できます。

http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html

Cisco Virtual Security Gateway に関するマニュアル

Cisco VSG のマニュアルは、Cisco.com の次の URL で入手できます。

http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html

Cisco Nexus 1000V シリーズ スイッチのマニュアル

Cisco Nexus 1000V シリーズ スイッチ のマニュアルは、Cisco.com の次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバックフォームよりご連絡ください。 ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『What's New in Cisco Product Documentation』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。 RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

概要

Cisco Virtual Network Management Center（VNMC）は、Cisco 仮想サービスのデバイスおよびセキュリティ ポリシーを一元管理できる仮想アプライアンスで、Red Hat Enterprise Linux に基づいています。 VNMC はマルチテナント操作用に設計されており、仮想化されたデータセンターおよびクラウド環境をシームレスかつスケーラブルに、自動化ベースで管理します。 GUI および XML API の両方を内蔵した VNMC では、管理者またはプログラムによる Cisco 仮想サービスの一元管理ができるようになります。

VNMC は、各管理対象デバイスがパラメータで定義されたそのサブコンポーネント（つまり、オブジェクト）により表される、情報モデル主導のアーキテクチャに基づいて構築されています。 このモデル中心のアプローチにより、VNMC は Cisco Adaptive Security Appliance 1000V（ASA 1000V）および Cisco Virtual Security Gateway（VSG）仮想サービスに安全なマルチテナントの仮想化インフラストラクチャを提供できます。

次の表で、VNMC の主な機能について説明します。

表 *1*：*VNMC 2.0* 機能

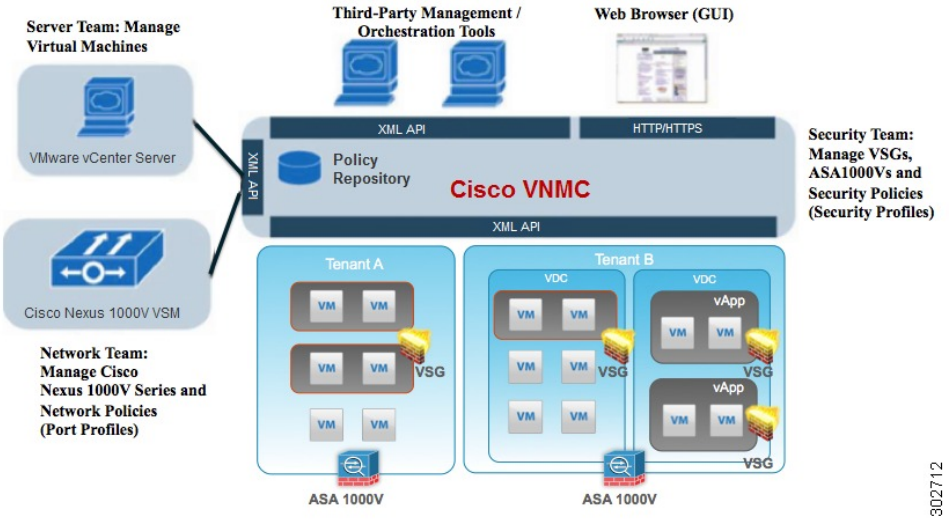
機能	説明
Multiple-Device 管理	ASA 1000V および VSG はすべて一元管理されるため、スケールアウト データセンターでのプロビジョニングとトラブルシューティングが簡略化されます。 指定したデバイス設定ポリシーを備えたデバイス プロファイルを使用することで、1 つ以上のプロファイルの管理対象リソースに整合性あるポリシーを展開できます。

機能	説明
セキュリティ プロファイル	セキュリティ プロファイルにより、プロファイルで次に示すセキュリティ ポリシー設定を表すことができます。 • プロビジョニングの簡略化 • セキュリティポリシー変更中の管理エラーの低減 • 監査の複雑さの軽減 • 高度にスケールアウトされたデータセンター環境の構築
ステートレスなデバイス プロビジョニング	VSG および ASA 1000V の管理エージェントはステートレスで、VNMC から情報を受信することで、拡張性を強化します。
セキュリティ ポリシー管理	データセンター内のすべての VSG および ASA 1000V にセキュリティ ポリシーが作成、編集およびプロビジョニングされます。これにより、セキュリティ ポリシーの操作と管理が簡略化されると同時に、関連付けられたセキュリティ ポリシーで必要なセキュリティを正確に表すことができます。
コンテキスト対応セキュリティ ポリシー	VNMC は VMware vCenter とやり取りして、仮想インフラストラクチャ全体に非常に固有なポリシー コントロールを構成できる仮想マシン（VM）コンテキストを作成できます。
動的セキュリティ ポリシーおよびゾーン プロビジョニング	VNMC は Cisco Nexus 1000V Virtual Supervisor Module（VSM）とやり取りして、セキュリティ プロファイルを対応する Cisco Nexus 1000V シリーズ スイッチ ポート プロファイルにバインドします。 VM が動的にインスタンス化され、適切なポート プロファイルに適用されると、トラストゾーンとの関連付けも確立されます。

機能	説明
マルチテナント管理	VNMC はデンス マルチテナント環境でコンピュート ファイアウォールおよびエッジ ファイアウォールのセキュリティ ポリシーを管理できます。テナントの追加や削除、テナント固有の設定やセキュリティ ポリシーの更新を高速で処理できます。 この機能により、管理エラーを大幅に減らし、管理チーム内の作業をセグメント化して監査手順を簡略化することができます。
ロールベース アクセス コントロール	ロールベースアクセスコントロール（RBAC）により、さまざまなタイプの管理者にわたって操作タスクが簡略される一方、特定分野の専門家は通常の手順を続行できます。 このサポートにより管理エラーを減らし、ユーザ特権をきめ細かく管理でき、監査要件を簡略化します。
XML ベースの API	VNMC XML アプリケーションプログラミングインターフェイス（API）では、外部システムの管理および調整ツールを使用して、プログラムによる VSG および ASA 1000V と、透過的でスケーラブルな動作管理を実現できます。

次の図は、VNMC と仮想マシン、仮想サービス、ユーザ インターフェイスおよびプログラム インターフェイスなど、マルチテナント環境のその他のコンポーネントとの関係を示しています。

図 *1*： マルチテナント環境における *VNMC*



VNMC は、マルチテナント仮想データセンターおよびプライベートまたはパブリック クラウドで、VSG および ASA 1000V のデバイスおよびポリシーを一元管理します。

VNMC は、セキュリティ ポリシーのテンプレートを使用した設定のセキュリティ プロファイルを使用します。 セキュリティ プロファイルとは、事前定義し、VM のインスタンス化時にオンデマンドで適用できるセキュリティ ポリシーの集合です。 このプロファイル駆動型アプローチは、デンス マルチテナント環境でのセキュリティ ポリシーの作成、導入、管理を大幅に簡略化しながら、導入のアジリティとスケールを向上させます。 セキュリティ プロファイルは、管理エラーの低減と監査の簡略化にも役立ちます。

VNMC XML API により、VSG および ASA 1000V のプログラムによるプロビジョニングおよび管理を行うためのサードパーティ プロビジョニング ツールとの調整が容易になります。

VNMC では視覚的な制御とプログラムによる制御が可能なため、セキュリティ作業チームは、仮想化されたインフラストラクチャのセキュリティ ポリシーを作成および管理でき、サーバとネットワークの作業チームとの連携を高めます。 この管理モデルでは、管理業務を分離したまま、管理エラーを最小限に抑え、法規制の遵守および監査を簡素化できます。 たとえば、ご使用の環境で VNMC を Cisco Nexus 1000V シリーズ VSM とともに使用して、スタッフは次のように運用と責任の整合性を保つことができます。

- セキュリティ管理者：セキュリティ プロファイルを作成および管理し、VSG および ASA 1000V インスタンスを管理します。
- ネットワーク管理者：ポート プロファイルを作成および管理し、Cisco Nexus 1000V シリーズスイッチを管理します。 参照されたセキュリティ プロファイルを備えたポート プロファイルは、Nexus 1000V VSM の VMware vCenter とのプログラム インターフェイスを介して、VMware vCenter で使用できます。

- サーバ管理者：仮想マシンをインスタンス化する場合に、VMware vCenter の適切なポートプロファイルを選択します。

VNMC は情報モデル駆動型アーキテクチャを実装し、ASA 1000V または VSG などの各管理対象デバイスはデバイスのオブジェクト情報モデルによって表されます。 特に、このモデル駆動型アーキテクチャは、次を使用する場合に役立ちます。

- ステートレス管理対象デバイス：セキュリティ ポリシーおよびオブジェクトの設定は、一元化されたリポジトリに抽象化されます。
- 動的なデバイス割り当て：リソースの一元管理機能は、動作中のデバイスのプールと動作可能なデバイスのプールを管理します。 このアプローチにより、管理対象デバイスを事前にインスタンス化してからオンデマンドで設定できるため、大規模な導入を簡素化できます。 また、動作中および動作可能プール全体でデバイスの動的な割り当てと割り当て解除を行うことができます。
- スケーラブルな管理：各管理対象デバイスで埋め込み管理エージェントを使用して実装される分散管理プレーン機能により、より拡張性を高めることができます。

第 2 章

VNMC GUI の概要

VNMC はブラウザ型インターフェイスで、管理対象エンドポイントの設定、管理運用作業の実施、ポリシーおよびプロファイルの定義と適用を行うことができます。 また、UI を使用して、VSG および ASA 1000V など、コンピュート ファイアウォールおよびエッジ ファイアウォールを管理およびプロビジョニングできます。

ここでは、VNMC ユーザ インターフェイスの概要について説明します。

VNMC およびファイアウォール アクセス

VNMC サーバがファイアウォールで保護されている場合、次のポートをイネーブルにする必要があります。

- 80：HTTP
- 443：HTTPS
- 843：Adobe Flash

VNMC ログイン

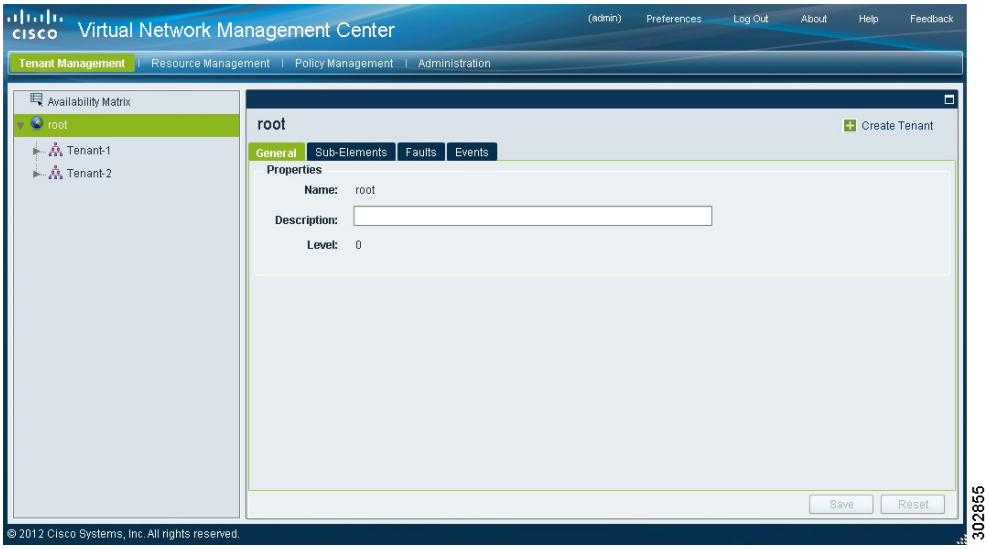
VNMC ユーザ インターフェイスにログインするためのデフォルト HTTPS URL は、https://*VNMC-ip-address* です。ここで、*VNMC-ip-address* は、VNMC サーバに割り当てられた IP アドレスです。 この IP アドレスは管理ポートのアドレスです。

（注） HTTP を使用してログインすると、HTTPS リンクに自動的にリダイレクトされます。

ユーザ インターフェイスのコンポーネント

VNMC にログインすると、ユーザ インターフェイスは次に示す図のように表示されます。

図 *2*：*VNMC* ユーザ インターフェイス



VNMCユーザインターフェイスには、次に示す表で説明するコンポーネントが含まれています。

表 *2*：*VNMC* ユーザ インターフェイスのコンポーネント

コンポーネント	説明
タイトル	「Cisco Virtual Network Management Center」を表示します。

コンポーネント	説明
ツールバー	非アクティブ タイムアウト値の設定、VNMC バージョン番号の取得、オンライン ヘルプへのアクセス、製品のフィードバックの提供ができます。
タブ	ご使用の環境のプライマリ VNMC コンポーネントにアクセスできます。 • Tenant Management • Resource Management • Policy Management • Administration
[Navigation] ペイン	VNMC インスタンスのすべてのオブジェクトへのナビゲーションを行います。 [Navigation] ペインは、タブの下の外面の左側に表示されます。 [Navigation] ペインに表示されているオブジェクトは、選択されたタブにより異なります。
[Content] ペイン	[Navigation] ペインで選択されたオブジェクトの情報を表示し、オプションを提供します。

次の表は、VNMC GUI のタブに関する情報を説明しています。

表 *3*：*VNMC GUI* のタブ

タブ	説明
Tenant Management	現在の VNMC インスタンスのテナントを管理できます。 システム管理者またはサーバ管理者は、このタブを使用して、組織階層を作成し、マルチテナント管理ドメインをイネーブルにします。 組織階層レベルは、[Tenant] > [Virtual Data Center] > [Application] > [Tier] になります。

タブ	説明
Resource Management	VSG、ASA 1000V、VSM、vCenter などの論理リソースを管理できます。 [Resource Management] のサブタブは次のとおりです。 • Managed Resources • Resources • Capabilities • Diagnostics
Policy Management	サービスおよびデバイス ポリシーおよびプロファイルを設定し、ポリシーをプロファイルへ割り当てることができます。 [Policy Management] のサブタブは次のとおりです。 • Service Profiles • Service Policies • Device Configurations • Capabilities • Diagnostics
Administration	VNMC の管理に必要なツールを提供します。 [Administration] のサブタブは次のとおりです。 • Access Control • Service Registry • VNMC Profile • VM Managers • Diagnostics • Operations

ツールバー

VNMC ツールバーは、ユーザインターフェイスの上右側に表示されます。 次の表で、ツールバーオプションについて説明します。

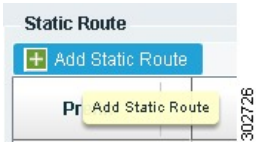
表 *4*：ツールバー オプション

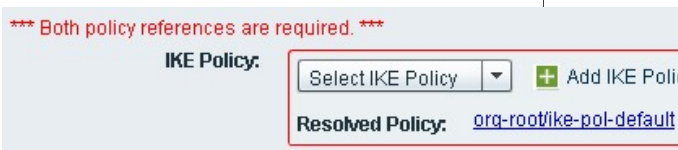
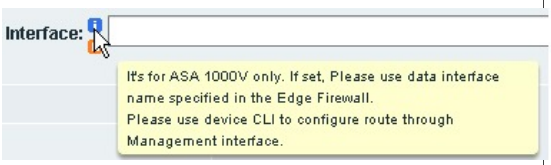
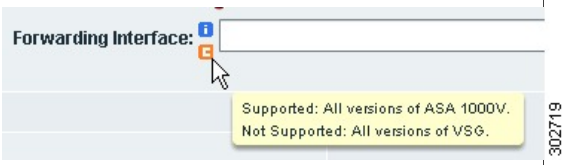
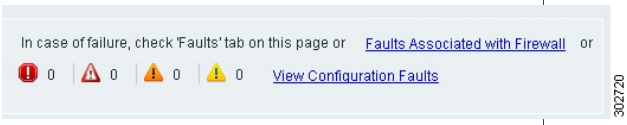
オプション	説明
(*username*)	現在の VNMC セッションのユーザ名。
Preferences	セッションがタイムアウトする前に、VNMC セッションが非アクティブの状態を保つことができる時間を指定できます。 指定する値は、VNMC にログインしたシステムに適用されます。
Log Out	現在のセッションからログアウトします。
About	VNMC バージョン情報を表示します。
Help	現在表示されている画面のオンラインヘルプを起動します。
Feedback	VNMC に関するフィードバックを表示できます。

フィールド支援機能

VNMC には、ポリシーおよびプロファイルの設定、障害のトラブルシューティング、特定のウィンドウまたはダイアログボックスの情報の検索など、作業を支援する次のような支援機能が組み込まれています。

表 *5*：*VNMC* フィールド支援機能

機能	説明	例
ツールチップ	カーソルをフィールドの上にかざすと、フィールドに関する情報が表示されます。	

機能	説明	例
赤いフィールドまたはボックス	情報が必要なことを示します。 情報を入力したときにフィールドが赤色の状態になっている場合、エントリに誤りがあります（IP アドレスが不完全など）。 カーソルをフィールドの上にかざすと、エラーに関する情報を取得できます。	
フィールドアイコン	2 つのフィールドアイコン（i および c）で、フィールドの情報が表示されます。 • 「i」アイコンは、フィールドの情報を表示します。 • 「c」アイコンは、フィールドの機能サポートを示しています。たとえば、ある機能は VSG ではなく ASA 1000V に対応しています。 カーソルをアイコンの上にかざすと、情報が表示されます。	 
障害リンク	障害情報および障害情報へのリンクが、Resource Management のエッジ ファイアウォールおよびコンピュート ファイアウォールごとに利用できます。 特定のコンピュート ファイアウォールまたはエッジ ファイアウォールに移動して、オブジェクトの状態、障害の数、障害の重大度を表示します。同じペインに、該当する障害のページへのリンクが表示されます。	
オンラインヘルプ	状況依存オンライン ヘルプは、VNMC ペインおよびダイアログボックスごとに利用できます。 ヘルプにアクセスするには、アクティブなペインで [Help] をクリックするか、またはアクティブなダイアログボックスで **?** をクリックします。	

非アクティブ タイムアウト

[Preferences] ダイアログボックスを使用すると、現在のマシン上の VNMC セッションが閉じるまでに非アクティブでいられる期間を、5～60分の間で指定できます。 ここで指定した値は、VNMC にログインするのに使用したシステムに適用されます。

第 3 章

プライマリ認証の設定

この項では、次のトピックについて取り上げます。

プライマリ認証

Cisco VNMC では、ユーザ ログインを認証するために、2 種類の方法がサポートされています。

- Cisco VNMC に対してローカル
- LDAP からのリモート

ロケール ユーザへのロールとロケールの割り当ては、VNMC で変更できます。 リモート ユーザへのロールとロケールの割り当ては、LDAP で変更できます。 ユーザに割り当てられた次のいずれかの情報を変更する場合、管理者は、新しい権限が有効になるように、そのユーザの既存のセッションをすべて削除する必要があります。

- Role
- ロールの権限
- ロケール
- ロケール内の組織

リモート認証プロバイダー

システムが対応しているリモート認証サービスについて設定されている場合、そのサービスのプロバイダーを作成し、VNMC とサービスに対して設定されているシステムが通信できるようにする必要があります。

リモート認証サービスのユーザ アカウント

VNMC またはリモート認証サーバでユーザ アカウントを作成できます。

リモート認証サービスを介してログインしているユーザの一時的なセッションは、VNMC GUI で表示できます。

リモート認証サービスのユーザ ロールおよびロケール

リモート認証サーバでユーザ アカウントを作成する場合は、ユーザが VNMC で作業するために必要なロールとロケールをアカウントに含め、それらのロールとロケールの名前をVNMCで使用される名前と一致させる必要があります。 必要なロールとロケールがアカウントに割り当てられていないと、そのユーザには読み取り専用権限だけが与えられます。

ユーザの LDAP 属性

VNMC では、LDAP ユーザ ロールおよびロケールを含む LDAP 属性がプリセットされます。 この属性は、常に、名前と値のペアで指定されます。 たとえば、デフォルトでは、CiscoAvPair でユーザのロールおよびロケール情報を指定します。フィルタが指定されている場合、LDAP 検索は、定義されたフィルタと一致する値に制限されます。 デフォルトでは、フィルタは sAMAccountName=$userid です。 ユーザは、LDAP サーバの設定と一致するようにこれらの値を変更できます。 ユーザがログインすると、リモート認証サービスにクエリーを実行してユーザを検証するときに、属性の値が VNMC によってチェックされます。 値はユーザ名と同じである必要があります。

次に、LDAP プロパティの設定例を示します。

- [Timeout]：30
- [Retries]：1
- [Attribute]：CiscoAvPair
- [Filter]：sAMAccountName=$userid
- [Base DN]：DC=cisco, DC=com（VNMC が LDAP ユーザのクエリーを開始する LDAP 階層の特定の場所）

LDAP プロバイダーの作成

はじめる前に

VNMC のユーザ ロールとロケール情報を保持する属性でユーザを設定します。 VNMC ユーザ ロールおよびロケールにマップされた既存のLDAP属性を使用するか、または1.3.6.1.4.1.9.287247.1

の属性 ID を持つ CiscoAVPair 属性などのカスタム属性を作成できます。 LDAP ユーザを LDAP サーバに追加する場合は、属性にロールとロケールを指定します（例 shell:roles=network,aaa shell:locale=sanjose,dallas）。

手順

ステップ 1 [Administration] タブで、[Access Control] > [LDAP] を選択します。

ステップ 2 [Work] ペインで、[Create LDAP Provider] をクリックします。

ステップ 3 [Create LDAP Provider] ダイアログボックスで、次の情報を入力します。

フィールド	説明
Hostname/IP Address	LDAP プロバイダーのホスト名または IP アドレス。 SSL がイネーブルの場合、このフィールドは、LDAP データベースのセキュリティ証明書内の通常名（CN）と一致している必要があります。 （注） IP アドレスではなくホスト名を使用する場合、VNMC サーバで DNS サーバを設定する必要があります。
Key	[Root DN] フィールドで指定した LDAP データベース アカウントのパスワード。 最大で 32 文字まで指定可能です。
Root DN	ベース DN の下にあるすべてのオブジェクトに対する読み取りおよび検索の権限を持つ LDAP データベース アカウントの識別名（DN）。 サポートされるストリングの最大長は 128 文字です。
Port	VNMC が LDAP データベースと通信するために使用されるポート。 デフォルト ポート番号は、389 です。
Enable SSL	オンにすると、SSL がイネーブルになります。 [Port] フィールドに 636 を入力した場合、このオプションは使用できません。

（注） テーブルで選択したオブジェクトに応じて、テーブルの上部に異なるオプションが表示されます。

ステップ 4 [OK] をクリックしてから、[Save] をクリックします。

以下に LDAP プロバイダーの作成例を示します。

- [Hostname/IP Address]：Provider-blr-sam-aaa-10.cisco.com
- [Key]：xxxxxx （[Root DN] フィールドで指定した LDAP データベース アカウントのパスワードを入力します）
- [Root DN]：CN=bob,DC=cisco,DC=com（CN の値は、クエリー権限を持つユーザの名前です。DC は、ユーザを作成する LDAP ディレクトリ内の場所です）
- [Port]：389
- [Enable SSL]：チェックボックスをオンにします

次の作業

プライマリ認証サービスとして LDAP を選択します。 詳細については、プライマリ認証サービスの選択, （20 ページ）を参照してください。

LDAP プロバイダーの編集

手順

ステップ 1 [Administration] タブで、[Access Control] > [LDAP] を選択します。

ステップ 2 [Work] ペインで、必要な LDAP プロバイダを選択します。

ステップ 3 [Edit] をクリックします。

ステップ 4 [Edit] ダイアログボックスで、次のテーブルをガイドとして使用し、必要に応じて設定を変更します。

フィールド	説明
Name	LDAP プロバイダーのホスト名または IP アドレス（読み取り専用）。 SSL がイネーブルの場合、このフィールドは、LDAP データベースのセキュリティ証明書内の通常名（CN）と一致している必要があります。 （注） IP アドレスではなくホスト名を使用する場合、VNMC サーバで DNS サーバを設定する必要があります。

フィールド	説明
Key	[Root DN] フィールドで指定した LDAP データベース アカウントのパスワード。 最大で 32 文字まで指定可能です。
Set	事前共有キーが適切に設定されている（読み取り専用）かどうか。 [Set] の値が Yes で、[Key] フィールドが空の場合は、キーが以前に指定されていることを意味します。
Root DN	ベース DN の下にあるすべてのオブジェクトに対する読み取りおよび検索の権限を持つ LDAP データベース アカウントの識別名（DN）。 サポートされるストリングの最大長は 128 文字です。
Port	VNMC が LDAP データベースと通信するために使用されるポート。 デフォルト ポート番号は、389 です。
Enable SSL	オンにすると、SSL がイネーブルになります。 [Port] フィールドに 636 を入力した場合、このオプションは使用できません。

ステップ 5 [OK] をクリックしてから、[Save] をクリックします。

LDAP プロバイダーの削除

手順

ステップ 1 [Administration] タブで、[Access Control] > [LDAP] を選択します。

ステップ 2 [Work] ペインで、削除する LDAP プロバイダをクリックし、[Delete] をクリックします。

ステップ 3 削除を確認し、[Save] をクリックします。

プライマリ認証サービスの選択

（注） デフォルトの認証が LDAP に設定されていて、LDAP サーバが動作しない、または到達不能の場合は、ローカル管理ユーザが随時ログインして認証、許可、アカウンティング（AAA）システムを変更できます。

手順

ステップ 1 [Administration] > [Access Control] > [Authentication] を選択します。

ステップ 2 [Properties] タブで、次のテーブルで説明されている情報を入力し、[OK] をクリックします。

フィールド	説明
Default Authentication	ユーザがリモートログインする際にユーザを認証するデフォルトの方法。 • [LDAP]：ユーザは、この VNMC インスタンスに指定された LDAP サーバで定義しておく必要があります。 • [Local]：ユーザはこのローカルの VNMC インスタンスで定義しておく必要があります。 • [None]：ユーザがリモートログインする際に、パスワードは必要ありません。
Role Policy to Remote Users	ユーザがログインを試みたときに、LDAP サーバから認証情報ありのユーザ ロールが提供されなかった場合のアクション。 • [assign-default-role]：ユーザは、読み取り専用ユーザ ロールでログインできます。 • [no-login]：ユーザはシステムにログインできません（ユーザ名とパスワードが正しい場合であっても）。

第 4 章

RBAC の設定

ここでは、次の内容について説明します。

RBAC

ロールベース アクセス コントロール（RBAC）は、ユーザのロールとロケールに基づいてユーザのシステムアクセスを制限または許可する方法です。 ロールによってシステム内でのユーザの権限が定義され、ロケールによってユーザがアクセス可能な組織（ドメイン）が定義されます。 権限がユーザに直接割り当てられることはないため、個々のユーザ権限の管理では、適切なロールとロケールを割り当てることが主な作業になります。

必要なシステム リソースへの書き込みアクセス権限がユーザに与えられるのは、割り当てられたロールによりアクセス権限が与えられ、割り当てられたロケールによりアクセスが許可されている場合に限ります。 たとえば、エンジニアリング組織内のサーバ管理者ロールを持つユーザは、エンジニアリング組織内のサーバ設定を更新できますが、そのユーザに割り当てられたロケールに財務組織が含まれていなければ、財務組織内のサーバ設定を更新できません。

VNMC のユーザ アカウント

ユーザ アカウントは、システムにアクセスするために使用されます。 各 VNMC インスタンスで、最大 128 個のローカルユーザ アカウントを設定できます。 各ユーザ アカウントには、一意のユーザ名が必要です。

ローカル ユーザは、パスワードまたは SSH 公開キーを使用して認証できます。 公開キーは、OpenSSH と SECSH のいずれかの形式で設定できます。

デフォルトのユーザ アカウント

各 VNMC インスタンスには、変更も削除もできないデフォルトのユーザ アカウント admin が存在します。 このアカウントは、システム管理者またはスーパーユーザアカウントであり、すべての権限が与えられています。 admin アカウントには、デフォルトのパスワードは割り当てられません。初期システム セットアップ時にパスワードを選択する必要があります。

ユーザ アカウントの有効期限

ユーザ アカウントは、事前に定義した時間に有効期限が切れるように設定できます。 有効期限の時間になると、ユーザ アカウントはディセーブルになります。

デフォルトでは、ユーザ アカウントの有効期限はありません。

VNMC ユーザ名のガイドライン

ユーザ名は、VNMC のログイン ID としても使用されます。 VNMC ユーザ アカウントにユーザ名を割り当てるときは、次のガイドラインおよび制約事項を考慮してください。

- ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。
  - 任意の英数字文字
  - ピリオド（.）
  - アンダースコア（_）
  - ハイフン（-）
  - アットマーク（@）
- 一意のユーザ名もローカル ユーザのユーザ名も数字のみでは構成できません。
- 一意のユーザ名の先頭を数字にすることはできません。
- AAA サーバ（LDAP）にすべて数字のユーザ名が存在し、ログイン時にこのユーザ名が入力された場合、VNMC はユーザをログインさせることができません。

ユーザ アカウントの作成後は、ユーザ名を変更できません。 ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

（注） 1 つの VNMC インスタンスには、最大 128 個のユーザ アカウントを作成できます。

VNMC パスワードのガイドライン

認証上の理由により、各ユーザアカウントにはパスワードが必要です。ユーザが安全性の低いパスワードを選択しないように、強力なパスワードを要求する必要があります。 [Password Strength Check] オプションがイネーブルになっている場合、VNMC は次の要件を満たさないパスワードを拒否します。

- 最低 8 文字を含む。
- 次の少なくとも 3 種類を含む。
  - 小文字の英字
  - 大文字の英字
  - 数字
  - 特殊文字
- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。 たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。
- 次の記号を含まない。ドル記号（$）、疑問符（?）、等号（=）。
- ローカル ユーザ アカウントおよび admin アカウントのパスワードは空白にしない。

（注） [Password Strength Check] オプションはデフォルトでイネーブルになっています。 [Locally Authenticated Users] ペイン（[Administration] > [Access Control] > [Locally Authenticated Users]）からディセーブルにできます。

（注） VNMC が、LDAP でリモート認証を使用するように設定されている場合、これらのリモートアカウントのパスワードは空白にできます。 この設定では、リモート クレデンシャル ストアは認証だけに使用され、許可には使用されません。 ローカル ユーザ ロールの定義は、リモート認証されたユーザに適用されます。

VNMC のユーザ ロール

ユーザ ロールには、そのロールを割り当てられたユーザに対して許可される操作を定義した 1 つ以上の権限が含まれます。 ユーザには、ロールを 1 つ以上割り当てることができます。 複数のロールを割り当てられたユーザは、すべての割り当てロールを組み合わせた権限を持ちます。 たとえば、Role1 にポリシー関連の権限が含まれ、Role2 にテナント関連の権限が含まれている場合、Role1 と Role2 の両方を割り当てられたユーザは、ポリシー関連の権限とテナント関連の権限を持つことになります。

すべてのロールには、VNMC インスタンス内のすべての設定に対する読み取りアクセス権限が含まれています。 読み取り専用ロールと他のロールとの違いは、読み取り専用ロールのみを割り当てられたユーザは、システム状態を変更できないことです。 別のロールを割り当てられたユーザは、そのユーザの割り当て領域においてシステム状態を変更できます。

システムには、次のデフォルトのユーザ ロールが用意されています。

aaa

ユーザには、ユーザ、ロール、および AAA 設定への読み取りおよび書き込みアクセス権があり、残りのシステムに読み取りアクセス権があります。

admin

ユーザには、システム全体への読み取りおよび書き込みアクセス権があり、ほとんどの権限があります。 ただし、ユーザはファイルを作成または削除したり、システムをアップグレードしたりすることはできません。 これらの機能は、デフォルトの admin アカウントでのみ行うことができます。 デフォルトの admin アカウントには、デフォルトでこのロールが割り当てられ、変更できません。

ネットワーク

ユーザは、組織、セキュリティ ポリシー、およびデバイス プロファイルを作成します。

operations

ユーザは障害を確認し、ロギング設定などの基本的な操作を実行します。

read-only

ユーザにはシステム設定および動作ステータスへの読み取り専用アクセス権はありますが、操作を実行する権限はありません。

ロールは、作成、変更（新しい権限の追加や既存の権限の削除）、および削除できます。 ロールを変更すると、そのロールに割り当てられているすべてのユーザに新しい権限が適用されます。 権限の割り当ては、デフォルトロールに定義されている権限に限定されません。 つまり、カスタムの権限の組み合わせを使用して、独自のロールを作成できます。 たとえば、デフォルトの Network および Operations ロールには異なる権限のセットがありますが、両方のロールの権限を組み合わせた新しい Network および Operations ロールを作成できます。

ロールがユーザへの割り当て後に削除されると、それらのユーザ アカウントからも削除されます。

ロケール ユーザへのロールとロケールの割り当ては、VNMC で変更できます。 リモート ユーザへのロールとロケールの割り当ては、LDAP で変更できます。 ユーザに割り当てられた次のいずれかの情報を変更する場合、管理者は、新しい権限が有効になるように、そのユーザの既存のセッションをすべて削除する必要があります。

- Role
- ロールの権限
- ロケール
- ロケール内の組織

Privileges

ユーザの権限

ユーザ ロールを割り当てられたユーザは、権限により、特定のシステム リソースへアクセスしたり、特定のタスクを実行したりできるようになります。 次の表に各権限とその説明を一覧表示します。

権限の名前	説明
AAA	システム セキュリティおよび AAA。
Admin	システム管理。
read-only	読み取り専用アクセス権。 読み取り専用は、権限として選択できません。この権限は、すべてのユーザ ロールに割り当てられます。
Resource Configuration	エッジ ファイアウォールおよびコンピュート ファイアウォールの設定。
Policy Management	エッジ ファイアウォールおよびコンピュート ファイアウォールのポリシー。
Fault Management	アラームおよびアラーム ポリシー。
Operations	ログ、コア ファイル管理、および **show tech-support** コマンド。

権限の名前	説明
Tenant Management	テナントおよび組織コンテナの作成、削除、変更。

権限とロールの割り当て

次の表に各権限のデフォルトのロール名（そのまま使用可）を一覧表示します。

デフォルトのロール名	権限の名前
aaa	aaa
admin	admin
network	policy, res-config, tenant
operations	fault, operations
read-only	read-only

ユーザ ロケール

ユーザには、ロケールを 1 つ以上割り当てることができます。 各ロケールでは、ユーザにアクセスを許可する 1 つ以上の組織またはドメイン（総称してリソースと呼ばれる）を定義します。 さらに、ユーザには割り当てられたロケール外や組織ツリーの上部での読み取り専用のアクセス権限があります。 これにより、ユーザはポリシーの作成時にこれらのリソースを使用できます。 このルールの 1 つの例外として、組織が指定されていないロケールがあります。この場合、すべての組織内のシステム リソースに対して無制限のアクセスが可能になります。 組織の下にあるオブジェクトだけがロケールによって制御されます。 組織ツリーに存在しないユーザ、ロール、およびリソースなどの他のオブジェクトへのアクセスは、ロケールの影響を受けません。

AAA 管理者権限（AAA 管理者ロール）を持つユーザは、他のユーザのロケールに組織を割り当てることができます。 組織の割り当ては、それを行うユーザのロケール内の組織だけに制限されます。 たとえば、ロケールにエンジニアリング組織しか含まれていない場合、そのロケールを割り当てられたユーザは、他のユーザにエンジニアリング組織のみを割り当てることできます。

（注） AAA 権限を持つユーザは、他のユーザの権限とロールの割り当てを管理できるので、この権限は慎重に割り当てる必要があります。

組織は階層的に管理できます。 トップ レベルの組織に割り当てられたユーザは、自動的にその下にあるすべての組織にアクセスできます。 たとえば、エンジニアリング組織が、ソフトウェア エンジニアリング組織とハードウェア エンジニアリング組織で構成されているとします。 ソフト

ウェアエンジニアリング組織のみを含むロケールでは、その組織内のシステムリソースにしかアクセスできません。一方、エンジニアリング組織が含まれるロケールでは、ソフトウェア エンジニアリング組織とハードウェア エンジニアリング組織の両方のリソースにアクセスできます。

ロケール ユーザへのロールとロケールの割り当ては、VNMC で変更できます。 リモート ユーザへのロールとロケールの割り当ては、LDAP で変更できます。 ユーザに割り当てられた次のいずれかの情報を変更する場合、管理者は、新しい権限が有効になるように、そのユーザの既存のセッションをすべて削除する必要があります。

- Role
- ロールの権限
- ロケール
- ロケール内の組織

ユーザ ロールの設定

ユーザ ロールの作成

手順

ステップ 1 [Administration] > [Access Control] > [Roles] を選択します。

ステップ 2 [Create Role] をクリックします。

ステップ 3 [Create Role] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	ユーザ ロール名です。

フィールド	説明
Privileges	使用可能な権限。 選択したロールに権限を割り当てるには、次のチェックボックスのうち 1 つ以上をオンにします。 • Admin • AAA • Fault Management • Operations • Policy Management • Resource Configuration • Tenant Management （注） すべての権限を持つ admin 権限を割り当てるか、個別に権限を割り当てることができます。

ユーザ ロールの編集

手順

ステップ 1 [Administration] > [Access Control] > [Roles] を選択します。

ステップ 2 編集するロールを選択し、[Edit] をクリックします。

ステップ 3 [Edit] ダイアログボックスで、ロールを追加する権限の各チェックボックスをオンまたはオフにし、[OK] をクリックします。

ユーザ ロールの削除

admin および読み取り専用ロールを除き、環境に適切でないユーザ ロールを削除できます。

手順

ステップ 1 [Administration] > [Access Control] > [Roles] を選択します。

ステップ 2 削除するユーザ ロールを選択し、[Delete] をクリックします。

（注） admin または読み取り専用ロールは削除できません。

ステップ 3 [Confirm] ダイアログボックスで、[Yes] をクリックします。

ユーザ ロケールの設定

ロケールの作成

はじめる前に

ロケールを作成するには、1 つ以上の組織が存在する必要があります。

手順

ステップ 1 [Administration] > [Access Control] > [Locales] を選択します。

ステップ 2 [Create Locale] をクリックします。

ステップ 3 [Create Locale] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	ロケール名。 この名前には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。保存後は、この名前を変更できません。
Description	ロケールの簡単な説明。 このフィールドには、1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。
Assigned Organizations	
Assign Organization	クリックすると、組織をロケールに割り当てることができます。

フィールド	説明
Assigned Organization	既存の組織から成るリスト。

次の作業

ロケールを 1 つまたは複数のユーザ アカウントに追加します。 詳細については、ローカル認証されたユーザ アカウントに割り当てられたロケールの変更, （36 ページ）を参照してください。

ロケールの編集

手順

ステップ 1 [Administration] > [Access Control] > [Locales] を選択します。

ステップ 2 ロケールのリストで、編集するロケールをクリックし、[Edit] をクリックします。

ステップ 3 [Description] フィールドで、必要に応じて説明を変更します。

ステップ 4 [Assign Organization] をクリックします。

ステップ 5 [Assign Organization] ダイアログボックスで、次の手順を実行します。

a) [root] ノードを展開して、利用可能な組織を表示します。

b) ロケールに割り当てる組織のチェックボックスをオンにします。

ステップ 6 開いているダイアログボックスの [OK] ボタンをクリックして、変更内容を保存します。

ロケールの削除

はじめる前に

注意 削除するロケールが任意のユーザに割り当てられている場合は、ロケールのユーザ リストからそのロケールを削除します。

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。
ステップ 2 [Navigation] ペインの [Access Control] サブタブをクリックします。
ステップ 3 [Navigation] ペインで、[Locales] ノードをクリックします。
ステップ 4 [Work] ペインで、削除するロケールをクリックします。
ステップ 5 [Delete] をクリックします。
ステップ 6 [Confirm] ダイアログボックスで、[Yes] をクリックします。

ロケールへの組織の割り当て

手順

ステップ 1 [Administration] > [Access Control] > [Locales] を選択します。
ステップ 2 必要なロケールを選択し、[Assign Organization] をクリックします。
ステップ 3 [Assign Organization] ダイアログボックスで、次の手順を実行します。
a) [root] を展開して利用可能な組織を表示します。
b) ロケールを追加する組織のチェックボックスをオンにします。
ステップ 4 開いているダイアログボックスで [OK] をクリックし、[Save] をクリックしてロケールをクリックします。

ロケールからの組織の削除

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。
ステップ 2 [Navigation] ペインの [Access Control] サブタブをクリックします。
ステップ 3 [Navigation] ペインで、[Locales] を展開します。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Assigned Organizations] 領域で、削除する組織をクリックします。
ステップ 6 [Delete Organization] リンクをクリックします。
ステップ 7 [Confirm] ダイアログボックスで、[Yes] をクリックします。

ローカル認証されたユーザ アカウントの設定

ユーザ アカウントの作成

手順

ステップ 1 [Administration] > [Access Control] > [Locally Authenticated Users] を選択します。

ステップ 2 [Create Locally Authenticated Users] をクリックします。

ステップ 3 [Properties] 領域で、次のフィールドに値を入力します。

フィールド	説明
Login ID	ログイン名 この名前は固有であるとともに、VNMCユーザアカウントに関する次のガイドラインと制約事項を満たしている必要があります。 • ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。 ◦ 任意の英数字文字 ◦ アンダースコア（_） ◦ ハイフン（-） ◦ アットマーク（@） • 各ユーザ アカウントのユーザ名をすべて数字にすることはできません。 • また、ユーザ名の先頭を数字にすることはできません。 ユーザ名を保存した後に変更することはできません。 ユーザアカウントを削除し、新しいユーザ アカウントを作成する必要があります。
Description	ユーザの説明。
First Name	ユーザの名。 このフィールドには、32 文字までの値を入力できます。

フィールド	説明
Last Name	ユーザの姓。 このフィールドには、32 文字までの値を入力できます。
Email	ユーザの電子メール アドレス。
Phone	ユーザの電話番号。

フィールド	説明
Password	このアカウントに関連付けられているパスワード。 セキュリティを最大限にするため、強力なパスワードにする必要があります。 [Password Strength Check] チェックボックスがオンになっている場合、システムは次の要件を満たさないパスワードを拒否します。 • 最低 8 文字を含む。 • 次のうち、少なくとも 3 種類を含む。 ◦ 小文字の英字 ◦ 大文字の英字 ◦ 数字 ◦ 特殊文字 • aaabbb など連続して 3 回を超えて繰り返す文字を含まない。 • ユーザ名と同一、またはユーザ名を逆にしたものではない。 • パスワード ディクショナリ チェックに合格する。 たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。 • 次の記号を含まない。 ドル記号（$）、疑問符（?）、等号（=）。 • ローカル ユーザ アカウントおよび admin アカウントのパスワードは空白にしない。 （注） [Locally Authenticated Users] ペインの [password strength] チェックボックスをオフにすると、強力なパスワードを必要としなくなることを示します。 ただし、最低 8 文字を含んでいる必要があります。 パスワード フィールドは必須フィールドであるため、ユーザを作成するにはパスワードを指定する必要があります。

フィールド	説明
Confirm Password	確認のために新しいパスワードを再入力します。
Password Expires	パスワード有効期間をイネーブルにするかどうか。パスワード有効期間をイネーブルにするには、このチェックボックスをオンにします。
Expiration Date	パスワード有効期間をイネーブルにした場合に使用できます。 パスワードが期限切れになる日付です。

ステップ 4 [Roles/Locales] タブ領域で、次のフィールドに値を入力します。

フィールド	説明
Assigned Roles	ユーザに 1 つまたは複数のロールを割り当てるには、該当するチェックボックスをオンにします。 • aaa • admin • network • operations • read-only
Assigned Locale	ユーザに 1 つまたは複数のロケールを割り当てるには、該当するチェックボックスをオンにします。

ステップ 5 [SSH] タブ領域で、次のフィールドに値を入力します。

フィールド	説明
Key	SSH キー [Key] オプション ボタンを選択すると、[SSH Data] フィールドが表示されます。
Password	SSH パスワード。

フィールド	説明
SSH Data	[Key] を選択した場合に使用できます。 SSH 公開キーを入力します。

ステップ 6 [OK] をクリックします。

ローカル認証されたユーザアカウントに割り当てられたロケールの変更

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。

ステップ 2 [Navigation] ペインの [Access Control] サブタブをクリックします。

ステップ 3 [Navigation] ペインで、[Locally Authenticated Users] ノードを展開します。

ステップ 4 *User_name*（ロケールを修正するユーザ アカウントのユーザ名を選択）をクリックします。

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

ステップ 6 [Work] ペインで、[Roles/Locales] タブをクリックします。

ステップ 7 [Assigned Locale(s)] 領域で、次の手順を実行します。

- ユーザアカウントに新しいロケールを割り当てるには、適切なチェックボックスをオンにします。
- ユーザアカウントからロケールを削除するには、適切なチェックボックスをオフにします。

ステップ 8 [Save] をクリックします。

ローカル認証されたユーザアカウントに割り当てられたロールの変更

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。

ステップ 2 [Navigation] ペインの [Access Control] サブタブをクリックします。

ステップ 3 [Navigation] ペインで、[Locally Authenticated Users] ノードを展開します。

ステップ 4 *User_name*（ロケールを修正するユーザ アカウントのユーザ名を選択）をクリックします。

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

ステップ 6 [Roles/Locales] タブをクリックします。

ステップ 7 [Assigned Role(s)] 領域で、次の手順を実行します。

- ユーザ アカウントに新しいロールを割り当てるには、適切なチェックボックスをオンにします。
- ユーザ アカウントからロールを削除するには、適切なチェックボックスをオフにします。

ステップ 8 [Save] をクリックします。

ユーザ セッションのモニタリング

ローカル認証されたユーザとリモート認証されたユーザの両方について、セッションをモニタできます。

手順

ステップ 1 [Administration] > [Access Control] を選択し、次のいずれかを選択します。

- [Locally Authenticated Users] > [user]。
- [Remotely Authenticated Users] > [*user*]。

ステップ 2 [Sessions] タブをクリックしてユーザ セッションを表示します。

フィールド	説明
Host	ユーザのログイン元である IP アドレス。
Login Time	セッションが開始された日時。

フィールド	説明
UI	このセッションのユーザ インターフェイス： • [web]：GUI ログイン • [shell]：CLI ログイン • [ep]：エンド ポイント • なし
Terminal Type	ユーザがログインするときに使用する端末の種類。

第 5 章

トラスト ポイントの設定

この項では、次のトピックについて取り上げます。

トラスト ポイント

VNMC のユーザ認証に Secure Sockets Layer（SSL）プロトコルで LDAP を設定する場合、各 LDAP サーバにトラスト ポイントを作成する必要があります。 トラスト ポイントの証明書は、次のいずれかです。

- LDAP サーバ証明書を発行した認証局（CA）の証明書。
- 認証局（CA）が階層で組織されている場合、階層内の任意の CA の証明書。
- LDAP サーバの証明書。

トラスト ポイントの設定

トラスト ポイントの作成

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。

ステップ 2 [Navigation] ペインの [Access Control] サブタブをクリックします。

ステップ 3 [Navigation] ペインで、[Trusted Point] ノードをクリックします。

ステップ 4 [Work] ペインで、[Create Trusted Point] リンクをクリックします。

ステップ 5 [Create Trusted Point] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
Name	トラスト ポイント名。 この名前には、ID となる 1 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。作成後は、この名前を変更できません。
Certificate Chain	このトラスト ポイントの証明書情報。 この説明には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。

ステップ 6 [OK] をクリックします。

トラスト ポイントの編集

手順

ステップ 1 [Administration] > [Access Control] > [Trusted Point] を選択します。

ステップ 2 編集するトラスト ポイントを選択し、[Edit] をクリックします。

ステップ 3 [Edit] ダイアログボックスで、必要に応じて証明書チェーンを変更し、[OK] をクリックします。[Fingerprint] フィールドは変更できません。

トラスト ポイントの削除

手順

ステップ 1 [Administration] > [Access Control] > [Trusted Point] を選択します。

ステップ 2 削除するトラスト ポイントを選択し、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、[Yes] をクリックして削除を確認します。

第 6 章

VNMC プロファイルの設定

この項では、次のトピックについて取り上げます。

VNMC プロファイル

Cisco VNMC プロファイルは設定可能です。

Cisco VNMC には、デフォルト プロファイルがあります。 デフォルト プロファイルはシステムで生成され、変更できますが、削除することはできません。 管理者は、syslog ポリシー、コア ポリシー、障害ポリシー、ログ ポリシー、タイム ゾーンを追加できます。 DNS および NTP ポリシーも作成できます。 設定されたポリシーは VNMC プロファイルに割り当てることができます。

VNMC プロファイルには、システムのブート設定時に付けられる、事前設定の DNS ドメイン名があります。 そのドメインは Cisco VNMC インスタンスに表示されます。 新しい DNS ドメインは作成できません。 ただし、ドメイン名の説明は変更できます。

Cisco VNMC 追加 VNMC プロファイルの作成はサポートされていません。

VNMC プロファイルのポリシー

複数のポリシーを作成し、これらを VNMC プロファイルに割り当てることができます。 VNMC プロファイルのポリシーは、[VNMC Profile] タブで作成および削除されます。 ポリシーは VNMC プロファイルに割り当てることができます。 VNMC プロファイルは、名前解決を使用してポリシーの割り当てを解決します。 詳細については、マルチテナント環境における名前解決，（84 ページ）を参照してください。

[Device Policies] 領域のルートのみで作成された次のポリシーは、VNMC プロファイルに表示されます。

- コア ファイル ポリシー
- 障害ポリシー
- ロギング ポリシー
- Syslog ポリシー

ルートで作成されたポリシーは、VNMCプロファイルとデバイスプロファイルの両方に表示されます。

DNS サーバ、NTP サーバ、ドメイン名はインラインポリシーとして割り当てることができます。タイム ゾーン設定もプロファイルに割り当てることができます。

システムの起動時、次のポリシーにはすでに既存のデフォルト ポリシーが割り当てられています。

- 障害ポリシー
- ロギング ポリシー
- Syslog ポリシー

デフォルト ポリシーは削除できませんが、変更できます。

ポリシーの設定

コア ファイル ポリシーの設定

VNMC プロファイルへのコア ファイル ポリシーの追加

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Policies] > [Core File] を選択します。

ステップ 2 [General] タブで、[Add Core File Policy] をクリックします。

ステップ 3 [Add Core File Policy] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	コア ファイル ポリシー名。 この名前には、1 ～ 32 文字の英数字を使用できます。 スペースや特殊文字は使用できません。また、オブジェクトの作成後は、この名前を変更できません。
Description	ポリシーの簡単な説明。 このフィールドには、ID となる 1 ～ 256 文字を使用できます。 ハイフン（-）、アンダースコア（_）、ドット（.）などの英数文字を使用できます。
Admin State	ポリシーの管理状態をイネーブルにするか、またはディセーブルにするかを指定します。
Hostname	このポリシーに使用するホスト名または IP アドレス。 IP アドレスではなくホスト名を使用する場合、VNMC で DNS サーバを設定する必要があります。
Port	コア ダンプ ファイルの送信に使用されるポート番号。
Protocol	コア ダンプ ファイルのエクスポートに使用されるプロトコル（読み取り専用）。
Path	リモート システムにコア ダンプ ファイルを保存するときに使用するパス。 デフォルト パスが /tftpboot のため、たとえば、/tftpboot/*test* を使用します。*test* はサブフォルダです。

VNMC プロファイルのコア ファイル ポリシーの編集

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Policies] > [Core File] を選択します。

ステップ 2 [General] タブで、編集するコア ファイル ポリシーをクリックし、[Edit] をクリックします。

ステップ 3 [Edit] ダイアログボックスで、必要に応じて次のフィールドを変更します。

フィールド	説明
Name	コア ファイル ポリシーの名前（読み取り専用）。
Description	ポリシーの簡単な説明。
Admin State	ポリシーの管理状ステータス：イネーブルまたはディセーブル。
Hostname	ホスト名または IP アドレス。 （注） ホスト名を使用する場合、DNS サーバを設定する必要があります。
Port	コア ダンプ ファイルをエクスポートするときに使用するポート番号。
Protocol	コア ダンプ ファイルのエクスポートに使用されるプロトコル（読み取り専用）。
Path	リモート システムにコア ダンプ ファイルを保存するときに使用するパス。 デフォルトのパスは /tftpboot です。 tftpboot の下位のサブフォルダを指定するには、/tftpboot/*folder* の形式を使用します。*folder* がサブフォルダです。

ステップ 4 [OK] をクリックします。

VNMC プロファイルからのコア ファイル ポリシーの削除

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Policies] > [Core File] を選択します。

ステップ 2 [General] タブで、削除するコア ファイル ポリシーをクリックし、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

障害ポリシーの設定

VNMC プロファイルへの障害ポリシーの追加

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Policies] > [Fault] を選択します。

ステップ 2 [General] タブで、[Add Fault Policy] をクリックします。

ステップ 3 [Add Fault Policy] ダイアログボックスで、次のテーブルで説明されている情報を入力し、[OK] をクリックします。

フィールド	説明
Name	障害ポリシー名。 この名前には、ID となる 1 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。作成後は、この名前を変更できません。
Description	ポリシーの簡単な説明。

フィールド	説明
Flapping Interval	システムによって障害の状態が変更されるまでに経過する必要がある時間の長さ（時間数、分数、および秒数）。 障害が発生し、すぐに何度かクリアされると、フラッピングが発生します。 これを防止するため、システムでは、最後に状態が変更されてからこの時間が経過するまで、障害が発生しても状態は変更されません。 フラッピング間隔中に同じ条件が再発生した場合は、障害がアクティブ状態に戻ります。 フラッピング間隔中に同じ条件が再発生しない場合は、障害がクリアされます。 その時点で発生する処理は、[Clear Faults Retention Action] フィールドの設定によって異なります。 デフォルトのフラッピング間隔は 10 秒です。
Clear Faults Retention Action	障害がクリアされたときに実行するアクション： • [retain]：クリアされた障害を保持します。 • [delete]：障害メッセージは、クリア対象のマークが付くと即時削除されます。
Clear Faults Retention Interval	クリアされた障害メッセージをシステムで保持する期間： • [Forever]：すべての障害メッセージは、クリアされても、経過時間に関係なく、そのまま保持されます。 • [Other]：クリアされた障害メッセージは、指定された期間の間保持されます。 このオプションを選択したときに表示されるスピンボックスで、クリアされた障害メッセージをシステムで保持する期間（日数、時間数、分数、および秒数）を入力します。

VNMC プロファイルの障害ポリシーの編集

（注） システムの起動時、すでにデフォルト ポリシーが存在します。 デフォルト ポリシーは削除できませんが、変更できます。

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Policies] > [Fault] を選択します。

ステップ 2 [General] タブで、編集する障害ポリシーを選択し、[Edit] をクリックします。

ステップ 3 [Edit Fault Policy] ダイアログボックスで、必要に応じて次のテーブルの情報を使用してフィールドを変更し、[OK] をクリックします。

フィールド	説明
Name	ポリシー名（読み取り専用）。
Description	ポリシーの簡単な説明。
Flapping Interval	システムによって障害の状態が変更されるまでに経過する必要がある時間の長さ（時間数、分数、および秒数）。 障害が発生し、すぐに何度かクリアされると、フラッピングが発生します。 これを防止するため、システムでは、最後に状態が変更されてからこの時間が経過するまで、障害が発生しても状態は変更されません。 フラッピング間隔中に同じ条件が再発生した場合は、障害がアクティブ状態に戻ります。 フラッピング間隔中に同じ条件が再発生しない場合は、障害がクリアされます。 次のアクションは、[Clear Faults Retention Action] フィールドの設定によって異なります。 デフォルトのフラッピング間隔は 10 秒です。
Clear Faults Retention Action	使用可能な、障害を保持するアクション： • [retain]：システムにより、障害メッセージが保持されます。 • [delete]：障害メッセージにクリア対象のマークを付けた時点で、それらのメッセージが削除されます。

フィールド	説明
Clear Faults Retention Interval	クリアされた障害メッセージをシステムで保持する期間： • [Forever]：すべての障害メッセージは、クリアされても、経過時間に関係なく、そのまま保持されます。 • [Other]：クリアされた障害メッセージは、指定された期間の間保持されます。 このオプションを選択したときに表示されるスピンボックスで、クリアされた障害メッセージをシステムで保持する期間（日数、時間数、分数、および秒数）を入力します。

VNMC プロファイルからの障害ポリシーの削除

（注） システムの起動時、すでにデフォルト ポリシーが存在します。 デフォルト ポリシーは削除できませんが、変更できます。

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。

ステップ 2 [Navigation] ペインの [VNMC Profile] タブをクリックします。

ステップ 3 [Navigation] ペインで、[root] > [Advanced] > [VNMC Policies] を展開します。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ 5 [General] タブで、削除する障害ポリシーをクリックします。

ステップ 6 [Delete] をクリックします。

ステップ 7 [Confirm] ダイアログボックスで、[OK] をクリックします。

ロギング ポリシーの設定

VNMC プロファイルへのロギング ポリシーの追加

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Policies] > [Log File] を選択します。

ステップ 2 [General] タブで、[Add Logging Policy] をクリックします。

ステップ 3 [Add Logging Policy] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
Name	ロギング ポリシー名。 この名前には、ID となる 1 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。作成後は、この名前を変更できません。
Description	ポリシーの簡単な説明。
Log Level	次のいずれかのロギング重大度レベル： • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical デフォルトのレベルは info です。
Backup Files Count	書き込みに使用されるバックアップ ファイルの数。この数を超えると上書きされます。 範囲は 1 ～ 9 ファイルで、デフォルトは 2 ファイルです。

フィールド	説明
File Size（bytes）	バックアップ ファイルのサイズ。 範囲は 1 ～ 100 MB で、デフォルトは 5 MB です。

ステップ 4 [OK] をクリックします。

VNMC プロファイルのロギング ポリシーの編集

（注） システムの起動時、すでにデフォルト ポリシーが存在します。 デフォルト ポリシーは削除できませんが、変更できます。

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Policies] > [Log File] を選択します。

ステップ 2 [General] タブで、編集するロギング ポリシーを選択し、[Edit] をクリックします。

ステップ 3 [Edit Log File Policy] ダイアログボックスで、必要に応じて次のテーブルの情報を使用して情報を変更し、[OK] をクリックします。

フィールド	説明
Name	ロギング ポリシー名（読み取り専用）。
Description	ポリシーの簡単な説明。

フィールド	説明
Log Level	次のいずれかのロギング レベル： • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical デフォルトのレベルは info です。
Backup Files Count	書き込みに使用されるバックアップ ファイルの数。この数を超えると上書きされます。 範囲は 1 ～ 9 ファイルで、デフォルトは 2 ファイルです。
File Size（bytes）	バックアップ ファイルのサイズ。 範囲は 1 ～ 100 MB で、デフォルトは 5 MB です。

VNMC プロファイルからのロギング ポリシーの削除

（注） システムの起動時、すでにデフォルト ポリシーが存在します。 デフォルト ポリシーは削除できませんが、変更できます。

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Policies] > [Log File] を選択します。

ステップ 2 [General] タブで、削除するロギング ポリシーをクリックし、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

Syslog ポリシーの設定

VNMC プロファイルへの Syslog ポリシーの追加

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Policies] > [Syslog] を選択します。

ステップ 2 [General] タブで、[Add Syslog] をクリックします。

ステップ 3 [Add Syslog Policy] ダイアログボックスで、次のテーブルで説明されている情報を入力し、[OK] をクリックします。
VNMC プロファイル用に設定した Syslog メッセージの設定は、VNMC Syslog メッセージにのみ適用されます。 これらの設定は、他の非 VNMC Syslog メッセージには影響しません。

フィールド	説明
[General] タブ	
Name	ポリシー名。
Description	ポリシーの簡単な説明。
Use Emblem Format	このチェックボックスをオンにして、syslog メッセージで Emblem フォーマットを使用します。 このオプションは ASA 1000V でサポートされています。 VSG ではサポートされていません。
Continue if Host is Down	このチェックボックスをオンにして、syslog サーバがダウンした場合でもロギングを続行します。 このオプションは ASA 1000V でサポートされています。 VSG ではサポートされていません。
[Servers] タブ	

フィールド	説明
Add Syslog Server	新規 syslog サーバを追加する場合にクリックします。
[Syslog Servers] テーブル	設定されている syslog サーバのリスト。
[Local Destinations] タブ	
[Console] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[alert]、[critical]、または [emergency]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。
[Monitor] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[emergency]、[alert]、[critical]、[error]、[warning]、[notification]、[information]、または [debugging]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。

フィールド	説明
[File] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[emergency]、[alert]、[critical]、[error]、[warning]、[notification]、[information]、または [debugging]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。 • [File Name]：メッセージが記録されるファイルの名前。 • [Size (bytes)]：システムがメッセージの上書きを開始する最大ファイル サイズ（バイト数）。

フィールド	説明
[Buffer] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[emergency]、[alert]、[critical]、[error]、[warning]、[notification]、[information]、または [debugging]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。 • [Buffer Size (Bytes)]：syslog メッセージのバッファのサイズ（バイト数）。 • [Wrap to Flash]：バッファが消去される（一杯になった）場合に、バッファの内容をフラッシュ メモリに保存するかどうかを指定します。 このチェックボックスをオンにすると、バッファが消去される場合に、内容をフラッシュ メモリに保存します。 • [Max File Size in Flash (KB)]：syslog バッファが使用できる最大サイズ（KB 単位）。 [Wrap to Flash] オプションがイネーブルの場合のみ、このオプションはイネーブルになります。 • [Min Free Flash Size (KB)]：syslog バッファに割り当てられる最小サイズ（KB 単位）。 [Wrap to Flash] オプションがイネーブルの場合のみ、このオプションはイネーブルになります。

VNMC プロファイル用 Syslog ポリシーの編集

（注） システムの起動時、すでにデフォルト ポリシーが存在します。 デフォルト ポリシーは削除できませんが、変更できます。

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Policies] > [Syslog] を選択します。

ステップ 2 [General] タブで、編集する Syslog ポリシーを選択し、[Edit] をクリックします。

ステップ 3 [Edit Syslog Policy] ダイアログボックスで、必要に応じて次のテーブルの情報を使用して情報を更新し、[OK] をクリックします。

フィールド	説明
[General] タブ	
Name	ポリシー名。
Description	ポリシーの簡単な説明。
Use Emblem Format	このチェックボックスをオンにして、syslogメッセージで Emblem フォーマットを使用します。 このオプションは ASA 1000V でサポートされています。 VSG ではサポートされていません。
Continue if Host is Down	このチェックボックスをオンにして、syslogサーバがダウンした場合でもロギングを続行します。 このオプションは ASA 1000V でサポートされています。 VSG ではサポートされていません。
[Servers] タブ	
Add Syslog Server	新規 syslog サーバを追加する場合にクリックします。
[Syslog Servers] テーブル	設定されている syslog サーバのリスト。
[Local Destinations] タブ	

フィールド	説明
[Console] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[alert]、[critical]、または [emergency]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。
[Monitor] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[emergency]、[alert]、[critical]、[error]、[warning]、[notification]、[information]、または [debugging]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。
[File] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[emergency]、[alert]、[critical]、[error]、[warning]、[notification]、[information]、または [debugging]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。 • [File Name]：メッセージが記録されるファイルの名前。 • [Size (bytes)]：システムがメッセージの上書きを開始する最大ファイル サイズ（バイト数）。

フィールド	説明
[Buffer] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[emergency]、[alert]、[critical]、[error]、[warning]、[notification]、[information]、または [debugging]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。 • [Buffer Size (Bytes)]：syslog メッセージのバッファのサイズ（バイト数）。 • [Wrap to Flash]：バッファが消去される（一杯になった）場合に、バッファの内容をフラッシュ メモリに保存するかどうかを指定します。 このチェックボックスをオンにすると、バッファが消去される場合に、内容をフラッシュ メモリに保存します。 • [Max File Size in Flash (KB)]：syslog バッファが使用できる最大サイズ（KB 単位）。 [Wrap to Flash] オプションがイネーブルの場合のみ、このオプションはイネーブルになります。 • [Min Free Flash Size (KB)]：syslog バッファに割り当てられる最小サイズ（KB 単位）。 [Wrap to Flash] オプションがイネーブルの場合のみ、このオプションはイネーブルになります。

VNMC プロファイルからの Syslog ポリシーの削除

（注） システムの起動時、すでにデフォルト ポリシーが存在します。 デフォルト ポリシーは削除できませんが、変更できます。

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Policies] > [Syslog] を選択します。

ステップ 2 [General] タブでは、削除する syslog ポリシーをクリックし、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

VNMC プロファイルへの Syslog サーバの追加

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Policies] > [Syslog] を選択します。

ステップ 2 [General] タブで、[Add Syslog Policy] をクリックします。

ステップ 3 [Add Syslog Policy] ダイアログボックスで、[Add Syslog Server] をクリックします。

ステップ 4 [Add Syslog Server] ダイアログボックスで、次のテーブルで説明されている情報を入力します。

フィールド	説明
Server Type	次のいずれかのサーバ タイプ： • primary • secondary • tertiary
Hostname/IP Address	syslog ファイルが置かれている場所のホスト名または IP アドレス。

フィールド	説明
Severity	次のいずれかの重大度レベル： • emergencies（0） • alerts（1） • critical（2） • errors（3） • warnings（4） • notifications（5） • information（6） • debugging（7）
Forwarding Facility	次のいずれかの転送するファシリティ： • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp

フィールド	説明
Admin State	ポリシーの管理状態：イネーブルまたはディセーブル。
Port	syslog サーバへのデータの送信に使用するポート。 ポートの有効な値は、TCP と UDP のいずれでも 1025 ～ 65535 です。 デフォルトの TCP ポートは 1470 です。 デフォルトの UDP ポートは 514 です。
Protocol	このポリシーに使用するプロトコル：TCP または UDP。
Use Transport Layer Security	このチェックボックスをオンにして、トランスポート層セキュリティを使用します。 このオプションは、TCP の場合にのみ使用できます。
Server Interface	syslog サーバにアクセスするために使用するインターフェイス。

ステップ 5 開いているダイアログボックスで [OK] をクリックします。

VNMC プロファイル用 Syslog サーバの編集

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Policies] > [Syslog] を選択します。

ステップ 2 [General] タブで、編集する Syslog サーバを持つ Syslog ポリシーをクリックし、[Edit] をクリックします。

ステップ 3 [Edit Syslog Policy] ダイアログボックスで、[Servers] タブをクリックします。

ステップ 4 編集する Syslog サーバを選択し、[Edit] をクリックします。

ステップ 5 [Edit Syslog Server] ダイアログボックスで、必要に応じて次のテーブルの情報を使用して情報を編集します。

名前	説明
Server Type	次のいずれかのサーバ タイプ：primary、secondary、または tertiary（読み取り専用）。
Hostname/IP Address	syslog ファイルが置かれている場所のホスト名または IP アドレス。
Severity	次のいずれかの重大度レベル： • emergencies（0） • alerts（1） • critical（2） • errors（3） • warnings（4） • notifications（5） • information（6） • debugging（7）

名前	説明
Forwarding Facility	次のいずれかの転送するファシリティ： • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp
Admin State	ポリシーの管理状態：イネーブルまたはディセーブル。
Port	syslog サーバへのデータの送信に使用するポート。 ポートの有効な値は、TCP と UDP のいずれでも 1025 ～ 65535 です。 デフォルトの TCP ポートは 1470 です。 デフォルトの UDP ポートは 514 です。
Protocol	使用するプロトコル：TCP または UDP。

名前	説明
Use Transport Layer Security	このチェックボックスをオンにして、トランスポート層セキュリティを使用します。 このオプションは、TCP の場合にのみ使用できます。
Server Interface	syslog サーバにアクセスするために使用するインターフェイス。 このオプションは、ASA 1000V にのみ適用されます。 エッジ ファイアウォールで指定されているデータ インターフェイス名を入力します。 デバイス CLI を使用して、管理インターフェイス経由でのルートを設定します。

ステップ 6 開いているダイアログボックスで [OK] をクリックします。

VNMC プロファイルからの Syslog サーバの削除

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。
ステップ 2 [Navigation] ペインの [VNMC Profile] タブをクリックします。
ステップ 3 [Navigation] ペインで、[root] > [Advanced] > [VNMC Policies] を展開します。
ステップ 4 [Navigation] ペインで、[Syslog] ノードをクリックします。
ステップ 5 [Work] ペインで、[General] タブをクリックします。
ステップ 6 [General] タブで、[Add Syslog] リンクをクリックします。
ステップ 7 [Add Syslog] ダイアログボックスで、[Servers] タブをクリックします。
ステップ 8 [Servers] タブで、削除する Syslog サーバをクリックします。
ステップ 9 [Delete] をクリックします。
ステップ 10 [Confirm] ダイアログボックスで、[Yes] をクリックします。

デフォルト プロファイルの設定

VNMC デフォルト プロファイルの編集

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Profile] > [default] を選択します。

ステップ 2 [General] タブで、必要に応じて情報を更新します。

フィールド	説明
Name	デフォルトプロファイル名（読み取り専用）。
Description	プロファイルの簡単な説明。
Time Zone	使用可能な時間帯名。 デフォルトの時間帯は UTC です。

ステップ 3 [Policy] タブで、必要に応じて情報を更新します。

フィールド	説明
DNS Servers	
Add DNS Server	新規 DNS サーバを追加する場合にクリックします。
Delete	[DNS Servers] テーブルで選択された DNS サーバを削除します。
Up and down arrows	選択したDNSサーバの優先順位を変更します。 VNMC は、DNS サーバをテーブルに表示される順に使用します。
[DNS Servers] テーブル	システムで設定されている DNS サーバを指定します。
NTP Servers	
Add NTP Server	新規 NTP サーバを追加する場合にクリックします。

フィールド	説明
Delete	[NTP Servers] テーブルで選択された NTP サーバを削除します。
Up and down arrows	選択した NTP サーバの優先順位を変更します。 VNMC は、NTP サーバをテーブルに表示される順に使用します。
[NTP Servers] テーブル	システムで設定されている NTP サーバを指定します。
DNS Domains	
Edit	[DNS Domains] テーブルで選択された DNS ドメインを編集します。 デフォルトの DNS ドメインは編集できません。
DNS Domains	システムで設定されている DNS ドメインおよびデフォルトのドメイン名を指定します。
Other Options	
Syslog	このプロファイルに関連付けられた syslog ポリシーを選択、追加、または編集できます。 指定したポリシーを確認または変更するには、[Resolved Policy] フィールドをクリックします。
Fault	このプロファイルに関連付けられた障害ポリシーを選択、追加、または編集できます。 指定したポリシーを確認または変更するには、[Resolved Policy] フィールドをクリックします。
Core File	このプロファイルに関連付けられたコア ファイル ポリシーを選択、追加、または編集できます。 指定したポリシーを確認または変更するには、[Resolved Policy] フィールドをクリックします。
Log File	このプロファイルに関連付けられたログ ファイル ポリシーを選択、追加、または編集できます。 指定したポリシーを確認または変更するには、[Resolved Policy] フィールドをクリックします。

ステップ 4 [Save] をクリックします。

DNS サーバの設定

DNS サーバの追加

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Profile] > [default] を選択します。

ステップ 2 [Policy] タブをクリックします。

ステップ 3 [DNS Servers] 領域で、[Add DNS Server] をクリックします。

ステップ 4 [Add DNS Server] ダイアログボックスで、DNS サーバの IP アドレスを入力します。
最大 4 個の DNS サーバを指定できます。

ステップ 5 [Save] をクリックします。

DNS サーバの削除

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。

ステップ 2 [Navigation] ペインの [VNMC Profile] タブをクリックします。

ステップ 3 [Navigation] ペインで、[root] > [VNMC Profile] を展開します。

ステップ 4 [Navigation] ペインで、[default] をクリックします。

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

ステップ 6 [DNS Servers] 領域で、削除する IP アドレスをクリックします。

ステップ 7 [Delete] リンクをクリックします。

ステップ 8 [Confirm] ダイアログボックスで、[Yes] をクリックします。

ステップ 9 [Work] ペインで、[Save] をクリックします。

NTP サーバの設定

NTP サーバの追加

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Profile] > [default] を選択します。

ステップ 2 [Policy] タブで、[Add NTP Server] をクリックします。

ステップ 3 [Add NTP server] ダイアログボックスで、ドメイン ネーム システム（NTP）サーバのホスト名または IP アドレスを入力します。

（注） 最大 4 個の NTP サーバを含めることができます。 リストの一番上に最も優先順位の高いサーバが来るように、上下の矢印を使用して優先順位の高いものから低いものに配置します。

ステップ 4 [Save] をクリックします。

NTP サーバの削除

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Profile] > [default] を選択します。

ステップ 2 [Policy] タブをクリックします。

ステップ 3 [NTP Servers] 領域で、削除するサーバをクリックし、[Delete] をクリックします。

ステップ 4 確認の画面が表示されたら、削除を確認します。

ステップ 5 [Save] をクリックします。

DNS ドメインの設定

DNS ドメインの編集

注意 DNS ドメインを変更すると、接続が失われてしまい、エラーメッセージが表示され、セッションが閉じ、新しい VNMC 証明書が表示されます。 この状況は、VNMC ホスト名か、 VNMC ドメイン名、またはその両方が変更されると発生します。 VM Manager 拡張ファイルを再びエクスポートし、vCenter にインストールする必要があります。 続行するには、VNMC 証明書を受け入れ、VNMC に再度ログインします。

手順

ステップ 1 [Administration] > [VNMC Profile] > [root] > [VNMC Profile] > [default] を選択します。

ステップ 2 [Policy] タブをクリックします。

ステップ 3 [DNS Domains] テーブルで、編集するドメインをクリックし、[Edit] をクリックします。

ステップ 4 [Edit DNS Domains] ダイアログボックスで、必要に応じて [Domain Name] フィールドを編集し、[OK] をクリックします。

ステップ 5 [Save] をクリックします。

第 7 章

VM Manager の設定

この項では、次のトピックについて取り上げます。

VM Manager の概要

VNMC VM Manager は、ポート 80 で vCenter と接続します。 VM Manager と vCenter の接続を確立するには、vCenter 拡張ファイルが必要です。 拡張ファイルは VNMC からエクスポートされ、[VM Managers] タブでリンクされます。 vCenter 拡張ファイルをプラグインとして、接続するすべての vCenter サーバにインストールします。

ご使用の環境と要件に応じて、[Administration] または [Resource Management] で VNMC に VM Manager をインストールできます。 詳細については、次のトピックを参照してください。

- [Administration] での VM Manager の追加, （74 ページ）
- [Resource Management] での VM Manager の追加, （77 ページ）

（注） VMware では、VM はリソース内で入れ子にできます。 たとえば、VM は仮想アプリケーション（vApp）に常駐するリソースプールの一部になることができます。 ただし、VM プロパティを表示する場合（[Resource Management] > [Resources] > [Virtual Machines] > [VM Managers] > [*vm-manager*] > [*vm*]）、最上部のリソースのみ表示されます。 この例では、リソースプールの名前ではなく vApp 名だけが表示されます。

[Administration] での VM Manager の設定

[Administration] での VM Manager の追加

[Resource Management] または [Administration] で VM Manager を VNMC に追加できます。 この手順では、[Administration] で VM Manager を追加する方法について説明します。 [Resource Management] で VM Manager を追加する方法については、[Resource Management] での VM Manager の追加, （77 ページ）を参照してください。

はじめる前に

vCenter と VM Manager 間の安全な接続を確立するには、vCenter 拡張ファイルが必要です。 [Export vCenter Extension] をクリックし、vCenter 拡張ファイルをすべての vCenter サーバにプラグインとしてインストールして、vCenter 拡張ファイルをエクスポートします。

次の場所から [Export vCenter Extension] オプションを探します。

- [Resource Management] > [Resources] > [Virtual Machines] > [VM Managers] を選択し、[VM Managers] タブをクリックします。
- [Administration] > [VM Managers] > [VM Managers] を選択し、[VM Managers] タブをクリックします。

（注） vCenter の [Plug-In Manager] ページで、ページの最後までスクロールし、右クリックして [New Plug-in] メニューを表示します。

手順

ステップ 1 [Administration] > [VM Managers] > [VM Managers] を選択します。

ステップ 2 [VM Managers] タブで、[Add VM Manager] をクリックします。

ステップ 3 [Add VM Manager] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	VM Manager 名。 この名前には、ID となる 1 ～ 256 文字を使用できます。 ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。 保存後は、この説明を変更できません。

フィールド	説明
Description	VM Manager の簡単な説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。
Hostname/IP Address	VM Manager のホスト名または IP アドレス。
Port Number	VM Manager との通信に使用するポート。

VM Manager を追加すると、VNMC が Nexus 1000V ポートプロファイルが添付された、vCenter で利用可能な VM を取得し、それらを [Resource Management] > [Resources] > [Virtual Machines] に表示します。

VM Manager の編集

手順

ステップ 1 [Administration] > [VM Managers] > [VM Managers] を選択します。

ステップ 2 [VM Managers] タブで、編集する VM Manager をクリックし、[Edit] をクリックします。

ステップ 3 [Edit VM Manager] ダイアログボックスで、必要に応じて情報を編集し、[OK] をクリックします。

名前	説明
Name	VM Manager 名（読み取り専用）。
Description	VM Manager の説明。
Hostname/IP Address	VM Manager のホスト名または IP アドレス（読み取り専用）。
Port Number	VM Manager との通信に使用するポート（読み取り専用）。

名前	説明
Admin State	VM Manager の次のいずれかの管理状態。 • [enable]：管理状態がイネーブルで vCenter を VNMC に追加した場合、システムはすべての VM インベントリを vCenter から取得します。 vCenter で発生した VM のすべての変更も取得されます。 • [disable]：管理状態がディセーブルの VNMC に vCenter を追加した場合に、vCenter から検出されたすべての VM が表示されます。 vCenter で発生した VM の変更は取得されません。 管理状態をイネーブルに変更すると、VNMC によって変更が取得されます。 VM Manager の管理状態は、システムの動作状態に応じて変更します。 • システムの管理状態をイネーブルに変更するには、動作状態を down にしておく必要があります。 • システムの管理状態をディセーブルに変更するには、動作状態を up にしておく必要があります。 管理状態を変更する要求に失敗する場合は、正しいシステムの動作状態で要求を再送信します。
Type	VM Manager ベンダー（読み取り専用）。
Version	VM Manager のバージョン（読み取り専用）。
Operational State	次のいずれかの動作状態（読み取り専用）。 • up • unreachable • bad-credentials • comm-error • admin-down • unknown

名前	説明
Operational State Reason	動作状態が *up* でない場合の動作状態の原因を表示します（読み取り専用）。

VM Manager の削除

手順

ステップ 1 [Administration] > [VM Managers] > [VM Managers] を選択します。

ステップ 2 [VM Managers] タブで、削除する VM Manager をクリックし、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

[Resource Management] での VM Manager の設定

[Resource Management] での VM Manager の追加

[Resource Management] または [Administration] で VM Manager を VNMC に追加できます。 この手順では、[Resource Management] で VM Manager を追加する方法について説明します。 [Administration] で VM Manager をインストールする方法については、[Administration] での VM Manager の追加, （74 ページ）を参照してください。

はじめる前に

vCenter と VM Manager 間の安全な接続を確立するには、vCenter 拡張ファイルが必要です。 [Export vCenter Extension] をクリックし、vCenter 拡張ファイルをすべての vCenter サーバにプラグインとしてインストールして、vCenter 拡張ファイルをエクスポートします。

次の場所から [Export vCenter Extension] オプションを探します。

- [Resource Management] > [Resources] > [Virtual Machines] > [VM Managers] を選択し、[VM Managers] タブをクリックします。
- [Administration] > [VM Managers] > [VM Managers] を選択し、[VM Managers] タブをクリックします。

（注） [vCenter Plug-In Manager] ページで、ページの最後までスクロールし、右クリックして [New Plug-in] メニューを表示します。

手順

ステップ 1 [Resource Management] > [Resources] > [Virtual Machines] > [VM Managers] を選択します。

ステップ 2 [VM Managers] タブで、[Add VM Manager] をクリックします。

ステップ 3 [Add VM Manager] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	VM Manager 名。 この名前には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。保存後は、この説明を変更できません。
Description	VM Manager の簡単な説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。
Hostname/IP Address	VM Manager のホスト名または IP アドレス。
Port Number	VM Manager との通信に使用するポート。

VM Manager を追加すると、VNMC が Nexus 1000V ポート プロファイルが添付された、vCenter で利用可能な VM を取得し、それらを [Resource Management] > [Resources] > [Virtual Machines] に表示します。

VM Manager の編集

手順

ステップ 1 [Resource Management] > [Resources] > [Virtual Machines] > [VM Managers] を選択します。

ステップ 2 [VM Managers] タブで、編集する VM Manager をクリックし、[Edit] をクリックします。

ステップ 3 [Edit VM Manager] ダイアログボックスで、必要に応じて情報を編集し、[OK] をクリックします。

名前	説明
Name	VM Manager 名（読み取り専用）。
Description	VM Manager の説明。
Hostname/IP Address	VM Manager のホスト名または IP アドレス（読み取り専用）。
Port Number	VM Manager との通信に使用するポート（読み取り専用）。

名前	説明
Admin State	VM Manager の次のいずれかの管理状態。 • [enable]：管理状態がイネーブルで vCenter を VNMC に追加した場合、システムはすべての VM インベントリを vCenter から取得します。 vCenter で発生した VM のすべての変更も取得されます。 • [disable]：管理状態がディセーブルの VNMC に vCenter を追加した場合に、vCenter から検出されたすべての VM が表示されます。 vCenter で発生した VM の変更は取得されません。 管理状態をイネーブルに変更すると、VNMC によって変更が取得されます。 VM Manager の管理状態は、システムの動作状態に応じて変更します。 • システムの管理状態をイネーブルに変更するには、動作状態を down にしておく必要があります。 • システムの管理状態をディセーブルに変更するには、動作状態を up にしておく必要があります。 管理状態を変更する要求に失敗する場合は、正しいシステムの動作状態で要求を再送信します。
Type	VM Manager ベンダー（読み取り専用）。
Version	VM Manager のバージョン（読み取り専用）。
Operational State	次のいずれかの動作状態（読み取り専用）。 • up • unreachable • bad-credentials • comm-error • admin-down • unknown

名前	説明
Operational State Reason	動作状態が *up* でない場合の動作状態の原因を表示します（読み取り専用）。

VM Manager の削除

手順

ステップ 1 [Navigation] ペインの [Resource Management] タブをクリックします。

ステップ 2 [Navigation] ペインの [Resources] サブタブをクリックします。

ステップ 3 [Navigation] ペインで、[Virtual Machines] をクリックします。

ステップ 4 [Work] ペインで、[VM Managers] タブをクリックします。

ステップ 5 [VM Managers] テーブルで、削除する VM Manager をクリックします。

ステップ 6 [Delete] をクリックします。

ステップ 7 [Confirm] ダイアログボックスで、[Yes] をクリックします。

第 8 章

テナントの設定

この項では、次のトピックについて取り上げます。

テナント管理

テナント管理およびマルチテナント環境

VNMCには、マルチテナント環境をサポートする機能があります。 マルチテナント環境により、大規模な物理インフラストラクチャを組織と呼ばれる論理エンティティに分割できます。 その結果、各組織に専用の物理インフラストラクチャを設けなくても各組織を論理的に分離できます。

管理者は、マルチテナント環境で関連する組織を通して、各テナントに一意のリソースを割り当てることができます。 これらのリソースには、異なるポリシー、プール、デバイス プロファイル、ファイアウォールなどを含めることができます。 特定の組織へのアクセスを制限する必要がある場合、管理者はロケールを使用して、ユーザ権限とロールを組織別に割り当てたり、制限したりすることができます。

VNMC は、次のような厳格な組織階層を提供します。

1. ルート
2. テナント
3. データセンター
4. アプリケーション

5 階層

ルートには、複数のテナントを含めることができます。 各テナントには複数のデータセンターを含めることができます。 各データセンターには複数のアプリケーションを、各アプリケーションには複数の階層を含めることができます。

ルート レベルで作成されたポリシーとプールはシステム全体を対象とし、システムのすべての組織が利用できます。 ただし、ルート レベルより下の組織で作成されたポリシーおよびプールは、同じ階層のその組織の下にあるリソースにのみ使用できます。

たとえば、システムにCompany AとCompany Bというテナントがある場合、Company AはCompany B組織で作成されたポリシーを使用できません。 Company Bは、Company A組織で作成されたポリシーにアクセスできません。 しかし、Company AとCompany Bは両方とも、ルート組織のポリシーとプールを使用できます。

マルチテナント環境における名前解決

マルチテナント環境では、VNMCは組織の階層を使用して、ポリシーおよびリソースプールの名前を解決します。 VNMCがポリシーおよびリソース プールの名前を解決する手順は次のとおりです。

1. VNMCは、デバイス プロファイルまたはセキュリティ ポリシーに割り当てられた組織内のポリシーとプールで指定された名前をチェックします。
2. ポリシーまたはプールが見つからない場合、VNMCはそのポリシーまたはプールを使用します。
3. ポリシーまたはプールにそのローカル レベルで使用できるリソースが含まれていない場合、VNMCは親組織まで階層を移動し、指定された名前のポリシーをチェックします。 VNMCは、ルート組織に到達するまでこの手順を繰り返します。

（注） オブジェクト名参照解決では、オブジェクト名を使用して、組織コンテナからのオブジェクトを、ツリーのルート レベルまでで最も近くにある同じ名前のオブジェクトに解決します。 指定された名前のオブジェクトが見つからない場合は、対応するデフォルト オブジェクトが使用されます。 たとえば、データセンターにMySNMPと呼ばれるSNMPポリシーがあり、同じツリーのテナントにもMySNMPというSNMPポリシーがあるとします。 この場合、ユーザはテナントのMySNMPポリシーを明示的に選択することができません。 ユーザがテナントのSNMPポリシーを選択するには、そのツリーでオブジェクトに一意の名前を付ける必要があります。

4. 検索がルート組織に到達し、割り当てられたポリシーまたはプールが見つからない場合は、VNMCは現在のレベルからルート レベルまでの間でデフォルト ポリシーまたはプールを探します。 デフォルト ポリシーまたはプールが見つからない場合は、VNMCがそれを使用しています。 ポリシーが使用できない場合、障害が生成されます。

テナントの設定

テナントの作成

手順

ステップ 1 [Tenant Management] > [root] を選択します。

ステップ 2 [Create Tenant] をクリックします。

ステップ 3 [Create Tenant] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	テナント名。 この名前には、ID となる 1 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。作成後は、この名前を変更できません。
Description	テナントの簡単な説明。 このフィールドには、1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。

テナントの編集

手順

ステップ 1 [Tenant Management] > [root] を選択します。

ステップ 2 [Sub-Elements] タブをクリックします。

ステップ 3 編集するテナントを選択し、[Edit] をクリックします。

ステップ 4 [Edit Tenant] ダイアログボックスで、説明を変更し、[OK] をクリックします。 [Level] フィールドは、テナントのレベルを階層で識別し、読み取り専用です。

テナントの削除

（注） 組織を削除すると、サブ組織、コンピュート ファイアウォール、エッジ ファイアウォール、リソース プール、ポリシーなど、その組織に含まれるすべてのデータが削除されます。

手順

ステップ 1 [Tenant Management] > [root] を選択します。

ステップ 2 [General] タブで、削除するテナントをクリックし、[Delete Tenant] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

データセンターの設定

仮想データセンターの作成

手順

ステップ 1 [Tenant Management] > [root] > [*tenant*] を選択します。ここで [*tenant*] は新しい仮想データセンターの場所です。

ステップ 2 [General] タブで [Create Virtual Data Center] をクリックします。

ステップ 3 [Create Virtual Data Center] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	VDC の名前を指定します。 この名前には、ID となる 1 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。作成後は、この名前を変更できません。
Description	VDC の簡単な説明。 このフィールドには、1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。

仮想データセンターの編集

手順

ステップ 1 [Navigation] ペインの [Tenant Management] タブをクリックします。

ステップ 2 [Tenant Management] > [root] > [*tenant*] を選択します。

ステップ 3 [Sub-Elements] タブをクリックします。

ステップ 4 [Sub-Elements] タブで、編集する仮想データセンターを選択し、[Edit] をクリックします。

ステップ 5 [Edit Virtual Data Center] ダイアログボックスで、説明を変更し、[OK] をクリックします。 [Level] フィールドは、仮想データセンターのレベルを階層で識別し、読み取り専用です。

仮想データセンターの削除

（注） 仮想データセンターを削除すると、サブ組織、ファイアウォール、リソースプール、ポリシーなど、その仮想データセンターに含まれるすべてのデータが削除されます。

手順

ステップ 1 [Tenant Management] > [root] > [*tenant*] を選択します。ここで [*tenant*] は削除する仮想データセンターを持つテナントです。

ステップ 2 [Sub-Elements] タブをクリックします。

ステップ 3 削除する仮想データセンターを選択し、[Delete Virtual Data Center] をクリックします。

ステップ 4 確認の画面が表示されたら、削除を確認します。

アプリケーションの設定

アプリケーションの作成

手順

ステップ 1 [Tenant Management] > [root] > [*tenant*] > [*vdc*] を選択します。ここで [*vdc*] は新しいアプリケーションの場所です。

ステップ 2 [General] タブで [Create Application] をクリックします。

ステップ 3 [Create Application] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	アプリケーションの名前。 この名前には、ID となる 1 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。作成後は、この名前を変更できません。
Description	アプリケーションの簡単な説明。 このフィールドには、1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。

アプリケーションの編集

手順

ステップ 1 [Tenant Management] > [root] > [*tenant*] > [*virtual-data-center*] を選択します。ここで [*virtual-data-center*] は編集するアプリケーションと仮想データセンターです。

ステップ 2 [Sub-Elements] タブをクリックします。

ステップ 3 編集するアプリケーションを選択し、[Edit] をクリックします。

ステップ 4 [Edit Application] ダイアログボックスで、必要に応じて説明を変更し、[OK] をクリックします。[Level] フィールドは、アプリケーションのレベルを階層で識別し、読み取り専用です。

アプリケーションの削除

（注） アプリケーションを削除すると、サブ組織、ファイアウォール、リソース プール、ポリシーなど、そのアプリケーションに含まれるすべてのデータが削除されます。

手順

ステップ 1 [Navigation] ペインの [Tenant Management] タブをクリックします。

ステップ 2 [Tenant Management] > [root] > [*tenant*] > [*virtual-data-center*] を選択します。ここで [*virtual-data-center*] は削除するアプリケーションと仮想データセンターです。

ステップ 3 [Sub-Elements] タブをクリックします。

ステップ 4 削除するアプリケーションを選択し、[Delete Application] をクリックします。

ステップ 5 確認の画面が表示されたら、削除を確認します。

階層の設定

階層の作成

手順

ステップ 1 [Tenant Management] > [root] > [*tenant*] > [*vdc*] > [*application*] を選択します。ここで [*application*] は新しい階層の場所です。

ステップ 2 [General] タブで [Create Tier] をクリックします。

ステップ 3 [Create Tier] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	階層の名前。 この名前には、ID となる 1 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。作成後は、この名前を変更できません。
Description	階層の説明。 このフィールドには、1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。

階層の編集

手順

ステップ 1 [Tenant Management] > [root] > [*tenant*] > [*virtual-data-center*] > [*application*] > [*tier*] を選択します。ここで [*tier*] は編集する階層です。

ステップ 2 [Properties] タブで、必要に応じて説明を変更し、[Save] をクリックします。

階層の削除

（注） 階層を削除すると、サブ組織、ファイアウォール、リソース プール、ポリシーなど、その階層に含まれるすべてのデータが削除されます。

手順

ステップ 1 [Tenant Management] > [root] > [*tenant*] を選択します。ここで [*tenant*] は削除する階層を含むテナントです。

ステップ 2 [Sub-Elements] タブの中で、削除する階層に移動し、[Delete Tier] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

第 9 章

サービス ポリシーおよびプロファイルの設定

この項では、次のトピックについて取り上げます。

サービス ポリシーの設定

ここでは、サービス ポリシーおよびポリシーセットの設定の概念およびオプションについて説明します。

ACL ポリシーとポリシー セットの設定

ここでは、ACL ポリシーとポリシー セットの作成方法について説明します。

ACL ポリシーの追加

VNMC を使用すると、時刻と頻度、または定義されたグループの包含に基づいて、アクセスコントロール リストを実装することができます。 この機能には、次のような利点があります。

- 日または週を通じて、ネットワーク リソースへのアクセスを緊密に制御できるようになります。
- ポリシーベース ルーティングおよびキューイング機能を強化します。
- 費用対効果を実現するために、1 日のうちの特定の時間にトラフィックが自動的に再ルーティングされます。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [ACL] > [ACL Policies] を選択します。

ステップ 2 [General] タブで、[Add ACL Policy] をクリックします。

ステップ 3 [Add ACL Policy] ダイアログボックスに、ポリシーの名前および簡単な説明を入力し、[Add Rule] をクリックします。

ステップ 4 [Add Rule] ダイアログボックスで、[Add Rule] ダイアログボックス, （95 ページ）で説明されている必須情報を入力し、[OK] をクリックします。

（注） 単一の ACL ルールのすべてのネットワーク ポートの条件は、[Attribute Value] フィールドで選択した値と同じ値でなければなりません。 たとえば、ネットワーク ポートの属性名を指定するすべてのルール条件の [Attribute Value] ドロップダウン リストから [FTP] を選択します。

[Add Rule] ダイアログボックスには、ACL ポリシーの時間のルールの設定が含まれます。 ACL ポリシーで時間範囲の使用する方法の詳細については、ACL ポリシー ルールの時間範囲, （99 ページ）を参照してください。

[Add Rule] ダイアログボックス

フィールド	説明
Name	ルール名。 この名前には、2 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。 この名前は、保存後には変更できません。
Description	ルールの簡単な説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。
Action	**1** ルール条件が満たされた場合に実行するアクションを選択します。 • [Drop]：トラフィックをドロップする、つまりアクセスを拒否します。 • [Permit]：トラフィックを転送する、つまりアクセスを許可します。 • [Reset]：接続をリセットします。 **2** [Log] チェックボックスをオンにして、ロギングをイネーブルにします。

フィールド	説明
Protocol	ルールが適用されるプロトコルを指定します。 • ルールをすべてのプロトコルに適用するには、[Any] チェックボックスをオンにします。 • ルールを特定のプロトコルに適用するには、次の手順を実行します。 **1** [Any] チェックボックスをオフにします。 **2** [Operator] ドロップダウン リストから、修飾子 [Equal]、[Not Equal]、[Member]、[Not Member]、[In range]、または [Not in range] を選択します。 **3** [Value] フィールドで、プロトコル、オブジェクト グループ、または範囲を指定します。
EtherType	このルールに対して検査する、カプセル化されているプロトコルを指定します。 • カプセル化されているすべてのプロトコルを検査するには、[Any] チェックボックスをオンにします。 • カプセル化されている特定のプロトコルを検査するには、次の手順を実行します。 **1** [Any] チェックボックスをオフにします。 **2** [Operator] ドロップダウン リストから、修飾子 [Equal]、[Not equal]、[Greater than]、[Less than]、[Member]、[Not Member]、[In range]、または [Not in range] を選択します。 **3** [Value] フィールドで、16 進数、オブジェクト グループ、または 16 進数の範囲を指定します。
Time Range Options	

フィールド	説明
To apply the rule all the time	[Always] チェックボックスをオンにします。
To apply the rule for a specific time range	**1** [Always] チェックボックスをオフにします。 **2** [Range] チェックボックスをオンにします。 **3** [Absolute Start Time] のフィールドに開始日時を入力します。 **4** [Absolute End Time] のフィールドに終了日時を入力します。
To apply the rule on a periodic basis as a member of an object group	**1** [Always] チェックボックスをオフにします。 **2** [Pattern] チェックボックスをオンにします。 **3** [Operator] ドロップダウン リストから、[range（In range）] を選択します。 **4** [Begin] のフィールドで、次の操作を行います。 　**1** [Begin] ドロップダウン リストから、週の開始曜日または時間範囲の頻度を選択します。 　**2** 開始時刻および AM/PM を選択します。 **5** [End] のフィールドで、次の操作を行います。 　**1** [End] ドロップダウン リストから、週の終了曜日または頻度を選択します。 　（注） [Begin] ドロップダウン リストで頻度を選択した場合は、[End] ドロップダウンリストでも同じ頻度を選択します。たとえば、[Weekdays] を [Begin] ドロップダウン リストと [End] ドロップダウンリストの両方で選択します。 　**2** 終了時刻および AM/PM を選択します。

フィールド	説明
To apply the rule on a periodic basis, with the frequency you specify	**1** [Always] チェックボックスをオフにします。 **2** [Pattern] チェックボックスをオンにします。 **3** [Operator] ドロップダウン リストから、[range（In range）] を選択します。 **4** [Begin] のフィールドで、次の操作を行います。 **1** [Begin] ドロップダウン リストから、週の開始曜日または時間範囲の頻度を選択します。 **2** 開始時刻および AM/PM を選択します。 **5** [End] のフィールドで、次の操作を行います。 **1** [End] ドロップダウン リストから、週の終了曜日または頻度を選択します。 **2** 終了時刻および AM/PM を選択します。 （注） [Begin] ドロップダウン リストで頻度を選択した場合は、[End] ドロップダウン リストでも同じ頻度を選択します。 たとえば、[Weekdays] を [Begin] ドロップダウン リストと [End] ドロップダウンリストの両方で選択します。
Source Conditions	
Add Rule Condition	ルール条件を追加する場合にクリックします。
Attribute Name	属性の名前
Operator	送信元の条件に使用する演算子。
Attribute Value	送信元の条件に使用する値。
Destination Conditions	
Add Rule Condition	ルール条件を追加する場合にクリックします。
Attribute Name	属性の名前

フィールド	説明
Operator	宛先の条件に使用する演算子。
Attribute Value	宛先の条件に使用する値。

ACL ポリシー ルールの時間範囲

VNMC では、次のいずれかの方法で ACL ポリシー ルールの時間範囲を設定できます。

- ACL ポリシー ルールの時間範囲を指定する。
- ACL ポリシー ルールに ACL オブジェクト グループを関連付ける。

VNMC は、次の種類の時間範囲をサポートします。

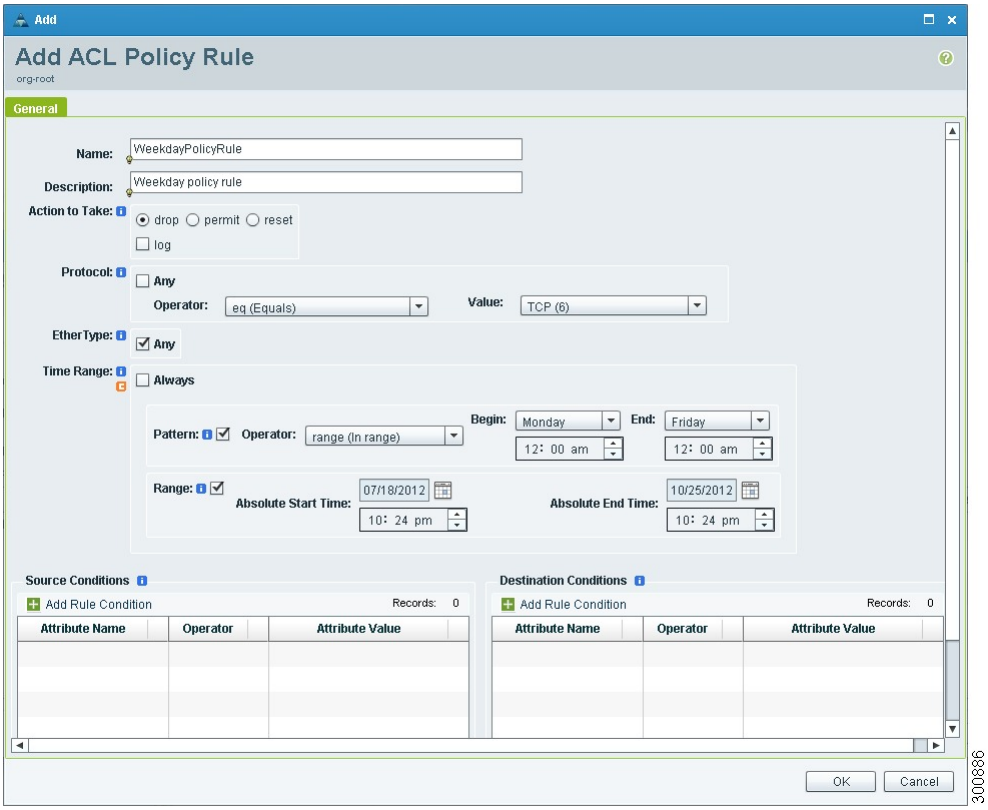
- 定期：曜日の開始時間および終了時間（日曜日から日曜日など）または頻度（毎日、平日、または週末など）で指定します。 定期範囲の開始時間と終了時間には、時間と分のオプションも含まれます。
- 絶対：開始時間および終了時間をカレンダーの日時で指定します。たとえば、2012 年 9 月 1 日午前 12 時から 2012 年 12 月 31 日午前 12 時など。

各 ACL のポリシー ルールでは、次を保持できます。

- 絶対時間範囲 1 つ。
- 任意の数の定期時間範囲、または定期時間範囲なし。
  - 単一の定期時間範囲を指定するには、それを ACL ポリシー ルールに追加します。
  - 複数の定期時間範囲を指定するには、ACL ポリシー オブジェクト ルールを使用します。

次の図に、ACL ポリシー ルールの時間範囲フィールドを示します。

図 3 : *ACL* ポリシー ルールの時間範囲フィールド



ACL ポリシー セットの追加

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [ACL] > [ACL Policy Sets] を選択します。

ステップ 2 [General] タブで、[Add ACL Policy Set] をクリックします。

ステップ 3 [Add ACL Policy Set] ダイアログボックスで、次のテーブルで説明されている必須情報を入力し、[OK] をクリックします。

フィールド	説明
Name	ポリシー セット名。 この名前には、2 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。 保存後は、この名前を変更できません。
Description	ポリシー セットの簡単な説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。 ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。
Admin State	ポリシーの管理状態：イネーブルまたはディセーブル。 このフィールドは、一部のポリシーセットでは使用できません。
Policies	
Add Policy	新規ポリシーを追加する場合にクリックします。
Available	ポリシー セットに割り当て可能なポリシー。 カラム間の矢印を使用して、カラム間でポリシーを移動します。
Assigned	ポリシー セットに割り当てられたポリシー。
Up and down arrows	選択されたポリシーの優先順位を変更します。 ポリシーを優先順位の高い順からリストします。

接続タイムアウト ポリシーの設定

VNMC を使用すると、さまざまなトラフィック タイプにタイムアウト制限を設けられるように接続タイムアウト ポリシーを設定することができます。

接続タイムアウトポリシーを作成したら、それをエッジプロファイルに関連付けることができます。 詳細については、エッジデバイス プロファイルの設定, （138 ページ）を参照してください。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [Connection Timeout] を選択します。

ステップ 2 [General] タブで、[Add Connection Timeout Policy] をクリックします。

ステップ 3 [Add Connection Timeout Policy] ダイアログボックスの中で、次を実行します。

a) ポリシーの名前と説明を入力します。

b) ポリシーの管理ステータスをイネーブルまたはディセーブルのいずれにするかを選択します。

ステップ 4 ポリシーにルールを追加するには、[Add Rule] をクリックします。

ステップ 5 [Add Connection Timeout Policy Rule] ダイアログボックスで、[Add Connection Timeout Policy Rule] ダイアログボックス, （102 ページ）で説明されている情報を入力します。

[Add Connection Timeout Policy Rule] ダイアログボックス

表 *6* : *[Add Connection Timeout Policy Rule]* ダイアログボックス

フィールド	説明
Name	ポリシー名。
Description	ポリシーの簡単な説明。
Action	
Idle TCP	どれほどの時間（日、時間、分、秒）だけTCP接続がアイドル状態でいると切断されるかを示します。
Half-Closed	どれほどの時間（日、時間、分、秒）だけハーフクローズTCP接続がアイドル状態でいると解放されるかを示します。
Send Reset To Idle Connection	このチェックボックスをオンにすると、TCP接続がタイムアウトになったときにTCPエンドポイントにリセットが送信されます。
Idle UDP	どれほどの時間（日、時間、分、秒）だけUDP接続がアイドル状態でいると切断されるかを示します。 時間は1分以上である必要があり、デフォルト値は2分です。 タイムアウトをディセーブルにするには、0:0:0:0 を入力します。

フィールド	説明
ICMP	どれほどの時間（日、時間、分、秒）だけICMP状態がアイドル状態でいると終了するかを示します。
Protocol	設定不可。
Source Conditions	
Destination Conditions	

DHCP ポリシーの設定

VNMC により、次に示す DHCP ポリシーを作成し、それらをエッジ ファイアウォールに適用できます。

- DHCP リレー サーバ ポリシー
- DHCP サーバ ポリシー

これらのポリシーは組織レベルで作成でき、エッジ ファイアウォールの Inside インターフェイスにのみ適用できます。 適用されると、DHCP ポリシーによりエッジ ファイアウォールは、Inside ネットワークのすべての VM について、DHCP サーバまたは DHCP リレーのいずれかの役割を果たすことができます。

エッジ ファイアウォールの Inside インターフェイスには、DHCP サーバまたはリレー プロファイルは一度に 1 つしか適用できません。

詳細については、次のトピックを参照してください。

- DHCP リレー サーバの追加, （103 ページ）
- DHCP リレー ポリシーの設定, （104 ページ）
- DHCP サーバ ポリシーの設定, （105 ページ）

DHCP リレー サーバの追加

DHCP リレー サーバは、同一の物理サブネット上にないクライアントとサーバ間で DHCP 要求および応答を転送するために使用されます。 IP データグラムがネットワーク間でスイッチングされる IP ルータの転送とは対照的に、DHCP リレー サーバは DHCP メッセージを受信した後、別のインターフェイス上で送信するための新たなメッセージを生成します。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [DHCP] > [DHCP Relay Server] を選択します。

ステップ 2 [General] タブで、[Add DHCP Relay Server] をクリックします。

ステップ 3 [New DHCP Relay Server] ダイアログボックスで、[Add DHCP Relay Server] ダイアログボックス,（104 ページ）で説明した情報を入力し、[OK] をクリックします。

[Add DHCP Relay Server] ダイアログボックス

フィールド	説明
Name	リレー サーバ名。
Description	リレー サーバの簡単な説明。
Relay Server IP	リレー サーバの IP アドレス。
Interface Name	リレー サーバに到達するために使用するインターフェイス。

DHCP リレー ポリシーの設定

この手順で説明するように、VNMC を使用すると、DHCP リレー ポリシーに DHCP リレー サーバを関連付けることができます。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [DHCP] > [DHCP Relay] を選択します。

ステップ 2 [General] タブで、[Add DHCP Relay Policy] をクリックします。

ステップ 3 [New DHCP Relay Policy] ダイアログボックスで、[Add DHCP Relay Policy] ダイアログボックス,（105 ページ）で説明した情報を入力し、[OK] をクリックします。

[Add DHCP Relay Policy] ダイアログボックス

名前	説明
Name	ポリシー名。
Description	ポリシーの簡単な説明。
DHCP Relay Server Assignment	次のいずれかの方法で DHCP リレー サーバを割り当てます。 • [Add DHCP Relay Server] をクリックして、新しいDHCP リレーサーバを追加します。 • [Available Relay Servers] リストで、使用可能なリレー サーバの 1 台を選択して、[Assigned Relay Servers] リストに移動します ポリシーには少なくとも 1 つの DHCP リレーサーバを割り当てる必要があります。

DHCP サーバ ポリシーの設定

DHCP サーバ ポリシーは、ping やリース タイムアウト、IP アドレス範囲、DNS と WINS の設定などのポリシーの特性を定義することができます。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [DHCP] > [DHCP Server] を選択します。

ステップ 2 [General] タブで、[Add DHCP Server Policy] をクリックします。

ステップ 3 [New DHCP Server Policy] ダイアログボックスで、[Add DHCP Server Policy] ダイアログボックス, （105 ページ） で説明した情報を入力し、[OK] をクリックします。

[Add DHCP Server Policy] ダイアログボックス

フィールド	説明
[General] タブ	
Name	ポリシー名。

フィールド	説明
Description	ポリシーの簡単な説明。
Ping Timeout（Milliseconds）	クライアント割り当て用のプールアドレスへの到達の試行を中止するまでに、DHCP サーバが ping の応答を待機する時間（ミリ秒単位）。 有効な範囲は 10 ～ 10000 ミリ秒です。
Lease Timeout（seconds）	DHCP サーバが DHCP クライアントに IP アドレスを割り当ててから、その IP アドレスを回収し、別のクライアントに割り当てなおすまでの時間の長さ（秒単位）。 デフォルト値は 3600 秒です。
Edge Firewall Interface Using the DHCP Client for DHCP Server Auto Configuration	DHCP サーバの自動設定をイネーブルにするには、DHCP クライアントを使用するエッジファイアウォールインターフェイスの名前を入力します。 ASA 1000V インスタンスの場合、このインターフェイスには必ず outside インターフェイスを指定します。 このフィールドを空白のままにすると、自動設定機能がディセーブルになります。
[Policies] タブ	
DNS Settings	DHCP クライアントを設定するときにエッジファイアウォールが使用する DNS 設定。 新しいエントリを追加するには、[Add DNS Setting] をクリックし、必要な情報を追加します。
WINS Servers	DHCP クライアントからアクセスできる Windows Internet Naming Service（WINS）ネーム サーバ。 新しい WINS サーバを追加するには、[Add WINS Server] をクリックし、WINS サーバ IP アドレスを追加します。 WINS サーバがプリファレンスの順に上からリストされます。テーブルでエントリを選択し、テーブルの上の矢印を使用して、サーバの優先順位を変更します。

フィールド	説明
IP Address/Range	DHCP アドレス プールに関する次の情報を入力します。 • [Start IP Address]：プールの開始 IP アドレス。 • [End IP Address]：プールの終了 IP アドレス。 • [Subnet Mask]：アドレス プールに適用するサブネット マスク。

IP 監査ポリシーおよび IP 監査シグニチャ ポリシーの設定

IP 監査機能は、ASA 1000V インスタンスに対して、基本的な侵入防御システム（IPS）サポートを実現しています。VNMC は基本的なシグニチャのリストをサポートし、ユーザは、シグニチャに一致するトラフィックに適用するアクションを 1 つ以上指定するポリシーを設定できます。

次に示す IP 監査ポリシーが使用できます。

- 監査ポリシー
- シグニチャ ポリシー

IP 監査ポリシーをデバイスと関連付ける場合、ポリシーはデバイスの outside インターフェイス上のすべてのトラフィックに適用されます。

ここでは、これらのポリシーの設定方法について説明します。

IP 監査ポリシーの設定

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [IP Audit] > [Audit Policies] を選択します。

ステップ 2 [General] タブで、[Add IP Audit Policy] をクリックします。

ステップ 3 [Add IP Audit Policy] ダイアログボックスで、次の情報を入力します。

- ポリシー名
- ポリシーの説明

- [Admin State] フィールドで、ポリシーの管理状態をイネーブルまたはディセーブルのいずれにするかを選択します。

ステップ 4 ポリシーにルールを追加するには、[Add Rule] をクリックします。

ステップ 5 [Add IP Audit Policy Rule] ダイアログボックスで、[Add IP Audit Policy Rule] ダイアログボックス,（108 ページ）で説明されている情報を入力し、[OK] をクリックします。

[Add IP Audit Policy Rule] ダイアログボックス

表 *7*：*[IP Audit Policy Rule]* ダイアログボックス

フィールド	説明
Name	ルール名。
Description	ルールの簡単な説明。
Attack-Class Action	ルールの条件が満たされた場合に署名タイプ [Attack] に対して実行するアクションのチェックボックスをオンにします。 • [Log]：パケットが署名に一致したことを示すメッセージを送信します。 • [Drop]：パケットをドロップします。 • [Reset Flow]：パケットをドロップし、接続をリセットします。
Information-Class Action	ルールの条件が満たされた場合に署名タイプ [Informational] に対して実行するアクションのチェックボックスをオンにします。 • [Log]：パケットが署名に一致したことを示すメッセージを送信します。 • [Drop]：パケットをドロップします。 • [Reset Flow]：パケットをドロップし、接続をリセットします。

フィールド	説明
Protocol	設定不可。
Source Conditions	
Destination Conditions	

IP 監査シグニチャ ポリシーの設定

IP監査シグニチャポリシーは、有効および無効になった署名を識別します。デフォルトでは、すべてのポリシーが有効になります。 正当なトラフィックがほとんどの状況でシグニチャに一致する結果、誤報になる場合、シグニチャを無効にすることができます。 ただし、シグニチャの無効化はグローバルレベルで実行されるので、シグニチャが無効な場合、トラフィック（たとえ不正なトラフィックでも）がシグネチャをトリガしなくなります。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [IP Audit] > [Signature Policies] を選択します。

ステップ 2 [General] タブで、[Add IP Audit Signature Policy] をクリックします。

ステップ 3 [Add IP Audit Signature Policy] ダイアログボックスに、ポリシーの名前および説明を入力します。

ステップ 4 [Signatures] 領域で、必要に応じて [Enabled Signatures] と [Disabled Signatures] リスト間でシグニチャを移動させます。

（注） これを行うことによる影響を理解したかどうか定かでない場合は、シグニチャを無効にしないことをお勧めします。

必要なシグニチャを選択し、[Properties] をクリックすることで、シグニチャについての詳細情報を表示できます。

ステップ 5 すべての調整を終了したら、[OK] をクリックします。

NAT/PAT ポリシーとポリシー セットの設定

VNMCは、展開されているネットワークのアドレス変換を制御するために、ネットワークアドレス変換（NAT）ポリシーおよびポート アドレス変換（PAT）ポリシーをサポートしています。 これらのポリシーは、IP アドレスおよびポートのスタティックおよびダイナミック両方の変換を行います。

VNMC では、次に示すポリシー項目を設定できます。

- NAT ポリシー：一致するものが見つかるまで順番に評価される、複数の規則を入れることができます。

- NAT ポリシー セット：エッジ セキュリティ プロファイルに関連付けることができる NAT ポリシーのグループ。 プロファイルが適用されると、NAT ポリシーは入力トラフィックにのみ適用されます。
- PAT ポリシー：エッジ ファイアウォールで、ソース ダイナミック インターフェイス PAT および宛先スタティック インターフェイス PAT をサポートします。

ここでは、NAT ポリシーおよび PAT ポリシー、また NAT ポリシー セットの設定方法について説明します。

NAT/PAT ポリシーの設定

この手順では、VNMC で NAT/PAT ポリシーを設定する方法について説明します。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [NAT] > [NAT Policies] を選択します。

ステップ 2 [General] タブで、[Add NAT Policy] をクリックします。

ステップ 3 [Add NAT Policy] ダイアログボックスに、ポリシーの一意の名前および説明を入力します。

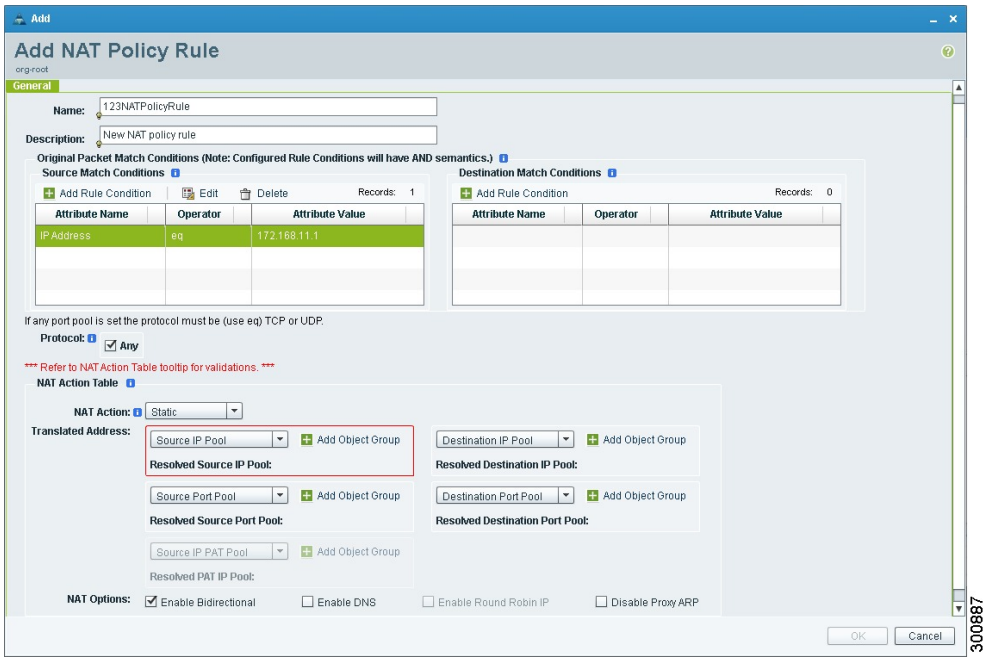
ステップ 4 [Admin State] フィールドで、ポリシーの管理状態をイネーブルにするか、またはディセーブルにするかを指定します。

ステップ 5 ポリシーにルールを追加するには、[Add Rule] をクリックします。

ステップ 6 [Add NAT Policy Rule] ダイアログボックス（[Add NAT Policy Rule] ダイアログボックス，（111 ページ）を参照）で、[Add NAT Policy Rule] ダイアログボックス，（111 ページ）で説明されている情報を入力し、[OK] をクリックします。

[Add NAT Policy Rule] ダイアログボックス

図 *4*：*[Add NAT Policy Rule]* ダイアログボックス



[Add NAT Policy Rule] ダイアログボックス

表 *8*：*[Add NAT Policy Rule]* ダイアログボックス

フィールド	説明
Name	ルール名。
Description	ルールの簡単な説明。
Original Packet Match Conditions	
Source Match Conditions	現在のポリシーを適用するために一致する必要がある送信元属性。 新しい条件を追加するには、[Add Rule Condition] をクリックします。 使用可能な送信元属性は、IP アドレスとネットワーク ポートです。

フィールド	説明
Destination Match Conditions	現在のポリシーを適用するために一致する必要がある宛先属性。 新しい条件を追加するには、[Add Rule Condition] をクリックします。 使用可能な宛先属性は、IP アドレスとネットワーク ポートです。
Protocol	ルールが適用されるプロトコルを指定します。 • ルールをすべてのプロトコルに適用するには、[Any] チェックボックスをオンにします。 • ルールを特定のプロトコルに適用するには、次の手順を実行します。 1 [Any] チェックボックスをオフにします。 2 [Operator] ドロップダウン リストから、修飾子 [Equal]、[Not equal]、[Member]、[Not Member]、[In range]、または [Not in range] を選択します。 3 [Value] フィールドで、プロトコル、オブジェクト グループ、または範囲を指定します。
[NAT Action] テーブル	
NAT Action	このドロップダウン リストから、[Static] または [Dynamic] のうち、必要な方のトランスレーション オプションを選択します。

フィールド	説明
Translated Address	元のパケットの一致条件ごとに、変換されたアドレスのプールを次のオプションの中から選択します。 • Source IP Pool • Source Port Pool • Source IP PAT Pool • Destination IP Pool • Destination Port Pool たとえば、送信元 IP アドレスの一致条件を指定する場合は、[Source IP Pool] オブジェクト グループを選択する必要があります。 同様に、宛先ネットワーク ポートの場合は、[Destination Port Pool] オブジェクト グループを選択する必要があります。 [Source IP PAT Pool] オプションは、ダイナミック変換を選択した場合にのみ使用可能です。 変換アクション用のオブジェクト グループを追加するには、[Add Object Group] をクリックします。
NAT Options	機能をイネーブルにするには、そのチェックボックスをオンにします。 • [Enable Bidirectional]：「ホストから」と「ホストへの」の双方向で接続を開始できるかどうか。 スタティック アドレス変換の場合のみ使用可能です。 • [Enable DNS]：NAT で DNS をイネーブルにするかどうか。 • [Enable Round Robin IP]：IP アドレスがラウンドロビン方式を割り当てるかどうか。 ダイナミック アドレス変換の場合のみ使用可能です。

NAT ポリシー セットの設定

ポリシー セットを使用すると、プロファイルに含めるために同じタイプ（NAT、ACL、またはインターフェイス）の複数のポリシーをグループ化できます。 NAT ポリシー セットとは、エッジ セキュリティ プロファイルに関連付けられる NAT ポリシーのグループです。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [NAT] > [NAT Policy Sets] を選択します。

ステップ 2 [General] タブで、[Add NAT Policy Set] をクリックします。

ステップ 3 [Add NAT Policy Set] ダイアログボックスに、ポリシー セットの名前および説明を入力します。

ステップ 4 [Admin State] フィールドで、ポリシーの管理ステータスをイネーブルにするか、またはディセーブルにするかを指定します。

ステップ 5 [Policies] 領域で、このポリシー セットに含めるポリシーを選択します。

a) [Available] リストの中で、1 つ以上のポリシーを選択し、それらを [Assigned] リストに移動します。

b) リストの上にある矢印キーを使用して、割り当てられたポリシーの優先順位を調整します。

c) 必要に応じて、[Add NAT Policy] をクリックして新しいポリシーを追加し、[Assigned] リストにそれを含めます。
NAT ポリシーの設定については、NAT/PAT ポリシーの設定, （110 ページ）を参照してください。

ステップ 6 [OK] をクリックします。

エッジ ファイアウォール用の PAT の設定

VNMC では、ASA 1000V など、エッジ ファイアウォールのソース インターフェイス PAT および宛先インターフェイス PAT を設定できます。 詳細については、次のトピックを参照してください。

送信元ダイナミック インターフェイス PAT

VNMC では、ASA 1000V など、エッジ ファイアウォールの送信元ダイナミック インターフェイス PAT を設定することができます。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [NAT] > [NAT Policies] を選択します。

ステップ 2 [General] タブで、[Add NAT Policy] をクリックします。

ステップ 3 [Add NAT Policy] ダイアログボックスに、ポリシーの一意の名前および説明を入力します。

ステップ 4 [Admin State] フィールドで、ポリシーの管理状態をイネーブルにするか、またはディセーブルにするかを指定します。

ステップ 5 [Add Rule] をクリックし、このポリシーにルールを追加します。

ステップ 6 [Add NAT Policy Rule] ダイアログボックスで、[Add NAT Policy Rule] ダイアログボックス，（111 ページ）に説明された情報を次の特定の設定で指定します。

a) [NAT Action] ドロップダウン リストから、[Dynamic] を選択します。

b) [Translated Address] 領域で、ASA 1000V の外部インターフェイスの IP アドレスが含まれている発信元 IP プールのオブジェクト グループを追加します。

ステップ 7 [OK] をクリックします。

宛先スタティック インターフェイス PAT の設定

VNMC を使用すると、次の手順で説明するように、ASA 1000V などのエッジ ファイアウォールの宛先スタティック インターフェイス PAT を設定することができます。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [NAT] > [NAT Policies] を選択します。

ステップ 2 [General] タブで、[Add NAT Policy] をクリックします。

ステップ 3 [Add NAT Policy] ダイアログボックスに、ポリシーの一意の名前および説明を入力します。

ステップ 4 [Admin State] フィールドで、ポリシーの管理状態をイネーブルにするか、またはディセーブルにするかを指定します。

ステップ 5 [Add Rule] をクリックし、このポリシーにルールを追加します。

ステップ 6 [Add NAT Policy Rule] ダイアログボックスで、[Destination Match Conditions] のルール条件として ASA 1000V の外部インタフェースの IP アドレスを入力します。

ステップ 7 [Add NAT Policy Rule] ダイアログボックス，（111 ページ）で説明されているように、[Add NAT Policy Rule] ダイアログボックスの他のオプションを設定します。

（注） IP アドレスのいずれかのフィールドに、ASA 1000V の外部インターフェイスの IP アドレスで開始または終了する範囲が含まれている場合、ASA 1000V インターフェイスの IP アドレスを識別し、それに重複するエラー メッセージが表示されます。

ステップ 8 [OK] をクリックします。

パケット インスペクション ポリシーの設定

VNMCを使用すると、アプリケーション層プロトコルインスペクションのためのポリシーを設定することができます。 インスペクションは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。 インスペクションが設定されると、エンドデバイスはすぐにパケットを渡す代わりに、ディープ パケット インスペクションを実行します。 そのため、インスペクションがデバイスのスループット全体に影響を与えることがあります。

パケット インスペクション ポリシー用にサポートされるプロトコル, （116 ページ）に、VNMCでサポートされるアプリケーション層プロトコルを示します。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [Packet Inspection] を選択します。

ステップ 2 [General] タブで、[Add Packet Inspection Policy] をクリックします。

ステップ 3 [Add Packet Inspection Policy] ダイアログボックスに、ポリシーの名前および説明を入力します。

ステップ 4 [Admin State] フィールドで、ポリシーの管理ステータスをイネーブルにするか、またはディセーブルにするかを指定します。

ステップ 5 ポリシーにルールを追加するには、[Add Rule] をクリックします。

ステップ 6 [Add Packet Inspection Policy Rule] ダイアログボックスで、[Add Packet Inspection Policy Rule] ダイアログボックス, （117 ページ）で説明されている情報を入力し、[OK] をクリックします。

パケット インスペクション ポリシー用にサポートされるプロトコル

パケット インスペクション ポリシー用にサポートされるプロトコル

CTIQBE	ICMP	PPTP	SQLNet
DCE/RPC	ICMP Error	RSH	SunRPC
DNS	ILS	RSTP	TFTP
FTP	IP オプション	SIP	WAAS
H323 H225	IPsec パススルー	Skinny	XDMCP
H323 RAS	MGCP	SMTP	
HTTP	NetBIOS	SNMP	

[Add Packet Inspection Policy Rule] ダイアログボックス

表 *9*：*[Add Packet Inspection Policy Rule]* ダイアログボックス

フィールド	説明
Name	ルール名。
Description	ルールの簡単な説明。
Action	ルール条件が満たされた場合に検査するプロトコルに対する [Enable Inspection] フィールドのチェックボックスをオンにします。
Protocol	設定不可。
Source Conditions	
Destination Conditions	

ルーティング ポリシーの設定

VNMC では、エッジ ファイアウォールの管理対象エンドポイントのスタティック ルートを設定するために、ルーティング ポリシーを使用できます。

（注） VNMC を使用して設定できるのは、エッジ ファイアウォール上の内部インターフェイスと外部インターフェイスのみです。 エッジ ファイアウォールの管理インターフェイス上でルートを設定するには、CLI を使用します。

スタティック ルートのルーティング ポリシーを設定すると、次の方法でポリシーを実装できます。

- エッジ デバイス プロファイルのルーティング ポリシーを含めます。
- エンドポイントを管理しているエッジ ファイアウォールへのエッジ デバイス プロファイルを適用します。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [Routing] を選択します。

ステップ 2 [General] タブで、[Add Routing Policy] をクリックします。

ステップ 3 [Add Routing Policy] ダイアログボックスに、ルーティング ポリシーの名前および簡単な説明を入力します。

ステップ 4 新しいスタティック ルートを追加するには、[Add Static Route] をクリックします。

ステップ 5 [Add Static Route] ダイアログボックスで、次の情報を入力します。

a) [Destination Network] フィールドで、IP ルート プレフィックスと宛先のプレフィックス マスクを入力します。

b) [Forwarding (Next Hop)] フィールドで、宛先ネットワークに到達するために使用可能なネクスト ホップの IP アドレスを入力します。

（注） [Forwarding Interface] フィールドは、ASA 1000V データ インターフェイスにのみ適用されます。 ASA 1000V 管理インターフェイス上でルートを設定するには、CLI を使用してください。

c) （任意）[Distance Metric] フィールドで、距離メトリックを入力します。

ステップ 6 [OK] をクリックします。

TCP 代行受信ポリシーの設定

VNMC を使用すると、エッジ セキュリティ プロファイルに関連付けられるように TCP 代行受信ポリシーを設定することができます。 エッジ セキュリティ プロファイルを介してデバイスに関連付ける TCP 代行受信ポリシーは、デバイスの外部インターフェイス上のすべてのトラフィックに適用されます。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [TCP Intercept] を選択します。

ステップ 2 [General] タブで、[Add TCP Intercept Policy] をクリックします。

ステップ 3 [Add TCP Intercept Policy] ダイアログボックスに、ポリシーの名前および簡単な説明を入力します。

ステップ 4 [Admin State] フィールドで、ポリシーの管理状態をイネーブルにするか、またはディセーブルにするかを指定します。

ステップ 5 ポリシーにルールを追加するには、[Add Rule] をクリックします。

ステップ 6 [Add TCP Intercept Policy Rule] ダイアログボックスで、[Add TCP Intercept Policy Rule] ダイアログボックス，（119 ページ）で説明されている情報を入力します。

[Add TCP Intercept Policy Rule] ダイアログボックス

フィールド	説明
Name	ルール名。
Description	ルールの簡単な説明。
Maximum Number of Embryonic TCP Connections（0 ～ 65535）	全体およびクライアントで許可する初期TCP接続数： 1 [Total] フィールドに、許可する初期 TCP 接続の最大数を入力します。 2 [client] フィールドに、1 つのクライアントで許可する初期 TCP 接続の最大数を入力します。 デフォルト値 0（ゼロ）は、接続数に上限がないことを意味します。
Protocol	設定不可。
Source Conditions	
Destination Conditions	

サイト間 IPsec VPN ポリシーの設定

VNMC では、サイト間 IPsec VPN を設定できます。 また、クリプト マップ ポリシーを設定し、それをエッジ プロファイルに添付できます。 設定しやすくし、論理 IPsec エンティティを分けておくため、設定を次の項に分けています。

- クリプト マップ ポリシーの設定
- IKE ポリシーの設定
- インターフェイス ポリシー セットの設定
- IPsec ポリシーの設定
- ピア認証ポリシーの設定
- VPN デバイス ポリシーの設定

VPN ポリシーにアクセスするには、次の図に示すように [Policy Management] > [Service Policies] > [root] > [Policies] > [VPN] を選択します。

図 5 : *VNMC の VPN ポリシー*

クリプト マップ ポリシーの設定

VNMC を使用すると、次のものを含むクリプト マップ ポリシーを作成することができます。

- 発信元と宛先の条件のルール。
- IPsec ポリシーを含む IP Security（IPsec）オプションのルール。
- ピア デバイスを含むインターネット キー交換（IKE）オプション。

クリプト マップ ポリシーはインターフェイス ポリシー セットおよびエッジ セキュリティ ポリシーに組み込むことでインターフェイスに適用されます。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [VPN] > [Crypto Map Policies] を選択します。

ステップ 2 [General] タブで、[Add Crypto Map Policy] をクリックします。

ステップ 3 [Add Crypto Map Policy] ダイアログボックスで、[Add Crypto Map Policy] ダイアログボックス，（121 ページ）で説明されている情報を入力し、[OK] をクリックします。

ステップ 4 ポリシー ルールを追加するには、[General] タブの [Add Rule] をクリックし、[Add Crypto Map Policy Rule] ダイアログボックス，（123 ページ）で説明されている必須情報を入力します。

[Add Crypto Map Policy] ダイアログボックス

フィールド	説明
[General] タブ	
Name	ポリシー名。
Description	ポリシーの簡単な説明。
Admin State	ポリシーの管理ステータスが、イネーブルまたはディセーブルのいずれであるか。
[Rule] テーブル	
Add Rule	[Add Rule] をクリックし、現在のポリシーに新しいルールを追加します。
[IPsec Settings] タブ	
SA Lifetime	セキュリティ アソシエーション（SA）の有効期間（日数、時間数、分数、秒数）。
SA Lifetime Traffic（KB）	特定の SA が期限切れになるまでにそのアソシエーションを使用して IPsec ピア間を通過できるトラフィック量（KB 単位）。

フィールド	説明
Enable Perfect Forwarding Secrecy	完全転送秘密（PFS）をイネーブルにするかどうか。 PFS は、導き出される共有秘密値に関連する暗号特性です。 PFS を使用すると、1 つのキーが損なわれても、これ以降のキーは前のキーの取得元から取得されないため、前および以降のキーには影響しません。
Diffie-Hellman Group	PFS がイネーブルになっている場合に使用できます。 このポリシーには Diffie-Hellman（DH）グループを選択します。 • [Group 1]：768 ビットの DH グループ。 • [Group 2]：1024 ビットの DH グループ。 • [Group 5]：1536 ビットの DH グループ。
IPsec Policies	現在のポリシーに適用される IPsec ポリシー。 既存の IPsec ポリシーを選択するか、または [Add IPsec Policy] をクリックして新しいポリシーを作成します。
Peer Device	ピア デバイス。 既存のピアを選択するか、または [Add Peer Device] をクリックして新しいピアを追加します。 [Add Peer Device] ダイアログボックスに、ピアデバイス IP アドレスまたはホスト名を入力します。
[Other Settings] タブ	
Enable NAT Traversal	IPsec ピアが NAT デバイスを介して接続を確立できるようにするかどうか。
Enable Reverse Route Injection	スタティック ルートが自動的にルーティングテーブルに追加され、プライベートネットワーク上のネイバーに通知されるようにするかどうか。

フィールド	説明
Connection Type	このポリシーの接続タイプは、次のとおりです。 • [Answer-Only]：初期の独自交換中に着信 IKE 接続にのみ応答して、接続対象のピアを決定します。 • [Bidirectional]：このポリシーに基づいて、接続を受け入れるとともに、接続を開始します。 • [Originate-Only]：最初の独自交換を開始して、接続対象のピアを決定します。
Negotiation Mode	キー情報の交換と SA の設定に使用するモード： • [Aggressive Mode]：高速なモードで、使用するパケットと交換回数を少なくすることができますが、通信パーティの ID は保護されません。 • [Main Mode]：低速なモードで、パケットと交換回数が多くなりますが、通信パーティの ID を保護します。
DH Group for Aggressive Mode	アグレッシブ モードで使用する DH グループ（[Group 1]、[Group 2]、または [Group 5]）。

[Add Crypto Map Policy Rule] ダイアログボックス

フィールド	説明
Name	ルール名。
Description	ルールの簡単な説明。
VPN Action	このルールに基づいて実行するアクション：[Permit] または [Deny]。

フィールド	説明
Protocol	このルールに対して検査するプロトコル。 • すべてのプロトコルを検査する場合は、[Any] チェックボックスをオンにします。 • 特定のプロトコルを検査するには、次の手順を実行します。 1 [Any] チェックボックスをオフにします。 2 [Operator] ドロップダウン リストから、修飾子 [Equal]、[Not equal]、[Member]、[Not Member]、[In range]、または [Not in range] を選択します。 3 [Value] フィールドで、プロトコル、オブジェクト グループ、または範囲を指定します。
Source Conditions	ルールを適用するために一致する必要がある送信元属性。 新しい条件を追加するには、[Add Rule Condition] をクリックします。 使用可能な送信元属性は、IP アドレスとネットワーク ポートです。
Destination Conditions	ルールを適用するために一致する必要がある宛先属性。 新しい条件を追加するには、[Add Rule Condition] をクリックします。 使用可能な宛先属性は、IP アドレスとネットワーク ポートです。

IKE ポリシーの設定

Internet Key Exchange（IKE; インターネット キー交換）プロトコルは、Internet Security Association and Key Management Protocol（ISAKMP）フレームワーク内で Oakley と SKEME キー交換を実装するハイブリッド プロトコルです。 初期の IKE 実装では IPsec プロトコルが使用されましたが、他のプロトコルでも IKE を使用できます。 IKE は、IPsec ピアを認証し、IPsec キーをネゴシエーションし、IPsec Security Associations（SA; セキュリティ アソシエーション）を実行します。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [VPN] > [IKE Policies] を選択します。

ステップ 2 [General] タブで、[Add IKE Policy] をクリックします。

ステップ 3 [Add IKE Policy] ダイアログボックスに、ポリシーの一意の名前および説明を入力します。

ステップ 4 IKE V1 または IKE V2 ポリシーのいずれかを設定します。

- IKE V1 ポリシー
  1. [Add IKE V1 Policy] をクリックします。
  2. [Add IKE V1 Policy] ダイアログボックスで、[IKE V1 Policy] ダイアログボックス，（125 ページ）で説明した情報を入力し、[OK] をクリックします。
- IKE V2 ポリシー
  1. [Add IKE V2 Policy] をクリックします。
  2. [Add IKE V2 Policy] ダイアログボックスで、[IKE V2 Policy] ダイアログボックス，（126 ページ）で説明した情報を入力し、[OK] をクリックします。

ステップ 5 [OK] をクリックします。

[IKE V1 Policy] ダイアログボックス

フィールド	説明
DH Group	Diffie-Hellman グループ：[Group 1]、[Group 2]、または [Group 5]。
Encryption	暗号化方式：3DES、AES、AES-192、AES-256、または DES。
Hash	ハッシュ アルゴリズム：MD5 または SHA。
Authentication	認証方法は事前共有キーです。
SA Lifetime	SA の有効期間（日数、時間数、分数、秒数）。

[IKE V2 Policy] ダイアログボックス

フィールド	説明
DH Group	Diffie-Hellman グループ：[Group 1]、[Group 2]、[Group 5] または [Group 14]。
Encryption	暗号化方式：3DES、AES、AES-192、AES-256、または DES。
Hash	ハッシュ整合性アルゴリズム：MD5、SHA、SHA256、SHA384、または SHA512。
Pseudo Random Function Hash	疑似乱数機能（PRF）のアルゴリズムは次のいずれか：MD5、SHA、SHA256、SHA384、または SHA512。
SA Lifetime	SA の有効期間（日数、時間数、分数、秒数）。

インターフェイス ポリシー セットの設定

インターフェイス ポリシー セットを使用すると、エッジ セキュリティ プロファイルに含めるために複数のポリシーをグループ化できます。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [VPN] > [Interface Policy Sets] を選択します。

ステップ 2 [General] タブで、[Add Interface Policy Set] をクリックします。

ステップ 3 [Add Interface Policy Set] ダイアログボックスで、[Add Interface Policy Set] ダイアログボックス，（126 ページ）で説明されている情報を入力し、[OK] をクリックします。

[Add Interface Policy Set] ダイアログボックス

[General] タブ

フィールド	説明
Name	ポリシー セット名。
Description	ポリシー セットの簡単な説明。

フィールド	説明
Admin State	ポリシーセットの管理状態：イネーブルまたはディセーブル。
[Policies] 領域	
Add Crypto Map Policy	新規ポリシーを追加する場合にクリックします。
Available	ポリシー セットに割り当て可能なポリシー。 カラム間の矢印を使用して、カラム間でポリシーを移動します。
Assigned	ポリシー セットに割り当てられたポリシー。
Up and down arrows	選択されたポリシーの優先順位を変更します。 ポリシーを優先順位の高い順からリストします。

[Domain Settings] タブ

フィールド	説明
Enable IKE（少なくとも 1 つをオンにする必要あり）	IKE V1 または IKE V2 を指定する場合は、該当するチェックボックスをオンにします。
Enable IPsec Pre-fragmentation	暗号化の前にパケットをフラグメント化する場合は、このチェックボックスをオンにします。事前のフラグメンテーションを行うと、事後のフラグメンテーション（暗号化後のフラグメンテーション）とその結果必要となる復号化前のリアセンブリが最小限で済み、それによりパフォーマンスが向上します。

フィールド	説明
Do Not Fragment	[Enable IPsec Pre-fragmentation] チェックボックスをオンにしている場合のみ使用可能になります。 ドロップダウンリストから、カプセル化されているヘッダー内の [Don't Fragment（DF）] ビットで実行するアクションを選択します。 • Clear • Copy • Set

IPsec ポリシーの設定

IPsec ポリシーは、VPN 用に安全な IPSec トンネルを作成するのに使用する IPsec ポリシー オブジェクトを定義します。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [VPN] > [IPsec Policies] を選択します。

ステップ 2 [General] タブで、[Add IPsec Policy] をクリックします。

ステップ 3 [Add IPsec Policy] ダイアログボックスに、ポリシーの名前および説明を入力します。
IPsec ポリシー用に IKE V1 または IKE V2 のいずれかのプロポーザルを設定する必要があります。

ステップ 4 IKE V1 プロポーザルの設定手順

a) [IKE v1 Proposal Table] 領域で、[Add IPsec IKEv1 Proposal] をクリックします。

b) [IPsec IKEv1 Proposal] ダイアログボックスで、で説明した情報を入力し、[OK] をクリックします。[IPsec IKEv1 Proposal] ダイアログボックス, （129 ページ）

ステップ 5 IKE V2 プロポーザルの設定手順

a) [IKE v2 Proposal Table] 領域で、[Add IPsec IKE v2 Proposal] をクリックします。

b) [IPsec IKEv2 Proposal] ダイアログボックスで、で説明した情報を入力し、[OK] をクリックします。[IPsec IKEv2 Proposal] ダイアログボックス, （130 ページ）

ステップ 6 [OK] をクリックしてポリシーを保存します。

[IPsec IKEv1 Proposal] ダイアログボックス

フィールド	説明
Mode	IPSec トンネルが動作するモード。 Tunnel モードでは、IPsec トンネルは IP パケット全体をカプセル化します。
ESP Encryption	カプセル化セキュリティ プロトコル（ESP）暗号化方式： • [3DES]：56 ビット キーを使用するデータ暗号規格（DES）に従って暗号化を 3 回実行します。 • [AES]：128 ビット キーを使用する高度暗号化規格（AES）に従って暗号化を実行します。 • [AES-192]：192 ビット キーを使用する AES に従って暗号化を実行します。 • [AES-256]：256 ビット キーを使用する AES に従って暗号化を実行します。 • [DES]：56 ビット キーを使用する DES に従って暗号化を実行します。 • [Null]：ヌル暗号化アルゴリズム。[ESP-Null] を使用して定義されたトランスフォーム セットでは、暗号化なしの認証を提供します。この方法は、通常、テスト目的にだけ使用されます。
ESP Authentication	ハッシュ認証アルゴリズム： • [MD5]：128 ビットのダイジェストを生成します。 • [Null]：認証を実行しません。 • [SHA]：160 ビットのダイジェストを生成します。

[IPsec IKEv2 Proposal] ダイアログボックス

フィールド	説明
[ESP Encryption Algorithm] テーブル	ESP 暗号化方式を追加するには、次の手順を実行します。 1 [Add ESP Encryption Algorithm] をクリックします。 2 [ESP Encryption] ドロップダウン リストから、暗号化方式を選択します。 • [3DES]：56 ビット キーを使用するデータ暗号規格（DES）に従って暗号化を 3 回実行します。 • [AES]：128 ビット キーを使用する高度暗号化規格（AES）に従って暗号化を実行します。 • [AES-192]：192 ビット キーを使用する AES に従って暗号化を実行します。 • [AES-256]：256 ビット キーを使用する AES に従って暗号化を実行します。 • [DES]：56 ビット キーを使用する DES に従って暗号化を実行します。 • [Null]：ヌル暗号化アルゴリズム。[ESP-Null] を使用して定義されたトランスフォーム セットでは、暗号化なしの認証を提供します。この方法は、通常、テスト目的にだけ使用されます。

フィールド	説明
[Integrity Algorithm] テーブル	整合性アルゴリズムを追加するには、次の手順を実行します。 1 [Add Integrity Algorithm] をクリックします。 2 [Integrity Algorithm] ドロップダウン リストから、認証アルゴリズムを選択します。 • [MD5]：128 ビットのダイジェストを生成します。 • [Null]：認証を実行しません。 • [SHA]：160 ビットのダイジェストを生成します。

ピア認証ポリシーの設定

ピア認証ポリシーを使用して、ピアの認証に使用する方式を定義します。

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [VPN] > [Peer Authentication] を選択します。

ステップ 2 [General] タブで、[Add Peer Authentication Policy] をクリックします。

ステップ 3 [Add Peer Authentication Policy] ダイアログボックスに、ポリシーの名前および説明を入力します。

ステップ 4 [Add Policy to Authenticate Peer] をクリックします。

ステップ 5 [Add Policy to Authenticate Peer] ダイアログボックスで、[Add Policy to Authenticate Peer] ダイアログボックス，（131 ページ）で説明した情報を入力し、[OK] をクリックします。

ステップ 6 [OK] をクリックしてポリシーを保存します。

[Add Policy to Authenticate Peer] ダイアログボックス

フィールド	説明
Peer Device (Unique)	ピアの固有の IP アドレスまたはホスト名。
[IKEv1] 領域	
Local	事前共有キー。

フィールド	説明
Confirm	確認用の事前共有キー。
Set	事前共有キーが適切に設定されている（読み取り専用）かどうか。
[IKEv2] 領域	
Local	ローカルの事前共有キー。
Confirm	確認用のローカルの事前共有キー。
Set	ローカルの事前共有キーが適切に設定されている（読み取り専用）かどうか。
Remote	リモートの事前共有キー。
Confirm	確認用のリモートの事前共有キー。
Set	リモートの事前共有キーが適切に設定されている（読み取り専用）かどうか。

VPN デバイス ポリシーの設定

VPN デバイス ポリシーを使用すると、次のような VPN グローバル設定を指定することができます。

- IKE ポリシー
- IKE グローバル設定
- IPsec グローバル設定
- ピア認証ポリシー

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policies] > [VPN] > [VPN Device Policies] を選択します。

ステップ 2 [General] タブで、[Add VPN Device Policy] をクリックします。

ステップ 3 [Add VPN Device Policy] ダイアログボックスで、[Add VPN Device Policy] ダイアログボックス，（133 ページ）で説明されている情報を入力します。

ステップ 4 必要に応じて、次の表で説明する情報を入力してください。

- IKE ポリシーの設定，（124 ページ）
- ピア認証ポリシーの設定，（131 ページ）

ステップ 5 [OK] をクリックしてポリシーを作成します。

[Add VPN Device Policy] ダイアログボックス

[General] タブ

（注） VPN デバイス ポリシーには、IKE ポリシーとピア認証ポリシーの両方が必要です。

フィールド	説明
Name	ポリシー名。
Description	ポリシーの簡単な説明。
IKE Policy	ドロップダウン リストから既存のポリシーを選択するか、または [Add IKE Policy] をクリックして新しいポリシーを追加します。
Peer Authentication Policy	ドロップダウン リストから既存のポリシーを選択するか、または [Add Peer Authentication Policy] をクリックして新しいポリシーを追加します。

[IKE Settings] タブ

フィールド	説明
Enable IPsec over TCP	IPsec over TCP のトラフィックを許可するかどうか。 IPsec over TCP の方式がイネーブルになっている場合は、この方式がその他のすべての接続方式よりも優先されます。
Send Disconnect Notification	セッションが切断されることをクライアントに通知するかどうか。
Allow Inbound Aggressive Mode	着信アグレッシブ モードを許可するかどうか。

フィールド	説明
Wait for Termination before Rebooting	アクティブなセッションがすべて非強制的に終了された場合のみリブートを実行するかどうか。
Threshold for Cookie Challenge (0-100 Percent)	使用可能な最大 SA 数に対して、今後のセキュリティ アソシエーション（SA）のネゴシエーション用に Cookie チャレンジが発行されるまでネゴシエーション中（未処理）にできる SA 数のパーセンテージ。
Negotiation Threshold for Maximum SAs (0-100 Percent)	使用可能な最大 SA 数に対して、追加の接続が拒否されるまでネゴシエーション中にできる SA 数のパーセンテージ。 デフォルト値は 100 % です。
IKE Identity	フェーズ 2 識別方法： • [Automatic]：接続タイプによって ISAKMP ネゴシエーションが決まります。 ◦ 事前共有キーの IP アドレス。 ◦ 証明書認証の cert DN。 • [IP Address]：ISAKMP アイデンティティ情報を交換するホストの IP アドレス。 • [Hostname]：ISAKMP アイデンティティ情報を交換するホストの完全修飾ドメイン名。 • [Key ID]：リモート ピアが事前共有キーを検索するために使用するストリング。
Key for IKE Identity	IKE での識別方法がキー ID の場合に IKE での識別に使用するキー。
NAT Traversal	IPsec ピアが NAT デバイスを介して接続を確立できるようにするかどうか。

フィールド	説明
Keep-Alive Time for NAT Traversal	デバイスがピアにキープアライブメッセージを送信するまで、トンネルがアクティビティなしでいることのできる時間の長さ（時間、分、秒）。 有効な値は 10 ～ 3600 秒で、デフォルト値は 20 秒です。
IKE Version 2 Maximum Security Associations	ノードの IKE V2 SA の総数を設定可能にするかどうか。
Maximum number of SA	許可する SA 接続の最大数。
IKE V1 over TCP Port Table	1 [Add IKE V1 Over TCP Port] をクリックして、新しいポートを追加します。 2 [Port] フィールドに、IKE V1 に使用する TCP ポートを入力します。

[IPsec Settings] タブ

フィールド	説明
Anti Replay	SA アンチリプレイをイネーブルにするかどうか。
Anti Replay Window Size	パケットの重複を検出して防止するのに使用するウィンドウ サイズ。 使用するウィンドウ サイズを大きくするほど、復号器が検出できるパケットが多くなります。
SA Lifetime	SA の有効期間（日数、時間数、分数、秒数）。
SA Lifetime Volume (KB)	特定の SA が期限切れになるまでにそのアソシエーションを使用して IPsec ピア間を通過できるトラフィック量（KB 単位）。

プロファイルに関する作業

プロファイルはポリシーの集合です。 選択したポリシーでプロファイルを作成し、そのプロファイルをエッジ ファイアウォールなど複数のオブジェクトに適用することで、それらのオブジェクトのポリシーの整合性を保つことができます。

プロファイルをデバイスに適用する前に、デバイスを VNMC に登録する必要があります。

VNMC では、次のタイプのプロファイルを作成し、適用できます。

- コンピュート セキュリティ プロファイル：ACL ポリシーおよびユーザ定義属性を含むコンピュート ファイアウォール プロファイルです。
- エッジデバイス プロファイル：ルーティング、VPN、DHCP、IP 監査ポリシーを含むエッジ ファイアウォール プロファイルです。
- エッジ セキュリティ プロファイル：アクセス ポリシーおよび脅威緩和ポリシーを含むエッジ ファイアウォール プロファイルです。

ここでは、プロファイルの設定方法および適用方法について説明します。

コンピュート セキュリティ プロファイルの設定

VNMC を使用すると、ルート レベルまたはテナント レベルでコンピュート セキュリティ プロファイルを作成できます。 ルート レベルでコンピュート セキュリティ プロファイルを作成すると、複数のテナントに同じプロファイルを適用できます。

手順

ステップ 1 [Policy Management] > [Service Profiles] > [root] > [Compute Firewall] > [Compute Security Profiles] を選択します。

ステップ 2 [General] タブで、[Add Compute Security Profile] をクリックします。

ステップ 3 [Add Compute Security Profile] ダイアログボックスで、[Add Compute Security Profile] ダイアログボックス，（137 ページ）で説明されている情報を入力し、[OK] をクリックします。

[Add Compute Security Profile] ダイアログボックス

[General] タブ

フィールド	説明
Name	プロファイル名。 この名前には、ID となる 2 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。保存後は、この名前を変更できません。
Description	プロファイルの簡単な説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。
Policy Set	ポリシー セットのドロップダウン リスト。
Add ACL Policy Set	このリンクをクリックすると、ACL ポリシー セットを追加できます。
Resolved Policy Set	このリンクをクリックすると、解決されたポリシー セットを編集できます。
[Resolved Policies] 領域	
(Un)assign Policy	このリンクをクリックすると、ポリシーを割り当てまたは割り当て解除できます。
Name	ルール名。
Source Condition	ルールの送信元条件。
Destination Condition	ルールの宛先条件。
Protocol	ルールが適用されるプロトコル。
EtherType	ルールが適用される、カプセル化されているプロトコル。
Action	ルール条件が満たされた場合に実行するアクション。
Description	ルールの説明。

[Attributes] タブ

フィールド	説明
Add User Defined Attribute	属性を追加するダイアログボックスが開きます。
Name	属性名。
Value	属性値。

コンピュート ファイアウォール ポリシーの確認

アクティブなポリシーを確認し、必要に応じてコンピュート ファイアウォールのポリシー オブジェクトを変更するには、次の手順を使用します。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Compute Firewalls] > [*compute-firewall*] を選択します。

ステップ 2 [Compute Security Profiles] タブで、必要なポリシーを選択し、[Show Resolved Policies] をクリックします。

ステップ 3 [Edit] ダイアログボックスの [Resolved Policies] テーブルで必要なポリシーをクリックし、送信元と宛先の条件などのポリシーの詳細を表示します。

ステップ 4 ポリシーを変更するには、[Policy Set] 領域で、ドロップダウン リストから別のポリシーを選択するか、[Add ACL Policy Set] をクリックして新しいポリシーを設定します。

ステップ 5 [Apply] をクリックして変更を受け入れるか、ポリシーの確認が終わったら [OK] をクリックします。

エッジ デバイス プロファイルの設定

エッジデバイスプロファイルには、アドレス変換のタイムアウト値に加えて、次のポリシーが含まれています。

- DHCP
- IP 監査シグニチャ
- ルーティング

- VPN デバイス

組織階層の任意のレベル（ルート、テナント、仮想データセンター（VDC）、アプリ、または層）でエッジ デバイス プロファイルを作成することができます。 ルート レベルでエッジ デバイス プロファイルを作成すると、異なるテナントに複数のエッジ ファイアウォールを適用できます。

手順

ステップ 1 [Policy Management] > [Service Profiles] > [root] > [Edge Firewall] > [Edge Device Profiles] を選択します。

ステップ 2 [General] タブで、[Add Edge Device Profile] をクリックします。

ステップ 3 [Add Edge Device Profile] ダイアログボックスで、[Edge Device Profile] ダイアログボックス，（139 ページ）で説明されている情報を入力し、[OK] をクリックします。

[Edge Device Profile] ダイアログボックス

フィールド	説明
[General] タブ	
Name	プロファイル名。
Description	プロファイルの簡単な説明。
[Policies] タブ	
Routing Policy	既存のポリシーを選択するか、または [Add Routing Policy] をクリックして新しいポリシーを追加します。 割り当てたポリシーを確認または変更するには、[Resolved Policy] リンクをクリックします。
IP Audit Signature Policy	既存のポリシーを選択するか、または [Add IP Audit Signature Policy] をクリックして新しいポリシーを追加します。 割り当てたポリシーを確認または変更するには、[Resolved Policy] リンクをクリックします。

フィールド	説明
VPN Device Policy	既存のポリシーを選択するか、または[Add VPN Device Policy] をクリックして新しいポリシーを追加します。 割り当てたポリシーを確認または変更するには、[Resolved Policy] リンクをクリックします。
Address Translations Timeout	期限切れになるまでの、変換が未使用のままの期間（日、時間、分、および秒単位）。
DHCP Policy	
Edge DHCP Policy	新しいDHCPポリシーを追加する場合にクリックします。
Type	DHCP サービス タイプ（リレーまたはサーバ）。
Interface Name	DHCP ポリシーが適用されるインターフェイス。
Server/Relay Policy	DHCP ポリシー名。

[Events] タブ

フィールド	説明
ID	イベントの固有識別子。
User	次のいずれかのユーザ タイプ： • admin • internal • blank
Created at	障害が発生した日時。
Cause	イベント原因に関連付けられた固有識別情報。
Description	イベントの説明。

エッジ セキュリティ プロファイルの設定

エッジ セキュリティ プロファイルには、次のいずれかを含めることができます。

- ACL ポリシー セット（入力および出力）
- 接続タイムアウト ポリシー
- IP 監査ポリシー
- NAT ポリシー セット
- パケット インスペクション ポリシー
- TCP 代行受信ポリシー
- VPN インターフェイス ポリシー セット

組織階層の任意のレベル（ルート、テナント、VDC、アプリ、または層）でエッジセキュリティプロファイルを作成することができます。 ルート レベルでエッジ セキュリティ プロファイルを作成すると、異なるテナントに複数のエッジ ファイアウォールを適用できます。

手順

ステップ 1 [Policy Management] > [Service Profiles] > [Edge Firewall] > [Edge Security Profiles] を選択します。

ステップ 2 [General] タブで、[Add Edge Security Profile] をクリックします。

ステップ 3 [Add Edge Security Profile] ダイアログボックスで、[Add Edge Security Profile] ダイアログボックス,（141 ページ）で説明されている情報を入力します。

[Add Edge Security Profile] ダイアログボックス

フィールド	説明
[General] タブ	
Name	プロファイル名。
Description	プロファイルの簡単な説明。
[Ingress] タブ	

フィールド	説明
Policy Set	既存のポリシー セットを選択するか、または [Add ACL Policy Set] をクリックして新しいポリシー セットを追加します。 割り当てたポリシー セットを変更するには、[Resolved Ingress Policy Set] リンクをクリックします。
Resolved Policies	[(Un)assign Policy] をクリックすると、現在のポリシーセットにおいてポリシーが割り当てられるか、または削除されます。
[Egress] タブ	
Policy Set	既存のポリシー セットを選択するか、または [Add ACL Policy Set] をクリックして新しいポリシー セットを追加します。 割り当てたポリシー セットを変更するには、[Resolved Egress Policy Set] リンクをクリックします。
Resolved Policies	[(Un)assign Policy] をクリックすると、現在のポリシーセットにおいてポリシーが割り当てられるか、または削除されます。
[NAT] タブ	
Policy Set	既存のポリシー セットを選択するか、または [Add NAT Policy Set] をクリックして新しいポリシー セットを追加します。 割り当てたポリシー セットを変更するには、[Resolved NAT Policy Set] リンクをクリックします。
Resolved Policies	[(Un)assign Policy] をクリックすると、現在のポリシーセットにおいてポリシーが割り当てられるか、または削除されます。
[VPN] タブ	

フィールド	説明
Policy Set	既存のポリシー セットを選択するか、または [Add Interface Policy Set] をクリックして新しいポリシー セットを追加します。 割り当てたポリシー セットを変更するには、[Resolved VPN Interface Policy Set] リンクをクリックします。
[Advanced] タブ	
Packet Inspection Policy	既存のポリシーを選択するか、または [Add Packet Inspection Policy] をクリックして新しいポリシーを追加します。 割り当てたポリシーを変更するには、[Resolved Policy] リンクをクリックします。
Connection Timeout Policy	既存のポリシーを選択するか、または [Add Connection Timeout Policy] をクリックして新しいポリシーを追加します。 割り当てたポリシーを変更するには、[Resolved Policy] リンクをクリックします。
TCP Intercept Policy	既存のポリシーを選択するか、または [Add TCP Intercept Policy] をクリックして新しいポリシーを追加します。 割り当てたポリシーを変更するには、[Resolved Policy] リンクをクリックします。
IP Audit Policy	既存のポリシーを選択するか、または [Add IP Audit Policy] をクリックして新しいポリシーを追加します。 割り当てたポリシーを変更するには、[Resolved Policy] リンクをクリックします。

エッジ デバイス プロファイルの適用

エッジ デバイス プロファイルを作成したら、複数のエッジ ファイアウォールにプロファイルを適用し、ファイアウォール全体で一貫したポリシーを使用できます。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Edge Firewalls] > [*edge-firewall*] を選択します。

ステップ 2 [General] タブで、[Edge Device Profile] フィールドの [Select] をクリックします。

ステップ 3 [Select Edge Device Profile] ダイアログボックスで、必要なプロファイルを選択し、[OK] をクリックします。

ステップ 4 [Save] をクリックします。

エッジ セキュリティ プロファイルの適用

エッジ セキュリティ プロファイルを作成したら、エッジ ファイアウォール インスタンスにそれを適用し、インターフェイス上で一貫したポリシーを使用できます。

（注） エッジ セキュリティ プロファイルは、エッジ ファイアウォールの外部インターフェイスにのみ適用できます。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Edge Firewalls] > [*edge-firewall*] を選択します。

ステップ 2 [Interfaces] テーブルで、必要な外部インターフェイスを選択し、[Edit] をクリックします。

ステップ 3 [Edit] ダイアログボックスで、[Edge Security Profile] フィールドの [Select] をクリックします。

ステップ 4 [Select Edge Security Profile] ダイアログボックスで、必要なプロファイルを選択し、[OK] をクリックします。

ステップ 5 開いているダイアログボックスで [OK] をクリックし、[Save] をクリックします。

エッジ ファイアウォール ポリシーの確認

アクティブなポリシーを確認し、必要に応じてエッジファイアウォールのポリシーオブジェクトを変更するには、次の手順を使用します。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Edge Firewalls] > [*edge-firewall*] を選択します。

ステップ 2 [Edge Security Profiles] タブで、必要な Syslog ポリシーを選択し、[Show Resolved Policies] をクリックします。

ステップ 3 ポリシーまたはポリシー セットの詳細を表示するには、[Edit] ダイアログボックスのタブを使用して、必要なポリシーまたはポリシー セットに移動し、[Resolved] フィールドの中で必要なポリシーまたはポリシー セットをクリックします。

ステップ 4 異なるポリシーまたはポリシーセットを使用するには、必要なポリシーまたはポリシーセットに移動し、ドロップダウンリストから異なるポリシーまたはポリシーセットを選択するか、新しいポリシーまたはポリシー セットを追加します。

ステップ 5 [Apply] をクリックして変更を受け入れるか、ポリシーの確認が終わったら [OK] をクリックします。

セキュリティ プロファイルの設定

コンピュート ファイアウォールのセキュリティ プロファイルの編集

手順

ステップ 1 [Policy Management] > [Service Profiles] > [root] > [Compute Firewalls] > [Compute Security Profiles] を選択します。

ステップ 2 [General] タブで、編集するプロファイルを選択し、[Edit] をクリックします。

ステップ 3 [Edit Compute Security Profile] ダイアログボックスで、必要に応じて次のテーブルの情報を使用してフィールドを編集し、[OK] をクリックします。

表 *10* : *[General]* タブ

フィールド	説明
Name	プロファイル名。
Description	ポリシーの簡単な説明。
Policy Set	使用可能なポリシー セットのリスト。

フィールド	説明
Add ACL Policy Set	新規 ACL ポリシー セットを追加する場合にクリックします。
Resolved Policy Set	このリンクをクリックすると、解決されたポリシーセットを表示したり、必要に応じて編集したりすることができます。
Resolved Policies	
(Un)assigned Policy	クリックすると、ポリシーを割り当てまたは割り当て解除できます。
Source Condition	ポリシーの送信元条件。
Destination Condition	ポリシーの宛先条件。
Protocol	ポリシーで指定するプロトコル。
Ethertype	ポリシーで指定する EtherType。
Action	指定した条件が満たされた場合に実行するアクション。
Description	ポリシーの簡単な説明。

表 ***11*** : ***[Attributes]*** タブ

フィールド	説明
Add User Defined Attribute	カスタム属性を追加する場合にクリックします。
Name	属性名。
Value	属性値。

エッジ ファイアウォールのセキュリティ プロファイルの編集

この手順では、エッジファイアウォールに関連付けられているセキュリティプロファイルを編集できます。

手順

ステップ 1 [Policy Management] > [Service Profiles] > [root] > [Edge Firewall] > [Edge Security Profiles] を選択します。

ステップ 2 [General] タブで、編集するエッジセキュリティプロファイルを選択し、[Edit] をクリックします。

ステップ 3 [Edit Edge Security Profile] ダイアログボックスで、必要に応じて次のテーブルの情報を使用してエントリを編集し、[OK] をクリックします。

フィールド	説明
[General] タブ	
Name	プロファイル名。
Description	プロファイルの簡単な説明。
ID	固有プロファイル識別情報。
[Ingress] タブ	
Policy Set	既存のポリシー セットを選択するか、または [Add ACL Policy Set] をクリックして新しいポリシー セットを追加します。 割り当てたポリシー セットを変更するには、[Resolved Ingress Policy Set] リンクをクリックします。
Resolved Policies	[(Un)assign Policy] をクリックすると、現在のポリシーセットにおいてポリシーが割り当てられるか、または削除されます。
[Egress] タブ	
Policy Set	既存のポリシー セットを選択するか、または [Add ACL Policy Set] をクリックして新しいポリシー セットを追加します。 割り当てたポリシー セットを変更するには、[Resolved Egress Policy Set] リンクをクリックします。

フィールド	説明
Resolved Policies	[(Un)assign Policy] をクリックすると、現在のポリシーセットにおいてポリシーが割り当てられるか、または削除されます。
[NAT] タブ	
Policy Set	既存のポリシー セットを選択するか、または [Add NAT Policy Set] をクリックして新しいポリシー セットを追加します。 割り当てたポリシー セットを変更するには、[Resolved NAT Policy Set] リンクをクリックします。
Resolved Policies	[(Un)assign Policy] をクリックすると、現在のポリシーセットにおいてポリシーが割り当てられるか、または削除されます。
[VPN] タブ	
Policy Set	既存のポリシー セットを選択するか、または [Add Interface Policy Set] をクリックして新しいポリシー セットを追加します。 割り当てたポリシー セットを変更するには、[Resolved VPN Interface Policy Set] リンクをクリックします。
[Advanced] タブ	
Packet Inspection Policy	既存のポリシーを選択するか、または [Add Packet Inspection Policy] をクリックして新しいポリシーを追加します。 割り当てたポリシーを変更するには、[Resolved Policy] リンクをクリックします。
Connection Timeout Policy	既存のポリシーを選択するか、または [Add Connection Timeout Policy] をクリックして新しいポリシーを追加します。 割り当てたポリシーを変更するには、[Resolved Policy] リンクをクリックします。

フィールド	説明
Threat Migration	既存のポリシーを選択するか、または[Add TCP Intercept Policy] をクリックして新しいポリシーを追加します。 割り当てたポリシーを変更するには、[Resolved Policy] リンクをクリックします。
IP Audit Policy	既存のポリシーを選択するか、または [Add IP Audit Policy] をクリックして新しいポリシーを追加します。 割り当てたポリシーを変更するには、[Resolved Policy] リンクをクリックします。

セキュリティ プロファイルの削除

手順

ステップ 1 [Navigation] ペインの [Policy Management] タブをクリックします。

ステップ 2 [Navigation] ペインの [Security Policies] サブタブをクリックします。

ステップ 3 [Navigation] ペインで、[root] > [Security Profiles] を展開します。

ステップ 4 [Work] ペインで、削除するセキュリティ プロファイルをクリックします。

ステップ 5 [Delete] をクリックします。

ステップ 6 [Confirm] ダイアログボックスで、[OK] をクリックします。

セキュリティ プロファイル属性の削除

手順

ステップ 1 [Navigation] ペインの [Policy Management] タブをクリックします。
ステップ 2 [Navigation] ペインの [Security Policies] サブタブをクリックします。
ステップ 3 [Navigation] ペインで、[root] > [Security Profiles] を展開します。
ステップ 4 [Navigation] ペインで、削除する属性を含むセキュリティ プロファイルをクリックします。
ステップ 5 [Work] ペインで、[Attributes] タブをクリックします。
ステップ 6 削除する属性をクリックします。
ステップ 7 [Delete] をクリックします。
ステップ 8 [Confirm] ダイアログボックスで、[OK] をクリックします。

ポリシーの割り当て

手順

ステップ 1 [Navigation] ペインの [Policy Management] タブをクリックします。
ステップ 2 [Navigation] ペインの [Security Policies] サブタブをクリックします。
ステップ 3 [Navigation] ペインで、[root] > [Security Profiles] を展開します。
ステップ 4 [Navigation] ペインで、ポリシーを割り当てるプロファイルをクリックします。
ステップ 5 [Work] ペインで、[(Un)assign Policy] リンクをクリックします。
ステップ 6 [(Un)assign Policy] ダイアログボックスで、割り当てるポリシーを [Assigned] リストに移動します。
ステップ 7 [OK] をクリックします。

ポリシーの割り当て解除

手順

ステップ 1 [Navigation] ペインの [Policy Management] タブをクリックします。

ステップ 2 [Navigation] ペインの [Security Policies] サブタブをクリックします。

ステップ 3 [Navigation] ペインで、[root] > [Security Profiles] を展開します。

ステップ 4 [Navigation] ペインで、ポリシーの割り当てを解除するプロファイルをクリックします。

ステップ 5 [Work] ペインで、[(Un)assign Policy] リンクをクリックします。

ステップ 6 [(Un)assign Policy] ダイアログボックスで、割り当てを解除するポリシーを [Available] リストに移動します。

ステップ 7 [OK] をクリックします。

セキュリティ ポリシー属性の設定

オブジェクト グループの設定

オブジェクト グループの追加

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [*tenant*] > [Policy Helpers] > [Object Groups] を選択します。

ステップ 2 [General] タブで、[Add Object Group] をクリックします。

ステップ 3 [Add Object Group] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

（注） オブジェクト グループ式を追加する前に、属性のタイプと名前を指定する必要があります。

フィールド	説明
Name	オブジェクト グループ名。 この名前には、ID となる 2 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。保存後は、この名前を変更できません。

フィールド	説明
Description	オブジェクト グループの簡単な説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。
Attribute Type	使用可能な属性タイプ。 オブジェクトグループ式を追加するには、属性タイプと属性名を設定する必要があります。
Attribute Name	使用可能な属性名。
[Expression] テーブル	
Add Object Group Expression	クリックすると、オブジェクトグループ式が追加されます。
Operator	選択した式に使用する演算子。
Value	選択した式に使用する値。

オブジェクト グループ式の追加

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policy Helpers] > [Object Groups] を選択します。

ステップ 2 [General] タブで、オブジェクト グループ式に追加するオブジェクト グループを選択し、[Edit] をクリックします。

（注） 新しいオブジェクト グループの場合は、オブジェクト グループ式を追加する前に、属性のタイプと名前を指定する必要があります。

ステップ 3 [Edit Object Group] ダイアログボックスで、[Add Object Group Expression] をクリックします。

ステップ 4 [Add Object Group Expression] ダイアログボックスで、次のテーブルで説明されている情報を使用してオブジェクト グループ式を指定し、開いているダイアログボックスで [OK] をクリックします。

フィールド	説明
Attribute Name	属性（読み取り専用）

フィールド	説明
Operator	この属性に使用可能な演算子。
Attribute Value	この式に使用する属性値。

オブジェクト グループの編集

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [*tenant*] > [Policy Helpers] > [Object Groups] を選択します。

ステップ 2 [General] タブで、編集するオブジェクト グループを選択し、[Edit] をクリックします。

ステップ 3 [Edit Object Group] ダイアログボックスで、次のようにフィールドを変更し、[OK] をクリックします。

フィールド	説明
Name	オブジェクト グループ名（読み取り専用）。
Description	オブジェクト グループの説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。
Attribute Type	指定されている属性タイプ（読み取り専用）。
Attribute Name	指定されている属性名（読み取り専用）。
[Expression] テーブル	
Add Object Group Expression	クリックすると、新しいオブジェクト グループ式が追加されます。
Operator	式の演算子。
Value	式の属性値。

オブジェクト グループ式の編集

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policy Helpers] > [Object Groups] を選択します。

ステップ 2 [General] タブで、編集する式を持つオブジェクト グループをクリックし、[Edit] をクリックします。

ステップ 3 [Edit Object Group] ダイアログボックスの [Expression] テーブルで編集する式を選択し、[Edit] をクリックします。

ステップ 4 [Edit Object Group Expression] ダイアログボックスで、必要に応じてフィールドを編集し、開いているダイアログボックスで [OK] をクリックします。

フィールド	説明
Attribute Name	属性名（読み取り専用）。
Operator	この式に使用可能な演算子。
Attribute Value	この式に使用する属性値。

オブジェクト グループの削除

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policy Helpers] > [Object Groups] を選択します。

ステップ 2 [General] タブで、削除するオブジェクト グループをクリックし、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

オブジェクト グループ式の削除

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policy Helpers] > [Object Groups] を選択します。

ステップ 2 [General] タブで、削除する式を含むオブジェクト グループをクリックし、[Edit] をクリックします。

ステップ 3 [Edit Object Group] ダイアログボックスの [Expression] テーブルで削除する式を選択し、[Delete] をクリックします。

ステップ 4 確認の画面が表示されたら、削除を確認します。

ステップ 5 開いているダイアログボックスの [OK] ボタンをクリックして、変更内容を保存します。

セキュリティ プロファイル ディクショナリの設定

セキュリティ プロファイル ディクショナリの追加

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [*tenant*] > [Policy Helpers] > [Security Profile Dictionary] を選択します。

（注） セキュリティ プロファイル ディクショナリは、ルート レベルに 1 つ、各テナントに 1 つ作成できます。

ステップ 2 [General] タブで、[Add Security Profile Dictionary] をクリックします。

ステップ 3 [Add Security Profile Dictionary] ダイアログボックスで、必要に応じて次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	セキュリティ プロファイル ディクショナリの名前。 この名前には、1～16 文字の英数字を使用できます。 スペースや特殊文字は使用できません。また、オブジェクトの保存後は、この名前を変更できません。 （注） セキュリティ プロファイル ディクショナリは、ルート レベルに 1 つ、およびテナント レベルに 1 つ作成できます。

フィールド	説明
Description	セキュリティ プロファイル ディクショナリの説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。
[Attributes] テーブル	
Add Security Profile Custom Attribute	新しい属性を追加する場合にクリックします。
Name	カスタム属性名。
Description	カスタム属性の説明。

セキュリティ プロファイル ディクショナリ属性の追加

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [*tenant*] > [Policy Helpers] > [Security Profile Dictionary] を選択します。

ステップ 2 [General] タブで、属性に追加するセキュリティ プロファイル ディクショナリを選択し、[Edit] をクリックします。

ステップ 3 [Edit Security Profile Dictionary] ダイアログボックスで、[Add Security Profile Custom Attribute] リンクをクリックします。

ステップ 4 [Add Security Profile Custom Attribute] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	属性名。 この名前には、1 ～ 16 文字の英数字を使用できます。スペースや特殊文字は使用できません。また、オブジェクトの保存後は、この名前を変更できません。

フィールド	説明
Description	属性の説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。

セキュリティ プロファイル ディクショナリの編集

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policy Helpers] > [Security Profile Dictionary] を選択します。

ステップ 2 [General] タブで、編集するセキュリティ プロファイル ディクショナリをクリックし、[Edit] をクリックします。

ステップ 3 [Edit Security Profile Dictionary] ダイアログボックスで、必要に応じて次のフィールドを変更し、[OK] をクリックします。

フィールド	説明
Name	セキュリティ プロファイル ディクショナリの名前（読み取り専用）。
Description	セキュリティ プロファイル ディクショナリの説明。
Attributes	
Add Security Profile Custom Attribute	カスタム属性を追加する場合にクリックします。
Name	属性名。
Description	属性の説明。

セキュリティ プロファイル ディクショナリ属性の編集

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policy Helpers] > [Security Profile Dictionary] を選択します。

ステップ 2 [General] タブで、編集する属性を含むセキュリティ プロファイルディクショナリをクリックし、[Edit] をクリックします。

ステップ 3 [Edit Security Profile Dictionary] ダイアログボックスで、編集する属性を選択し、[Edit] をクリックします。

ステップ 4 [Edit Security Custom Attribute] ダイアログボックスで、必要に応じて [Description] フィールドを編集し、開いているダイアログボックスで [OK] をクリックして変更を保存します。

セキュリティ プロファイル ディクショナリの削除

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policy Helpers] > [Security Profile Dictionary] を選択します。

ステップ 2 [General] タブで、削除するセキュリティ プロファイル ディクショナリをクリックし、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

セキュリティ プロファイル ディクショナリ属性の削除

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policy Helpers] > [Security Profile Dictionary] を選択します。
[General] タブで、削除する属性を含むディクショナリをクリックし、[Edit] をクリックします。

ステップ 2 [Edit Security Profile Dictionary] ダイアログボックスの [Attributes] テーブルで、削除する属性を選択し、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

vZones の操作

仮想ゾーン（vZone）は、VM またはホストを論理的にグループ化したものです。 vZones により、ポリシーおよびプロファイルの操作が円滑に行われます。vZones では、vZone 名を使用して vZone 属性に基づくポリシーを作成できるためです。

次に VNMC における vZones の操作の流れをおおまかに示します。

1. vZone に含めるため、それぞれ 1 つ以上条件を指定して、vZone を定義します。
2. ゾーンまたはネットワークの条件に基づくルールを持ったサービス ポリシーを定義します。
3. 手順 2 で定義したサービス ポリシーを含むポリシー セットを作成します。
4. 手順 3 で作成されたポリシー セットを含むセキュリティ プロファイルを作成します。
5. セキュリティ プロファイルを ASA 1000V または VSG のポート プロファイルにバインドします。
6. セキュリティ プロファイルを VNMC で ASA 1000V または VSG に割り当てます。

vZones の操作の詳細については、次のトピックを参照してください。

vZone の追加

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policy Helpers] > [vZones] を選択します。

ステップ 2 [General] タブで、[Add vZone] をクリックします。

ステップ 3 [Add vZone] ダイアログボックスで、次のテーブルで説明されている必須情報を入力し、[OK] をクリックします。

フィールド	説明
Name	vZone 名。 この名前には、2 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。 この名前は、保存後には変更できません。
Description	vZone の簡単な説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。 ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。
vZone Condition	
Add Zone Condition	ゾーン条件を追加する場合にクリックします。

フィールド	説明
Attribute Name	条件の属性名。
Operator	条件の演算子。
Attribute Value	条件の属性値。

vZone の編集

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policy Helpers] > [vZones] を選択します。

ステップ 2 [General] タブで、編集する vZone を選択し、[Edit] をクリックします。

ステップ 3 [Edit vZone] ダイアログボックスの [General] タブで、必要に応じてフィールドを編集し、[OK] をクリックします。

フィールド	説明
Name	vZone 名（読み取り専用）。
Description	vZone の簡単な説明。
vZone Condition	
Add vZone	vZone 条件を追加する場合にクリックします。
Up and down arrows	選択したポリシーの優先順位を変更します。
Attribute Name	選択した vZone 条件の属性名。
Operator	選択した vZone 条件の演算子。
Attribute Value	選択した vZone 条件の属性値。

ステップ 4 vZone 条件の変更方法：

a) [vZone Condition] テーブルで、編集する属性を選択し、[Edit] をクリックします。

b) [Edit Zone Condition] ダイアログボックスで、次の情報を使用して必要な変更を行います。

フィールド	説明
Attribute Type	条件の属性タイプ（読み取り専用）
Attribute Name	条件の属性名（読み取り専用）
Operator	条件を適用する演算子
Attribute Value	条件の属性値。

ステップ 5 開いているダイアログボックスで [OK] をクリックし、[Save] をクリックします。

vZone 条件の削除

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policy Helpers] > [vZones] を選択します。

ステップ 2 [General] タブで、削除する条件を持つ vZone をクリックし、[Edit] をクリックします。

ステップ 3 [Edit vZone] ダイアログボックスの [vZone Condition] テーブルで、削除する条件をクリックし、[Delete] をクリックします。

ステップ 4 削除を確認します。

ステップ 5 [Edit vZone] ダイアログボックスで、[OK] または [Apply] をクリックします。

vZone の削除

手順

ステップ 1 [Policy Management] > [Service Policies] > [root] > [Policy Helpers] > [vZones] を選択します。

ステップ 2 [General] タブで、削除する vZone をクリックし、[Delete] をクリックします。

ステップ 3 削除を確認します。

第 10 章

デバイス ポリシーおよびプロファイルの設定

この項では、次のトピックについて取り上げます。

デバイス ポリシーおよびプロファイル

VNMC では、任意の組織レベルでデバイス プロファイルおよびポリシーを作成できます。

デバイス プロファイル

VNMC デバイス プロファイルは、カスタム セキュリティ属性およびデバイス ポリシーのセットです。 Nexus 1000V VSM の場合、デバイス プロファイルはポート プロファイルに追加されています。 ポート プロファイルは Nexus 1000V VSM vNIC に割り当てられます。これで、デバイス プロファイルは仮想マシン（VM）の一部になります。 デバイス プロファイルを VM に追加すると、カスタム属性を VM に追加できるようになります。 カスタム属性を使用して、VM 間のトラフィックを通過またはドロップさせるファイアウォール ルールを作成できます。

[Resource Management] > [Managed Resources] を選択し、ルート レベルまたはテナント レベルにある必要なコンピュートファイアウォールまたはエッジファイアウォールに移動することで、デバ

イス プロファイルをコンピュート ファイアウォールおよびエッジ ファイアウォールに適用します。 ファイアウォール ペインの [Firewall Settings] 領域には、[Device Profile] オプションが組み込まれています。

VNMC には、ルート レベルでデフォルトのデバイス プロファイルが含まれています。 デフォルトのデバイス プロファイルは編集できますが、削除はできません。

ポリシー

VNMC は、ポリシーに関連した次のオブジェクトをサポートします。

- ポリシーセット：ポリシーが入っています。 ポリシーセットを作成したら、それをプロファイルに割り当てることができます。 既存のデフォルト ポリシー セットが、システムの起動時に自動的に割り当てられます。
- ポリシー：命令できるルールが入っています。 既存のデフォルト ポリシーが、システムの起動時に自動的に割り当てられます。 デフォルト ポリシーには、drop というアクションのあるルールが入っています。
- ルール：トラフィックを規制する条件が入っています。 デフォルト ポリシーには、drop というアクションのあるルールが入っています。 ルールの条件は、ネットワーク、カスタム、および仮想マシン属性を使用して設定できます。
- オブジェクト グループ：組織ノードで作成できます。 オブジェクト グループは、システム定義属性またはユーザ定義属性で条件式の集合を定義します。 オブジェクト グループは、メンバまたは非メンバ演算子の選択時にポリシー ルール条件で参照できます。 オブジェクト グループの式のいずれかが true の場合、オブジェクト グループを参照するルール条件は true に解決します。
- セキュリティ プロファイル ディクショナリ：セキュリティ属性の論理集合です。 セキュリティ プロファイルで使用するディクショナリ属性を定義します。 セキュリティ プロファイル ディクショナリは、ルートまたはテナント ノードで作成されます。 1 つのテナントに 1 つ、ルートに 1 つのディクショナリのみを作成できます。 ユーザは、セキュリティ プロファイルディクショナリを使用して、カスタム属性の名前を定義できます。 カスタム属性値は、セキュリティ プロファイル オブジェクトで指定します。 カスタム属性は、ポリシー ルール条件の定義に使用できます。 ルート レベル ディクショナリで設定された属性は、任意のテナントで使用できます。 テナント レベルの下にはディクショナリを作成できません。
- ゾーン：条件に基づいた VM のセットです。 ゾーン名は、オーサリング ルールで使用されます。

セキュリティ ポリシーは作成後、Cisco VSG にプッシュされます。

デバイス設定

VNMC では、ポリシーをデバイスプロファイルに追加し、そのプロファイルをデバイスに適用することでデバイスを設定できます。デバイスプロファイルには、次に示すポリシーおよび設定のオプションが入っています。

- DNS サーバとドメイン
- NTP サーバ
- SNMP ポリシー
- Syslog ポリシー
- 障害ポリシー
- コア ポリシー
- ログ ファイル ポリシー
- ポリシー エンジン ロギング
- 認証ポリシー

デバイス ポリシー

VNMC では、次に示すポリシーを作成し、コンピュート ファイアウォール、エッジ ファイアウォール、VSG に適用するため、デバイス プロファイルに割り当てることができます。

- AAA ポリシー
- コア ファイル ポリシー
- 障害ポリシー
- ロギング ポリシー
- SNMP ポリシー
- Syslog ポリシー

VNMC は、障害、ロギング、SNMP、syslog の各ポリシーについてデフォルト ポリシーを提供しています。 デフォルト ポリシーは削除できませんが、変更できます。 デバイス プロファイルでは、名前解決を使用してポリシーの割り当てを解決します。 詳細については、マルチテナント環境における名前解決, （84 ページ）を参照してください。

ルートで作成されたポリシーは、VNMCプロファイルとデバイスプロファイルの両方に表示されます。

デバイス ポリシーの設定

VNMC では、次のタイプのデバイス ポリシーを設定し、管理できます。

- AAA
- Core File
- Fault
- Logging
- SNMP
- Logging

AAA ポリシーの設定

AAA 認証ポリシーは、ユーザにネットワークおよびネットワーク サービスへのアクセスを許可する前に、ユーザを検証します。 VNMC の AAA 認証ポリシーを作成し、デバイス プロファイルを使用してポリシーをオブジェクトと関連付けることで、認証されたユーザのみがオブジェクトにアクセスできるようにできます。

VNMC は、エッジ ファイアウォールと、次のプロトコルを使用するサーバ グループの AAA 認証と認可をサポートしています。

- Kerberos
- Lightweight Directory Access Protocol（LDAP）
- Windows NT
- RADIUS
- RSA SecurID（SDI）
- TACACS+

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Auth Policies] を選択します。

ステップ 2 [General] タブで、[Add Auth Policy] をクリックします。

ステップ 3 [Add Auth Policy] ダイアログボックスで、[Add Auth Policy] ダイアログボックス, （167 ページ）で説明されている情報を入力し、[OK] をクリックします。

（注） 新しいサーバ ホストを持つ新しいサーバ グループを使用してリモート サーバ グループを追加する場合、ホスト用に入力する必要のある情報は使用するプロトコルに応じて異なります。 たとえば、RADIUS サーバ ホストに必要な情報は、LDAP サーバ ホストに必要な情報とは異なります。

選択したプロトコルに必要な情報については、オンライン ヘルプを参照してください。

フィールドの説明

[Add Auth Policy] ダイアログボックス

フィールド	説明
Name	ポリシー名。
Description	ポリシーの簡単な説明。
Authorization	サーバ認証によって承認を有効にする場合は、[Enable] チェックボックスをオンにします。
Remote Access Methods	
Add Remote Access Method	ポリシーにリモート アクセス方法を追加します。 詳細については、[Remote Access Method] ダイアログボックス，（168 ページ）を参照してください。
Access Method	次のいずれかのアクセス方法： • Enable Mode • HTTP • Serial • SSH • Telnet
Admin State	ポリシーの管理状態をイネーブルにするかまたはディセーブルにするか。
Remote Server Group	リモート サーバ グループ名。
Local Auth	このカラムは使用されません。

[Remote Access Method] ダイアログボックス

フィールド	説明
Access Method	次のいずれかのアクセス方法： • Enable Mode • HTTP • Serial • SSH • Telnet
Admin State	アクセス方法の管理状態をイネーブルにするか、ディセーブルにするか。
Server Group	使用するサーバ グループを指定します。 **1** [Protocol for Creation] フィールドで、必要なプロトコルを選択します。 **2** [Server Group] フィールドで、次のいずれかを実行します。 • ドロップダウン リストから、使用可能なリモート サーバ グループを選択します。 • [Add Remote Server Group - *protocol*] をクリックして、新しいリモート サーバ グループを追加します。 （注） 新しいリモート サーバ グループを追加する場合、サーバ グループとホストのために提供する情報は、使用するプロトコルによって異なります。 たとえば、RADIUS のサーバ グループおよびホストに必要な情報は、LDAP のサーバ グループおよびホストに必要な情報とは異なります。

コア ファイル ポリシーの設定

デバイスのコア ファイル ポリシーの追加

どの組織レベルでもコア ポリシーを追加できます。

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Core File] を選択します。

ステップ 2 [General] タブで、[Add Core File Policy] をクリックします。

ステップ 3 [Add Core File Policy] ダイアログボックスで、次のテーブルで説明されている情報を追加し、[OK] をクリックします。

フィールド	説明
Name	コア ファイル ポリシー名。 この名前には、1 ～ 32 文字の英数字を使用できます。 スペースや特殊文字は使用できません。また、オブジェクトの作成後は、この名前を変更できません。
Description	ポリシーの簡単な説明。 このフィールドには、ID となる 1 ～ 256 文字を使用できます。 ハイフン（-）、アンダースコア（_）、ドット（.）などの英数文字を使用できます。
Admin State	ポリシーの管理状態をイネーブルにするか、またはディセーブルにするかを指定します。
Hostname	このポリシーに使用するホスト名または IP アドレス。 IP アドレスではなくホスト名を使用する場合、VNMC で DNS サーバを設定する必要があります。
Port	コア ダンプ ファイルの送信に使用されるポート番号。
Protocol	コア ダンプ ファイルのエクスポートに使用されるプロトコル（読み取り専用）。

フィールド	説明
Path	リモート システムにコア ダンプ ファイルを保存するときに使用するパス。 デフォルト パスが /tftpboot のため、たとえば、/tftpboot/*test* を使用します。*test* はサブフォルダです。

デバイス プロファイルのコア ファイル ポリシーの編集

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Core File] を選択します。

ステップ 2 [General] タブで、編集するコア ファイル ポリシーをクリックし、[Edit] をクリックします。

ステップ 3 [Edit Core File Policy] ダイアログボックスで、必要に応じて次のテーブルの情報を使用してフィールドを編集し、[OK] をクリックします。

フィールド	説明
Name	コア ファイル ポリシーの名前（読み取り専用）。
Description	ポリシーの簡単な説明。
Admin State	ポリシーの管理状ステータス：イネーブルまたはディセーブル。
Hostname	ホスト名または IP アドレス。 （注） ホスト名を使用する場合、DNS サーバを設定する必要があります。
Port	コア ダンプ ファイルをエクスポートするときに使用するポート番号。
Protocol	コア ダンプ ファイルのエクスポートに使用されるプロトコル（読み取り専用）。

フィールド	説明
Path	リモート システムにコア ダンプ ファイルを保存するときに使用するパス。 デフォルトのパスは /tftpboot です。 tftpboot の下位のサブフォルダを指定するには、/tftpboot/*folder* の形式を使用します。*folder* がサブフォルダです。

デバイス プロファイルからのコア ファイル ポリシーの削除

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Core File] を選択します。

ステップ 2 [General] タブで、削除するコア ファイル ポリシーを選択し、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

障害ポリシーの設定

デバイス プロファイル用障害ポリシーの追加

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Fault] を選択します。

ステップ 2 [General] タブで、[Add Fault Policy] をクリックします。

（注） どの組織レベルでもポリシーを追加できます。

ステップ 3 [Add Fault Policy] ダイアログボックスで、次のテーブルで説明されている情報を入力し、[OK] をクリックします。

フィールド	説明
Name	障害ポリシー名。 この名前には、ID となる 1 ～ 32 文字を使用できます。 ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。 作成後は、この名前を変更できません。
Description	ポリシーの簡単な説明。
Flapping Interval	システムによって障害の状態が変更されるまでに経過する必要がある時間の長さ（時間数、分数、および秒数）。 障害が発生し、すぐに何度かクリアされると、フラッピングが発生します。 これを防止するため、システムでは、最後に状態が変更されてからこの時間が経過するまで、障害が発生しても状態は変更されません。 フラッピング間隔中に同じ条件が再発生した場合は、障害がアクティブ状態に戻ります。 フラッピング間隔中に同じ条件が再発生しない場合は、障害がクリアされます。 その時点で発生する処理は、[Clear Faults Retention Action] フィールドの設定によって異なります。 デフォルトのフラッピング間隔は 10 秒です。
Clear Faults Retention Action	障害がクリアされたときに実行するアクション： • [retain]：クリアされた障害を保持します。 • [delete]：障害メッセージは、クリア対象のマークが付くと即時削除されます。

フィールド	説明
Clear Faults Retention Interval	クリアされた障害メッセージをシステムで保持する期間： • [Forever]：すべての障害メッセージは、クリアされても、経過時間に関係なく、そのまま保持されます。 • [Other]：クリアされた障害メッセージは、指定された期間の間保持されます。 このオプションを選択したときに表示されるスピンボックスで、クリアされた障害メッセージをシステムで保持する期間（日数、時間数、分数、および秒数）を入力します。

デバイス プロファイルの障害ポリシーの編集

（注） システムの起動時、すでにデフォルト ポリシーが存在します。 デフォルト ポリシーは削除できませんが、変更できます。

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Fault] を選択します。

ステップ 2 [General] タブで、編集する障害ポリシーを選択し、[Edit] をクリックします。

ステップ 3 [Edit Fault Policy] ダイアログボックスで、必要に応じて次のフィールドを変更し、[OK] をクリックします。

フィールド	説明
Name	ポリシー名（読み取り専用）。
Description	ポリシーの簡単な説明。

フィールド	説明
Flapping Interval	システムによって障害の状態が変更されるまでに経過する必要がある時間の長さ（時間数、分数、および秒数）。 障害が発生し、すぐに何度かクリアされると、フラッピングが発生します。 これを防止するため、システムでは、最後に状態が変更されてからこの時間が経過するまで、障害が発生しても状態は変更されません。 フラッピング間隔中に同じ条件が再発生した場合は、障害がアクティブ状態に戻ります。 フラッピング間隔中に同じ条件が再発生しない場合は、障害がクリアされます。 次のアクションは、[Clear Faults Retention Action] フィールドの設定によって異なります。 デフォルトのフラッピング間隔は 10 秒です。
Clear Faults Retention Action	使用可能な、障害を保持するアクション： • [retain]：システムにより、障害メッセージが保持されます。 • [delete]：障害メッセージにクリア対象のマークを付けた時点で、それらのメッセージが削除されます。
Clear Faults Retention Interval	クリアされた障害メッセージをシステムで保持する期間： • [Forever]：すべての障害メッセージは、クリアされても、経過時間に関係なく、そのまま保持されます。 • [Other]：クリアされた障害メッセージは、指定された期間の間保持されます。 このオプションを選択したときに表示されるスピンボックスで、クリアされた障害メッセージをシステムで保持する期間（日数、時間数、分数、および秒数）を入力します。

デバイス プロファイルの障害ポリシーの削除

（注） システムの起動時、すでにデフォルト ポリシーが存在します。 デフォルト ポリシーは削除できませんが、変更できます。

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Fault] を選択します。

ステップ 2 [General] タブで、削除する障害ポリシーをクリックし、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

ログ ファイル ポリシーの設定

デバイス プロファイルのロギング ポリシーの追加

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Log File] を選択します。

ステップ 2 [General] タブで、[Add Logging Policy] をクリックします。

（注） どの組織レベルでもポリシーを追加できます。

ステップ 3 [Add Logging Policy] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	ロギング ポリシー名。 この名前には、ID となる 1 ～ 32 文字を使用できます。 ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。 作成後は、この名前を変更できません。
Description	ポリシーの簡単な説明。

フィールド	説明
Log Level	次のいずれかのロギング重大度レベル： • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical デフォルトのレベルは info です。
Backup Files Count	書き込みに使用されるバックアップ ファイルの数。この数を超えると上書きされます。 範囲は 1 ～ 9 ファイルで、デフォルトは 2 ファイルです。
File Size（bytes）	バックアップ ファイルのサイズ。 範囲は 1 ～ 100 MB で、デフォルトは 5 MB です。

デバイス プロファイルのロギング ポリシーの編集

（注） システムの起動時、すでにデフォルト ポリシーが存在します。 デフォルト ポリシーは削除できませんが、変更できます。

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Log File] を選択します。

ステップ 2 [General] タブで、編集するログ ファイル ポリシーをクリックし、[Edit] をクリックします。

ステップ 3 [Edit Log File Policy] ダイアログボックスで、必要に応じて次のテーブルの情報を使用してフィールドを編集し、[OK] をクリックします。

フィールド	説明
Name	ロギング ポリシー名（読み取り専用）。
Description	ポリシーの簡単な説明。
Log Level	次のいずれかのロギング レベル： • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical デフォルトのレベルは info です。
Backup Files Count	書き込みに使用されるバックアップ ファイルの数。この数を超えると上書きされます。 範囲は 1 ～ 9 ファイルで、デフォルトは 2 ファイルです。
File Size（bytes）	バックアップ ファイルのサイズ。 範囲は 1 ～ 100 MB で、デフォルトは 5 MB です。

デバイス プロファイルのロギング ポリシーの削除

（注） システムの起動時、すでにデフォルト ポリシーが存在します。 デフォルト ポリシーは削除できませんが、変更できます。

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Log File] を選択します。

ステップ 2 [General] タブで、削除するロギング ポリシーをクリックし、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

SNMP のポリシーの設定

SNMP ポリシーの追加

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [SNMP] を選択します。
（注） どの組織レベルでもポリシーを追加できます。

ステップ 2 [General] タブで、[Add SNMP Policy] をクリックします。

ステップ 3 [Add SNMP] ダイアログボックスで、必要に応じて次のフィールドに値を入力します。

表 *12* : *[General]* タブ

フィールド	説明
Name	SNMP ポリシー名。 この名前には、ID となる 1 ～ 32 文字を使用できます。 ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。 作成後は、この名前を変更できません。
Description	SNMP ポリシーの説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。 ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。

フィールド	説明
Admin State	ポリシーの管理ステータスをイネーブルにするか、またはディセーブルにするかを指定します。
Location	デバイスの物理的な場所。
Contact	デバイスの担当者。
SNMP Port	SNMP エージェントが、要求がないかどうか監視するポート。 このフィールドは編集できません。

ステップ 4 [Communities] タブをクリックしてから、次の手順を実行します。

a) [Add SNMP Community] をクリックします。

b) [Add SNMP Community] ダイアログボックスで、必要に応じて次のフィールドに値を入力し、[OK] をクリックします。

名前	説明
Community	SNMP コミュニティ名。
Role	コミュニティ ストリングに関連付けられるロール。 このフィールドは編集できません。

ステップ 5 [Add SNMP] ダイアログボックスで、[OK] をクリックします。

SNMP ポリシーの編集

（注） システムの起動時、すでにデフォルト ポリシーが存在します。 デフォルト ポリシーは削除できませんが、変更できます。

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [SNMP] を選択します。

ステップ 2 [General] タブで、編集する SNMP ポリシーをクリックし、[Edit] をクリックします。

ステップ 3 [Edit SNMP Policy] ダイアログボックスで、必要に応じて次のテーブルの情報を使用して [General] タブの情報を編集します。

フィールド	説明
Name	SNMP ポリシー名（読み取り専用）。
Description	ポリシーの簡単な説明。
Admin State	ポリシーの管理状態：イネーブル（デフォルト）またはディセーブル。
Location	デバイスの物理的な場所。
Contact	デバイスの担当者。
SNMP Port	SNMP エージェントが要求を受信するポート（読み取り専用）。

ステップ 4 [Communities] タブで、必要に応じて情報を編集します。

フィールド	説明
Add SNMP Community	クリックして、SNMP コミュニティを追加します。
Community	SNMP コミュニティ名。
Role	SNMP コミュニティに関連付けられるロール。

ステップ 5 [Traps] タブで、必要に応じて情報を編集します。

フィールド	説明
Add SNMP Trap	クリックして、SNMP トラップを追加します。
Hostname	SNMP ホストの IP アドレス。
Port	SNMP エージェントが、要求がないかどうか監視するポート。

フィールド	説明
Community	SNMP コミュニティ名。

ステップ 6 [OK] をクリックします。

SNMP ポリシーの削除

（注） システムの起動時、すでにデフォルト ポリシーが存在します。 デフォルト ポリシーは削除できませんが、変更できます。

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [SNMP] を選択します。

ステップ 2 [General] タブで、削除する SNMP ポリシーをクリックし、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

SNMP トラップ レシーバの追加

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [SNMP] を選択します。

ステップ 2 [General] タブで、[Add SNMP Policy] をクリックします。

ステップ 3 [Add SNMP Policy] ダイアログボックスで、[Traps] タブをクリックします。

ステップ 4 [Traps] タブで、[Add SNMP Trap] をクリックします。

ステップ 5 [Add SNMP Trap] ダイアログボックスで、次の情報を入力し、[OK] をクリックします。

フィールド	説明
Hostname/ IP Address	SNMP ホストのホスト名または IP アドレス。
Port	SNMP エージェントが、要求がないかどうか監視するポート。 デフォルト ポートは 162 です。

フィールド	説明
Community	SNMP コミュニティ名。

SNMP トラップ レシーバの編集

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [SNMP] を選択します。

ステップ 2 [General] タブで、編集する SNMP トラップを持つ SNMP ポリシーをクリックし、[Edit] をクリックします。

ステップ 3 [Edit SNMP Policy] ダイアログボックスで、[Traps] タブをクリックします。

ステップ 4 [Traps] タブで、編集するエントリを選択し、[Edit] をクリックします。

ステップ 5 [Edit SNMP Trap] ダイアログボックスで、必要に応じて次の情報を使用して [General] タブの情報を編集します。

フィールド	説明
Hostname/IP Address	SNMP ホストのホスト名または IP アドレス（読み取り専用）。
Port	SNMP エージェントが、要求がないかどうか監視するポート。
Community	SNMP コミュニティ名。

ステップ 6 開いているダイアログボックスで [OK] をクリックします。

SNMP トラップ レシーバの削除

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [SNMP] を選択します。

ステップ 2 [General] タブで、削除する SNMP トラップを持つ SNMP ポリシーをクリックし、[Edit] をクリックします。

ステップ 3 [Edit SNMP Policy] ダイアログボックスで、[Traps] タブをクリックします。

ステップ 4 [Traps] タブで、削除するエントリを選択し、[Delete] をクリックします。

ステップ 5 確認の画面が表示されたら、削除を確認します。

Syslog ポリシーの設定

デバイスの Syslog ポリシーの追加

VNMC を使用すると、Syslog メッセージの Syslog ポリシーを設定し、そのプロファイルを使用するすべてのデバイスに実装するためのデバイス プロファイルに作成した Syslog ポリシーを付加することができます。

後から確認するために、リモート Syslog サーバまたはローカル バッファに Syslog メッセージのロギング用の Syslog ポリシーを作成できます。

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Syslog] を選択します。

ステップ 2 [General] タブで、[Add Syslog Policy] をクリックします。

ステップ 3 [Add Syslog] ダイアログボックスで、[Add Syslog Policy] ダイアログボックス，（183 ページ）で説明されている情報を入力し、[OK] をクリックします。

フィールドの説明

[Add Syslog Policy] ダイアログボックス

フィールド	説明
[General] タブ	
Name	ポリシー名。

フィールド	説明
Description	ポリシーの簡単な説明。
Use Emblem Format	このチェックボックスをオンにして、syslogメッセージで Emblem フォーマットを使用します。 このオプションは ASA 1000V でサポートされています。 VSG ではサポートされていません。
Continue if Host is Down	このチェックボックスをオンにして、syslogサーバがダウンした場合でもロギングを続行します。 このオプションは ASA 1000V でサポートされています。 VSG ではサポートされていません。
[Servers] タブ	
Add Syslog Server	新規 syslog サーバを追加する場合にクリックします。
[Syslog Servers] テーブル	設定されている syslog サーバのリスト。
[Local Destinations] タブ	
[Console] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[alert]、[critical]、または [emergency]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。

フィールド	説明
[Monitor] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[emergency]、[alert]、[critical]、[error]、[warning]、[notification]、[information]、または [debugging]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。
[File] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[emergency]、[alert]、[critical]、[error]、[warning]、[notification]、[information]、または [debugging]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。 • [File Name]：メッセージが記録されるファイルの名前。 • [Size (bytes)]：システムがメッセージの上書きを開始する最大ファイル サイズ（バイト数）。

フィールド	説明
[Buffer] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[emergency]、[alert]、[critical]、[error]、[warning]、[notification]、[information]、または [debugging]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。 • [Buffer Size (Bytes)]：syslog メッセージのバッファのサイズ（バイト数）。 • [Wrap to Flash]：バッファが消去される（一杯になった）場合に、バッファの内容をフラッシュ メモリに保存するかどうかを指定します。 このチェックボックスをオンにすると、バッファが消去される場合に、内容をフラッシュ メモリに保存します。 • [Max File Size in Flash (KB)]：syslog バッファが使用できる最大サイズ（KB 単位）。 [Wrap to Flash] オプションがイネーブルの場合のみ、このオプションはイネーブルになります。 • [Min Free Flash Size (KB)]：syslog バッファに割り当てられる最小サイズ（KB 単位）。 [Wrap to Flash] オプションがイネーブルの場合のみ、このオプションはイネーブルになります。

デバイス プロファイルの Syslog ポリシーの編集

この手順で説明するように、VNMC を使用すると、既存の Syslog ポリシーを編集できます。

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Syslog] を選択します。

ステップ 2 [General] タブで、編集するポリシーを選択し、[Edit] をクリックします。

ステップ 3 [Edit Syslog Policy] ダイアログボックスの [General] タブで、必要に応じて次の情報を使用して情報を編集します。

フィールド	説明
Name	ポリシー名（読み取り専用）。
Description	ポリシーの簡単な説明。
Use Emblem Format	このチェックボックスをオンにして、syslog メッセージで Emblem フォーマットを使用します。 このオプションは ASA 1000V でサポートされています。 VSG ではサポートされていません。
Continue if Host is Down	このチェックボックスをオンにして、syslog サーバがダウンした場合でもロギングを続行します。 このオプションは ASA 1000V でサポートされています。 VSG ではサポートされていません。

ステップ 4 [Servers] タブで、[Add Syslog Server] をクリックして新しい Syslog サーバを追加するか、既存のサーバを選択して [Edit] をクリックし、既存のサーバを編集します。

ステップ 5 [Local Destinations] タブで、次の情報を使用して、必要に応じて情報を編集します。

フィールド	説明
[Console] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[alert]、[critical]、または [emergency]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。

フィールド	説明
[Monitor] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[alert]、[critical]、[emergency]、[error]、[warning]、[notification]、[information]、または [debugging]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。
[File] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[alert]、[critical]、[emergency]、[error]、[warning]、[notification]、[information]、または [debugging]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。 • [File Name]：メッセージが記録されるファイルの名前。 • [Size (bytes)]：システムがメッセージの上書きを開始する最大ファイル サイズ（バイト数）。

フィールド	説明
[Buffer] 領域	• [Admin State]：ポリシーの管理状態：イネーブルまたはディセーブル。 • [Level]：メッセージ レベル：[alert]、[critical]、[emergency]、[error]、[warning]、[notification]、[information]、または [debugging]。 [Admin State] がイネーブルになっている場合は、表示するメッセージの最も低いレベルを選択します。 コンソールにはそのレベル以上のメッセージが表示されます。 • [Buffer Size (Bytes)]：syslog メッセージのバッファのサイズ（バイト数）。 • [Wrap to Flash]：バッファが消去される（一杯になった）場合に、バッファの内容をフラッシュ メモリに保存するかどうかを指定します。 このチェックボックスをオンにすると、バッファが消去される場合に、内容をフラッシュ メモリに保存します。 • [Max File Size in Flash (KB)]：syslog バッファが使用できる最大サイズ（KB 単位）。 このオプションは、[Wrap to Flash] オプションがイネーブルの場合のみイネーブルになります。 • [Min Free Flash Size (KB)]：syslog バッファに割り当てられる最小サイズ（KB 単位）。 このオプションは、[Wrap to Flash] オプションがイネーブルの場合のみイネーブルになります。

ステップ 6 [OK] をクリックします。

デバイス プロファイルの Syslog ポリシーの削除

（注） システムの起動時、すでにデフォルト ポリシーが存在します。 デフォルト ポリシーは削除できませんが、変更できます。

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Syslog] を選択します。

ステップ 2 [General] タブで、削除する syslog ポリシーを選択し、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

デバイス プロファイルの Syslog サーバの追加

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Syslog] を選択します。

ステップ 2 [General] タブで、[Add Syslog Policy] をクリックします。

ステップ 3 [Add Syslog Policy] ダイアログボックスで、[Servers] タブをクリックし、[Add Syslog Server] をクリックします。

ステップ 4 [Add Syslog Server] ダイアログボックスで、[Add Syslog Server] ダイアログボックス, （190 ページ）で説明されている情報を入力し、[OK] をクリックします。

フィールドの説明

[Add Syslog Server] ダイアログボックス

フィールド	説明
Server Type	次のいずれかのサーバ タイプ： • primary • secondary • tertiary
Hostname/IP Address	syslog ファイルが置かれている場所のホスト名または IP アドレス。

フィールド	説明
Severity	次のいずれかの重大度レベル： • emergencies（0） • alerts（1） • critical（2） • errors（3） • warnings（4） • notifications（5） • information（6） • debugging（7）
Forwarding Facility	次のいずれかの転送するファシリティ： • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp

フィールド	説明
Admin State	ポリシーの管理状態：イネーブルまたはディセーブル。
Port	syslog サーバへのデータの送信に使用するポート。 ポートの有効な値は、TCP と UDP のいずれでも 1025 ～ 65535 です。 デフォルトの TCP ポートは 1470 です。 デフォルトの UDP ポートは 514 です。
Protocol	このポリシーに使用するプロトコル：TCP または UDP。
Use Transport Layer Security	このチェックボックスをオンにして、トランスポート層セキュリティを使用します。 このオプションは、TCP の場合にのみ使用できます。
Server Interface	syslog サーバにアクセスするために使用するインターフェイス。

デバイス プロファイルの Syslog サーバの編集

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Syslog] を選択します。

ステップ 2 [General] タブで、必要な Syslog ポリシーを選択し、[Edit] をクリックします。

ステップ 3 [Edit Syslog Policy] ダイアログボックスで、[Servers] タブをクリックします。

ステップ 4 [Servers] タブで、編集する Syslog サーバをクリックし、[Edit] をクリックします。

ステップ 5 [Edit Syslog Server] ダイアログボックスで、必要に応じて次のテーブルの情報を使用してフィールドを編集します。

フィールド	説明
Server Type	次のいずれかのサーバ タイプ：primary、secondary、または tertiary（読み取り専用）。
Hostname/IP Address	syslog ファイルが置かれている場所のホスト名または IP アドレス。

フィールド	説明
Severity	次のいずれかの重大度レベル： • emergencies（0） • alerts（1） • critical（2） • errors（3） • warnings（4） • notifications（5） • information（6） • debugging（7）
Forwarding Facility	次のいずれかの転送するファシリティ： • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp

フィールド	説明
Admin State	ポリシーの管理状態：イネーブルまたはディセーブル。
Port	syslog サーバへのデータの送信に使用するポート。 ポートの有効な値は、TCP と UDP のいずれでも 1025 ～ 65535 です。 デフォルトの TCP ポートは 1470 です。 デフォルトの UDP ポートは 514 です。
Protocol	使用するプロトコル：TCP または UDP。
Use Transport Layer Security	このチェックボックスをオンにして、トランスポート層セキュリティを使用します。 このオプションは、TCP の場合にのみ使用できます。
Server Interface	syslog サーバにアクセスするために使用するインターフェイス。 このオプションは、ASA 1000V にのみ適用されます。 エッジ ファイアウォールで指定されているデータ インターフェイス名を入力します。 デバイス CLI を使用して、管理インターフェイス経由でのルートを設定します。

ステップ 6 開いているダイアログボックスの [OK] ボタンをクリックして、変更内容を保存します。

デバイス プロファイルの Syslog サーバの削除

手順

ステップ 1 [Navigation] ペインの [Policy Management] タブをクリックします。
ステップ 2 [Navigation] ペインの [Device Configurations] サブタブをクリックします。
ステップ 3 [Policy Management] > [Device Configurations] > [root] > [Policies] > [Syslog] を選択します。
ステップ 4 [General] タブで、削除するサーバと Syslog ポリシーをクリックし、[Edit] をクリックします。
ステップ 5 [Edit Syslog Policy] ダイアログボックスで、[Servers] タブをクリックします。
ステップ 6 [Servers] タブで、削除する Syslog サーバをクリックし、[Delete] をクリックします。
ステップ 7 確認の画面が表示されたら、削除を確認します。
ステップ 8 [OK] をクリックしてポリシーを保存します。

デバイス プロファイルの設定

ファイアウォール デバイス プロファイルの追加

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Device Profiles] を選択します。
ステップ 2 [General] タブで、[Add Device Profile] をクリックします。
ステップ 3 [New Device Profile] ダイアログボックスの [General] タブで次の情報を入力します。

フィールド	説明
Name	プロファイル名。 この名前には、ID となる 1 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。作成後は、この名前を変更できません。
Description	プロファイルの簡単な説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。

フィールド	説明
Time Zone	ドロップダウン リストから必要な時間帯を選択します。

ステップ 4 [Policies] タブで次の情報を入力します。

フィールド	説明
DNS Servers	
Add DNS Server	クリックすると、DNS サーバを追加します。
Delete	クリックすると、[IP Address] テーブルで選択された DNS サーバの IP アドレスを削除します。
Up and down arrows	選択した DNS サーバの IP アドレスの優先度を変更します。
[IP Address] テーブル	システムで設定されている DNS サーバの IP アドレス。 VNMC は、テーブルに表示される順序で DNS サーバを使用します。
NTP Servers	
Add NTP Server	クリックすると、NTP サーバを追加します。
Delete	クリックすると、[Hostname] テーブルで選択された NTP サーバ ホスト名を削除します。
Up and down arrows	選択した NTP サーバ ホスト名の優先度を変更します。
[IP Address] テーブル	システムで設定されている NTP サーバ ホスト名が含まれています。 VNMC は、テーブルに表示されている順序で NTP サーバ ホスト名を使用します。
DNS Domains	
Add	クリックすると、DNS ドメイン名を追加します。

フィールド	説明
Edit	クリックすると、[DNS Domains] テーブルで選択された DNS ドメイン名を編集します。 デフォルトの DNS 名は編集できません。
Delete	クリックすると、[DNS Domains] テーブルで選択された DNS ドメイン名を削除します。
[DNS Domains] テーブル	システムのデフォルトの DNS ドメイン名およびドメイン。
Other Options	
SNMP	このプロファイルに関連付けられた SNMP ポリシーを選択、追加、または編集できます。 指定したポリシーを確認または変更するには、[Resolved Policy] フィールドをクリックします。
Syslog	このプロファイルに関連付けられた syslog ポリシーを選択、追加、または編集できます。 指定したポリシーを確認または変更するには、[Resolved Policy] フィールドをクリックします。
Fault	このプロファイルに関連付けられた障害ポリシーを選択、追加、または編集できます。 指定したポリシーを確認または変更するには、[Resolved Policy] フィールドをクリックします。
Core File	このプロファイルに関連付けられたコア ファイル ポリシーを選択、追加、または編集できます。 指定したポリシーを確認または変更するには、[Resolved Policy] フィールドをクリックします。
Policy Agent Log File	このプロファイルに関連付けられたポリシー エージェント ログ ファイル ポリシーを選択、追加、または編集できます。 指定したポリシーを確認または変更するには、[Resolved Policy] フィールドをクリックします。
Policy Engine Logging	ロギングを有効または無効にするには、適切なオプション ボタンを選択します。

フィールド	説明
Auth Policy	利用可能な認証ポリシーを選択するか、[Add Auth Policy] をクリックし、新しい認証ポリシーを追加します。

ステップ 5 [OK] をクリックします。

ファイアウォール デバイス プロファイルの編集

ファイアウォールデバイスプロファイルを作成したら、必要に応じてそれを編集することができます。

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Device Profiles] を選択します。

ステップ 2 [Device Profiles] タブで、編集するプロファイルをクリックし、[Edit] をクリックします。

ステップ 3 [Edit Firewall Device Policy] ダイアログボックスで、次のテーブルで説明されているように、[General] タブの情報を更新します。

フィールド	説明
Name	プロファイル名。 この名前には、ID となる 1 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。作成後は、この名前を変更できません。
Description	プロファイルの簡単な説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。
Time Zone	ドロップダウンリストから必要な時間帯を選択します。

ステップ 4 [Policies] タブで、次のテーブルで説明されている情報を更新します。

フィールド	説明
DNS Servers	
Add DNS Server	クリックすると、DNS サーバを追加します。
Delete	クリックすると、[IP Address] テーブルで選択された DNS サーバの IP アドレスを削除します。
Up and down arrows	選択した NTP サーバ ホスト名の優先度を変更します。
[IP Address] テーブル	システムで設定されている DNS サーバの IP アドレス。 VNMC は、テーブルに表示される順序で DNS サーバを使用します。
NTP Servers	
Add NTP Server	クリックすると、NTP サーバを追加します。
Delete	クリックすると、[Hostname] テーブルで選択された NTP サーバ ホスト名を削除します。
Up and down arrows	選択した NTP サーバ ホスト名の優先度を変更します。
[IP Address] テーブル	システムで設定されている NTP サーバ ホスト名が含まれています。 VNMC は、テーブルに表示されている順序で NTP サーバ ホスト名を使用します。
DNS Domains	
Add	クリックすると、DNS ドメイン名を追加します。
Edit	クリックすると、[DNS Domains] テーブルで選択された DNS ドメイン名を編集します。 デフォルトの DNS 名は編集できません。
Delete	クリックすると、[DNS Domains] テーブルで選択された DNS ドメイン名を削除します。

フィールド	説明
[DNS Domains] テーブル	システムのデフォルトの DNS ドメイン名およびドメイン。
Other Options	
SNMP	必要に応じて、SNMP ポリシーを選択、追加、または編集します。
Syslog	必要に応じて、Syslog ポリシーを選択、追加、または編集します。
Fault	必要に応じて、障害ポリシーを選択、追加、または編集します。
Core File	必要に応じて、コア ファイル ポリシーを選択、追加、または編集します。
Policy Agent Log File	必要に応じて、ポリシー エージェント ログ ファイルを選択、追加、または編集します。
Policy Engine Logging	ロギングを有効または無効にするには、適切なオプション ボタンを選択します。
Auth Policy	利用可能な認証ポリシーを選択するか、[Add Auth Policy] をクリックし、新しい認証ポリシーを追加します。

ステップ 5 [OK] をクリックします。

ファイアウォール デバイス プロファイルの削除

手順

ステップ 1 [Navigation] ペインの [Policy Management] タブをクリックします。

ステップ 2 [Navigation] ペインの [Device Configurations] サブタブをクリックします。

ステップ 3 [Navigation] ペインで、[root] > [Device Profiles] を展開します。

ステップ 4 [Navigation] ペインで、[Device Profiles] ノードをクリックします。

ステップ 5 [Work] ペインで、削除するデバイス プロファイルをクリックします。

ステップ 6 [Delete] をクリックします。

ステップ 7 [Confirm] ダイアログボックスで、[OK] をクリックします。

NTP の設定

ネットワーク タイム プロトコル（NTP）は、マシンのネットワーク上で時間を同期させる場合に使用する、ネットワーキング プロトコルです。 NTP ネットワークは通常、タイム サーバに接続されたラジオ クロックやアトミック クロックなど、正規の時刻源から時刻を取得します。

VNMC では、コンピュート ファイアウォール、エッジ ファイアウォール、および VNMC 自体の NTP を設定できます。

コンピュート ファイアウォールまたはエッジ ファイアウォールの NTP を設定する場合は、次の手順に従う必要があります。

1. NTP によるデバイス プロファイルの設定
2. コンピュート ファイアウォールまたはエッジ ファイアウォールへのデバイス プロファイルの適用

ここでは、このような手順の実行方法について説明します。

VNMC で NTP を設定する方法の詳細については、NTP サーバの追加, （70 ページ）を参照してください。

NTP を使用したデバイス プロファイルの作成

この手順では、エッジまたはコンピュート ファイアウォールに適用できる、NTP を使用したデバイス プロファイルを作成する方法について説明します。

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Device Profiles] を選択します。

ステップ 2 [General] タブで、[Add Device Profile] をクリックします。

ステップ 3 [New Device Profile] ダイアログボックスで、次の情報を指定します。

- [Name]：プロファイル名。
- [Description]：プロファイルの簡単な説明。
- [Time Zone]：ドロップダウン リストから、タイム ゾーンを選択します。

ステップ 4 [Policies] タブをクリックします。

ステップ 5 [NTP servers] 領域で、[Add NTP Server] リンクをクリックします。

ステップ 6 [Add NTP Server] ダイアログボックスで、[Add NTP Server] ダイアログボックス, （202 ページ）で説明されている情報を入力し、[OK] をクリックします。

ステップ 7 [OK] をクリックします。

次の作業

デバイス プロファイルを設定したら、次のトピックで説明するようにファイアウォールにプロファイルを適用することができます。

- エッジ ファイアウォールへのデバイス プロファイルの適用, （204 ページ）
- コンピュート ファイアウォールへのデバイス プロファイルの追加, （203 ページ）

フィールドの説明

[Add NTP Server] ダイアログボックス

フィールド	説明
Hostname/IP Address	NTP サーバ名または IP アドレス。 VNMC および VSG の場合は、ホスト名、または IP アドレスを入力できます。 ASA 1000V の場合は、IP アドレスを入力する必要があります。

フィールド	説明

Interface Name	NTP サーバに到達するためのデバイスインターフェイス。
	次の情報が適用されます。
	• ASA 1000V のみがインターフェイス名をサポートしています。
	  • インターフェイスを指定する場合は、エッジ ファイアウォールで規定されたインターフェイス名を使用してください。
	  • 管理インターフェイスを使用するには、CLI を使用してルートを設定する必要があります。
	• VSG はインターフェイス名をサポートしません。
	• このフィールドは、VNMC NTP サーバ設定では表示されません。

Authentication Key	NTP サーバにアクセスする認証キー。 次の情報が適用されます。 • ASA 1000V のみが認証キーをサポートします。 • VSG では認証キーをサポートしていません。 • このフィールドは、VNMC NTP サーバ設定では表示されません。

コンピュート ファイアウォールへのデバイス プロファイルの追加

デバイスプロファイルを作成したら、コンピュートファイアウォールにプロファイルを適用することができます。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Compute Firewalls] > [*compute-firewall*] を選択します。

ステップ 2 [General] タブで、[Device Profile] フィールドの [Select] をクリックします。

ステップ 3 [Select Device Profile] ダイアログボックスで、目的のプロファイルを選択し、[OK] をクリックします。

ステップ 4 [Save] をクリックします。

エッジ ファイアウォールへのデバイス プロファイルの適用

デバイスプロファイルを作成したら、エッジファイアウォールにプロファイルを適用することができます。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Edge Firewalls] > [*edge-firewall*] を選択します。

ステップ 2 [General] タブで、[Device Profile] フィールドの [Select] をクリックします。

ステップ 3 [Select Device Profile] ダイアログボックスで、目的のプロファイルを選択し、[OK] をクリックします。

ステップ 4 [Save] をクリックします。

デバイス ポリシーとプロファイルの関連付け

デバイス ポリシーを作成したら、それをデバイス プロファイルに関連付けることができます。そうすることによって、デバイス プロファイルに関連付けられたすべてのデバイスが同じポリシーを使用するようにできます。

手順

ステップ 1 [Policy Management] > [Device Configurations] > [root] > [Device Profiles] > [*profile*] を選択します。この [*profile*] は、デバイス ポリシーを追加するデバイス プロファイルです。

ステップ 2 [Policies] タブをクリックします。

ステップ 3 [Policies] タブで、[Syslog] または [Auth Policy] など、関連付けたいポリシーの種類のドロップダウン リストを探します。

ステップ 4 ドロップダウン リストから、プロファイルに追加するポリシーを選択し、[Save] をクリックします。
ポリシーが選択されたプロファイルを使用して自動的にすべてのデバイスに適用されます。

第 11 章

管理対象リソースの設定

この項では、次のトピックについて取り上げます。

Resource Management

[Resource Management] タブには、VNMC よって管理される次のリソースが表示されます。

- 仮想マシン（VM）
- ASA 1000V エッジ ファイアウォール
- VSG コンピュート ファイアウォール
- Virtual Supervisor Module（Nexus 1000V VSM）

ASA 1000V および VSG を管理するには、それらを稼働させます。

- ASA 1000V を使用するには、組織内にエッジ ファイアウォールを作成し、ASA 1000V をそのエッジ ファイアウォールに割り当てます。
- VSG を使用するには、組織内にコンピュート ファイアウォールを作成し、VSG をそのコンピュート ファイアウォールに割り当てます。

VM を管理するには、Nexus 1000V ポート プロファイルに設定されている少なくとも 1 つのネットワーク インターフェイスを持つ VM を検出します。

Resource Manager

Resource Manager は、論理的なエッジ ファイアウォールとコンピュート ファイアウォール、また、それぞれ、それらの ASA 1000V および VSG との関連付けを管理します。 エッジ ファイアウォールが ASA 1000V に関連付けられている場合、（エッジ ファイアウォールにより定義された）デバイス設定プロファイル情報は ASA 1000V にプッシュされます。今度はこれにより ASA 1000V が起動され、Policy Manager からセキュリティ プロファイルおよびポリシーをダウンロードします。

Resource Manager は、次のサービスを実施します。

- ASA 1000V、VSG、および VSM のインベントリの維持。
- ユーザ入力による、コンピュートファイアウォールの定義とプロビジョニングに向けた VSG との関連付け
- ユーザ入力による、エッジファイアウォールの定義とプロビジョニングに向けた ASA 1000V との関連付け
- VM 属性を取得するための VMware vCenter インスタンスとの統合

仮想マシン

仮想化により、同じ物理マシン上で隣どうしで独立して動作する複数の VM を作成できます。 各 VM には仮想 RAM、仮想 CPU と NIC、およびオペレーティング システムとアプリケーションがあります。 仮想化により、オペレーティング システムは、実際の物理ハードウェア コンポーネントに関係なく、一貫性のあるハードウェア一式を認識します。

VM は、保存、コピー、プロビジョニングを高速化するためにファイルにカプセル化されます。 つまり、システム全体、設定済みアプリケーション、オペレーティング システム、BIOS、仮想ハードウェアを数秒で 1 つの物理サーバから別のサーバに移動できます。 カプセル化されたファイルでは、ダウンタイムを生じさせることなくメンテナンスを行い、作業負荷をとぎれることなく統合できます。

Cisco VNMC のインスタンスは VM にインストールされます。

Virtual Security Gateway

VSG は、ネットワーク トラフィックに基づいて VNMC ポリシーを評価します。 VSG の主な機能は次のとおりです。

- 仮想ネットワーク サービス データ パス（vPath）からトラフィックを受け取ります。

  すべての新規フローについて、vPath コンポーネントは最初のパケットをカプセル化し、Nexus 1000V ポート プロファイルの指定に従って VSG に送信します。 VSG は、vPath のレイヤ 2 隣接であると想定します。 vPath と VSG 間の通信に使用されるメカニズムは、パケット VLAN 上の VEM と Nexus 1000V VSM の通信に似ています。

- FTP、TFTP、RSH などのアプリケーション フィックスアップ処理を実行します。
- ネットワーク、VM、カスタム属性を使用して、vPath によって送信されたパケットを検査して、ポリシーを評価します。
- ポリシー評価結果を vPath に転送します。

各 vPath コンポーネントは、VSG ポリシー評価結果をキャッシュに入れるためのフロー テーブルを維持します。

ASA 1000V Cloud Firewall

Cisco Adaptive Security Appliance 1000V Cloud Firewall（ASA 1000V）は、Cisco Nexus 1000V 展開を使用したマルチテナント環境でテナントエッジのセキュリティを確保するために、ASA インフラストラクチャを使用して開発された仮想アプライアンスです。 ASA 1000V ファイアウォールは、次のエッジ機能を提供します。

- サイト間 VPN、NAT、および DHCP をサポートします。
- デフォルト ゲートウェイの役割を果たします。
- ネットワークを利用したあらゆる攻撃に対して、テナント内の VM のセキュリティを確保します。

VNMC では、エッジ ファイアウォール オブジェクトは ASA 1000V インスタンスに関連付けられています。 関連付けられたら、ASA 1000V デバイス タイプの該当するすべてのプロファイル タイプは ASA 1000V インスタンスにプッシュされます。 エッジ ファイアウォール オブジェクトと同じ組織レベルで作成されたすべてのエッジプロファイルオブジェクトは、そのデバイスにプッシュされます。

コンピュート ファイアウォールの管理

VNMC では、コンピュート ファイアウォールを追加、編集、削除できます。 また、VSG をコンピュート ファイアウォールに割り当てることができ、それによって VSG を稼働させます。 ここでは、これらのアクティビティについてさらに詳しく説明します。

コンピュート ファイアウォールの追加

この手順では、VNMC にコンピュート ファイアウォールを追加して、それを VSG に追加して VSG を動作状態にする方法について説明します。

新しいコンピュート ファイアウォールを追加する場合、ファイアウォールがさまざまな組織パスを持っている限り、ファイアウォール データの IP アドレスは VNMC 内の既存のコンピュート・ファイアウォールのデータ IP アドレスと同じにすることができます。 つまり、ファイアウォールが、親と子の組織を含む同じ組織内に存在していない限り、上記のことが言えます。

（注） コンピュート ファイアウォールは、ルート レベルではなく、テナント レベル以下に追加することを推奨します。

手順

ステップ 1 [Resource Management] タブで、[Managed Resources] > [root] > [*tenant*] > [Compute Firewalls] を選択します。

ステップ 2 [General] タブで、[Add Compute Firewall] をクリックします。

ステップ 3 [Add Compute Firewall] ダイアログボックスで、次のテーブルで説明されている必須情報を入力し、[OK] をクリックします。

フィールド	説明
Name	オブジェクト名。 この名前には、ID となる 1 ～ 32 文字を使用できます。 ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。 作成後は、この名前を変更できません。
Description	オブジェクトの簡単な説明。
[Firewall Settings] 領域	
Device Profile	デバイスプロファイルをファイアウォールに適用するには、次の手順を実行します。 **1** [Select] をクリックします。 **2** [Select Device Profile] ダイアログボックスで、必要なプロファイルを選択し、[OK] をクリックします。
Management Hostname	ファイアウォールの管理ホスト名。

フィールド	説明
Data IP Address	データ IP アドレス。 各 VEM で動作する vPath コンポーネントは、データ IP アドレスを使用して、VSG の MAC アドレスを特定します（ARP 経由）。 VSG MAC アドレスが解決されると、vPath は MAC カプセル化の MAC を使用して VSG と通信できます。 その後、VM によって新しいフローが始まるたびに、vPath はフローの最初のパケットをポリシー評価のために VSG に送信します。 vPath は、VSG ポリシーの決定をフロー テーブルのキャッシュに入れます。 これは、Nexus 1000V ポート プロファイルの **vservice** CLI コマンドで設定された IP アドレスと同じです。
Data IP Subnet	データ IP サブネット。

コンピュート ファイアウォールの編集

必要に応じて、既存のコンピュート ファイアウォールを編集することができます。

手順

ステップ 1 [Resource Management] タブで、[Managed Resources] > [root] > [*tenant*] > [Compute Firewalls] を選択します。ここで [*tenant*] は必須のテナントです。

ステップ 2 [General] タブで、編集するコンピュート ファイアウォールをクリックし、[Edit] をクリックします。

ステップ 3 [Edit] ダイアログボックスで、必要に応じて次のフィールドを変更し、[OK] をクリックします。

[General] タブ

フィールド	説明
Name	コンピュートファイアウォール名（読み取り専用）。
Description	ファイアウォールの簡単な説明。

フィールド	説明
Pool Name	コンピュートファイアウォールに割り当てられているプール（存在する場合）。 一度にコンピュート ファイアウォールに割り当てられるプールは 1 つだけです。 プールを変更する場合は、[Assign Pool] をクリックします。
States	
Config State	次のいずれかのコンピュートファイアウォール設定状態：[not-applied]、[applying]、[failed-to-apply]、または [applied]。
Association State	次のいずれかのコンピュートファイアウォール設定状態：[unassociated]、[associating]、[associated]、[disassociating]、または [failed]。
Faults Associated with Firewall	ファイアウォールに関連付けられている障害を表示します。 この情報は、コンピュートファイアウォールが VSG に関連付けられている場合のみ使用可能です。
View Device Faults	デバイスに関連付けられている障害を表示します。 この情報は、コンピュートファイアウォールが VSG に関連付けられている場合のみ使用可能です。
Firewall Settings	
Device Profile	ファイアウォールに関連付けられているデバイス プロファイル。 デバイス プロファイルを変更する場合は、[Select] をクリックし、目的のプロファイルを選択します。
Management Hostname	コンピュート ファイアウォールの管理ホスト名。

フィールド	説明
Data IP Address	コンピュート ファイアウォール データ IP アドレス。 各 VEM で動作する vPath コンポーネントは、データ IP アドレスを使用して、VSG の MAC アドレスを特定します（ARP 経由）。 VSG MAC アドレスが解決されると、vPath は MAC カプセル化の MAC を使用して VSG と通信できます。 その後、VM によって新しいフローが始まるたびに、vPath はフローの最初のパケットをポリシー評価のために VSG に送信します。 vPath は、VSG ポリシーの決定をフロー テーブルのキャッシュに入れます。 これは、Nexus 1000v ポート プロファイルの **vservice** CLI コマンドで設定された IP アドレスと同じです。
Data IP Subnet	ファイアウォール データ IP サブネット マスク。
VSG Details この情報は、コンピュート ファイアウォールが VSG に関連付けられている場合のみ使用可能です。	
Task	クリックすると、[Edit VSG] ダイアログボックスが開きます。
VSG Service ID	VSG の内部識別番号。
VSG Mgmt IP	VSG 管理 IP アドレス。
HA Role	VSG のハイ アベイラビリティ（HA）ロール：HA またはスタンドアロン モード。
Association	VSG の関連付けの状態：[unassociated]、[associating]、[associated]、[disassociating]、または [failed]。
Reachable	VSG に到達できるかどうか。

[Compute Security Profiles] タブ

フィールド	説明
Show Resolved Policies	クリックすると、コンピュートファイアウォールに適用されたセキュリティポリシーを表示したり、必要に応じてそれを変更したりすることができます。 このオプションは、選択されたプロファイルが対応する VSM ポート プロファイル内で設定されている場合のみ使用可能です。
Properties	コンピュートファイアウォールに関連付けられているポートプロファイルのプロパティを表示します。
Compute Security Profile	コンピュート ファイアウォール セキュリティ プロファイルの名前。
Port Profile	関連付けられているポート プロファイルの名前。
Org	組織の識別名（DN）。
VSG Data IP	VSG データ IP アドレス。
Config State	VSG の設定状態。

コンピュート ファイアウォールの削除

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Compute Firewalls] を選択します。

ステップ 2 [General] タブで、削除するコンピュート ファイアウォールをクリックし、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

VSG の割り当て

コンピュート ファイアウォールに VSG を割り当てると、VSG を動作させ、VNMC を使用してそれを管理することができます。 コンピュート ファイアウォールに VSG を割り当てる前に、次を実行する必要があります。

- VSG を VNMC に登録します。 VSG を VNMC に登録することの詳細については、『*Cisco Virtual Security Gateway, Release 4.2(1)VSG1(4.1) and Cisco Virtual Network Management Center, Release 2.0 Installation and Upgrade Guide*』を参照してください。
- コンピュート ファイアウォールを VNMC に追加します。 詳細については、コンピュート ファイアウォールの追加, （210 ページ）を参照してください。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Compute Firewalls] を選択します。

ステップ 2 [General] タブで、VSG を割り当てるコンピュート ファイアウォールを選択し、[Assign VSG] をクリックします。

ステップ 3 [Assign VSG] ダイアログボックスで、目的の IP アドレスを [VSG Management IP] ドロップダウンリストから選択し、[OK] をクリックします。

VSG の割り当て解除

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Compute Firewalls] を選択します。

ステップ 2 [Compute Firewalls] テーブルで、割り当てを解除する VSG を持つファイアウォール選択します。

ステップ 3 [Unassign VSG/Pool] をクリックします。

ステップ 4 [Confirm] ダイアログボックスで、[Yes] をクリックします。

エッジ ファイアウォールの管理

エッジ ファイアウォールの管理では、ASA 1000V を稼働させるため、エッジ ファイアウォールの VNMC への追加、エッジ ファイアウォール データ インターフェイスの設定、ASA 1000V のエッジファイアウォールへの割り当てが必要です。 ここでは、これらのアクティビティについてさらに詳しく説明します。

エッジ ファイアウォールの追加

この手順では、VNMC にエッジ ファイアウォールを追加し、それを ASA 1000V インスタンスに割り当てて、ASA 1000V を動作状態にする方法について説明します。

新しいエッジ ファイアウォールを追加する場合、ファイアウォールがさまざまな組織パスを持っている限り、内部データ インターフェイスのプライマリ IP アドレスとして識別されたファイアウォール データの IP アドレスは、VNMC 内の既存のエッジ ファイアウォール用の内部データ インターフェイスの IP アドレスと同じにすることができます。 つまり、エッジ ファイアウォールが、親と子の組織を含む同じ組織内に存在していない限り、上記のことが言えます。

（注） エッジ ファイアウォールは、ルート レベルではなく、テナント レベル以下に追加することを推奨します。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Edge Firewalls] を選択します。

ステップ 2 [Add Edge Firewall] をクリックします。

ステップ 3 [Add Edge Firewall] ダイアログボックスで、[Add Edge Firewall] ダイアログボックス，（216 ページ）で説明されている情報を入力し、[OK] をクリックします。

次の作業

エッジ ファイアウォールを追加したら、ASA 1000V をそれに追加して、VNMC を使用して ASA 1000V を管理できるようにします。 詳細については、ASA 1000V の割り当て，（218 ページ）を参照してください。

[Add Edge Firewall] ダイアログボックス

フィールド	説明
Name	エッジ ファイアウォール名。
Description	エッジ ファイアウォールの簡単な説明。
HA Mode	エッジ ファイアウォールのハイ アベイラビリティ（HA）ロール：HA またはスタンドアロン。

フィールド	説明
Device Profile	デバイスプロファイルを適用するには、次の手順を実行します。 1 [Select] をクリックします。 2 [Select Device Profile] ダイアログボックスで、必要なプロファイルを選択し、[OK] をクリックします。
Edge Device Profile	エッジデバイスプロファイルを適用するには、次の手順を実行します。 1 [Select] をクリックします。 2 [Select Edge Device Profile] ダイアログボックスで、必要なプロファイルを選択し、[OK] をクリックします。

データ インターフェイスの追加

エッジのファイアウォールを追加する場合、データ通信用の内部インターフェイスと外部インターフェイスを指定する必要があります。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Edge Firewalls] を選択します。

ステップ 2 [Edge Firewalls] ペインで、データ インターフェイスを追加または変更するエッジ ファイアウォールを選択し、[Edit] をクリックします。

ステップ 3 [Edit Edge Firewall] ダイアログボックスで、[Add Data Interface] をクリックします。

ステップ 4 追加されたインターフェイスごとに、[Add Data Interface] ダイアログボックスで説明されているように情報を入力し、[OK] をクリックします。

[Add Data Interface] ダイアログボックス

フィールド	説明
Name	インターフェイス名。
Description	インターフェイスの簡単な説明。

フィールド	説明
Role	インターフェイスが内部通信用であるか、または外部通信用であるか。
DHCP	outside インターフェイスにのみ使用可能です。 インターフェイスで DHCP をイネーブルにするには、[Enable DHCP] チェックボックスをオンにします。
Primary IP Address	このインターフェイスの IP アドレス。
Secondary IP Address	エッジ ファイアウォールがハイ アベイラビリティ（HA）モードの場合に使用可能です。 このインターフェイスのセカンダリ IP アドレスです。
Subnet Mask	IP アドレスに適用するマスク。
Edge Security Profile	outside インターフェイスにのみ使用可能です。 エッジ セキュリティ プロファイルを適用するには、次の手順を実行します。 **1** [Select] をクリックします。 **2** [Select Edge Security Profile] ダイアログボックスで、必要なプロファイルを選択し、[OK] をクリックします。

ASA 1000V の割り当て

VNMC にエッジ ファイアウォールを追加したら、ASA 1000V インスタンスをそれに追加して ASA 1000V インスタンスが関連するポリシーおよびプロファイルで動作するようにする必要があります。 ASA 1000V をエッジ ファイアウォールに割り当てるには、次を実行する必要があります。

- ASA 1000V を VNMC に登録する。 詳細については、『*Cisco Virtual Network Management Center 2.0 Quick Start Guide*』を参照してください。
- エッジ ファイアウォールを VNMC に追加します。 詳細については、エッジ ファイアウォールの追加, （216 ページ）を参照してください。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Edge Firewalls] > [*edge-firewall*] を選択します。

ステップ 2 [Assign ASA 1000V] をクリックします。

ステップ 3 [Assign ASA 1000V] ダイアログボックスで、ドロップダウン リストから必要な ASA 1000V を選択し、[OK] をクリックします。

ASA 1000V の割り当て解除

必要に応じて、エッジ ファイアウォールから ASA 1000V の割り当てを解除できます。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Edge Firewalls] > [*edge-firewall*] を選択します。

ステップ 2 [Unassign ASA 1000V/Pool] をクリックします。

ステップ 3 確認ダイアログボックスで、[OK] をクリックします。

ASA 1000V、VSG、および VSM 登録の確認

VNMC を使用すると、ASA 1000V、VSG、および VSM が正常に登録されているか確認できます。

手順

ステップ 1 [Administration] > [Service Registry] > [Clients] を選択します。

ステップ 2 [Clients] テーブルで、[Oper State] カラムに ASA 1000V、VSG、および VSM エントリに対して [*registered*] が含まれているか確認します。

障害の詳細の調査

VNMC では、ポリシーを正常に適用できなくするようなポリシーおよび設定上のエラーを調査できます。 たとえば、ポリシーをエッジ ファイアウォールに適用し、[Config State] フィールドに

[Failed-to-Apply] という状態が表示される場合、問題を特定し解決するために、設定エラーを調査できます。

同じインターフェイスを使用して、次に示すタスクを実行できます。

- 適用されたポリシーおよび設定を使用して、エッジファイアウォールに関連付けられた障害およびイベントを調査する。
- コンピュート ファイアウォールに関連付けられた障害を調査する。

ここでは、これらの機能についてさらに詳しく説明します。

エッジ ファイアウォールの障害および設定エラーの調査

VNMCでは、エッジファイアウォール、およびそのポリシーと設定に関連する障害およびイベントを表示できます。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Edge Firewalls] > [*edge-firewall*] を選択します。

ステップ 2 [General] タブの [States] 領域で、設定、関連付け、および障害の情報を確認します。

ステップ 3 障害が示されている場合、障害の詳細を次のように表示します。

- [Faults] タブをクリックします。
- [Events] タブをクリックします。
- [Faults Associated with Firewall] をクリックします。
- [View Configuration Faults] をクリックします。

ステップ 4 詳細を表示するには、任意のテーブルのエントリをダブルクリックします。
新しいブラウザ ウィンドウの [Faults] テーブルでは、[Refresh Now] をクリックして最新情報を表示できます。

コンピュート ファイアウォールの障害の調査

VNMC を使用すると、コンピュート ファイアウォールの障害およびイベントを調査できます。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Compute Firewalls] > [*compute-firewall*] を選択します。

ステップ 2 [General] タブの [States] 領域で、設定、関連付け、および障害の情報を確認します。

ステップ 3 障害が示されている場合、障害の詳細を次のように表示します。

- [Faults] タブをクリックします。
- [Events] タブをクリックします。
- [Faults Associated with Firewall] をクリックします。
- [View Configuration Faults] をクリックします。

ステップ 4 詳細を表示するには、任意のテーブルのエントリをダブルクリックします。

VNMC からの ASDM の起動

VNMC を使用すると、Cisco Adaptive Security Device Manager（ASDM）をデスクトップ上で Web Start アプリケーションとして起動できます。

ASDM が VNMC 管理モードまたは ASDM 管理モードのいずれかに設定されている場合、ASA 1000V が ASDM を使用するように設定できます。 ASA 1000V が VNMC 管理モードを使用するように設定されると、ASDM を使用して ASA 1000V のステータスを監視できますが、設定を管理するのには使用できません。

はじめる前に

VNMC から ASDM を起動する前に、次のタスクを完了する必要があります。

1 次のいずれかを実行します。

- ASA 1000V OVA をまだ導入していないのであれば、すぐに導入してください。導入の際に、ASDM クライアントの IP アドレスを指定します。
- すでに ASA 1000V OVA を導入している場合は、vSphere クライアントで VM コンソールを使用して次の設定を適用します。
  - 次のコマンドを発行して、ASDM クライアントのサブネットへのルートを管理インターフェイス上に追加します。
    ```
    ASA1000V(config)# route interface ip subnet next-hop-ip
    ```
    ここで、*interface* は ASDM クライアント サブネットに対する管理インターフェイスで、*ip* は ASDM にアクセスするホストの IP アドレスで、*subnet* は ASDM クライアント サブネットで、*next-hop-ip* はゲートウェイの IP アドレスです。

（注） このステップは、ASA 1000V を導入する際に、ネクスト ホップ ゲートウェイの IP アドレスが指定されていない場合にのみ実行します。

- 次のコマンドを入力して、ASDM クライアントの管理インターフェイス経由で HTTP アクセスが可能になるようにします。

```
ASA1000V(config)# http ip subnet interface
```

ここで *ip* は、ASDM にアクセスするホストの IP アドレスで、*interface* は ASDM クライアント インターフェイスです。

（注） このステップは、ASA 1000V を導入する際に、ASDM クライアントの IP アドレスが指定されていない場合にのみ実行します。

2 次の内容を確認します。
   - ASA 1000V が VNMC に登録されている
   - ASA 1000V VM コンソールに有効なユーザ名とパスワードが存在する。

3 ASA 1000V インスタンスにエッジ ファイアウォールを割り当てます。 エッジ ファイアウォールが ASA 1000V インスタンスに割り当てられていない場合、ASDM オプションは UI には表示されません。

4 ご使用のシステムが、ダウンロードした Java Web Start アプリケーションを実行するように設定されているか確認します。

ASDM の設定に関する詳細については、『*Cisco ASA 1000V Cloud Firewall Getting Started Guide*』を参照してください。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Edge Firewalls] > [*edge-firewall*] を選択します。ここで [*edge-firewall*] は、ASDM を起動する対象となるエッジ ファイアウォールです。

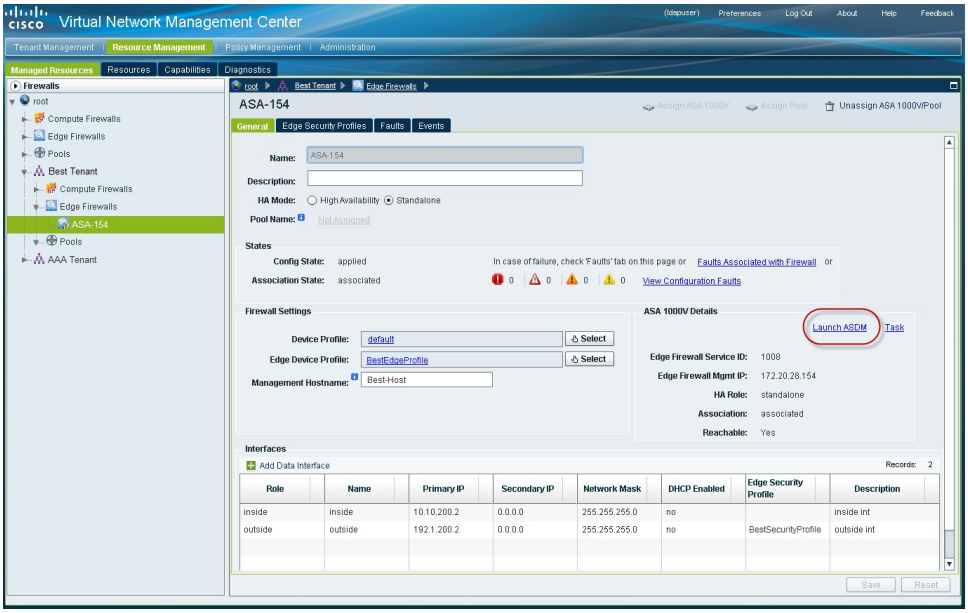
ステップ 2 [General] タブで、[ASA 1000V Details] 領域で [Launch ASDM] をクリックします。 ASDM の画面例, （224 ページ）を参照してください。
[ASDM Launch] 画面で、新しいブラウザ ウィンドウが開きます。

ステップ 3 [ASDM Launch] 画面で、[Run ASDM] をクリックします。
ASDM Web Start アプリケーションが自動的にダウンロードされ、実行されます。 要求されたら、証明書を受け入れます。
（注） [ASDM login] ダイアログボックスが表示されたら、ログイン クレデンシャルを入力することなく [OK] をクリックできます。

ASDM の画面例, （224 ページ） に示すように、ASDM がデスクトップ上の新しいウィンドウに開きます。

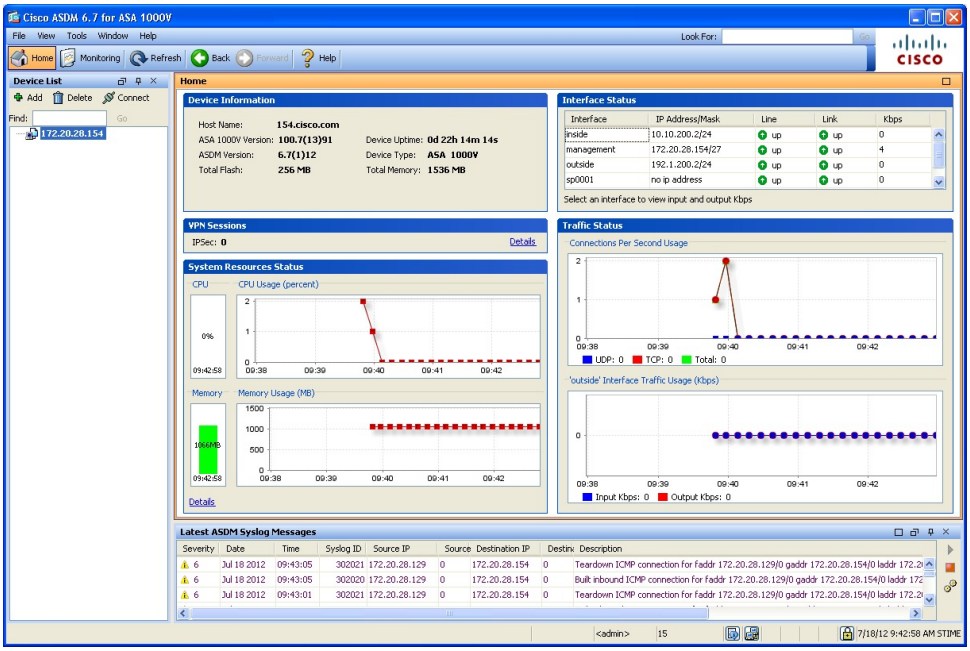
ASDM の画面例

図 *6*：*VNMC* インターフェイスの *[Launch ASDM]* リンク



300891

図 *7*：*[ASDM]* ウィンドウ



300892

プールの管理

プールの追加

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Pools] を選択します。

ステップ 2 [General] タブで、[Add Pool] をクリックします。

ステップ 3 [Add Pool] ダイアログボックスで、次のテーブルで説明されている情報を入力し、[OK] をクリックします。

フィールド	説明
Name	プール名。 この名前には、ID となる 1 ～ 32 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。作成後は、この名前を変更できません。
Description	プールの簡単な説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。
[Pool Members] 領域	
(Un)Assign	クリックすると、プールにプール メンバを追加したり、プールからプール メンバを削除したりすることができます。
Management IP Address	プール メンバの管理 IP アドレス。
Firewall	関連付けられているコンピュート ファイアウォールまたはエッジ ファイアウォール。
Association State	プール メンバの関連付けの状態： [unassociated]、[associating]、[associated]、[disassociating]、または [failed]。
Service ID	プール メンバの固有識別子。
Operational State	プール メンバの動作状態。

ステップ 4 （任意）次のタスクを実行して、プール メンバをプールに割り当てます。

a) [(Un)Assign] をクリックします。

b) [(Un)Assign Pool Member(s)] ダイアログボックスで、割り当てるファイアウォールを選択し、矢印をクリックしてそれを [Assigned Firewalls] リストに移動します。

c) [OK] をクリックします。

ステップ 5 [OK] をクリックします。

プールの割り当て

プールを作成したら、コンピューとまたはエッジ ファイアウォールに割り当てることができます。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [Compute Firewalls] または [Edge Firewalls] を選択します。

ステップ 2 ファイアウォールのリストで、必要なファイアウォールを選択し、[Assign Pool] をクリックします。

ステップ 3 [Assign Pool] ダイアログボックスで、[Name] ドロップダウン リストからプールを選択するか、[Add Pool] をクリックして新しいプールを追加します。

ステップ 4 [OK] をクリックします。

プールの編集

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Pools] を選択します。

ステップ 2 [General] タブで、編集するプールを選択し、[Edit] をクリックします。

ステップ 3 [Edit Pool] ダイアログボックスで、必要に応じて次のテーブルの情報を使用して情報を編集し、[OK] をクリックします。

フィールド	説明
Name	プール名（読み取り専用）。

フィールド	説明
Description	プールの簡単な説明。
Pool Members	
(Un)Assign	クリックすると、プールメンバを割り当てまたは割り当て解除できます。
IP Address	プール メンバ IP アドレス。
Compute Firewall	コンピュート ファイアウォールのリスト。
Association State	プール メンバの管理状態。
Service ID	プール メンバのサービス ID 番号。
Operational State	プール メンバの動作状態。

プールの割り当て解除

必要に応じて、コンピュートファイアウォールやエッジファイアウォールからプールの割り当てを解除できます。

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [Compute Firewalls] または [Edge Firewalls] を選択します。

ステップ 2 ファイアウォールのリストで、必要なファイアウォールを選択し、[Unassign *object*/Pool] をクリックします。ここで *object* は、エッジファイアウォールまたはコンピュート ファイアウォールのいずれかを選択したかに応じて、ASA 1000V または VSG のいずれかになります。

ステップ 3 確認の画面が表示されたら、削除を確認します。

プールの削除

手順

ステップ 1 [Resource Management] > [Managed Resources] > [root] > [*tenant*] > [Pools] を選択します。

ステップ 2 [General] タブで、削除するプールをクリックし、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

第 12 章

管理操作の設定

この項では、次のトピックについて取り上げます。

管理操作の規則

次の規則は、この項で説明されている管理操作を実行する際に適用されます。

- 指定するリモート ファイルの場所は、スラッシュ（/）で開始し、フル パスとファイル名を含める必要があります。 相対パスは使用しないでください。
- リモートシステムのユーザ名およびパスワードは正しい必要があり、指定されたユーザは、リモート システムでの読み取りおよび書き込み権限を持っている必要があります。
- リモートシステム上のファイルは有効なファイルである必要があり、サイズはゼロにできません。
- バックアップおよびエクスポート操作において、[Task] タブに [Remote Err Description] が [*No such file*] のものが含まれている場合、vCenter で VNMC VM をリブートします。

バックアップ操作の設定

バックアップ操作の作成

はじめる前に

バックアップ サーバの IP アドレスまたはホスト名および認証クレデンシャルを取得します。

手順

ステップ 1 [Administration] > [Operations] > [Backups] を選択します。

ステップ 2 [Create Backup Operation] をクリックします。

ステップ 3 [Create Backup Operation] ダイアログボックスで、次のフィールドに入力し、[OK] をクリックします。

フィールド	説明
Admin State	次のいずれかの管理状態： • [enabled]：バックアップはイネーブルになります。 [OK] をクリックすると、バックアップ操作が実行されます。 • [disabled]：バックアップはディセーブルになります。 [OK] をクリックしても、バックアップ操作は実行されません。 このオプションを選択した場合でも、ダイアログボックスのすべてのフィールドは表示されたままになります。
Type	バックアップ タイプ。 バックアップにより、データベースファイル全体のコピーが作成されます。 システムですべての設定を再作成する必要になった場合に、ディザスタリカバリとしてこのファイルを使用できます。 このフィールドは編集できません。

フィールド	説明
Protocol	リモートサーバとの通信時に使用するプロトコル。 （注） バックアップおよび復元操作にTFTPを使用しないでください。 • FTP • SCP • SFTP • TFTP
Hostname/IP Address	バックアップファイルが格納されているデバイスのホスト名またはIPアドレス。 操作を編集するときにこのエントリを変更することはできません。 （注） IPアドレスではなくホスト名を使用する場合、DNSサーバを設定する必要があります。
User	システムがリモートサーバへのログインに使用するユーザ名。 このフィールドは、[Protocol] フィールドで [TFTP] が選択された場合は表示されません。
Password	システムがリモートサーバへのログインに使用するパスワード。 このフィールドは、[Admin State] フィールドで [enabled] が選択された場合に表示されます。 このフィールドは、[Protocol] フィールドで [TFTP] が選択された場合は表示されません。 （注） VNMCではこのパスワードは保存されません。 バックアップ操作をすぐにイネーブルにして、実行する予定がない限り、このパスワードを入力する必要はありません。
Absolute Path Remote File	フル パスでのバックアップ ファイル名。 このエントリはスラッシュ（/）で始まる必要があり、相対パスを指定することはできません。

バックアップ操作の実行

手順

ステップ 1 [Administration] > [Operations] > [Backups] > [*Backup-server*] を選択します。ここで、*backup-server* は、バックアップ ファイルが格納されているサーバです。

ステップ 2 [General] タブで、次の情報を入力します。

a) [Admin State] フィールドで、[enabled] を選択します。

b) TFTP 以外のプロトコルの場合、[Password] フィールドに、指定したユーザのパスワードを入力します。

c) （任意）その他の使用可能なフィールドでコンテンツを変更します。

ステップ 3 [Save] をクリックします。
VNMC は、選択された設定タイプのスナップショットを作成し、ファイルをネットワークの場所にエクスポートします。

ステップ 4 （任意）バックアップ操作の進捗状況を表示するには、[Task] タブをクリックします。 [Task] タブは、次のテーブルに記載された情報を提供します。 操作は完了するまで実行し続けます。

名前	説明
Description	タスクの説明。
Status	タスク ステータス。
Stage Descriptor	現在のステージの説明。
Tries	タスクが試行された回数。
Previous Status	前タスク ステータス。
Remote Err Code	リモート エラー コード。
Remote Err Description	リモート エラー コードの説明。
Remote Inv Result	リモート エラー結果。
Time Stamp	タスクが完了した日時。
Progress	現在のタスクの経過表示。

バックアップ操作の編集

はじめる前に

バックアップ サーバの IP アドレスまたはホスト名および認証クレデンシャルを取得します。

手順

ステップ 1 [Administration] > [Operations] > [Backups] を選択します。

ステップ 2 編集するバックアップ操作を選択し、[Edit] をクリックします。

ステップ 3 [Edit Backup] ダイアログボックスで、必要に応じて情報を変更し、[OK] をクリックします。

フィールド	説明
Admin State	次のいずれかの管理状態： • [enabled]：バックアップはイネーブルになります。 [OK] をクリックすると、バックアップ操作が実行されます。 • [disabled]：バックアップはディセーブルになります。 [OK] をクリックしても、バックアップ操作は実行されません。 このオプションを選択した場合でも、ダイアログボックスのすべてのフィールドは表示されたままになります。
Type	バックアップ タイプ。 バックアップにより、データベースファイル全体のコピーが作成されます。 システムですべての設定を再作成する必要になった場合に、ディザスタリカバリとしてこのファイルを使用できます。 このフィールドは編集できません。
Protocol	リモートサーバとの通信時に使用するプロトコル。 （注） バックアップおよび復元操作に TFTP を使用しないでください。 • FTP • SCP • SFTP • TFTP

フィールド	説明
Hostname/IP Address	バックアップファイルが格納されているデバイスのホスト名または IP アドレス。 操作を編集するときにこのエントリを変更することはできません。 （注） IP アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。
User	システムがリモートサーバへのログインに使用するユーザ名。 このフィールドは、[Protocol] フィールドで [TFTP] が選択された場合は表示されません。
Password	システムがリモートサーバへのログインに使用するパスワード。 このフィールドは、[Admin State] フィールドで [enabled] が選択された場合に表示されます。 このフィールドは、[Protocol] フィールドで [TFTP] が選択された場合は表示されません。 （注） VNMC ではこのパスワードは保存されません。 バックアップ操作をすぐにイネーブルにして、実行する予定がない限り、このパスワードを入力する必要はありません。
Absolute Path Remote File	フル パスでのバックアップ ファイル名。 このエントリはスラッシュ（/）で始まる必要があり、相対パスを指定することはできません。

バックアップ操作の削除

手順

ステップ 1 [Administration] > [Operations] > [Backups] を選択します。

ステップ 2 削除するバックアップ操作を選択し、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

バックアップ設定の復元

手順

ステップ 1 VNMC 仮想マシンをインストールします。 詳細については、『*Cisco Virtual Network Management Center 2.0 Quick Start Guide*』を参照してください。

ステップ 2 VSG ポリシー エージェントをアンインストールします。 このタスク用の VSG コンソールにセキュア シェルを接続します。 このステップではトラフィックが中断されることはありません。

例：
```
vsg# conf t
vsg (config)# vnmc-policy-agent
vsg (config-vnmc-policy-agent)# no policy-agent-image
```
（注） 復元する VNMC に関連付けられているすべての VSG で、このステップを実行します。

ステップ 3 ASA 1000V ポリシー エージェントをディセーブルにします。

例：
```
ASA-154# conf t
ASA-154(config)# no vnmc policy-agent
```

ステップ 4 VSM ポリシー エージェントをアンインストールします。 このタスク用の VSM コンソールにセキュア シェルを接続します。 このステップではトラフィックが中断されることはありません。

例：
```
vsm# conf t
vsm (config)# vnmc-policy-agent
vsm (config-vnmc-policy-agent)# no policy-agent-image
```
（注） 復元する VNMC に関連付けられているすべての VSM で、このステップを実行します。

ステップ 5 VNMC データベースを復元します。 このタスク用の VNMC CLI にセキュア シェルを接続します。 VNMC バックアップ ロケーションに基づいて、FTP、SCP、または SFTP を使用して復元します。

例：
```
vnmc# connect local-mgmt
vnmc(local-mgmt)# restore scp://username@server/path
```

ステップ 6 VNMC UI で、[Administration] > [Service Registry] > [Clients] を選択し、[General] タブで次の手順を実行します。

a) 登録された各 VSM で、動作ステータスに lost-visibility と表示されるまで待ちます。

b) 各 VSM を選択し、[Delete Client] をクリックします。

ステップ 7 VNMC UI で [Resource Management] > [Resources] > [Virtual Supervisor Modules] を選択し、削除した VSM が表示されていないことを確認します。

ステップ 8 VSM ごとに次のコマンドを入力し、VNMC に関連付けられた VSM を再登録します。

例：
```
VSM# conf t
VSM (config)# vnmc-policy-agent
VSM (config-vnmc-policy-agent)# registration-ip vsm-ip-address
VSM (config-vnmc-policy-agent)# shared-secret password
```

ステップ 9 VSM ポリシー エージェントを再インストールします。

（注） VSMポリシーエージェントをアップグレードする必要がある場合は、新しいソフトウェアをインストールしてください。

例：
```
VSM# conf t
VSM (config)# vnmc-policy-agent
VSM (config-vnmc-policy-agent)# policy-agent-image bootflash:vnmc-vsmpa.1.0.1g.bin
```

ステップ 10 すべての VSM がサービス レジストリに登録され、[Resource Management] > [Resources] > [Virtual Supervisor Modules] に表示されるまで待ちます。

ステップ 11 VSG ごとに次のコマンドを入力し、VNMC に関連付けられた VSG を再登録します。

例：
```
VSG# conf t
VSG (config)# vnmc-policy-agent
VSG (config-vnmc-policy-agent)# registration-ip vsg-ip-address
VSG (config-vnmc-policy-agent)# shared-secret password
```

ステップ 12 VSG ポリシー エージェントを再インストールします。

（注） VSGポリシーエージェントをアップグレードする必要がある場合は、新しいソフトウェアをインストールしてください。

例：
```
VSG# conf t
VSG (config)# vnmc-policy-agent
VSG (config-vnmc-policy-agent)# policy-agent-image bootflash:vnmc-vsgpa.1.0.1g.bin
```

ステップ 13 ASA 1000V ポリシー エージェントを再度有効にします。

例：
```
ASA-154# conf t
ASA-154(config)# vnmc policy-agent
```

```
ASA-154(config-vnmc-policy-agent)# shared-secret password
ASA-154(config-vnmc-policy-agent)# registration host host-ip-address
```

ステップ 14 復元プロセスの完了後、次のステートを確認します。

（注） セットアップ環境により、復元プロセスに数分を要する場合があります。

a) VSG CLI を使用して、設定が初期ステートに復元されていることを確認します。

b) VNMC UI を使用して、オブジェクトおよびポリシーが初期ステートに復元されていることを確認します。

c) ASA 1000V CLI を使用して、設定が初期ステートに復元されていることを確認します。

エクスポート操作の設定

エクスポート操作の作成

はじめる前に

エクスポートを実行する前に、リモート ファイル サーバの IP アドレスまたはホスト名、および認証クレデンシャルを取得します。

（注） コンピュート ファイアウォールおよびエッジ ファイアウォールのそれぞれ VSG と ASA 1000V との関連付けは、エクスポート データやインポート データに含まれていません。 デバイス プロファイルおよびポリシーなどのファイアウォールの定義のみが含まれます。 インポートしたファイアウォールがシステムに存在しない場合は、インポート操作後のコンピュート ファイアウォールの VSG または ASA 1000V への関連付けはありません。 インポート済みファイアウォールがすでにシステムに存在する場合、関連付けの状態は同じままになります。

手順

ステップ 1 [Administration] > [Operations] > [Backups] を選択します。

ステップ 2 [Create Export Operation] をクリックします。

ステップ 3 [Create Export Operation] ダイアログボックスで、次のテーブルで説明されている必須情報を入力し、[OK] をクリックします。

フィールド	説明
Admin State	次のいずれかの管理状態： • [enabled]：エクスポートはイネーブルになります。 [OK] をクリックすると、エクスポート操作が実行されます。 • [disabled]：エクスポートはディセーブルになります。 [OK] をクリックしても、エクスポート操作は実行されません。 このオプションを選択した場合でも、ダイアログボックスのすべてのフィールドは表示されたままになります。
Type	次のいずれかのエクスポート タイプ： • config-all • config-logical • config-system
Protocol	リモート サーバとの通信時に使用するプロトコル。 • FTP • SCP • SFTP • TFTP
Hostname/IP Address	エクスポート ファイルが格納されるデバイスのホスト名または IP アドレス。 操作を編集するときにこのエントリを変更することはできません。 （注） IP アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。
User	システムがリモート サーバへのログインに使用するユーザ名。 このフィールドは、[Protocol] フィールドで [TFTP] が選択された場合は表示されません。

フィールド	説明
Password	システムがリモートサーバへのログインに使用するパスワード。 このフィールドは、[Admin State] フィールドで [enabled] が選択された場合に表示されます。 このフィールドは、[Protocol] フィールドで [TFTP] が選択された場合は表示されません。 （注） VNMC ではこのパスワードは保存されません。 エクスポート操作をすぐにイネーブルにして、実行する予定がない限り、このパスワードを入力する必要はありません。
Absolute Path Remote File（.tgz）	フル パスでの .tgz ファイル名。 このエントリはスラッシュ（/）で始まる必要があり、相対パスを指定することはできません。

エクスポート操作の編集

はじめる前に

バックアップ サーバの IP アドレスおよび認証クレデンシャルを取得します。

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。

ステップ 2 [Navigation] ペインの [Operations] サブタブをクリックします。

ステップ 3 [Navigation] ペインで、[Backups] ノードをクリックします。

ステップ 4 [Work] ペインで、テーブル内の項目を展開し、編集するエクスポート操作を選択します。

ステップ 5 [Edit] をクリックします。

ステップ 6 [Edit] ダイアログボックスで、必要に応じて次のフィールドを変更します。

フィールド	説明
Admin State	次のいずれかの管理状態： • [enabled]：エクスポートはイネーブルになります。 [OK] をクリックすると、エクスポート操作が実行されます。 • [disabled]：エクスポートはディセーブルになります。 [OK] をクリックしても、エクスポート操作は実行されません。 このオプションを選択した場合でも、ダイアログボックスのすべてのフィールドは表示されたままになります。
Type	次のいずれかのエクスポート タイプ： • config-all • config-logical • config-system
Protocol	リモート サーバとの通信時に使用するプロトコル。 • FTP • SCP • SFTP • TFTP
Hostname/IP Address	エクスポート ファイルが格納されるデバイスのホスト名または IP アドレス。 操作を編集するときにこのエントリを変更することはできません。 （注） IP アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。
User	システムがリモート サーバへのログインに使用するユーザ名。 このフィールドは、[Protocol] フィールドで [TFTP] が選択された場合は表示されません。

フィールド	説明
Password	システムがリモートサーバへのログインに使用するパスワード。 このフィールドは、[Admin State] フィールドで [enabled] が選択された場合に表示されます。 このフィールドは、[Protocol] フィールドで [TFTP] が選択された場合は表示されません。 （注） VNMC ではこのパスワードは保存されません。 エクスポート操作をすぐにイネーブルにして、実行する予定がない限り、このパスワードを入力する必要はありません。
Absolute Path Remote File（.tgz）	フル パスでの .tgz ファイル名。 このエントリはスラッシュ（/）で始まる必要があり、相対パスを指定することはできません。

ステップ 7 [OK] をクリックします。

エクスポート操作の削除

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。
ステップ 2 [Navigation] ペインの [Operations] サブタブをクリックします。
ステップ 3 [Navigation] ペインで、[Backups] ノードをクリックします。
ステップ 4 [Work] ペインで、削除するエクスポート操作をクリックします。
ステップ 5 [Delete] をクリックします。
ステップ 6 [Confirm] ダイアログボックスで、[Yes] をクリックします。

インポート操作の設定

インポート操作の作成

はじめる前に

リモートファイルサーバのIPアドレスまたはホスト名および認証クレデンシャルを取得します。

（注） コンピュートファイアウォールおよびエッジファイアウォールのそれぞれVSGとASA 1000Vとの関連付けは、エクスポートデータやインポートデータに含まれていません。 デバイスプロファイルおよびポリシーなどのコンピュートおよびエッジファイアウォールの定義のみが含まれます。 このため、インポートしたファイアウォールがシステムに存在していなかった場合は、インポート操作後のファイアウォールのVSGまたはASA 1000Vへの関連付けはありません。 インポート済みファイアウォールがすでにシステムに存在する場合、関連付けの状態は同じままになります。

注意 設定データがVNMCサーバにインポートされると、エラーメッセージが表示されログアウトされ、新しいVNMC証明書が表示されることがあります。 このエラーは、VNMCホスト名、ドメイン名、またはその両方が変更されたために発生します。 VM Manager拡張を再びエクスポートし、vCenterにインストールする必要があります。 インポートを続行するには、VNMC証明書を受け入れ、VNMCに再度ログインします。

手順

ステップ 1 [Administration] > [Operations] > [Backups] を選択します。

ステップ 2 [Create Import Operation] をクリックします。

ステップ 3 [Create Import Operation] ダイアログボックスで、必要に応じて次の情報を入力し、[OK] をクリックします。

フィールド	説明
Admin State	次のいずれかの管理状態： • [enabled]：インポートはイネーブルになります。 [OK] をクリックするとすぐにインポート操作が実行されます。 • [disabled]：インポートはディセーブルになります。 [OK] をクリックしても、インポート操作は実行されません。 このオプションを選択した場合でも、ダイアログボックスのすべてのフィールドは表示されたままになります。
Action	ファイルに対して行うアクション：マージ。
Protocol	リモートサーバとの通信時に使用するプロトコル。 • FTP • SCP • SFTP • TFTP
Hostname/IP Address	インポートファイルが格納されているデバイスのホスト名または IP アドレス。 操作を編集するときにこのエントリを変更することはできません。 （注） IP アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。
User	システムがリモートサーバへのログインに使用するユーザ名。 このフィールドは、[Admin State] フィールドで [enabled] が選択された場合に表示されます。 このフィールドは、[Protocol] フィールドで [TFTP] が選択された場合は表示されません。

フィールド	説明
Password	システムがリモートサーバへのログインに使用するパスワード。 このフィールドは、[Protocol] フィールドで [TFTP] が選択された場合は表示されません。 （注） VNMC ではこのパスワードは保存されません。 インポート操作をすぐにイネーブルにして、実行する予定がない限り、このパスワードを入力する必要はありません。
Absolute Path Remote File（.tgz）	フル パスでの .tgz ファイル名。 このエントリはスラッシュ（/）で始まる必要があり、相対パスを指定することはできません。

インポート操作の編集

はじめる前に

リモートファイルサーバのIPアドレスまたはホスト名および認証クレデンシャルを取得します。

手順

ステップ 1 [Administration] > [Operations] > [Backups] を選択します。

ステップ 2 編集するインポート操作を選択し、[Edit] をクリックします。

ステップ 3 [Edit] ダイアログボックスで、必要に応じてフィールドを変更し、[OK] をクリックします。

フィールド	説明
Admin State	次のいずれかの管理状態： • [enabled]：インポートはイネーブルになります。 [OK] をクリックするとすぐにインポート操作が実行されます。 • [disabled]：インポートはディセーブルになります。 [OK] をクリックしても、インポート操作は実行されません。 このオプションを選択した場合でも、ダイアログボックスのすべてのフィールドは表示されたままになります。
Action	ファイルに対して行うアクション：マージ。
Protocol	リモートサーバとの通信時に使用するプロトコル。 • FTP • SCP • SFTP • TFTP
Hostname/IP Address	インポートファイルが格納されているデバイスのホスト名または IP アドレス。 操作を編集するときにこのエントリを変更することはできません。 （注） IP アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。
User	システムがリモートサーバへのログインに使用するユーザ名。 このフィールドは、[Admin State] フィールドで [enabled] が選択された場合に表示されます。 このフィールドは、[Protocol] フィールドで [TFTP] が選択された場合は表示されません。

フィールド	説明
Password	システムがリモートサーバへのログインに使用するパスワード。 このフィールドは、[Protocol] フィールドで [TFTP] が選択された場合は表示されません。 （注） VNMC ではこのパスワードは保存されません。 インポート操作をすぐにイネーブルにして、実行する予定がない限り、このパスワードを入力する必要はありません。
Absolute Path Remote File（.tgz）	フル パスでの .tgz ファイル名。 このエントリはスラッシュ（/）で始まる必要があり、相対パスを指定することはできません。

インポート操作の削除

手順

ステップ 1 [Administration] > [Operations] > [Backups] を選択します。

ステップ 2 削除するインポート操作を選択し、[Delete] をクリックします。

ステップ 3 確認の画面が表示されたら、削除を確認します。

索 引

P

R

S

T

V

い

え

お

か

き

く

こ

さ

し

せ

そ

つ

て

と

な

は

ひ

ふ

へ

ほ

ま

も

ゆ

り

る

ろ

わ