测试和故障排除

本章介绍如何对 ASA 进行故障排除和测试基本连接。

恢复启用密码和 Telnet 密码

忘记启用密码或 Telnet 密码时，可在 ASA virtual 和 ISA 3000 模式下恢复这些密码。必须使用 CLI 执行该任务。

注释 您无法恢复在其他平台上丢失的密码。您只能恢复出厂默认配置，并将密码重置为默认值。如需了解 Firepower 4100/9300，请参阅《FXOS 配置指南》。对于其他模型，请参阅 FXOS 故障排除指南。

恢复 ISA 3000 上的密码

要恢复 ISA 3000 平台上的密码，请执行以下步骤：

过程

步骤 1 连接到 ASA 控制台端口。

步骤 2 关闭 ASA，然后重新启动。

步骤 3 启动后，当系统提示进入 ROMMON 模式时按下 **Escape** 键。

步骤 4 要更新配置寄存器值，请输入以下命令：

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

ASA 将显示当前的配置注册值以及配置选项列表。记录当前配置寄存器值，以便稍后恢复。

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ..... auto-boot index 1 image in disks
```

步骤 5 通过输入以下命令重新加载 ASA：

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

ASA 加载默认配置，而非启动配置。

步骤 6 通过输入以下命令访问特权 EXEC 模式：

```
ciscoasa# enable
```

步骤 7 系统提示输入密码时，请按 **Enter** 键。

密码为空。

步骤 8 通过输入以下命令加载启动配置：

```
ciscoasa# copy startup-config running-config
```

步骤 9 通过输入以下命令访问全局配置模式：

```
ciscoasa# configure terminal
```

步骤 10 通过输入以下命令，根据需要在默认配置中更改密码：

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

步骤 11 通过输入以下命令加载默认配置：

```
ciscoasa(config)# no config-register
```

默认配置寄存器值为 0x1。有关配置寄存器的详细信息，请参阅命令参考。

步骤 12 通过输入以下命令，将新密码保存至启动配置：

```
ciscoasa(config)# copy running-config startup-config
```

恢复 ASA Virtual上的密码或映像

要恢复 ASA virtual 上的密码或映像，请执行以下步骤：

过程

步骤 1 将运行的配置复制到 ASA virtual 上的备份文件：

copy running-config *filename*

示例：

```
ciscoasa# copy running-config backup.cfg
```

步骤 2 重新启动 ASA virtual：

reload

步骤 3 从 GNU GRUB 菜单，按向下箭头，选择 <**filename**> **with no configuration load** 选项，然后按 **Enter** 键。文件名为 ASA virtual 上的默认启动映像文件名。默认启动映像永远不会通过 **fallback** 命令自动启动。然后加载选定的启动映像。

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

示例：

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

步骤 4 将备份配置文件复制到运行的配置。

copy *filename* **running-config**

示例：

```
ciscoasa (config)# copy backup.cfg running-config
```

步骤 5 重置密码。

enable password 密码

示例：

```
ciscoasa(config)# enable password cisco123
```

步骤 6 保存新配置。

write memory

示例：

```
ciscoasa(config)# write memory
```

禁用 ISA 3000 硬件的密码恢复

注释 在 ASA virtual、 Cisco Secure Firewall 型号上无法禁用密码恢复。

要禁用密码恢复以确保非授权用户无法使用密码恢复机制来损害 ASA，请执行以下步骤。

开始之前

在 ASA 上，使用 **noservice password-recovery** 命令可防止您在配置完整无损的情况下进入 ROMMON 模式。当进入 ROMMON 模式时，ASA 会提示您擦除所有闪存文件系统。不先执行该擦除操作就无法进入 ROMMON 模式。如果您选择不擦除闪存文件系统，ASA 将重新加载。因为密码恢复取决于使用 ROMMON 模式并维护现有配置，所以该擦除可防止恢复密码。但是，禁用密码恢复可以防止未授权用户查看配置或插入不同的密码。在此情况下，要将系统恢复到操作状态，请加载新映像和备份配置文件（如可用）。

service password-recovery 命令显示在配置文件中，仅供参考。在 CLI 提示符处输入命令时，设置保存在 NVRAM 中。更改设置的唯一方法是在 CLI 提示符下输入命令。使用不同版本的命令加载新配置不会更改设置。如果在将 ASA 配置为启动时（准备密码恢复）忽略启动配置并禁用密码恢复，则 ASA 会更改设置以便照常加载启动配置。如果使用故障转移并将备用设备配置为忽略启动配置，则会对配置注册进行与 **no service password- recovery** 命令复制到备用设备时相同的更改。

过程

禁用密码恢复。

no service password-recovery

示例：

```
ciscoasa (config)# no service password-recovery
```

使用 Packet Capture Wizard 配置和运行捕获

您可以使用 Packet Capture Wizard 配置和运行捕获以对错误进行故障排除。捕获可以使用 ACL 来限制捕获的流量类型、源地址和目标地址与端口，以及一个或多个接口。该向导在每个入口接口和出口接口上运行一个捕获。您可以在 PC 上保存捕获以在数据包分析器中对它们进行检查。

注释 此工具不支持无客户端 SSL VPN 捕获。

要配置和运行捕获，请执行以下步骤：

过程

步骤 1 依次选择**向导** > **数据包捕获向导**。

系统将显示**数据包捕获概述**屏幕，其中列出向导将指导您完成的任务。这些任务包括：

- 选择入口接口。
- 选择出口接口。
- 设置缓冲区参数。
- 运行捕获。
- 将捕获保存到 PC（可选）。

步骤 2 点击“**下一步**”。

在集群环境中，系统将显示**集群选项**屏幕。转至步骤 3。

在非集群环境中，系统将显示 **Ingress Traffic Selector** 屏幕。转至步骤 4。

步骤 3 在 **Cluster Option** 屏幕中选择以下选项之一以运行捕获：**This device only** 或 **The whole cluster**，然后点击 **Next** 以显示 **Ingress Selector** 屏幕。

步骤 4 点击 **Select Interface** 单选按钮以捕获接口上的数据包。

在集群环境中，要仅捕获集群控制平面数据包，请选中CP-Cluster复选框。

步骤 5 点击 **Use backplane channel** 单选按钮以捕获 ASA CX 数据层面上的数据包。

步骤 6 在 **Packet Match Criteria** 区域执行以下其中一项操作：

- 点击 **选择访问列表** 单选按钮以指定用于匹配数据包的 ACL，然后从 **选择 ACL** 下拉列表中选择 ACL。点击 **Manage** 以显示 **ACL Manager** 窗格，以便将之前配置的 ACL 添加到当前下拉列表中。选择一个 ACL，然后点击 **OK**。

  启用交换机数据包捕获时，会禁用访问列表选项。有关详细信息，请参阅进口流量选择器，第 8 页。

- 点击 **Specify Packet Parameters** 单选按钮以指定数据包参数。

a) 在 **ICMP 捕获**下拉列表中执行以下操作之一：

注释 当您在上一个窗口中选择**整个集群**作为集群选项时，才会填充 **ICMP 捕获**字段。

- 选择**包括已解密**，在包含正常流量和已解密流量的已解密 IPsec 数据包进入防火墙设备后对其进行捕获。
- 选择**保持**，以捕获集群设备上的持久数据包。

步骤 7 要继续，请参阅进口流量选择器，第 8 页。

步骤 8 点击**下一步**，以显示**出口流量选择器**屏幕。

步骤 9 点击“**选择接口**”单选按钮，捕获接口上的数据包。

在集群环境中，要捕获集群控制平面数据包，请选中CP-Cluster复选框。

注释 要了解有关出口流量选择器字段的更多详细信息，请参阅 出口流量选择器，第 9 页。

要了解有关出口流量选择器字段的更多详细信息，请参阅 出口流量选择器，第 9 页。

步骤 10 点击**下一步**，以显示**缓冲区和捕获**屏幕。请参阅 缓冲区以继续。

步骤 11 在 **Capture Parameters** 区域选中 **Get capture every 10 seconds** 复选框以便每隔 10 秒钟自动获取最新捕获。默认情况下，此捕获使用循环缓冲区。

步骤 12 您可在 **Buffer Parameters** 区域指定缓冲区大小和数据包大小。缓冲区大小是捕获可用于存储数据包的最大内存量。数据包大小是捕获可以容纳的最长数据包。我们建议您使用最长的数据包大小以捕获尽可能多的信息。

a) （可选。仅适用于安全防火墙 3100 设备）选中 **交换机** 复选框以存储捕获的交换机数据包。
b) 输入数据包大小。有效的大小范围为 14 - 1522 个字节。对于交换机数据包捕获，有效大小范围为 64 到 9006 字节。
c) 输入缓冲区大小。有效的大小范围为 1534 - 33554432 个字节。对于交换机数据包捕获，有效大小范围为 256 到 2048 字节。
d) 选中 **Use circular buffer** 复选框以存储捕获的数据包。

注释 选择此设置时，如果所有缓冲存储空间都已占用，则捕获将开始覆盖最旧的数据包。

步骤 13 点击**下一步**以显示**摘要**屏幕，该屏幕将显示集群中所有设备的集群选项（如果使用的是集群）、流量选择器和已输入的缓冲区参数。请参阅 摘要以继续。

步骤 14 点击**下一步**以显示**运行捕获**屏幕，然后点击**开始**以开始捕获数据包。点击“**停止**”，结束捕获。要继续，请参阅运行捕获，第 10 页。如果您使用的是集群，请转至步骤 16。

步骤 15 点击“**获取捕获缓冲区**”，确定剩余的缓冲区空间。点击 **Clear Buffer on Device** 以删除当前内容并在缓冲区中腾出空间以捕获更多数据包。

步骤 16 在集群环境中，在 **Run Captures** 屏幕上执行以下一个或多个步骤：

- 点击 **Get Cluster Capture Summary** 以查看集群中所有设备的数据包捕获信息汇总，其后显示每台设备的数据包捕获信息。
- 点击 **Get Capture Buffer** 以确定每台集群设备中剩余的缓冲区空间。系统将显示 **Capture Buffer from Device** 对话框。
- 点击 **Clear Capture Buffer** 以删除集群中一台或全部设备上当前的内容，并在缓冲区中流出空间来捕获更多数据包。

步骤 17 点击**保存捕获**以显示**保存捕获**对话框。您可以选择保存入口捕获、出口捕获，或同时保存两者。请参阅 保存捕获以继续。

步骤 18 点击 **Save Ingress Capture** 以显示 **Save capture file** 对话框。指定 PC 上的存储位置，然后点击 **Save**。

步骤 19 点击**启动网络嗅探器应用**，以启动在**工具** > **首选项**中指定的数据包分析应用，以便分析入口捕获。

步骤 20 点击 **Save Egress Capture** 以显示 **Save capture file** 对话框。指定 PC 上的存储位置，然后点击 **Save**。

步骤 21 点击**启动网络嗅探器应用**，以启动在**工具** > **首选项**中指定的数据包分析应用，以便分析出口捕获。

步骤 22 点击 **Close**，然后点击 **Finish** 退出向导。

数据包捕获准则

情景模式

- 您可以配置某种情景内集群控制链路上的捕获；仅捕获与集群控制链路中发送的情景关联的数据包。
- 在多情景模式下，一个共享 VLAN 只能配置一个捕获，仅使用配置的最后一个捕获。
- 如果删除最后配置的（活动）捕获，则没有捕获会变成活动状态，即使您之前已在其他情景中配置捕获；您必须删除捕获并重新添加才能让它变成活动状态。
- 流入该捕获所关联的接口的所有流量都将被捕获，包括流向共享 VLAN 上的其他情景的流量。因此，如果您在情景 A 中为同时被情景 B 使用的 VLAN 启用捕获，则将同时捕获情景 A 和情景 B 的进口流量。
- 对于出口流量，将只捕获带活动捕获的情景的流量。唯一的例外是当您未启用ICMP检查时（因此 ICMP 流量在加速路径中没有会话）。在这种情况下，将捕获共享 VLAN 上所有情景的入口和出口 ICMP 流量。

其他准则

- 如果 ASA 收到的数据包带有格式不正确的 TCP 报头，并因 *invalid-tcp-hdr-length* ASP 丢弃原因而丢弃这些数据包，则接收这些数据包的接口上的**show capture** 命令输出不会显示这些数据包。
- 您只能捕获 IP 流量；不能捕获非 IP 数据包（如 ARP）。
- 对于内联 SGT 标记数据包，捕获的数据包包含您的 PCAP 查看器可能无法识别的其他 CMD 报头。
- 数据包捕获包括系统由于检测、NAT、TCP 规范化或其他调整数据包内容的功能而修改或注入到连接的数据包。
- 数据路径中注入的虚拟数据包的生命周期跟踪无法准确反映数据路径如何处理物理数据包。这种差异取决于注入的虚拟数据包的软件版本、配置和类型。以下配置设置可能导致差异：
  - 至少存在同一主机的 2 条 NAT 语句。
  - 连接的正向和反向流采用不同协议。例如，正向流采用 UDP 或 TCP，反向流采用 ICMP。
  - 正在启用 ICMP 错误检测。

进口流量选择器

要配置入口接口、源和目标主机或网络，以及数据包捕获协议，请执行以下步骤：

过程

步骤 1 从下拉列表中选择入口接口名称。

步骤 2 输入入口源主机和网络。点击 **Use backplane channel** 单选按钮以捕获 ASA CX 数据层面上的数据包。

步骤 3 输入入口目标主机和网络。

步骤 4 输入要捕获的协议类型。可用的协议包括：ah、eigrp、esp、gre、icmp、icmp6、igmp、igrp、ip、ipinip、nos、ospf、pcp、pim、snp、tcp 或 udp。

a) 仅为 ICMP 输入 ICMP 类型。可用的类型包括：all、alternate address、conversion-error、echo、echo-reply、information-reply、information-request、mask-reply、mask-request、mobile-redirect、parameter-problem、redirect、router-advertisement、router-solicitation、source-quench、time-exceeded、timestamp-reply、timestamp-request、traceroute 或 unreachable。

b) 仅为 TCP 和 UDP 协议指定源和目标端口服务。可用的选项包括：

- 选择 **All Services** 以包含所有服务。
- 选择 **Service Groups** 以包含服务组。

  要包含特定服务，请选择以下其中一项：aol、bgp、chargen、cifx、citrix-ica、ctiqbe、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、https、ident、imap4、irc、kerberos、klogin、kshell、ldap、ldaps、login、lotusnotes、

lpd、netbios-ssn、nntp、pcanywhere-data、pim-auto-rp、pop2、pop3、pptp、rsh、rtsp、sip、smtp、sqlnet、ssh、sunrpc、tacacs、talk、telnet、uucp 或 whois。

步骤 5 在 **Security Group Tagging** 区域选中 **SGT number** 复选框并输入安全组标签编号以为思科 TrustSec 服务启用数据包捕获。有效的安全组标签编号范围为 2-65519。

步骤 6 （可选。仅适用于 Cisco Secure Firewall 3100 设备和 Cisco Secure Firewall 4200 型号设备）要启用交换机数据包捕获，请在**交换机控制 (Switch Control)** 区域中，选中**交换机 (Switch)** 复选框。

注释 启用交换机数据包捕获时，访问列表选项将被禁用。

步骤 7 （可选。启用交换机数据包捕获时，此选项适用。）要为 Secure Firewall 4200 型号设备的数据包捕获配置进口流量方向参数，请在**方向控制 (Direction Control)** 区域的**方向 (Direction)** 下拉列表中选择一个方向。

出口流量选择器

要配置出口接口、源和目标主机/网络，以及数据包捕获的源和目标端口服务，请执行以下步骤：

过程

步骤 1 点击 **Select Interface** 单选按钮以捕获接口上的数据包。点击 **Use backplane channel** 单选按钮以捕获 ASA CX 数据层面上的数据包。

步骤 2 从下拉列表中选择出口接口名称。

步骤 3 输入出口源主机和网络。

步骤 4 输入出口目标主机和网络。

在入口配置时选择的协议类型已列出。

步骤 5 （可选。仅适用于安全防火墙 3100 设备 和 Cisco Secure Firewall 4200 型号设备）如果已启用交换机数据包捕获，请指定内部 VLAN 和外部 VLAN 范围（1 至 4096）。要启用交换机数据包捕获，请参阅 进口流量选择器，第 8 页。

步骤 6 （可选。启用交换机数据包捕获时，此选项适用。）要为 Cisco Secure Firewall 4200 型号设备的数据包捕获配置出口流量方向参数，请在**方向控制 (Direction Control)** 区域的**方向 (Direction)** 下拉列表中选择一个方向。

缓冲区

要配置数据包大小、缓冲区大小，以及在数据包捕获中使用循环缓冲区，请执行以下步骤：

过程

步骤 1 输入捕获可以容纳的最长数据包。使用可用的最长数据包以捕获尽可能多的信息。

步骤 2 输入捕获可用于存储数据包的最大内存量。

步骤 3 使用循环缓冲区来存储数据包。当循环缓冲区已使用所有缓冲存储空间时，捕获将先覆盖最旧的数据包。

摘要

Summary 屏幕显示了集群选项（如果使用的是集群）、流量选择器，以及在之前的向导屏幕中选择的数据包捕获的缓冲区参数。

运行捕获

要启动和停止捕获会话、查看捕获缓冲区、启动网络分析器应用、保存数据包捕获和清除缓冲区，请执行以下步骤：

过程

步骤 1 点击 **Start** 以启动选定接口上的数据包捕获会话。

步骤 2 点击 **Stop** 以停止选定接口上的数据包捕获会话。

步骤 3 点击 **Get Capture Buffer** 以获取接口上的捕获数据包快照。

步骤 4 点击 **Ingress** 以显示入口接口上的捕获缓冲区。

步骤 5 点击 **Egress** 以显示出口接口上的捕获缓冲区。

步骤 6 点击 **Clear Buffer on Device** 以清除设备上的缓冲区。

步骤 7 点击**启动网络嗅探器应用**以启动数据包分析应用，以便分析在**工具** > **首选项**中指定的入口捕获或出口捕获。

步骤 8 点击 **Save Captures** 以使用 ASCII 或 PCAP 格式保存入口和出口捕获。

保存捕获

要将入口和出口数据包捕获保存到 ASCII 或 PCAP 文件格式以进行进一步的数据包分析，请执行以下步骤：

过程

步骤 1 点击 **ASCII** 以使用 ASCII 格式保存捕获缓冲区。

步骤 2 点击 **PCAP** 以使用 PCAP 格式保存捕获缓冲区。

步骤 3 点击**保存入口捕获 (Save ingress capture)** 以指定要在其中保存入口数据包捕获的文件。

步骤 4 点击**保存出口捕获 (Save egress capture)** 以指定要在其中保存出口数据包捕获的文件。

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。

中的 vCPU 使用率ASA Virtual

在 ASA virtual 上使用 **show cpu usage** 命令显示 CPU 利用率统计信息。ASA virtual 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。

云服务提供商（例如 VMware、Azure、OCI 等）报告的 vCPU 使用情况包括所述的 ASA virtual 使用情况以及：

- ASA virtual 空闲时间
- 用于 ASA Virtual VM 的 %SYS 开销
- 在 vSwitch、vNIC 和 pNIC 之间移动数据包的开销。此开销可能会非常大。

CPU 使用率示例

在以下示例中，报告的 vCPU 使用率截然不同：

- ASA Virtual 报告：40%
- DP：35%
- 外部进程：5%
- vSphere 报告：95%
- ASA（如 ASA virtual 报告）：40%
- ASA 空闲轮询：10%
- 开销：45%

开销用于执行虚拟机监控程序功能，以及使用 vSwitch 在 NIC 与 vNIC 之间移动数据包。

由于 ESXi 服务器能够代表 ASA virtual 将其他计算资源用于开销，因此使用率可能会超过 100%。

VMware CPU 使用率报告

在 vSphere 中，点击“**虚拟机性能**”选项卡，然后点击“**高级**”以显示“**图表选项**”下拉列表，该列表将显示 VM 的每种状态的 vCPU 使用率（%USER、%IDLE、%SYS 等）。此信息有助于从 VMware 的角度了解使用 CPU 资源的位置。

在 ESXi 服务器外壳上（使用 SSH 访问外壳以连接主机），esxtop 是可用的。Esxtop 具有一个与 Linux **top** 命令类似的外观，为 vSphere 性能提供了 VM 状态信息，包括以下信息：

- vCPU、内存和网络使用率的详细信息
- 每个 VM 的每种状态的 vCPU 使用率
- 内存（运行时键入 M）和网络（运行时键入 N），以及统计信息和 RX 丢弃的数量

ASA Virtual 和 vCenter 图表

ASA virtual 与 vCenter 之间的 CPU 使用率 (%) 存在差异：

- vCenter 图表值始终大于 ASA virtual 值。
- vCenter 称之为 %CPU 使用率； ASA virtual 称之为 %CPU 利用率。

术语“%CPU 利用率”和“%CPU 使用率”表示不同的东西：

- CPU 利用率提供了物理 CPU 的统计信息。
- CPU 使用率提供了基于 CPU 超线程的逻辑 CPU 统计信息。但是，由于只使用一个 vCPU，因此超线程未打开。

vCenter 按如下方式计算 CPU 使用率 (%)：

当前使用的虚拟 CPU 的用量，以总可用 CPU 的百分比表示

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式为：以 MHz 为单位的使用率/虚拟 CPU 数量 x 核心频率

当比较以 MHz 为单位的使用率时，vCenter 和 ASA virtual 值是一致的。根据 vCenter 图，MHz % CPU 使用率的计算方式为：60/(2499 x 1 个 vCPU) = 2.4

Amazon CloudWatch CPU 使用情况报告

您可以查看指标资源管理器，以按标签和属性监控资源。执行以下步骤以查看特定实例的CPU利用率统计信息：

过程

步骤 1 打开 **CloudWatch** 控制台，然后在导航窗格中选择 **指标** 。

步骤 2 选择 **EC2** 指标命名空间，然后选择 **每实例指标** 维度。

步骤 3 在搜索字段中输入 **CPUUtilization** 并按 Enter 键。选择所需实例的行，以显示该实例的 **CPUUtilization** 指标图形。

有关更多信息，请参阅 Amazon CloudWatch 文档 。

ASA Virtual 和 Amazon CloudWatch Graphs

由于在 ASA virtual 和 CloudWatch 上计算 CPU 使用率的方式不同，因此 Amazon CloudWatch 图形数字高于数字。

ASA virtual 在轮询模式下运行时，每个 CPU 都会运行一个轻量级命令循环，而不是进入省电模式或任何其他空闲状态。通过保持每个核心始终处于活动状态，而不必打开/关闭或根据 Intel 电源状态调整其时钟，从而提高性能。

在 ASA virtual 内部，此活动被理解为空闲行为，并且 CPU 使用率已正确计算。但是，在 Amazon CloudWatch 上，空闲行为看起来像正常的 CPU 活动，因为所有 CPU 周期都有要运行的指令，这会导致 CloudWatch 显示高 CPU 使用率百分比 (85-90%)。

Azure CPU 使用率报告

执行以下步骤，使用 Azure Monitor 中的 VM Insights 查看所有受监控 VM 的 CPU 利用率：

过程

步骤 1 转到 Azure 门户，选择 **监控** ，然后在 **解决方案** 部分选择 **虚拟机** 。

步骤 2 选择 **性能** 选项卡以显示 **CPU Utilization %** 图表。此图表显示平均处理器使用率最高的前五台计算机。

执行以下步骤，直接从特定 Azure VM 查看 CPU 利用率百分比图表：

过程

步骤 1 转到 Azure 门户并选择 **虚拟机**。

步骤 2 从 VM 列表中，选择 VM。

步骤 3 在 **监控** 部分中，选择 **见解**。

步骤 4 选择 **Performance** 选项卡。

有关详细信息，请参阅 如何使用 VM Insights 绘制性能图表 。

ASA Virtual 和 Azure Graphs

ASA virtual 与 Azure 之间的 CPU 使用率 (%) 存在差异。Azure 图形数字始终高于 ASA virtual 数字，因为 Azure 将 CPU 使用率计算为活动使用的虚拟 CPU 的数量，指定为总可用 CPU 的百分比。

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式为：以 MHz 为单位的使用率/虚拟 CPU 数量 x 核心频率

Azure 还对访客操作系统请求的 CPU 数量进行速率限制。请考虑以下场景： ASA virtual 报告 CPU 使用率 40%，虚拟机监控程序报告 CPU 使用率 90%。现在，如果 ASA virtual 需要更高的处理能力，CPU 使用率可能会超过 80%，然后虚拟机监控程序可能会报告 CPU 使用率超过 95%。这会导致虚拟机监控程序对 ASA virtual CPU 进行节流，即使 ASA virtual 只是在轮询模式下运行一个轻量级命令循环，表现出空闲行为。

Hyper-V CPU 使用率报告

除了查看可用云服务器的 CPU、RAM 和磁盘空间配置信息外，您还可以查看磁盘、I/O 和网络信息。使用这些信息可帮助您确定哪种云服务器适合您的需求。您可以通过命令行 nova 客户端或**云控制面板 (Cloud Control Panel)** 界面来查看可用的服务器。

在命令行中运行以下命令：

```
nova flavor-list
```

系统将显示所有可用的服务器配置。该列表包含了以下信息：

- ID - 服务器配置 ID
- 名称 - 按 RAM 大小和性能类型标记的配置名称
- Memory_MB - 配置的 RAM 量
- 磁盘 - 磁盘大小（以 GB 为单位）（对于一般用途的云服务器，即为系统磁盘的大小）
- 临时 - 数据磁盘的大小
- 交换 - 交换空间的大小
- VCPUs - 与配置关联的虚拟 CPU 的数量
- RXTX_Factor - 分配给连接到服务器的 PublicNet 端口、ServiceNet 端口和隔离网络（云网络）的带宽量（以 Mbps 为单位）

- Is_Public - 未使用

ASA Virtual 和 Hyper-V 图形

ASA Virtual 与 Hyper-V 之间的 CPU 使用率 (%) 存在差异：

- Hyper-V 图表值始终大于 ASA Virtual 值。
- Hyper-V 称之为 %CPU 使用率；ASA Virtual 称之为 %CPU 利用率。

术语“%CPU 利用率”和“%CPU 使用率”表示不同的东西：

- CPU 利用率提供了物理 CPU 的统计信息。
- CPU 使用率提供了基于 CPU 超线程的逻辑 CPU 统计信息。但是，由于只使用一个 vCPU，因此超线程未打开。

Hyper-V 按如下方式计算 CPU 使用率 (%)：

当前使用的虚拟 CPU 的用量，以总可用 CPU 的百分比表示

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式为：以 MHz 为单位的使用率/虚拟 CPU 数量 x 核心频率

注释 建议查看 ASA Virtual 报告，以获取准确的 CPU 使用率百分比。

OCI CPU 使用率报告

您可以使用计算实例指标（ **oci_computeagent**）查看 OCI 中的 CPU 利用率百分比。CPU 利用率指标显示 CPU 的活动级别，以占总时间的百分比表示。执行以下步骤以查看单个计算实例的指标图表：

过程

步骤 1 打开导航菜单，然后点击 **计算**下的 **实例** 。

步骤 2 点击实例，然后点击 **资源**下的 **指标** 。

步骤 3 在度量命名空间列表中选择 **oci_computeagent** 。

有关详细信息，请参阅 计算实例指标 。

ASA Virtual 和 OCI 图形

OCI 图形数字始终高于 ASA virtual 数字，因为 OCI 将 CPU 使用率计算为活动使用的虚拟 CPU 的数量，指定为可用 CPU 总数的百分比。

此计算值是基于主机的 CPU 使用率，而不是基于来宾操作系统，是虚拟机中所有可用虚拟 CPU 的平均 CPU 利用率。

例如，如果某个带一个虚拟 CPU 的虚拟机在一个具有四个物理 CPU 的主机上运行且 CPU 使用率为 100%，则该虚拟机已完全用尽一个物理 CPU。虚拟 CPU 使用率计算方式为：以 MHz 为单位的使用率/虚拟 CPU 数量 x 核心频率

测试配置

本节介绍如何为单模式 ASA 或每个安全情景测试连接，如何 ping ASA 接口，以及如何让一个接口上的主机 ping 到另一个接口上的主机。

测试基本连接：Ping 通地址

ping 是一种简单命令，可用于确定特定地址是否处于活动状态以及是否会做出响应。以下主题详细介绍此命令以及您可以使用此命令完成什么类型的测试。

使用 Ping 可测试的信息

当您 ping 设备时，系统会向设备发送数据包并且设备会返回回复。此过程可以让网络设备相互发现、识别和测试。

您可以使用 ping 来执行以下测试：

- 回环测试两个接口 - 可以在同一个 ASA 上从一个接口向另一个接口发起 ping，以外部回环测试方式来验证每个接口的基本“up”状态和操作。
- Ping 连接 ASA - 可以在其他 ASA 上 ping 某个接口，以验证其是否已打开并正在响应。
- Ping 通过 ASA - 可以通过在 ASA 的另一端 ping 某个设备来 ping 通过中间 ASA。数据包在每个方向传输时将通过两个中间 ASA 的接口。此操作会对中间设备的接口、操作和响应时间执行基本测试。
- Ping 测试网络设备的可疑操作 - 可以从某个 ASA 接口 ping 连接您怀疑运行不正常的网络设备。如果接口配置正确但没有收到回送，则可能是设备存在问题。
- Ping 测试中间通信 - 可以从某个 ASA 接口 ping 连接已知运行正常的网络设备. 如果接收到回送，任意中间设备的正确操作和物理连接都得以确认。

在 ICMP 和 TCP ping 之间进行选择

ASA 包括传统 ping，它会发送 ICMP 回送请求数据包并会在返回中获取回送回复数据包。如果所有相关网络设备都允许 ICMP 流量，这就是标准工具并且会正常运行。通过 ICMP ping，您可以 ping IPv4 或 IPv6 地址或主机名。

但是，某些网络会禁止 ICMP。如果您的网络禁止 ICMP，则可以改用 TCP ping 测试网络连接。对于 TCP ping，ping 会发送 TCP SYN 数据包，如果在响应中收到 SYN-ACK，则系统将 ping 视为成功。通过 TCP ping，您可以 ping IPv4 地址或主机名，但是不可以 ping IPv6 地址。

请记住，ICMP 或 TCP ping 成功只说明您使用的地址处于活动状态并会响应该特定类型的流量。这意味着基本连接正常工作。在设备上运行的其他策略可能会阻止特定类型的流量成功通过设备。

启用 ICMP

默认情况下，您可以从安全性高的端口 ping 到安全性低的端口。只需启用 ICMP 检测即可允许回程流量通行。如果要想从低到高进行 ping，则需要应用 ACL 来允许流量。

当 ping ASA 接口时，应用于接口的所有 ICMP 规则都必须允许回送请求数据包和回送响应数据包。ICMP 规则是可选的：如果您不配置这些规则，则系统会允许流入接口的所有 ICMP 流量。

此程序介绍要启用 ASA 接口的 ICMP ping 或通过 ASA 执行 ping，您可能需要完成的所有 ICMP 配置。

过程

步骤 1 确保 ICMP 规则允许回送请求/回送响应。

ICMP 规则是可选的，应用于直接发送到接口的 ICMP 数据包。如果不应用 ICMP 规则，系统会允许所有 ICMP 访问。在这种情况下，不需要进行任何操作。

但是，如果实施 ICMP 规则，请确保在每个接口上包含允许用于回送消息和回送回复消息的任意地址的规则。在 **Configuration > Device Management > Management Access > ICMP** 窗格中配置 ICMP 规则。

步骤 2 确保访问规则允许 ICMP。

当通过 ASA ping 主机时，访问规则必须允许 ICMP 流量流出和返回。访问规则必须至少允许回送请求数据包/回送回复 ICMP 数据包。您可以将这些规则添加为全局规则。

如果您没有访问规则，则还需要允许所需的其他流量类型，因为向接口应用任何访问规则都会增加一个隐式拒绝，因此会丢弃所有其他流量。

在 **Configuration > Firewall > Access Rules** 窗格中配置访问规则。如果仅为测试目的添加规则，则可以在完成测试后删除所添加的规则。

步骤 3 启用 ICMP 检测。

与 ping 接口相反，通过 ASA 执行 ping 时，需要执行 ICMP 检测。检测允许返回流量（即，回送回复数据包）返回到发起 ping 的主机，同时确保每个数据包都有一个响应，以防止特定类型的攻击。

您只要在默认全局检测策略中启用 ICMP 检测即可。

a) 依次选择 **Configuration > Firewall > Service Policy Rules**。
b) 编辑 **inspection_default** 全局规则。
c) 在 **Rule Actions > Protocol Inspection** 选项卡上，选择 ICMP。
d) 点击 **OK**，然后点击 **Apply**。

Ping 主机

要 ping 任何设备，只需依次选择 **Tools > Ping**，然后输入要 ping 的目标的 IP 地址或主机名，然后点击 **Ping**。对于 TCP ping，应选择 **TCP**，并且还应包含目标端口。这通常可满足您需要执行的任何测试要求。

ping 成功的输出示例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

如果 ping 失败，对于每次失败尝试，系统都会输出 ?，并且成功率会显示为低于 100%（完全失败显示 0%）：

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

但是，您还可以添加参数以控制 ping 的一些方面。以下是基本选项：

- ICMP ping - 您可以选择用于源 IP 地址的接口；但是，出口接口由使用数据路由表的路由查找确定。您可以 ping IPv4 或 IPv6 地址或主机名。
- TCP ping - 您还必须为要 ping 的目标选择 TCP 端口。例如，选择 **www.example.com 80** 来 ping HTTP 端口。您可以 ping IPv4 地址或主机名，但是不可以 ping IPv6 地址。

  您还可以选择指定用于源 IP 地址的接口；但是，出口接口由使用数据路由表的路由查找确定。

  最后，您可以指定重复 ping 的频率（默认值为 5 次）或每次尝试的超时时间（默认值为 2 秒）。

系统地测试 ASA 连接

如果您要对 ASA 连接进行更系统的测试，可以采用以下一般程序。

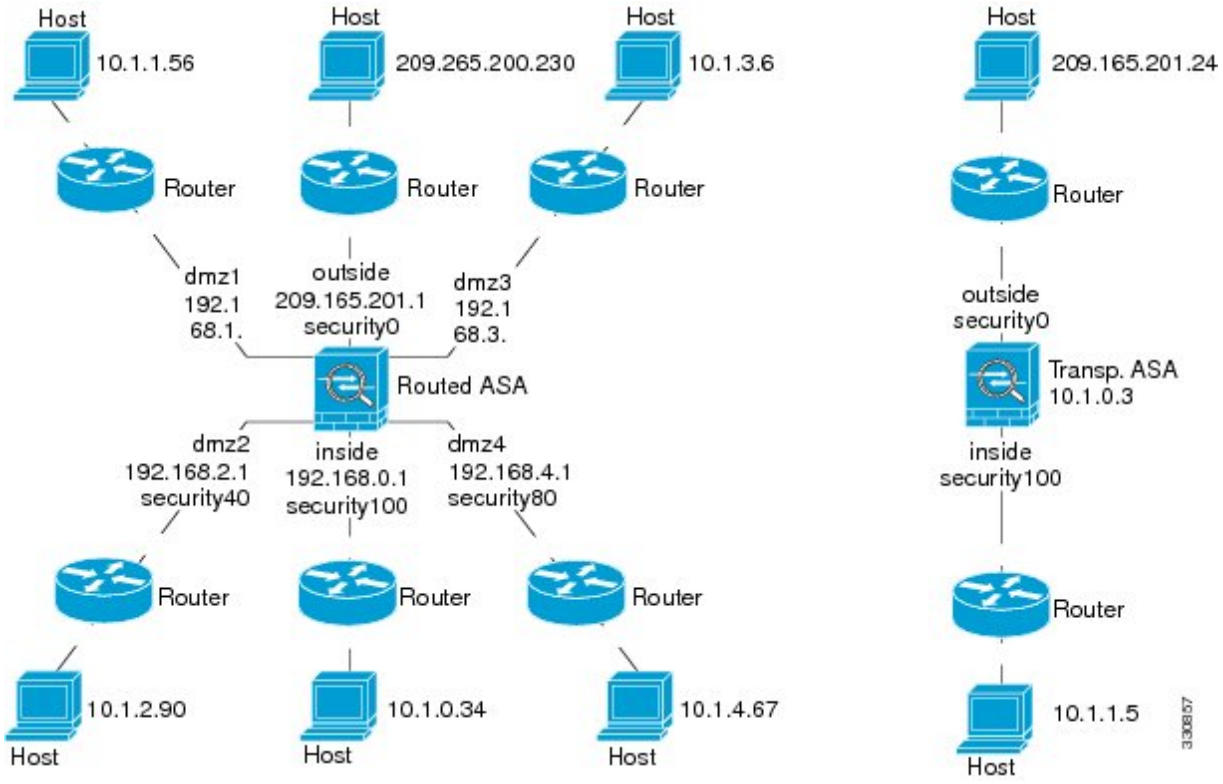
开始之前

如果要查看程序中提及的系统日志消息，请启用日志记录（使用 **logging enable** 命令，或在 ASDM 中依次选择 **Configuration > Device Management > Logging > Logging Setup**）。

过程

步骤 1 绘制显示接口名称、安全级别和 IP 地址的单模式 ASA 或安全情景的示意图。示意图也应包括所有直接连接的路由器和一台主机，该主机位于用于 ping ASA 的路由器的另一侧。

图 *1:* 接口、路由器和主机的网络图



步骤 2 从直接连接的路由器 ping 每个 ASA 接口。对于透明模式，ping BVI IP 地址。此测试可确保 ASA 接口处于活动状态，并且接口配置正确。

如果 ASA 接口处于非活动状态、接口配置不正确，或 ASA 与路由器之间的交换机关闭（参阅下图），ping 操作可能会失败。在这种情况下，数据包不能到达 ASA，因此调试消息或系统日志消息不会显示。

图 *2: ASA* 接口的 *ping* 故障

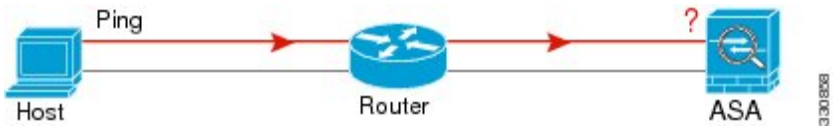
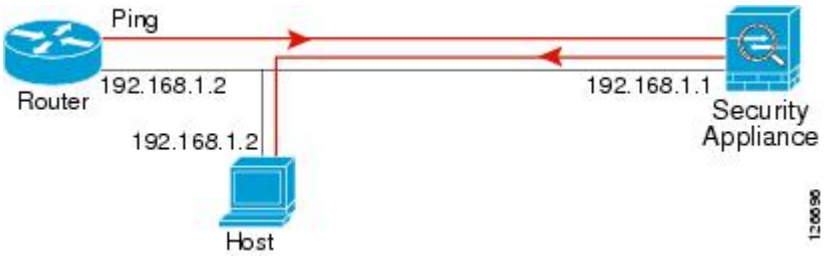


图 *3: IP* 寻址问题引发的 *Ping* 故障



如果 ping 回复没有返回到路由器，则可能存在交换机环路或冗余 IP 地址（参阅下图）。

步骤 3 从远程主机上 ping 每个 ASA 接口。对于透明模式，ping BVI IP 地址。此测试检查直接连接的路由器是否能在主机和 ASA 之间路由数据包，以及 ASA 是否可以正确地将数据包路由回主机。

如果 ASA 没有通过中间路由器返回路由到主机，ping 操作可能失败（参阅下图）。在这种情况下，调试消息显示 ping 成功，但系统会显示系统日志消息 110001，指示出现路由故障。

图 *4: ASA* 没有返回路由引发的 *ping* 故障

步骤 4 从 ASA 接口 ping 到已知正常运行的网络设备。

- 如果没有收到 ping，传输硬件或接口配置中可能存在问题。
- 如果 ASA 接口已正确配置但没有收到来自“已知良好的”设备的回送回复，接口硬件的接收功能可能存在问题。如果另一个具有“已知良好的”接收功能的接口可以在 ping 过该“已知良好的”设备后收到回送，则可以确认第一个接口硬件的接收功能存在问题。

步骤 5 从一个源接口的主机或路由器 ping 另一个接口上的主机或路由器。无论要检查多少接口对，都可以重复此步骤。如果使用 NAT，测试显示 NAT 运行正常。

如果 ping 成功，系统将显示系统日志消息确认路由模式的地址转换（305009 或 305011），并确认已创建一个 ICMP 连接（302020）。您还可以输入 **show xlate** 或 **show conns** 命令查看此信息。

如果 NAT 配置错误，ping 操作可能会失败。在这种情况下，系统会显示系统日志消息，指示 NAT 失败（305005 或 305006）。如果在没有静态转换的情况下从外部主机 ping 内部主机，您将会收到消息 106010。

图 *5: ASA* 未进行地址转换引发的 *ping* 故障

跟踪主机路由

如果您向某个 IP 地址发送流量时遇到问题，可以跟踪主机路由以确定网络路径是否有问题。

过程

步骤 1 使 ASA 在跟踪路由中可见，第 21 页。

步骤 2 确定数据包路由，第 21 页。

使 ASA 在跟踪路由中可见

默认情况下，ASA 不会作为跃点显示在跟踪路由中。要使其显示，您需要递减通过 ASA 的数据包上的生存时间，并增加对 ICMP 不可达消息的速率限制。

过程

步骤 1 使用服务策略减小 TTL。

a) 依次选择 **Configuration > Firewall > Service Policy Rules**。

b) 添加或编辑规则。例如，如果您已具有可以添加减小 TTL 的选项的规则，则不需要创建新规则。

c) 通过向导前进至 Rule Actions 页面，将规则应用于全局或某个接口，并指定流量匹配。例如，您可以创建全局匹配 any 规则。

d) 在 Rule Actions 页面上，点击 **Connection Settings** 选项卡，然后选择 **Decrement time to live for a connection**。

e) 点击 **OK** 或 **Finish**，然后点击 **Apply**。

步骤 2 增加 ICMP 不可达消息的速率限制。

a) 依次选择 **Configuration > Device Management > Management Access > ICMP**。

b) 在页面底部增加 **IPv4 ICMP Unreachable Message Limits > Rate Limit** 值。例如，将此值增至 50。

c) 点击**应用**。

确定数据包路由

使用 Traceroute 帮助您确定数据包到达目标地址所要经过的路由。跟踪路由通过向无效端口上的目标发送 UDP 数据包或 ICMPv6 回应来工作。由于端口无效，连接到该目标的路由器会以 ICMP 或 ICMPv6 超时消息做出响应，并向 ASA 报告该错误。

跟踪路由显示发送的每个探测的结果。每行输出以递增顺序对应一个 TTL 值。下表对输出符号进行了说明。

输出符号	说明
*	在超时期限内未收到对探测的响应。
U	没有通往目标的路由。
nn msec	各节点指定探测数的往返时间（以毫秒为单位）。
!N.	无法访问 ICMP 网络。对于 ICMPv6，地址超出范围。
!H	无法访问 ICMP 主机。
!P	无法访问 ICMP。对于 ICMPv6，端口不可访问。
!A	管理性禁止 ICMP。
?	未知 ICMP 错误。

过程

步骤 1 依次选择 **Tools** > **Traceroute**。

步骤 2 输入您跟踪路由的目标主机名或 IP 地址。将 DNS 服务器配置为使用主机名。

步骤 3 （可选）配置跟踪的特征。在大多数情况下默认值都适用。

- **Timeout** - 超时之前等待响应的时间。默认值为 3 秒。
- **Port** - 要使用的 UDP 端口。默认值为 33434。
- **Probe** - 在每个 TTL 级别发送多少探测。默认值为 3。
- **TTL** - 探测的最小和最大生存时间值。默认最小值为 1，但也可以设置更高值来阻止显示已知跃点。最大默认值为 30。当数据包到达目标地址或达到最大值时，跟踪路由终止。
- **Specify source interface or IP address** - 要用作跟踪源的接口。您可以按名称或 IP 地址指定接口。对于 Ipv6，无法指定源接口；只能指定源 IP 地址。IPv6 地址仅当已在 ASA 上启用 IPv6 时有效。在透明模式下，您必须使用管理地址。
- **Reverse Resolve** - 指定如果配置了 DNS 名称解析，是否要求输出显示所遇到的跃点的名称。取消选择此选项将仅显示 IP 地址。
- **Use ICMP** - 是否发送 ICMP 探测数据包，而不发送 UDP 探测数据包。

步骤 4 点击 **Trace Route** 开始跟踪路由。

Traceroute Output 区域显示有关跟踪路由结果的详细消息。

使用数据包跟踪器测试策略配置

您可以通过根据源和目标寻址以及协议特征为数据包建模，测试您的策略配置。跟踪会执行策略查找以测试访问规则、NAT、路由等，以便查看系统会允许还是拒绝数据包。

通过这样测试数据包，您可以看到策略结果并测试系统是否会按照需要处理要允许或拒绝的流量类型。除了验证配置之外，您还可以使用跟踪器调试意外行为，例如数据包本应被允许，但却被拒绝的情况。

过程

步骤 1 依次选择**工具** > **数据包跟踪器**。

步骤 2 选择数据包跟踪的源**接口**。

步骤 3 指定用于数据包跟踪的**数据包类型**。可用的协议类型包括：ICMP、IP、TCP、UDP, SCTP。

步骤 4 （可选。）如果要跟踪将安全组标签值嵌入第 2 层 CMD 报头 (Trustse) 的数据包，请选中 **SGT number**，然后输入安全组标签编号 0-65533。

步骤 5 （透明模式）如果您希望数据包跟踪器进入父接口（稍后将被重定向至子接口），请选中 **VLAN ID** 并输入 ID (1 - 4096)。仅当输入接口不是子接口时，VLAN ID 才可用。

步骤 6 （透明模式）指定**目标 MAC 地址**。

步骤 7 为数据包指定源和目标。

如果使用思科 Trustsec，可以指定 IPv4 或 IPv6 地址、完全限定域名 (FQDN) 或安全组名称或标记。对于源地址，您还可以指定 Domain\username 格式的用户名。

步骤 8 指定协议特征：

- ICMP - 输入 ICMP 类型、ICMP 代码 (0-255)，并且可以选择键入 ICMP 标识符。
- TCP/UDP/SCTP - 输入源和目标端口号。
- Raw IP - 输入协议编号，0-255。

步骤 9 使用数据包跟踪器跨集群设备调试数据包。从**集群捕获**下拉列表中选择：

a) **已解密** - 将已解密的数据包注入 VPN 隧道，还可以模拟通过 VPN 隧道的数据包。
b) **保持** - 注入您想要跨集群设备跟踪的数据包。
c) **绕行检查** - 跳过 ACL、VPN 筛选器、IPsec 欺骗和 uRPF 等安全检查。
d) **传输** - 允许模拟数据包传出 ASA。

步骤 10 点击 **Start** 开始跟踪数据包。

Information Display Area 显示有关数据包跟踪结果的详细信息。

监控性能和系统资源

您可以监控各种系统资源以确定性能或其他潜在问题。

监控性能

可以图形或图表格式查看 ASA 性能信息。

过程

步骤 1 依次选择 **Monitoring** > **Properties** > **Connection Graphs** > **Perfmon**。

步骤 2 您可以在 **Graph Window Title** 中为图形窗口输入标题，也可以选择现有标题。

步骤 3 从“可用图表”(Available Graphs) 列表中选择最多四个条目，然后点击**添加 (Add)** 将其移至“选定的图表”(Selected Graphs) 列表。可用的选项如下：

- AAA Perfmon - 身份验证、授权和记帐请求的每秒请求数。
- Inspection Perfmon - HTTP、FTP 和 TCP 检测的每秒数据包数。
- Web Perfmon - URL 访问和 URL 服务器请求的每秒请求数。
- Connections Perfmon - 所有连接、UDP 连接、TCP 连接和 TCP 拦截的每秒连接数。
- Xlate Perfmon - 每秒 NAT 转换数。

步骤 4 点击 **Show Graphs**。

您可以在图形视图与表视图之间切换每个图表。您也可以更改数据刷新的频率以及导出或打印数据。

监控内存块

您可以用图形或表格的形式查看可用和已用内存块信息。

过程

步骤 1 依次选择 **Monitoring** > **Properties** > **System Resources Graphs** > **Blocks**。

步骤 2 您可以在 **Graph Window Title** 中为图形窗口输入标题，也可以选择现有标题。

步骤 3 从 Available Graphs 列表中选择相应条目，然后点击 **Add** 将其移至 Selected Graphs 列表。可用的选项如下：

- Blocks Used - 显示 ASA 的已用内存块。

- Blocks Free - 显示 ASA 的可用内存块。

步骤 4 点击 **Show Graphs**。

您可以在图形视图与表视图之间切换每个图表。您也可以更改数据刷新的频率以及导出或打印数据。

监控 CPU

您可以查看 CPU 利用率。

过程

步骤 1 依次选择 **Monitoring** > **Properties** > **System Resources Graphs** > **CPU**。

步骤 2 您可以在 **Graph Window Title** 中为图形窗口输入标题，也可以选择现有标题。

步骤 3 将 CPU Utilization 添加到 Selected Graphs 列表。

步骤 4 点击 **Show Graphs**。

您可以在图形视图与表视图之间切换图表。您也可以更改数据刷新的频率以及导出或打印数据。

监控内存

您可以用图形或表格的形式查看内存利用率信息。

过程

步骤 1 依次选择 **Monitoring** > **Properties** > **System Resources Graphs** > **Memory**。

步骤 2 您可以在 **Graph Window Title** 中为图形窗口输入标题，也可以选择现有标题。

步骤 3 从 Available Graphs 列表中选择相应条目，然后点击 **Add** 将其移至 Selected Graphs 列表。可用的选项如下：

- Free Memory - 显示 ASA 的可用内存。
- Used Memory - 显示 ASA 的已用内存。

步骤 4 点击 **Show Graphs**。

您可以在图形视图与表视图之间切换每个图表。您也可以更改数据刷新的频率以及导出或打印数据。

监控每个进程的 CPU 使用率

您可以监控 CPU 上运行的进程。您可以获得某个进程的 CPU 使用百分比信息。CPU 使用率统计信息以降序排序显示，占比最高的进程排在顶部。其中也包括有关每个进程的CPU负载信息，显示日志时间之前 5 秒、1 分钟和 5 分钟的数据。此信息每 5 秒自动更新一次，提供实时的统计信息。在 ASDM 中，统计信息每 30 秒更新一次。

要查看每个进程的 CPU 使用率，请依次选择**监控 > 属性 > 每个进程的 CPU 使用情况**。

您可以停止自动刷新、手动刷新信息，或将其保存到某个文件中。您还可以点击 **Configure CPU Usage Colors**，根据使用率百分比选择背景和前景颜色，以更方便地扫描高使用率进程。

监控连接

要以表格的形式查看当前连接，请在 ASDM 主窗口中依次选择 **Monitoring > Properties > Connections**。每个连接的信息包括协议、源和目标地址特征、最后一次发送或接收数据包后的空闲时间，以及连接中的流量数量。

测试和故障排除历史记录

功能名称	平台版本	说明
跟踪路由支持 IPv6	9.7(1)	**traceroute** 命令已修改为接受 IPv6 地址。 修改了以下菜单项：**工具 > Traceroute**
对于网桥组成员接口，支持使用 Packet Tracer	9.7(1)	现在，对于网桥组成员接口可以使用 Packet Trac 在 packet-tracer 菜单项“**工具 > 数据包跟踪器**”**VLAN ID** 和**目标 MAC 地址**字段
手动开始和停止数据包捕获	9.7(1)	您现在可以手动停止和开始捕获。 添加/修改的菜单项：**向导 > 数据包捕获向导 >** 这 添加/修改的选项：**开始**按钮、**停止**按钮

功能名称	平台版本	说明
增强了数据包跟踪器和数据包捕获功能	9.9(1)	数据包跟踪器通过以下功能得到增强： • 在集群设备之间传递数据包时跟踪该数 • 允许模拟数据包传出 ASA。 • 绕过对模拟数据包的安全检查。 • 将模拟数据包视为 IPSec/SSL 解密数据包 数据包捕获通过以下功能得到增强： • 在解密后捕获数据包。 • 捕获跟踪并将其保留在永久列表中。 新增或修改的菜单项： **工具 > 数据包跟踪器** 添加了**集群捕获**字段以支持以下选项：**解密、检查、传输** 在**所有会话**下拉列表下面的**筛选依据**视图中添选项：**来源**和**来源 ID** **监控 > VPN > VPN 统计信息 > 数据包跟踪器** 在“数据包捕获向导”菜单项中添加了**ICMI向导 > 数据包捕获向导** 添加了两个选项**包括已解密**和**保持**，以支持 I
无需使用 ACL 便可匹配 IPv6 流量的数据包捕获支持	9.10(1)	如果您在 **capture** 命令中使用 **match** 关键字，字仅匹配 IPv4 流量。现在，您可以指定 **any4** 键字，以捕获 IPv4 或 IPv6 流量。**any** 关键字 IPv4 流量。 新增/修改的命令：**capture match** 无 ASDM 支持。
适用于 Forepower 9300/4100 的新**debug telemetry**命令。	9.14(1)	如果您使用的是 **debug telemetry** 命令，则会相关的调试消息。生成遥测报告时，调试有助的原因。 未修改任何菜单项。

功能名称	平台版本	说明
ping 命令更改	9.18(2)	为了支持对环回接口执行 ping 操作，**ping** 命令 改行为。如果您在命令中指定接口，则源 IP 地址 接口 IP 地址匹配，但实际出口接口将由使用数据 路由查找来确定。 新增/修改的命令：**ping**
交换机的数据包捕获	9.20(1)	您现在可以配置以捕获交换机的出口和进口流量 此选项仅适用于 Cisco Secure Firewall 4200 型号 新增/修改的菜单项：**向导 (Wizards)** > **数据包捕 (Packet Capture Wizard)** > **进口流量选择器 (Ingr Selector)**和**向导 (Wizards)** > **数据包捕获向导 (Pa Capture Wizard)** > **出口流量选择器 (Egress Traffi**

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。