SECURITY

AAA Identity Management Security

Vivek Santuka
Premdeep Banga
Brandon J. Carroll

ciscopress.com

AAA Identity Management Security

Vivek Santuka, CCIE #17621

Premdeep Banga, CCIE #21713

Brandon J. Carroll, CCIE #23837

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Monitoring and Reports

The Monitoring and Reports drawer replaces the Reports and Activity section of previous versions of ACS. You can now view reports based on different criteria such as Access Service, End Point, and Failure Reason, among others. ACS 5.x also introduces a configurable dashboard for reports and alarms.

Note ACS 5.x has added monitoring, reporting, and troubleshooting capabilities that are similar to those available is ACSView 4.0. ACSView is an independent reporting and monitoring platform available for ACS 4.x.

Covering the entire Monitoring and Reports section in depth is beyond the scope of this book. This section of the text will focus on the reports that are most important and touch on the rest briefly.

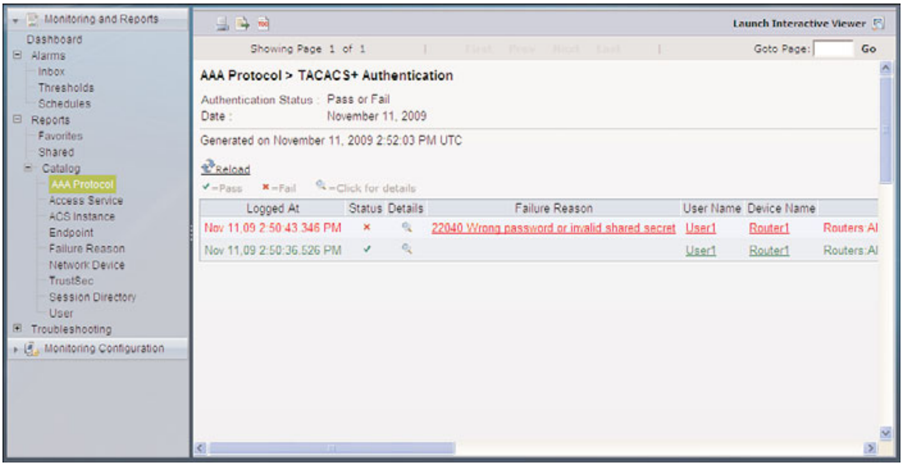
The Monitoring and Reports drawer contains the Launch Monitoring and Report Viewer option. Click this option to open the Monitoring and Reports Viewer in another browser window or tab. The layout of the new window is similar to the main window but contains only the following two drawers:

- Monitoring and Reports
- Monitoring Configuration

The Monitoring and Reports drawer contains the following options:

- **DashBoard:** ACS 5.1 provides a new customizable dashboard that contains tabs and portlets where your favorite queries, recent alarms and reports, and health status of ACS reside. Each of these tabs can have multiple portlets, with each portlet containing an application of your choice. You can select an application from the available list. Some of the important applications available in the dashboard by default are as follows:
    - **Recent Five Alarms:** This application is available in the General tab and shows the latest five alarms.
    - **Favorite Reports:** This application contains links to favorite reports. The favorite list is configuration from the Reports option discussed later.
    - **Live Authentications:** This application is available in the Troubleshooting tab and shows authentication requests received in real time. This is a very useful application for troubleshooting. By default, it refreshes every 10 seconds and is configured to monitor RADIUS requests.
    - **NAD Show Command:** A neat little application that can connect to a network device using SSH or Telnet and run a **show** command. You have to provide the login details and the **show** command to run. ACS will display the output in a new window. This is also a very useful application. It saves you from jumping between ACS GUI and Telnet or SSH clients.
    - **ACS Health Status:** Shows the health of the ACS server.

- **Alarms:** ACS 5.x introduces alarms. The monitoring component retrieves data from ACS and generates alarms to notify you of critical system conditions. These alarms can be viewed in the Inbox option in this drawer or can be received through Syslog and email. There are two types of alarms in ACS: Threshold and System. Threshold alarms are defined on logs collected from ACS. You can configure a threshold alarm to notify you of different events such as authentication activity, system health, and process status, among others. System alarms notify you of critical conditions encountered during the execution of the ACS Monitoring and Reporting viewer. System alarms also provide the informational status of system activities, such as data purge events or the failure of the log collector to populate the View database. You cannot configure system alarms. This drawer contains the following options:
  - **Inbox:** Generated alarms can be viewed in the Inbox. After you view an alarm, you can edit the status of the alarm, assign the alarm to an administrator, and add notes to track the event.
  - **Thresholds:** You can configure thresholds from this page. A maximum of 100 thresholds can be configured in an ACS server. Four thresholds exist by default, out of which only the System Errors threshold is enabled.
  - **Schedules:** Each threshold has a schedule associated with it. The schedule defines when a threshold is run. You need to configure schedules on this page before you can use them in thresholds. By default, ACS has a nonstop schedule that monitors events 24 hours a day, seven days a week.
- **Reports:** The Reports section contains different predefined reports that you can use to monitor and troubleshoot ACS. These reports include authentication and authorization reports (similar to passed and failed reports from ACS 4.x), access service reports, ACS configuration and operation audits, and network device summary, among others. You can add any of the reports to your Favorites and those will be displayed in the General tab of the dashboard. The following report categories are available in the catalog:
  - **AAA Protocol:** Contains RADIUS and TACACS+ authentication, authorization (TACACS+ only) and accounting reports, AAA diagnostics, and authentication trend. Passed and failed logs from previous ACS version have been divided into protocol-specific authentication and authorization reports. Figure 4-26 shows the TACACS+ authentication report.
  - **Access Service:** Contains a graphical summary report and a top count report for authentication in respect to access services.
  - **ACS Instance:** Contains different system-related reports such as configuration and operations audit reports, health summary, administrator logins and entitlement reports, and ACS system diagnostics.
  - **Endpoint:** Contains MAC address-based authentication summary reports, MAC address-based top authentications reports, and machine-based top authentication reports.



AAA Protocol > TACACS+ Authentication

Authentication Status : Pass or Fail
Date : November 11, 2009

Generated on November 11, 2009 2:52:03 PM UTC

Logged At	Status	Details	Failure Reason	User Name	Device Name	
Nov 11,09 2:50:43.346 PM	✖	🔍	22040 Wrong password or invalid shared secret	User1	Router1	Routers:Al
Nov 11,09 2:50:36.526 PM	✓	🔍		User1	Router1	Routers:Al

Figure 4-26 *TACACS+ Authentication Report*

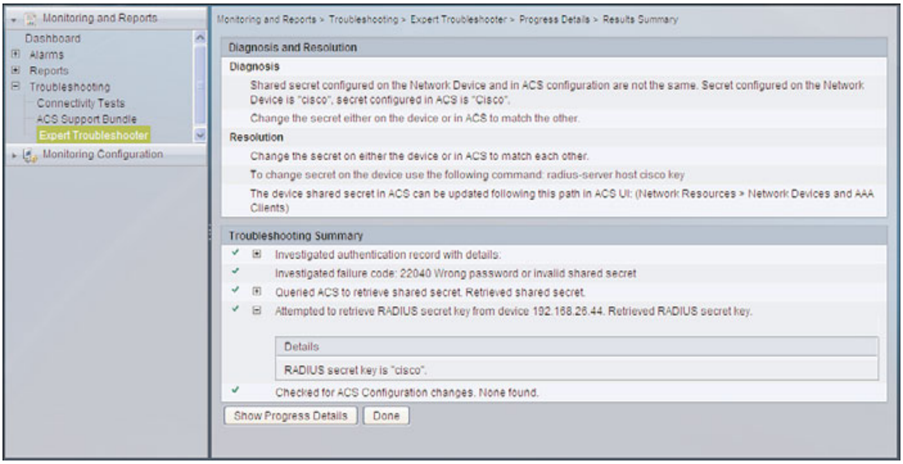
- **Failure Reason:** Contains summary and top authentication failure reports. This is one of the most important reporting sections. A close look at this section can tell you about any access attacks being carried out against your network.
- **Network Device:** Contains summary and top authentication reports in respect to network devices. These reports are useful in tracking which devices are generating the maximum number of requests.
- **Session Directory:** Contains active session, terminated sessions, and session history reports for RADIUS and TACACS+. Accounting packets received from devices are used to maintain session information.
- **User:** Contains summary and top authentication reports in respect to users.

- **Troubleshooting:** ACS 5.x contains some nice troubleshooting options. The following options are available in the Troubleshooting section:

- **Connectivity Tests:** You can run a ping, traceroute, and nslookup for a hostname or IP address to see whether the device is reachable from ACS. This is important to see whether the requests from a device and replies from ACS to the device are not getting dropped in the network.

- **ACS Support Bundle:** The support bundle is a zip archive of diagnostic information, including system log files. You can also choose to include ACS configuration, ACS debug log files, ACS localstore log files, and core files. This support bundle will be needed by the Cisco Technical Assistance Center (TAC) for troubleshooting.

- **Expert Troubleshooter:** This section contains some nice tools to check the configuration of a device and ACS. Using RADIUS Authentication troubleshooting tool, you can select a failed or passed log from RADIUS authentication report and have it check the ACS and device configuration to see why the authentication failed or passed. Figure 4-27 shows the report generated by this tool when changing the RADIUS shared key on the device. This section also contains the NAD **show** command application from the dashboard and the Evaluate Configuration Validator, which checks the configuration of a device to see whether it is configured properly for a task such as 802.1x authentication.



Diagnosis and Resolution

Diagnosis

Shared secret configured on the Network Device and in ACS configuration are not the same. Secret configured on the Network Device is "cisco", secret configured in ACS is "Cisco".

Change the secret either on the device or in ACS to match the other.

Resolution

Change the secret on either the device or in ACS to match each other.

To change secret on the device use the following command: radius-server host cisco key

The device shared secret in ACS can be updated following this path in ACS UI: (Network Resources > Network Devices and AAA Clients)

Troubleshooting Summary

✓ ⊞ Investigated authentication record with details:

✓ Investigated failure code: 22040 Wrong password or invalid shared secret

✓ ⊞ Queried ACS to retrieve shared secret. Retrieved shared secret.

✓ ⊟ Attempted to retrieve RADIUS secret key from device 192.168.26.44. Retrieved RADIUS secret key.

Details

RADIUS secret key is "cisco".

✓ Checked for ACS Configuration changes. None found.

Figure 4-27 *RADIUS Authentication Troubleshooting Tool at Work*

The Monitoring Configuration drawer contains various configuration options for the Monitoring and Report Viewer. Configuration of ACS View (the Monitoring and Reporting part of ACS 5.x) is out of the scope of this book.

Note The System Administration drawer contains various advanced configuration options for ACS. These options are covered in Chapter 15.

ACS 5.1 Command-Line Interface (CLI)

ACS 5.x, unlike previous versions, provides a CLI for configuration and monitoring along with a GUI. You can access the ACS CLI through a secure shell (SSH) client or the console port.

Two different types of accounts are available for accessing the CLI:

- **Admin:** Admin accounts have full configuration and monitoring access.
- **Operator:** Operator accounts have monitoring access only.

This section assumes use of an Admin account to access the CLI.

The ACS CLI is similar to IOS CLI in look, feel, modes, and command structure. You can use the question mark (?) to see the help and the Tab key to complete a command. Logging in to the ACS server places you in the Operator (user) mode or the Admin (EXEC) mode. Typically, logging in requires a username and password.

You can always tell when you are in the Operator (user) mode or Admin (EXEC) mode by looking at the prompt. A right angle bracket (>) appears at the end of the Operator (user) mode prompt; a pound sign (#) appears at the end of the Admin mode prompt, regardless of the submode.

Three command modes are available on the CLI:

- **EXEC:** EXEC commands primarily include system-level commands such as **show** and **reload** (for example, application installation, application start and stop, copy files and installations, restore backups, and display information). In addition, certain EXEC-mode commands have ACS-specific abilities (for example, start an ACS instance, display and export ACS logs, and reset an ACS configuration to factory default settings).
- **ACS Configuration:** Commands in this mode can be used to set the debug log level for the ACS management and runtime components, show system settings, reset server certificates and IP address access lists, and manage import and export processes. To access the ACS configuration mode, run the **acs-config** command in EXEC mode as demonstrated in Example 4-1.

Example 4-1 *ACS CLI—Changing to ACS Configuration Mode*

```
ACS51/admin# acs-config
Escape character is CNTL/D.

Username: ACSAdmin
Password:

ACS51/ACSAdmin(config-acs)#
```

- **Configuration:** Commands in this mode can be used to configure various system options such as interface, repository, SNMP server, and NTP, among others. To access the Configuration mode, run the **configure** command in EXEC mode as demonstrated in Example 4-2.

Example 4-2 *ACS CLI—Changing to Configuration Mode*

```
ACS51/admin# configure
Enter configuration commands, one per line.  End with CNTL/Z.
ACS51/admin(config)#
```

It is not possible to cover all the commands available in the CLI. The list that follows highlights a few important tasks and their related commands:

- **Starting and Stopping ACS Services:** ACS services can be started or stopped from the EXEC mode using the **acs {start | stop}** command.

- **Reset ACS Configuration:** To reset ACS configuration to the factory default, use the **acs reset-config** command at the EXEC mode.
- **Reset ACSAdmin Password:** To reset the password of the default GUI admin, use the **acs reset-password** command from the EXEC mode.
- **Verify Configuration:** To see the current configuration, use the **show running-config** command from the EXEC mode.
- **Verify Version Information:** To see the current version, use the **show version** command from the EXEC mode.
- **Verify Status of ACS Processes:** To verify the status of the ACS processes, use the **show application status acs** EXEC command.
- **Troubleshoot Connectivity:** To troubleshoot network connectivity, use the **ping** *ip address or hostname*, **traceroute** *ip address or hostname*, and **nslookup** *ip address or hostname* commands from the EXEC mode.
- **Change IP Address:** To change the IP address of the interface, use the **ip address** *ip address subnet mask* command in the Interface mode. To go to the Interface mode, use the **interface GigabitEthernet 0** command in the Configuration mode.
- **Add a Route:** To add a route to the routing table of ACS, use the **ip route** *network-address netmask* **gateway** *gateway-address* command in the Configuration mode.
- **Disable ICMP Echo Response:** To stop the device from sending ICMP echo responses to echo requests received, use the **icmp echo off** command. Use **icmp echo on** command to enable the device to send echo responses.
- **Change Hostname:** To change the hostname of the server, use the **hostname** *name* command in the Configuration mode.

For more details on ACS CLI commands, see the “CLI Reference Guide for the Cisco Secure Access Control System 5.1.”

Summary

At this point, you should be familiar with the interface of ACS 5.1 and the process of adding and creating different elements. Remember the flow of adding network devices and users, creating policy elements and access services. You are now prepared to add external user repositories and create complex access services for different AAA scenarios.