Hyper-V を使用した ASAv の導入

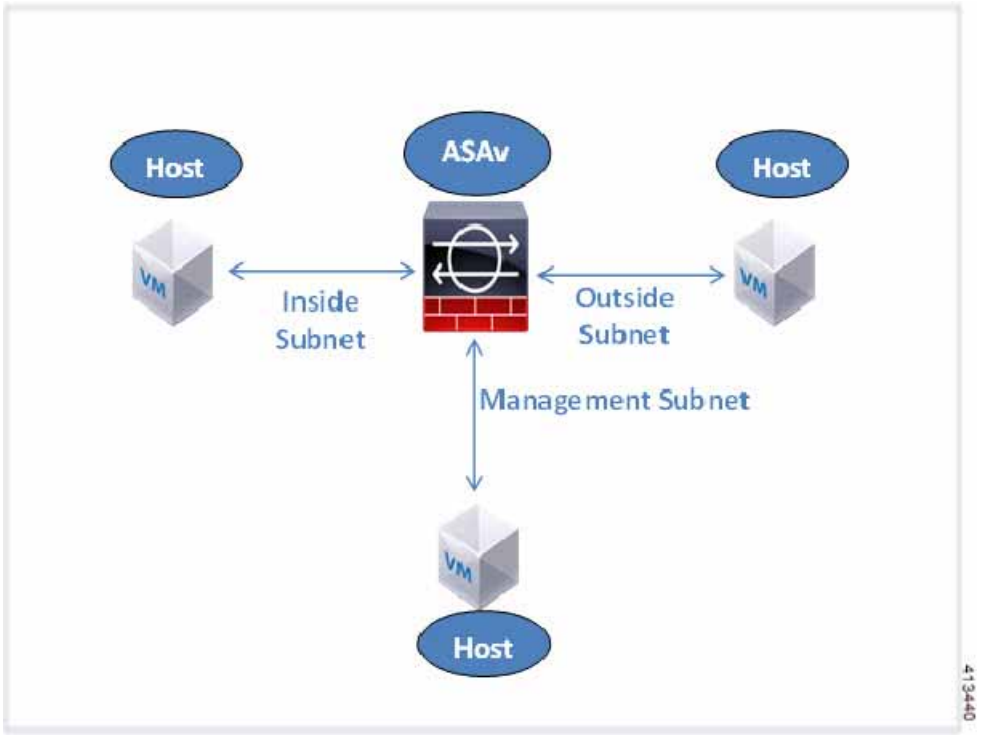
Microsoft Hyper-V を使用して ASAv を導入できます。

Hyper-V を使用した ASAv の導入について

スタンドアロンの Hyper-V サーバ上に、または Hyper-V マネージャを介して Hyper-V を導入できます。Powershell の CLI コマンドを使用してインストールする手順については、コマンドラインを使用した Hyper-V への ASAv のインストール（50 ページ）を参照してください。Hyper-V マネージャを使用してインストールする手順については、Hyper-V マネージャを使用した Hyper-V への ASAv のインストール（51 ページ）を参照してください。Hyper-V はシリアル コンソール オプションを提供していません。管理インターフェイスを介して SSH または ASDM を通じて Hyper-V を管理できます。SSH をセットアップするための情報については、SSH の設定（60 ページ）を参照してください。

図 1（46 ページ）は、ルーテッド ファイアウォール モードでの ASAv の推奨トポロジを示しています。ASAv 向けに Hyper-V でセットアップされた、管理、内部、および外部の 3 つのサブネットがあります。

図 1　ルーテッド ファイアウォール モードの ASAv の推奨トポロジ



ASAv および Hyper-V のガイドラインと制限事項

- プラットフォーム サポート
  - Cisco UCS B シリーズ サーバ
  - Cisco UCS C シリーズ サーバ
  - Hewlett Packard Proliant DL160 Gen8
- サポートされる OS
  - Windows Server 2012
  - ネイティブ Hyper-V

  注: ASAv は、現在、仮想化に使用されている最新の 64 ビット高性能プラットフォームの大多数で稼働します。
- ファイル形式

  Hyper-V への ASAv の初期導入の場合は、VHDX 形式をサポートしています。
- 第 0 日用（Day 0）構成

  必要な ASA CLI 設定コマンドを含むテキスト ファイルを作成します。手順については、第 0 日のコンフィギュレーション ファイルの準備（47 ページ）を参照してください。
- 第 0 日用構成のファイアウォール トランスペアレント モード

  設定行「firewall transparent」は、第 0 日用コンフィギュレーション ファイルの先頭に配置する必要があります。ファイル内のそれ以外の場所にあると、異常な動作が起きる場合があります。手順については、第 0 日のコンフィギュレーション ファイルの準備（47 ページ）を参照してください。

- フェールオーバー

  Hyper-V 上の ASAv はアクティブ/スタンバイ フェールオーバーをサポートしています。ルーテッド モードとトランスペアレント モードの両方でアクティブ/スタンバイ フェールオーバーを実行するには、すべての仮想ネットワーク アダプタで MAC アドレス スプーフィングを有効化する必要があります。MAC アドレス スプーフィングの設定（60 ページ）を参照してください。スタンドアロン ASAv のトランスペアレント モードの場合、管理インターフェイスの MACアドレス スプーフィングは有効にしないでください。アクティブ/アクティブ フェールオーバーはサポートされていません。

- Hyper-V は最大 8 つのインターフェイスをサポートします。Management 0/0 および GigabitEthernet 0/0 ～ 0/6。フェールオーバー リンクとして GigabitEthernet を使用できます。
- VLANs

  トランク モードでインターフェイスに VLAN を設定するには、**Set-VMNetworkAdapterVLan** Hyper-V Powershell コマンドを使用します。管理インターフェイスの NativeVlanID は、特定の VLAN として、または VLAN がない場合は「0」として設定できます。トランク モードは、Hyper-V ホストをリブートした場合は保持されません。各リブート後に、トランク モードを再設定する必要があります。

- レガシー ネットワーク アダプタはサポートされていません。
- 第 2 世代仮想マシンはサポートされていません。
- Microsoft Azure はサポートされていません。

ASAv と Hyper-V の前提条件

- MS Windows 2012 に Hyper-V をインストールします。
- 第 0 日用コンフィギュレーション テキスト ファイルを使用する場合は、それを作成します。

  ASAv の初回導入前に、第 0 日用構成を追加する必要があります。追加しない場合は、第 0 日用構成を使用するために ASAv から **write erase** を実行する必要があります。手順については、第 0 日のコンフィギュレーション ファイルの準備（47 ページ）を参照してください。

- Cisco.com から ASAv VHDX ファイルをダウンロードします。

  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。

- Hyper-V スイッチには、3 つ以上のサブネット/VLAN が構成されます。
- Hyper-V システム要件については、「Cisco ASA Compatibility」を参照してください。

第 0 日のコンフィギュレーション ファイルの準備

ASAv を起動する前に、第 0 日（Day 0）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 サーバをセットアップ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。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。

注: ASAv の初回起動前に、第 0 日用コンフィギュレーション ファイルを追加する必要があります。ASAv の初回起動後に第 0 日用コンフィギュレーション ファイルを使用することにした場合は、**write erase** コマンドを実行し、第 0 日用コンフィギュレーション ファイルを適用してから、ASAv を起動する必要があります。

注: 初期導入時に自動的に ASAv をライセンス許諾するには、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 日用コンフィギュレーション ファイルと同じディレクトリに保存します。

注: 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 コンフィギュレーション ファイルを第 0 日用コンフィギュレーション ファイルとして使用します。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。

注: 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。

手順

1. 「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ことです。day0-config 内の行の順序は重要で、既存の **show run** 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 9.5.1
   !
   interface management0/0
      nameif management
      security-level 100
      ip address 192.168.1.2 255.255.255.0
      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
   ```

2. (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。

3. (任意)ダウンロードしたファイルから ID トークンをコピーし、ID トークンのみを含むテキスト ファイルを作成します。

4. (任意)ASAv の初期導入時に自動的にライセンス許諾を行う場合は、day0-config ファイルに次の情報が含まれていることを確認してください。

   - 管理インターフェイスの IP アドレス
   - (任意)SSmart Licensing で使用する HTTP プロキシ
   - HTTP プロキシ(指定した場合)または tools.cisco.com への接続を有効にする **route** コマンド
   - tools.cisco.com を IP アドレスに解決する DNS サーバ
   - 要求する ASAv ライセンスを指定するための Smart Licensing の設定
   - (任意)CSSM での ASAv の検索を容易にするための一意のホスト名

5. 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。

```
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 (byptes): 10
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

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

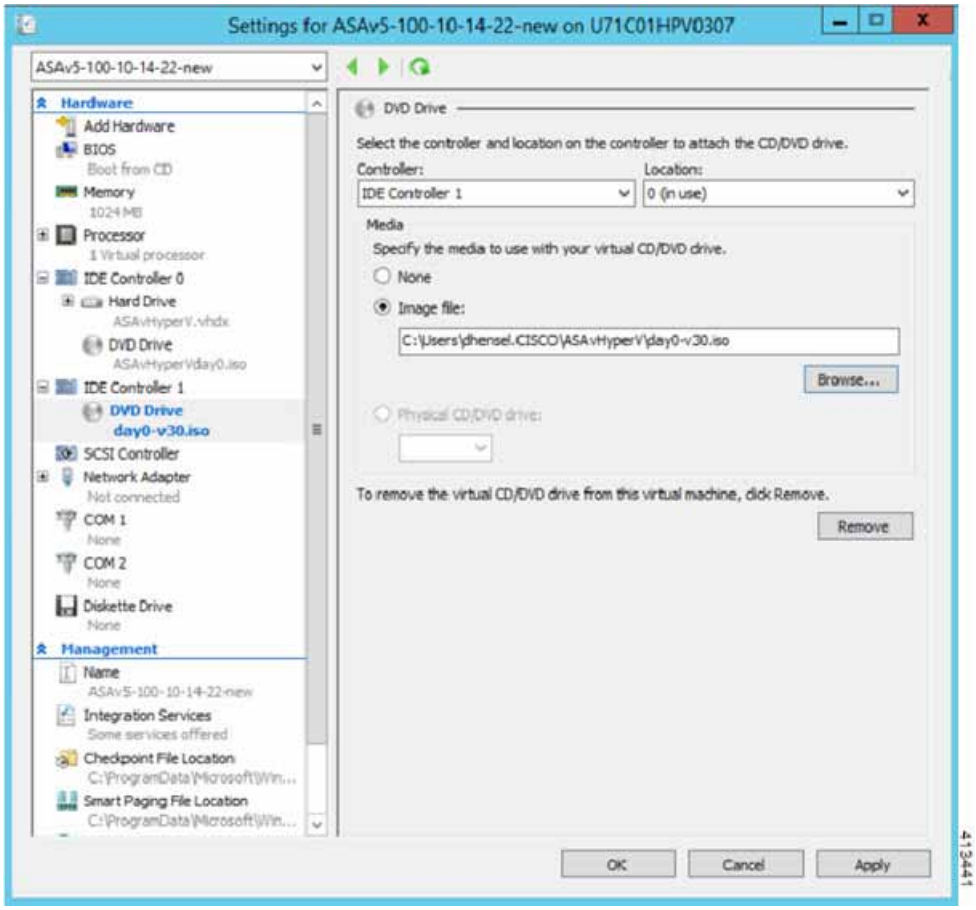
6. ステップ 1から 5 を繰り返し、導入する ASAv ごとに、適切な IP アドレスを含むデフォルトのコンフィギュレーション ファイルを作成します。

Hyper-V マネージャを使用した ASAv と第 0 日用コンフィギュレーション ファイルの導入

第 0 日用コンフィギュレーション ファイルをセットアップした後(第 0 日のコンフィギュレーション ファイルの準備 (47 ページ))、Hyper-V マネージャを使用してそれを導入できます。

手順

1. [Server Manager] > [Tools] > [Hyper-V Manager] に移動します。
2. Hyper-V マネージャの右側にある [Settings] をクリックします。[Settings] ダイアログボックスが開きます。左側の [Hardware] の下で、[IDE Controller 1] をクリックします。



3. 右側のペインの [Media] の下で、[Image file] のラジオ ボタンを選択して、第 0 日用 ISO コンフィギュレーション ファイルを保存するディレクトリを参照し、[Apply] をクリックします。ASAv は、初回起動時に、第 0 日用コンフィギュレーション ファイルの内容に基づいて構成されます。

コマンドラインを使用した Hyper-V への ASAv のインストール

Windows Powershell コマンドラインを介して Hyper-V に ASAv をインストールできます。スタンドアロンの Hyper-V サーバ上にいる場合は、コマンド ラインを使用して Hyper-V をインストールする必要があります。

手順

1. Windows Powershell を開きます。
2. ASAv を導入します。

```
new-vm -name $fullVMName -MemoryStartupBytes $memorysize -Generation 1 -vhdpath
C:\Users\jsmith.CISCO\ASAvHyperV\$ImageName.vhdx -Verbose
```

3. ASAv のモデルに応じて、CPU 数をデフォルトの 1 から変更します。

```
set-vm -Name $fullVMName -ProcessorCount 4
```

4. （任意）インターフェイス名をわかりやすい名前に変更します。

```
Get-VMNetworkAdapter -VMName $fullVMName -Name "Network Adapter" | Rename-vmNetworkAdapter -NewName
mgmt
```

5. （任意）ネットワークで必要な場合は、VLAN ID を変更します。

```
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1151 -Access -VMNetworkAdapterName "mgmt"
```

6. Hyper-V が変更を反映するように、インターフェイスを更新します。

```
Connect-VMNetworkAdapter -VMName $fullVMName -Name "mgmt" -SwitchName 1151mgmtswitch
```

7. 内部インターフェイスを追加します。

```
Add-VMNetworkAdapter -VMName $fullVMName -name "inside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1552 -Access -VMNetworkAdapterName "inside"
```

8. 外部インターフェイスを追加します。

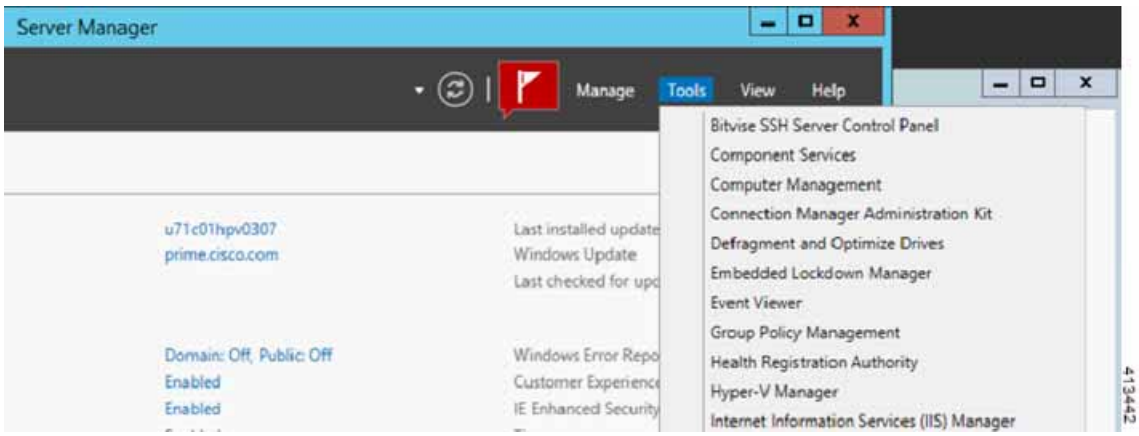
```
Add-VMNetworkAdapter -VMName $fullVMName -name "outside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1553 -Access -VMNetworkAdapterName "outside"
```

Hyper-V マネージャを使用した Hyper-V への ASAv のインストール

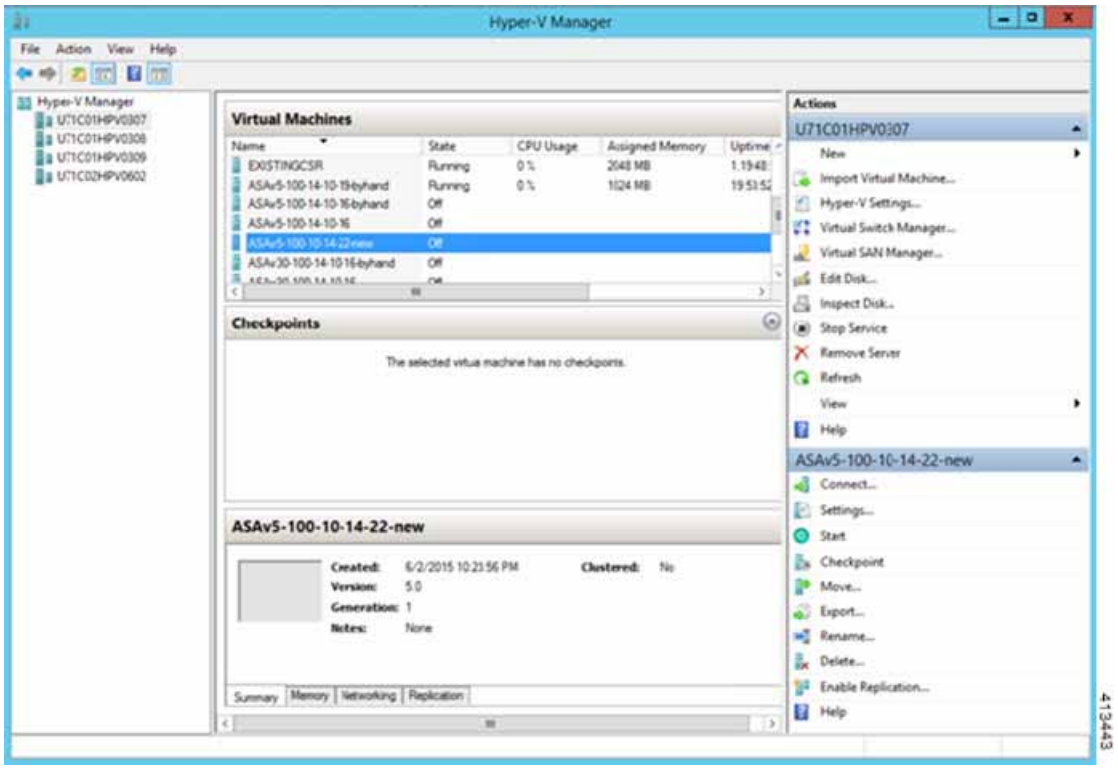
Hyper-V マネージャを使用して、Hyper-V に ASAv をインストールできます。

手順

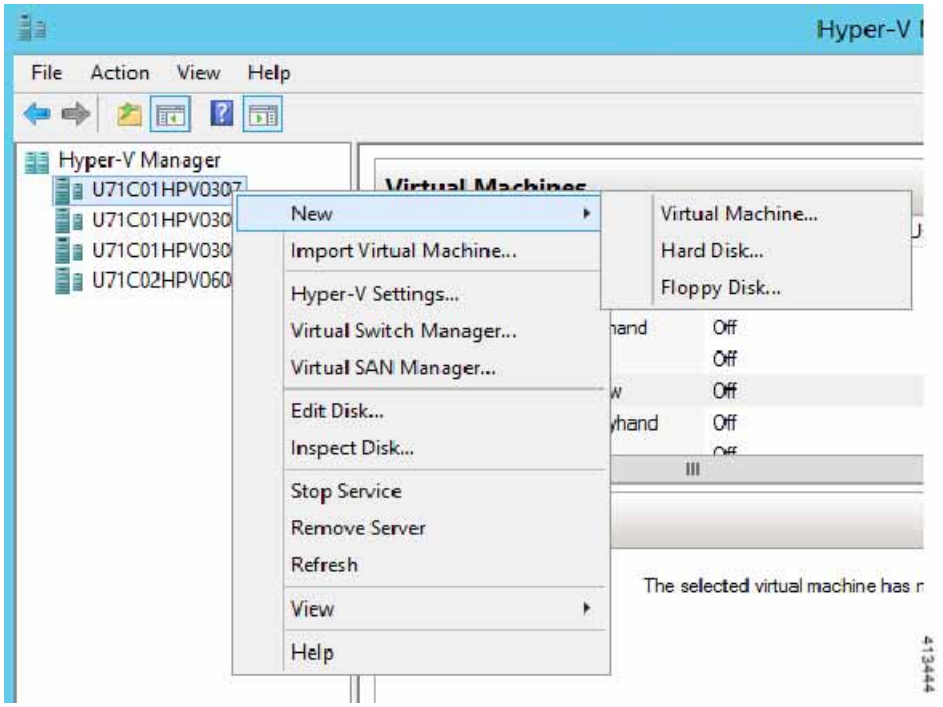
1. [Server Manager] > [Tools] > [Hyper-V Manager] に移動します。



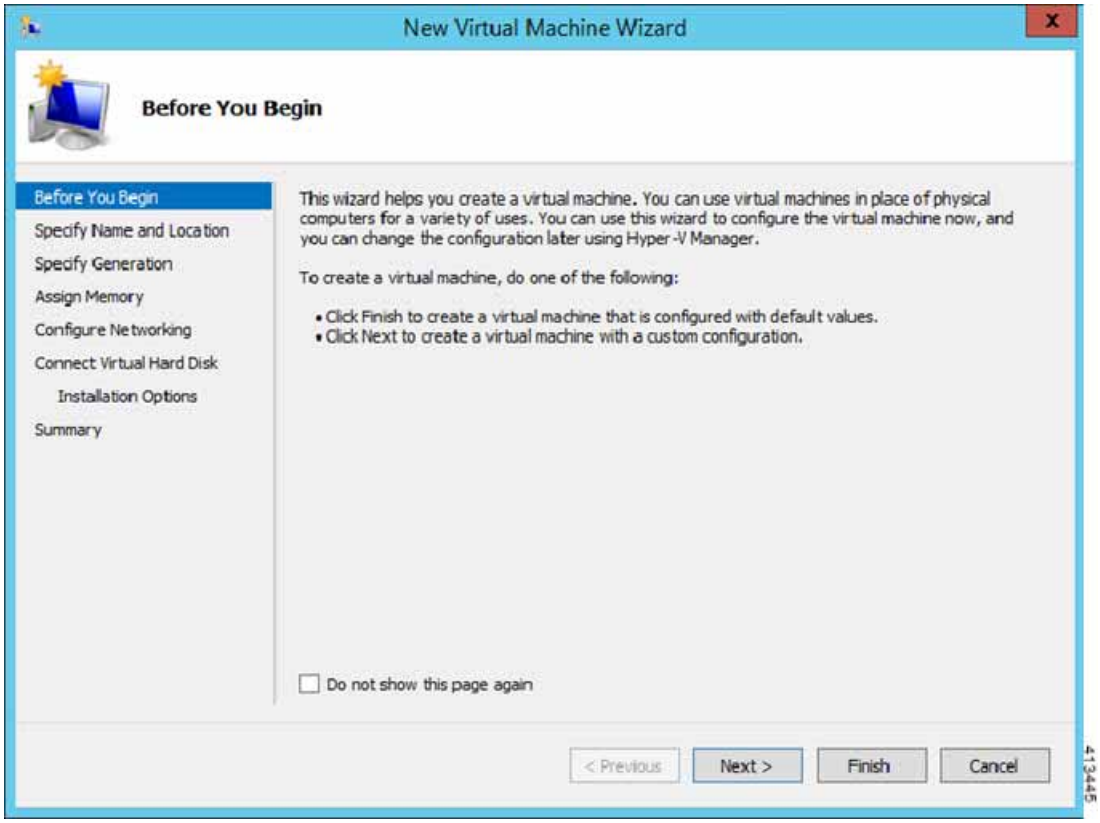
2. Hyper-V マネージャが表示されます。



3. 右側のハイパーバイザのリストから、目的のハイパーバイザを右クリックし、[New] > [Virtual Machine] を選択します。



4. [New Virtual Machine] ウィザードが表示されます。

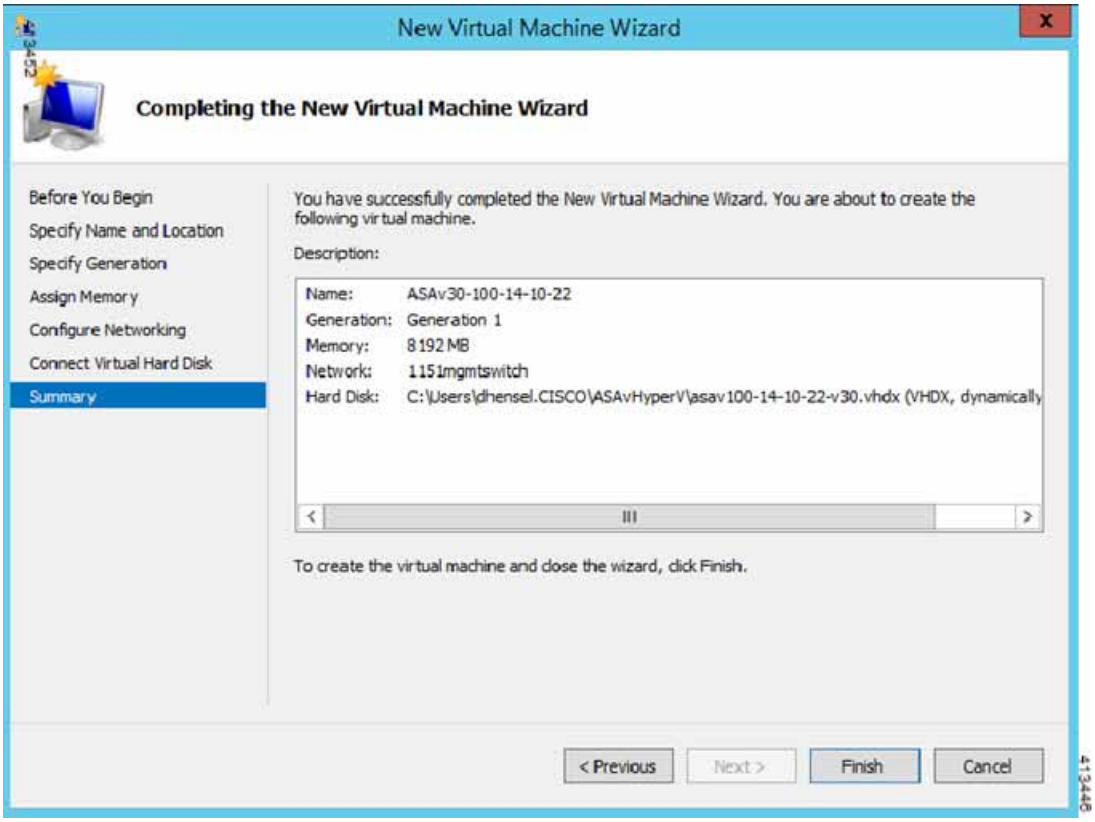


5. ウィザードを通じて作業し、次の情報を指定します。
   - ASAv の名前と場所
   - ASAv の世代

     ASAv でサポートされている唯一の世代は [Generation 1] です。
   - ASAv のメモリ量（ASAv5 の場合は 1024 MB、ASAv10 の場合は 2048 MB、ASAv30 の場合は 8192 MB）
   - ネットワーク アダプタ（セットアップ済みの仮想スイッチに接続）
   - 仮想ハード ディスクと場所

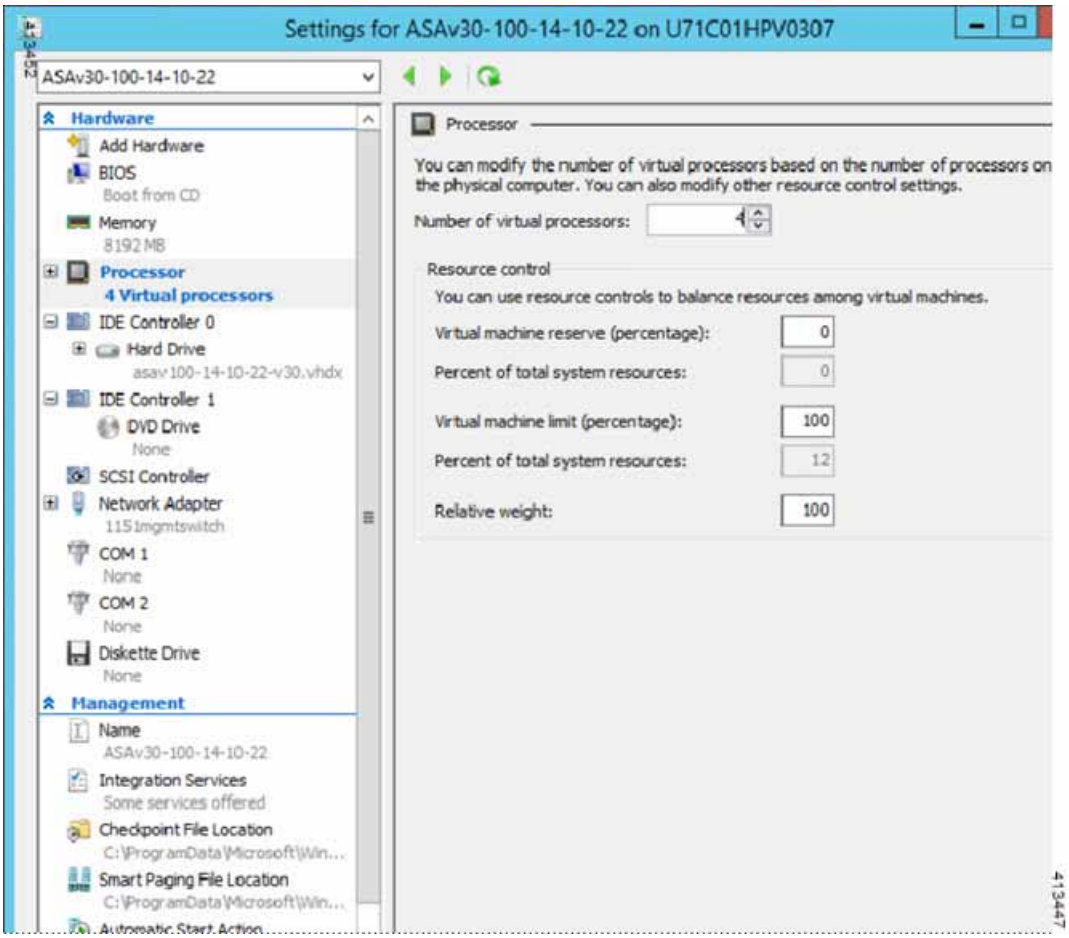
     [Use an existing virtual hard disk] を選択し、VHDX ファイルの場所を参照します。

6. [Finish] をクリックすると、ASAv 構成を示すダイアログボックスが表示されます。

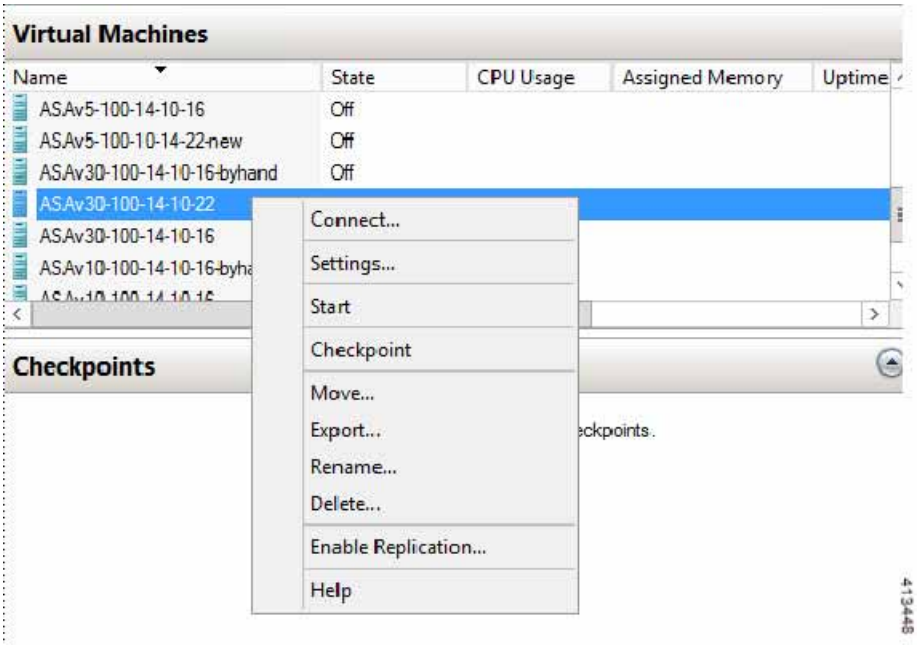


7. ASAv に 4 つの vCPU がある場合は、ASAv を起動する前に、vCPU 値を変更する必要があります。Hyper-V マネージャの右側にある [Settings] をクリックします。[Settings] ダイアログボックスが開きます。左側の [Hardware] メニューで、[Processor] をクリックし、[Processor] ペインを表示します。[Number of virtual processors] を 4 に変更します。

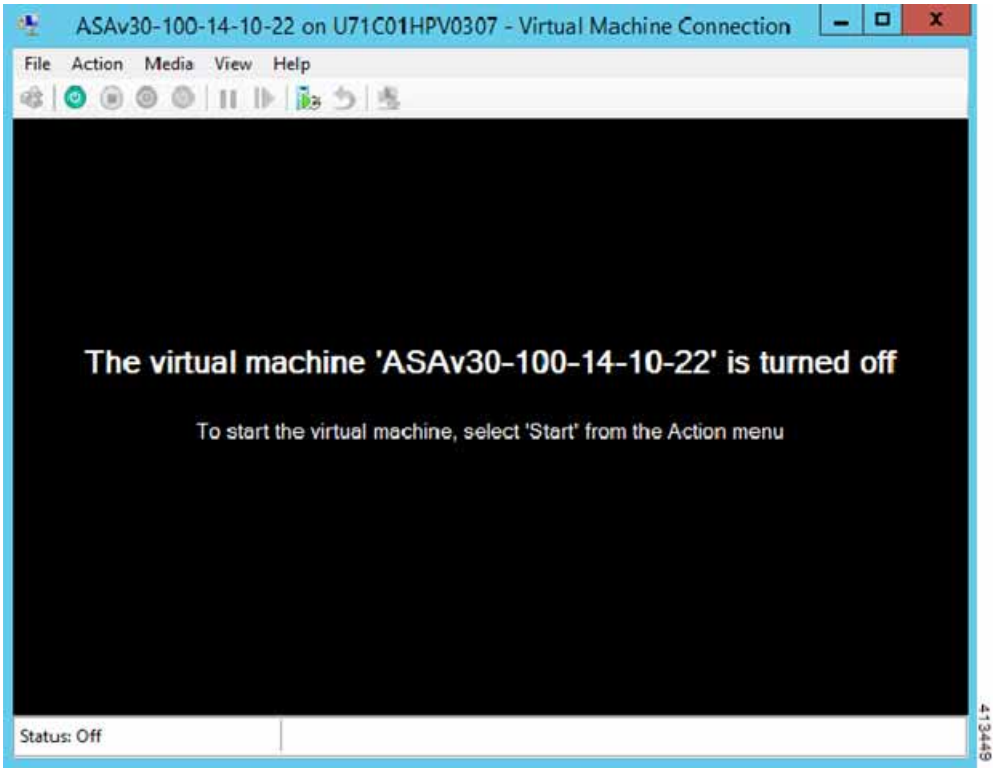
   ASAv5 と ASAv10 には 1 つの vCPU があり、ASAv30 には 4 つの vCPU があります。デフォルトは 1 です。



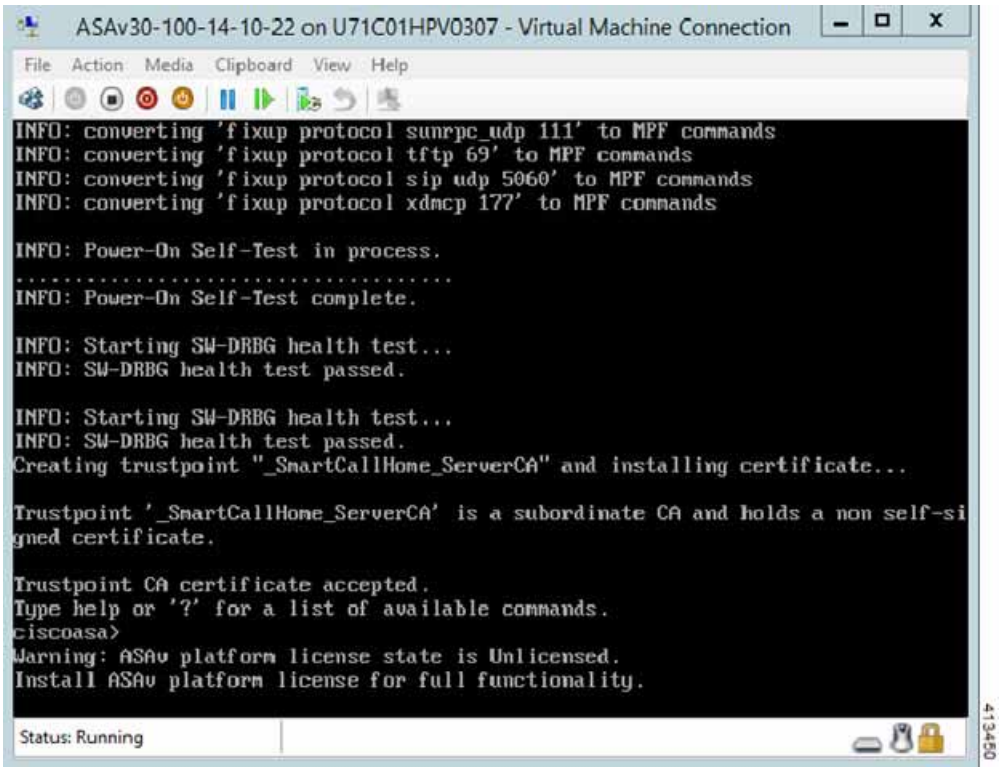
8. [Virtual Machines] メニューで、リスト内の ASAv の名前を右クリックし、[Connect] をクリックして、ASAv に接続します。コンソールが開き、停止されている ASAv が示されます。



9. [Virtual Machine Connection] コンソール ウィンドウで、青緑色の開始ボタンをクリックして、ASAv を起動します。



10. ASAv の起動の進行状況がコンソールに表示されます。



Hyper-V マネージャからのネットワーク アダプタの追加

新しく導入された ASAv のネットワーク アダプタは 1 つだけです。さらに 2 つ以上のネットワーク アダプタを追加する必要があります。この例では、内部ネットワーク アダプタを追加します。

はじめる前に

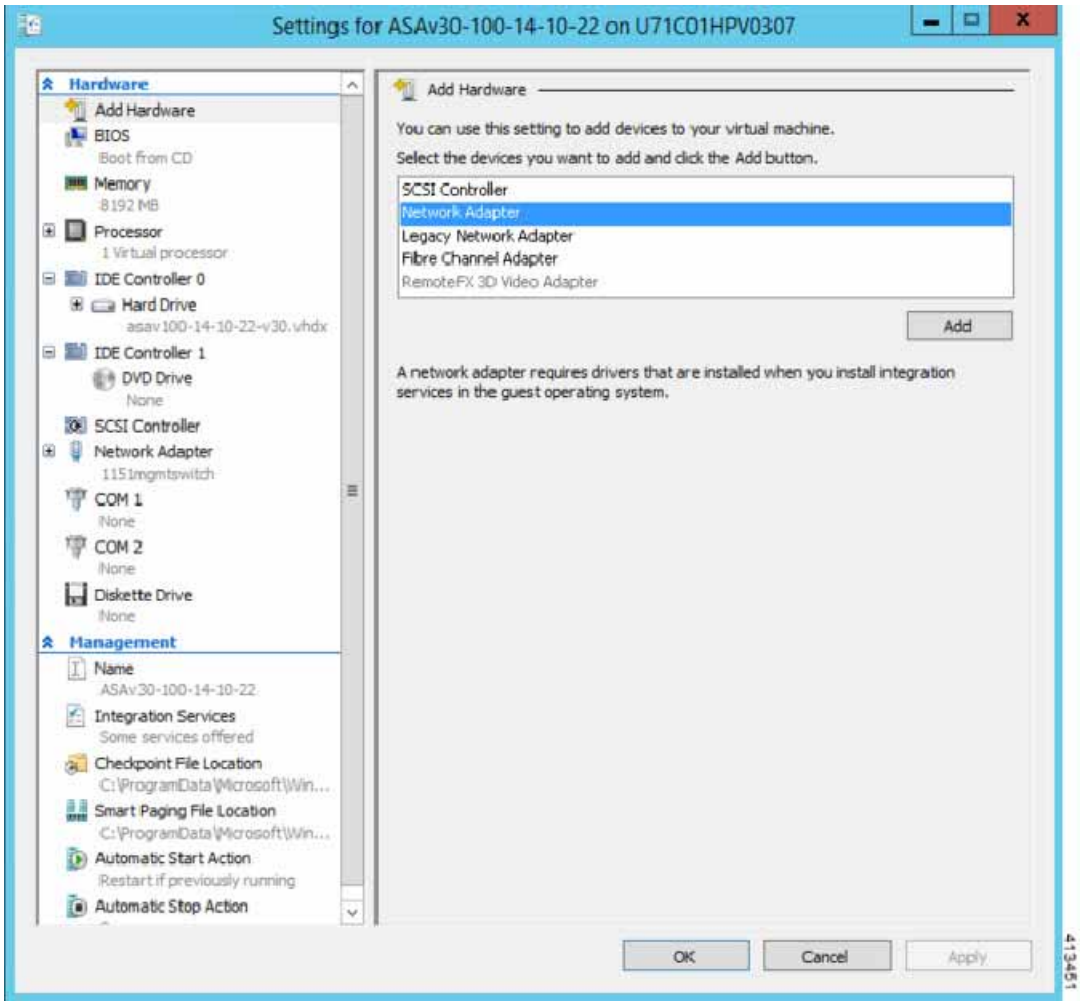
- ASAv はオフ状態になっている必要があります。

手順

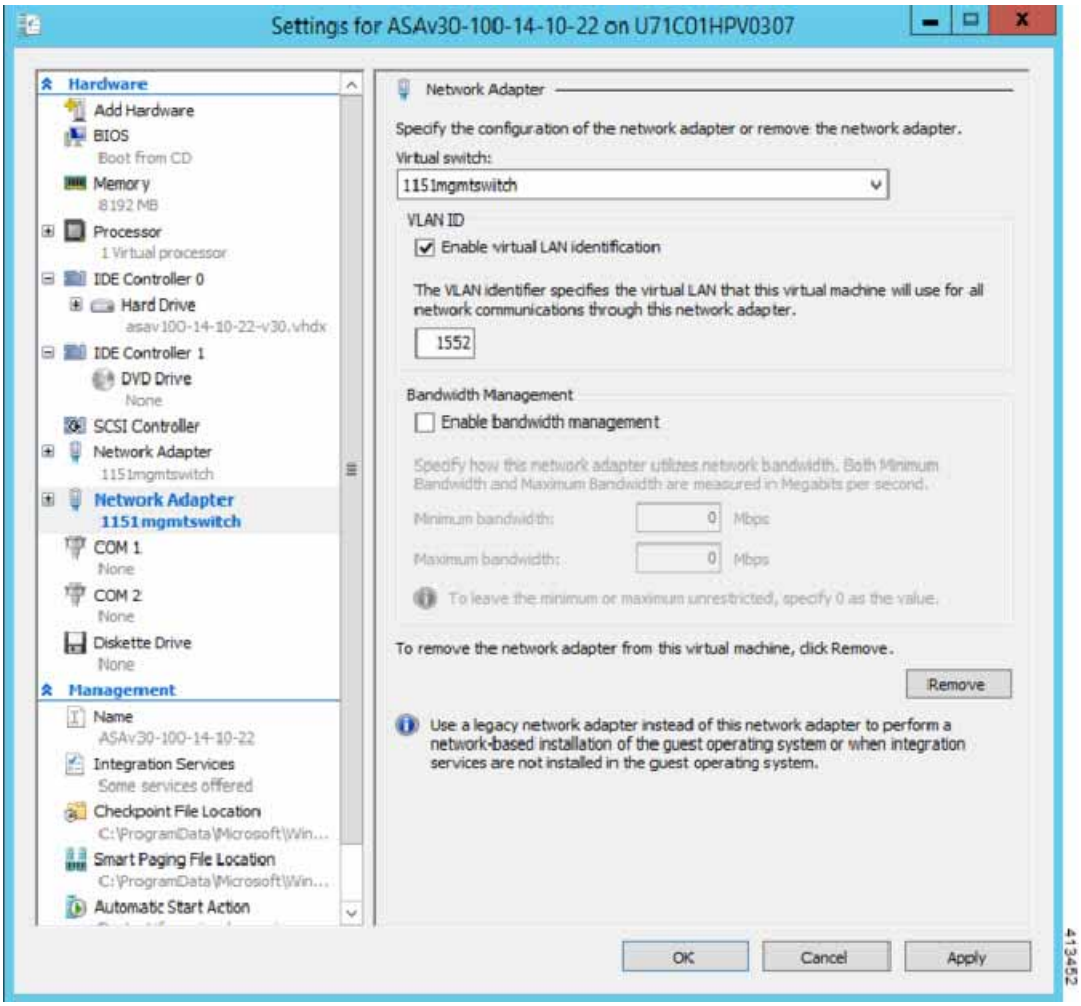
1. Hyper-V マネージャの右側にある [Settings] をクリックします。[Settings] ダイアログボックスが開きます。左側の [Hardware] メニューで、[Add Hardware] をクリックし、次に [Network Adapter] をクリックします。

   注: レガシー ネットワーク アダプタを使用しないでください。

Hyper-V マネージャからのネットワーク アダプタの追加



2. ネットワーク アダプタの追加後、仮想スイッチとその他の機能を変更できます。また、必要に応じて VLAN ID を設定できます。



ネットワーク アダプタの名前の変更

Hyper-V では、「Network Adapter」という汎用ネットワーク インターフェイス名が使用されます。このため、ネットワーク インターフェイスがすべて同じ名前であると、紛らわしい場合があります。Hyper-V マネージャを使用して名前を変更することはできません。Windows Powershell コマンドを使用して変更する必要があります。

例

```
$NICRENAME= Get-VMNetworkAdapter -VMName 'ASAvVM' -Name "Network Adapter"
rename-VMNetworkAdapter -VMNetworkAdapter $NICRENAME[0] -newname inside
rename-VMNetworkAdapter -VMNetworkAdapter $NICRENAME[1] -newname outside
```

MAC アドレス スプーフィングの設定

ASAv がトランスペアレント モードでパケットを渡し、HA アクティブ/スタンバイ フェールオーバーに対応できるように、すべてのインターフェイスの MAC アドレス スプーフィングをオンにする必要があります。Hyper-V マネージャ内で、または Powershell コマンドを使用して、これを実行できます。

Hyper-V マネージャでの手順

1. Hyper-V マネージャの右側にある [Settings] をクリックします。[Settings] ダイアログボックスが開きます。左側の [Hardware] メニューで、[Inside] をクリックし、メニューを展開して [Advanced Features] をクリックし、MAC アドレス オプションを表示します。[Enable MAC address spoofing] ラジオ ボタンをクリックします。
2. 外部インターフェイスでステップ 1 を繰り返します。

Powershell コマンド

```
Set-VMNetworkAdapter -VMName $vm_name\
-ComputerName $computer_name -MacAddressSpoofing On\
-VMNetworkAdapterName $network_adapter\r"
```

SSH の設定

Hyper-V マネージャの [Virtual Machine Connection] から管理インターフェイスを介して SSH アクセスできるように ASAv を設定できます。第 0 日用コンフィギュレーション ファイルを使用している場合は、ASAv への SSH アクセスを追加できます。詳細については、「第 0 日のコンフィギュレーション ファイルの準備（47 ページ）」を参照してください。

手順

1. RSAキー ペアが存在することを確認します。

   ```
   asav# show crypto key mypubkey rsa
   ```

2. RSAキー ペアがない場合は、RSA キー ペアを生成します。

   ```
   asav(conf t)# crypto key generate rsa modulus 2048
   ```

   例

   ```
   asav((conf t)#
   username test password test123 privilege 15
   aaa authentication ssh console LOCAL
   ssh 10.7.24.0 255.255.255.0 management
   ssh version 2
   ```

3. 別の PC から SSH を使用して ASAv にアクセスできることを確認します。