



用于 AAA 的 Kerberos 服务器

以下主题介绍如何配置 AAA 中使用的 Kerberos 服务器。您可以使用 Kerberos 服务器对管理连接、网络访问和 VPN 用户访问进行身份验证。

- [用于 AAA 的 Kerberos 服务器准则](#)，第 1 页
- [配置用于 AAA 的 Kerberos 服务器](#)，第 1 页
- [监控用于 AAA 的 Kerberos 服务器](#)，第 4 页
- [用于 AAA 的 Kerberos 服务器历史记录](#)，第 5 页

用于 AAA 的 Kerberos 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 Kerberos 服务器

以下主题介绍如何配置 Kerberos 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 Kerberos AAA 服务器组

如果要使用 Kerberos 服务器进行身份验证，必须首先创建至少一个 Kerberos 服务器组，并向每个组添加一个或多个服务器。

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 **Kerberos** 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 （可选。）选择 **验证 KDC** 以启用 Kerberos 密钥分发中心 (KDC) 验证。

要完成身份验证，还必须导入从 Kerberos 密钥分发中心 (KDC) 导出的密钥表文件。通过验证 KDC，可以防止攻击者伪装 KDC，从而根据攻击者的 Kerberos 服务器对用户凭证进行身份验证。

有关如何上传 keytab 文件的信息，请参阅 [配置 Kerberos 密钥分发中心验证](#)，第 3 页。

步骤 9 点击 **确定 (OK)**。

将 Kerberos 服务器添加到 Kerberos 服务器组

在使用 Kerberos 服务器组之前，必须至少将一个 Kerberos 服务器添加到该组。

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。服务器端口是端口号 88 或 ASA 与 Kerberos 服务器进行通信所用的 TCP 端口号。
- 步骤 9** 配置 Kerberos 领域。

Kerberos 领域名称仅使用数字和大写字母，最多可包含 64 个字符。该名称应与在 Kerberos 领域的 Active Directory 服务器上运行的 Microsoft Windows `set USERDNSDOMAIN` 命令的输出匹配。在以下示例中，EXAMPLE.COM 是 Kerberos 领域名：

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

虽然 ASA 接受在名称中使用小写字母，但不会将小写字母转换为大写字母。请务必仅使用大写字母。

- 步骤 10** 点击确定 (OK)。

示例

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

配置 Kerberos 密钥分发中心验证

您可以配置 Kerberos AAA 服务器组以对组中的服务器进行身份验证。要完成身份验证，必须导入从 Kerberos 密钥分发中心 (KDC) 导出的密钥表文件。通过验证 KDC，可以防止攻击者伪装 KDC，从而根据攻击者的 Kerberos 服务器对用户凭证进行身份验证。

当您启用 KDC 验证时，在获取票证授予票证 (TGT) 并验证用户后，系统还会代表用户请求主机/ASA_hostname 的服务票证。然后，系统根据 KDC 的密钥验证返回的服务票证，该密钥存储在您从 KDC 生成并上传到 ASA 的密钥表文件中。如果 KDC 身份验证失败，则服务器被视为不受信任，且用户未通过身份验证。

以下操作步骤说明如何完成 KDC 身份验证。

开始之前

不能将 KDC 验证与 Kerberos 约束委派 (KCD) 结合使用。如果服务器组用于 KCD，则 `validate KDC` 选项将被忽略。

过程

步骤 1（在 KDC 上。）在 Microsoft Active Directory 中为 ASA 创建用户帐户（转到“开始 > 程序 > 管理工具 > Active Directory 用户和计算机”）。例如，如果 ASA 的完全限定域名 (FQDN) 为 asahost.example.com，请创建名为 asahost 的用户。

步骤 2（在 KDC 上。）使用 FQDN 和用户帐户为 ASA 创建主机服务主体名称 (SPN):

```
C:> setspn -A HOST/asahost.example.com asahost
```

步骤 3（在 KDC 上。）为 ASA 创建密钥表文件（为清楚起见，添加了换行）:

```
C:\Users\Administrator> ktpass /out new.keytab +rndPass
/princ host/asahost@EXAMPLE.COM
/mapuser asahost@example.com
/ptype KRB5_NT_SRV_HST
/mapop set
```

步骤 4（在 ASA 上。）依次选择工具 > 文件管理，然后从文件传输菜单中，选择相应的选项将 keytab 文件上传到闪存，具体取决于文件是在工作站上还是在远程服务器上。

步骤 5（在 ASA 上。）依次选择配置 > 设备管理 > 用户/AAA > AAA Kerberos，然后点击浏览闪存并选择上传的密钥表文件。

步骤 6（在 ASA 上。）将验证 KDC 选项添加到 Kerberos AAA 服务器组配置。keytab 文件仅由使用此选项配置的服务器组使用。

- a) 依次选择配置 > 设备管理 > 用户/AAA > AAA 服务器组。
- b) 选择 Kerberos 服务器组并点击“编辑”。或者，您也可以这次创建一个新组。
- c) 选择验证 KDC 选项。
- d) 点击确定 (OK)。

监控用于 AAA 的 Kerberos 服务器

您可以使用以下命令来监控和清除与 Kerberos 相关的信息。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** 命令可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** 命令可删除 AAA 服务器配置。

- show aaa kerberos [username 用户]

显示所有 Kerberos 票证或给定用户名的票证。

- **clear aaa kerberos tickets** [username 用户]
清除所有 Kerberos 票证或给定用户名的票证。
- **show aaa kerberos keytab**
显示有关 Kerberos keytab 文件的信息。
- **clear aaa kerberos keytab**
清除 Kerberos keytab 文件。

用于 AAA 的 Kerberos 服务器历史记录

功能名称	平台版本	说明
Kerberos服务器	7.0(1)	支持AAA的Kerberos服务器。 引入了以下菜单项： 配置 > 设备管理 > 用户/AAA > AAA 服务器组 。
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200AAA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。
Kerberos 密钥分发中心 (KDC) 身份验证。	9.8 (4) 及后续版本9.14 (1)	您可以从Kerberos密钥分发中心(KDC)导入keytab文件，并且系统可以验证Kerberos服务器没有受欺骗，然后再使用它来验证用户身份。要完成KDC验证，您必须在Kerberos KDC上设置 host/ASA_hostname 服务主体名称(SPN)，然后导出该SPN的keytab。然后，您必须将keytab上传到ASA，并配置Kerberos AAA服务器组以验证KDC。 我们新增/修改的菜单项： 配置 > 设备管理 > 用户/AAA > AAA Kerberos 、 配置 > 设备管理 > 用户/AAA > AAA 服务器组Kerberos 服务器组的添加/编辑对话框。

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。