Kerberos Servers for AAA

The following topics explain how to configure Kerberos servers used in AAA. You can use Kerberos servers for the authentication of management connections, network access, and VPN user access.

Guidelines for Kerberos Servers for AAA

- You can have up to 200 server groups in single mode or 8 server groups per context in multiple mode.
- Each group can have up to 16 servers in single mode or 8 servers in multiple mode. When a user logs in, the servers are accessed one at a time starting with the first server you specify in the configuration, until a server responds.

Configure Kerberos Servers for AAA

The following topics explain how to configure Kerberos server groups. You can then use these groups when configuring management access or VPNs.

Configure Kerberos AAA Server Groups

If you want to use a Kerberos server for authentication, you must first create at least one Kerberos server group and add one or more servers to each group.

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups**.

Step 2 Click **Add** in the **AAA Server Groups** area.

The **Add AAA Server Group** dialog box appears.

Step 3 Enter a name for the group in the **Server Group** field.

Step 4 Choose the **Kerberos** server type from the **Protocol** drop-down list:

Step 5 Click **Depletion** or **Timed** in the **Reactivation Mode** field.

In Depletion mode, failed servers are reactivated only after all of the servers in the group are inactive. In depletion mode, when a server is deactivated, it remains inactive until all other servers in the group are inactive. When and if this occurs, all servers in the group are reactivated. This approach minimizes the occurrence of connection delays due to failed servers.

In Timed mode, failed servers are reactivated after 30 seconds of down time.

Step 6 If you chose the Depletion reactivation mode, enter a time interval in the **Dead Time** field.

The dead time is the duration of time, in minutes, that elapses between the disabling of the last server in a group and the subsequent re-enabling of all servers. Deadtime applies only if you configure fallback to the local database; authentication is attempted locally until the deadtime elapses.

Step 7 Specify the maximum number of failed AAA transactions with a AAA server in the group before trying the next server.

This option sets the number of failed AAA transactions before declaring a nonresponsive server to be inactive.

Step 8 (Optional.) Select **Validate KDC** to enable Kerberos Key Distribution Center (KDC) validation.

To accomplish the authentication, you must also import a keytab file that you exported from the Kerberos Key Distribution Center (KDC). By validating the KDC, you can prevent an attack where the attacker spoofs the KDC so that user credentials are authenticated against the attacker's Kerberos server.

For information about how to upload the keytab file, see Configure Kerberos Key Distribution Center Validation, on page 3.

Step 9 Click **OK**.

Add Kerberos Servers to a Kerberos Server Group

Before you can use a Kerberos server group, you must add at least one Kerberos server to the group.

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups**.

Step 2 Select the server group to which you want to add a server.

Step 3 Click **Add** in the **Servers in the Selected Group** area.

The **Add AAA Server Group** dialog box appears for the server group.

Step 4 Choose the **Interface Name** through which the authentication server resides.

Step 5 Enter either the name or IP address for the server that you are adding to the group.

Step 6 Specify the timeout value for connection attempts to the server.

Specify the timeout interval (1-300 seconds) for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts (based on the retry interval) until the timeout is reached. If the number of consecutive failed transactions reaches the maximum-failed-attempts limit specified in the AAA server

group, the AAA server is deactivated and the ASA starts sending requests to another AAA server if it is configured.

Step 7 Select the retry interval, which is the time the system waits before retrying a connection request. You can select from 1-10 seconds. The default is 10 seconds.

Step 8 Specify the server port. The server port is either port number 88, or the TCP port number used by the ASA to communicate with the Kerberos server.

Step 9 Configure the Kerberos realm.

Kerberos realm names use numbers and upper case letters only, and can be up to 64 characters. The name should match the output of the Microsoft Windows **set USERDNSDOMAIN** command when it is run on the Active Directory server for the Kerberos realm. In the following example, EXAMPLE.COM is the Kerberos realm name:

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

Although the ASA accepts lower case letters in the name, it does not translate lower case letters to upper case letters. Be sure to use upper case letters only.

Step 10 Click **OK**.

Example

```
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)#
```

Configure Kerberos Key Distribution Center Validation

You can configure a Kerberos AAA server group to authenticate the servers in the group. To accomplish the authentication, you must import a keytab file that you exported from the Kerberos Key Distribution Center (KDC). By validating the KDC, you can prevent an attack where the attacker spoofs the KDC so that user credentials are authenticated against the attacker's Kerberos server.

When you enable KDC validation, after obtaining the ticket-granting ticket (TGT) and validating the user, the system also requests a service ticket on behalf of the user for host/ASA_hostname. The system then validates the returned service ticket against the secret key for the KDC, which is stored in a keytab file that you generated from the KDC and then uploaded to the ASA. If KDC authentication fails, the server is considered untrusted and the user is not authenticated.

The following procedure explains how to accomplish KDC authentication.

Before you begin

You cannot use KDC validation in conjunction with Kerberos Constrained Delegation (KCD). The validate KDC option will be ignored if the server group is used for KCD.

Procedure

Step 1 (On the KDC.) Create a user account in the Microsoft Active Directory for the ASA (go to **Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers**). For example, if the fully-qualified domain name (FQDN) of the ASA is asahost.example.com, create a user named asahost.

Step 2 (On the KDC.) Create a host service principal name (SPN) for the ASA using the FQDN and user account:

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

Step 3 (On the KDC.) Create a keytab file for the ASA (line feeds added for clarity):

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

Step 4 (On the ASA.) Choose **Tools** > **File Management**, and then from the **File Transfer** menu, select the appropriate option to upload the keytab file to flash, depending on whether it is on your workstation or on a remote server.

Step 5 (On the ASA.) Choose **Configuration** > **Device Management** > **Users/AAA** > **AAA Kerberos**, then click **Browse Flash** and select the uploaded keytab file.

Step 6 (On the ASA.) Add the **Validate KDC** option to the Kerberos AAA server group configuration. The keytab file is used only by server groups that are configured with this option.

a) Choose **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups**.
b) Select the Kerberos server group and click **Edit**. Alternatively, you can create a new group at this time.
c) Select the **Validate KDC** option.
d) Click **OK**.

Monitor Kerberos Servers for AAA

You can use the following commands to monitor and clear Kerberos-related information. Enter commands from the **Tools** > **Command Line Interface** window.

- **Monitoring** > **Properties** > **AAA Servers**

  This window shows the AAA server statistics.

- **show aaa-server**

  Shows the AAA server statistics. Use the **clear aaa-server statistics** command to clear the server statistics.

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

  Shows the AAA servers that are configured for the system. Use the **clear configure aaa-server** command to remove the AAA server configuration.

- **show aaa kerberos** [**username** *user*]

  Shows all Kerberos tickets, or tickets for a given username.

- **clear aaa kerberos tickets** [**username** *user*]

Clears all Kerberos tickets, or tickets for a given username.

- **show aaa kerberos keytab**

  Shows information about the Kerberos keytab file.

- **clear aaa kerberos keytab**

  Clears the Kerberos keytab file.

History for Kerberos Servers for AAA

Feature Name	Platform Releases	Description
Kerberos Servers	7.0(1)	Support for Kerberos servers for AAA. We introduced the following screens: **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups**
IPv6 addresses for AAA	9.7(1)	You can now use either an IPv4 or IPv6 address for the AAA server.
Increased limits for AAA server groups and servers per group.	9.13(1)	You can configure more AAA server groups. In single context mode, you can configure 200 AAA server groups (the former limit was 100). In multiple context mode, you can configure 8 (the former limit was 4). In addition, in multiple context mode, you can configure 8 servers per group (the former limit was 4 servers per group). The single context mode per-group limit of 16 remains unchanged. We modified the AAA screens to accept these new limits.
Kerberos Key Distribution Center (KDC) authentication.	9.8(4) and subsequent interim releases until 9.14(1)	You can import a keytab file from a Kerberos Key Distribution Center (KDC), and the system can authenticate that the Kerberos server is not being spoofed before using it to authenticate users. To accomplish KDC authentication, you must set up a **host**/*ASA_hostname* service principal name (SPN) on the Kerberos KDC, then export a keytab for that SPN. You then must upload the keytab to the ASA, and configure the Kerberos AAA server group to validate the KDC. We added or modified the following screens: **Configuration** > **Device Management** > **Users/AAA** > **AAA Kerberos**, **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups** Add/Edit dialog box for Kerberos server groups.