Cisco ASA の概要

Cisco ASA は、高度なステートフル ファイアウォールと VPN コンセントレータの機能を 1 台のデバイスに集約した製品です。モデルによっては、IPS などのサービス モジュールが統合されています。ASA は多数の高度な機能を備えています。たとえば、マルチ セキュリティ コンテキスト（仮想ファイアウォールに類似）、クラスタリング（複数のファイアウォールを結合して 1 つのファイアウォールにする）、トランスペアレント（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ 3）ファイアウォール動作、高度なインスペクション エンジン、IPsec VPN、SSL VPN、クライアントレス SSL VPN のサポートなどがあります。

この章は、次の項で構成されています。

ハードウェアとソフトウェアの互換性

サポートされているハードウェアおよびソフトウェアの完全なリストについては、『*Cisco ASA Compatibility*』を参照してください。

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

VPN 仕様

次の URL にある『*Supported VPN Platforms, Cisco ASA 5500 Series*』を参照してください。

http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html

新機能

（注）　syslog メッセージ ガイド に、追加、変更、および非推奨化された syslog メッセージを示します。

ASA 9.1(1) の新機能

表 1-1 に ASA バージョン 9.1(1) の新機能を示します。

（注）　8.4(4.x) および 8.4(5) で追加された機能は、9.0(1) の機能表に表示されていない限り、9.1(1) には含まれていません。

表 1-1　ASA バージョン 9.1(1) の新機能

機能	説明
モジュール機能	
ASA 5512-X ～ ASA 5555-X に対する ASA CX SSP のサポート	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X に対する ASA CX SSP ソフトウェア モジュールのサポートが導入されました。ASA CX ソフトウェア モジュールを使用するには、ASA 上に Cisco ソリッド ステート ドライブ（SSD）が必要です。SSD の詳細については、ASA 5500-X のハードウェア ガイドを参照してください。 **session cxsc**、**show module cxsc**、**sw-module cxsc** の各コマンドが変更されました。

スイッチにおける ASA サービス モジュール の動作

Cisco IOS ソフトウェアを搭載した Catalyst 6500 シリーズおよび Cisco 7600 シリーズ スイッチで、スイッチのスーパーバイザおよび統合型 MSFC の両方に ASASM をインストールできます。

（注）　Catalyst オペレーティング システム（OS）はサポートされていません。

ASA は独自のオペレーティング システムで動作します。

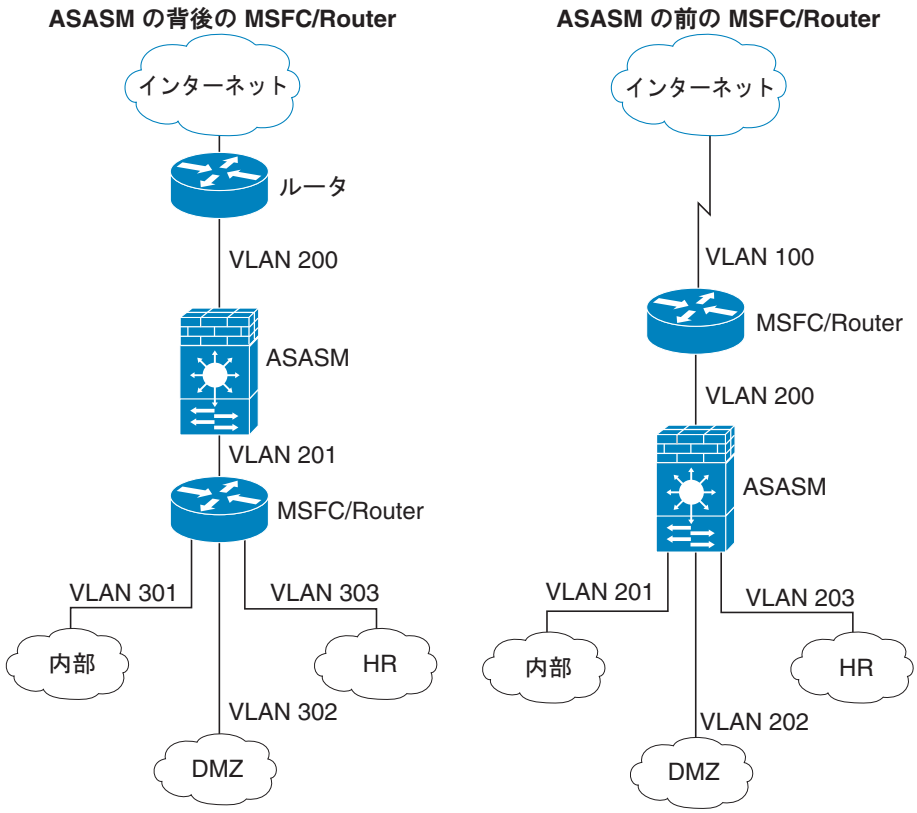
スイッチにはスイッチング プロセッサ（スーパーバイザ）とルータ（MSFC）が組み込まれています。MSFC はシステムの一部として必要ですが、使用しなくてもかまいません。使用することを選択する場合、MSFC に 1 つまたは複数の VLAN インターフェイスを割り当てることができます。MSFC の代わりに外部ルータを使用できます。

シングル コンテキスト モードでは、ファイアウォールの向こう側にルータを配置することも、ファイアウォールより手前に配置することもできます（図 1-1 を参照）。

ルータの位置は、割り当てる VLAN によって決まります。たとえば、図 1-1 の左側の例では、ASASM の内部インターフェイスに VLAN 201 を割り当てているので、ルータはファイアウォールより手前になります。図 1-1 の右側の例では、ASASM の外部インターフェイスに VLAN 200 を割り当てているので、ルータはファイアウォールの向こう側になります。

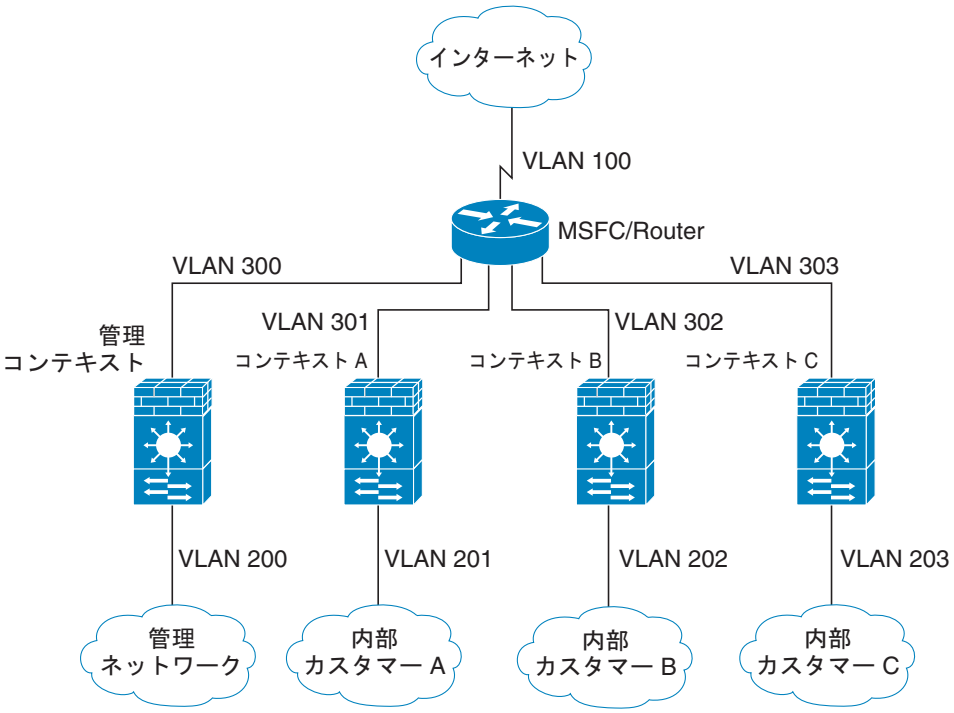
左側の例では、MSFC またはルータは VLAN 201、301、302、および 303 の間をルーティングします。宛先がインターネットの場合以外、内部トラフィックは ASASM を通過しません。右側の例では、ASASM は内部 VLAN 201、202、および 203 間のすべてのトラフィックを処理して保護します。

図 1-1　MSFC/Router の配置



マルチコンテキスト モードでは、ASASM より手前にルータを配置した場合、1 つのコンテキストに限定して接続する必要があります。ルータを複数のコンテキストに接続すると、ルータはコンテキスト間をルーティングすることになり、意図に反する可能性があります。複数のコンテキストの一般的なシナリオでは、インターネットとスイッチド ネットワーク間でルーティングするためにすべてのコンテキストの前にルータを使用します（図 1-2 を参照）。

図 1-2　マルチコンテキストの場合の MSFC/Router の配置



ファイアウォール機能の概要

ファイアウォールは、外部ネットワーク上のユーザによる不正アクセスから内部ネットワークを保護します。また、ファイアウォールは、人事部門ネットワークをユーザ ネットワークから分離するなど、内部ネットワーク同士の保護も行います。Web サーバまたは FTP サーバなど、外部のユーザが使用できるようにする必要のあるネットワーク リソースがあれば、ファイアウォールで保護された別のネットワーク（*Demiliterized Zone*（DMZ; 非武装地帯）と呼ばれる）上に配置します。ファイアウォールによって DMZ へのアクセスを制限できますが、DMZ には公開サーバしかないため、この地帯が攻撃されても影響を受けるのは公開サーバに限定され、他の内部ネットワークに影響が及ぶことはありません。また、特定アドレスだけに許可する、認証または許可を義務づける、または外部の URL フィルタリング サーバと協調するといった手段によって、内部ユーザが外部ネットワーク（インターネットなど）にアクセスする機会を制御することもできます。

ファイアウォールに接続されているネットワークに言及する場合、*外部*ネットワークはファイアウォールの手前にあるネットワーク、*内部*ネットワークはファイアウォールの背後にある保護されているネットワーク、そして *DMZ* はファイアウォールの背後にあるが、外部ユーザに制限付きのアクセスが許されているネットワークです。ASA を使用すると、数多くのインターフェイスに対してさまざまなセキュリティ ポリシーが設定できます。このインターフェイスには、多数の内部インターフェイス、多数の DMZ、および必要に応じて多数の外部インターフェイスが含まれるため、ここでは、このインターフェイスの区分は一般的な意味で使用するだけです。

この項は、次の内容で構成されています。

セキュリティ ポリシーの概要

他のネットワークにアクセスするために、ファイアウォールを通過することが許可されるトラフィックがセキュリティ ポリシーによって決められます。デフォルトでは、内部ネットワーク（高セキュリティ レベル）から外部ネットワーク（低セキュリティ レベル）へのトラフィックは、自由に流れることが ASA によって許可されます。トラフィックにアクションを適用してセキュリティ ポリシーをカスタマイズすることができます。この項は、次の内容で構成されています。

アクセス リストによるトラフィックの許可または拒否

アクセスリストは、内部から外部へのトラフィックを制限するため、または外部から内部へのトラフィックを許可するために使用できます。トランスペアレント ファイアウォール モードでは、非 IP トラフィックを許可するための EtherType アクセス リストも適用できます。

NAT の適用

NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません。
- NAT はローカル アドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- NAT は、重複 IP アドレスをサポートすることで、IP ルーティングの問題を解決できます。

IP フラグメントからの保護

ASA は IP フラグメント保護を提供します。この機能は、すべての ICMP エラー メッセージの完全リアセンブリ、および ASA を介してルーティングされる残りの IP フラグメントの仮想リアセンブリを実行します。セキュリティ チェックに失敗したフラグメントは、ドロップされログに記録されます。仮想リアセンブリはディセーブルにできません。

通過トラフィックに対する AAA の使用

HTTP など特定のタイプのトラフィックに対して、認証と許可のいずれかまたは両方を要求することができます。ASA は、RADIUS サーバまたは TACACS+ サーバにアカウンティング情報を送信することもあります。

HTTP、HTTPS、または FTP フィルタリングの適用

アクセス リストを使用して、特定の Web サイトまたは FTP サーバへの発信アクセスを禁止できますが、このような方法で Web サイトの使用方法を設定し管理することは、インターネットの規模とダイナミックな特性から、実用的とはいえません。ASA を、次のインターネット フィルタリング製品のいずれかを実行している別のサーバと連携させて使用することをお勧めします。

- Websense Enterprise
- Secure Computing SmartFilter

アプリケーション インスペクションの適用

インスペクション エンジンは、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。これらのプロトコルは、ASA が詳細なパケット インスペクションを行うことを要求します。

IPS モジュールへのトラフィックの送信

使用しているモデルが侵入防御用の IPS モジュールをサポートしている場合、トラフィックをモジュールに送信して検査することができます。IPS モジュールは、多数の埋め込み型シグニチャ ライブラリに基づいて異常や悪用を探索することでネットワーク トラフィックのモニタおよびリアルタイム分析を行います。システムで不正なアクティビティが検出されると、侵入防御サービス機能は、該当する接続を終了して攻撃元のホストを永続的にブロックし、この事象をログに記録し、さらにアラートを Device Manager に送信します。その他の正規の接続は、中断することなく独立した動作を継続します。詳細については、IPS モジュールのマニュアルを参照してください。

コンテンツ セキュリティおよび制御モジュールへのトラフィックの送信

使用しているモデルでサポートされていれば、CSC SSM により、ウイルス、スパイウェア、スパム、およびその他の不要トラフィックから保護されます。これは、FTP、HTTP、POP3、および SMTP トラフィックをスキャンすることで実現されます。そのためには、これらのトラフィックを CSC SSM に送信するように ASA を設定しておきます。

QoS ポリシーの適用

音声やストリーミング ビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。QoS は、この種のトラフィックにプライオリティを設定するネットワーク機能です。QoS とは、選択したネットワーク トラフィックによりよいサービスを提供するネットワークの機能です。

接続の制限と TCP 正規化の適用

TCP 接続、UDP 接続、および初期接続を制限することができます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

TCP 正規化は、正常に見えないパケットをドロップするように設計された高度な TCP 接続設定で構成される機能です。

脅威検出のイネーブル化

スキャン脅威検出と基本脅威検出、さらに統計情報を使用して脅威を分析する方法を設定できます。

基本脅威検出は、DoS 攻撃などの攻撃に関係している可能性のあるアクティビティを検出し、自動的にシステム ログ メッセージを送信します。

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA のスキャンによる脅威の検出機能では、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定したり、自動的にホストを回避したりできます。

ボットネット トラフィック フィルタのイネーブル化

マルウェアとは、知らないうちにホストにインストールされている悪意のあるソフトウェアです。個人情報（パスワード、クレジット カード番号、キー ストローク、または独自データ）の送信などのネットワーク アクティビティを試みるマルウェアは、マルウェアが既知の不正な IP アドレスへの接続を開始したときにボットネット トラフィック フィルタによって検出できます。ボットネット トラフィック フィルタは、着信と発信の接続を既知の不正なドメイン名と IP アドレス（ブラックリスト）のダイナミック データベースと照合して確認し、不審なアクティビティのログを記録します。マルウェア アクティビティに関する syslog メッセージを確認すると、ホストを切り離して感染を解決するための手順を実行できます。

Cisco Unified Communications の設定

Cisco ASA 5500 シリーズは、統合された通信構成にプロキシの機能を提供する戦略的なプラットフォームです。プロキシの目的は、クライアントとサーバ間の接続を終端し、再発信することです。プロキシは、トラフィック インスペクション、プロトコルとの適合性、ポリシー制御など幅広いセキュ

リティ機能を提供し、内部ネットワークのセキュリティを保証します。プロキシの機能として広く普及しているのが、暗号化された接続を終端して、接続の機密性を維持しながらセキュリティ ポリシーを適用する機能です。

ファイアウォール モードの概要

ASA は、次の 2 つのファイアウォール モードで動作します。

- ルーテッド
- 透過

ルーテッド モードでは、ASA は、ネットワークのルータ ホップと見なされます。

トランスペアレント モードでは、ASA は「Bump In The Wire」または「ステルス ファイアウォール」のように動作し、ルータ ホップとは見なされません。ASA では、内部インターフェイスと外部インターフェイスに同じネットワークが接続されます。

トランスペアレント ファイアウォールは、ネットワーク コンフィギュレーションを簡単にするために使用できます。トランスペアレント モードは、攻撃者からファイアウォールが見えないようにする場合にも有効です。トランスペアレント ファイアウォールは、他の場合にはルーテッド モードでブロックされるトラフィックにも使用できます。たとえば、トランスペアレント ファイアウォールでは、EtherType アクセス リストを使用するマルチキャスト ストリームが許可されます。

ステートフル インスペクションの概要

ASA を通過するトラフィックはすべて、アダプティブ セキュリティ アルゴリズムを使用して検査され、通過が許可されるか、またはドロップされます。単純なパケット フィルタは、送信元アドレス、宛先アドレス、およびポートが正しいかどうかはチェックできますが、パケット シーケンスまたはフラグが正しいかどうかはチェックしません。また、フィルタはすべてのパケットをフィルタと照合してチェックするため、処理が低速になる場合があります。

（注） TCP ステート バイパス機能を使用すると、パケット フローをカスタマイズできます。ファイアウォール コンフィギュレーション ガイドの “TCP State Bypass” section on page 19-3 を参照してください。

ただし、ASA のようなステートフル ファイアウォールは、パケットの次のようなステートについて検討します。

- 新規の接続かどうか。

  新規の接続の場合、ASA は、パケットをアクセス リストと照合してチェックする必要があり、これ以外の各種のタスクを実行してパケットの許可または拒否を決定する必要があります。このチェックを行うために、セッションの最初のパケットは「セッション管理パス」を通過しますが、トラフィックのタイプに応じて、「コントロール プレーン パス」も通過する場合があります。

  セッション管理パスで行われるタスクは次のとおりです。

  - アクセス リストとの照合チェック
  - ルート ルックアップ
  - NAT 変換（xlates）の割り当て
  - 「ファスト パス」でのセッション確立

ASA は、TCP トラフィックのファスト パスに転送フローとリバース フローを作成します。ASA は、高速パスも使用できるように、UDP、ICMP（ICMP インスペクションがイネーブルの場合）などのコネクションレス型プロトコルの接続状態の情報も作成するので、これらのプロトコルもファスト パスを使用できます。

（注）　SCTP などの他の IP プロトコルの場合、ASA はリバース パス フローを作成しません。そのため、これらの接続を参照する ICMP エラー パケットはドロップされます。

レイヤ 7 インスペクションが必要なパケット（パケットのペイロードの検査または変更が必要）は、コントロール プレーン パスに渡されます。レイヤ 7 インスペクション エンジンは、2 つ以上のチャネルを持つプロトコルで必要です。2 つ以上のチャネルの 1 つは周知のポート番号を使用するデータ チャネルで、その他はセッションごとに異なるポート番号を使用するコントロール チャネルです。このようなプロトコルには、FTP、H.323、および SNMP があります。

- 確立済みの接続かどうか。

  接続がすでに確立されている場合は、ASA でパケットの再チェックを行う必要はありません。一致するパケットの大部分は、両方向で「高速」パスを通過できます。高速パスで行われるタスクは次のとおりです。

  - IP チェックサム検証
  - セッション ルックアップ
  - TCP シーケンス番号のチェック
  - 既存セッションに基づく NAT 変換
  - レイヤ 3 ヘッダー調整およびレイヤ 4 ヘッダー調整

  レイヤ 7 インスペクションを必要とするプロトコルに合致するデータ パケットも高速パスを通過できます。

  確立済みセッション パケットの中には、セッション管理パスまたはコントロール プレーン パスを引き続き通過しなければならないものがあります。セッション管理パスを通過するパケットには、インスペクションまたはコンテンツ フィルタリングを必要とする HTTP パケットが含まれます。コントロール プレーン パスを通過するパケットには、レイヤ 7 インスペクションを必要とするプロトコルのコントロール パケットが含まれます。

VPN 機能の概要

VPN は、TCP/IP ネットワーク（インターネットなど）上のセキュアな接続で、プライベートな接続として表示されます。このセキュアな接続はトンネルと呼ばれます。ASA は、トンネリング プロトコルを使用して、セキュリティ パラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを通したパケットの送信または受信、パケットのカプセル化の解除を行います。ASA は、双方向のトンネル エンドポイントとして機能します。たとえば、プレーン パケットを受信してカプセル化し、それをトンネルのもう一方の側に送信することができます。そのエンドポイントで、パケットはカプセル化が解除され、最終的な宛先に送信されます。また、セキュリティ アプライアンスは、カプセル化されたパケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

ASA が実行する機能は次のとおりです。

- トンネルの確立
- トンネル パラメータのネゴシエーション
- ユーザの認証

- ユーザ アドレスの割り当て
- データの暗号化と復号化
- セキュリティ キーの管理
- トンネルを通したデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信データと発信データの転送の管理

ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

セキュリティ コンテキストの概要

1 台の ASA を、セキュリティ コンテキストと呼ばれる複数の仮想デバイスに分割することができます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、多くの機能がサポートされます。VPN、ダイナミック ルーティング プロトコルなど、いくつかの機能はサポートされません。

マルチ コンテキスト モードの場合、ASA には、セキュリティ ポリシー、インターフェイス、およびスタンドアロン デバイスで設定できるほとんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者がコンテキストを追加および管理するには、コンテキストをシステム コンフィギュレーションに設定します。これが、シングル モード設定と同じく、スタートアップ コンフィギュレーションとなります。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただし、ユーザが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。

ASA クラスタリングの概要

ASA クラスタリングを利用すると、複数の ASA をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、マスター ユニット上でのみ実行します。コンフィギュレーションは、メンバ ユニットに複製されます。