多情景模式

本章介绍如何在 ASA 上配置多个安全情景。

关于安全情景

您可以将一台ASA设备分区成多个虚拟设备，这些虚拟设备被称为安全情景。每个情景都可以作为独立设备，拥有自己的安全策略、接口和管理员。多情景类似于拥有多台独立设备。有关在多情景模式下不支持的功能，请参阅多情景模式指南， 第 12 页。

本节提供安全情景的概述。

安全情景的公共用途

您可能希望在以下情况下使用多安全情景：

- 您作为运营商，希望向众多客户销售安全服务。通过在ASA上启用多个安全情景，可以实施具有成本效益且节约空间的解决方案，这样不仅可以确保所有客户流量的独立性和安全性，还可以简化配置。
- 您所在的组织是一家大型企业或大学校园，并且希望保持各部门完全分隔。
- 您所在的组织是一家企业，需要为不同部门提供不同的安全策略。

- 您有需要多个 ASA 的网络。

情景配置文件

本部分介绍 ASA 如何实施多情景模式配置。

情景配置

对于每个情景，ASA 都包括一项配置，用于确定安全策略、接口以及可以在独立设备中配置的所有选项。您可以在闪存中存储情景配置，也可以从 TFTP、FTP 或 HTTP(S) 服务器下载情景配置。

系统配置

系统管理员通过在系统配置（与单模式配置类似的启动配置）中配置每个情景配置位置、分配的接口以及其他情景运行参数，从而添加并管理情景。系统配置可标识ASA的基本设置。系统配置本身并不包含任何网络接口或网络设置；相反，当系统需要访问网络资源（例如，从服务器下载情景）时，它使用指定为管理情景的某个情景。系统配置中包含一个仅用于故障切换流量的专用故障切换接口。

管理情景配置

管理情景与任何其他情景一样，不同之处在于，当用户登录到管理情景时，该用户将具有系统管理员权限并可访问系统和所有其他情景。管理情景在任何情况下都不受限制，可用作常规情景。但是，由于登录到管理情景会授予用户针对所有情景的管理员权限，因此可能需要将对管理情景的访问限定于适当的用户。管理情景必须位于闪存中，而不是远程位置。

如果您的系统已处于多情景模式下，或者您从单模式进行转换，则管理情景会自动在内部闪存中创建名为 admin.cfg 的文件。此情景名为“admin”。如果您不希望将 admin.cfg 用作管理情景，则可以更改管理情景。

ASA 如何对数据包分类

必须对进入 ASA 的每个数据包进行分类，以便 ASA 能够确定将数据包发送到哪个情景。

注释 如果目标 MAC 地址为组播或广播 MAC 地址，则数据包会复制并传递到每个情景。

有效分类器条件

本节介绍分类器使用的条件。

注释 对于以接口为目标的管理流量，使用接口 IP 地址进行分类。

不使用路由表对数据包进行分类。

唯一接口

如果仅有一个情景与传入接口相关联，则ASA会将数据包分类至该情景。在透明防火墙模式下，要求情景具有唯一接口，因此总是使用此方法对数据包进行分类。

唯一 MAC 地址

如果多情景共享一个接口，则分类器在每个情景中使用分配给该接口的唯一 MAC 地址。上游路由器无法直接路由至不具有唯一MAC地址的情景。您可以启用MAC地址的自动生成。在配置每个接口时，您也可以手动设置 MAC 地址。

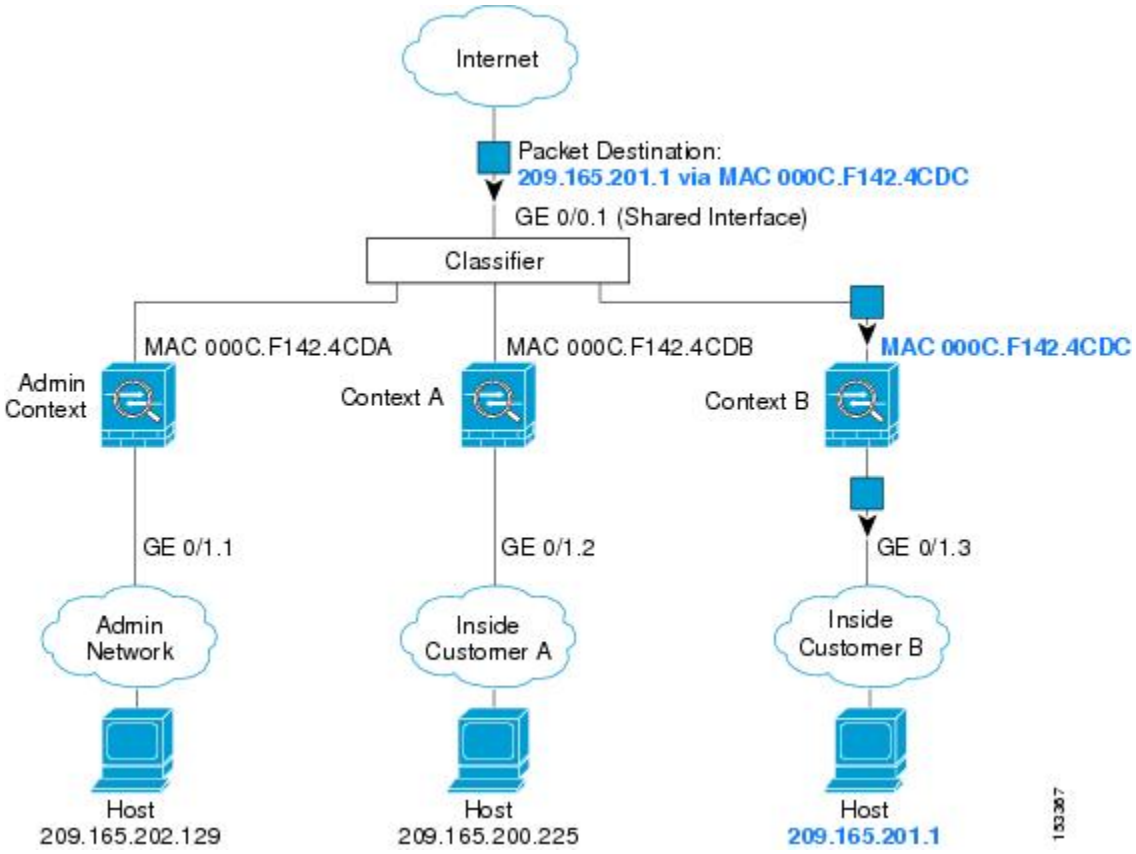
NAT 配置

如果不使用唯一 MAC 地址，ASA 将在您的 NAT 配置中使用映射地址对数据包进行分类。我们建议使用 MAC 地址而不是 NAT，这样，无论 NAT 配置的完整性如何，都可以进行流量分类。

分类示例

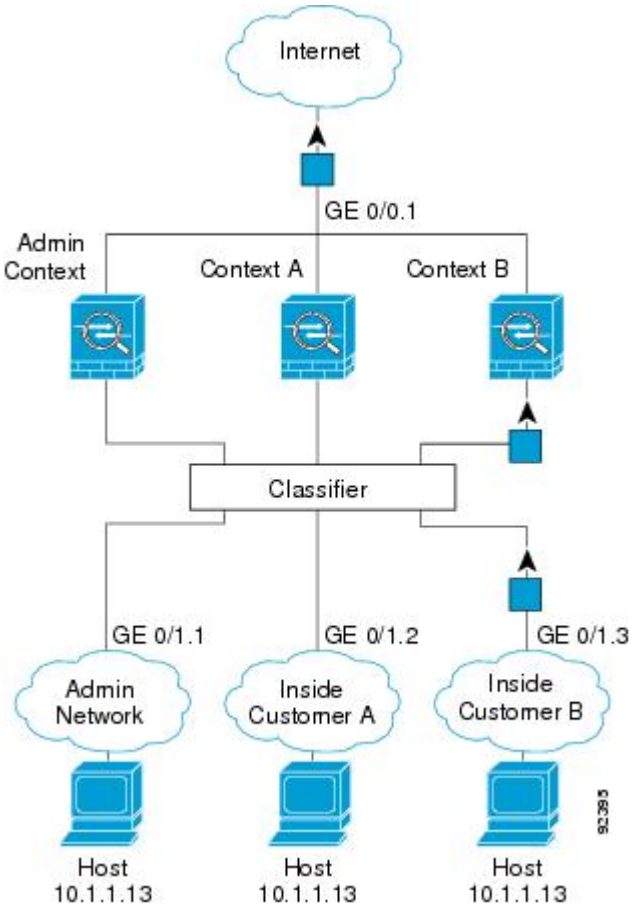
下图显示共享外部接口的多个情景。因为情景 B 包含路由器将数据包发送到的 MAC 地址，因此分类器会将该数据包分配至情景 B。

图 *1:* 使用 ***MAC*** 地址通过共享接口进行数据包分类



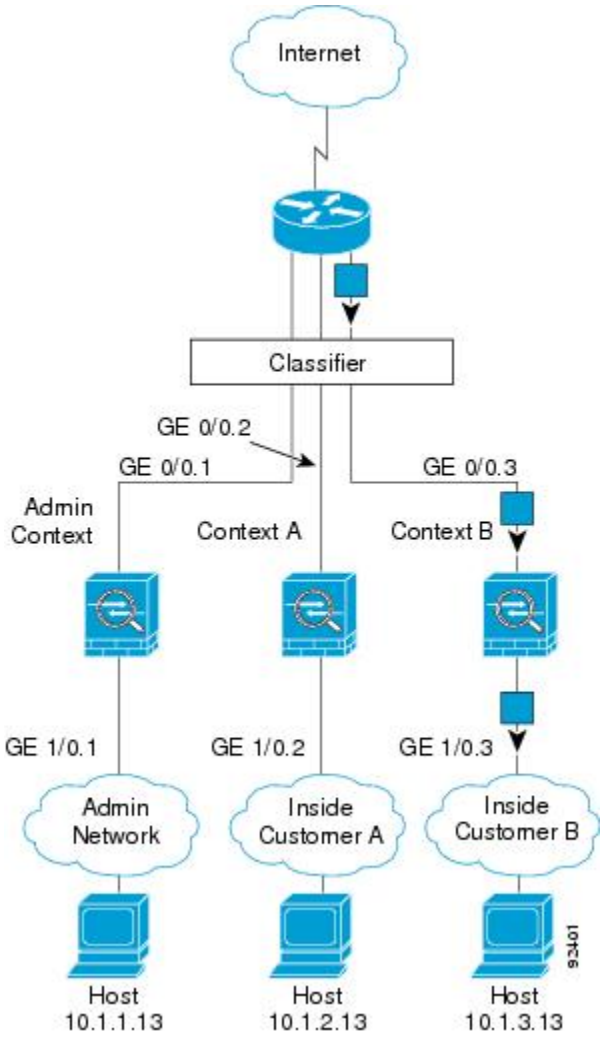
请注意，必须对所有新的传入流量加以分类，即使其来自内部网络。下图展示了情景 B 内部网络上的主机访问互联网。由于传入接口是分配至情景 B 的千兆以太网 0/1.3，因此分类器会将数据包分配至情景 B。

图 *2:* 来自内部网络的传入流量



对于透明防火墙，您必须使用唯一接口。下图展示了来自互联网并以情景 B 内部网络上的主机为目标的数据包。由于传入接口是分配至情景 B 的千兆以太网 1/0.3，因此分类器会将数据包分配至情景 B。

图 *3:* 透明防火墙情景



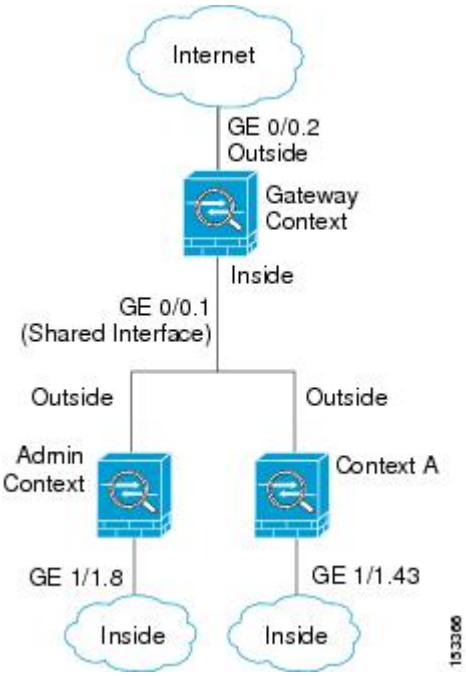
级联安全情景

将一个情景直接置于另一情景之前称为级联情景；一个情景的外部接口与另一个情景的内部接口是同一接口。如果您希望通过在顶级情景中配置共享参数，从而简化某些情景的配置，则可能要使用级联情景。

注释 级联情景要求每个情景接口具有唯一 MAC 地址。由于在不具有 MAC 地址的共享接口上对数据包进行分类存在限制，我们不建议在不具有唯一 MAC 地址的情况下使用级联情景。

下图显示了在网关后有两个情景的网关情景。

图 *4:* 级联情景



对安全情景的管理访问

ASA 提供了多情景模式下的系统管理员访问以及面向单个情景管理员的访问。

系统管理员访问

您可以通过两种方式以系统管理员身份访问 ASA：

- 访问 ASA 控制台。

  您可以从控制台访问系统执行空间，这意味着您输入的所有命令仅会影响系统配置或系统的运行（对于运行时命令而言）。

- 使用 Telnet、SSH 或 ASDM 访问管理情景。

作为系统管理员，您可以访问所有情景。

系统执行空间不支持任何 AAA 命令，但是，您可以在本地数据库中配置其自己的启用密码及用户名，以便提供单独的登录。

情景管理员访问

您可以使用 Telnet、SSH 或 ASDM 来访问情景。如果您登录到一个非管理情景，则只能访问该情景的配置。您可以提供该情景的单独登录。

管理接口使用情况

管理接口是一个仅用于管理流量的独立接口。

在路由防火墙模式下，您可以在所有情景中共享管理接口。

在透明防火墙模式下，管理接口是特殊的。除了允许的最大通过流量接口之外，您还可以将管理接口用作单独的仅管理接口。然而，在多情景模式下，您无法跨情景共享任何接口。您可以改为使用管理接口的子接口，并为每个情景分配一个子接口。但是，只有 Firepower 设备型号 允许管理接口上的子接口。ASA 5585-X ，必须使用数据接口或数据接口的子接口，并将其添加到情景中的桥接组。

对于 Firepower 4100/9300 机箱 透明情景，管理接口和子接口都不会保留其特殊状态。在这种情况下，必须将其视为数据接口，并将其添加到桥接组。（请注意，在单情景模式下，管理接口会保留其特殊状态。）

有关透明模式的另一个注意事项：当您启用多情景模式时，所有配置的接口都会自动分配到管理情景。例如，如果您的默认配置包括管理接口，则该接口将分配给管理情景。一个选项是让主接口分配给管理情景，并使用本地 VLAN 对其进行管理，然后使用子接口管理每个情景。请记住，如果将管理情景设为透明，其 IP 地址将被删除；您必须将其分配给网桥组，并将 IP 地址分配给 BVI。

关于资源管理

默认情况下，除非为每个情景强制设置了最大限制，否则所有安全情景对ASA资源的访问都是不受限制的；但VPN资源是唯一一种例外情况，这些资源默认是禁用的。例如，如果您发现一个或者多个情景使用了过多资源，并且导致其他情景出现拒绝连接的情况，则您可以配置资源管理来限制每个情景对资源的使用。对于 VPN 资源，您必须将资源管理配置为允许任何 VPN 隧道。

资源类

ASA 通过向资源类分配情景来管理资源。每个情景使用由类设置的资源限制。要使用某个类的设置，请在定义情景时向该类分配情景。所有未分配给其他类的情景都属于默认类；您不必主动向默认类分配情景。只能将情景分配给一个资源类。此规则的例外是，在成员类中未定义的限制继承自默认类；因此，一个情景实际可能是默认类和另一个类的成员。

资源限制

您可以将单一资源的限制设置为百分比（如果存在硬性系统限制）或绝对值。

对于大多数资源，ASA 不会为分配至该类的每个情景预留部分资源，而是会由 ASA 为情景设置最大限制。如果您超订用资源或允许某些资源不受限制，则少数情景可能会“用尽”这些资源，从而潜在影响为其他情景提供服务。VPN 资源类型除外，您不能超订用此类资源，因此，分配给每个情景的资源量可以得到保证。为应对 VPN 会话数临时激增超过所分配数量的情况，ASA 会支持“突发”VPN 资源类型，其数量等于剩余的未分配 VPN 会话。突发会话可以超订用，并按照先到先得原则供情景使用。

默认类

所有未分配给其他类的情景都属于默认类；您不必主动向默认类分配情景。

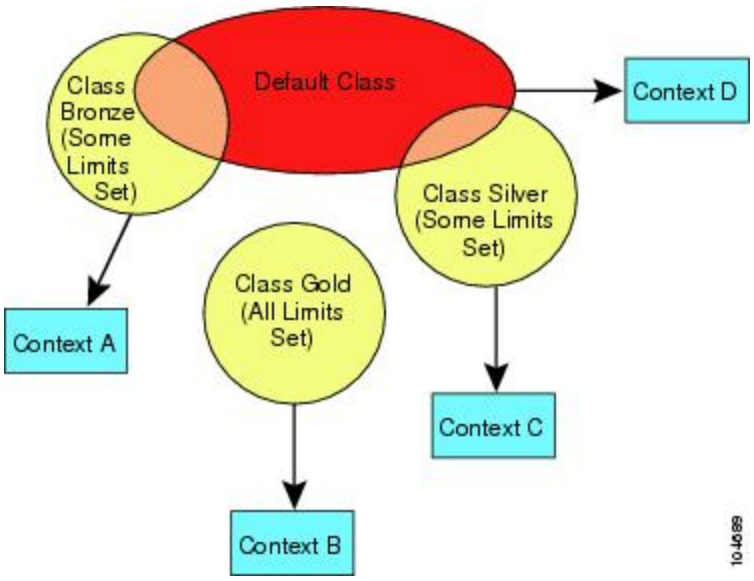
如果某个情景属于除默认类以外的类，则其类设置始终覆盖默认类设置。但是，如果另一个类具有任何未定义的设置，则成员情景为这些限制使用默认类。例如，如果创建的类对所有并发连接具有2%的限制，但没有任何其他限制，则所有其他限制都继承自默认类。相反，如果创建对所有资源都有限制的类，则该类不使用默认类中的任何设置。

对于大多数资源，默认类会为所有情景提供无限制的资源访问，但以下限制除外：

- Telnet 会话 - 5 个会话。（每个情景的最大值。）
- SSH 会话 - 5 个会话。（每个情景的最大值。）
- ASDM 会话 - 5 个会话。（每个情景的最大值。）
- IPsec 会话 - 5 个会话（每个情景的最大值。）
- MAC 地址 - 65535 个条目。（系统最大值。）
- AnyConnect 客户端 对等体- 0 个会话。（您必须将该类手动配置为允许任何 AnyConnect 客户端对等体。）
- VPN 站点间隧道 - 0 个会话。（您必须将该类手动配置为允许任何 VPN 会话。）
- HTTPS 会话 - 6 个会话。（每个情景的最大值。）

下图显示了默认类与其他类之间的关系。情景 A 和 C 属于设置了某些限制的类；其他限制继承自默认类。情景 B 不会从默认类继承任何限制，因为所有限制都在其类（Gold 类）中进行设置。情景 D 未分配给某个类，因此会默认成为默认类的成员。

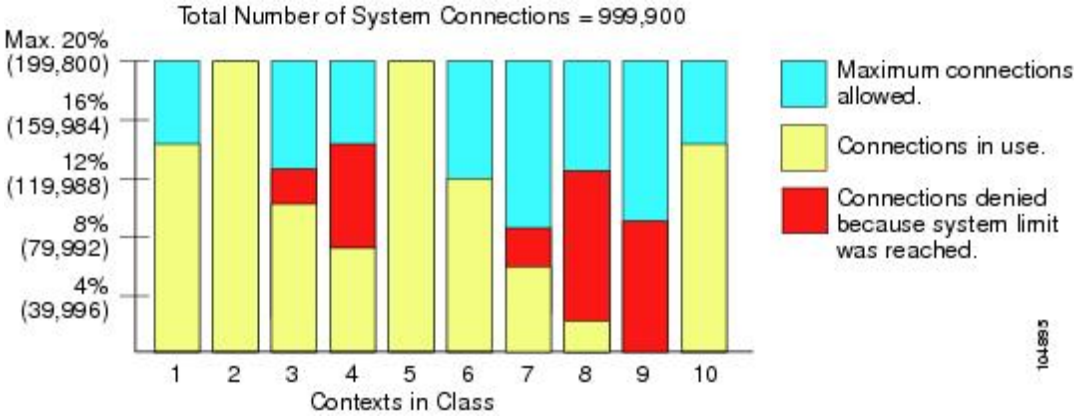
图 *5:* 资源类



使用超订用资源

您可以通过在所有情景范围内分配超过 100% 的资源（非突发 VPN 资源除外）来超订用 ASA。例如，您可以设置 Bronze 类，以便将连接限制为每个情景 20%，然后将 10 个情景分配给该类（总计 200%）。如果情景并发使用超过系统限制，则每个情景获得的数量少于您希望设置的 20%。

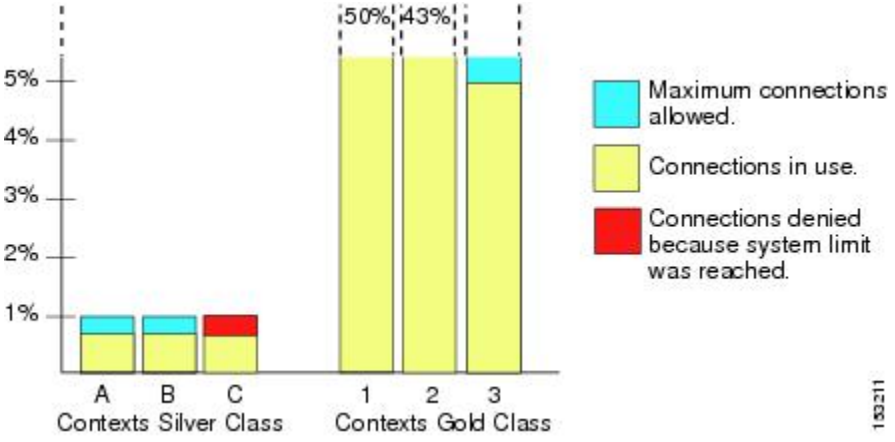
图 *6:* 资源超订用



使用不受限制的资源

通过 ASA，您可以分配对类中一个或多个资源的不受限制访问权限，而不是只分配一定的百分比或是一个绝对的数字。当资源不受限制时，情景可以使用系统可提供的所有资源。例如，情景 A、B 和 C 属于 Silver 类，该类限制每个类成员可使用 1% 的连接（总计 3%）；但是，三个情景当前仅在使用共计 2% 的连接。Gold 类不限制对连接的访问。Gold 类中的情景可使用超过 97% 的“未分配”连接；它们还可以使用情景 A、B 和 C 当前未使用的 1% 的连接，即使这意味着情景 A、B 和 C 无法达到其 3% 的合并限制。设置不受限制的访问权限类似于超额订用 ASA，只是对您超额订用系统的量不太好控制。

图 *7:* 不受限制的资源



关于 MAC 地址

您可以手动分配MAC地址以覆盖默认值。对于多情景模式，您可以自动生成唯一的MAC地址（适用于分配给情景的所有接口）和单情景模式（适用于子接口）。.

注释 您可能想要为 ASA 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于MAC地址生成的，因此将唯一MAC地址分配给子接口会允许使用唯一IPv6链路本地地址，这能够避免 ASA 上特定实例内发生流量中断。

多情景模式下的 MAC 地址

MAC地址用于在情景中对数据包进行分类。如果您共享某个接口，但在每个情景中没有该接口的唯一 MAC 地址，则可尝试可能不会提供完全覆盖的其他分类方法。

为了允许情景共享接口，您应该为每个共享情景接口启用自动生成虚拟 MAC 地址的功能。

自动 MAC 地址

在多情景模式下，自动生成会为分配给情景的所有接口分配唯一的 MAC 地址。

如果您手动分配MAC地址，并且同时启用自动生成，则会使用手动分配的MAC地址。如果您随后删除了手动 MAC 地址，则会使用自动生成的地址（如果已启用）。

在出现生成的MAC地址与网络中的另一个专用MAC地址冲突这种极少发生的情况下，您可以为接口手动设置 MAC 地址。

由于自动生成的地址（使用前缀时）以 A2 开头，因此如果您同时希望使用自动生成，则不能使用以 A2 开头的手动 MAC 地址。

ASA 使用以下格式生成 MAC 地址：

A2*xx.yyzz.zzzz*

其中，*xx.yy* 是用户定义的前缀或根据接口 MAC 地址的最后两个字节自动生成的前缀，*zz.zzzz* 是由 ASA 生成的内部计数器。对于备用 MAC 地址，地址完全相同，但内部计数器会加 1。

如何使用前缀的示例如下：如果将前缀设置为 77，则 ASA 会将 77 转换为十六进制值 004D (*yyxx*)。在 MAC 地址中使用时，该前缀会反转 (*xxyy*)，以便与 ASA 的本地形式匹配：

A2**4D.00***zz.zzzz*

对于前缀 1009 (03F1)，MAC 地址为：

A2**F1.03***zz.zzzz*

注释 没有前缀的MAC地址格式是旧式版本。有关传统格式的详细信息，请参阅命令参考中的**mac-address auto** 命令。

VPN 支持

对于 VPN 资源，您必须将资源管理配置为允许任何 VPN 隧道。

您可以在多情景模式下使用站点间 VPN。

对于远程接入 VPN，您必须使用 AnyConnect 3.x 及更高版本的 SSL VPN 和 IKEv2 协议。 您可以按情景自定义用于 AnyConnect 客户端 映像和定制的闪存，以及跨所有情景使用共享闪存。有关不支持的功能，请参阅多情景模式指南，第 12 页。有关每个 ASA 版本支持的 VPN 功能的详细列表，请参阅多情景模式的历史，第 41 页。

注释 多情景模式下需要 AnyConnect Apex Apex 许可证；您无法使用默认或传统许可证。

多情景模式许可

型号	许可证要求
Firepower 1010	不支持。
Firepower 1100	标准 许可证：2 个情景。 可选许可证，最多： *Firepower 1120：5* *Firepower 1140：10* *Firepower 1150：25*
Firepower 2100	标准 许可证：2 个情景。 可选许可证，最多： *Firepower 2110：25* *Firepower 2120：25* *Firepower 2130：30* *Firepower 2140：40*
Secure Firewall 3100	标准 许可证：2 个情景。 可选许可证，最多： *Secure Firewall 3110: 100* *Secure Firewall 3120: 100* *Secure Firewall 3130: 100* *Secure Firewall 3140: 100*

型号	许可证要求
Firepower 4100	标准 许可证：10 个情景。 可选许可证：最多 *250* 个情景。
Firepower 9300	标准 许可证：10 个情景。 可选许可证：最多 *250* 个情景。
ISA 3000	不支持。
ASA 虚拟	不支持。

注释 如果管理情景仅包含仅管理接口，并且不包括直通流量的任何数据接口，则不计入限制。

注释 多情景模式下需要 AnyConnect Apex Apex 许可证；您无法使用默认或传统许可证。

多情景模式的先决条件

在进入多情景模式后，请连接到系统或管理情景，以便访问系统配置。不能在非管理情景配置系统。默认情况下，在启用多情景模式之后，可以使用默认管理 IP 地址连接到管理情景。

多情景模式指南

故障切换

仅在多情景模式下支持主用/主用模式故障切换。

IPv6

跨情景 IPv6 路由不受支持。

不支持的功能

多情景模式不支持以下功能：

- RIP
- OSPFv3。（支持 OSPFv2。）
- 组播路由

- 威胁检测
- 统一通信
- QoS
- 虚拟隧道接口 (VTI)
- 静态路由跟踪

多情景模式当前不支持远程访问 VPN 的以下功能：

- AnyConnect 2.x 及更低版本
- IKEv1
- SAML
- WebLaunch
- VLAN Mapping
- HostScan
- VPN 负载均衡
- 可以定制
- L2TP

其他准则

- 情景模式（单情景或多情景）不会存储在配置文件中，即使该模式经过重新启动也是如此。如果您需要将配置复制到另一台设备，请将新设备设置为匹配的模式。
- 如果将情景配置存储在闪存的根目录中，则在某些型号上可能会用尽该目录中的空间，即使有可用内存也是如此。在这种情况下，请为配置文件创建子目录。背景：某些型号使用 FAT 16 文件系统的内部闪存，并且，如果您未使用兼容 8.3 格式的短名称，或使用大写字符，则只能存储少于 512 个的文件和文件夹，因为文件系统会用尽所有插槽来存储长文件名（请参阅 http://support.microsoft.com/kb/120138/en-us）。
- 在 ACI 中，使用所有枝叶上的相同 MAC 地址执行基于策略的重定向 (PBR) 运行状况检查（L2 ping）。这会导致 MAC 摆动。要解决 MAC 摆动问题，可以在内联集上配置分流模式选项。但是，如果 威胁防御 配置了高可用性，则必须在故障切换期间启用 MAC 获知以进行连接处理。因此，在 威胁防御 使用内联集接口的高可用性对的 ACI 环境中，为避免丢包，请在独立或集群中部署 威胁防御 。

多情景模式默认设置

- 默认情况下，ASA 处于单情景模式下。

- 请参阅默认类，第 7 页。

配置多情景

过程

步骤 1 启用或禁用多情景模式，第 14 页。

步骤 2 （可选）配置用于资源管理的类，第 16 页。

注释　　要支持 VPN，必须在资源类中配置 VPN 资源；默认类不允许使用 VPN。

步骤 3 在系统执行空间中配置接口。

- Firepower 1100、设备模式下的 Firepower 2100、Secure Firewall 3100—基本接口配置。
- 平台模式下 的 Firepower 2100：请参阅《入门指南》。
- Firepower 4100/9300-逻辑设备 Firepower 4100/9300

步骤 4 配置安全情景，第 20 页。

步骤 5 （可选）自动为情景接口分配 MAC 地址，第 24 页。

步骤 6 完成情景中的接口配置。请参阅路由模式接口和透明模式接口。

启用或禁用多情景模式

根据您从思科订购 ASA 的方式，您的 ASA 可能以针对多个安全情景进行了配置。如果您需要从单模式转换为多模式，请遵循本节中的程序。

启用多情景模式

当您从单模式转换为多模式时，ASA 会将运行配置转换为两个文件：一个是包含系统配置的新启动配置，另一个是包含管理情景的 admin.cfg（位于内部闪存的根目录中）。原始运行配置另存为 old_running.cfg（位于内部闪存的根目录中）。系统不会保存原始启动配置。ASA 自动向系统配置中添加一个管理情景的条目，名称为“admin”。

开始之前

如果启动配置与运行配置不同，请备份启动配置。当您从单模式转换为多模式时，ASA 会将运行配置转换为两个文件。系统不会保存原始启动配置。请参阅备份和恢复配置或其他文件。

过程

切换到多情景模式。

mode multiple

示例：

系统将提示您更改模式并转换配置，然后系统将会重新加载。

注释 您必须在管理情景中重新生成 RSA 密钥对，才能重新建立 SSH 连接。在控制台中，输入 **crypto key generate rsa modulus** 命令。有关详细信息，请参阅 配置 SSH 访问。

示例：

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

Converting the configuration - this may take several minutes for a large configuration

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple
ciscoasa(config)#


***
*** --- START GRACEFUL SHUTDOWN ---
***
*** Message to all terminals:
***
***   change mode
Shutting down isakmp
Shutting down webvpn
Shutting down License Controller
Shutting down File system



***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
```

恢复单情景模式

要将旧运行配置复制到启动配置，并将模式切换到单情景模式，请执行以下步骤：

开始之前

在系统执行空间中执行此程序。

过程

步骤 1 将原始运行配置的备份版本复制到当前启动配置：

copy disk0:old_running.cfg startup-config

示例：

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

步骤 2 将模式设置为单模式：

mode single

示例：

```
ciscoasa(config)# mode single
```

系统将提示您重新启动 ASA。

配置用于资源管理的类

要在系统配置中配置某个类，请执行下述步骤。您可以通过重新输入带有新值的命令来更改特定资源限制的值。

开始之前

- 在系统执行空间中执行此程序。
- 下表列出了资源类型和限制。另请参阅 **show resource types** 命令。

注释 如果系统限制为“不适用”，则无法设置该资源的百分比，因为该资源不存在硬性系统限制。

表 *1:* 资源名称和限制

资源名称	速率或并发	每个情景的最小和最大数量限制	系统限制	说明
asdm	并发	1（最小值） 5（最大值）	200	ASDM 管理会话。 ASDM 会话使用两个 HTTPS 连接：一个用于监控（始终存在），另一个用于进行配置更改（仅当进行更改时才存在）。例如，系统限制为 200 个 ASDM 会话表示 HTTPS 会话数限制为 400 。
conns	并发或速率	不适用	并发连接数：有关适用于您的型号的连接限制，请参阅每个型号支持的功能许可证。 速率：不适用	任意两台主机之间的 TCP 或 UDP 连接数，包括一台主机和多台其他主机之间的连接。 **注释** 对于值小于 xlates 或 conns 的任一限制，会生成相应的系统日志消息。例如，如果将 xlates 限制设置为 7 并将 conns 限制设置为 9，则 ASA 仅会生成系统日志消息 321001（“Resource 'xlates' limit of 7 reached for context 'ctx1'”），而不会生成 321002（“Resource 'conn rate' limit of 5 reached for context 'ctx1'”）。
主机	并发	不适用	不适用	可以通过 ASA 连接的主机数。
http	并发	1（最小值） 6（最大值）	100	非 ASDM HTTPS 会话
inspects	速率	不适用	不适用	每秒应用检测数。
mac-addresses	并发	不适用	65,535	对于透明防火墙模式，表示 MAC 地址表中允许的 MAC 地址数量。
路由	并发	不适用	不适用	动态路由数。

资源名称	速率或并发	每个情景的最小和最大数量限制	系统限制	说明
vpn burst anyconnect	并发	不适用	您型号的 AnyConnect 客户端 高级对等体数减去为 **vpn anyconnect** 向所有情景分配的会话总和。	所允许的 AnyConnect 客户端 会话数超过了分配到某一包含 **vpn anyconnect** 的情景的会话数。例如，如果您的型号支持 5000 个对等体，而您为包含 **vpn anyconnect** 的所有情景共分配了 4000 个对等体，则剩余 1000 个对等体可用于 **vpn burst anyconnect**。不同于能保证情景会话的 **vpn anyconnect**，**vpn burst anyconnect** 有可能被超订用；突发池将根据先到先得的原则可用于所有情景。
vpn anyconnect	并发	不适用	有关适用于您的型号的 AnyConnect 客户端 高级对等体数的信息，请参阅每个型号支持的功能许可证。	AnyConnect 客户端 对等体。不能超订用此资源；所有情景分配的总和不得超过型号限制。为此资源分配的对等体数保证可供相应情景使用。
vpn burst other	并发	不适用	您型号的其他 VPN 会话数量减去为**vpn other** 向所有情景分配的会话总和。	所允许的站点间 VPN 会话数超过了分配到某一包含 **vpn other** 的情景的会话数。例如，如果您的产品型号支持 5000 个会话，您为具有 **vpn other** 的所有情景分配了 4000 个会话，其余 1000 个会话可用于 **vpn burst other**。不同于能保证情景会话的**vpn other**，**vpn burst other** 有可能被超订用；突发池将根据先到先得的原则可用于所有情景。
vpn other	并发	不适用	有关适用于您的型号的其他 VPN 会话数的信息，请参阅每个型号支持的功能许可证。	站点间 VPN 会话数。不能超订用此资源；所有情景分配的总和不得超过型号限制。为此资源分配的会话数保证可供相应情景使用。
ikev1 in-negotiation	并发（仅百分比）	不适用	分配到此情景的其他 VPN 会话的百分比。请参阅 **vpn other** 资源，为情景分配会话。	传入 IKEv1 SA 协商，占情景其他 VPN 限制的百分比。
ssh	并发	1（最小值） 5（最大值）	100	SSH 会话数。

资源名称	速率或并发	每个情景的最小和最大数量限制	系统限制	说明
storage	MB	最大值取决于您指定的闪存驱动器	最大值取决于您指定的闪存驱动器	情景目录的存储限制 (MB)。使用 **storage-url** 命令指定驱动器。
syslogs	速率	不适用	不适用	每秒系统日志消息数。
telnet	并发	1（最小值） 5（最大值）	100	Telnet 会话数。
xlates	并发	不适用	不适用	网络地址转换数。

过程

步骤 1 指定类名并进入类配置模式：

class *name*

示例：

```
ciscoasa(config)# class gold
```

name 是最大长度为 20 个字符的字符串。要设置默认类的限制，请输入 **default** 作为名称。

步骤 2 设置资源类型的资源限制：

limit-resource [**rate**] *resource_name number*[**%**]

示例：

```
ciscoasa(config-class)# limit-resource rate inspects 10
```

- 有关资源类型列表，请参阅前面的表。如果指定 **all**，则会将所有资源都配置为相同的值。如果还指定了特定资源的值，则该限制会覆盖为 **all** 设置的限制。
- 输入 **rate** 参数以设置特定资源的每秒速率。
- 对于大多数资源，请将 *number* 指定为 **0**，从而将资源设置为不受限制或使用系统限制（如果适用）。对于 VPN 资源，**0** 表示将限制设置为无。
- 对于没有系统限制的资源，不能设置百分比 (**%**)；只能设置绝对值。
- 如果您还在情景中设置 **quota management-session** 命令以设置最大管理会话数（SSH 等），则将使用较小的值。

示例

例如，要将默认类的连接数限制设置为 10% 而非不受限制，并允许使用 5 个站点间 VPN 隧道（其中两个隧道预留用于 VPN 突发），请输入以下命令：

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 5
ciscoasa(config-class)# limit-resource vpn burst other 2
```

所有其他资源保持不受限制。

要添加名为 gold 的类，请输入以下命令：

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 5000
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5
```

为情景配置了资源类时，会进行检查。如果在尝试 VPN 远程访问连接之前未安装适当的许可证，会生成安装警告。然后，管理员必须获取 AnyConnect Apex 许可证。例如，可能显示如下警告：

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn anyconnect 10.0%
ciscoasa(config-class)# context test
Creating context 'text'...Done. (3)
ciscoasa(config-ctx)# member vpn
WARNING: Multi-mode remote access VPN support requires an AnyConnect Apex license.
Warning: An Access Context license is required for remote-access VPN support in multi-mode.
ciscoasa(config-ctx)#
```

配置安全情景

系统配置中的安全情景定义确定情景名称、配置文件 URL、情景可使用的接口以及其他设置。

开始之前

- 在系统执行空间中执行此程序。
- 配置接口。对于透明模式情景，您无法在情景之间共享接口，因此您可能需要使用子接口。要计划管理接口使用，请参阅 管理接口使用情况，第 7 页。
  - Firepower 1100、设备模式下的 Firepower 2100、Secure Firewall 3100—基本接口配置。

- 平台模式下 的 Firepower 2100：请参阅《入门指南》。
- Firepower 4100/9300-逻辑设备 Firepower 4100/9300

- 如果您没有管理情景（例如，如果清除了配置），则必须先通过输入以下命令指定管理情景名称：

```
ciscoasa(config)# admin-context name
```

虽然此情景在配置中尚不存在，但是可以随后输入 **context** *name* 命令来继续进行管理情景配置。

过程

步骤 1 添加或修改情景：

context *name*

示例：

```
ciscoasa(config)# context admin
```

name 是最大长度为 32 个字符的字符串。此名称区分大小写，因此您可以具有名为“customerA”和“CustomerA”的两个情景。您可以使用字母、数字或连字符，但名称不能以连字符开头或结尾。

注释 “System”或“Null”（采用大写或小写字母）是保留名称，因此不能使用。

步骤 2 （可选） 为此情景添加描述：

description 文本、

示例：

```
ciscoasa(config-ctx)# description Admin Context
```

步骤 3 指定您可以在此情景中使用的接口：

要分配接口，请执行以下操作：

allocate-interface *interface_id* [*mapped_name*] [**visible** | **invisible**]

要分配一个或多个子接口，请执行以下操作：

allocate-interface *interface_id.subinterface* [*-interface_id.subinterface*] [*mapped_name*[*-mapped_name*]] [**visible** | **invisible**]

示例：

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

注释　　请勿在接口类型和端口号之间包含空格。

- 多次输入这些命令可指定不同的范围。如果使用此命令的**no**形式删除某项分配，则包括此接口的所有情景命令都将从运行的配置中删除。
- 如果需要，可以在路由模式下将相同接口分配给多情景。透明模式不允许使用共享接口。
- *Mapped_name* 是可在情景中使用的接口的字母数字别名，而不是接口 ID。如果不指定映射名称，则会在情景中使用接口 ID。出于安全目的，您可能不希望情景管理员知道情景使用的是哪些接口。映射名称必须以字母开头，以字母或数字结尾，并且内部字符只能是字母、数字或下划线。例如，您可以使用以下名称：**int0**、**inta**、**int_0**。
- 如果指定子接口的范围，则可以指定匹配的映射名称的范围。关于范围，请遵循以下准则：
  - 映射名称必须由后跟数字部分的字母部分组成。映射名称的字母部分必须与范围的两端均匹配。例如，可输入以下范围：**int0-int10**。例如，如果输入 gig0/1.1-gig0/1.5 **happy**1-**sad**5，则命令会失败。
  - 映射名称的数字部分必须与子接口范围包含相同的数字数量。例如，两个范围都包括 100 个接口：**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100**。例如，如果输入 gig0/0.**100**-gig0/0.**199** int**1**-int**15**，则命令会失败。
- 如果设置了映射的名称，则指定 **visible** 可在 **show interface** 命令中查看实际接口 ID。默认关键字 **invisible** 仅显示映射的名称。

步骤 4 标识系统从其下载情景配置的 URL。

config-url *url*

示例：

```
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
```

步骤 5 （可选） 允许每个情景使用闪存来存储 VPN 数据包（例如 AnyConnect 客户端）以及为 AnyConnect 客户端 和无客户端 SSL VPN 门户自定义提供存储。例如，如果使用多个情景模式来配置具有动态访问策略的 AnyConnect 客户端 配置文件，则必须计划特定于情景的专用存储。每个情景可使用私有存储空间以及共享的只读存储空间。**注意**：请使用**mkdir**命令确保目标目录已存在于指定磁盘中。

storage-url {**private** | **shared**} [**disk***n***:/**]*path* [*context_label*]

示例：

```
ciscoasa(config)# mkdir disk1:/private-storage
ciscoasa(config)# mkdir disk1:/shared-storage
ciscoasa(config)# context admin
ciscoasa(config-ctx)# storage-url private disk1:/private-storage context
ciscoasa(config-ctx)# storage-url shared disk1:/shared-storage shared
```

您可以为每个情景指定一个**private**存储空间。您可以从情景中的此目录（以及从系统执行空间）执行读取/写入/删除操作。如果您不指定磁盘编号，则默认为 disk0。在指定的 *path* 下，ASA 将在情景后创建一个子目录。例如，对于 contextA，如果指定 **disk1:/private-storage** 作为路径，则 ASA 会在 **disk1:/private-storage/contextA/** 为此情景创建一个子目录。或者，您也可以使用 *context_label* 在情

景内为路径命名，这样文件系统不会暴露给情景管理员。例如，如果指定 *context_label* 作为 **context**，则此目录将在情景内称为 **context:**。要控制每个情景允许的磁盘空间量，请参阅配置用于资源管理的类，第 16 页。

您可以对每个情景指定一个只读**shared**存储空间，但可以创建多个共享目录。为了减少可以在所有情景之间共享的大型公共文件的副本，例如 AnyConnect 客户端 包，可以使用共享存储空间。ASA 不会为此存储空间创建情景子目录，因为该存储空间是多个情景的共享空间。只有系统执行空间可以从共享目录写入和删除。

步骤 6 （可选） 将情景分配给资源类：

member *class_name*

示例：

```
ciscoasa(config-ctx)# member gold
```

如果不指定类，则情景属于默认类。只能将情景分配给一个资源类。

步骤 7 （可选） 将情景分配给主用/主用故障切换中的故障切换组：

join-failover-group {**1** | **2**}

示例：

```
ciscoasa(config-ctx)# join-failover-group 2
```

默认情况下，情景处于组 1 中。管理情景必须始终处于组 1 中。

步骤 8 （可选） 为此情景启用云网络安全：

scansafe [**license** *key*]

示例：

```
ciscoasa(config-ctx)# scansafe
```

如果不指定**license**，该情景会使用在系统配置中配置的许可证。ASA 将身份验证密钥发送到云网络安全代理服务器，以指明请求从哪个组织发出。身份验证密钥是一个 16 字节的十六进制数。

有关 ScanSafe 的详细信息，请参阅防火墙配置指南。

示例

以下示例将管理情景设置为“administrator”，在内部闪存中创建一个名为“administrator”的情景，然后从 FTP 服务器添加两个情景：

```
ciscoasa(config)# admin-context admin
ciscoasa(config)# context admin
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
```

```
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold


ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

自动为情景接口分配 MAC 地址

本节介绍如何配置 MAC 地址的自动生成。MAC 地址用于在情景中对数据包进行分类。

开始之前

- 当在情景中为接口配置 **nameif** 命令时，系统会立即生成新的 MAC 地址。如果在配置情景接口后启用此功能，则在启用之后，会立即为所有接口生成 MAC 地址。如果禁用此功能，则每个接口的 MAC 地址会恢复为默认 MAC 地址。例如，GigabitEthernet0/1 的子接口恢复为使用 GigabitEthernet0/1 的 MAC 地址。
- 在出现生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突这种极少发生的情况下，您可以在情景中为接口手动设置 MAC 地址。

过程

自动向每个情景接口分配专用 MAC 地址：

mac-address auto [**prefix** *prefix*]

示例：

```
ciscoasa(config)# mac-address auto prefix 19
```

如果未输入前缀，ASA 根据接口 (ASA 5500-X) 的最后两个字节自动生成前缀。

如果您手动输入前缀，则 *prefix* 是介于 0 和 65535 之间的十进制值。此前缀会转换为一个四位数的十六进制数字，并用作 MAC 地址的一部分。

在情景和系统执行空间之间更改

如果您登录到系统执行空间（或管理情景），则可以在情景之间切换，并在每个情景中执行配置和监控任务。您在配置模式下编辑或在 **copy** 或 **write** 命令中使用的运行配置取决于您的位置。当您处于系统执行空间时，运行配置仅包含系统配置；当您处于某个情景时，运行配置仅包含该情景。例如，您无法通过输入 **show running-config** 命令查看所有运行配置（系统配置以及所有情景配置）。系统仅显示当前配置。

过程

步骤 1 切换到情景：

changeto context *name*

提示符切换到 ciscoasa/*name*#

步骤 2 切换到系统执行空间：

changeto system

提示符切换到 ciscoasa#

管理安全情景

本部分介绍如何管理安全情景。

删除安全情景

除非您使用 **clear context** 命令删除所有情景，否则无法删除当前管理情景。

注释 如果使用故障切换，则从主用设备上删除情景到在备用设备上删除该情景之间存在一定延迟。您可能会看到错误消息，表明主用设备和备用设备上的接口数不一致；此错误是临时的，可以忽略。

开始之前

在系统执行空间中执行此程序。

过程

步骤 1 删除单个情景：

no context *name*

此外，还会删除所有情景命令。系统不会从配置 URL 位置中删除情景配置文件。

步骤 2 删除所有情景（包括管理情景）：

clear context

系统不会从配置 URL 位置中删除情景配置文件。

更改管理情景

系统配置本身并不包含任何网络接口或网络设置；相反，当系统需要访问网络资源（例如，从服务器下载情景）时，它使用指定为管理情景的某个情景。

管理情景与任何其他情景一样，不同之处在于，当用户登录到管理情景时，该用户将具有系统管理员权限并可访问系统和所有其他情景。管理情景在任何情况下都不受限制，可用作常规情景。但是，由于登录到管理情景会授予用户针对所有情景的管理员权限，因此可能需要将对管理情景的访问限定于适当的用户。

开始之前

- 可以将任何情景设置为管理情景，只要配置文件存储在内部闪存中即可。
- 在系统执行空间中执行此程序。

过程

设置管理情景：

admin-context *context_name*

示例：

```
ciscoasa(config)# admin-context administrator
```

连接到管理情景的所有远程管理会话（如 Telnet、SSH 或 HTTP）都会终止。必须重新连接到新的管理情景。

某些系统配置命令（包括 **ntp server**）会标识属于管理情景的接口名称。如果您更改管理情景，并且新的管理情景中不存在该接口名称，请务必更新引用该接口的所有系统命令。

更改安全情景 URL

本节介绍如何更改情景 URL。

开始之前

- 在没有通过新的 URL 重新加载配置的情况下，不能更改安全情景 URL。ASA 会将新的配置与当前的运行配置合并。
- 重新输入同一 URL 也可将已保存的配置与运行配置合并。
- 合并会将新配置中的所有新命令添加到运行配置中。
  - 如果配置相同，则不会发生任何更改。
  - 如果命令冲突或命令影响情景的运行，则合并的影响取决于命令。可能会发生错误，也可能出现意外结果。如果运行配置为空（例如，如果服务器不可用且从未下载配置），则使用新的配置。
- 如果您不想合并配置，可清除运行配置（该操作通过情景中断所有通信），然后从新的URL重新加载配置。
- 在系统执行空间中执行此程序。

过程

步骤 1 （可选，前提是您不需要执行合并）切换到情景并清除配置：

changeto context *name*

clear configure all

示例：

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(config)# clear configure all
```

如果要执行合并，请跳至步骤 2。

步骤 2 切换到系统执行空间：

changeto system

示例：

```
ciscoasa/ctx1(config)# changeto system
ciscoasa(config)#
```

步骤 3 进入要更改的情景的情景配置模式。

context *name*

示例：

```
ciscoasa(config)# context ctx1
```

步骤 4 输入新 URL。系统会立即加载情景，以便其正常运行。

config-url *new_url*

示例：

```
ciscoasa(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg
```

重新加载安全情景

您可以通过两种方式重新加载情景：

- 清除运行配置，然后导入启动配置。

  此操作会清除与情景关联的大多数属性，例如，连接和 NAT 表。

- 从系统配置中删除情景。

  此操作会清除其他属性，例如，可能有助于故障排除的内存分配。但是，将情景添加回系统要求重新指定 URL 和接口。

通过清除配置来重新加载

过程

步骤 1 切换到要重新加载的情景：

changeto context *name*

示例：

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(comfig)#
```

步骤 2 清除运行配置：

clear configure all

此命令会清除所有连接。

步骤 3 重新加载配置：

copy startup-config running-config

示例：

```
ciscoasa/ctx1(config)# copy startup-config running-config
```

ASA 会从系统配置中指定的 URL 中复制配置。不能在情景中更改此 URL。

通过删除和重新添加情景来重新加载

要通过删除情景再重新添加来重新加载情景，请执行以下步骤。

过程

步骤 1 删除安全情景，第 25 页。**同时从磁盘中删除配置 URL 文件**

步骤 2 配置安全情景，第 20 页

监控安全情景

本节介绍如何查看和监控情景信息。

查看情景信息

从系统执行空间中，您可以查看情景列表，包括名称、分配的接口和配置文件 URL。

过程

显示所有情景：

show context [*name* | **detail**| **count**]

如果要显示特定情景的信息，请指定 *name*。

detail 选项用于显示其他信息。有关详细信息，请参阅以下样本输出。

count 选项用于显示情景的总数。

示例

以下是 **show context** 命令的输出示例。以下样本输出显示三个情景：

```
ciscoasa# show context

Context Name      Interfaces                    URL
*admin            GigabitEthernet0/1.100        disk0:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200        disk0:/contexta.cfg
```

```
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300        disk0:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

下表显示了每个字段的说明。

表 *2: show context Fields*

字段	说明 (Description)
Context Name	列出所有情景名称。名称中带有星号 (*) 的情景是管理情景。
Interfaces	分配给情景的接口。
URL	ASA 从中加载情景配置的 URL。

以下是 **show context detail** 命令的输出示例：

```
ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk0:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

有关 **detail** 输出的详细信息，请参阅命令参考。

以下是 **show context count** 命令的输出示例：

```
ciscoasa# show context count
Total active contexts: 2
```

查看资源分配

从系统执行空间中，您可以查看每种资源跨所有类和类成员的分配情况。

过程

显示资源分配：

show resource allocation [**detail**]

此命令显示资源分配情况，但不显示实际正在使用的资源。有关实际资源使用情况的详细信息，请参阅查看资源使用情况，第 33 页。

detail 参数用于显示其他信息。有关详细信息，请参阅以下样本输出。

示例

以下样本输出以绝对值和可用系统资源百分比的形式，显示每个资源的总分配情况：

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Routes                      5000           N/A
 Telnet                        35           35.00%
 Xlates                     91749           N/A
 AnyConnect                  1000           10%
 AnyConnectBurst              200           2%
 Other VPN Sessions            20           2.66%
 Other VPN Burst               20           2.66%
 All                    unlimited
```

下表显示每个字段的说明。

***表 3: show resource allocation* 字段**

字段	说明 (Description)
Resource	可限制的资源的名称。
Total	跨所有情景分配的资源总量。此数量是每秒的并发实例或实例的绝对数量。如果在类定义中指定了百分比，则 ASA 会在显示该值时将百分比转换为绝对数量。
% of Avail	跨所有情景分配的总系统资源的百分比（如果资源有硬性系统限制）。如果资源没有系统限制，则此列将显示 N/A。

以下是 **show resource allocation detail** 命令的样本输出：

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%

Hosts            default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      26214      26214      N/A
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      N/A

SSH              default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%

Telnet           default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%

Routes           default          all       C  unlimited                N/A
                 gold               1       D  unlimited          5     N/A
                 silver             1      CA         10         10     N/A
                 bronze             0      CA          5                N/A
                 All Contexts:      3                            20     N/A

Xlates           default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      23040      23040     N/A
                 bronze             0      CA      11520
                 All Contexts:      3                         23040     N/A

mac-addresses    default          all       C      65535
```

```
gold                1       D       65535       65535    100.00%
silver              1      CA        6553        6553      9.99%
bronze              0      CA        3276
All Contexts:       3                          137623    209.99%
```

下表显示每个字段的说明。

表 *4: show resource allocation detail* 字段

字段	说明 (Description)
Resource	可限制的资源的名称。
Class	每个类（包括默认类）的名称。 All contexts 字段显示所有类的全部值。
Mmbrs	分配给每个类的情景数量。
Origin	资源限制的源，如下所示： • A - 使用 **all** 选项设置此限制，而不是将其设置为单独资源。 • C - 此限制派生自成员类。 • D - 此限制未在成员类中定义，而是派生自默认类。对于分配给默认类的情景，值将会是“C”而不是“D”。 ASA 可以将“A”和“C”或“D”结合使用。
Limit	每个情景的资源限制，显示为绝对数量。如果在类定义中指定了百分比，则ASA会在显示该值时将百分比转换为绝对数量。
Total	跨类中的所有情景分配的资源总量。此数量是每秒的并发实例或实例的绝对数量。如果资源不受限制，则显示为空白。
% of Avail	跨类中的所有情景分配的总系统资源的百分比。如果资源不受限制，则显示为空白。如果资源没有系统限制，则此列将显示 N/A。

查看资源使用情况

从系统执行空间中，您可以查看每个情景的资源使用情况，并显示系统资源使用情况。

过程

查看每个情景的资源使用情况：

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system**] [**resource** {*resource_name* | **all**} | **detail**] [**counter** *counter_name* [*count_threshold*]]

- 默认情况下，系统会显示**所有**情景的使用情况；每个情景会单独列出。
- 输入 **top** *n* 关键字可显示对指定资源的使用排名前 *n* 的用户的情景。对于此选项，必须指定单个资源类型，而不能指定 **resource all**。
- **summary** 选项用于显示所有情景的综合使用情况。
- **system** 选项用于显示所有情景的综合使用情况，但显示的是资源的系统限制，而不是综合情景限制。
- 对于 **resource** *resource_name*，请参阅配置用于资源管理的类，第 16 页以获取可用资源名称。另请参阅 **show resource type** 命令。指定 **all**（默认值）表示所有类型。
- **detail** 选项用于显示所有资源的资源使用情况，包括无法管理的那些资源。例如，可以查看 TCP 拦截次数。
- **counter** *counter_name* 是以下关键字之一：
  - **current** - 显示活动并发实例数或资源的当前使用率。
  - **denied** - 显示由于超过 Limit 列中所示的资源限制而被拒绝的实例的数量。
  - **peak** - 显示自上一次清除统计信息（使用 **clear resource usage** 命令或由于设备重启）以来，峰值并发实例数或资源的峰值使用率。
  - **all** -（默认）显示所有统计信息。
- *count_threshold* 设置一个数值，如果超过此数值，则会显示资源。默认值为 1。如果资源的使用率低于所设置的数字，则不会显示资源。如果为计数器名称指定 **all**，则 *count_threshold* 适用于当前使用情况。
- 要显示所有资源，请将 *count_threshold* 设置为 **0**。

示例

以下是 **show resource usage context** 命令的样本输出，其中显示管理情景的资源使用情况：

```
ciscoasa# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

以下是 **show resource usage summary** 命令的样本输出，其中显示所有情景和所有资源的资源使用情况。以下样本显示 6 个情景的限制。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
```

```
Syslogs [rate]           1743         2132      N/A              0 Summary
Conns                     584          763      280000(S)        0 Summary
Xlates                   8526         8966      N/A              0 Summary
Hosts                     254          254      N/A              0 Summary
Conns [rate]              270          535      N/A           1704 Summary
Inspects [rate]           270          535      N/A              0 Summary
AnyConnect                2             25      1000             0 Summary
AnyConnectBurst           0              0      200              0 Summary
Other VPN Sessions        0             10      10             740 Summary
Other VPN Burst           0             10      10             730 Summary

S = System: Combined context limits exceed the system limit; the system limit is shown.
```

以下是 **show resource usage summary** 命令的样本输出，其中显示 25 种情景的限制：由于 Telnet 和 SSH 连接的情景限制是每个情景 5 个连接，因此总共限制为 125 个连接。系统限制仅为 100 个链接，因此会显示系统限制。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit    Denied   Context
Telnet                      1            1        100[S]      0   Summary
SSH                         2            2        100[S]      0   Summary
Conns                      56           90        130000(S)   0   Summary
Hosts                      89          102        N/A         0   Summary
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

以下内容是 **show resource usage system** 命令的样本输出，其中显示所有情景的资源使用情况，但是该命令显示的是系统限制，而不是综合情景限制。**counter all 0** 选项用于显示当前未使用的资源。Denied statistics 显示由于系统限制而拒绝资源的次数，如适用。

```
ciscoasa# show resource usage system counter all 0

Resource              Current         Peak      Limit         Denied    Context
Telnet                      0            0        100                0    System
SSH                         0            0        100                0    System
ASDM                        0            0         32                0    System
Routes                      0            0        N/A                0    System
IPSec                       0            0          5                0    System
Syslogs [rate]              1           18        N/A                0    System
Conns                       0            1     280000                0    System
Xlates                      0            0        N/A                0    System
Hosts                       0            2        N/A                0    System
Conns [rate]                1            1        N/A                0    System
Inspects [rate]             0            0        N/A                0    System
AnyConnect                  2           25      10000                0    System
AnyConnectBurst             0            0        200                0    System
Other VPN Sessions          0           10        750              740    System
Other VPN Burst             0           10        750              730    System
```

监控情景中的 SYN 攻击

ASA 使用 TCP 拦截防止 SYN 攻击。TCP 拦截使用 SYN cookie 算法防范 TCP SYN 泛洪攻击。SYN 泛洪攻击包含一系列通常源于欺骗性 IP 地址的 SYN 数据包。SYN 数据包的持续泛滥使服务器 SYN 队列始终保持充满状态，致使其无法处理连接请求。当超过初期连接阈值时，ASA 会充当服务器代

理，并生成对客户端 SYN 请求的 SYN-ACK 响应。当 ASA 收到来自客户端的 ACK 后，即可对客户端进行身份验证，并且允许连接到服务器。

过程

步骤 1 监控各个情景的攻击速率：

show perfmon

步骤 2 监控 TCP 拦截对于各个情景使用的资源量：

show resource usage detail

步骤 3 监控 TCP 拦截对于整个系统使用的资源量：

show resource usage summary detail

示例

以下是 **show perfmon** 命令的样本输出，其中显示名为 admin 的情景的 TCP 拦截速率。

```
ciscoasa/admin# show perfmon

Context:admin
PERFMON STATS:   Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept    322779/s      322779/s
```

以下是 **show resource usage detail** 命令的样本输出，其中显示 TCP 拦截对各个情景使用的资源量。（ **粗体**形式的样本文本显示 TCP 拦截信息。）

```
ciscoasa(config)# show resource usage detail
Resource              Current         Peak      Limit        Denied Context
memory                 843732       847288  unlimited             0 admin
chunk:channels             14           15  unlimited             0 admin
chunk:fixup                15           15  unlimited             0 admin
chunk:hole                  1            1  unlimited             0 admin
chunk:ip-users             10           10  unlimited             0 admin
chunk:list-elem            21           21  unlimited             0 admin
chunk:list-hdr              3            4  unlimited             0 admin
chunk:route                 2            2  unlimited             0 admin
```

```
chunk:static                1           1  unlimited              0 admin
tcp-intercepts         328787      803610  unlimited              0 admin
np-statics                  3           3  unlimited              0 admin
statics                     1           1  unlimited              0 admin
ace-rules                   1           1  unlimited              0 admin
console-access-rul          2           2  unlimited              0 admin
fixup-rules                14          15  unlimited              0 admin
memory                 959872      960000  unlimited              0 c1
chunk:channels             15          16  unlimited              0 c1
chunk:dbgtrace              1           1  unlimited              0 c1
chunk:fixup                15          15  unlimited              0 c1
chunk:global                1           1  unlimited              0 c1
chunk:hole                  2           2  unlimited              0 c1
chunk:ip-users             10          10  unlimited              0 c1
chunk:udp-ctrl-blk          1           1  unlimited              0 c1
chunk:list-elem            24          24  unlimited              0 c1
chunk:list-hdr              5           6  unlimited              0 c1
chunk:nat                   1           1  unlimited              0 c1
chunk:route                 2           2  unlimited              0 c1
chunk:static                1           1  unlimited              0 c1
tcp-intercept-rate      16056       16254  unlimited              0 c1
globals                     1           1  unlimited              0 c1
np-statics                  3           3  unlimited              0 c1
statics                     1           1  unlimited              0 c1
nats                        1           1  unlimited              0 c1
ace-rules                   2           2  unlimited              0 c1
console-access-rul          2           2  unlimited              0 c1
fixup-rules                14          15  unlimited              0 c1
memory              232695716   232020648  unlimited              0 system
chunk:channels             17          20  unlimited              0 system
chunk:dbgtrace              3           3  unlimited              0 system
chunk:fixup                15          15  unlimited              0 system
chunk:ip-users              4           4  unlimited              0 system
chunk:list-elem          1014        1014  unlimited              0 system
chunk:list-hdr              1           1  unlimited              0 system
chunk:route                 1           1  unlimited              0 system
block:16384               510         885  unlimited              0 system
block:2048                 32          34  unlimited              0 system
```

以下样本输出显示 TCP 拦截对整个系统使用的资源量。（粗体形式的样本文本显示 TCP 拦截信息。）

```
ciscoasa(config)# show resource usage summary detail
Resource              Current         Peak      Limit        Denied Context
memory             238421312    238434336  unlimited             0 Summary
chunk:channels             46           48  unlimited             0 Summary
chunk:dbgtrace              4            4  unlimited             0 Summary
chunk:fixup                45           45  unlimited             0 Summary
chunk:global                1            1  unlimited             0 Summary
chunk:hole                  3            3  unlimited             0 Summary
chunk:ip-users             24           24  unlimited             0 Summary
chunk:udp-ctrl-blk          1            1  unlimited             0 Summary
chunk:list-elem          1059         1059  unlimited             0 Summary
chunk:list-hdr             10           11  unlimited             0 Summary
chunk:nat                   1            1  unlimited             0 Summary
chunk:route                 5            5  unlimited             0 Summary
chunk:static                2            2  unlimited             0 Summary
block:16384               510          885  unlimited             0 Summary
block:2048                 32           35  unlimited             0 Summary
tcp-intercept-rate     341306       811579  unlimited             0 Summary
globals                     1            1  unlimited             0 Summary
np-statics                  6            6  unlimited             0 Summary
```

```
statics                     2           2        N/A             0 Summary
nats                        1           1        N/A             0 Summary
ace-rules                   3           3        N/A             0 Summary
console-access-rul          4           4        N/A             0 Summary
fixup-rules                43          44        N/A             0 Summary
```

查看分配的 MAC 地址

您可以查看系统配置或情景中的自动生成的 MAC 地址。

在系统配置中查看 MAC 地址

本节介绍如何查看系统配置中的 MAC 地址。

开始之前

如果您手动向接口分配MAC地址，但也启用了自动生成，则自动生成的地址会继续显示在配置中，即使正在使用的是手动MAC地址也如此。如果随后删除手动MAC地址，则会使用所显示的自动生成的地址。

过程

从系统执行空间显示分配的 MAC 地址：

show running-config all context [*name*]

查看分配的 MAC 地址必须使用 **all** 选项。虽然 **mac-address auto** 命令仅在全局配置模式下可由用户配置，但是该命令在情景配置模式下会与分配的 MAC 地址一起显示为只读条目。只有在情景中使用 **nameif** 命令配置的已分配接口会具有分配的 MAC 地址。

示例

show running-config all context admin 命令的以下输出显示了分配给 Management0/0 接口的主用 MAC 地址和备用 MAC 地址。

```
ciscoasa# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

show running-config all context 命令的以下输出显示了所有情景接口的所有 MAC 地址（主用 MAC 地址和备用 MAC 地址）。请注意，由于未在情景中使用 **nameif** 命令配置 GigabitEthernet0/0 和 GigabitEthernet0/1 主接口，因此没有为其生成 MAC 地址。

```
ciscoasa# show running-config all context
```

```
admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

查看情景中的 MAC 地址

本节介绍如何查看情景中的 MAC 地址。

过程

显示情景中的每个接口正在使用的 MAC 地址：

show interface | include (Interface)|(MAC)

示例

例如：

```
ciscoasa/context# show interface | include (Interface)|(MAC)
```

```
Interface GigabitEthernet1/1.1 "g1/1.1", is down, line protocol is down
        MAC address a201.0101.0600, MTU 1500
Interface GigabitEthernet1/1.2 "g1/1.2", is down, line protocol is down
        MAC address a201.0102.0600, MTU 1500
Interface GigabitEthernet1/1.3 "g1/1.3", is down, line protocol is down
        MAC address a201.0103.0600, MTU 1500
...
```

注释 **show interface** 命令显示正在使用的 MAC 地址；如果您手动分配 MAC 地址，并且也启用了自动生成，则只能查看系统配置中未使用的自动生成地址。

多情景模式示例

以下示例：

- 使用自定义前缀自动设置情景中的 MAC 地址。
- 将默认类的连接数限制设置为 10% 而非不受限制，并将 VPN 其他会话连接数限制设置为 10 且 VPN 突发连接数限制为 5。
- 创建 gold 资源类。
- 将管理情景设置为“administrator”。
- 在内部闪存上创建一个名为“administrator”的情景，该情景将属于默认资源类。
- 从 FTP 服务器添加两个情景，作为 gold 资源类的一部分。

```
ciscoasa(config)# mac-address auto prefix 19

ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5

ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
ciscoasa(config-class)# limit-resource vpn other 100
ciscoasa(config-class)# limit-resource vpn burst other 50

ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
```

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member gold
```

多情景模式的历史

表 *5:* 多情景模式的历史

功能名称	平台版本	功能信息
多个安全情景	7.0(1)	引入了多情景模式。 引入了以下命令：**context**、**mode** 和 **class**。
自动 MAC 地址分配	7.2(1)	引入了将 MAC 地址自动分配给情景接口的功能。 引入了以下命令：**mac-address auto**。
资源管理	7.2(1)	引入了资源管理。 引入了以下命令：**class**、**limit-resource** 和 **member**。
适用于 IPS 的虚拟传感器	8.0(2)	运行 IPS 软件版本 6.0 及更高版本的 AIP SSM 可以运行多个虚拟传感器，这意味着您可以在该 AIP SSM 上配置多个安全策略。您可以向一个或多个虚拟传感器分配每个情景或单模式 ASA，也可以向同一个虚拟传感器分配多个安全情景。 引入了以下命令：**allocate-ips**。
自动 MAC 地址分配增强功能	8.5(2) 9.0(1)	MAC 地址格式更改为使用前缀，以便使用固定起始值 (A2)，并在故障切换对中为主设备和辅助设备 MAC 地址使用不同方案。现在，MAC 地址在重新加载之后也会保持不变。现在，命令解析器会检查是否已启用自动生成；如果您还希望手动分配 MAC 地址，则手动 MAC 地址不能以 A2 开头。 修改了以下命令：**mac-address auto prefix**。

功能名称	平台版本	功能信息
增加了 ASA 5550 和 5580 的最大情景数量。	8.4(1)	ASA 5550 的最大安全情景数量已从 50 增加到 100。ASA 5580 的最大安全情景数量已从 50 增加到 250。
默认情况下会启用自动 MAC 地址分配。	8.5(1)	现在，默认情况下会启用自动 MAC 地址分配。 修改了以下命令：**mac-address auto**。
自动生成 MAC 地址前缀	8.6(1)	在多情景模式下，ASA 现在支持将自动 MAC 地址生成配置转换为使用默认前缀。ASA 基于接口 (ASA 5500-X) 或背板 (ASASM) MAC 地址的最后两个字节自动生成前缀。当您重新加载或重新启用 MAC 地址生成时，系统自动执行此转换。前缀生成方法提供许多好处，包括更好地保证 MAC 地址在网段上的唯一性。您可以通过输入 **show running-config mac-address** 命令查看自动生成的前缀。如果要更改前缀，可以使用自定义前缀重新配置此功能。传统的 MAC 地址生成方法不再可用。 **注释** 为了保持故障切换对无中断升级，如果已启用故障切换，ASA 在重新加载时不会转变现有配置中的 MAC 地址方法。但是，我们强烈建议您在使用故障切换时手动更改前缀生成方法，特别是对于 ASASM。如果没有前缀方法，安装在不同插槽编号的 ASASM 在故障切换时会遇到 MAC 地址变更，并可能会遇到流量中断。升级后，要使用 MAC 地址生成的前缀方法，请重新启用 MAC 地址生成来使用前缀。 修改了以下命令：**mac-address auto**。
默认所有型号（除 ASASM 之外）上均已禁用自动 MAC 地址分配	9.0(1)	现在，自动 MAC 地址分配默认处于禁用状态（除 ASASM 之外）。 修改了以下命令：**mac-address auto**。
安全情景中的动态路由	9.0(1)	现在，在多情景模式下支持 EIGRP 和 OSPFv2 动态路由协议。不支持 OSPFv3、RIP 和组播路由。
用于路由表条目的新资源类型	9.0(1)	系统创建了新的资源类型 routes，用于设置每个情景中的最大路由表条目数。 修改了以下命令：**limit-resource**、**show resource types**、**show resource usage** 和 **show resource allocation**。
多情景模式下的站点间 VPN	9.0(1)	现在，在多情景模式下支持站点间 VPN 隧道。
用于站点间 VPN 隧道的新资源类型	9.0(1)	系统创建了新的资源类型（即 vpn other 和 vpn burst other），用于设置每个情景中站点间 VPN 隧道的最大数量。 修改了以下命令：**limit-resource**、**show resource types**、**show resource usage** 和 **show resource allocation**。

功能名称	平台版本	功能信息
SA IKEv1 SA 协商的新资源类型	9.1(2)	创建了新的资源类型 ikev1 in-negotiation，用于在每个情景中设置 IKEv1 SA 协商的最大百分比，以防 CPU 和加密引擎被淹没。在某些情况下（大型证书、CRL 检查），您可能希望限制此资源。 修改了以下命令：**limit-resource**、**show resource types**、**show resource usage** 和 **show resource allocation**。
支持多情景模式下的远程接入VPN	9.5(2)	现在您可在多情景模式中使用以下远程接入功能： • AnyConnect 3.x 及更高版本（仅支持 SSL VPN；无 IKEv2 支持） • 集中 AnyConnect 客户端 映像配置 • AnyConnect 客户端 映像升级 • 对 AnyConnect 客户端 连接进行情景资源管理 **注释** 多情景模式下需要 AnyConnect Apex Apex 许可证；您无法使用默认或传统许可证。 引入了以下命令：**limit-resource vpn anyconnect**、**limit-resource vpn burst anyconnect**
多情景模式的 Pre-fill/Username-from-cert 功能	9.6(2)	AnyConnect 客户端 SSL 支持已扩展，允许 pre-fill/username-from-certificate 功能 CLI（以前其仅在单情景模式下可用）在多情景模式下也可启用。 未修改任何命令。
使用闪存虚拟化实现远程访问VPN	9.6(2)	多情景模式下的远程访问 VPN 现在支持闪存虚拟化。每个情景都可以根据可用的总闪存拥有专用存储空间和共享存储位置： • 专用存储 - 仅存储与该用户关联且特定于您希望该用户具有的内容的文件。 • 共享存储 - 将文件上传到此空间，并且将其启用后，可供任何用户情景进行读/写访问。 引入了以下命令：**limit-resource storage**、**storage-url**
在多情景设备中支持AnyConnect客户端客户端配置文件	9.6(2)	在多情景设备中支持AnyConnect 客户端 客户端配置文件要使用 ASDM 添加新配置文件，您必须要有 AnyConnect 客户端 版本 4.2.00748 或 4.3.03013 及更高版本。
多情景模式下 AnyConnect 客户端连接的有状态故障切换	9.6(2)	现在，多情景模式下 AnyConnect 客户端 连接支持有状态故障切换 未修改任何命令。
多情景模式下支持远程访问 VPN 动态访问策略 (DAP)	9.6(2)	现在，可以在多情景模式下按情景配置 DAP。 未修改任何命令。

功能名称	平台版本	功能信息
多情景模式下支持远程访问 VPN CoA（授权更改）	9.6(2)	现在，可以在多情景模式下按情景配置 CoA。 未修改任何命令。
多情景模式下支持远程访问 VPN 本地化	9.6(2)	支持全局本地化。只有一组跨不同情景共享的本地化文件。 未修改任何命令。
支持多情景模式下的 IKEv2 远程接入 VPN	9.9(2)	您可以为 IKEv2 配置多情景模式的远程接入 VPN。
可配置管理会话限制	9.12(1)	现在，您可以配置汇聚管理会话数、每用户管理会话数和每协议管理会话数的最大值。以前，您只能配置汇聚会话数。此功能不会影响控制台会话。需要注意的是，在多情景模式下，如果最大 HTTPS 会话数固定为 5，则无法配置会话数。此外，系统配置中也不再接受 **quota management-session** 命令，您只能在情景配置中进行此设置。现在，最大汇聚会话数为 15。如果您已将其配置为 0（无限制）或大于 16 的值，在升级设备时，此值会自动更改为 15。 新增/修改的命令： **quota management-session**、**show quota management-session**
HTTPS 资源管理	9.12(1)	现在，您可以在资源类中设置非 ASDM HTTPS 会话的最大数量。默认情况下，限制设置为每个情景最多 6 个。在所有情景中最多可使用 100 个 HTTPS 会话。 新增/修改的命令：limit-resource http 无 ASDM 支持。
Firepower 1140 最大情景数从 5 增加到 10	9.16（1）	Firepower 1140 现在最多支持 10 个情景。

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。