Local AAA Server

Last Updated: January 15, 2012

The Local AAA Server feature allows you to configure your router so that user authentication and authorization attributes currently available on AAA servers are available locally on the router. The attributes can be added to existing framework, such as the local user database or subscriber profile. The local AAA server provides access to the complete dictionary of Cisco IOS supported attributes.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Local AAA Server

- Before using this feature, you must have the **aaa new-model**command enabled.

Information About Local AAA Server

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Local Authorization Attributes Overview

The AAA subsystem (authentication, authorization, and accounting) is responsible for managing all supported attributes that are available to the various services within the Cisco IOS software. As such, it maintains its own local dictionary of all supported attributes. However, prior to Cisco IOS Release 12.3(14)T, most of these authorization options were not available for local (on-box) authorizations.

Local AAA Attribute Support

Effective with Cisco IOS Release 12.3(14)T, you can configure your router so that AAA authentication and authorization attributes currently available on AAA servers are made available on existing Cisco IOS devices. The attributes can be added to existing framework, such as the local user database or subscriber profile. For example, an attribute list can now be added to an existing username, providing the ability for the local user database to act as a local AAA server. For situations in which the local username list is relatively small, this flexibility allows you to provide complete user authentication or authorization locally within the Cisco IOS software without having a AAA server. This ability can allow you to maintain your user database locally or provide a failover local mechanism without having to sacrifice policy options when defining local users.

A subscriber profile allows domain-based clients to have policy applied at the end-user service level. This flexibility allows common policy to be set for all users under a domain in one place and applied there whether or not user authorization is done locally. Effective with Cisco IOS Release 12.3(14)T, an attribute list can be added to the subscriber profile, allowing the profile to apply all attributes that can be applied to services using AAA servers. Attributes that are configured under the AAA attribute list are merged with the existing attributes that are generated with the existing subscriber profile and passed to the Subscriber Server Switch (SSS) framework for application.

Note Accounting is still done on a AAA server and is not supported by this feature.

AAA Attribute Lists

AAA attribute lists define user profiles that are local to the router. Every attribute that is known to the AAA subsystem is made available for configuration.

The AAA attributes that are defined in the AAA attribute list are standard RADIUS or TACACS+ attributes. However, they are in the Cisco IOS internal format for that attribute. The attributes must be converted from the RADIUS format (for a RADIUS case) to the Cisco IOS AAA interface format. TACACS+ attributes are generally identical to the Cisco IOS AAA interface format.

Converting from RADIUS Format to Cisco IOS AAA Format

You can use the **show aaa attributes protocol radius** command to get the Cisco IOS AAA format of the Internet Engineering Task Force (IETF) RADIUS attribute. The **show** command output provides a complete list of all the AAA attributes that are supported.

Note The conversion from RADIUS to internal AAA is done internally within the AAA framework. RADIUS vendor-specific attributes (VSAs) are usually accurately reflected during conversion. TACACS+ attributes are also usually identical to the local attributes and do not require the conversion process. However, IETF numbered attributes and some special VSAs often require the conversion process.

Validation of Attributes

Attributes are not validated at configuration. The AAA subsystem “knows” only the format that is expected by the services when the service defines a given attribute inside a definition file. However, it cannot validate the attribute information itself. This validation is done by a service when it first uses the attribute. This validation applies whether the AAA server is RADIUS or TACACS+. Thus, if you are not familiar with configuring a AAA server, it is advisable that you test your attribute list on a test device with the service that will be using the list before configuring and using it in a production environment.

How to Configure Local AAA Server

Defining a AAA Attribute List

To define an AAA attribute list, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa attribute list** *list-name*
4. **attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*]
5. **attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*]
6. **attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*]
7. **attribute type** {*name*} {*value*}
8. **attribute type** {*name*} {*value*}
9. **attribute type** {*name*} {*value*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa attribute list** *list-name* **Example:** `Router (config)# aaa attribute list TEST`	Defines a AAA attribute list.
Step 4	**attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*] **Example:** `Router (config-attr-list)# attribute type addr-pool poolname service ppp protocol ip`	Defines an IP address pool to use.
Step 5	**attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*] **Example:** `Router (config-attr-list)# attribute type ip-unnumbered loopbacknumber service ppp protocol ip`	Defines the loopback interface to use.
Step 6	**attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*] **Example:** `Router (config-attr-list)# attribute type vrf-id vrfname service ppp protocol ip`	Defines the virtual route forwarding (VRF) to use.
Step 7	**attribute type** {*name*} {*value*} **Example:** `Router (config-attr-list)# attribute type ppp-authen-list aaalistname`	Defines the AAA authentication list to use.

	Command or Action	Purpose
Step 8	**attribute type** {*name*} {*value*} **Example:** `Router (config-attr-list)# attribute type ppp-author-list aaalistname`	Defines the AAA authorization list to use.
Step 9	**attribute type** {*name*} {*value*} **Example:** `Router (config-attr-list)# attribute type ppp-acct-list “aaa list name”`	Defines the AAA accounting list to use.

Defining a Subscriber Profile

To define a subscriber profile, perform the following steps.

Note RADIUS users should use the **show aaa attributes** command to map the RADIUS version of the particular attribute to the Cisco IOS AAA version of the string attribute. See the example Mapping from the RADIUS Version of a Particular Attribute to the Cisco IOS AAA Version Example.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber authorization enable**
4. **policy-map type service** *domain-name*
5. **service local**
6. **exit**
7. **aaa attribute list** *list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**subscriber authorization enable** **Example:** `Router (config)# subscriber authorization enable`	Enables subscriber authorization.
Step 4	**policy-map type service** *domain-name* **Example:** `Router (config)# policy-map type example.com`	Specifies the username domain that has to be matched and enters subscriber profile configuration mode.
Step 5	**service local** **Example:** `Router (subscriber-profile)# service local`	Specifies that local subscriber authorization should be performed.
Step 6	**exit** **Example:** `Router (subscriber-profile)# exit`	Exits subscriber profile configuration mode.
Step 7	**aaa attribute list** *list-name* **Example:** `Router (config)# aaa attribute list TEST`	Defines the AAA attribute list from which RADIUS attributes are retrieved.

Monitoring and Troubleshooting a Local AAA Server

The following debug commands may be helpful in monitoring and troubleshooting, especially to ensure that domain-based service authorization is being triggered and that location authorization is being called on the local AAA server, which triggers the service.

SUMMARY STEPS

1. **enable**
2. **debug aaa authentication**
3. **debug aaa authorization**
4. **debug aaa per-user**
5. **debug ppp authentication**
6. **debug ppp error**
7. **debug ppp forward**
8. **debug ppp negotiation**
9. **debug radius**
10. **debug sss error**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug aaa authentication** **Example:** `Router# debug aaa authentication`	Displays the methods of authentication being used and the results of these methods.
Step 3	**debug aaa authorization** **Example:** `Router# debug aaa authorization`	Displays the methods of authorization being used and the results of these methods.
Step 4	**debug aaa per-user** **Example:** `Router# debug aaa per-user`	Displays information about PPP session per-user activities.
Step 5	**debug ppp authentication** **Example:** `Router# debug ppp authentication`	Indicates whether a client is passing authentication.

	Command or Action	Purpose
Step 6	**debug ppp error** **Example:** `Router (config)# debug ppp error`	Displays protocol errors and error statistics that are associated with PPP connection negotiation and operation.
Step 7	**debug ppp forward** **Example:** `Router# debug ppp forward`	Displays who is taking control of a session.
Step 8	**debug ppp negotiation** **Example:** `Router# debug ppp negotiation`	Displays PPP packets sent during PPP startup, where PPP options are negotiated.
Step 9	**debug radius** **Example:** `Router# debug radius`	Displays information about the RADIUS server.
Step 10	**debug sss error** **Example:** `Router# debug sss error`	Displays diagnostic information about errors that may occur during SSS call setup.

Configuration Examples for Local AAA Server

Local AAA Server Example

The following example shows a Point to Point over Ethernet (PPPoE) group named “bba-group” that is configured for subscriber profile cisco.com (thus, any user with the domain name cisco.com will execute the subscriber profile cisco.com authorization policy). The cisco.com subscriber profile is configured to attach the AAA attribute list “TEST,” which has both “ip vrf forwarding” and “ip unnumbered” configured for PPP service under Link Control Protocol (LCP) negotiation. This configuration will essentially cause

the named attributes to be applied on the session with the cisco.com domain under the bba-group “pppoe grp1.”

```
aaa authentication ppp template1 local
aaa authorization network template1 local
!
aaa attribute list TEST
   attribute type interface-config "ip unnumbered FastEthernet0" service ppp protocol lcp
   attribute type interface-config "ip vrf forwarding blue" service ppp protocol lcp
!
ip vrf blue
 description vrf blue template1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
subscriber authorization enable
!
policy-map type service example.com
 service local
 aaa attribute list TEST
!
bba-group pppoe grp1
 virtual-template 1
 service profile example.com
!
interface Virtual-Template1
 no ip address
 no snmp trap link-status
 no peer default ip address
 no keepalive
 ppp authentication pap template1
 ppp authorization template1
!
```

Note In some versions of Cisco IOS software, it is better to use the explicit attribute instead of interface- config because it provides better scalability (full VAccess interfaces are not required, and sub interfaces could be used to provide the service). In such a case, you might configure “attribute type ip-unnumbered ‘FastEthernet0’ service ppp protocol ip” instead of “attribute type interface-config ‘ip unnumbered FastEthernet0’ service ppp protocol lcp.”

Mapping from the RADIUS Version of a Particular Attribute to the Cisco IOS AAA Version Example

The following output example of the **show aaa attributes** command lists RADIUS attributes, which can be used when configuring this feature.

```
Router#
show aaa attributes protocol radius
IETF defined attributes:
   Type=4     Name=acl                              Format=Ulong
      Protocol:RADIUS
        Unknown       Type=11    Name=Filter-Id             Format=Binary
Converts attribute 11 (Filter-Id) of type Binary into an internal attribute
named "acl" of type Ulong.  As such, one can configure this attributes locally
by using the attribute type "acl."
Cisco VSA attributes:
  Type=157   Name=interface-config               Format=String
Simply expects a string for the attribute of type "interface-config."
```

Note The **aaa attribute list** command requires the Cisco IOS AAA version of an attribute, which is defined in the “Name” field above.

Additional References

Related Document

Related Topic	Document Title
AAA, AAA attribute lists, AAA method lists, and subscriber profiles	Configuring Local AAA Server feature module and the User Database--Domain to VRF in *Cisco 10000 Series Broadband Aggregation and Leased-Line Configuration Guide*
Cisco IOS security commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	http://www.cisco.com/go/mibs To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Local AAA Server

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Local AAA Server

Feature Name	Releases	Feature Information
Local AAA Server	12.3(14)T 12.2(28)SB 12.2(33)SRC	The Local AAA Server feature allows you to configure your router so that user authentication and authorization attributes currently available on AAA servers are available locally on the router. The attributes can be added to existing framework, such as the local user database or subscriber profile. The local AAA server provides access to the complete dictionary of Cisco IOS supported attributes.