用于 AAA 的 RSA SecurID 服务器

以下主题介绍如何配置 AAA 中使用的 RSA SecurID 服务器。RSA SecureID 服务器也称为 SDI 服务器，因为 SDI 是用于与其通信的协议。您可以使用 RSA SecurID 服务器对管理连接，网络访问和 VPN 用户访问进行身份验证。

关于 RSA SecurID 服务器

您可以直接使用 RSA SecurID 服务器进行身份验证，也可以间接使用 RSA SecurID 服务器作为身份验证的第二因素。在后一种情况下，您需要在 SecurID 服务器和 RADIUS 服务器之间配置与 SecurID 服务器的关系，并将 ASA 配置为使用 RADIUS 服务器。

但是，如果要直接针对 SecurID 服务器进行身份验证，则需要为 SDI 协议（用于与这些服务器通信的协议）创建 AAA 服务器组。

使用 SDI 时，在创建 AAA 服务器组时只需指定主 SecurID 服务器。ASA 将在首次连接到服务器时检索 sdiconf.rec 文件，该文件列出所有 SecurID 服务器副本。然后，如果主服务器不响应，ASA 可以使用这些副本进行身份验证。

此外，您必须在 RSA 身份验证管理器中将 ASA 注册为身份验证代理。注册 ASA 之前，身份验证尝试将失败。

用于 AAA 的 RSA SecurID 服务器指南

- 在单模式下可以有最多 200 个服务器组，在多模式下每个情景可以有 8 个服务器组。
- 在单模式下每个组可以有最多 16 个服务器，在多模式下每个组可以有 8 个服务器。当用户登录时，从您在配置中指定的第一个服务器开始，一次访问一个服务器，直到服务器响应为止。

配置用于 AAA 的 RSA SecurID 服务器

以下主题介绍如何配置RSA SecurID服务器组。然后，您可以在配置管理访问或VPN时使用这些组。

配置 RSA SecurID AAA 服务器组

如果要使用与RSA SecurID服务器的直接通信进行身份验证，必须首先至少创建一个SDI服务器组，并向每个组添加一个或多个服务器。如果在与 RADIUS 服务器的代理关系中使用的是 SecurID 服务器，则无需在 ASA 上配置 SDI AAA 服务器组。

过程

步骤 1 创建 SDI AAA 服务器组并进入 aaa-server-group 配置模式。

aaa-server *server_group_name* **protocol sdi**

示例：

```
ciscoasa(config)# aaa-server watchdog protocol sdi
```

步骤 2 （可选。）指定在尝试下一服务器前，会向组中带有 AAA 服务器的失败的 AAA 事务最大数量发送的请求的最大数量。

max-failed-attempts 编号

示例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 参数的范围可介于 1 到 5 之间。默认值为 3。

如果您使用本地数据库（仅用于管理访问）配置了回退方法，并且组中的所有服务器都无法响应，或者其响应无效，则会将该组视为无响应，并将尝试回退方法。该服务器组会在10分钟（默认值）内保持标记为无响应，以确保该时段内其他AAA请求不会尝试联系该服务器组，而是立即使用回退方法。要更改默认的无响应期间，请参阅下一步中的 **reactivation-mode** 命令。

如果没有回退方法，则 ASA 将继续重试该组中的服务器。

步骤 3 （可选。）指定用于重新激活组中的故障服务器的方法（重新激活策略）。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

示例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

depletion 关键字仅在组中的所有服务器都处于非活动状态后才会重新激活故障服务器。该模式为默认模式。

deadtime *minutes* 关键字参数对用于指定从禁用组中的最后一个服务器到随后重新启用所有服务器所经过的时间，范围介于 0 到 1440（以分钟为单位）之间。默认值为 10 分钟。

timed 关键字可在 30 秒停机时间后重新激活故障服务器。

将 RSA SecurID 服务器添加到 SDI 服务器组

在使用 SDI 服务器组之前，必须至少向该组添加一个 RSA SecurID 服务器。

SDI 服务器组中的服务器使用身份验证和服务器管理协议 (ACE) 与 ASA 通信。

过程

步骤 1 将 RSA SecurID 服务器添加到 SDI 服务器组。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

示例：

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

如果不指定接口，则 ASA 默认使用**内部**接口。

您可以使用 IPv4 或 IPv6 地址。

步骤 2 指定与服务器的连接尝试超时值。

timeout 秒

指定服务器的超时间隔（1-300 秒）；默认值为 10 秒。对于每个 AAA 事务，ASA 将重试连接尝试（基于 **retry-interval** 命令中定义的间隔），直到达到超时。如果连续失败事务数量达到 AAA 服务器组中 **max-failed-attempts** 命令上指定的上限，则将会停用 AAA 服务器，并且ASA 将开始向另一台 AAA 服务器（如果已配置）发送请求。

示例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

步骤 3 指定重试间隔，即系统在重试连接请求之前等待的时间。

retry-interval 秒

您可以指定 1-10 秒。默认值为 10 秒。

示例：

```
ciscoasa(config-aaa-server-host)# retry-interval 6
```

步骤 4 如果服务器端口与默认 RSA SecurID 端口 (TCP / 5500) 不同，请指定服务器端口。ASA 在此端口上联系 RSA SecurID 服务器。

server-port *port_number*

示例：

```
ciscoasa(config-aaa-server-host)# server-port 5555
```

导入 SDI 节点密钥文件

您可以手动导入 RSA 身份验证管理器 (SecurID) 服务器生成的 node-secret 文件。

过程

步骤 1 从 RSA 身份验证管理器服务器导出节点密钥文件。有关详细信息，请参阅 RSA 身份验证管理器文档。

步骤 2 将节点加密文件的解压版本放在可从 ASA 访问的服务器上，或将其复制到 ASA 本身。

服务器必须支持以下传输协议之一：FTP、HTTP、HTTPS、SCP、SMB、TFTP。

步骤 3 导入节点密钥文件。

aaa sdi import-node-secret *filepath rsa_server_address password*

其中：

- *filepath* 是从 RSA 身份验证管理器导出的未压缩节点密钥文件的完整路径。本地系统上的文件可以编址为 disk0:、disk1: 或 flash:。对于远程服务器上的文件，请使用标准 URL 表示法，例如 ftp://。
- *rsa_server_address* 是节点密钥所属的 RSA 身份验证管理器服务器的 IP 地址或完全限定主机名。
- 密码是导出文件时用于保护文件的密码。

示例：

```
ciscoasa# aaa sdi import-node-secret nodesecret.rec rsaam.example.com mysecret
nodesecret.rec imported successfully
ciscoasa#
```

监控用于 AAA 的 RSA SecurID 服务器

您可以使用以下命令监控和清除 RSA SecurID 相关信息。

- **show aaa-server**

  显示 AAA 服务器统计信息。使用 **clear aaa-server statistics** 命令清除服务器统计信息。

- **show running-config aaa-server**

  显示为系统配置的 AAA 服务器。使用 **clear configure aaa-server** 命令删除 AAA 服务器配置。

- **show aaa sdi node-secrets**

  显示哪些 RSA SecurID 服务器具有导入的节点密钥文件。使用 **clear aaa sdi node-secret** 命令删除节点密钥文件。

用于 AAA 的 RSA SecurID 服务器的历史记录

功能名称	平台版本	说明
SecurID 服务器	7.2(1)	支持 AAA 的 SecurID 服务器进行管理身份验证。以前版本的 VPN 身份验证版本支持 SecurID。
用于AAA 的 IPv6 地址	9.7(1)	现在可以将 IPv4 或 IPv6 地址用于 AAA 服务器。
每个组的 AAA 服务器组和服务器的数量上限都增加了。	9.13(1)	您可以配置更多 AAA 服务器组。在单情景模式下，您可以配置 200 AAA 服务器组（前一个限制为100）。在多情景模式下，您可以配置 8（前一个限制为4个）。 此外，在多情景模式下，您可以每组配置 8 个服务器（每个组的前一个限制为 4 个服务器）。单情景模式的每组限制 16，保持不变。 修改了以下命令以接受这些新限制：**aaa-server**、**aaa-server host**。
从用于 SDI AAA 服务器组的 RSA 身份验证管理器手动导入节点密钥文件。	9.15(1)	您可以导入从RSA身份验证管理器导出的节点密钥文件，以用于 SDI AAA 服务器组。 添加了以下命令：**aaa sdi import-node-secret**、**clear aaa sdi node-secret**、**show aaa sdi node-secrets**。

用于 AAA 的 RSA SecurID 服务器的历史记录