



Firepower 9300 シャーシの ASA クラスタ

クラスタリングを利用すると、複数のFirepower 9300 シャーシ ASA をグループ化して、1つの論理デバイスにすることができます。Firepower 9300 シャーシシリーズには、Firepower 9300。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。



(注) FirePOWER 9300 は複数のシャーシにまたがる（シャーシ間）クラスタをサポートしません。シャーシ内クラスタリングのみをサポートします。



(注) 一部の機能は、クラスタリングを使用する場合、サポートされません。「[クラスタリングでサポートされない機能（6 ページ）](#)」を参照してください。

- [Firepower 9300 シャーシでのクラスタリングについて（1 ページ）](#)
- [ASA の各機能とクラスタリング（5 ページ）](#)
- [Firepower 9300 シャーシでのクラスタリングの要件と前提条件（12 ページ）](#)
- [上のクラスタリングのライセンス Firepower 9300 シャーシ（12 ページ）](#)
- [クラスタリングガイドラインと制限事項（13 ページ）](#)
- [クラスタリングの設定 Firepower 9300 シャーシ（13 ページ）](#)
- [FXOS：クラスタメンバの削除（29 ページ）](#)
- [ASA：クラスタメンバの管理（31 ページ）](#)
- [ASA：での ASA クラスタのモニタリング Firepower 9300 シャーシ（36 ページ）](#)
- [クラスタリングの参考資料（40 ページ）](#)
- [Firepower 9300 シャーシ上の ASA クラスタリングの履歴（47 ページ）](#)

Firepower 9300 シャーシでのクラスタリングについて

クラスタは、単一の論理ユニットとして機能する複数のデバイスから構成されます。Firepower 9300 シャーシにクラスタを展開すると、以下の処理が実行されます。

- ユニット間通信用のクラスタ制御リンク（デフォルトのポートチャネル 48）を作成します。シャーシ内クラスタリングでは、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。
- アプリケーション内のクラスタブートストラップコンフィギュレーションを作成します。
クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ構成が Firepower 9300 シャーシスーパーバイザからプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部は、アプリケーション内でユーザが設定できます。
- スパンドインターフェイスとして、クラスタにデータインターフェイスを割り当てます。
シャーシ内クラスタリングでは、スパンドインターフェイスは、シャーシ間クラスタリングのように EtherChannel に制限されません。Firepower 9300 スーパーバイザは共有インターフェイスの複数のモジュールにトラフィックをロードバランシングするために内部で EtherChannel テクノロジーを使用するため、スパンドモードではあらゆるタイプのデータインターフェイスが機能します。



(注) 管理インターフェイス以外の個々のインターフェイスはサポートされていません。

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

ここでは、クラスタリングの概念と実装について詳しく説明します。[クラスタリングの参考資料 \(40 ページ\)](#) も参照してください。

ブートストラップコンフィギュレーション

クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ構成が Firepower 9300 シャーシスーパーバイザからプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部はユーザが設定できます。

クラスタメンバー

クラスタメンバーは連携して動作し、セキュリティポリシーおよびトラフィックフローの共有を達成します。

クラスタ内のメンバの 1 つが **マスター** ユニットです。マスターユニットは自動的に決定されます。他のすべてのメンバは **スレーブ** ユニットです。

すべてのコンフィギュレーション作業はマスターユニット上でのみ実行する必要があります。コンフィギュレーションはその後、スレーブユニットに複製されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能についてはマスターユニットがすべてのトラフィックを処理します。[クラスタリングの中央集中型機能（6 ページ）](#) を参照してください。。

マスターおよびスレーブ ユニットの役割

クラスタ内のメンバの 1 つがマスター ユニットです。マスター ユニットは自動的に決定されます。他のすべてのメンバはスレーブ ユニットです。

すべてのコンフィギュレーション作業はマスターユニット上でのみ実行する必要があります。コンフィギュレーションはその後、スレーブ ユニットに複製されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能についてはマスターユニットがすべてのトラフィックを処理します。[クラスタリングの中央集中型機能（6 ページ）](#) を参照してください。。

クラスタ制御リンク

クラスタ制御リンクはユニット間通信用の EtherChannel（ポートチャンネル 48）です。シャーシ内クラスタリングでは、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- マスター選定。
- コンフィギュレーションの複製
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスタ制御リンク ネットワーク

Firepower 9300 シャーシは、シャーシ ID およびスロット ID (`127.2.chassis_id.slot_id`) に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。FXOS とアプリケーション内のどちらでも、この IP アドレスを手動で設定することはできません。クラスタ制御リンク ネットワークには、ユニット間のルータを含めることはできません。レイヤ 2 スイッチングのみが許可されます。

クラスタ インターフェイス

シャーシ内クラスタリングでは、物理インターフェイス、EtherChannel（ポートチャネルとも呼ばれる）の両方を割り当てることができます。クラスタに割り当てられたインターフェイスはクラスタ内のすべてのメンバーのトラフィックのロードバランシングを行うスパンドインターフェイスです。

管理インターフェイス以外の個々のインターフェイスはサポートされていません。

VSS または vPC への接続

インターフェイスに冗長性を確保するため、EtherChannel を VSS または vPC に接続することを推奨します。

設定の複製

クラスタ内のすべてのユニットは、単一のコンフィギュレーションを共有します。コンフィギュレーション変更を加えることができるのはマスターユニット上だけであり、変更は自動的にクラスタ内の他のすべてのユニットに同期されます。

ASA クラスタの管理

ASA クラスタリングを使用することの利点の1つは、管理のしやすさです。ここでは、クラスタを管理する方法について説明します。

管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンドインターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各単位に直接接続できます。

メインクラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在のマスターユニットに属します。アドレス範囲も設定して、現在のマスターを含む各ユニットがその範囲内のローカルアドレスを使用できるようにします。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。マスターユニットが変更されると、メインクラスタ IP アドレスは新しいマスターユニットに移動するので、クラスタの管理をシームレスに続行できます。

たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在のマスターユニットに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。

TFTP や syslog などの発信管理トラフィックの場合、マスターユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバに接続します。

マスターユニット管理とスレーブユニット管理

すべての管理とモニタリングはマスターユニットで実行できます。マスターユニットから、すべてのユニットの実行時統計情報やリソース使用状況などのモニタリング情報を調べることができます。また、クラスタ内のすべてのユニットに対してコマンドを発行することや、コンソールメッセージをスレーブユニットからマスターユニットに複製することもできます。

必要に応じて、スレーブユニットを直接モニタできます。マスターユニットからでもできますが、ファイル管理をスレーブユニット上で実行できます（コンフィギュレーションのバックアップや、イメージの更新など）。次の機能は、マスターユニットからは使用できません。

- ユニットごとのクラスタ固有統計情報のモニタリング。
- ユニットごとの Syslog モニタリング（コンソール レプリケーションが有効な場合にコンソールに送信される syslog を除く）。
- SNMP
- NetFlow

RSA キー複製

マスターユニット上で RSA キーを作成すると、そのキーはすべてのスレーブユニットに複製されます。メインクラスタ IP アドレスへの SSH セッションがある場合に、マスターユニットで障害が発生すると接続が切断されます。新しいマスターユニットは、SSH 接続に対して同じキーを使用するので、新しいマスターユニットに再接続するときに、キャッシュ済みの SSH ホスト キーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメインクラスタ IP アドレスに接続する場合は、IP アドレス不一致に関する警告メッセージが表示されます。これは、証明書で使用されているのがローカル IP アドレスであり、メインクラスタ IP アドレスではないからです。このメッセージは無視して、ASDM 接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメインクラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。

ASA の各機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部はマスターユニットだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

これらの機能は、クラスタリングがイネーブルのときは設定できず、コマンドは拒否されません。

- TLS プロキシを使用するユニファイド コミュニケーション機能
- 次のアプリケーション インспекション：
 - CTIQBE
 - GTP
 - H323、H225、および RAS
 - IPsec パススルー
 - MGCP
 - MMP
 - RTSP
 - SCCP (Skinny)
 - WAAS
 - WCCP
- Botnet Traffic Filter
- Auto Update Server
- DHCP クライアント、サーバ、およびプロキシDHCP リレーがサポートされている。
- フェールオーバー
- デッド接続検出 (DCD)

クラスタリングの中央集中型機能

次の機能は、マスターユニット上だけでサポートされます。クラスタの場合もスケーリングされません。



(注) 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバユニットからマスターユニットに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、マスター以外のユニットに転送されることがあります。この場合は、トラフィックがマスターユニットに送り返されます。

中央集中型機能については、マスターユニットで障害が発生するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

• 次のアプリケーションインスペクション :

- DCERPC
 - NetBIOS
 - PPTP
 - RADIUS
 - RSH
 - SUNRPC
 - TFTP
 - XDMCP
-
- ダイナミック ルーティング
 - スタティック ルート モニタリング
 - IGMP マルチキャスト コントロール プレーン プロトコル 処理 (データ プレーン フォワーディングはクラスタ全体に分散されます)
 - PIM マルチキャスト コントロール プレーン プロトコル 処理 (データ プレーン 転送はクラスタ全体に分散されます)
 - ネットワーク アクセスの認証および許可。アカウントリングは非集中型です。
 - フィルタリング サービス

個々のユニットに適用される機能

これらの機能は、クラスタ全体またはマスターユニットではなく、各 ASA ユニットに適用されます。

- QoS : QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは、各ユニットに対して個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。3 ユニットから成るクラスタがあり、トラ

フィックが均等に分散している場合は、適合レートは実際にクラスタのレートの3倍になります。

- 脅威検出：脅威検出は、各ユニットに対して個別に機能します。たとえば、上位統計情報は、ユニット別です。たとえば、ポート スキャン検出が機能しないのは、スキャントラフィックが全ユニット間で分散されるので、1つのユニットがすべてのトラフィックを読み取ることはないからです。
- リソース管理：マルチ コンテキスト モードでのリソース管理は、ローカル使用状況に基づいて各ユニットに個別に適用されます。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウントिंगの3つのコンポーネントで構成されます。認証および許可は、クラスタリングマスター上で中央集中型機能として実装されており、データ構造がクラスタスレーブに複製されます。マスターが選定されたときは、確立済みの認証済みユーザおよびユーザに関連付けられた許可を引き続き中断なく運用するのに必要なすべての情報を、新しいマスターが保有します。ユーザ認証のアイドルおよび絶対タイムアウトは、マスターユニット変更が発生したときも維持されます。

アカウントिंगは、クラスタ内の分散型機能として実装されています。アカウントINGはフロー単位で実行されるので、フローを所有するクラスタユニットがアカウントING開始と停止のメッセージを AAA サーバに送信します（フローに対するアカウントINGが設定されているとき）。

FTP とクラスタリング

- FTPデータチャンネルとコントロールチャンネルのフローがそれぞれ別のクラスタメンバによって所有されている場合は、データチャンネルのオーナーは定期的にアイドルタイムアウトアップデートをコントロールチャンネルのオーナーに送信し、アイドルタイムアウト値を更新します。ただし、コントロールフローのオーナーがリロードされて、コントロールフローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロールフローのアイドルタイムアウトは更新されません。
- FTPアクセスにAAAを使用している場合、制御チャンネルのフローはマスターユニットに集中化されます。

アイデンティティ ファイアウォールとクラスタリング

マスターユニットのみがADからuser-groupを取得し、ADエージェントからuser-ipマッピングを取得します。マスターユニットからユーザ情報がスレーブに渡されるので、スレーブは、セキュリティポリシーに基づいてユーザIDの一致の決定を行うことができます。

マルチキャストルーティングとクラスタリング

ファーストパス転送が確立されるまでの間、マスターユニットがすべてのマルチキャストルーティングパケットとデータパケットを処理します。接続が確立された後は、各スレーブがマルチキャストデータパケットを転送できます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。着信および発信の NAT パケットが、クラスタ内のそれぞれ別の ASA に送信されることがあります。これは、ロードバランシングアルゴリズムは IP アドレスとポートに依存していますが、NAT が使用される場合、着信と発信でパケットの IP アドレスやポートが異なるためです。NAT オーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるので、大量のトラフィックがクラスタ制御リンク上で発生します。NAT オーナーはセキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成するため、受信側ユニットは転送フローをオーナーに作成しません。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

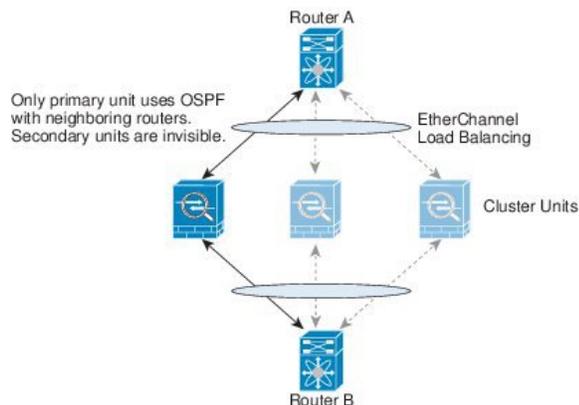
- **ダイナミック PAT 用 NAT プールアドレス分散**：マスターユニットは、アドレスをクラスタ全体に均等に分配します。メンバーが接続を受信したときに、そのメンバーのアドレスが1つも残っていない場合は、接続はドロップされます（他のメンバーにはまだ使用可能なアドレスがある場合でも）。最低でも、クラスタ内のユニットと同数の NAT アドレスが含まれていることを確認してください。各ユニットが確実に1つのアドレスを受け取るようにするためです。アドレス割り当てを表示するには、**show nat pool cluster** コマンドを使用します。
- **ラウンドロビンなし**：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- **マスターユニットによって管理されるダイナミック NAT xlate**：マスターユニットが xlate テーブルを維持し、スレーブユニットに複製します。ダイナミック NAT を必要とする接続をスレーブユニットが受信したときに、その xlate がテーブル内にない場合は、スレーブはマスターユニットに xlate を要求します。スレーブユニットが接続を所有します。
- **Per-session PAT 機能**：クラスタリングに限りませんが、Per-session PAT 機能によって PAT のスケーラビリティが向上します。クラスタリングの場合は、各スレーブユニットが独自の PAT 接続を持てるようになります。対照的に、Multi-Session PAT 接続はマスターユニットに転送する必要があり、マスターユニットがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックは per-session PAT xlate を使用します。これに対し、ICMP および他のすべての UDP トラフィックは multi-session を使用します。TCP および UDP に対しこれらのデフォルトを変更するように per-session NAT ルールを設定できますが、ICMP に per-session PAT を設定することはできません。H.323、SIP、または Skinny などの multi-session PAT のメリットを活用できるトラフィックでは、関連付けられている TCP ポートに対し per-session PAT を無効にできます（それらの H.323 および SIP の UDP ポートはデフォルトですでに multi-session になっています）。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

- 次のインスペクション用のスタティック PAT はありません。
 - FTP
 - PPTP
 - RSH
 - SQLNET
 - TFTP
 - XDMCP
 - SIP

ダイナミック ルーティングおよびクラスタリング

ルーティング プロセスはマスター ユニット上だけで実行されます。ルートはマスター ユニットを介して学習され、セカンダリに複製されます。ルーティング パケットがスレーブに到着した場合は、マスター ユニットにリダイレクトされます。

図 1: ダイナミック ルーティング



スレーブ メンバがマスター ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、マスター ユニットからスレーブ ユニットに同期されません。マスターユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

SIP インспекションとクラスタリング

制御フローは、任意のユニットで作成できます（ロードバランシングのため）。その子データフローは同じユニットに存在する必要があります。

TLS プロキシ設定はサポートされていません。

SNMP とクラスタリング

SNMP エージェントは、個々の ASA を、そのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メインクラスタ IP アドレスではなく、常にローカルアドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合は、新しいマスターが選定されたときに、新しいマスターユニットのポーリングに失敗します。

syslog および NetFlow とクラスタリング

- **Syslog** : クラスタの各ユニットは自身の syslog メッセージを生成します。各ユニットの syslog メッセージヘッダー フィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名コンフィギュレーションはクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようロギングを設定した場合は、どのユニットで生成された syslog メッセージも 1 つのユニットからのように見えます。クラスタ ブートストラップ コンフィギュレーションで割り当てられたローカルユニット名をデバイス ID として使用するようロギングを設定した場合は、syslog メッセージはそれぞれ別のユニットからのように見えます。
- **NetFlow** : クラスタの各ユニットは自身の NetFlow ストリームを生成します。NetFlow コレクタは、各 ASA を独立した NetFlow エクスポートとしてのみ扱うことができます。

Cisco TrustSec とクラスタリング

マスターユニットだけがセキュリティ グループ タグ (SGT) 情報を学習します。マスターユニットからこの SGT がスレーブに渡されるので、スレーブは、セキュリティ ポリシーに基づいて SGT の一致決定を下せます。

Firepower9300シャーシでのクラスタリングの要件と前提条件

モデルあたりの最大クラスタリングユニット

- Firepower 9300 : 16 モジュール。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。

スイッチ要件

- Firepower 9300 シャーシのクラスタリングを設定する前に、スイッチの設定を完了し、シャーシからスイッチまですべての EtherChannel を良好に接続してください。
- サポートされているスイッチのリストについては、「[Cisco FXOS Compatibility](#)」を参照してください。

上のクラスタリングのライセンス Firepower 9300 シャーシ

マスターユニットでのみライセンスを要求できます。ライセンスはスレーブユニットでは集約されます。複数のユニットにライセンスがある場合は、これらが統合されて単一の実行 ASA クラスタ ライセンスとなります。マスターユニットで完了したライセンス設定はスレーブユニットに複製されません。クラスタリングを無効にし、ライセンスを設定し、クラスタリングを再度有効にした場合限り、スレーブユニットに個別のライセンス権限付与を設定できます。



- (注) ASDM や他の高度暗号機能を使用するには、クラスタ展開後にマスターユニットで ASA CLI を使用して高度暗号化 (3DES) ライセンスを有効にする必要があります。このライセンスは、スレーブユニットによって継承されます。このライセンスは、各ユニットで個別に設定する必要はありません。高度暗号化 (3DES) ライセンスの評価ライセンスは一切ありません。



- (注) マスターユニットに障害が発生し、30 日 (ライセンス猶予期間) 以内に再参加しない場合、継承されたライセンスは消滅します。その場合、新しいマスターユニットに消滅したライセンスを手動で設定する必要があります。

クラスタリング ガイドラインと制限事項

- 大々的なトポロジ変更が発生する場合（EtherChannel インターフェイスの追加または削除、Firepower 9300 シャーシ上でのインターフェイスまたはスイッチの有効化または無効化、VSS または vPC を形成するための追加スイッチの追加など）、ヘルス チェック機能や無効なインターフェイスのインターフェイスモニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。
- ユニットの既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel インターフェイスに接続された Windows 2003 Server を使用している場合、syslog サーバポートがダウンしたときにサーバが ICMP エラーメッセージを抑制しないと、多数の ICMP メッセージがクラスタに送信されることとなります。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラーメッセージを調節することを推奨します。
- 冗長性を持たせるため、VSS または vPC に EtherChannel を接続することを推奨します。
- シャーシ内では、スタンドアロン モードで一部のシャーシセキュリティ モジュールをクラスタ化し、他のセキュリティモジュールを実行することはできません。クラスタ内にすべてのセキュリティ モジュールを含める必要があります。

デフォルト

- クラスタのヘルス チェック機能は、デフォルトでイネーブルになり、ホールド時間は 3 秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングがイネーブルになっています。
- 接続再分散は、デフォルトでは無効になっています。接続再分散を有効にした場合の、デフォルトの負荷情報交換間隔は 5 秒です。

クラスタリングの設定 Firepower 9300 シャーシ

クラスタは、Firepower 9300 シャーシスーパーバイザから簡単に展開できます。すべての初期設定が各ユニットに自動的に生成されます。このセクションでは、デフォルトのブートストラップ設定と ASA で実行できるオプションのカスタマイズについて説明します。また、ASA 内からクラスタメンバーを管理する方法についても説明します。クラスタメンバーシップは Firepower 9300 シャーシからも管理できます。詳細については、Firepower 9300 シャーシのマニュアルを参照してください。

手順

-
- ステップ1 [FXOS : ASA クラスタの追加 \(14 ページ\)](#)
 - ステップ2 [ASA : ファイアウォール モードとコンテキスト モードの変更 \(21 ページ\)](#)
 - ステップ3 [ASA : データ インターフェイスの設定 \(22 ページ\)](#)
 - ステップ4 [ASA : クラスタ設定のカスタマイズ \(25 ページ\)](#)
 - ステップ5 [ASA : クラスタ メンバの管理 \(31 ページ\)](#)
-

FXOS : ASA クラスタの追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、することもできます。

ASA クラスタの作成

クラスタは、Firepower 9300 シャーシスーパーバイザから簡単に展開できます。すべての初期設定が各ユニットに自動的に生成されます。

モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュールスロットでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

マルチコンテキストモードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチコンテキストモードを有効にする必要があります。

ASA をトランスペアレントファイアウォールモードに変更するには、初期導入を完了し、ASA CLI 内でファイアウォールモードを変更します。

クラスタを導入すると、Firepower 9300 シャーシスーパーバイザが次のブートストラップコンフィギュレーションで各 ASA アプライアンスを設定します。ブートストラップコンフィギュレーションの一部 (**太字**のテキストで示されている部分) は、後から必要に応じて ASA から変更できます。

```
interface Port-channel48
  description Clustering Interface
  cluster group <service_type_name>
  key <secret>
  local-unit unit-<chassis#-module#>

  cluster-interface port-channel48 ip 127.2.<chassis#>.<module#> 255.255.255.0
  priority <auto>
  health-check holdtime 3
  health-check data-interface auto-rejoin 3 5 2
  health-check cluster-interface auto-rejoin unlimited 5 1
  enable

ip local pool cluster_ipv4_pool <ip_address>-<ip_address> mask <mask>

interface <management_ifc>
```

```

management-only individual
nameif management
security-level 0
ip address <ip_address> <mask> cluster-pool cluster_ipv4_pool
no shutdown

http server enable
http 0.0.0.0 0.0.0.0 management
route management <management_host_ip> <mask> <gateway_ip> 1

```



(注) **local-unit** 名は、クラスタリングを無効化した場合にのみ変更できます。

始める前に

- 論理デバイスに使用するアプリケーションイメージを Cisco.com からダウンロードして、そのイメージを Firepower 9300 シャーシにアップロードします。
- 次の情報を用意します。
 - 管理インターフェイス ID、IP アドレス、およびネットワーク マスク
 - ゲートウェイ IP アドレス

手順

ステップ 1 インターフェイスを設定します。

- a) クラスタを展開する前に、1つ以上のデータタイプのインターフェイスまたは EtherChannel (ポートチャネルとも呼ばれる) を追加します。

デフォルトでは、すべてのインターフェイスがクラスタに割り当てられます。導入後にもクラスタにデータ インターフェイスを追加できます。

- b) 管理タイプのインターフェイスまたは EtherChannel を追加します。

管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません (FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前が表示されます)。

ステップ 2 セキュリティ サービス モードを開始します。

scope ssa

例 :

```

Firepower# scope ssa
Firepower /ssa #

```

ステップ 3 デフォルトのイメージバージョンを設定します。

- a) 使用可能なイメージを表示します。使用するバージョン番号をメモします。

show app

例 :

```
Firepower /ssa # show app
  Name      Version      Author      Supported Deploy Types CSP Type      Is
Default App
-----
asa         9.9.1         cisco       Native      Application No
asa         9.10.1        cisco       Native      Application Yes
ftd         6.2.3         cisco       Native      Application Yes
```

- b) 範囲をイメージバージョンに設定します。

scope app asa application_version

例 :

```
Firepower /ssa # scope app asa ftd 9.10.1
Firepower /ssa/app #
```

- c) このバージョンをデフォルトとして設定します。

set-default

例 :

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

- d) 終了して ssa モードを開始します。

exit

例 :

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

例 :

```
Firepower /ssa # scope app asa 9.12.1
Firepower /ssa/app # set-default
Firepower /ssa/app* # exit
Firepower /ssa* #
```

ステップ 4 クラスタを作成します。**enter logical-device device_name asa slots clustered**

- *device_name* : Firepower 9300 シャーシスーパーバイザがクラスタリングを設定してインターフェイスを割り当てるために使用します。この名前は、セキュリティモジュール設定で使

用されるクラスタ名ではありません。まだハードウェアをインストールしていなくても、3つのセキュリティ モジュールすべてを指定する必要があります。

- スロット: シャーシモジュールをクラスタに割り当てます。Firepower 4100 の場合は、**1** を指定します。Firepower 9300 の場合は、**1、2、3** を指定します。モジュールがインストールされていない場合でも、Firepower 9300 シャーシの3つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3つすべてのモジュールを設定していないと、クラスタは機能しません。

例 :

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

ステップ5 クラスタ ブートストラップ パラメータを設定します。

これらの設定は、初期導入専用、またはディザスタリカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

- a) クラスタ ブートストラップ オブジェクトを作成します。

enter cluster-bootstrap

例 :

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- b) クラスタ制御リンクの制御トラフィックの認証キーを設定します。

set key

例 :

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

共有秘密を入力するように求められます。

共有秘密は、1～63文字のASCII文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパストラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパストラフィックは、常にクリアテキストとして送信されます。

- c) クラスタ インターフェイス モードを設定します。

set mode spanned-etherchannel

スパンド EtherChannel モードは、サポートされている唯一のモードです。

例 :

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
```

```
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- d) セキュリティ モジュール設定のクラスタ グループ名を設定します。

```
set service-type cluster_name
```

名前は 1 ～ 38 文字の ASCII 文字列である必要があります。

例 :

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- e) 管理 IP アドレス情報を設定します。

この情報は、セキュリティモジュール設定で管理インターフェイスを設定するために使用されます。

- ローカル IP アドレスのプールを設定します。このアドレスの 1 つが、このインターフェイス用に各クラスタユニットに割り当てられます。

```
set ipv4 pool start_ip end_ip
```

```
set ipv6 pool start_ip end_ip
```

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。Firepower 9300 の場合、すべてのモジュールスロットが埋まっていないとしても、シャーシごとに 3 つのアドレスを含める必要があることに注意してください。クラスタを拡張する予定の場合は、アドレスを増やします。現在のマスターユニットに属する仮想 IP アドレス（メインクラスタ IP アドレスと呼ばれる）は、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つをメインクラスタ IP アドレス用に確保してください。IPv4 アドレスと IPv6 アドレス（どちらか一方も可）を使用できます。

- 管理インターフェイスのメインクラスタ IP アドレスを設定します。

```
set virtual ipv4 ip_address mask mask
```

```
set virtual ipv6 ip_address prefix-length prefix
```

この IP アドレスは、クラスタ プールアドレスと同じネットワーク上に存在している必要がありますが、プールに含まれてはなりません。

- ネットワーク ゲートウェイ アドレスを入力します。

```
set ipv4 gateway ip_address
```

```
set ipv6 gateway ip_address
```

例 :

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11
2001:DB8::27
```

```
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1
prefix-length 64
```

- f) クラスタ ブートストラップ モードを終了します。

exit

例 :

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

ステップ 6 管理ブートストラップパラメータを設定します。

これらの設定は、初期導入専用、またはディザスタリカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

- a) 管理ブートストラップ オブジェクトを作成します。

enter mgmt-bootstrap asa

例 :

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- b) **admin** とを指定します。

create bootstrap-key-secret PASSWORD

set value

値の入力 : *password*

値の確認 : *password*

exit

例 :

事前設定されている ASA 管理者ユーザはパスワードの回復時に役立ちます。FXOS アクセスができる場合、管理者ユーザ パスワードを忘れたときにリセットできます。

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
```

```
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- c) 管理ブートストラップ モードを終了します。

exit

例 :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

- ステップ 7** 設定を保存します。

commit-buffer

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。**show app-instance** コマンドを使用して、導入のステータスを確認します。**[Admin State]** が **[Enabled]** で、**[Oper State]** が **[Online]** の場合、アプリケーションインスタンスは実行中であり、使用できる状態になっています。

例 :

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name      Identifier Slot ID      Admin State Oper State      Running Version Startup
Version Deploy Type Profile Name Cluster State   Cluster Role
-----
ftd           cluster1  1           Enabled      Online          6.4.0.49      6.4.0.49
Native
ftd           cluster1  2           Enabled      Online          6.4.0.49      6.4.0.49
Native
ftd           cluster1  3           Disabled     Not Available   6.4.0.49
Native
Not Applicable None
```

- ステップ 8** マスター ユニット ASA に接続して、クラスタリング設定をカスタマイズします。

例

シャーシ 1 :

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
    set port-type data
    enable
    enter member-port Ethernet1/1
    exit
    enter member-port Ethernet1/2
    exit
  exit
```

```
enter port-channel 2
  set port-type data
  enable
  enter member-port Ethernet1/3
  exit
  enter member-port Ethernet1/4
  exit
  exit
enter port-channel 3
  set port-type data
  enable
  enter member-port Ethernet1/5
  exit
  enter member-port Ethernet1/6
  exit
  exit
enter port-channel 4
  set port-type mgmt
  enable
  enter member-port Ethernet2/1
  exit
  enter member-port Ethernet2/2
  exit
  exit
exit
exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
  enter cluster-bootstrap
  set chassis-id 1
  set ipv4 gateway 10.1.1.254
  set ipv4 pool 10.1.1.11 10.1.1.27
  set ipv6 gateway 2001:DB8::AA
  set ipv6 pool 2001:DB8::11 2001:DB8::27
  set key
  Key: f@arscape
  set mode spanned-etherchannel
  set service-type cluster1
  set virtual ipv4 10.1.1.1 mask 255.255.255.0
  set virtual ipv6 2001:DB8::1 prefix-length 64
  exit
exit
scope app asa 9.5.2.1
  set-default
  exit
commit-buffer
```

ASA : ファイアウォール モードとコンテキスト モードの変更

デフォルトでは、FXOS シャーシはルーテッドまたはトランスペアレントファイアウォールモード、およびシングルコンテキストモードでクラスタを展開します。

- ファイアウォールモードの変更：展開後にモードを変更するには、マスターユニットでモードを変更します。モードは一致するようにすべてのスレーブユニットで自動的に変更されます。を参照してください。[ファイアウォールモードの設定](#)マルチコンテキストモードでは、コンテキストごとにファイアウォールモードを設定します。

- マルチ コンテキスト モードに変更：展開後にマルチ コンテキスト モードに変更するには、マスター ユニットのモードを変更します。これにより、すべてのスレーブユニットのモードは一致するように自動的に変更されます。[マルチ コンテキスト モードの有効化](#)を参照してください。

ASA : データ インターフェイスの設定

この手順では、FXOS にクラスタを展開したときにクラスタに割り当てられた各データ インターフェイスの基本的なパラメータを設定します。シャーシ間クラスタリングの場合、データ インターフェイスは常にスパンド EtherChannel インターフェイスです。



- (注) 管理インターフェイスは、クラスタを展開したときに事前設定されました。ASA で管理インターフェイス パラメータを変更することもできますが、この手順はデータ インターフェイスに焦点を当てています。管理インターフェイスは、スパンドインターフェイスとは対照的に、個別のインターフェイスです。詳細については、「[管理インターフェイス \(4 ページ\)](#)」を参照してください。

始める前に

- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで開始します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。
- トランスペアレント モードの場合は、ブリッジ グループを設定します。
- シャーシ間クラスタリングにスパンド EtherChannel を使用している場合、クラスタリングが完全に有効になるまで、ポートチャネルインターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

手順

ステップ 1 インターフェイス ID を指定します

interface id

このクラスタに割り当てられているインターフェイスのFXOSシャーシを参照してください。インターフェイス ID には、次のものがあります。

- **port-channel integer**
- **ethernet slot/port**

例 :

```
ciscoasa(config)# interface port-channel 1
```

ステップ 2 インターフェイスをイネーブルにします。

no shutdown

ステップ 3 (オプション) このインターフェイス上に VLAN サブインターフェイスを作成する予定の場合は、この時点で作成します。

例 :

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

この手順の残りの部分は、サブインターフェイスに適用されます。

ステップ 4 (マルチ コンテキスト モード) インターフェイスをコンテキストに割り当ててから、コンテキストに変更し、インターフェイス モードを開始します。

例 :

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

マルチ コンテキスト モードの場合は、インターフェイス コンフィギュレーションの残りの部分は各コンテキスト内で行われます。

ステップ 5 インターフェイスの名前を指定します。

nameif name

例 :

```
ciscoasa(config-if)# nameif inside
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。

ステップ 6 ファイアウォール モードに応じて、次のいずれかを実行します。

- ルーテッド モード : IPv4 アドレスと IPv6 アドレスの一方または両方を設定します。

(IPv4)

ip address ip_address [mask]

(IPv6)

ipv6 address ipv6-prefix/prefix-length

例 :

```
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
```

DHCP、PPPoE、および IPv6 自動設定はサポートされません。

- トランスペアレント モード : インターフェイスをブリッジグループに割り当てます。

bridge-group *number*

例 :

```
ciscoasa(config-if)# bridge-group 1
```

number は、1 ~ 100 の整数です。ブリッジグループには最大 4 個のインターフェイスを割り当てることができます。同一インターフェイスを複数のブリッジグループに割り当てることはできません。BVI のコンフィギュレーションには IP アドレスが含まれていることに注意してください。

ステップ 7 セキュリティ レベルを設定します。

security-level *number*

例 :

```
ciscoasa(config-if)# security-level 50
```

number には、0 (最下位) ~ 100 (最上位) の整数を指定します。

ステップ 8 (シャーシ間クラスタリング) 潜在的なネットワークの接続問題を回避するために、スバンド EtherChannel のグローバル MAC アドレスを設定します。

mac-address *mac_address*

- *mac_address* : MAC アドレスは、H.H.H 形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

MAC アドレスが手動設定されている場合、その MAC アドレスは現在のマスターユニットに留まります。MAC アドレスを設定していない場合に、マスターユニットが変更された場合、新しいマスターユニットはインターフェイスに新しい MAC アドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

マルチコンテキストモードでは、コンテキスト間でインターフェイスを共有する場合は、MAC アドレスの自動生成を有効にして、手動で MAC アドレスを設定しなくてすむようにします。非共有インターフェイスの場合は、このコマンドを使用して MAC アドレスを手動で設定する必要があることに注意してください。

例 :

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

ASA : クラスタ設定のカスタマイズ

クラスタを展開した後にブートストラップ設定を変更する場合や、クラスタリングヘルスモニタリング、TCP 接続複製の遅延、フローモビリティ、およびその他の最適化など、追加のオプションを設定する場合は、マスターユニットで行うことができます。

ASA クラスタの基本パラメータの設定

マスターユニット上のクラスタ設定をカスタマイズできます。

始める前に

- マルチコンテキストモードでは、マスターユニット上のシステム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- local-unit name** およびその他の複数のオプションは、FXOS シャーシでのみ設定することができます。また、それらのオプションは、クラスタリングを無効にしている場合に ASA でのみ変更できます。そのため、次の手順には含まれていません。

手順

ステップ 1 このユニットがマスターユニットであることを確認します。

show cluster info

例 :

```
asa(config)# show cluster info
Cluster cluster1: On
  Interface mode: spanned
  This is "unit-1-2" in state MASTER
    ID       : 2
    Version  : 9.5(2)
    Serial No.: FCH183770GD
    CCL IP   : 127.2.1.2
    CCL MAC  : 0015.c500.019f
    Last join : 01:18:34 UTC Nov 4 2015
    Last leave: N/A
Other members in the cluster:
  Unit "unit-1-3" in state SLAVE
    ID       : 4
    Version  : 9.5(2)
    Serial No.: FCH19057ML0
    CCL IP   : 127.2.1.3
    CCL MAC  : 0015.c500.018f
```

```

Last join : 20:29:57 UTC Nov 4 2015
Last leave: 20:24:55 UTC Nov 4 2015
Unit "unit-1-1" in state SLAVE
ID       : 1
Version  : 9.5(2)
Serial No.: FCH19057ML0
CCL IP   : 127.2.1.1
CCL MAC  : 0015.c500.017f
Last join : 20:20:53 UTC Nov 4 2015
Last leave: 20:18:15 UTC Nov 4 2015

```

別のユニットがマスターユニットの場合は、接続を終了し、正しいユニットに接続します。ASA コンソールへのアクセス方法の詳細については、[Cisco ASA for Firepower 4100 クイック スタート ガイド \[英語\]](#) または [Cisco ASA for Firepower 9300 クイック スタート ガイド \[英語\]](#) を参照してください。

ステップ 2 クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。

mtu cluster bytes

例 :

```
ciscoasa(config)# mtu cluster 9000
```

MTU の最大値を 9000 バイトに設定し、最小値を 1400 バイトに設定することをお勧めします。

ステップ 3 クラスタの設定モードを開始します。

cluster group name

ステップ 4 (任意) スレーブユニットからマスターユニットへのコンソール複製をイネーブルにします。

console-replicate

この機能はデフォルトで無効に設定されています。ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力します。コンソール複製をイネーブルにすると、スレーブユニットからマスターユニットにコンソールメッセージが送信されるので、モニタが必要になるのはクラスタのコンソールポート 1 つだけとなります。

ステップ 5 (任意) LACP のダイナミック ポートの優先順位を無効にします。

clacp static-port-priority

一部のスイッチはダイナミック ポート プライオリティをサポートしていないため、このコマンドはスイッチの互換性を高めます。さらに、このコマンドは、9 ~ 32 のアクティブ スパンド EtherChannel メンバーのサポートをイネーブルにします。このコマンドを使用しないと、サポートされるのは 8 個のアクティブ メンバと 8 個のスタンバイ メンバのみです。このコマンドをイネーブルにした場合、スタンバイ メンバは使用できません。すべてのメンバがアクティブです。

のヘルス モニタリングの設定

この手順では、ユニットとインターフェイスのヘルス モニタリングを設定します。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。ポートチャンネル ID、または単一の物理インターフェイス ID をモニタできます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ 1 クラスタの設定モードを開始します。

```
cluster group name
```

ステップ 2 クラスタ ユニットのヘルス チェック機能を次のようにカスタマイズします。

```
health-check [holdtime timeout]
```

holdtime は、ユニットのキープアライブステータスメッセージの間隔を指定します。指定できる範囲は .8 ~ 45 秒で、デフォルトは 3 秒です。

ユニットのヘルスを確認するため、ASA のクラスタ ユニットはクラスタ制御リンクで他のユニットにキープアライブメッセージを送信します。ユニットが保留時間内にピアユニットからキープアライブメッセージを受信しない場合は、そのピアユニットは応答不能またはデッド状態と見なされます。

何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ASA、Firepower 9300 シャーシ、またはスイッチ上のインターフェイスの有効化/無効化、VSS または vPC を形成するスイッチの追加）を行うときには、ヘルス チェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください（**no health-check monitor-interface**）。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。

例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

ステップ 3 インターフェイスでインターフェイスヘルス チェックを次のように無効化します。

```
no health-check monitor-interface [interface_id]
```

インターフェイスのヘルスチェックはリンク障害をモニタします。特定の論理インターフェイスのすべての物理ポートが、特定のユニット上では障害が発生したが、別のユニット上の同じ論理インターフェイスでアクティブポートがある場合、そのユニットはクラスタから削除されます。ASA がメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。

デフォルトでは、ヘルスチェックはすべてのインターフェイスでイネーブルになっています。このコマンドの **no** 形式を使用してディセーブルにすることができます。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。ヘルスモニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ASA、Firepower 9300 シャーシ、またはスイッチ上のインターフェイスの有効化/無効化、VSS または vPC を形成するスイッチの追加）を行うときには、ヘルスチェック機能 (**no health-check**) を無効にし、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルスチェック機能を再度イネーブルにできます。

例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface port-channel1
```

ステップ 4 シャーシのヘルスチェック間隔を設定します。

app-agent heartbeat [interval ms] [retry-count number]

- **interval ms** : ハートビートの時間間隔を 300 ~ 6000 ms の範囲の 100 の倍数単位で設定します。デフォルトは 1000 ms です。
- **retry-count number** : 再試行の回数を 1 ~ 30 の範囲の値に設定します。デフォルトの試行回数は 3 回です。

ASA はホストの Firepower シャーシとのバックプレーンを介して通信できるかどうかをチェックします。

例：

```
ciscoasa(cfg-cluster)# app-agent heartbeat interval 300
```

接続の再分散

接続の再分散を設定できます。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group name

ステップ 2 (オプション) TCP トラフィックの接続の再分散を有効化します。

conn-rebalance [frequency seconds]

例 :

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

このコマンドは、デフォルトでディセーブルになっています。有効化されている場合は、ASA は負荷情報を定期的に交換し、新しい接続の負荷を高負荷のデバイスから低負荷のデバイスに移動します。負荷情報を交換する間隔を、1 ~ 360 秒の範囲内で指定します。デフォルトは 5 秒です。

FXOS : クラスタ メンバの削除

ここでは、メンバを一時的に、またはクラスタから永続的に削除する方法について説明します。

一時的な削除

たとえば、ハードウェアまたはネットワークの障害が原因で、クラスタメンバはクラスタから自動的に削除されます。この削除は、条件が修正されるまでの一時的なものであるため、クラスタに再参加できます。また、手動でクラスタリングを無効にすることもできます。

デバイスが現在クラスタ内にあるかどうかを確認するには、**show cluster info** コマンドを使用してアプリケーション内のクラスタ ステータスを確認します。

```
ciscoasa# show cluster info
Clustering is not enabled
```

- アプリケーションでのクラスタリングの無効化 : アプリケーション CLI を使用してクラスタリングを無効にすることができます。**cluster remove unit name** コマンドを入力して、ログインしているユニット以外のすべてのユニットを削除します。ブートストラップ コンフィギュレーションは変更されず、マスターユニットから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスターユニットを削除するためにスレーブ ユニットでこのコマンドを入力した場合は、新しいマスターユニットが選定されます。

デバイスが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。

クラスタリングを再度有効にするには、ASA で **cluster group name** を入力してから **enable** を入力します。

- アプリケーション インスタンスの無効化 : FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # scope slot 1
Firepower-chassis /ssa/slot # scope app-instance asa asal
Firepower-chassis /ssa/slot/app-instance # disable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

再度有効にするには、次の手順を実行します。

```
Firepower-chassis /ssa/slot/app-instance # enable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

- セキュリティ モジュール/エンジンのシャットダウン : FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope service-profile server 1/1
Firepower-chassis /org/service-profile # power down soft-shut-down
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

電源を投入するには、次の手順を実行します。

```
Firepower-chassis /org/service-profile # power up
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

- シャーシのシャットダウン : FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # shutdown no-prompt
```

完全な削除

次の方法を使用して、クラスタ メンバを完全に削除できます。

- 論理デバイスの削除 : FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # delete logical-device cluster1
Firepower-chassis /ssa* # commit-buffer
Firepower-chassis /ssa #
```

- サービスからのシャーシまたはセキュリティ モジュールの削除 : サービスからデバイスを削除する場合は、交換用ハードウェアをクラスタの新しいメンバーとして追加できます。

ASA : クラスタ メンバの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタ メンバを管理できます。

非アクティブなメンバーになる

クラスタの非アクティブなメンバーになるには、クラスタリングコンフィギュレーションは変更せずに、そのユニット上でクラスタリングをディセーブルにします。



- (注) ASAが（手で、またはヘルスチェックエラーにより）非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開させるには、クラスタリングを再びイネーブルにします。または、そのユニットをクラスタから完全に削除します。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

始める前に

- コンソールポートを使用する必要があります。クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

ステップ 1 クラスタの設定モードを開始します。

```
cluster group name
```

例 :

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをディセーブルにします。

```
no enable
```

このユニットがマスターユニットであった場合は、新しいマスターの選定が実行され、別のメンバーがマスターユニットになります。

クラスタコンフィギュレーションは維持されるので、後でクラスタリングを再度イネーブルにできます。

メンバーの非アクティブ化

ログインしているユニット以外のメンバーを非アクティブにするには、次のステップを実行します。



- (注) ASAが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもユニットがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

ユニットをクラスタから削除します。

cluster remove unit *unit_name*

ブートストラップ コンフィギュレーションは変更されず、マスターユニットから最後に同期されたコンフィギュレーションもそのままになるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスターユニットを削除するためにスレーブユニットでこのコマンドを入力した場合は、新しいマスターユニットが選定されます。

メンバーを一覧表示するには、**cluster remove unit ?** と入力するか、**show cluster info** コマンドを入力します。

例 :

```
ciscoasa(config)# cluster remove unit ?
Current active units in the cluster:
asa2
```

```
ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

クラスタへの再参加

ユニットがクラスタから削除された場合（たとえば、障害が発生したインターフェイスの場合、またはメンバーを手動で非アクティブにした場合）は、クラスタに手動で再参加する必要があります。

始める前に

- クラスタリングを再イネーブルするには、コンソールポートを使用する必要があります。他のインターフェイスはシャットダウンされます。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。
- クラスタへの再参加を試行する前に、障害が解決されていることを確認します。

手順

ステップ 1 コンソールで、クラスタ コンフィギュレーション モードを開始します。

cluster group name

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをイネーブルにします。

enable

マスターユニットの変更



注意 マスターユニットを変更する最良の方法は、マスターユニットでクラスタリングを無効にし、新しいマスターの選択を待ってから、クラスタリングを再度有効にする方法です。マスターにするユニットを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用してマスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

マスターユニットを変更するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

新しいユニットをマスター ユニットとして設定します。

cluster master unit *unit_name*

例 :

```
ciscoasa(config)# cluster master unit asa2
```

メイン クラスタ IP アドレスへの再接続が必要になります。

メンバ名を一覧表示するには、**cluster master unit ?**（現在のユニットを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

クラスタ全体でのコマンドの実行

コマンドをクラスタ内のすべてのメンバに、または特定のメンバに送信するには、次の手順を実行します。**show** コマンドをすべてのメンバーに送信すると、すべての出力が収集されて現在のユニットのコンソールに表示されます。（または、マスターユニットで **show** コマンドを入力するとクラスタ全体の統計情報を表示できます。）**capture** や **copy** などのその他のコマンドも、クラスタ全体での実行を活用できます。

手順

コマンドをすべてのメンバに送信します。ユニット名を指定した場合は、特定のメンバに送信されます。

cluster exec [unit unit_name] コマンド

例 :

```
ciscoasa# cluster exec show xlate
```

メンバー名を表示するには、**cluster exec unit ?** コマンドを入力するか（現在のユニットを除くすべての名前を表示する場合）、**show cluster info** コマンドを入力します。

例

同じキャプチャ ファイルをクラスタ内のすべてのユニットから同時に TFTP サーバにコピーするには、マスター ユニットで次のコマンドを入力します。

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ユニットから1つずつ）が TFTP サーバにコピーされます。宛先のキャプチャファイル名には自動的にユニット名が付加され、**capture1_asa1.pcap**、**capture1_asa2.pcap** などとなります。この例では、**asa1** および **asa2** がクラスタユニット名です。

次の **cluster exec show memory** コマンドの出力例では、クラスタの各メンバーのメモリ情報が表示されています。

```
ciscoasa# cluster exec show memory
unit-1-1 (LOCAL):*****
Free memory:      108724634538 bytes (92%)
Used memory:      9410087158 bytes ( 8%)
-----
Total memory:     118111600640 bytes (100%)

unit-1-3:*****
Free memory:      108749922170 bytes (92%)
Used memory:      9371097334 bytes ( 8%)
-----
Total memory:     118111600640 bytes (100%)

unit-1-2:*****
Free memory:      108426753537 bytes (92%)
Used memory:      9697869087 bytes ( 8%)
-----
Total memory:     118111600640 bytes (100%)
```

ASA : での ASA クラスタのモニタリング Firepower 9300 シャーシ

クラスタの状態と接続をモニタおよびトラブルシューティングできます。

クラスタ ステータスのモニタリング

クラスタの状態のモニタリングについては、次のコマンドを参照してください。

- **show cluster info [health], show cluster chassis info**

キーワードを指定しないで **show cluster info** コマンドを実行すると、クラスタ内のすべてのメンバーのステータスが表示されます。

show cluster info health コマンドは、インターフェイス、ユニットおよびクラスタ全体の現在の状態を表示します。

show cluster info コマンドの次の出力を参照してください。

```
asa(config)# show cluster info
Cluster cluster1: On
  Interface mode: spanned
  This is "unit-1-2" in state MASTER
    ID       : 2
    Version  : 9.5(2)
    Serial No.: FCH183770GD
    CCL IP   : 127.2.1.2
    CCL MAC  : 0015.c500.019f
    Last join : 01:18:34 UTC Nov 4 2015
    Last leave: N/A
  Other members in the cluster:
    Unit "unit-1-3" in state SLAVE
      ID       : 4
      Version  : 9.5(2)
      Serial No.: FCH19057ML0
      CCL IP   : 127.2.1.3
      CCL MAC  : 0015.c500.018f
      Last join : 20:29:57 UTC Nov 4 2015
      Last leave: 20:24:55 UTC Nov 4 2015
    Unit "unit-1-1" in state SLAVE
      ID       : 1
      Version  : 9.5(2)
      Serial No.: FCH19057ML0
      CCL IP   : 127.2.1.1
      CCL MAC  : 0015.c500.017f
      Last join : 20:20:53 UTC Nov 4 2015
      Last leave: 20:18:15 UTC Nov 4 2015
```

- **show cluster info transport {asp |cp}**

次のトランスポート関連の統計情報を表示します。

- **asp** : データプレーンのトランスポート統計情報。
- **cp** : コントロールプレーンのトランスポート統計情報。

- **show cluster history**

クラスタの履歴を表示します。

クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次のコマンドを参照してください。

cluster exec capture

クラスタ全体のトラブルシューティングをサポートするには、**cluster exec capture** コマンドを使用してマスターユニット上でのクラスタ固有トラフィックのキャプチャをイネーブルにします。これで、クラスタ内のすべてのスレーブユニットでも自動的にイネーブルになります。

クラスタ リソースのモニタリング

クラスタ リソースのモニタリングについては、次のコマンドを参照してください。

show cluster {cpu | memory | resource} [options]、show cluster chassis [cpu | memory | resource usage]

クラスタ全体の集約データを表示します。使用可能なオプションはデータのタイプによって異なります。

クラスタ トラフィックのモニタリング

クラスタ トラフィックのモニタリングについては、次のコマンドを参照してください。

- **show conn [detail | count]、cluster exec show conn**

show conn コマンドは、フローがディレクタ、バックアップ、またはフォワーダフローのいずれであるかを示します。**cluster exec show conn** コマンドを任意のユニットで使用すると、すべての接続が表示されます。このコマンドの表示からは、1つのフローのトラフィックがクラスタ内のさまざまな ASA にどのように到達するかがわかります。クラスタのスループットは、ロードバランシングの効率とコンフィギュレーションによって異なります。このコマンドを利用すると、ある接続のトラフィックがクラスタ内をどのように流れるかが簡単にわかります。また、ロードバランサがフローのパフォーマンスにどのように影響を与えるかを理解するのに役立ちます。

次に、**show conn detail** コマンドの出力例を示します。

```
ciscoasa/ASA2/slave# show conn detail
15 in use, 21 most used
Cluster:
  fwd connections: 0 in use, 0 most used
  dir connections: 0 in use, 0 most used
```

```

        centralized connections: 0 in use, 44 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
B - initial SYN from outside, b - TCP state-bypass or nailed,
C - CTIQBE media, c - cluster centralized,
D - DNS, d - dump, E - outside back connection, e - semi-distributed,
F - outside FIN, f - inside FIN,
G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
k - Skinny media, L - LISP triggered flow owner mobility
M - SMTP data, m - SIP media, n - GUP
N - inspected by Snort
O - outbound data, o - offloaded,
P - inside back connection,
Q - Diameter, q - SQL*Net data,
R - outside acknowledged FIN,
R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
V - VPN orphan, W - WAAS,
w - secondary domain backup,
X - inspected by service module,
x - per session, Y - director stub flow, y - backup stub flow,
Z - Scansafe redirection, z - forwarding stub flow

Cluster units to ID mappings:
ID 0: unit-2-1
ID 1: unit-1-1
ID 2: unit-1-2
ID 3: unit-2-2
ID 4: unit-2-3
ID 255: The default cluster member ID which indicates no ownership or affiliation

        with an existing cluster member

```

- **show cluster info [conn-distribution | packet-distribution | loadbalance]**

show cluster info conn-distribution および **show cluster info packet-distribution** コマンドは、すべてのクラスタユニット間のトラフィックの分布を表示します。これらのコマンドは、外部ロード バランサを評価し、調整するのに役立ちます。

show cluster info loadbalance コマンドは、接続再分散の統計情報を表示します。

- **show cluster {access-list | conn [count] | traffic | user-identity | xlate} [options]、show cluster chassis {access-list | conn | traffic | user-identity | xlate count}**

クラスタ全体の集約データを表示します。使用可能なオプションはデータのタイプによって異なります。

show cluster access-list コマンドの次の出力を参照してください。

```

ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B, unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list 101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238

```

```
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

使用中の接続の、すべてのユニットでの 合計数を表示するには、次のとおりに入力します。

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*****
124 in use, fwd connection 0 in use, dir connection 0 in use, centralized connection
0 in use (Cluster-wide aggregated)

unit-1-1(LOCAL):*****
40 in use, 48 most used, fwd connection 0 in use, 0 most used, dir connection 0 in
use,
0 most used, centralized connection 0 in use, 46 most used

unit-2-2:*****
18 in use, 40 most used, fwd connection 0 in use, 0 most used, dir connection 0 in
use,
0 most used, centralized connection 0 in use, 45 most used
```

- **show asp cluster counter**

このコマンドは、データパスのトラブルシューティングに役立ちます。

クラスタのルーティングのモニタリング

クラスタのルーティングについては、次のコマンドを参照してください。

- **show route cluster**
- **debug route cluster**

クラスタのルーティング情報を表示します。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次のコマンドを参照してください。

logging device-id

クラスタ内の各ユニットは、syslog メッセージを個別に生成します。**logging device-id** コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。

クラスタリングのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | service-module | transport]**

クラスタリングのデバッグ メッセージを表示します。

- **debug service-module**

スーパーバイザとアプリケーション間のヘルス チェックの問題を含め、ブレード レベルの問題に関するデバッグ メッセージを表示します。

- **show cluster info trace**

show cluster info trace コマンドは、トラブルシューティングのためのデバッグ情報を表示します。

show cluster info trace コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info trace
Feb 02 14:19:47.456 [DEBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
Feb 02 14:19:47.456 [DEBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
Feb 02 14:19:47.456 [DEBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
MASTER
```

クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合した場合、期待できる合計クラスタパフォーマンスの概算値は次のようになります。

- TCP または CPS の合計スループットの 80 %
- UDP の合計スループットの 90 %
- トラフィックの混在に応じて、イーサネット MIX (EMIX) の合計スループットの 60 %。

たとえば、TCP スループットについては、3つのモジュールを備えた Firepower 9300 は、単独で動作している場合、約 135 Gbps の実際のファイアウォールトラフィックを処理できます。2シャーシの場合、最大スループットの合計は 270 Gbps (2 シャーシ X 135 Gbps) の約 80 %、つまり 216 Gbps です。

マスターユニット選定

クラスタのメンバは、クラスタ制御リンクを介して通信してマスターユニットを選定します。方法は次のとおりです。

1. クラスタを展開すると、各ユニットは選定要求を 3 秒ごとにブロードキャストします。
2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティはクラスタの展開時に設定され、設定の変更はできません。
3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットがマスターになります。
4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的にマスターユニットになることはありません。既存のマスターユニットは常にマスターのままです。ただし、マスターユニットが応答を停止すると、その時点で新しいマスターユニットが選定されます。



(注) 特定のユニットを手動で強制的にマスターにすることができます。中央集中型機能については、マスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。

クラスタ内のハイアベイラビリティ

クラスタリングは、シャーシ、ユニットとインターフェイスの正常性を監視し、ユニット間で接続状態を複製することにより、ハイアベイラビリティを提供します。

シャーシアプリケーションのモニタリング

シャーシアプリケーションのヘルスモニタリングは常に有効になっています。Firepower 9300 シャーシスーパーバイザはASAアプリケーションを定期的を確認します (毎秒)。ASAが作動中で、Firepower 9300 シャーシスーパーバイザと 3 秒間通信できなければASAはsyslogメッセージを生成して、クラスタを離れます。

Firepower 9300 シャーシスーパーバイザが 45 秒後にアプリケーションと通信できなければ、ASAをリロードします。ASAがスーパーバイザと通信できなければ、自身をクラスタから削除します。

ユニットのヘルス モニタリング

マスターユニットは、各スレーブユニットをモニタするために、クラスタ制御リンクを介してキープアライブメッセージを定期的送信します（間隔は設定可能です）。各スレーブユニットは、同じメカニズムを使用してマスターユニットをモニタします。ユニットの健全性チェックが失敗すると、ユニットはクラスタから削除されます。

インターフェイス モニタリング

各ユニットは、使用中のすべてのハードウェア インターフェイスのリンク ステータスをモニタし、ステータス変更をマスターユニットに報告します。ヘルス モニタリングを有効にすると、デフォルトではすべての物理インターフェイスがモニタされます（EtherChannel インターフェイスのメインEtherChannelを含む）。アップ状態の指名されたインターフェイスのみモニタできます。たとえば、名前付き EtherChannel がクラスタから削除される前に、EtherChannel のすべてのメンバー ポートがエラーとなる必要があります（最小ポートバンドル設定に基づく）。ヘルスチェックは、インターフェイスごとに、モニタリングをオプションで無効にすることができます。

あるモニタ対象のインターフェイスが、特定のユニット上では障害が発生したが、別のユニットではアクティブの場合は、そのユニットはクラスタから削除されます。ASA がメンバーをクラスタから削除するまでの時間は、そのユニットが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。ASA は、ユニットがクラスタに参加する最初の 90 秒間はインターフェイスを監視しません。この間にインターフェイスのステータスに変化しても、ASA はクラスタから削除されません。設定済みのメンバーの場合は、500 ミリ秒後にユニットが削除されます

障害後のステータス

クラスタ内のユニットで障害が発生したときに、そのユニットでホスティングされている接続は他のユニットにシームレスに移管されます。トラフィックフローのステート情報は、クラスタ制御リンクを介して共有されます。

マスターユニットで障害が発生した場合は、そのクラスタの他のメンバーのうち、プライオリティが最高（番号が最小）のものがマスターユニットになります。

障害イベントに応じて、ASA は自動的にクラスタへの再参加を試みます。



- (注) ASA が非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのユニットがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはディセーブルになります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

クラスタへの再参加

クラスタメンバがクラスタから削除された後、クラスタに再参加できる方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：クラスタ制御リンクの問題を解決した後、ASA コンソールポートで **cluster group name** と入力してから **enable** と入力して、クラスタリングを再びイネーブルにすることによって、手動でクラスタに再参加する必要があります。
- データ インターフェイスの障害：ASA は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、ASA はクラスタリングをディセーブルにします。データ インターフェイスの問題を解決した後、ASA コンソールポートで **cluster group name** と入力してから **enable** と入力して、クラスタリングを手動でイネーブルにする必要があります。
- ユニットの障害：ユニットがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ユニットは再起動するとクラスタに再参加します。ユニットは 5 秒ごとにクラスタへの再参加を試みます。
- シャーシアプリケーション通信の障害：ASA がシャーシアプリケーションの状態が回復したことを検出すると、ASA は自動的にクラスタの再参加を試みます。
- 内部エラー：内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。問題を解決したら、コンソールポートで **cluster group name** 入力してから **enable** と入力することでクラスタリングを再び有効にして、クラスタに手動で再参加する必要があります。

データ パス接続状態の複製

どの接続にも、1つのオーナーおよび少なくとも1つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもありません。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 1: クラスタ全体で複製される機能

| Traffic | 状態のサポート | 注意 |
|-----------|---------|-------------------------|
| Up time | Yes | システム アップ タイムをトラッキングします。 |
| ARP Table | Yes | トランスペアレント モードのみ。 |

| Traffic | 状態のサポート | 注意 |
|------------------|---------|---|
| MAC アドレス テーブル | Yes | トランスペアレント モードのみ。 |
| ユーザ アイデンティティ | Yes | AAA ルール (uauth) とアイデンティティ ファイアウォールが含まれます。 |
| IPv6 ネイバー データベース | Yes | — |
| ダイナミック ルーティング | Yes | — |
| SNMP エンジン ID | なし | — |
| 集中型 VPN (サイト間) | なし | VPN セッションは、マスター ユニットで障害が発生すると切断されます。 |

クラスタが接続を管理する方法

接続をクラスタの複数のメンバにロードバランスできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- **オーナー**：通常、最初に接続を受信するユニット。オーナーは、TCP 状態を保持し、パケットを処理します。1つの接続に対してオーナーは1つだけです。元のオーナーに障害が発生すると、新しいユニットが接続からパケットを受信したときにディレクタがこれらのユニットの新しいオーナーを選択します。
- **バックアップ オーナー**：オーナーから受信した TCP/UDP ステート情報を格納するユニット。これにより、障害が発生した場合に新しいオーナーにシームレスに接続を転送できます。バックアップ オーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合は、その接続からパケットを受け取る最初のユニット（ロードバランシングに基づく）がバックアップ オーナーに問い合わせ、関連するステート情報を取得し、これでそのユニットが新しいオーナーになることができます。

ディレクタ（下記参照）がオーナーと同じユニットでない限り、ディレクタはバックアップ オーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

- **ディレクタ**：フォワーダからのオーナーバックアップ要求を処理するユニット。オーナーが新しい接続を受信すると、オーナーは、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにメッセージをそのディレクタに送信します。パケットがオーナー以外のユニットに到着した場合は、そのユニッ

トはどのユニットがオーナーかをディレクタに問い合わせます。これで、パケットを転送できるようになります。1つの接続に対してディレクタは1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

ディレクタがオーナーと同じユニットでない限り、ディレクタはバックアップオーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップオーナーが選択されます。

- **フォワーダ**：パケットをオーナーに転送するユニット。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせしてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。フォワーダが **SYN-ACK** パケットを受信した場合、フォワーダはパケットの **SYN** キーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCPシーケンスのランダム化をディセーブルにした場合は、**SYN Cookie** は使用されないの、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえば **DNS** や **ICMP**）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが1つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

接続でポートアドレス変換（PAT）を使用すると、PATのタイプ（**per-session** または **multi-session**）が、クラスタのどのメンバが新しい接続のオーナーになるかに影響します。

- **Per-session PAT**：オーナーは、接続の最初のパケットを受信するユニットです。
デフォルトでは、TCP および DNS UDP トラフィックは **per-session PAT** を使用します。
- **Multi-session PAT**：オーナーは常にマスターユニットです。 **multi-session PAT** 接続がスレーブユニットで最初に受信される場合、スレーブユニットはその接続をマスターユニットに転送します。
デフォルトでは、UDP（DNS UDP を除く）および ICMP トラフィックは **multi-session PAT** を使用するので、これらの接続は常にマスターユニットによって所有されています。

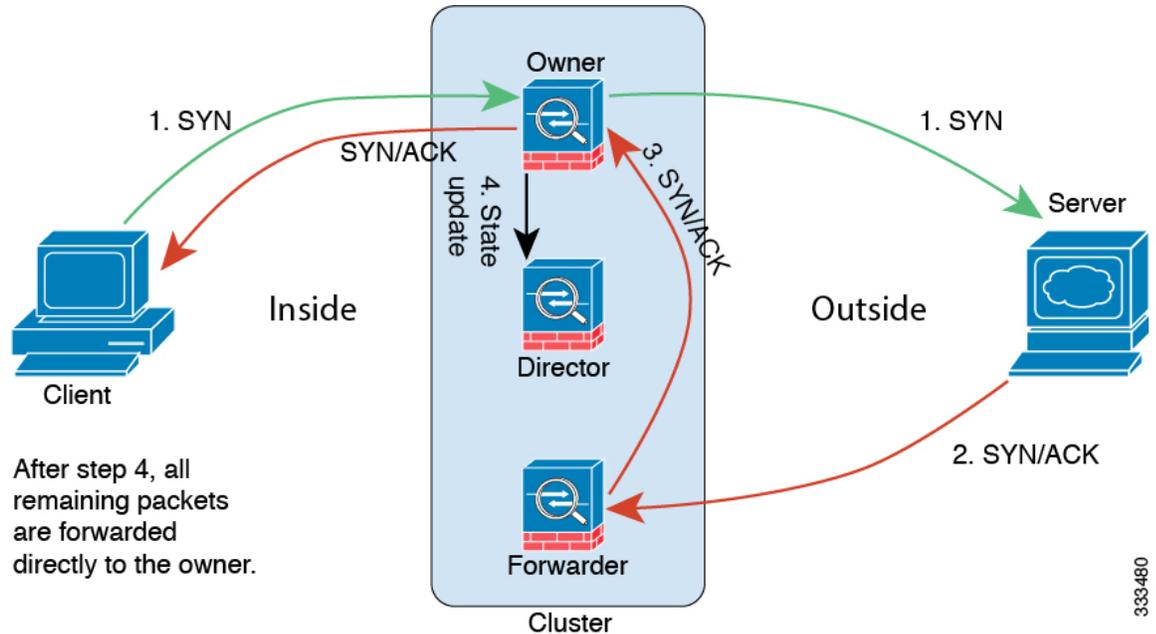
TCP および UDP の **per-session PAT** デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて **per-session** または **multi-session** で処理されます。ICMP の場合は、デフォルトの **multi-session PAT** から変更することはできません。 **per-session PAT** の詳細については、『ファイアウォールの構成ガイド』を参照してください。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのメンバに送信される場合は、そのユニットがその接続の両方向のオーナーとなります。接続のパケットが別のユニットに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーユニットに転送されます。逆方向のフローが別のユニットに到着した場合は、元のユニットにリダイレクトされます。

サンプルデータフロー

次の例は、新しい接続の確立を示します。



1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロードバランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロードバランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP ステート情報を記録します。ディレクタは、この接続のバックアップオーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のユニットに配信された場合は、そのユニットはディレクタに問い合わせ、オーナーを特定し、フローを確立します。
8. フローの状態が変化した場合、状態アップデートがオーナーからディレクタに送信されます。

Firepower 9300 シャーシ上の ASA クラスタリングの履歴

| 機能名 | バージョン | 機能情報 |
|---|---------------|---|
| Firepower 9300 用 シャーシ内 ASA クラ スタリング | 9.4 (1150) | FirePOWER 9300 シャーシ内では、最大 3 つセキュリティ モジュールをクラスタ化できません。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 次のコマンドを導入しました。 cluster replication delay 、 debug service-module 、 management-only individual 、 show cluster chassis |

