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 服务器准则

- 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 依次选择 **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups**。

步骤 2 在 **AAA Server Groups** 区域中，点击 **Add**。

系统将显示 **Add AAA Server Group** 对话框。

步骤 3 在 **Server Group** 字段中输入组的名称。

步骤 4 从 **Protocol** 下拉列表中选择 **SDI** 服务器类型：

步骤 5 点击 **Reactivation Mode** 字段中的 **Depletion** 或 **Timed**。

在 Depletion 模式下，只有在组中所有服务器都处于非活动状态后，故障服务器才重新激活。在 depletion 模式下，当停用服务器时，它将保持非活动状态，直到组中的所有其他服务器都处于非活动状态。如果发生这种情况，组内所有服务器都会被重新激活。这种方法可最大限度减少因出现故障的服务器而发生的连接延迟。

在 Timed 模式下，故障服务器会在 30 秒停机时间后被重新激活。

步骤 6 如果选择 Depletion 重新激活模式，请在 **Dead Time** 字段中输入时间间隔。

Dead Time 是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，以分钟为单位。仅当配置回退到本地数据库时，失效时间时间才适用；身份验证将在本地尝试，直到失效时间结束。

步骤 7 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。

此选项设置在宣布无响应服务器为非活动状态之前允许的失败的 AAA 事务。

步骤 8 点击**确定 (OK)**。

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 依次选择 **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups**。

步骤 2 选择要向其添加服务器的服务器组。

步骤 3 在 **Servers in the Selected Group** 区域点击 **Add**。

系统将为该服务器组显示 **Add AAA Server Group** 对话框。

步骤 4 选择身份验证服务器所在**接口的名称**。

步骤 5 为正添加到组中的服务器输入名称或 IP 地址。

步骤 6 指定与服务器的连接尝试超时值。

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（基于重试间隔），直到达到超时。如果连续失败事务的数量达到 AAA 服务器组中指定的 maximum-failed-attempts 上限，则将会停用 AAA 服务器，并且 ASA 开始向另一台 AAA 服务器（如果已配置）发送请求。

步骤 7 选择重试间隔，即系统在重试连接请求之前等待的时间。您可以选择 1 到 10 秒。默认值为 10 秒。

步骤 8 指定服务器端口。服务器端口是默认端口号 5500 或 ASA，或与 RSA SecurID 服务器进行通信所用的 TCP 端口号。

步骤 9 点击**确定 (OK)**。

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 依次选择**配置** > **设备管理** > **用户/AAA** > **AAA SDI**。

步骤 3 点击**上传 (Upload)**，选择从 RSA 身份验证管理器导出的解压缩节点密钥文件，并将其上传到系统。

步骤 4 在**导入 SDI 的节点加密密钥**下，输入以下信息：

- **服务器 IP** - 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** - 导出文件时用于保护文件的密码。
- **文件名** - 点击**浏览 (Browse)** 并选择已上传的解压缩节点密钥文件。

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。在**工具** > **命令行接口**窗口中输入命令。

- **监控** > **属性** > **AAA 服务器**

  此窗口显示 AAA 服务器统计信息。

- **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 AAA 屏幕以接受这些新的限制。
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。 添加了以下菜单项：**配置** > **设备管理** > **用户/AAA** > **AAA SDI**。

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。