



## 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，第 1 页](#)
- [本地数据库准则，第 6 页](#)
- [在本地数据库中添加用户帐户，第 6 页](#)
- [测试本地数据库身份验证和授权，第 7 页](#)
- [监控本地数据库，第 8 页](#)
- [本地数据库历史记录，第 8 页](#)

## 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 Kerberos AAA 服务器组](#)
- [配置 RSA SecurID AAA 服务器组](#)

有关使用 Kerberos 约束委派和 HTTP 表单的详细信息，请参阅 VPN 配置指南。

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
<b>本地数据库</b>			
管理员	兼容	兼容	否
VPN 用户	是	不兼容	不兼容
防火墙会话 (AAA 规则)	兼容	兼容	否
<b>RADIUS</b>			
管理员	兼容	兼容	兼容
VPN 用户	兼容	兼容	兼容
防火墙会话 (AAA 规则)	兼容	兼容	兼容
<b>TACACS+</b>			
管理员	兼容	兼容	兼容
VPN 用户	是	不兼容	是
防火墙会话 (AAA 规则)	兼容	兼容	兼容
<b>LDAP</b>			
管理员	是	不兼容	不兼容
VPN 用户	兼容	兼容	否
防火墙会话 (AAA 规则)	是	不兼容	不兼容
<b>Kerberos</b>			
管理员	是	不兼容	不兼容
VPN 用户	是	不兼容	不兼容
防火墙会话 (AAA 规则)	是	不兼容	不兼容

服务器类型和服务	身份验证	授权	记账
<b>SDI (RSA SecurID)</b>			
管理员	是	不兼容	不兼容
VPN 用户	是	不兼容	不兼容
防火墙会话 (AAA 规则)	是	不兼容	不兼容
<b>HTTP 形式</b>			
管理员	不兼容	不兼容	不兼容
VPN 用户	是	不兼容	不兼容
防火墙会话 (AAA 规则)	不兼容	不兼容	不兼容
<b>注意</b> <ul style="list-style-type: none"> <li>• RADIUS - 管理员的记帐不包括命令记帐。</li> <li>• 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。</li> <li>• TACACS+ - 管理员会计包括命令会计。</li> <li>• 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。</li> </ul>			

## 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。ASDM 允许您启用三个预定义的权限级别，其中命令分配到级别 15（管理员）、级别 5（只读）和级别 3（仅监控）。如果您使用预定义的级别，请将用户分配到这三个权限级别的其中一个。

- 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** 依次选择配置 > 设备管理 > 用户/AAA > 用户帐户，然后点击添加。

系统将显示 **Add User Account-Identity** 对话框。

**步骤 2** 输入长度为 4 到 64 个字符的用户名。

**步骤 3** （可选）输入长度为 8 到 127 个字符的密码。

密码区分大小写。它可以任意组合使用 ASCII 可打印字符（字符代码 32-126），但是下列除外。

- 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：
  - **abcuser1**
  - 用户**543**
  - 用户**aaaa**
  - 用户**2666**

此字段仅显示星号。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。

**注释** 要从 **User Accounts** 窗格中配置启用密码，请更改 **enable\_15** 用户的密码。**enable\_15** 用户始终显示在 **User Accounts** 窗格中，它代表默认用户名。这种配置启用密码的方法是在 **ASDM** 中进行系统配置的唯一可用方法。如果您在 **CLI** 中配置了其他启用级别的密码（例如，启用密码 10），则那些用户将列出为 **enable\_10**，依次类推。

**步骤 4** 请重新输入密码。

为安全起见，密码字段仅显示星号。

**步骤 5** 如果使用 MSCHAP 进行身份验证，请选中 **User authenticated using MSCHAP** 复选框。

**步骤 6** 在 **Access Restriction** 区域中设置用户的管理访问级别。您必须先通过点击 **配置 > 设备管理 > 用户/AAA > AAA 访问 > 授权选项卡** 上的执行 **exec** 外壳访问授权选项，启用管理授权。

选择以下其中一个选项：

- **Full Access (ASDM, Telnet, SSH and console)** - 如果配置了使用本地数据库对管理访问进行身份验证，则此选项使用户能够使用 ASDM、SSH、Telnet 和控制台端口。如果还启用了身份验证，则用户可以访问全局配置模式。
- **Privilege Level** - 为 ASDM 和本地命令授权设置权限级别。范围为 0（最低）到 15（最高）。要授予无限制的管理员访问权限，请指定值 15。预定义的 ASDM 角色将 15 用于表示管理员访问权限，5 用于表示只读访问权限，3 用于表示仅监控访问权限（用户仅限于访问 Home 窗格和 Monitoring 窗格）。
- **CLI login prompt for SSH, Telnet and console (no ASDM access)** - 如果配置了使用本地数据库对管理访问进行身份验证，则此选项使用户能够使用 SSH、Telnet 和控制台端口。如果配置了 HTTP 身份验证，则用户无法使用 ASDM 进行配置。允许进行 ASDM 监控。如果还配置了启用身份验证，则用户无法访问全局配置模式。
- **No ASDM、SSH、Telnet 或 console access** - 如果配置了使用本地数据库对管理访问进行身份验证，则此选项禁止用户访问任何配置了身份验证的管理访问方法（不包括 Serial 选项；允许进行串行访问）。

**步骤 7**（可选）要按每个用户对与 ASA 的 SSH 连接启用公钥身份验证，请参阅[配置用于 ASDM 的 HTTPS 访问、其他客户端](#)。

**步骤 8** 点击 **VPN Policy**，以便为此用户配置 VPN 策略属性。请参阅《VPN 配置指南》。

**步骤 9** 点击 **Apply**。

用户将添加到本地数据库中，并且更改将保存到运行配置。

**提示** 您可以在 **配置 > 设备管理 > 用户/AAA > 用户帐户** 窗格的每一列中搜索特定文本。请在 **Find** 框中输入要查找的特定文本，然后点击 **Up** 或 **Down** 箭头。在文本搜索中，还可以使用星号（“\*”）和问号（“?”）作为通配符。

## 测试本地数据库身份验证和授权

要确定 ASA 是否能够联系本地数据库并对用户进行身份验证或授权，请执行下列步骤：

## 过程

**步骤 1** 在配置 > 设备管理 > 用户/AAA > AAA 服务器组 > AAA 服务器组表中，点击服务器所在的服务器组。

**步骤 2** 在 **Servers in the Selected Group** 表中点击要测试的服务器。

**步骤 3** 点击 **Test**。

系统将针对所选服务器显示 **Test AAA Server** 对话框。

**步骤 4** 点击要执行的测试的类型 - **Authentication** 或 **Authorization**。

**步骤 5** 输入用户名。

**步骤 6** 如果要测试身份验证，请输入该用户名的密码。

**步骤 7** 点击 **OK**。

ASA 将向服务器发送身份验证或授权测试消息。如果测试失败，ASDM 将显示错误消息。

## 监控本地数据库

请参阅以下命令来监控本地数据库。

- **Monitoring > Properties > AAA Servers**

此窗格显示 AAA 服务器统计信息。

- **Tools > Command Line Interface**

您可以在此窗格中发出各种非交互式命令并查看结果。

## 本地数据库历史记录

表 2: 本地数据库历史记录

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。 引入了以下屏幕： Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Device Management > Users/AAA > User Accounts。



功能名称	平台版本	说明
对 SSH 公钥身份验证的支持	9.1(2)	<p>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。</p> <p>引入了以下菜单项：</p> <p>Configuration &gt; Device Management &gt; Users/AAA &gt; User Accounts &gt; Edit User Account &gt; Public Key Authentication            Configuration &gt; Device Management &gt; Users/AAA &gt; User Accounts &gt; Edit User Account &gt; Public Key Using PKF</p> <p>在 8.4(4.1) 中也可用；PKF 密钥格式支持仅在 9.1(2) 中提供。</p>
本地 <b>username</b> 和 <b>enable</b> 密码支持更长的密码（最多 127 个字符）	9.6(1)	<p>您现在可以创建最多 127 个字符的本地 <b>username</b> 和 <b>enable</b> 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。</p> <p>修改了以下菜单项：</p> <p>配置 &gt; 设备设置 &gt; 设备名称/密码 &gt; 启用密码            配置 &gt; 设备管理 &gt; 用户/AAA &gt; 用户账户 &gt; 添加/编辑用户账户 &gt; 身份</p>
SSH 公钥身份验证改进	9.6(2)	<p>在更早的版本中，您在启用 SSH 公钥身份验证时，可以不必启用基于本地用户数据库的 AAA SSH 身份验证。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。</p> <p>修改了以下菜单项：</p> <p>配置 &gt; 设备管理 &gt; 管理访问 &gt; ASDM/HTTPS/Telnet/SSH            配置 &gt; 设备管理 &gt; 用户/AAA &gt; 用户账户 &gt; 添加/编辑用户账户</p>

功能名称	平台版本	说明
对所有本地 <b>username</b> 和 <b>enable</b> 密码使用 PBKDF2 散列算法	9.7(1)	<p>配置中存储的所有长度的本地 <b>username</b> 和 <b>enable</b> 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。</p> <p>修改了以下菜单项:</p> <p><b>配置 &gt; 设备设置 &gt; 设备名称/密码 &gt; 启用密码</b></p> <p><b>配置 &gt; 设备管理 &gt; 用户/AAA &gt; 用户账户 &gt; 添加/编辑用户账户 &gt; 身份</b></p>
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)	<p>在 9.6(2) 以前的版本中, 您在启用 SSH 公钥身份验证 (<b>ssh authentication</b>) 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 (<b>aaa authentication ssh console LOCAL</b>)。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 <b>ssh authentication</b> 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 <b>aaa authentication ssh console radius_1</b>)。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。</p> <p>未修改任何菜单项。</p>

功能名称	平台版本	说明
更强的本地用户和启用密码要求	9.17(1)	<p>对于本地用户和启用密码，添加了以下密码要求：</p> <ul style="list-style-type: none"> <li>• 密码长度 - 至少为 8 个字符。以前，最小值为 3 个字符。</li> <li>• 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： <ul style="list-style-type: none"> <li>• <b>abcuser1</b></li> <li>• 用户<b>543</b></li> <li>• 用户<b>aaaa</b></li> <li>• 用户<b>2666</b></li> </ul> </li> </ul> <p>新增/修改的屏幕：</p> <ul style="list-style-type: none"> <li>• 配置 &gt; 设备管理 &gt; 用户/AAA &gt; 用户账号</li> <li>• 配置 &gt; 设备设置 &gt; 设备名称/密码</li> </ul>
本地用户锁定更改	9.17(1)	<p>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 <b>clear aaa local user lockout</b> 命令。权限级别为 15 的用户现在也受锁定设置的影响。</p> <p>新增/修改的命令：<b>aaa local authentication attempts max-fail</b>、<b>show aaa local user</b></p>
SSH 和 Telnet 密码更改提示	9.17(1)	<p>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。</p> <p>新增/修改的命令：<b>show aaa local user</b></p>



## 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。