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

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

aaa-server *server_group_name* **protocol kerberos**

示例：

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

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。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。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。

步骤 4 （可选。）启用 Kerberos 密钥分发中心 (KDC) 验证

validate-kdc

示例：

```
ciscoasa(config-aaa-server-group)# validate-kdc
```

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 4 页。

示例

以下示例创建名为 watchdogs 的 Kerberos 服务器组，添加服务器，并将领域设置为 EXAMPLE.COM。

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

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 将 Kerberos 服务器添加到 Kerberos 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 指定与默认 Kerberos 端口 (TCP / 88) 不同的服务器端口。ASA 在此端口上联系 Kerberos 服务器。

server-port *port_number*

示例：

```
ciscoasa(config-aaa-server-host)# server-port 8888
```

步骤 5 配置 Kerberos 领域。

kerberos-realm 名称

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。

示例：

```
ciscoasa(config-asa-server-group)# kerberos-realm EXAMPLE.COM
```

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** 命令将被忽略。

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。）使用 **aaa kerberos import-keytab** 命令将 keytab（在本例中为 new.keytab）导入到 ASA。

```
ciscoasa(config)# aaa kerberos import-keytab ftp://ftpserver.example.com/new.keytab
ftp://ftpserver.example.com/new.keytab imported successfully
```

步骤 5 （在 ASA 上。）将 **validate-kdc** 命令添加到 Kerberos AAA 服务器组配置。keytab 文件仅由包含此命令的服务器组使用。

```
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos
ciscoasa(config-aaa-server-group)# validate-kdc
```

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。

- **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。 引入了以下命令： **aaa-server protocol**、 **max-failed-attempts**、 **reactivation-mode**、 **aaa-server host**、 **kerberos-realm**、 **server-port**、 **clear aaa-server statistics**、 **clear configure aaa-server**、 **show aaa-server**、 **show running-config aaa-server**、 **timeout**.
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**。

功能名称	平台版本	说明
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。 添加了以下命令：**aaa kerberos import-keytab**、**clear aaa kerberos keytab**、**show aaa kerberos keytab**、**validate-kdc**。

用于 AAA 的 Kerberos 服务器历史记录

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。