使用 Hyper-V 部署 ASA 虚拟

您可以使用 Microsoft Hyper-V 部署 ASA 虚拟。

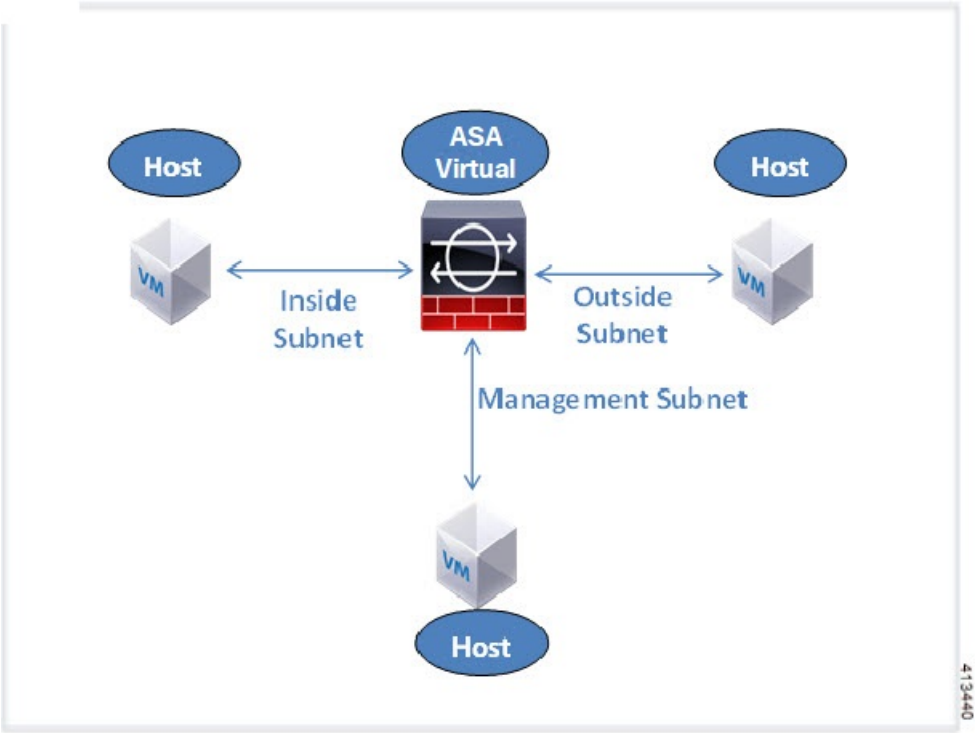
重要事项 从 9.13(1) 开始，ASA 虚拟的最低内存要求为 2GB。如果当前 ASA 虚拟的内存少于 2GB，您将无法在不增加 ASA 虚拟机内存的情况下，从早期版本升级到 9.13(1) 及更高版本。您也可以使用 9.13(1) 版本重新部署新的 ASA 虚拟机。

关于使用 Hyper-V 的 ASA 虚拟部署

您可以在独立的 Hyper-V 服务器上或通过 Hyper-V 管理器部署 Hyper-V。有关使用 Powershell CLI 命令进行安装的说明，请参阅“使用命令行在 Hyper-V 上安装 ASA 虚拟”，第 46 页。有关使用 Hyper-V 管理器进行安装的说明，请参阅“使用 Hyper-V 管理器在 Hyper-V 上安装 ASA 虚拟”，第 46 页。Hyper-V 未提供串行控制台选项。您可以在管理接口上通过 SSH 或 ASDM 管理 Hyper-V。有关设置 SSH 的信息，请参阅“配置 SSH”，第 54 页。

下图显示了在路由防火墙模式下建议用于 ASA 虚拟的网络拓扑。在 Hyper-V 中为 ASA 虚拟设置了三个子网 - 管理、内部和外部。

图 *1:* 在路由防火墙模式下建议用于 ***ASA*** 虚拟的网络拓扑



ASA 虚拟 和 Hyper-V 的准则和限制

- 平台支持
  - 思科 UCS B 系列服务器
  - 思科 UCS C 系列服务器
  - Hewlett Packard Proliant DL160 Gen8
- 操作系统支持
  - Windows Server 2012
  - 原生 Hyper-V

注释 ASA 虚拟 应该在当今用于虚拟化的最现代、64 位高性能平台上运行。

- 文件格式

  支持 VHDX 格式以便在 Hyper-V 上进行 ASA 虚拟 的初始部署。

- Day 0 配置

  您创建一个文本文件，其中包含您需要的 ASA CLI 配置命令。有关程序，请参阅准备 Day 0 配置文件。

- Day 0 配置的防火墙透明模式

  配置行“firewall transparent”必须位于 Day 0 配置文件的顶部；如果它出现在文件中的其他任何位置，您可能会遇到反常的行为。有关程序，请参阅准备 Day 0 配置文件。

- 故障转移

  Hyper-V 上的 ASA 虚拟 支持主用/备用故障转移。对于路由模式和透明模式下的主用/备用故障转移，您必须在所有虚拟网络适配器中启用 MAC 地址欺骗。请参阅“配置 MAC 地址欺骗”，第 53 页。对于独立 ASA 虚拟 的透明模式，管理接口不应启用 MAC 地址欺骗。不支持主用/主用故障转移。

- Hyper-V 最多支持八个接口。Management 0/0 和 GigabitEthernet 0/0 至 0/6。您可以将 GigabitEthernet 用作故障转移链路。

- VLAN

  使用 **Set-VMNetworkAdapterVLan** Hyper-V Powershell 命令在中继模式下的接口上设置 VLAN。您可以将管理接口的 NativeVlanID 设置为特定的 VLAN，或设置为“0”（如果没有 VLAN）。中继模式在 Hyper-V 主机重新启动期间不会持续存在。您必须在每次重新启动后重新配置中继模式。

- 不支持传统网络适配器。

- 不支持第 2 代虚拟机。

- 不支持 Microsoft Azure。

ASA 虚拟 和 Hyper-V 的前提条件

- 在 MS Windows 2012 上安装 Hyper-V。

- 创建 Day 0 配置文本文件（如果要使用）。

  在首次部署 ASA 虚拟 之前，必须先添加 Day 0 配置文件；否则，您必须从 ASA 虚拟 执行 write erase，才能使用 Day 0 配置。有关程序，请参阅准备 Day 0 配置文件。

- 从 Cisco.com 下载 ASA 虚拟 VHDX 文件。

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

注释 需要 Cisco.com 登录信息和思科服务合同。

- 至少配置有三个子网/VLAN 的 Hyper-V 交换机。

- 有关 Hyper-V 系统要求，请参阅思科 Cisco Secure Firewall ASA 兼容性。

准备 Day 0 配置文件

在启动 ASA 虚拟之前，您可以准备一个 Day 0 配置文件。此文件是包含将在 ASA 虚拟 启动时应用的 ASA 虚拟 配置的文本文件。此初始配置将放入您选择的工作目录中名为“day0-config”的文本文件，并写入首次启动时安装和读取的 day0.iso 文件。Day 0 配置文件必须至少包含将激活管理接口以及设置用于公共密钥身份验证的 SSH 服务器的命令，但它还可包含完整的 ASA 配置。day0.iso 文件（自定义 day0.iso 或默认 day0.iso）必须在首次启动过程中可用。

开始之前

我们在本示例中使用的是 Linux，但对于 Windows 也有类似的实用程序。

- 要在初始部署过程中自动完成 ASA 虚拟 的许可过程，请将从思科智能软件管理器下载的智能许可身份 (ID) 令牌放入与 Day 0 配置文件处于同一目录且名为“idtoken”的文本文件。
- 如果要在透明模式下部署 ASA 虚拟，则必须在透明模式下将已知的运行 ASA 配置文件用作 Day 0 配置文件。这不适用于路由防火墙的 Day 0 配置文件。
- 您必须在首次启动 ASA 虚拟 之前添加 Day 0 配置文件。如果您决定要在初始启动 ASA 虚拟 之后使用 Day 0 配置，则必须执行 **write erase** 命令，应用 Day 0 配置文件，然后启动 ASA 虚拟。

步骤 1 在名为“day0-config”的文本文件中输入 ASA 虚拟的 CLI 配置。添加三个接口的接口配置和所需的任何其他配置。

第一行应以 ASA 版本开头。day0-config 应该是有效的 ASA 配置。生成 day0-config 的最佳方式是从现有的 ASA 或 ASA 虚拟 复制一个运行配置的所需部分。day0-config 中的行顺序很重要，应与现有的 show run 命令输出中看到的顺序相符。

示例：

```
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
```

步骤 2 （可选）将思科智能软件管理器发布的智能许可证身份令牌文件下载到您的计算机。

步骤 3 （可选）从下载文件复制 ID 令牌并将其放入仅包含 ID 令牌的文本文件。

步骤 4 （可选）若要在初始 ASA 虚拟 部署过程中进行自动许可，请确保 day0-config 文件中包含以下信息：

- 管理接口 IP 地址
- （可选）要用于智能许可的 HTTP 代理
- 用于启用与 HTTP 代理（如果指定）或 tools.cisco.com 的连接的 route 命令
- 将 tools.cisco.com 解析为 IP 地址的 DNS 服务器
- 指定您正请求的 ASA 虚拟 许可证的智能许可配置
- （可选）更加便于 ASA 虚拟 在 CSSM 中进行查找的唯一主机名

步骤 5 通过将文本文件转换成 ISO 文件生成虚拟 CD-ROM：

```
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$
```

身份令牌自动向智能许可服务器注册 ASA 虚拟。

步骤 6 重复步骤 1 到 5，使用相应的 IP 地址为要部署的每个 ASA 虚拟 创建单独的默认配置文件。

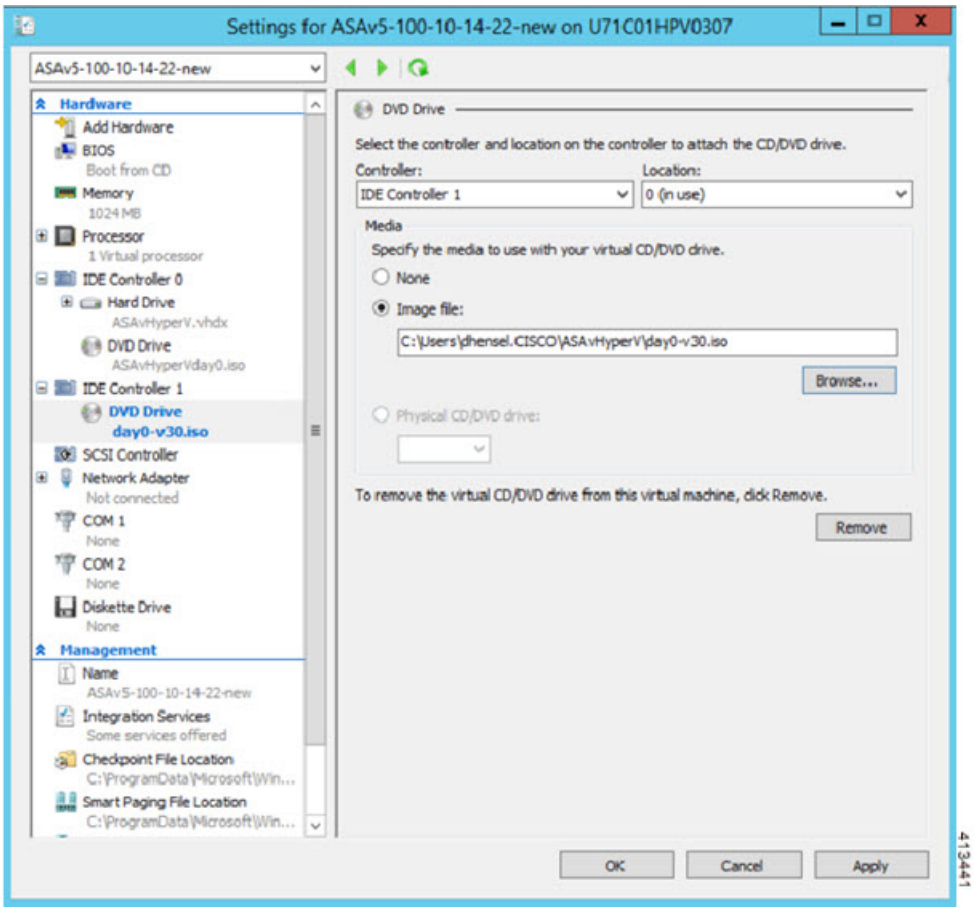
使用 Hyper-V 管理器通过 Day 0 配置文件部署 ASA 虚拟

在设置 Day 0 配置文件（准备 Day 0 配置文件）之后，您可以使用 Hyper-V 管理器进行部署。

步骤 1 转至**服务器管理器 (Server Manager)** > **工具 (Tools)** > **Hyper-V 管理器 (Hyper-V Manager)**。

步骤 2 在 Hyper-V 管理器右侧点击**设置 (Settings)**。“设置”(Settings) 对话框将打开。在左侧的**硬件 (Hardware)** 下，点击 **IDE 控制器 1 (IDE Controller 1)**。

图 *2: Hyper-V* 管理器



步骤 3 在右窗格的**媒体 (Media)** 下，选择**映像文件 (Image file)** 单选按钮，浏览到您保存 Day 0 ISO 配置文件的目录，然后点击**应用 (Apply)**。当您首次启动 ASA 虚拟时，系统将基于 Day 0 配置文件中的内容对其进行配置。

使用命令行在 Hyper-V 上安装 ASA 虚拟

您可以通过 Windows Powershell 命令行在 Hyper-V 上安装 ASA 虚拟。如果您在独立的 Hyper-V 服务器上，则必须使用命令行安装 Hyper-V。

步骤 1 打开 Windows Powershell。

步骤 2 部署 ASA 虚拟：

示例：

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

步骤 3 根据您的 ASA 虚拟型号，更改默认的 CPU 计数 (1)。

示例：

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

步骤 4 （可选）将接口名称更改为对您有意义的名称。

示例：

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

步骤 5 （可选）如果您的网络需要，请更改 VLAN ID。

示例：

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

步骤 6 刷新接口，以便 Hyper-V 获取所做的更改。

示例：

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

步骤 7 添加内部接口。

示例：

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

步骤 8 添加外部接口。

示例：

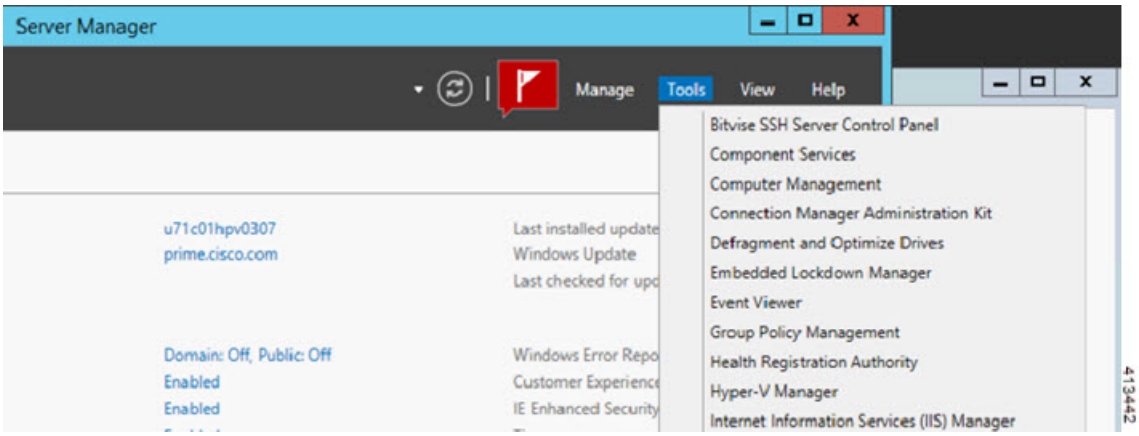
```
Add-VMNetworkAdapter -VMName $fullVMName -name "outside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1553 -Access -VMNetworkAdapterName “outside"
```

使用 Hyper-V 管理器在 Hyper-V 上安装 ASA 虚拟

您可以使用 Hyper-V 管理器在 Hyper-V 上安装 ASA 虚拟。

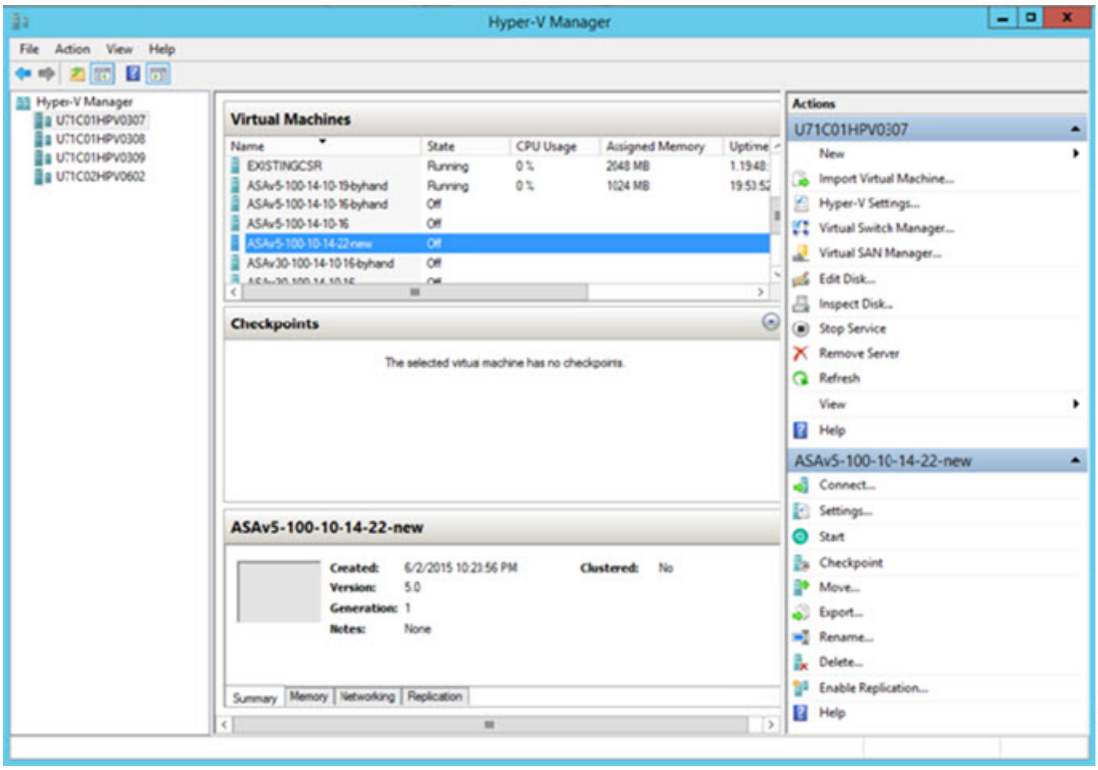
步骤 1 转至**服务器管理器 (Server Manager)** > **工具 (Tools)** > **Hyper-V 管理器 (Hyper-V Manager)**。

图 *3:* 服务器管理程序



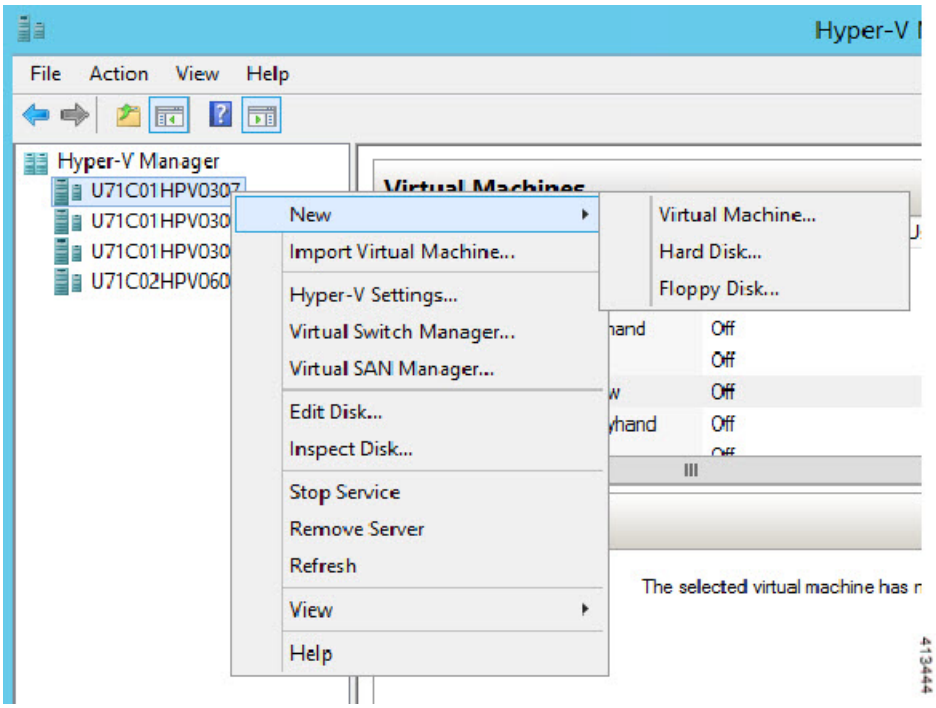
步骤 2 此时将出现 Hyper-V 管理器。

图 *4: Hyper-V* 管理器



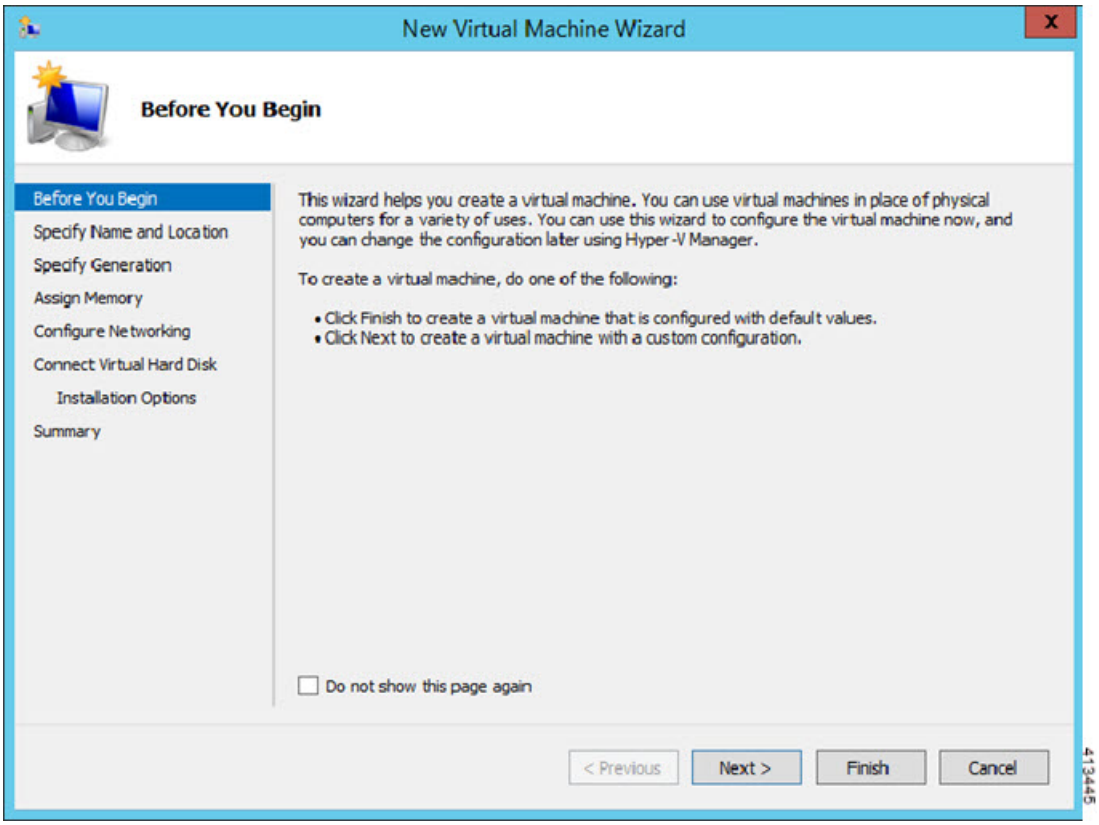
步骤 3 从右侧的虚拟机监控程序列表中，右键点击列表中的所需虚拟机监控程序，然后选择**新建 (New)** > **虚拟机 (Virtual Machine)**。

图 *5:* 启动新虚拟机



步骤 4 此时将出现“新建虚拟机向导”(New Virtual Machine Wizard)。

图 *6: New Virtual Machine Wizard*



步骤 5 执行该向导的各个步骤，指定以下信息：

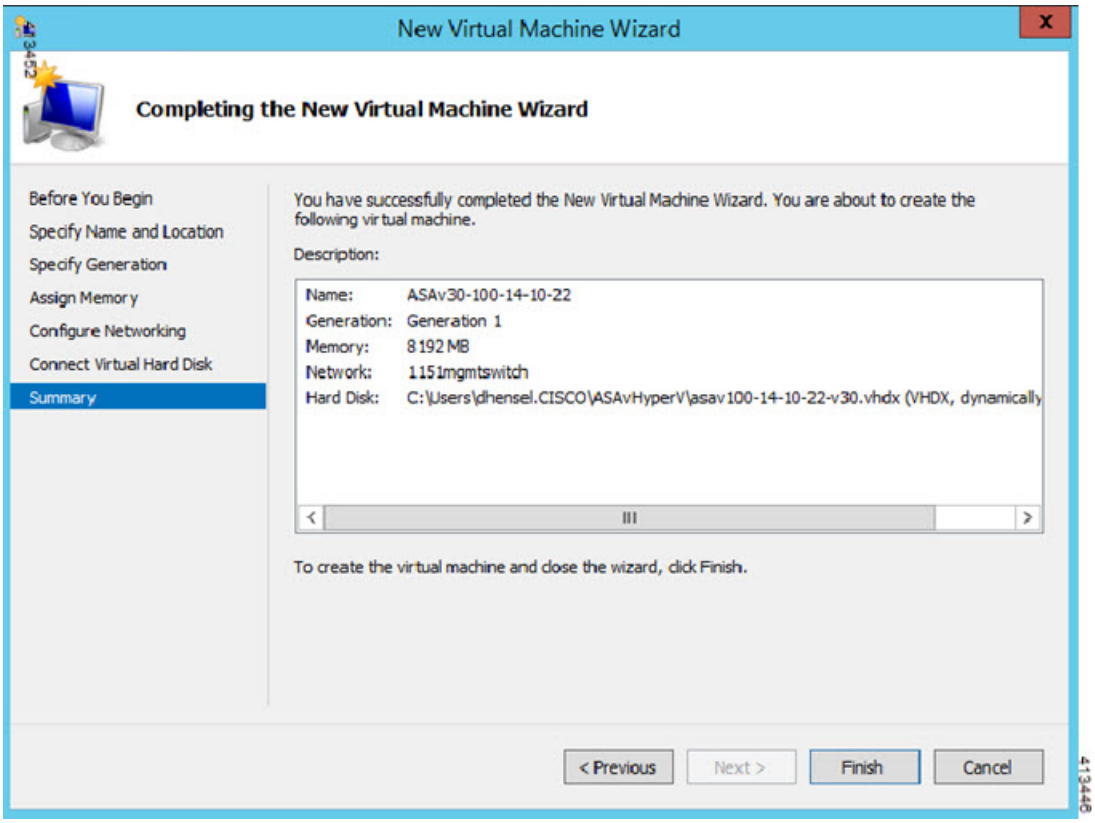
- 您的 ASA 虚拟 的名称和位置
- 生成您的 ASA 虚拟

  ASA 虚拟支持的唯一代系是**第 1 代**。
- ASA 虚拟的内存量 （100Mbps 为 1024 MB，1Gbps 为 2048 MB，2Gbps 为 8192 MB）
- 网络适配器（连接到您已设置的虚拟交换机）
- 虚拟硬盘和位置

  选择**使用现有的虚拟硬盘 (Use an existing virtual hard disk)**，然后浏览到 VHDX 文件的位置。

步骤 6 点击“完成”(Finish)，此时将出现一个显示 ASA 虚拟配置的对话框。

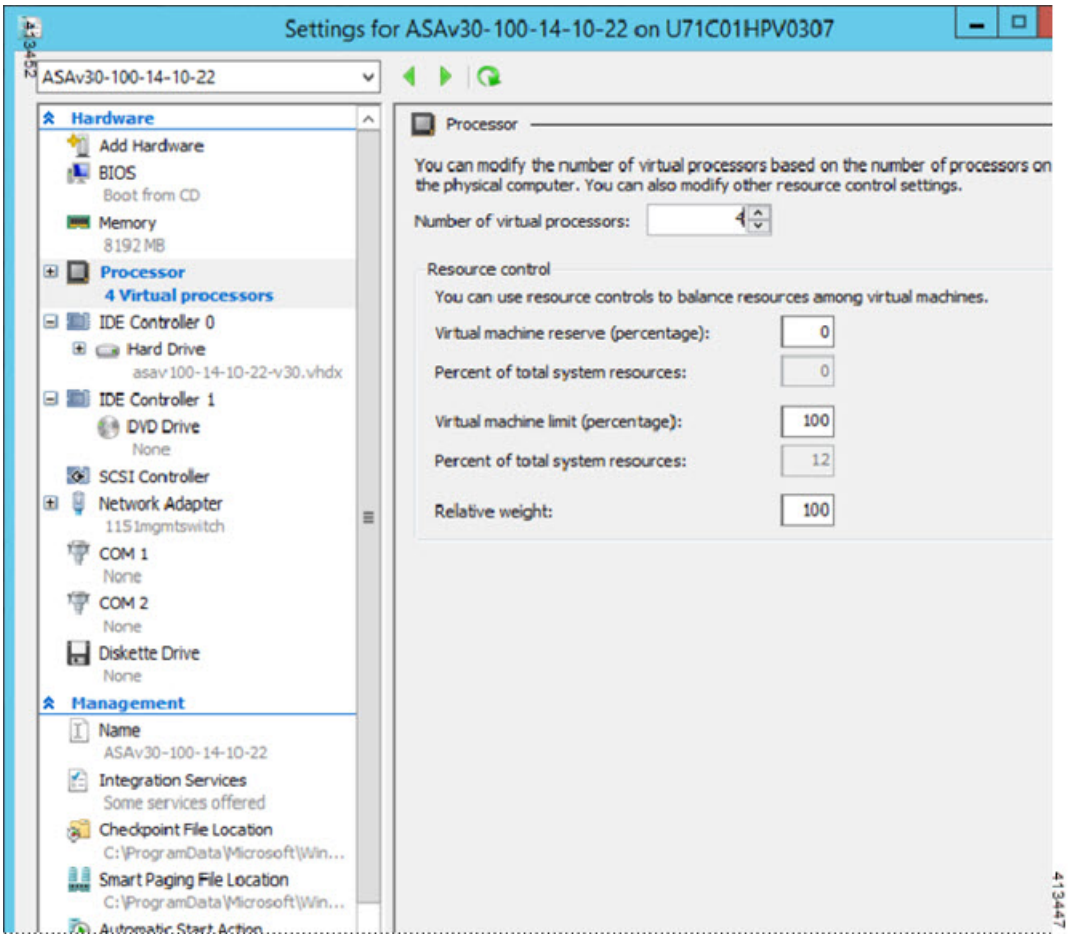
图 7: 新虚拟机摘要



步骤 7 如果您的 ASA 虚拟有四个 vCPU，则必须在启动 ASA 虚拟之前修改 vCPU 值。在 Hyper-V 管理器右侧点击**设置 (Settings)**。“设置”(Settings) 对话框将打开。在左侧的“硬件”(Hardware) 菜单下，点击**处理器 (Processor)** 以访问“处理器”(Processor) 窗格。将 **Number of virtual processors** 更改为 4。

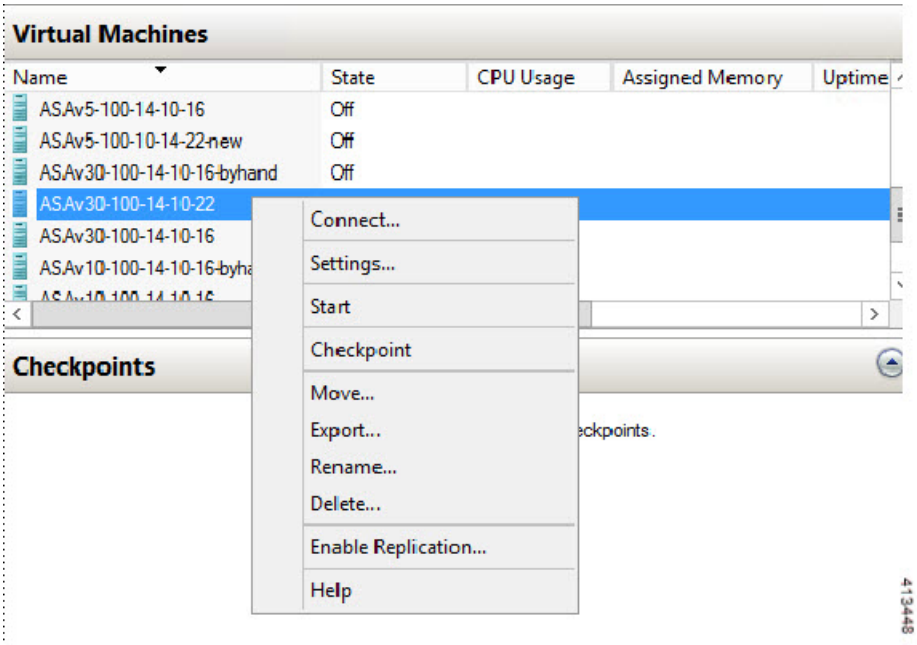
100Mbps 和1Gbps 授权具有一个 vCPU，2Gbps 授权具有四个 Vcpu。默认值为 1。

图 *8:* 虚拟机处理器设置



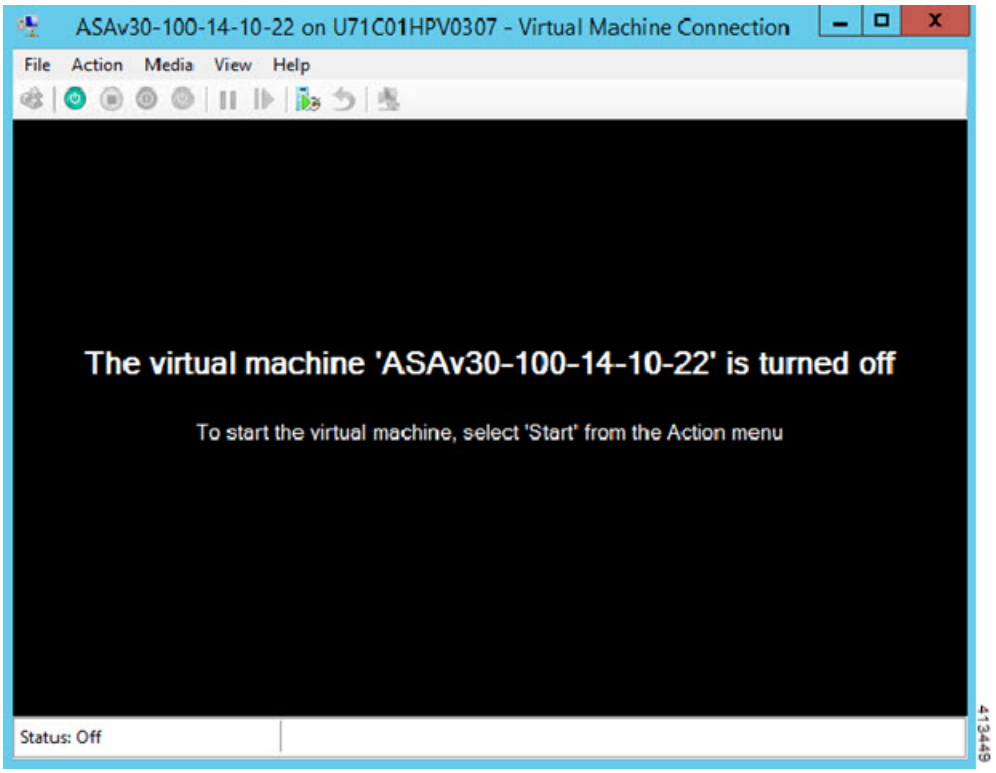
步骤 8 在“虚拟机”(Virtual Machines) 菜单中，连接到您的 ASA 虚拟，方法是右键点击列表中的 ASA 虚拟名称，然后点击**连接 (Connect)**。控制台将打开，显示已停止的 ASA 虚拟。

图 *9:* 连接到虚拟机



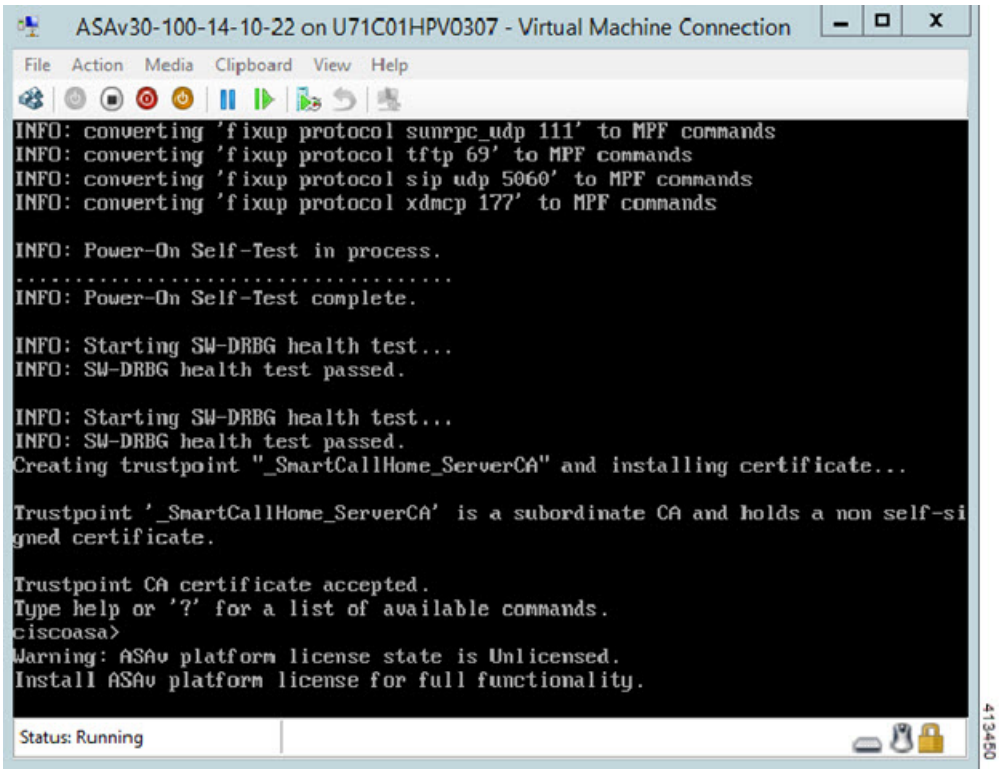
步骤 9 在“虚拟机连接”(Virtual Machine Connection) 控制台窗口中，点击蓝绿色的“启动”(Start) 按钮启动 ASA 虚拟。

图 *10:* 启动虚拟机



步骤 10 ASA 虚拟的启动过程会在控制台中显示。

图 *11:* 虚拟机启动过程



从 Hyper-V 管理器添加网络适配器

新部署的ASA虚拟只有一个网络适配器。您需要至少添加两个网络适配器。在本示例中，我们将添加内部网络适配器。

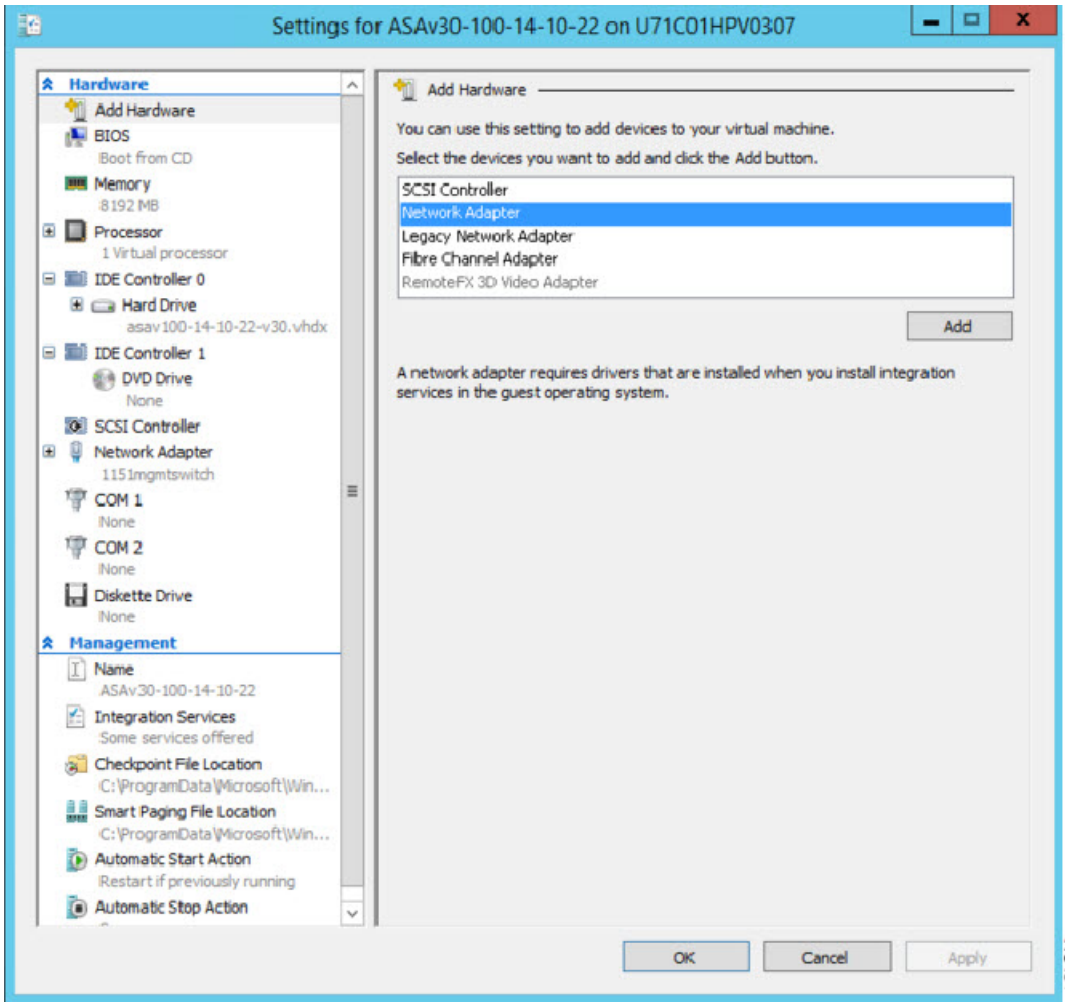
开始之前

- ASA 虚拟 必须处于关闭状态。

步骤 1 在 Hyper-V 管理器右侧点击**设置 (Settings)**。“设置”(Settings) 对话框将打开。在左侧的“硬件”(Hardware) 菜单下，点击**添加硬件 (Add Hardware)**，然后点击**网络适配器 (Network Adapter)**。

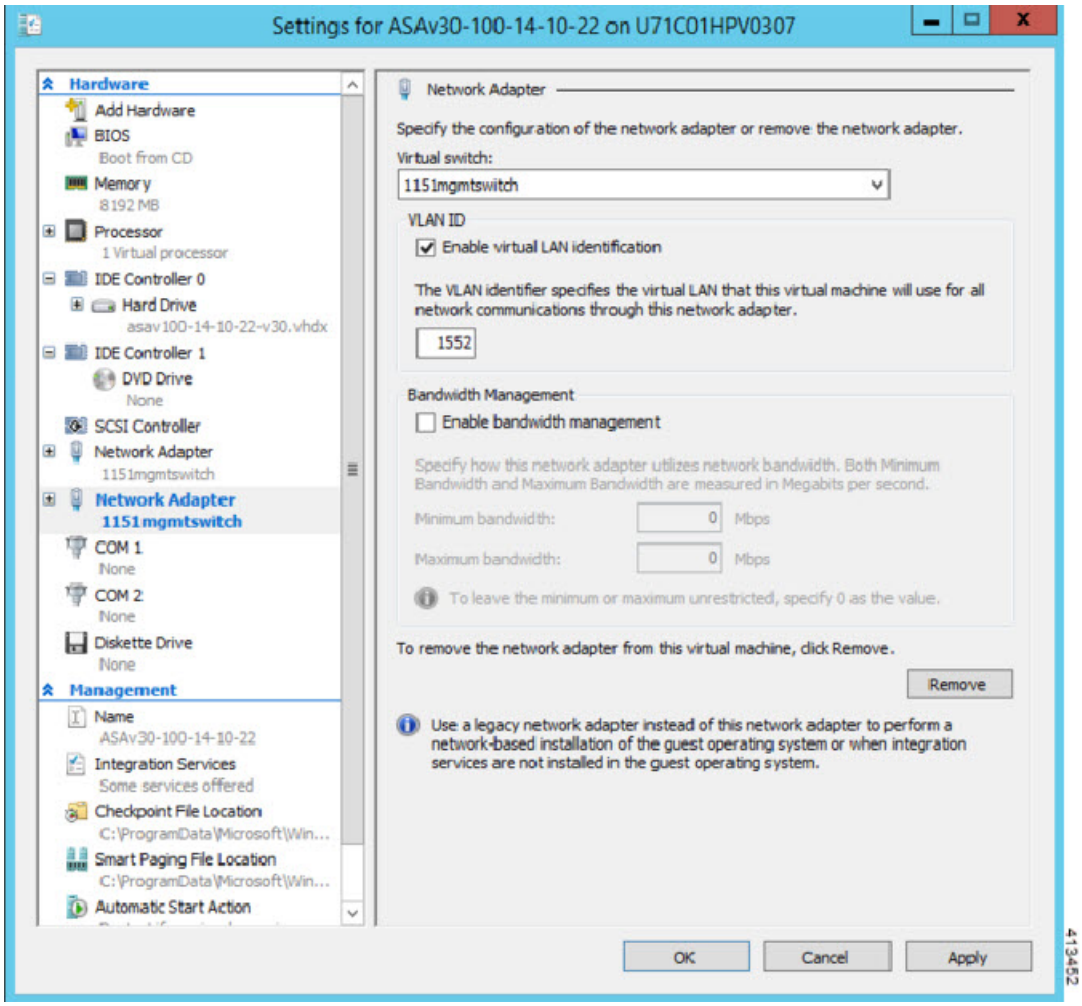
注释 请勿使用“旧版网路适配器”。

图 *12:* 添加网络适配器



步骤 2 在添加网络适配器后，可以修改虚拟交换机和其他功能。如果需要，还可以设置 VLAN ID。

图 *13:* 修改网络适配器设置



修改网络适配器名称

Hyper-V 中使用通用的网络接口名称“网络适配器”。如果网络接口都具有相同的名称，可能会造成混淆。您不能使用 Hyper-V 管理器修改名称。您必须使用 Windows Powershell 命令修改名称。

步骤 1 打开 Windows Powershell。

步骤 2 根据需要修改网络适配器。

示例：

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

MAC 地址欺骗

要使 ASA 虚拟以透明模式传送数据包，并实现高可用性主用/备用故障转移，必须为所有接口开启 MAC 地址欺骗。您可以在 Hyper-V 管理器中或使用 Powershell 命令执行此操作。

使用 Hyper-V 管理器配置 MAC 地址欺骗

您可以使用 Hyper-V 管理器在 Hyper-V 上配置 MAC 欺骗。

步骤 1 转至**服务器管理器 (Server Manager)** > **工具 (Tools)** > **Hyper-V 管理器 (Hyper-V Manager)**。

此时将出现 Hyper-V 管理器。

步骤 2 在 Hyper-V 管理器右侧点击**设置 (Settings)**，打开设置对话框。

步骤 3 在左侧的**硬件 (Hardware)** 菜单下：

1. 点击**内部 (Inside)** 并展开菜单。
2. 点击**高级功能 (Advanced Features)** 打开 MAC 地址选项。
3. 点击**启用 MAC 地址欺骗 (Enable MAC address spoofing)** 单选按钮。

步骤 4 对外部接口重复上述操作。

使用命令行配置 MAC 地址欺骗

您可以使用 Windows Powershell 命令行在 Hyper-V 上配置 MAC 欺骗。

步骤 1 打开 Windows Powershell。

步骤 2 配置 MAC 地址欺骗。

示例：

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

配置 SSH

您可以在 Hyper-V 管理器的 Virtual Machine Connection 中，通过管理接口为 ASA 虚拟配置 SSH 访问。如果要使用 Day 0 配置文件，您可以为其添加 SSH 访问。有关详细信息，请参阅准备 Day 0 配置文件。

步骤 1 验证是否存在 RSA 密钥对：

示例：

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

步骤 2 如果不存在 RSA 密钥对，请生成 RSA 密钥对：

示例：

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

username test password test123 privilege 15
aaa authentication ssh console LOCAL
ssh 10.7.24.0 255.255.255.0 management
ssh version 2
```

步骤 3 验证您是否可以从其他 PC 使用 SSH 访问 ASA 虚拟。

CPU 使用情况和报告

“CPU 利用率”(CPU Utilization) 报告汇总了指定时间内使用的 CPU 百分比。通常，核心在非高峰时段运行大约 30% 至 40% 的总 CPU 容量，在高峰时段运行大约 60% 至 70% 的容量。

ASA 虚拟中的 vCPU 使用率

ASA 虚拟 vCPU 使用率显示了用于数据路径、控制点和外部进程的 vCPU 用量。

Hyper-V 报告的 vCPU 使用率包括上述 ASA 虚拟使用率，及：

- ASA 虚拟空闲时间
- 用于 ASA 虚拟机的 %SYS 开销

CPU 使用率示例

show cpu usage 命令可用于显示 CPU 利用率统计信息。

示例

```
Ciscoasa#show cpu usage

CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

在以下示例中，报告的 vCPU 使用率截然不同：

- ASAv 虚拟报告：40%
- DP：35%
- 外部进程：5%
- ASA（作为 ASA 虚拟报告）：40%
- ASA 空闲轮询：10%
- 开销：45%

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。