AAA 和本地数据库

本章介绍身份验证、授权和记帐（AAA，也称为“3A”）。AAA 是一组服务，用于控制对计算机资源的访问、执行策略、评估使用情况并提供对服务进行计费所需的信息。这些过程对于高效进行网络管理和安全性而言至关重要。

本章还介绍如何为 AAA 功能配置本地数据库。对于外部 AAA 服务器，请参阅与您的服务器类型对应的章节。

关于 AAA 和本地数据库

本节介绍 AAA 和本地数据库。

身份验证

身份验证提供了一种识别用户的方法，这种方法通常先请用户输入有效用户名和有效密码，然后再授予访问权限。AAA 服务器将用户的身份验证凭证与数据库中存储的其他用户凭证进行比较。如果凭证匹配，则允许用户访问网络。如果凭证不匹配，则身份验证失败，并拒绝网络访问。

您可以将 ASA 配置为对以下项进行身份验证：

- 与 ASA 的所有管理连接，包括以下会话：
  - Telnet
  - SSH
  - 串行控制台
  - 使用 HTTPS 的 ASDM
  - VPN 管理访问

- **enable** 命令
- 网络接入
- VPN 接入

授权

授权是执行策略的过程：确定允许用户访问哪些类型的活动、资源或服务。对用户进行身份验证后，可能会授权该用户执行各种类型的访问或活动。

您可以配置 ASA 以便对下列各项进行授权：

- 管理命令
- 网络接入
- VPN 接入

会计

记账用于测量用户在访问期间使用的资源量，这可以包括系统时间长度或者用户在会话期间发送或接收的数据量。记账是通过记录会话统计信息和使用量信息来执行的，这些信息用于进行授权控制、计费、趋势分析、资源利用率和容量规划活动。

身份验证、授权和记账之间的交互

您可以单独使用身份验证功能，也可以将其与授权和记账功能配合使用。授权始终要求先对用户进行身份验证。您可以单独使用记账功能，也可以将其与身份验证和授权功能配合使用。

AAA 服务器和服务器组

AAA 服务器是用于进行访问控制的网络服务器。身份验证用于识别用户。授权用于实施策略，这些策略确定经过身份验证的用户能够访问哪些资源和服务。记账对时间和数据资源进行追踪，这些资源用于计费和分析。

如果要使用外部 AAA 服务器，必须先为外部服务器使用的协议创建 AAA 服务器组，然后将该服务器添加到该组。您可以为每个协议创建多个组，并为要使用的所有协议创建单独的组。每个服务器组都专门用于一种类型的服务器或服务。

有关如何创建组的详细信息，请参阅以下主题：

- 配置 RADIUS 服务器组
- 配置 TACACS+ 服务器组
- 配置 LDAP 服务器组
- 配置 RSA SecurID AAA 服务器组

有关使用 HTTP 表单的详细信息，请参阅 VPN 配置指南。

注释 从 ASA 9.22.1 起，不支持 Kerberos 协议。您不能再将 Kerberos 用于 AAA 服务。建议您使用下表中列出的其他受支持服务器。

下表总结了支持的服务器类型及其用途，包括本地数据库。

表 *1: AAA* 服务器支持的服务

服务器类型和服务	身份验证	授权	记账
本地数据库			
管理员	是	支持	否
VPN 用户	支持	否	否
防火墙会话（AAA 规则）	是	支持	否
RADIUS			
管理员	是	支持	支持
VPN 用户	是	支持	支持
防火墙会话（AAA 规则）	是	支持	支持
TACACS+			
管理员	是	支持	支持
VPN 用户	支持	否	是
防火墙会话（AAA 规则）	是	支持	支持
LDAP			
管理员	支持	否	否
VPN 用户	是	支持	否
防火墙会话（AAA 规则）	支持	否	否
SDI (RSA SecurID)			
管理员	支持	否	否
VPN 用户	支持	否	否
防火墙会话（AAA 规则）	支持	否	否

服务器类型和服务	身份验证	授权	记账
HTTP 形式			
管理员	否	否	否
VPN 用户	支持	否	否
防火墙会话（AAA 规则）	否	否	否

注意

- RADIUS - 管理员的记帐不包括命令记帐。
- RADIUS - 防火墙会话的授权仅支持用户特定的访问列表，这些列表在 RADIUS 身份验证响应中接收或指定。
- TACACS+ - 管理员会计包括命令会计。
- HTTP 形式 - 仅用于无客户端 SSL VPN 用户会话的身份验证和 SSO 操作。

关于本地数据库

ASA 维护了一个本地数据库，您可以使用用户配置文件填充该数据库。您可以使用本地数据库代替 AAA 服务器来提供用户身份验证、授权和记帐。

您可以使用本地数据库实现下列功能：

- ASDM 按用户访问
- 控制台身份验证
- Telnet 和 SSH 身份验证
- **enable** 命令身份验证

  此设置仅用于 CLI 访问，并不影响思科 ASDM 登录。
- 命令授权

  如果您使用本地数据库打开命令授权，则ASA将参考用户权限级别来确定可用的命令。否则，通常不使用权限级别。默认情况下，所有命令的权限级别均为 0 或 15。
- 网络访问身份验证
- VPN 客户端身份验证

对于多情景模式，您可以在系统执行空间中配置用户名，以便在 CLI 中使用 **login** 命令提供个人登录；但是，您不能在系统执行空间中配置任何使用本地数据库的 AAA 规则。

注释 您不能使用本地数据库进行网络访问授权。

回退支持

本地数据库可以用作多项功能的回退方法。此行为旨在帮助您避免意外被锁定而无法登录 ASA。

用户登录时，将从配置中指定的第一个服务器开始逐个访问组中的服务器，直到有服务器作出响应为止。如果组中的所有服务器都不可用，并且您已将本地数据库配置为回退方法（仅用于管理身份验证和授权），则 ASA 将尝试使用本地数据库。如果未配置任何回退方法，则 ASA 将继续尝试使用 AAA 服务器。

对于需要回退支持的用户，我们建议您确保本地数据库中的用户名和密码与AAA服务器上的用户名和密码匹配。这种做法将提供透明的回退支持。由于用户无法确定是AAA服务器还是本地数据库正在提供服务，因此，如果AAA服务器上使用的用户名和密码与本地数据库中的用户名和密码不同，用户将无法确定应提供哪个用户名和密码。

本地数据库支持下列回退功能：

- 控制台和启用密码身份验证 - 如果组中的服务器全部不可用，则 ASA 将使用本地数据库对管理访问进行身份验证，这还可以包括启用密码身份验证。
- 命令授权 - 如果组中的 TACACS+ 服务器全部不可用，则使用本地数据库根据权限级别进行命令授权。
- VPN 身份验证和授权 - 支持 VPN 身份验证和授权，以便在通常支持这些 VPN 服务的 AAA 服务器不可用时，启用对 ASA 的远程访问。如果管理员的 VPN 客户端指定了配置为回退到本地数据库的隧道组，只要本地数据库配置了必要的属性，即使AAA服务器组不可用，也可以建立 VPN 隧道。

组中存在多个服务器时的回退方式

如果在服务器组中配置了多个服务器，并且对于该服务器组允许回退到本地数据库，则该组中没有任何服务器对来自ASA的身份验证请求作出响应时，将会进行回退。为了说明这一点，请考虑以下场景：

您配置了一个 LDAP 服务器组，其中依次包含两个 Active Directory 服务器，即服务器 1 和服务器 2。当远程用户登录时，ASA 将尝试向服务器 1 进行身份验证。

如果服务器 1 作出了身份验证失败响应（例如找不到用户），则 ASA 不会尝试向服务器 2 进行身份验证。

如果服务器 1 在超时期限内未作出响应（或者尝试进行身份验证的次数超过配置的最大值），则 ASA 尝试服务器 2。

如果组中的两个服务器均未作出响应，并且 ASA 配置为回退到本地数据库，则 ASA 将尝试向本地数据库进行身份验证。

本地数据库准则

在使用本地数据库进行身份验证或授权时，请确保避免被锁定而无法登录 ASA。

在本地数据库中添加用户帐户

要向本地数据库添加用户，请执行以下步骤：

过程

步骤 1 创建用户帐户。

username *username* [**password** *password*] [**privilege** *priv_level*]

示例：

```
ciscoasa(config)# username exampleuser1 password madmaxfuryroadrules privilege 1
```

username *username* 关键字是长度为 3 到 64 个字符的字符串，可以任意组合使用 ASCII 可打印字符（字符代码 32-126），但是空格和问号除外。 **password** 密码 关键词是一个区分大小写的密码，长度为 8 到 127 个字符，可以任意组合使用 ASCII 可打印字符（字符代码 32-126），但是以下除外。

- 无空格
- 没有问号
- 不能使用三个或三个以上连续或重复的 ASCII 字符。例如，以下密码将被拒绝：
  - **abc**user1
  - 用户**543**
  - 用户**aaaa**
  - 用户2**666**

例如，如果您使用 SSH 公钥身份验证，则您可能想创建用户名而不创建密码。**privilege***priv_level* 关键字用于设置范围为 0 到 15 的权限级别。默认值为 2。此权限级别与命令授权一起使用。

注意
如果未使用命令授权（**AAA 授权控制台 LOCAL** 命令），则默认级别 2 允许对特权 EXEC 模式进行管理访问。如果要限制对特权 EXEC 模式的访问，请将权限级别设置为 0 或 1，或者使用 **service-type** 命令。

上面的语法中并未显示这些不常用的选项：**nopassword** 关键字用于创建可以接受任何密码的用户帐户；此选项不安全，因此不建议使用。

encrypted 关键字（在 9.6 和早期版本中，用于 32 个字符或以下的密码）或 **pbkdf2** 关键字（在 9.6 和更高版本中，用于长度超过 32 个字符的密码；在 9.7 和更高版本中，用于所有长度的密码）表示密码已被加密（使用基于 MD5 的散列或 PBKDF2（基于密码的密钥派生功能 2）散列）。请注意，现有密码将继续使用基于 MD5 的散列方法，除非您输入新的密码。当您在 **username** 命令中定义密码后，出于安全目的，ASA 会在将其保存到配置时进行加密。输入 **show running-config** 命令后，**username**命令不会显示实际密码；它将显示加密的密码，后跟 **encrypted** 或 **pbkdf2** 关键字。例如，如果输入密码“test”，则 **show running-config** 命令输出内容将与以下内容类似：

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

只有在您剪切和粘贴配置文件，以便 在另一 ASA 中使用，而且您使用相同的密码时， 才会真的在 CLI 上输入 **encrypted** 或 **pbkdf2** 关键字。

步骤 2 （可选）配置用户名属性。

username 用户名 **attributes**

示例：

```
ciscoasa(config)# username exampleuser1 attributes
```

username 参数是您在第一步中创建的用户名。

默认情况下，使用此命令添加的 VPN 用户没有属性或组策略关联。您必须使用 **username attributes** 命令明确配置所有值。有关更多信息，请参阅《VPN 配置指南》。

步骤 3 （可选）如果使用 **aaa authorization exec** 命令配置了管理授权，请配置用户级别。

service-type {**admin** | **nas-prompt** | **remote-access**}

示例：

```
ciscoasa(config-username)# service-type admin
```

admin 关键字允许完全访问 **aaa authentication console LOCAL** 命令指定的所有服务。**admin** 关键字是默认值。

在配置 **aaa authentication** {**telnet** | **ssh** | **serial**} **console** 命令时， **nas-prompt** 关键字将允许访问 CLI，但如果配置 **aaa authentication http console** 命令，则拒绝 ASDM 配置访问。允许 ASDM 监控访问。如果使用 **aaa authentication enable console** 命令启用了身份验证，则用户无法使用 **enable** 命令（或 **login** 命令）访问特权 EXEC 模式。

remote-access 关键字会拒绝管理访问。您无法使用 **aaa authentication console** 命令指定的任何服务（不包括 **serial** 关键字；允许进行串行访问）。

步骤 4 （可选） 有关按每个用户对与 ASA 的 SSH 连接进行公钥身份验证的信息，请参阅为公共密钥访问配置 SSH。

步骤 5 （可选） 如果要使用此用户名进行 VPN 身份验证，则可以为用户配置许多 VPN 属性。有关更多信息，请参阅《VPN 配置指南》。

示例

以下示例向管理员用户帐户分配权限级别 15：

```
ciscoasa(config)# username admin password farscape1 privilege 15
```

以下示例启用管理授权，创建具有密码的用户帐户，进入用户名配置模式，并指定**service-type**为 **nas-prompt**：

```
ciscoasa(config)# aaa authorization exec authentication-server
ciscoasa(config)# username user1 password gOrgeOus
ciscoasa(config)# username user1 attributes
ciscoasa(config-username)# service-type nas-prompt
```

监控本地数据库

请参阅以下命令来监控本地数据库。

- **show aaa-server**

  此命令可显示已配置的数据库统计信息。使用 **clear aaa-server statistics** 命令可清除 AAA 服务器统计信息。

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

  此命令可显示 AAA 服务器运行配置。使用 **clear configure aaa-server** 命令可清除 AAA 服务器配置。

本地数据库的历史记录

表 *2:* 本地数据库的历史记录

功能名称	平台版本	说明
AAA 的本地数据库配置	7.0(1)	介绍如何配置本地数据库以供 AAA 使用。 引入了以下命令： **username**、**aaa authorization exec authentication-server**、**aaa authentication console LOCAL**、**aaa authorization exec LOCAL**、**service-type**、**aaa authentication** {**telnet** | **ssh** | **serial**} **console LOCAL**、**aaa authentication http console LOCAL**、**aaa authentication enable console LOCAL**、**show running-config aaa-server**、**show aaa-server**、**clear configure aaa-server**、**clear aaa-server statistics**。

功能名称	平台版本	说明
对 SSH 公钥身份验证的支持	9.1(2)	对于与 ASA 的 SSH 连接，您现在可以基于每个用户启用公钥身份验证。您可以指定公钥文件 (PKF) 格式的密钥或 Base64 密钥。PKF 密钥的长度可达 4096 位。对于由于过长而导致 ASA 不支持使用 Base64 格式（限长 2048 位）的密钥，请使用 PKF 格式。 引入了以下命令：**ssh authentication**。 在 *8.4(4.1)* 中也可用；*PKF* 密钥格式支持仅在 *9.1(2)* 中提供。
本地 **username** 和 **enable** 密码支持更长的密码（最多 127 个字符）	9.6(1)	您现在可以创建最多 127 个字符的本地 **username** 和 **enable** 密码（过去的限制为 32 个字符）。在创建长度超过 32 个字符的密码时，它将使用 PBKDF2（基于密码的密钥派生功能 2）散列存储在配置中。较短的密码将继续使用基于 MD5 的散列处理方法。 修改了以下命令：**enable**、**username**
SSH 公钥身份验证改进	9.6(2)	在更早的版本中，您在启用 SSH 公钥身份验证 (**ssh authentication**) 时，可以不必启用基于本地用户数据库的 AAA SSH 身份验证 (**aaa authentication ssh console LOCAL**)。该配置现在已修复，您必须明确启用 AAA SSH 身份验证。要禁止用户使用密码而不是私钥，现在您可以创建未定义任何密码的用户名。 修改了以下命令：**ssh authentication**、**username**。
对所有本地 **username** 和 **enable** 密码使用 PBKDF2 散列算法	9.7(1)	配置中存储的所有长度的本地 **username** 和 **enable** 密码都将使用 PBKDF2 (基于密码的密钥派生函数 2) 散列算法。以前，32 个字符或以下的密码使用基于 MD5 的哈希处理方法。已经存在的密码仍将继续使用基于 MD5 的哈希值，但您输入的新密码除外。如需下载准则，请参阅一般操作配置指南中的“软件和配置”一章。 修改了以下命令：**enable**、**username**

功能名称	平台版本	说明
对使用 SSH 公钥身份验证的用户和具有密码的用户分别进行单独的身份验证	9.6(3)/9.8(1)	在 9.6(2) 以前的版本中，您在启用 SSH 公钥身份验证 (**ssh authentication**) 时，可以不必明确启用基于本地用户数据库的 AAA SSH 身份验证 (**aaa authentication ssh console LOCAL**)。在 9.6(2) 中，ASA 要求明确启用 AAA SSH 身份验证。在此版本中，您不再需要明确启用 AAA SSH 身份验证；当您为用户配置 **ssh authentication** 命令时，默认情况下会为使用此类型身份验证的用户启用本地身份验证。此外，在明确配置 AAA SSH 身份验证时，此配置将仅适用于具有密码的用户名，并且可以使用任何 AAA 服务器类型（例如 **aaa authentication ssh console radius_1**）。例如，某些用户可以使用公钥身份验证（使用本地数据库），而其他用户则可配合使用密码和 RADIUS。 未修改任何命令。
更强的本地用户和启用密码要求	9.17(1)	对于本地用户和启用密码，添加了以下密码要求： • 密码长度 - 至少为 8 个字符。以前，最小值为 3 个字符。 • 重复和连续字符 - 不允许使用三个或三个以上连续的连续或重复 ASCII 字符。例如，以下密码将被拒绝： • **abc**user1 • 用户**543** • 用户**aaaa** • 用户2**666** 新增/修改的命令： **enable password**、**username**
本地用户锁定更改	9.17(1)	ASA 可以在登录尝试失败达到可配置次数之后锁定账户。此功能不适用于权限级别为 15 的用户。此外，用户将被无限期锁定，直到管理员解锁其账户。现在，用户将在 10 分钟后解锁，除非管理员在此之前使用 **clear aaa local user lockout** 命令。权限级别为 15 的用户现在也受锁定设置的影响。 新增/修改的命令：**aaa local authentication attempts max-fail** 、**show aaa local user**

功能名称	平台版本	说明
SSH 和 Telnet 密码更改提示	9.17(1)	本地用户首次使用 SSH 或 Telnet 登录 ASA 时，系统会提示他们更改密码。在管理员更改密码后，系统还会提示他们进行首次登录。但是，如果 ASA 重新加载，则系统不会提示用户，即使是首次登录也是如此。 新增/修改的命令：**show aaa local user**

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。