VMware を使用した ASAv の導入

ASAv は、VMware ESXi を実行できる任意のサーバークラスの x86 CPU デバイスに導入できます。

ASAv の VMware 機能のサポート

次の表に、ASAv の VMware 機能のサポートを示します。

表 *1 : ASAv* の *VMware* 機能のサポート

機能	説明	サポート（あり/なし）	注釈
コールド クローン	クローニング中に VM の電源がオフになります。	あり	–
DRS	動的リソースのスケジューリングおよび分散電源管理に使用されます。	Yes	VMware のガイドラインを参照してください。

機能	説明	サポート（あり/なし）	注釈
ホット追加	追加時に VM が動作しています。	なし	–
ホット クローン	クローニング中に VM が動作しています。	なし	–
ホット リムーブ	取り外し中に VM が動作しています。	なし	–
Snapshot	VM が数秒間フリーズします。	あり	使用には注意が必要です。トラフィックが失われる可能性があります。フェールオーバーが発生することがあります。
一時停止と再開	VM が一時停止され、その後再開します。	あり	–
vCloud Director	VM の自動配置が可能になります。	なし	–
VM の移行	移行中に VM の電源がオフになります。	あり	–
VMotion	VM のライブ マイグレーションに使用されます。	あり	共有ストレージを使用します。vMotion に関するガイドライン（6 ページ）を参照してください。
VMware FT	VM の HA に使用されます。	なし	ASAv マシンの障害に対して ASAv のフェールオーバーを使用します。
VMware HA	ESXi およびサーバの障害に使用されます。	あり	ASAv マシンの障害に対して ASAv のフェールオーバーを使用します。
VM ハートビートの VMware HA	VM 障害に使用されます。	なし	ASAv マシンの障害に対して ASAv のフェールオーバーを使用します。

機能	説明	サポート（あり/なし）	注釈
VMware vSphere スタンドアロン Windows クライアント	VM を導入するために使用されます。	あり	–
VMware vSphere Web Client	VM を導入するために使用されます。	あり	–

ASAv と VMware の前提条件

VMware vSphere Web Client、vSphere スタンドアロンクライアント、または OVF ツールを使用して ASAv を導入できます。システム要件については、Cisco ASA の互換性 [英語] を参照してください。

vSphere 標準スイッチのセキュリティ ポリシー

vSphere スイッチについては、レイヤ 2 セキュリティ ポリシーを編集して、ASAv インターフェイスによって使用されるポート グループに対しセキュリティ ポリシーの例外を適用できます。次のデフォルト設定を参照してください。

- 無差別モード：**拒否**
- MAC アドレスの変更：**許可**
- 不正送信：**許可**

次の ASAv 設定の場合、これらの設定の変更が必要な場合があります。詳細については、vSphere のマニュアルを参照してください。

表 *2:* ポート グループのセキュリティ ポリシーの例外

セキュリティの例外	ルーテッド ファイアウォール モード		トランスペアレント ファイアウォール モード	
	フェールオーバーなし	フェールオーバー	フェールオーバーなし	フェールオーバー
無差別モード	<任意>	<任意>	承認	承認
MAC アドレスの変更	<任意>	承認	<任意>	承認
不正送信	<任意>	承認	承認	承認

VMware での ASAv のガイドラインと制限事項

ESXi サーバーに ASAv の複数のインスタンスを作成して導入できます。ASAv の導入に使用される特定のハードウェアは、導入されるインスタンスの数や使用要件によって異なります。作成する各仮想アプライアンスには、ホストマシン上での最小リソース割り当て（メモリ、CPU 数、およびディスク容量）が必要です。

ASAv を導入する前に、次のガイドラインと制限事項を確認します。

VMWare ESXi での ASAv のシステム要件

最適なパフォーマンスを確保するために、以下の仕様に準拠していることを確認してください。ASAvASAv には、次の要件があります。

- ホスト CPU は、仮想化拡張機能を備えたサーバークラスの x86 ベースの Intel または AMD CPU である必要があります。

  たとえば、ASAv パフォーマンステストラボでは、2.6GHz で動作する Intel® Xeon® CPU E5-2690v4 プロセッサを搭載した Cisco Unified Computing System™（Cisco UCS®）C シリーズ M4 サーバーを最低限使用しています。

- ASAv は、ESXi バージョン 6.0、6.5、6.7、7.0、7.0 アップグレード 1、7.0 アップグレード 2、および 7.0 アップグレード 3 をサポートします。

OVF ファイルのガイドライン

導入対象に基づいて、asav-vi.ovf ファイルまたは asav-esxi.ovf ファイルを選択します。

- asav-vi：vCenter に導入する場合
- asav-esxi：ESXi に導入する場合（vCenter なし）
- ASAv OVF の導入は、ローカリゼーション（非英語モードでのコンポーネントのインストール）をサポートしません。ご自身の環境の VMware vCenter と LDAP サーバーが ASCII 互換モードでインストールされていることを確認してください。
- ASAv をインストールして VM コンソールを使用する前に、キーボードを [United States English] に設定する必要があります。
- ASAv を導入すると、2 つの異なる ISO イメージが ESXi ハイパーバイザにマウントされます。
  - マウントされた最初のドライブには、vSphere によって生成された OVF 環境変数が備わってます。
  - マウントされた 2 番目のドライブは day0.iso です。

注目 ASAv マシンが起動したら、両方のドライブのマウントを解除できます。ただし、[電源投入時に接続（Connect at Power On）] がオフになっている場合でも、ドライブ 1（OVF 環境変数を使用）は、ASAv の電源をオフ/オンにするたびに常にマウントされます。

OVF テンプレートのガイドラインのエクスポート

vSphere の OVF テンプレートのエクスポート機能は、既存の ASAv インスタンスパッケージを OVF テンプレートとしてエクスポートするのに役立ちます。エクスポートされた OVF テンプレートを使用して、同じ環境または異なる環境に ASAv インスタンスを導入できます。エクスポートされた OVF テンプレートを使用して vSphere に ASAv インスタンスを導入する前に、OVF ファイルの構成の詳細を変更して、導入の失敗を防ぐ必要があります。

ASAv のエクスポートされた OVF ファイルを変更するには、次の手順を実行します。

1. OVF テンプレートをエクスポートしたローカルマシンにログインします。
2. テキストエディタで OVF ファイルを参照して開きます。
3. `<vmw:ExtraConfig vmw:key="monitor_control.pseudo_perfctr" vmw:value="TRUE"></vmw:ExtraConfig>` タグが存在することを確認します。
4. `<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>` タグを削除します。

   または

   `<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>` タグと `<rasd:ResourceSubType>vmware.cdrom.remotepassthrough</rasd:ResourceSubType>` タグを交換します。

   詳細については、VMware が公開した「Deploying an OVF fails on vCenter Server 5.1/5.5 when VMware tools are installed (2034422)」を参照してください。
5. `UserPrivilege`、`OvfDeployment`、および `ControllerType` のプロパティ値を入力します。

   次に例を示します。

```
- <Property ovf:qualifiers="ValueMap{"ovf", "ignore", "installer"}" ovf:type="string"
 ovf:key="OvfDeployment">
+ <Property ovf:qualifiers="ValueMap{"ovf", "ignore", "installer"}" ovf:type="string"
 ovf:key="OvfDeployment" ovf:value="ovf">

- <Property ovf:type="string" ovf:key="ControllerType">
+ <Property ovf:type="string" ovf:key="ControllerType" ovf:value="ASAv">

- <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
ovf:key="UserPrivilege">
+ <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
ovf:key="UserPrivilege" ovf:value="15">
```

6. OVF ファイルを保存します。

7. OVF テンプレートを使用して、ASAv を導入します。VMware vSphere Web Client を使用した ASAv の導入 [英語] を参照してください。

ハイ アベイラビリティ ガイドラインのためのフェールオーバー

フェールオーバー配置の場合は、スタンバイ装置が同じライセンス権限付与を備えていることを確認してください（たとえば、両方の装置が 2Gbps の権限付与であることなど）。

重要 ASAv を使用して高可用性ペアを作成する場合は、データインターフェイスを各 ASAv に同じ順序で追加する必要があります。完全に同じインターフェイスが異なる順序で各 ASAv に追加されると、ASAv コンソールにエラーが表示されることがあります。また、フェールオーバー機能にも影響が出ることがあります。

ASAv 内部インターフェイスまたは ASAv フェールオーバーの高可用性リンクに使用される ESX ポートグループについては、2 つの仮想 NIC を使用して ESX ポートグループのフェールオーバー順序を設定します（1 つはアクティブアップリンク、もう 1 つはスタンバイアップリンク）。この設定は、2 つの VM が相互に ping を実行したり、ASAv 高可用性リンクを稼働させたりするために必要です。

vMotion に関するガイドライン

- VMware では、vMotion を使用する場合、共有ストレージのみを使用する必要があります。ASAv の導入時に、ホスト クラスタがある場合は、ストレージをローカルに（特定のホスト上）または共有ホスト上でプロビジョニングできます。ただし、ASAv を vMotion を使用して別のホストに移行する場合、ローカル ストレージを使用するとエラーが発生します。

スループット用のメモリと vCPU の割り当てとライセンス

- ASAv に割り当てられたメモリのサイズは、スループットレベルに合わせたものです。異なるスループットレベルのライセンスを要求する場合を除いて、[Edit Settings] ダイアログボックスのメモリ設定または vCPU ハードウェア設定は変更しないでください。アンダープロビジョニングは、パフォーマンスに影響を与える可能性があります。

（注） メモリまたは vCPU ハードウェア設定を変更する必要がある場合は、ASAv のライセンスに記載されている値のみを使用してください。VMware が推奨するメモリ構成の最小値、デフォルト値、および最大値は使用しないでください。

場合によっては、ASAv5 のメモリが枯渇状態になります。この状態は、AnyConnect クライアントの有効化やファイルのダウンロードなど、特定のリソースの利用が多い場合に発生することがあります。自動的な再起動に関するコンソール メッセージやメモリ使用量に関する重大な syslog が、メモリ枯渇の状態を示します。このような場合、1.5 GB メモリの

VM に ASAv5 を導入できます。1 GB から 1.5 GB に変更するには、VM の電源をオフにして、メモリを変更し、VM の電源を再度オンにします。

CPU 予約

- デフォルトでは、ASAv の CPU 予約は 1000 MHz です。共有、予約、および制限の設定（[設定の編集（Edit Settings）] > [リソース（Resources）] > [CPU]）を使用することで、ASAv に割り当てられる CPU リソースの量を変更できます。より低い設定で必要なトラフィック負荷が課されている状況で ASAv が目的を達成できる場合は、CPU 予約の設定を 1000 Mhz 未満にできます。ASAv によって使用される CPU の量は、動作しているハードウェア プラットフォームだけでなく、実行している作業のタイプと量によっても異なります。

  仮想マシンの [Performance] タブの [Home] ビューに配置された [CPU Usage (MHz)] チャートから、すべての仮想マシンに関する CPU 使用率をホストの視点で確認できます。ASAv が標準的なトラフィック量を処理しているときの CPU 使用率のベンチマークを設定すると、その情報を CPU 予約の調整時の入力として使用できます。

  詳細については、VMware から発行されている『CPU Performance Enhancement Advice』を参照してください。

- リソース割り当てとオーバープロビジョニングまたはアンダープロビジョニングされたリソースを表示するには、ASAv **show vm** および **show cpu** コマンド、あるいは ASDM **[ホーム（Home）]** > **[デバイスダッシュボード（Device Dashboard）]** > **[デバイス情報（Device Information）]** > **[仮想リソース（Virtual Resources）]** タブまたは **[モニタリング（Monitoring）]** > **[プロパティ（Properties）]** > **[システムリソースグラフ（System Resources Graphs）]** > **[CPU]** ペインを使用できます。

UCS B シリーズ ハードウェアにおけるトランスペアレント モードに関するガイドライン

MAC フラップが、Cisco UCS B シリーズ ハードウェアのトランスペアレントモードで動作する一部の ASAv 設定で発生することがあります。MAC アドレスがさまざまな場所で出現した場合、パケットはドロップされます。

VMware 環境にトランスペアレントモードで ASAv を導入する場合に MAC フラップを回避するには、次のガイドラインを参考にしてください。

- VMware NIC チーミング：UCS B シリーズにトランスペアレントモードで ASAv を導入する場合、内部および外部インターフェイスに使用するポートグループにはアクティブアップリンクを 1 つだけ設定し、アップリンクは同じである必要があります。vCenter で VMware NIC チーミングを設定します。

  NIC チーミングの設定方法の詳細については、VMware ドキュメントを参照してください。

- ARP インスペクション：ASAv で ARP インスペクションを有効にし、受信インターフェイスで MAC および ARP エントリを静的に設定します。ARP インスペクションと有効化の詳細については、Cisco ASA シリーズ コンフィギュレーション ガイド（一般的な操作）[英語] を参照してください。

その他のガイドラインと制限事項

- ESXi 6.7、vCenter 6.7、ASA Virtual 9.12 以降を実行している場合、ASA Virtual は 2 つの CD/DVD IDE ドライブなしで起動します。
- vSphere Web Client は ASAv OVA の導入ではサポートされないため、vSphere Client を使用してください。

ASAv ソフトウェアの解凍と第 0 日用構成ファイルの作成

ASAv を起動する前に、第 0 日用のコンフィギュレーション ファイルを準備できます。このファイルは、ASAv の起動時に適用される ASAv の設定を含むテキストファイルです。この初期設定は、「day0-config」というテキスト ファイルとして指定の作業ディレクトリに格納され、さらに day0.iso ファイルへと処理されます。この day0.iso ファイルが最初の起動時にマウントされて読み取られます。第 0 日用コンフィギュレーション ファイルには、少なくとも、管理インターフェイスをアクティブ化するコマンドと、公開キー認証用 SSH サーバーを設定するコマンドを含める必要がありますが、すべての ASA 設定を含めることもできます。空の day0-config を含むデフォルトの day0.iso がリリースとともに提供されています。day0.iso ファイル（カスタム day0 またはデフォルトの day0.iso）は、最初の起動中に使用できなければなりません。

始める前に

この例では Linux が使用されていますが、Windows の場合にも同様のユーティリティがあります。

- 初期導入時に自動的に ASAv にライセンスを付与するには、Cisco Smart Software Manager からダウンロードした Smart Licensing Identity（ID）トークンを「idtoken」というテキスト ファイルに格納し、第 0 日用構成ファイルと同じディレクトリに保存します。
- トランスペアレントモードで ASAv を導入する場合は、トランスペアレントモードで実行される既知の ASA 構成ファイルを、第 0 日用構成ファイルとして使用する必要があります。これは、ルーテッド ファイアウォールの第 0 日用コンフィギュレーション ファイルには該当しません。
- ISO イメージが ESXi ハイパーバイザにどのようにマウントされるかの詳細については、VMware での ASAv のガイドラインと制限事項 （4 ページ）の OVF ファイルのガイドラインを参照してください。

手順

ステップ 1 ZIP ファイルを Cisco.com からダウンロードし、ローカル ディスクに保存します。

https://www.cisco.com/go/asa-software

（注） Cisco.com のログインおよびシスコ サービス契約が必要です。

ステップ 2 ファイルを作業ディレクトリに解凍します。ディレクトリからファイルを削除しないでください。次のファイルが含まれています。

- asav-vi.ovf：vCenter への導入用。
- asav-esxi.ovf：vCenter 以外への導入用。
- boot.vmdk：ブート ディスク イメージ。
- disk0.vmdk：ASAv ディスクイメージ。
- day0.iso：day0-config ファイルおよびオプションの idtoken ファイルを含む ISO。
- asav-vi.mf：vCenter への導入用のマニフェスト ファイル。
- asav-esxi.mf：vCenter 以外への導入用のマニフェスト ファイル。

ステップ 3 「day0-config」というテキストファイルに ASAv の CLI 設定を記入します。3 つのインターフェイスの設定とその他の必要な設定を追加します。

最初の行は ASA のバージョンで始める必要があります。day0-config は、有効な ASA 構成である必要があります。day0-config を生成する最適な方法は、既存の ASA または ASAv から実行コンフィギュレーションの必要な部分をコピーする方法です。day0-config 内の行の順序は重要で、既存の **show running-config** コマンド出力の順序と一致している必要があります。

例：

```
ASA Version 9.4.1
!
console serial
interface management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
call-home
http-proxy 10.1.1.1 port 443
license smart
feature tier standard
throughput level 2G
```

ステップ 4 （任意）Cisco Smart Software Manager により発行された Smart License ID トークン ファイルをコンピュータにダウンロードします。

ステップ 5 （任意）ダウンロードファイルから ID トークンをコピーし、ID トークンのみを含む「idtoken」というテキスト ファイルに保存します。

この ID トークンによって、Smart Licensing サーバーに ASAv が自動的に登録されます。

ステップ 6 テキスト ファイルを ISO ファイルに変換して仮想CD-ROM を生成します。

例：

```
stack@user-ubuntu:-/KvmAsa$ sudo genisoimage -r -o day0.iso day0-config idtoken
I: input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 252
Total directory bytes: 0
Path table size (bytes): 10
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

ステップ 7 day0.iso 用に Linux で新しい SHA1 値を計算します。

例：

```
openssl dgst -sha1 day0.iso
SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66 day0.iso
```

ステップ 8 新しいチェックサムを作業ディレクトリの asav-vi.mf ファイルに含め、day0.iso SHA1 値を新しく生成された値で置き換えます。

例：

```
SHA1(asav-vi.ovf)= de0f1878b8f1260e379ef853db4e790c8e92f2b2
SHA1(disk0.vmdk)= 898b26891cc68fa0c94ebd91532fc450da418b02
SHA1(boot.vmdk)= 6b0000ddebfc38ccc99ac2d4d5dbfb8abfb3d9c4
SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66
```

ステップ 9 ZIP ファイルを解凍したディレクトリに day0.iso ファイルをコピーします。デフォルト（空）の day0.iso ファイルが上書きされます。

このディレクトリから VM が導入される場合は、新しく生成された day0.iso 内の構成が適用されます。

VMware vSphere Web Client を使用した ASAv の導入

この項では、VMware vSphere Web Client を使用して ASAv を導入する方法について説明します。Web クライアントには、vCenter が必要です。vCenter がない場合は、「VMware vSphere スタンドアロンクライアントおよび第 0 日用構成を使用した ASAv の導入」、または「OVF ツールおよび第 0 日用構成を使用した ASAv の導入」を参照してください。

- vSphere Web Client へのアクセスとクライアント統合プラグインのインストール （11 ページ）
- VMware vSphere Web Client を使用した ASAv の導入 （10 ページ）

vSphere Web Client へのアクセスとクライアント統合プラグインのインストール

この項では、vSphere Web Client にアクセスする方法について説明します。また、ASAv コンソールアクセスに必要なクライアント統合プラグインをインストールする方法についても説明します。一部の Web クライアント機能（プラグインなど）は、Macintosh ではサポートされていません。完全なクライアントのサポート情報については、VMware の Web サイトを参照してください。

手順

ステップ 1 ブラウザから VMware vSphere Web Client を起動します。

https://*vCenter_server*:*port*/**vsphere-client/**

デフォルトでは、port は 9443 です。

ステップ 2 （1 回のみ）ASAv コンソールへのアクセスを可能にするため、クライアント統合プラグインをインストールします。

1. ログイン画面で、[Download the Client Integration Plug-in] をクリックしてプラグインをダウンロードします。
2. ブラウザを閉じてから、インストーラを使用してプラグインをインストールします。
3. プラグインをインストールしたら、vSphere Web Client に再接続します。

ステップ 3 ユーザー名とパスワードを入力し、[Login] をクリックするか、[Use Windows session authentication] チェックボックスをオンにします（Windows のみ）。

VMware vSphere Web Client を使用した ASAv の導入

ASAv を導入するには、VMware vSphere Web Client（または vSphere Client）、およびオープン仮想化フォーマット（OVF）のテンプレートファイルを使用します。シスコの ASAv パッケージを展開するには、vSphere Web Client で Deploy OVF Template ウィザードを使用します。このウィザードでは、ASAv OVA ファイルを解析し、ASAv を実行する仮想マシンを作成し、パッケージをインストールします。

ウィザードの手順のほとんどは、VMware に対し標準のものです。Deploy OVF Template の詳細については、VMware vSphere Web Client のオンライン ヘルプを参照してください。

始める前に

ASAv を導入する前に、vSphere（管理用）で少なくとも 1 つのネットワークを設定しておく必要があります。

手順

ステップ 1 ASAv ZIP ファイルを Cisco.com からダウンロードし、PC に保存します。

http://www.cisco.com/go/asa-software

（注） Cisco.com のログインおよびシスコ サービス契約が必要です。

ステップ 2 vSphere Web Client の [Navigator] ペインで、[vCenter] をクリックします。

ステップ 3 [Hosts and Clusters] をクリックします。

ステップ 4 ASAv を導入するデータセンター、クラスタ、またはホストを右クリックして、[Deploy OVF Template] を選択します。
[Deploy OVF Template] ウィザードが表示されます。

ステップ 5 ウィザード画面の指示に従って進みます。

ステップ 6 [Setup networks] 画面で、使用する各 ASAv インターフェイスにネットワークをマッピングします。

ネットワークはアルファベット順になっていない可能性があります。ネットワークを見つけることが非常に困難な場合は、[Edit Settings] ダイアログボックスからネットワークを後で変更できます。導入後、ASAv インスタンスを右クリックし、[Edit Settings] を選択して [Edit Settings] ダイアログボックスにアクセスします。ただし、この画面には ASAv インターフェイス ID は表示されません（ネットワーク アダプタ ID のみ）。次のネットワーク アダプタ ID と ASAv インターフェイス ID の対応一覧を参照してください。

ネットワーク アダプタ ID	ASAv インターフェイス ID
ネットワーク アダプタ 1	Management 0/0
ネットワーク アダプタ 2	GigabitEthernet 0/0
ネットワーク アダプタ 3	GigabitEthernet 0/1
ネットワーク アダプタ 4	GigabitEthernet 0/2
ネットワーク アダプタ 5	GigabitEthernet 0/3
ネットワーク アダプタ 6	GigabitEthernet 0/4
ネットワーク アダプタ 7	GigabitEthernet 0/5
ネットワーク アダプタ 8	GigabitEthernet 0/6
ネットワーク アダプタ 9	GigabitEthernet 0/7
ネットワーク アダプタ 10	GigabitEthernet 0/8

すべての ASAv インターフェイスを使用する必要はありません。ただし、vSphere Web Client ではすべてのインターフェイスにネットワークを割り当てる必要があります。使用しないインターフェイスについては、ASAv 設定内でインターフェイスを無効のままにしておくことができます。ASAv を導入した後、任意で vSphere Web Client に戻り、[Edit Settings] ダイアログボックスから余分なインターフェイスを削除することができます。詳細については、vSphere Web Client のオンライン ヘルプを参照してください。

（注） フェールオーバー/HA 配置では、GigabitEthernet 0/8 がフェールオーバー インターフェイスとして事前設定されます。

ステップ 7 インターネット アクセスに HTTP プロキシを使用する場合は、[Smart Call Home Settings] 領域でスマート ライセンスのプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

ステップ 8 フェールオーバー/HA 配置では、[Customize] テンプレート画面で次を設定します。

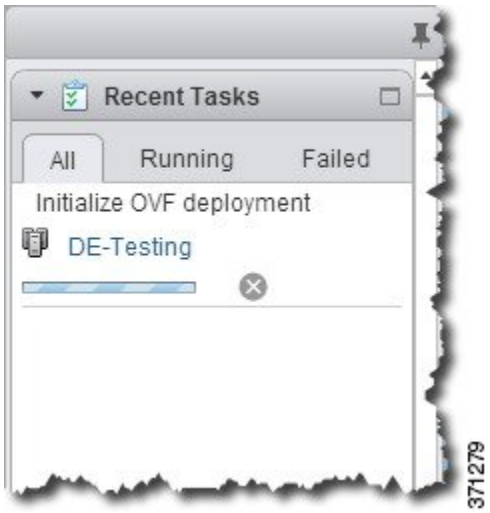
- スタンバイ管理 IP アドレスを指定します。

  インターフェイスを設定する場合、同じネットワーク上のアクティブ IP アドレスとスタンバイ IP アドレスを指定する必要があります。プライマリ装置が故障すると、セカンダリ装置はプライマリ装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。現在スタンバイになっている装置が、スタンバイの IP アドレスと MAC アドレスを引き継ぎます。ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

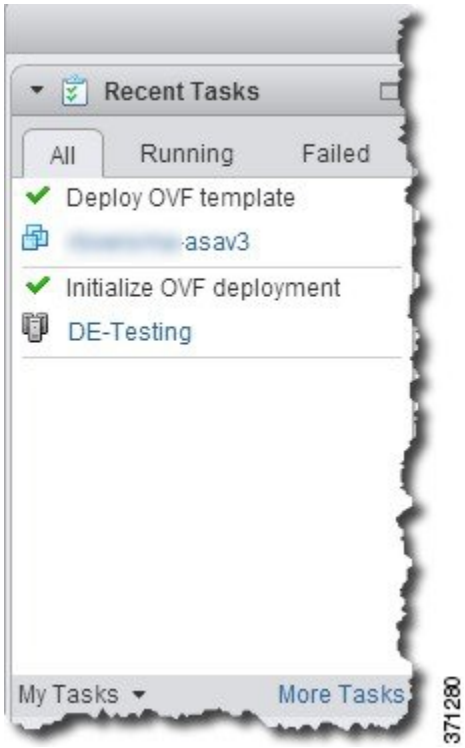
- [HA Connection Settings] 領域で、フェールオーバー リンクを設定します。

  フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。GigabitEthernet 0/8 がフェールオーバー リンクとして事前設定されています。同じネットワーク上のリンクに対するアクティブな IP アドレスとスタンバイの IP アドレスを入力します。

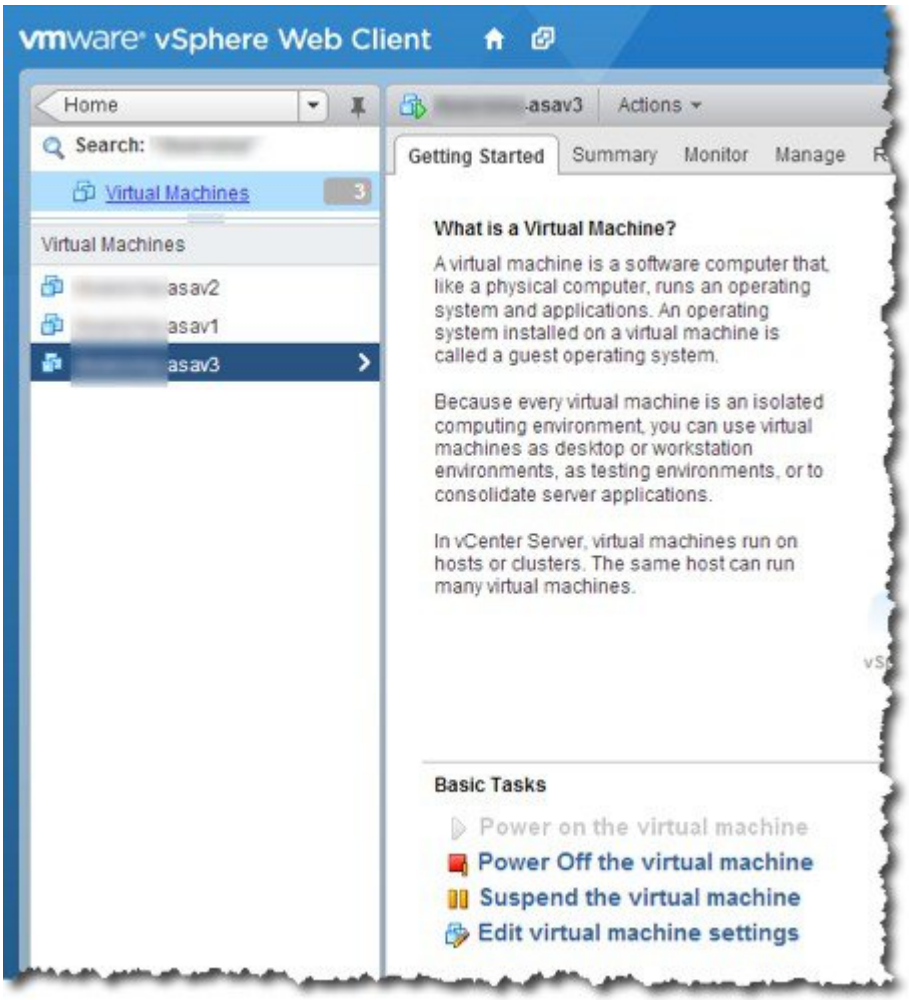
ステップ 9 ウィザードが完了すると、vSphere Web Client は VM を処理します。[Global Information] 領域の [Recent Tasks] ペインで [Initialize OVF deployment] ステータスを確認できます。



この手順が終了すると、[Deploy OVF Template] 完了ステータスが表示されます。



その後、ASAv インスタンスがインベントリ内の指定されたデータセンターの下に表示されます。



ステップ 10 ASAv マシンがまだ稼働していない場合は、[仮想マシンの電源をオン（Power on the virtual machine）] をクリックします。

ASDM で接続を試行したりコンソールに接続を試行する前に、ASAv が起動するのを待ちます。ASAv が初めて起動すると、OVF ファイルから提供されたパラメータを読み込み、それらを ASAv システム構成に追加します。その後、起動プロセスが自動的に再開され、稼働を開始します。この二重起動プロセスは、初めて ASAv を導入した場合にのみ発生します。起動メッセージを確認するには、[Console] タブをクリックして、ASAv コンソールにアクセスします。

ステップ 11 フェールオーバー/HA 配置の場合は、この手順を繰り返してセカンダリ装置を追加します。次のガイドラインを参照してください。

- プライマリ装置と同じスループット レベルを設定します。

- プライマリ装置とまったく同じ IP アドレス設定を入力します。両方の装置のブートストラップ設定は、プライマリまたはセカンダリとして装置を識別するパラメータを除いて同一にします。

次のタスク

Cisco Licensing Authority に ASAv を正常に登録するには、ASAv にインターネットアクセスが必要です。インターネットアクセスを実行して正常にライセンス登録するには、導入後に追加の設定が必要になることがあります。

VMware vSphere スタンドアロンクライアントおよび第 0 日用構成を使用した ASAv の導入

ASAv を導入するには、VMware vSphere Client およびオープン仮想化フォーマット（OVF）のテンプレートファイル（vCenter へ導入する場合は asav-vi.ovf、vCenter 以外へ導入する場合は asav-esxi.ovf）を使用します。シスコの ASAv パッケージを導入するには、vSphere Client で [OVFテンプレートの導入（Deploy OVF Template）] ウィザードを使用します。このウィザードでは、ASAv OVA ファイルを解析し、ASAv を実行する仮想マシンを作成し、パッケージをインストールします。

ウィザードの手順のほとんどは、VMware に対し標準のものです。[Deploy OVF Template] ウィザードの詳細については、VMware vSphere クライアントのオンライン ヘルプを参照してください。

始める前に

- ASAv を導入する前に、vSphere（管理用）で少なくとも 1 つのネットワークを設定しておく必要があります。
- ASAv ソフトウェアの解凍と第 0 日用構成ファイルの作成 （8 ページ）の手順に従って、第 0 日用構成を作成します。

手順

ステップ 1 VMware vSphere クライアントを起動し、**[File]** > **[Deploy OVF Template]** を選択します。

[Deploy OVF Template] ウィザードが表示されます。

ステップ 2 asav-vi.ovf ファイルを解凍した作業ディレクトリを参照し、それを選択します。

ステップ 3 [OVF Template Details] 画面が表示されます。次の画面に移動します。カスタムの第 0 日用コンフィギュレーション ファイルを使用する場合は、構成を変更する必要はありません。

ステップ 4 最後の画面に導入設定の要約が表示されます。[Finish] をクリックしてVM を導入します。

ステップ 5 ASAv の電源を投入し、VMware コンソールを開いて、2 回目の起動を待機します。

ステップ 6 ASAv に SSH 接続し、必要な構成を完了します。第 0 日用コンフィギュレーション ファイルに必要なすべての構成がされていない場合は、VMware コンソールを開いて、必要な構成を完了します。

これで、ASAv は完全に動作可能な状態です。

OVF ツールおよび第 0 日用構成を使用した ASAv の導入

このセクションでは、第 0 日用構成ファイルを必要とする OVF ツールを使用した ASAv の導入方法について説明します。

始める前に

- OVF ツールを使用して ASAv を導入する場合は、day0.iso ファイルが必要です。ZIP ファイルで提供されるデフォルトの空の day0.iso ファイルを使用するか、または、生成しカスタマイズした第 0 日用コンフィギュレーション ファイルを使用できます。第 0 日用コンフィギュレーション ファイルの作成方法については、ASAv ソフトウェアの解凍と第 0 日用構成ファイルの作成 （8 ページ）を参照してください。
- OVF ツールが Linux または Windows PC にインストールされ、ターゲット ESXi サーバーに接続できることを確認します。

手順

ステップ 1 OVF ツールがインストールされていることを確認します。

例：

```
linuxprompt# which ovftool
```

ステップ 2 必要な導入オプションを指定した .cmd ファイルを作成します。

例：

```
linuxprompt# cat launch.cmd
ovftool \
--name="asav-941-demo" \
--powerOn \
--deploymentOption=ASAv30 \
--diskMode=thin \
--datastore=datastore1 \
--acceptAllEulas \
--net:Management0-0="Portgroup_Mgmt" \
--net:GigabitEthernet0-1="Portgroup_Inside" \
--net:GigabitEthernet0-0="Portgroup_Outside" \
--prop:HARole=Standalone \
asav-esxi.ovf \
vi://root@10.1.2.3/
```

ステップ 3 cmd ファイルを実行します。

例：

```
linuxprompt# ./launch.cmd
```

ASAv の電源を投入し、2 回目の起動を待機します。

ステップ 4 ASAv に SSH 接続し、必要に応じて設定を完了します。さらに設定が必要な場合は、ASAv に対して VMware コンソールを開き、必要な設定を適用します。

これで、ASAv は完全に動作可能な状態です。

ASAv コンソールへのアクセス

ASDM を使用する場合、トラブルシューティングに CLI を使用する必要がある場合があります。デフォルトでは、組み込みの VMware vSphere コンソールにアクセスできます。または、コピー アンド ペーストなどのより優れた機能を持つネットワーク シリアル コンソールを設定できます。

- VMware vSphere コンソールの使用
- ネットワーク シリアル コンソール ポートの設定

VMware vSphere コンソールの使用

初期設定またはトラブルシューティングを行うには、VMware vSphere Web Client により提供される仮想コンソールから CLI にアクセスします。後で Telnet または SSH の CLI リモート アクセスを設定できます。

始める前に

vSphere Web Client では、ASAv コンソール アクセスに必要なクライアント統合プラグインをインストールします。

手順

ステップ 1 VMware vSphere Web Client で、インベントリの ASAv インスタンスを右クリックし、[Open Console] を選択します。または、[Summary] タブの [Launch Console] をクリックします。

ステップ 2 コンソールでクリックして Enter を押します。注：Ctrl + Alt を押すと、カーソルが解放されます。

ASAv がまだ起動中の場合は、起動メッセージが表示されます。

ASAv が初めて起動すると、OVF ファイルから提供されたパラメータを読み込み、それらを ASAv システム構成に追加します。その後、起動プロセスが自動的に再開され、稼働を開始します。この二重起動プロセスは、初めて ASAv を導入した場合にのみ発生します。

（注） ライセンスをインストールするまで、スループットは 100 Kbps に制限されるため、予備接続テストを実行できます。ライセンスは、通常の操作に必要です。ライセンスをインストールするまで、次のメッセージがコンソールで繰り返し表示されます。

```
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.
```

次のプロンプトが表示されます。

```
ciscoasa>
```

このプロンプトは、ユーザー EXEC モードで作業していることを示します。ユーザー EXEC モードでは、基本コマンドのみを使用できます。

ステップ 3 特権 EXEC モードにアクセスします。

例：

```
ciscoasa> enable
```

次のプロンプトが表示されます。

```
Password:
```

ステップ 4 Enter キーを押して、次に進みます。デフォルトでは、パスワードは空白です。以前にイネーブル パスワードを設定した場合は、Enter を押す代わりにこれを入力します。

プロンプトが次のように変化します。

```
ciscoasa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 5 グローバル コンフィギュレーション モードにアクセスします。

```
ciscoasa# configure terminal
```

プロンプトが次のように変化します。

```
ciscoasa(config)#
```

グローバル コンフィギュレーション モードから ASAv の設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit** コマンド、**quit** コマンド、または **end** コマンドを入力します。

ネットワーク シリアル コンソール ポートの設定

コンソール エクスペリエンスの向上のために、コンソール アクセスについて、ネットワーク シリアル ポートを単独で設定するか、または仮想シリアル ポート コンセントレータ（vSPC）に接続するように設定できます。各方法の詳細については、VMware vSphere のマニュアルを参照してください。ASAv では、仮想コンソールの代わりにシリアル ポートにコンソール出力を送信する必要があります。この手順では、シリアル ポート コンソールを有効にする方法について説明します。

手順

ステップ 1 VMware vSphere でネットワーク シリアル ポートを設定します。VMware vSphere のマニュアルを参照してください。

ステップ 2 ASAv で、「use_ttyS0」という名前のファイルを disk0 のルート ディレクトリに作成します。このファイルには内容が含まれている必要はありません。この場所に存在することのみが必要です。

disk0:/use_ttyS0

- ASDM から **[ツール（Tools）] > [ファイル管理（File Management）]** ダイアログボックスを使用して、この名前で空のテキストファイルをアップロードできます。
- vSphere コンソールで、ファイル システム内の既存のファイル（任意のファイル）を新しい名前にコピーできます。次に例を示します。

```
ciscoasa(config)# cd coredumpinfo
ciscoasa(config)# copy coredump.cfg disk0:/use_ttyS0
```

ステップ 3 ASAvをリロードします。

- ASDM から **[Tools] > [System Reload]** を選択します。
- vSphere コンソールで **reload** を入力します。

  ASAv は vSphere コンソールへの送信を停止し、代わりにシリアル コンソールに送信します。

ステップ 4 シリアル ポートの追加時に指定した vSphere のホスト IP アドレスとポート番号に Telnet 接続するか、または vSPC の IP アドレスとポートに Telnet 接続します。

vCPU またはスループット ライセンスのアップグレード

ASAv は、使用できる vCPU の数に影響するスループット ライセンスを使用します。

ASAv の vCPU の数を増やす（または減らす）場合は、新しいライセンスを要求してその新しいライセンスを適用し、新しい値と一致するように VMware の VM プロパティを変更します。

（注） 割り当てられた vCPU は、ASAv CPU ライセンスまたはスループットライセンスと一致している必要があります。RAM は、vCPU 用に正しくサイズ調整されている必要があります。アップグレードまたはダウングレード時には、この手順に従って、ライセンスと vCPU を迅速に調整するようにします。永続的な不一致がある場合、ASAv は適切に動作しません。

手順

ステップ 1 新しいライセンスを要求します。

ステップ 2 新しいライセンスを適用します。フェールオーバーペアの場合、両方の装置に新しいライセンスを適用します。

ステップ 3 フェールオーバーを使用するかどうかに応じて、次のいずれかを実行します。

- フェールオーバーあり：vSphere Web Client で、スタンバイ ASAv の電源を切断します。たとえば、ASAv をクリックしてから [仮想マシンの電源をオフ（Power Off the virtual machine）] をクリックするか、または ASAv を右クリックして [ゲストOSをシャットダウン（Shut Down Guest OS）] を選択します。
- フェールオーバーなし：vSphere Web クライアントで、ASAv の電源を切断します。たとえば、ASAv をクリックしてから [仮想マシンの電源をオフ（Power Off the virtual machine）] をクリックするか、または ASAv を右クリックして [ゲストOSをシャットダウン（Shut Down Guest OS）] を選択します。

ステップ 4 ASAv をクリックしてから [仮想マシンの設定の編集（Edit Virtual machine settings）] をクリックします（または ASAv を右クリックして [設定の編集（Edit Settings）] を選択します）。

[Edit Settings] ダイアログボックスが表示されます。

ステップ 5 新しい vCPU ライセンスの正しい値を確認するには、ASAv のライセンスにある CPU 要件とメモリ要件を参照してください。

ステップ 6 [Virtual Hardware] タブの [CPU] で、ドロップダウン リストから新しい値を選択します。

ステップ 7 [Memory] には、新しい RAM の値を入力します。

ステップ 8 [OK] をクリックします。

ステップ 9 ASAvの電源を入れます。たとえば、[Power On the Virtual Machine] をクリックします。

ステップ 10 フェールオーバー ペアの場合：

1. アクティブ装置へのコンソールを開くか、またはアクティブ装置で ASDM を起動します。
2. スタンバイ装置の起動が終了した後、スタンバイ装置にフェールオーバーします。
   - ASDM：**[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** を選択し、[Make Standby] をクリックします。
   - CLI： **failover active**

3. アクティブ装置に対して、ステップ 3 ～ 9 を繰り返します。

次のタスク

詳細については、「ASAv のライセンス」を参照してください。

トラフィックのモニタリングおよびシステム ダッシュボード

システムには、デバイスを通過するトラフィックおよびセキュリティ ポリシーの結果を分析するために使用できる複数のダッシュボードがあります。ダッシュボード情報は、構成全体の有効性を評価し、ネットワークの問題を特定して解決するために使用します。

（注） トラフィック関連のダッシュボードに使用されるデータは、接続またはファイル ロギングを有効にするアクセス コントロール ルールから収集されます。ダッシュボードには、ロギングが有効になっていないルールと一致するトラフィックは反映されません。自分にとって重要な情報をログに記録するルールを設定してください。また、ユーザー情報はユーザー ID を収集するアイデンティティ ルールを設定している場合にのみ利用できます。さらに、侵入、ファイル、マルウェア、および Web カテゴリの情報は、それらの機能のライセンスがあり、機能を使用するルールを設定している場合のみ使用できます。

手順

ステップ 1 メイン メニューの [モニタリング（Monitoring）] をクリックして、[ダッシュボード（Dashboards）] ページを開きます。

ダッシュボードのグラフと表に表示されるデータを制御するために、定義済みの時間範囲（最後の時間や週など）を選択できます。また、特定の開始時刻と終了時刻を指定してカスタムの時間範囲を定義することもできます。

トラフィック関連のダッシュボードには、次のタイプの表示が含まれます。

- 上位 5 つの棒グラフ：これらのグラフは [ネットワークの概要（Network Overview）] ダッシュボードに表示されます。また、ダッシュボードテーブルで項目をクリックした場合、項目ごとのサマリーのダッシュボードにも表示されます。[トランザクション（Transactions）] または [データの使用状況（Data Usage）]（送受信バイトの合計）のカウント間で情報を切り替えることができます。すべてのトランザクション、許可トランザクション、または拒否トランザクションを表示するために表示を切り替えることもできます。グラフと関連付けられている表を確認する場合は、[追加表示（View More）] をクリックします。

- 表：表には特定のタイプ（アプリケーションや Web カテゴリなど）の項目が、その項目の合計トランザクション、許可トランザクション、ブロックされたトランザクション、データの使用状況、送受信バイト数とともに表示されます。raw [値（Values）] と [パーセンテージ（Percentages）] 間の数字は切り替えることができ、上位 10、100、または 1000 エントリが表示されます。項目がリンクの場合、そのリンクをクリックして、より詳細な情報が含まれているサマリー ダッシュボードを表示します。

ステップ 2 目次にある [ダッシュボード（Dashboard）] リンクをクリックして、次のデータのダッシュボードを表示します。

- [ネットワークの概要（Network Overview）]：ネットワークのトラフィックに関する概要情報が表示されます。情報には、一致したアクセス ルール（ポリシー）、ユーザーが送信側のトラフィック、接続で使用されているアプリケーション、一致した侵入シグネチャ、アクセスされた URL の Web カテゴリ、最も頻繁に接続されている宛先が含まれます。
- [ユーザー（Users）]：ネットワークの上位ユーザーが表示されます。ユーザー情報を表示するには、アイデンティティ ポリシーを設定する必要があります。
- [アプリケーション（Applications）]：ネットワークで使用されている上位アプリケーション（Facebook など）が表示されます。この情報は、インスペクションを実行済みの接続にのみ提供されます。接続は、「許可」ルールと一致するか、またはゾーン、アドレス、およびポート以外の基準を使用するブロック ルールと一致するかどうかのインスペクションが実行されます。そのため、インスペクションが必要なルールにヒットする前に接続が信頼またはブロックされている場合、アプリケーション情報は使用できません。
- [Web カテゴリ（Web Categories）]：訪問した Web サイトのカテゴリに基づいて、ネットワークで使用されている Web サイトの上位カテゴリ（ギャンブルや教育機関など）が表示されます。この情報を取得するためには、トラフィックの一致基準として Web カテゴリを使用するアクセス コントロール ルールが少なくとも 1 つ必要です。情報は、ルールに一致するトラフィック、またはルールに一致するかどうかを判断するためにインスペクションを実行する必要があるトラフィックに関してのみ提供されます。最初の Web カテゴリのアクセス コントロール ルールよりも前にあるルールと一致する接続に関するカテゴリ（またはレピュテーション）情報は表示されません。
- [ポリシー（Policies）]：一致する上位のアクセス ルールがネットワーク トラフィック別に表示されます。
- [入力ゾーン（Ingress Zones）]：デバイスに入るトラフィックが通過する上位のセキュリティ ゾーンが表示されます。
- [出力ゾーン（Egress Zones）]：デバイスから出るトラフィックが通過する上位のセキュリティ ゾーンが表示されます。
- [宛先（Destinations）]：ネットワーク トラフィックの上位の宛先が表示されます。
- [攻撃者（Attackers）]：侵入イベントをトリガーする接続の送信元である上位の攻撃者が表示されます。この情報を表示するには、アクセス ルールに侵入ポリシーを設定する必要があります。
- [ターゲット（Targets）]：攻撃の被害者である、侵入イベントの上位のターゲットが表示されます。この情報を表示するには、アクセス ルールに侵入ポリシーを設定する必要があります。

- [脅威（Threats）]トリガーされた上位の侵入ルールが表示されます。この情報を表示するには、アクセス ルールに侵入ポリシーを設定する必要があります。
- [ファイルログ（File Logs）]：ネットワーク トラフィックで確認された上位のファイル タイプが表示されます。この情報を表示するには、アクセス ルールにファイル ポリシーを設定する必要があります。
- [システム（System）]：インターフェイスとインターフェイスのステータス（IP アドレスを確認するには、そのインターフェイスにマウスオーバーします）、システムの全体的なスループット、およびシステム イベント、CPU 使用率、メモリ使用率、ディスク使用率に関する概要情報など、システムの全体的情報が表示されます。すべてのインターフェイスではなく特定のインターフェイスを表示するように、スループット グラフを制限できます。

（注） [システム（System）]ダッシュボードに表示される情報は、全体的なシステム レベルの情報です。デバイスの CLI にログインすると、さまざまなコマンドを使用して詳細情報を確認できます。たとえば、**show cpu** および **show memory** コマンドには、他の詳細を示すパラメータが含まれますが、これらのダッシュボードには **show cpu system** および **show memory system** コマンドからのデータが表示されます。

ステップ 3 目次でこれらのリンクをクリックすることもできます。

- [イベント（Events）]：イベント発生時にイベントが表示する場合に選択します。個々のアクセス ルールに関連する接続イベントを表示するには、それぞれのアクセス ルールで接続のロギングを有効にする必要があります。これらのイベントは、ユーザーの接続の問題を解決するのに役立ちます。

翻訳について
このドキュメントは、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。