Objective

This tech note outlines the main differences in authentication, authorization and accounting (AAA), LDAP, RADIUS, and TACACS+ support between Cisco® NX-OS Software and Cisco IOS® Software. Sample configurations are included for Cisco NX-OS and Cisco IOS Software for some common features to demonstrate the similarities and differences. Please refer to the NX-OS documentation on Cisco.com for a complete list of supported features.

AAA Overview

AAA used in combination with LDAP, RADIUS or TACACS+ provides remote authentication, authorization and accounting security services for centralized system management. AAA services improve scalability and simplify security management by using a central security database rather than local databases.

Important Cisco NX-OS and Cisco IOS Software Differences

In Cisco NX-OS:

- LDAP and TACACS+ command-line interface (CLI) configuration and verification commands are not available until you enable the LDAP or TACACS+ feature with the **feature ldap** or **feature tacacs+** command (The RADIUS feature is enabled by default and cannot be disabled).
- The **aaa new-model** command is not required to enable AAA authentication, authorization, or accounting.
- LDAP version 3 can be configured to support authentication and authorization services. Cisco IOS software does not support LDAP for authentication or authorization services.
- The RADIUS vendor-specific attributes (VSA) feature is enabled by default. Cisco IOS Software requires the global **radius-server vsa send** configuration command to enable IETF attribute 26.
- Local command authorization can be performed using privilege-levels or role-based access control (RBAC) without a AAA server. Local privilege-levels or RBAC roles can be associated to users configured on the AAA server using VSAs (TACACS+ supports command authorization that can be configured on the AAA server).
- If a configured AAA server is not available for authentication, the local database (username/password) is automatically used for device access.
- The RADIUS and TACACS+ host keys are Triple Data Encryption Standard (3DES) encrypted in the configuration. Cisco IOS Software requires the **service password** command.
- All configuration commands are recorded in a local log (NVRAM) with user and time stamp information by default (no AAA configuration required). The log can be viewed with the **show accounting log** command.
- The **aaa accounting default** command enables accounting for start and stop records as well as command accounting (Exec mode and configuration mode). Cisco IOS Software requires additional **aaa accounting** commands to enable both types of accounting.
- RADIUS and TACACS+ support Cisco Fabric Services (CFS) for automated configuration synchronization between Nexus 7000 chassis.

Things You Should Know

The following list provides some additional facts about Cisco NX-OS that should be helpful when configuring and maintaining AAA, LDAP, RADIUS, and TACACS+ services.

- Different AAA, LDAP, RADIUS and TACACS+ policies can be applied per virtual device context (VDC). However, the console login policy only applies to the default VDC.
- Configuring a protocol for AAA is a multi-step configuration process: Define the server(s), create the server group, and associate the server group to the required AAA commands.
- If you remove a feature such as LDAP or TACACS+ with the global **no feature *<name>*** command, all relevant configuration information is removed from the running-configuration for the specified feature.
- 64 LDAP, 64 RADIUS and 64 TACACS+ servers can be configured per device.
- AAA server groups are associated with the **default** Virtual Route Forwarding (VRF) instance by default. Associate the proper VRF instance with the AAA server group if you are using the management port on the supervisor module or if the AAA server is in a non-default VRF instance.
- A RADIUS and TACACS+ source interface can be configured globally or per AAA server group to specify the source IP address for packets destined to remote AAA services.
- RADIUS and TACACS+ server keys can be specified for a group of servers or per individual server.
- By default, LDAP uses TCP port 389, RADIUS uses UDP ports 1812 (authentication) and 1813 (accounting), and TACACS+ uses TCP port 49. All server ports can be configured to use different values.
- Directed server requests are enabled by default for RADIUS and TACACS+.
- The **local** option can be used with AAA authorization to fallback to local privilege-levels or RBAC in the event a AAA server is not available for command authorization.
- RADIUS and TACACS+ support global server test monitoring (Per server monitoring takes precedence over global monitoring).
- Use the **show running-config** command with the **aaa**, **ldap**, **radius** or **tacacs+** option to display the running configuration for a specific feature.

Configuration Comparison

The following sample code shows configuration similarities and differences between the Cisco NX-OS and Cisco IOS Software CLIs. The configurations for the two operating systems are very similar.

Cisco IOS CLI	*Cisco NX-OS CLI*
Enabling LDAP	
	feature ldap
Configuring an LDAP Search Map	
	ldap search-map ldap-map userprofile attribute-name description search-filter "sAMAccountNAme=$userid" base-DN dc=cisco,dc=com
Configuring an LDAP Server	
	ldap-server host 192.168.1.1 rootDN cn=N7K-device,cn=Users,dc=cisco,dc=com password 7 Qxz12345
Configuring a RADIUS Server with a Key	
	radius-server host 192.168.1.1 key 7 "fewhg123"

Specifying Non defualt RADIUS UDP Ports

radius-server 192.168.1.1 auth-port 1645 acct-port 1646

Specifying the RADIUS Timeout Value (Global)

radius-server timeout 10

Specifying the RADIUS Source Interface (Global)

ip radius source-interface loopback0

Enabling TACACS+

feature tacacs+

Configuring a TACACS+ Server with a Key

tacacs-server host 192.168.1.1 key 7 "fewhg123"

Specifying a Nondefualt TACACS+ TCP Port

tacacs-server host 192.168.1.1 port 85

Specifying the TACACS+ Timeout Value (Global)

tacacs-server timeout 10

Specifying the TACACS+ Source Interface (Global)

ip tacacs source-interface loopback0

Configuring an AAA Server Group (LDAP)

aaa group server ldap AAA-Servers

server 192.168.1.1

ldap-search-map ldap-map

Configuring an AAA Server Group (RADIUS)

aaa group server radius AAA-Servers

server 192.168.1.1

Configuring an AAA Server Group for a VRF Instance (RADIUS)

aaa group server radius AAA-Servers

server 192.168.1.1

use-vrf management

Configuring the AAA Server Group Dead Time (RADIUS)

aaa group server radius AAA-Servers

deadtime 5

Configuring an AAA Server Group (TACACS+)

aaa group server tacacs+ AAA-Servers

server 192.168.1.1

Enabling AAA Authentication with an AAA Server Group

aaa authentication login default group AAA-Servers

Enabling AAA Authorization with an AAA Server Group

aaa authorization config-commands default group AAA-Servers

aaa authorization commands default group AAA-Servers

Enabling AAA Accounting with an AAA Server Group

aaa accounting default group AAA-Servers

Verification Command Comparison

The following table compares some useful **show** commands for verifying and troubleshooting AAA, LDAP, RADIUS and TACACS+ services.

Cisco NX-OS AAA	**Cisco IOS Software AAA**	**Command Description**
show aaa accounting	-	Displays the status of AAA accounting
show aaa authentication	-	Displays the default and console login methods
show aaa authentication login ascii-authentication	-	Displays the status of ascii authentication; enabled or disabled
show aaa authentication login chap	-	Displays the status of the Challenge Handshake authentication protocol (CHAP); enabled or disabled
show aaa authentication login error-enable	-	Displays the login error message status; enabled or disabled.
show aaa authentication login mschap	-	Displays the status of Microsoft CHAP (MS-CHAP); enabled or disabled.
show aaa authentication login mschapv2	-	Displays the status of MS-CHAPv2; enabled or disabled)
show aaa authorization	-	Displays the AAA authorization configuration
show aaa groups	-	Displays the AAA groups that are configured
show aaa users	show aaa user	Displays the AAA users that authenticated remotely
show accounting log	-	Displays the local AAA configuration accounting log

show ldap-search-map	-	Displays the global LDAP search map configuration
show ldap-server	-	Displays the LDAP server configuration for all servers
show ldap-server groups	-	Displays LDAP server groups
show ldap-server statistics <*x.x.x.x*>	-	Displays LDAP statistics for a specific server
show radius-server	-	Displays the RADIUS server configuration for all servers
show radius-server <*x.x.x.x*>	-	Displays a specific RADIUS server configuration
show radius-server directed-request	-	Displays the status of the directed-request feature (enabled or disabled)
show radius-server groups	show radius server-group	Displays RADIUS server groups
show radius-server sorted	-	Displays RADIUS servers sorted by name
show radius-server statistics <*x.x.x.x*>	show radius statistics	Displays RADIUS statistics for a specific server
show tacacs-server	show tacacs	Displays the TACACS+ server configuration for all servers
show tacacs-server <*x.x.x.x*>	-	Displays a specific TACACS+ server configuration
show tacacs-server directed-request	-	Displays the status of the directed-request feature (enabled or disabled)
show tacacs-server groups	-	Displays TACACS+ server groups
show tacacs-server sorted	-	Displays TACACS+ servers sorted by name
show tacacs-server statistics <*x.x.x.x*>	-	Displays TACACS+ statistics for a specific server
show user-account	-	Displays a list of locally configured users
show users	show users	Displays the users who are logged in