CHAPTER 1

ACS 5.2 Deployment Overview

The ACS 5.2 deployment model similar to ACS 4.x, consists of a single primary and multiple secondary ACS servers, where configuration changes are made on the primary ACS server. These configurations are replicated to the secondary ACS servers.

All primary and secondary ACS servers can process AAA requests. The primary ACS server is also the default log collector for the Monitoring and Report Viewer, although you can configure any ACS server to be the log collector.

Although you can manage with a single ACS server, we recommend that you have two or more ACS servers, to provide AAA request processing redundancy. ACS 5.2 provides syslog support for external logging, and interfaces for automated and batch configuration provisioning.

An ACS deployment can scale for increased AAA request processing capacity by adding secondary servers. In large deployments, the secondary servers can be dedicated for specific functions. For example, you can use the primary ACS server only for configuration changes and not for processing AAA requests. You can designate a secondary ACS server only as the log collector.

In large environments, you can use load balancers to distribute AAA requests among the ACS servers in the deployment, simplify AAA client management, and provide high availability.

ACS servers are typically placed in the data centers or close to user clusters, for example, at regional sites.

For additional deployment information, refer to Understanding the ACS Server Deployment in the *Installation and Upgrade Guide for the Cisco Secure Access Control System 5.2*.

Table 1-1 describes the various ACS server roles.

Table 1-1 ACS Server Roles

ACS Server Roles	Role Descriptions
Primary	The configuration changes performed on the primary ACS server are replicated to all the secondary ACS servers in the deployment. At a time, you can have only one ACS server as the primary server.
Secondary	All ACS servers that receive configuration changes from the ACS primary server, are secondary servers.
Log Collector	The ACS primary or secondary server that is also the log collector for the Monitoring and Report Viewer. There can only be one log collector in a deployment. Other ACS deployments (servers not synchronized with this deployment) cannot send ACS logs to this server.

The following sections describe the deployment differences between ACS 4.x and ACS 5.2, and some considerations when deploying ACS 5.2:

Windows Versus Linux Based Application

ACS 3.x and 4.x releases are available as Windows-based applications that can be installed on a Windows server platform. These applications are also available on an appliance called the ACS Solution Engine. This appliance is a hardware platform that is preloaded with ACS and Windows operating systems.

ACS 5.2 is a Linux flavour application and is packaged with a Linux operating system. The application and the operating system package are shipped on an appliance and can also be installed in a virtual machine on a VMware ESX Server.

There are functional and deployment differences between ACS for Windows and the ACS Solution Engine, but there is no functional difference between the ACS 5.2 hardware appliance and the ACS 5.2 installed on a virtual machine. Deployments that consists of ACS 5.2 hardware appliances and ACS 5.2 virtual machines, are also supported.

Replication

ACS 3.x and 4.x provide a loose replication model. The characteristics of the ACS 3.x and 4.x replication model are:

- The configuration blocks represent logical areas of ACS configuration. For example, users and usergroups, usergroups only, network devices, distribution table, interface configuration, interface security settings, password validation settings, EAP-FAST settings, network access profiles, and logging configuration.
- The option to replicate one or more of the configuration blocks from the primary to secondary server.
- The whole block is replicated, regardless of the size of the configuration change.
- Cascading replication, which is the ability for a secondary ACS server to push a replication update to another ACS server.
- Replication can be initiated manually or according to a schedule.
- TACACS+ password updates are received on the primary server only.

In this loose replication model, the replicated blocks are synchronized between the primary and secondary servers, but other parts of the configuration can be different and tailored for the local environment.

The ACS 5.2 replication model is simple, efficient, and robust. The characteristics of the ACS 5.2 replication model are:

- Full synchronization between the primary and secondary servers.
- Transparent and immediate replication.
- Only configuration changes are replicated.
- Configuration changes can be made only on the primary server.
- No cascading replication.
- Automatic recovery for missed updates.
- Ability to promote a secondary server to primary server.
- TACACS+ password updates can be received on any ACS instance.

Region-specific access policy must be implemented in the ACS 5.2 network access policy configuration. This is because ACS 5.2 configuration is fully synchronized between the primary and secondary servers, and configuration changes cannot be made directly to the secondary servers.

Identity Stores

The main difference related to identity store support between ACS 3.x and 4.x and 5.2, is that ACS 5.2 does not support ODBC for authentication to databases, and proxy forwarding of TACACS+ requests. ACS 5.2 supports the following identity stores for authentication:

- ACS internal store
- Active Directory
- LDAP directories
- One-time password servers, using the
  - RSA SecurID interface
  - RADIUS interface
- Proxy forwarding to other stores through RADIUS (RADIUS proxy)

Logging

In ACS 5.2, the Monitoring and Report Viewer functionality is part of ACS. In an ACS 5.2 deployment, an ACS server is designated as the log collector for the reporting and monitoring functionality. All the other ACS servers send log messages to the designated log collector.

ACS supports syslog for logging to external servers.

ACS 5.2 provides a web service interface for the Cisco Wireless Control System (WCS) to obtain user authentication information from the Monitoring and Report Viewer.

Configuration

In ACS 5.2, the primary mode for configuration is a web-based user interface. ACS 5.2 also has a command-line interface (CLI) through which system tasks and file-based configuration updates can be made.

You can access the CLI from the console port, keyboard, video, mouse (KVM), and SSH. A web-service interface is provided to develop password change applications for internal ACS users.

Table 1-2 provides the number of internal users and network devices supported by ACS. Users and network devices are the commonly used and largely populated ACS objects.

Table 1-2 Internal Users and Device Configuration Capacity

ACS Object	Configuration Capacity
Internal Users	300,000
Network Devices	50,000

Licensing

The 3.x and 4.x releases of ACS did not require application of the key or license files. However, you need to apply a license file for the 5.x releases. The ACS 5.2 licenses are available at: http://cisco.com/go/license

Table 1-3 lists the available ACS 5.2 licenses.

Table 1-3 Available ACS 5.2 Licenses

License	Description
Base Server	One for each ACS instance.
Large Deployment	One for each ACS deployment when the network device count (based on IP address) in ACS exceeds 500. Configuring the Default Network Device contributes to the device count.

Server Deployment Recommendations

Table 1-4 describes the component mapping from ACS 3.x and 4.x to ACS 5.2.

Table 1-4 Component Mapping

ACS 3.x and 4.x Component	ACS 5.2 Component	Notes
ACS for Windows	VM in VMware ESX or 1120/1121 appliance	There is no ACS 5.2 Windows option. ACS 5.2 is an application that can run on a VMWare or supported appliance.
ACS Solution Engine (1111, 1112, 1113)	VM in VMware ESX or 1120 or 1121 appliance	ACS 1111, 1112 and 1113 platforms do not support ACS 5.2. ACS 4.2 can run on the 1120.
ACS Remote Agent	N/A	Remote Agent is not required in ACS 5.2
ACS View 4.0	VM in VMware ESX or 1120/1121 appliance	ACS 5.2 has built-in ACS View functionality.

Deployment guidelines for ACS 5.2:

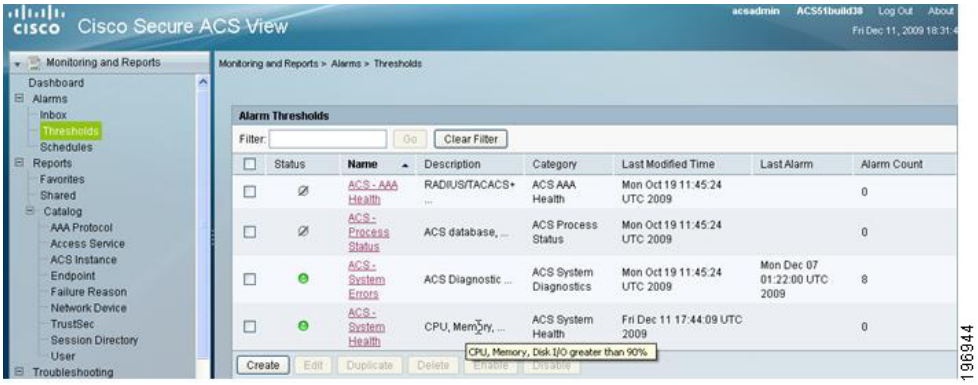
- In most cases, a one-to-one ACS server replacement is appropriate.

  The authentication performance of ACS 5.2 is same as the previous versions.
- Deploy at least two ACS instances to provide redundancy.
- Add more ACS servers to scale the authentication performance.

  Ensure that a single ACS server can handle peak authentication rates of its AAA clients and any AAA clients that rely on it as a backup AAA server.
- You can use secondary ACS servers to process AAA requests only to scale a deployment environment. Use the primary for configuration updates and log collection only.

  Use the most powerful hardware for the log collector. For example, the 1121 appliance over the 1120 appliance.
- Use load balancers to receive AAA requests, simplify AAA client management, improve resiliency, and better utilize ACS authentication capacity.
- Monitor the on-going resource utilization. You can do this by enabling the ACS system health alarm threshold in the Monitoring and Report Viewer as shown in Figure 1-1.

Figure 1-1 Alarm Threshold in ACS 5.2



Performance

A single ACS 5.2 server that does not act as the log collector can process more than 100 authentications per second. You should make sure that a single ACS server processing AAA requests is able to manage the load during peak hours. Peak hours typically occur when users arrive to work, or when network equipment reboots. This creates a large amount of authentications requests.

For example, 50,000 employees of a company log on to a network evenly, over a fifteen minute period. This translates to approximately 56 authentications per second as the peak authentication rate. In this case, a single ACS server which does not act as the log collector, can support this peak authentication rate.

Table 1-5 shows the number of authentications a single ACS server can support for different time periods, assuming a minimal rate of 100 authentications per second.

Table 1-5 Authentications Over Different Time Periods

1 second	100 authentications
60 seconds	6000 authentications
5 minutes	30000 authentications
15 minutes	90000 authentications
1 hour	360000 authentications

There are many factors that affect ACS authentication performance, such as configuration size, policy complexity, communication with external servers and authentication protocol complexity.

Table 1-6 lists the ACS performance for different authentication environments. This performance data represents the lower range of authentication rates observed while testing ACS with complex configurations. The performance is higher for simpler configurations.

Table 1-6 The Lower Range of ACS 5.2 Authentication Performance, in Authentications per Second

Authentication Types	Identity Stores		
	Internal	AD	LDAP
PAP	500	100	800
CHAP	500	500	N/A
TACACS+	400	160	1200
MSCHAP	500	300	N/A
PEAP-MSCHAP	200	100	N/A
PEAP-GTC	200	100	300
EAP-TLS	200	180	270
LEAP	330	280	N/A
FAST-MSCHAP	120	120	N/A
FAST-GTC	130	110	190
MAC-Auth Bypass	750	N/A	2000

Note The above numbers assume fast reconnect and session resume is in use for the applicable EAP methods.

There is an approximate 50% drop in authentication performance if the ACS server is also being used as the log collector for the Monitoring and Report Viewer.

There is an approximate 10% to 15% increase in performance, on the CSACS 1121 appliance than the numbers shown in Table 1-6.

Performance on a virtual machine is slower than on an actual 1120 appliance because of the virtual machine overhead. Performance of a virtual machine increases when you increase the CPU resources.

For virtual machine environments, the minimum requirements are similar to the 1121 appliance. For more information on virtual machine environments, refer to the *Installation and Upgrade Guide for the Cisco Secure Access Control System*.