CHAPTER 1

Introducing ACS 5.2

This section contains the following topics:

- Overview of ACS, page 1-1
- ACS Distributed Deployment, page 1-2
- ACS Management Interfaces, page 1-3

Overview of ACS

ACS is a policy-based security server that provides standards-compliant Authentication, Authorization, and Accounting (AAA) services to your network. ACS facilitates the administrative management of Cisco and non-Cisco devices and applications.

As a dominant enterprise network access control platform, ACS serves as an integration point for network access control and identity management.

ACS 5.x provides a rule-based policy model that allows you to control network access based on dynamic conditions and attributes. The rule-based policy is designed to meet complex access policy needs. For more information on the rule-based policy model in ACS, see Chapter 3, "ACS 5.x Policy Model."

Within the greater context of two major AAA protocols—RADIUS and TACACS+—ACS provides the following basic areas of functionality:

- Under the framework of the RADIUS protocol, ACS controls the wired and wireless access by users and host machines to the network and manages the accounting of the network resources used.

  ACS supports multiple RADIUS-based authentication methods that includes PAP, CHAP, MSCHAPv1, MSCHAPv2. It also supports many members of the EAP family of protocols, such as EAP-MD5, LEAP, PEAP, EAP-FAST, and EAP-TLS.

  In association with PEAP or EAP-FAST, ACS also supports EAP-MSCHAPv2 and EAP-GTC. For more information on authentication methods, see Appendix B, "Authentication in ACS 5.2".

- Under the framework of the TACACS+ protocol, ACS helps to manage Cisco and non-Cisco network devices such as switches, wireless access points, routers, and gateways. It also helps to manage services and entities such as dialup, Virtual Private Network (VPN), and firewall.

ACS is the point in your network that identifies users and devices that try to connect to your network. This identity establishment can occur directly by using the ACS internal identity repository for local user authentication or by using external identity repositories.

For example, ACS can use Active Directory as an external identity repository, to authenticate a user to grant the user access to the network. For more information about creating identities and supported identity services, see Chapter 8, "Managing Users and Identity Stores."

ACS provides advanced monitoring, reporting, and troubleshooting tools that help you administer and manage your ACS deployments. For more information on the monitoring, reporting, and troubleshooting capabilities of ACS, see Chapter 11, "Monitoring and Reporting in ACS.".

For more information about using ACS for device administration and network access scenarios, see Chapter 4, "Common Scenarios Using ACS."

Cisco Secure ACS:

- Enforces access policies for VPN and wireless users.
- Provides simplified device administration.
- Provides advanced monitoring, reporting, and troubleshooting tools.

There are several changes and enhancements in ACS 5.2 compared to ACS 5.1. For a complete list of new and changed features, see http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/release/notes/acs_52_rn.html.

Related Topics

- ACS Distributed Deployment, page 1-2
- ACS Management Interfaces, page 1-3

ACS Distributed Deployment

ACS 5.2 is delivered preinstalled on a standard Cisco Linux-based appliance, and supports a fully distributed deployment.

An ACS deployment can consist of a single instance, or multiple instances deployed in a distributed manner, where all instances in a system are managed centrally. One ACS instance becomes the *primary instance* and you can register additional ACS instances to the primary instance as *secondary instances*. All instances have the configuration for the entire deployment, which provides redundancy for configuration data.

The primary instance centralizes the configuration of the instances in the deployment. Configuration changes made in the primary instance are automatically replicated to the secondary instance.

You can force a *full replication* to the secondary instance. Full replication is used when a new secondary instance is registered and in other cases when the replication gap between the secondary instance and the primary instance is significant.

Related Topic

- ACS 4.x and 5.2 Replication, page 1-2

ACS 4.x and 5.2 Replication

In ACS 4.x, you must select the database object types (or classes) you wish to replicate from primary instance to the secondary instance. When you replicate an object, a complete configuration copy is made on the secondary instance.

In ACS 5.2, any configuration changes made in the primary instance are immediately replicated to the secondary instance. Only the configuration changes made *since the last replication* are propagated to the secondary instance.

ACS 4.x did not provide incremental replication, only full replication, and there was service downtime for replication. ACS 5.2 provides incremental replications with no service downtime.

You can also *force* a full replication to the secondary instance if configuration changes do not replicate it. Full replication is used when a new secondary instance is registered and other cases when the replication gap between the secondary instance and the primary instance is significant.

Table 1-1 lists some of the differences between ACS 4.x and 5.2 replication.

Table 1-1 Differences Between ACS 4.x and 5.2 Replication

ACS 4.x	ACS 5.2
You can choose the data items to be replicated.	You cannot choose the data items to be replicated. All data items, by default are replicated.
Supports multi-level or cascading replication.	Supports only a fixed flat replication. Cascading replication is not supported.
Some data items such as, the external database configurations are not replicated.	All data items are replicated.

For more information about setting up a distributed deployment, see Configuring System Operations, page 17-1.

Note Network Address Translation (NAT) is not supported in ACS distributed deployment environment. That is, if a primary or secondary instance's network address is translated then the database replication may not work properly, and displays a shared secret mismatch error.

ACS Licensing Model

You must have a valid license to operate ACS; ACS prompts you to install a valid base license when you first access the web interface. Each server requires a unique base license in a distributed deployment.

For information about the types of licenses you can install, see Types of Licenses, page 18-33. For more information about licenses, see Licensing Overview, page 18-33.

Related Topic

- ACS Distributed Deployment, page 1-2

ACS Management Interfaces

This section contains the following topics:

- ACS Web-Based Interface, page 1-4
- ACS Command Line Interface, page 1-4
- ACS Programmatic Interfaces, page 1-5

ACS Web-Based Interface

You can use the ACS web-based interface to fully configure your ACS deployment, and perform monitoring and reporting operations. The web interface provides a consistent user experience, regardless of the particular area that you are configuring.

The ACS web interface is supported on HTTPS-enabled Microsoft Internet Explorer, versions 6.x, 7.x, and 8.x, and Firefox version 3.x.

The new web interface design and organization:

- Reflects the new policy model, which is organized around the user's view of policy administration. The new policy model is easier to use, as it separates the complex interrelationships that previously existed among policy elements.

  For example, user groups, network device groups (NDGs), network access filters, network access profiles, and so on.

- Presents the configuration tasks in a logical order that you can follow for many common scenarios.

  For example, first you configure conditions and authorizations for policies in the Policy Elements drawer, and then you move on to the Policies drawer to configure the policies with the defined policy elements.

- Provides new page functionality, such as sorting and filtering lists of items.

See "Using the Web Interface" section on page 5-3 for more information.

Related Topics

- ACS Command Line Interface, page 1-4

ACS Command Line Interface

You can use the ACS command-line interface (CLI), a text-based interface, to perform some configuration and operational tasks and monitoring. Access to the ACS-specific CLI requires administrator authentication by ACS 5.2.

You do not need to be an ACS administrator or log into ACS 5.2 to use the non-ACS configuration mode. ACS configuration mode command sessions are logged to the diagnostics logs.

ACS 5.2 is shipped on the Cisco 1121 Secure Access Control System (CSACS 1121). The ADE-OS software supports these command modes:

- EXEC—Use these commands to perform system-level operation tasks. For example, install, start, and stop application; 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. Such commands are specifically mentioned in the documentation

- ACS configuration—Use these commands to set the debug log level (enable or disable) for the ACS management and runtime components, and show system settings.

- Configuration—Use these commands to perform additional configuration tasks for the appliance server in an ADE-OS environment.

Note The CLI includes an option to reset the configuration that, when issued, resets all ACS configuration information, but retains the appliance settings such as network configuration.

For information about using the CLI, see the *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.2*.

Related Topic

- ACS Web-Based Interface, page 1-4

ACS Programmatic Interfaces

ACS 5.2 provides web services and command-line interface (CLI) commands that allow software developers and system integrators to programmatically access some ACS features and functions. ACS 5.2 also provides you access to the Monitoring & Report Viewer database that you can use to create custom applications to monitor and troubleshoot ACS.

The UCP web service allows users, defined in the ACS internal database, to first authenticate and then change their own password. ACS exposes the UCP web service to allow you to create custom web-based applications that you can deploy in your enterprise.

The Monitoring & Report Viewer web services allow you to create custom applications to track and troubleshoot events in ACS.

You can develop shell scripts using the CLI commands that ACS offers to perform create, read, update, and delete (CRUD) operations on ACS objects. You can also create an automated shell script to perform bulk operations.

For more information on how to access these web services and their functionalities, see http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/sdk/sdkguide.html.

Hardware Models Supported by ACS

Table 1-2 shows the details of the CAM hardware models supported by ACS 5.2.

Table 1-2 CAM Hardware Models Suppported by ACS 5.2

Config	HDD	RAM	NIC
IBM 1121	2 x 250GB	4GB	4X10,100,1000 RJ-45
CAM25-1-2-4.	2 x 250GB	4 x 1GB	2 x 1GE
VMWare ESX 3.5 or 4.0	500GB	4GB	2 NICs
VMWare Server 2.0	60GB	4GB	1 or 2 virtual NICs