Understanding the ACS Server Deployment

This chapter provides an overview of possible ACS server deployments and their components.

This chapter contains:

- Deployment Scenarios, page 1
- Understanding the ACS Server Setup, page 5

Deployment Scenarios

This section describes three deployment scenarios in which ACS might be used:

- Small ACS Deployment, page 1
- Medium ACS Deployment, page 2
- Large ACS Deployment, page 3

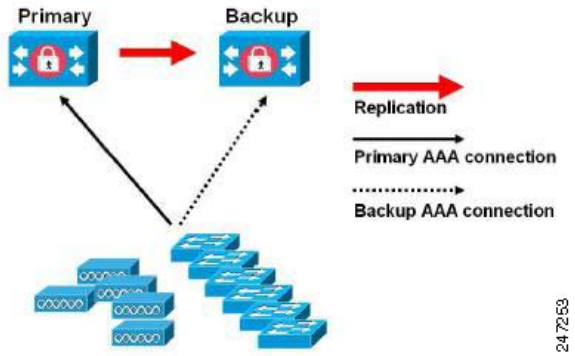
Small ACS Deployment

The most basic ACS deployment consists of two servers; see Figure 1 on page 1. One is the primary server that provides all of the configuration, authentication, and policy requirements for the network.

The second server is used as a backup server if the connectivity is lost between the AAA clients and the primary server. You use replication from the primary ACS server to the secondary server to keep the secondary server in synchronization with the primary server.

In a small network, this configuration allows you to configure the primary and secondary RADIUS or TACACS servers on all AAA clients in the same way.

Figure 1 Small ACS Deployment



As the number of users and AAA clients increases in an organization, Cisco recommends changing the deployment ACS from the basic design and using split ACS deployment design; see Figure 2 on page 2.

Split ACS Deployment

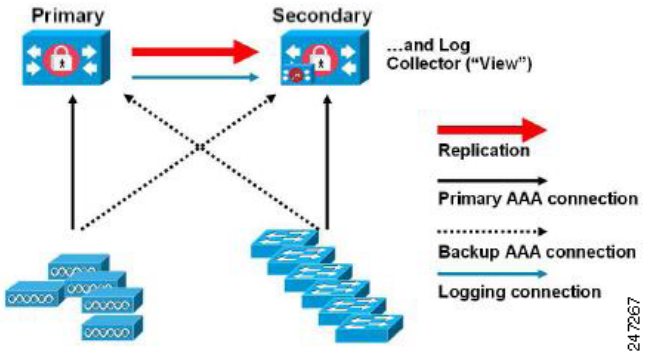
In split ACS deployment, you use primary and secondary servers as in a small ACS deployment, but the AAA load is split between the two servers to optimize AAA flow. Each server handles the full workload of both servers if there is a AAA connectivity problem, but during normal operations, neither server carries the full load of authentication requests.

This property of the servers allows for less stress on each ACS system, provides better loading, and makes you aware of the functional status of the secondary server through normal operations.

Another advantage of this arrangement is that each server can be used for specific operations, such as device administration and network admission, but can still be used to perform all the AAA functions in the event of a failure.

With two ACS systems now processing authentication requests and collecting accounting data from AAA clients, Cisco recommends using one of the systems as a log collector. Figure 2 on page 2 shows the secondary ACS server as the log collector.

Figure 2 Split ACS Deployment

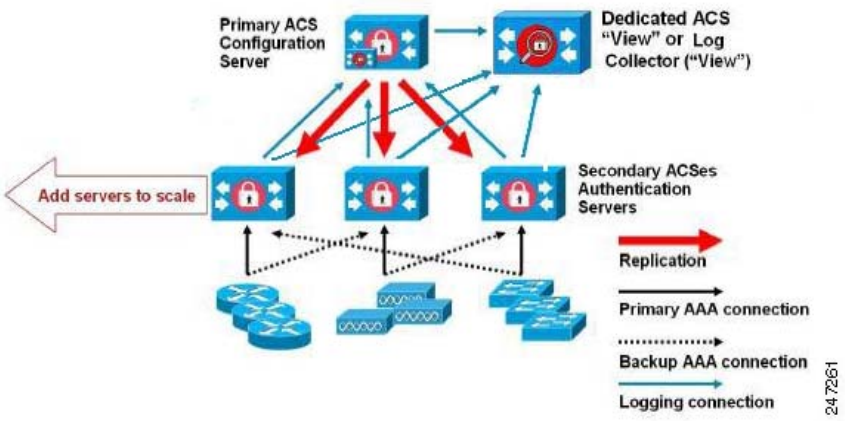


Another advantage of this design is that it also allows for growth as shown in Figure 3 on page 3.

Medium ACS Deployment

As the local network grows, you need to add more ACS servers to the system. In this scenario, you should consider promoting the primary server to perform configuration services and using the secondary servers for AAA functions. When the amount of log traffic increases, you should use one of the secondary servers as a centralized dedicated log collector server. ACS 5.8 supports one additional ACS instance in a deployment. The ACS 5.8 medium deployment supports 14 ACS instances. You can designate this additional ACS instance as a dedicated instance that can be promoted to a primary instance when the actual primary instance goes down.

Figure 3 Medium ACS Deployment



Large ACS Deployment

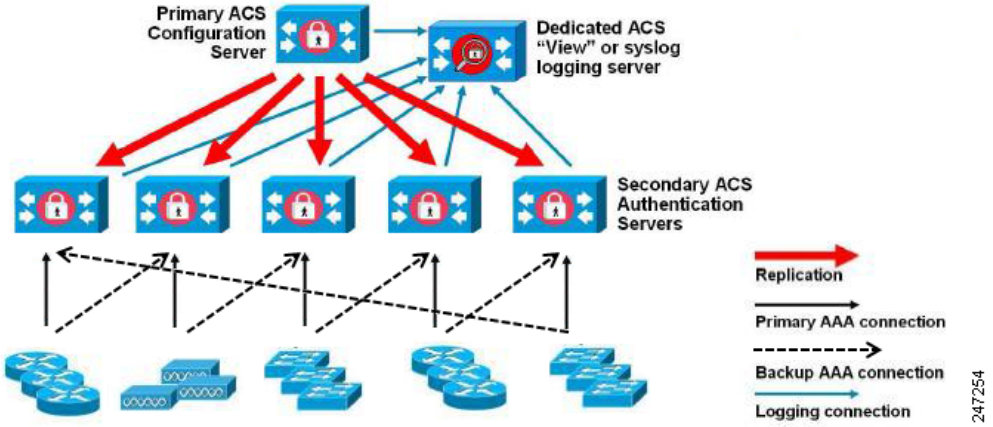
In a large ACS deployment, as shown in Figure 4 on page 4, centralized logging is highly recommended. ACS 5.8 supports one additional ACS instance in a deployment. The ACS 5.8 large deployment supports 22 ACS instances. You can designate this additional ACS instance as a dedicated instance that can be promoted to a primary instance when the actual primary instance goes down. Cisco recommends a dedicated logging server (Monitoring and Report server) because of the potentially high syslog traffic that a busy network can generate. Because ACS generates syslog messages for outbound log traffic, any RFC-3164-compliant syslog server will work to collect outbound logging traffic.

This type of server enables you to use the reports and alerts features that are available in ACS for all ACS servers. This requires special licensing, which is discussed in the User Guide for Cisco Secure Access Control System 5.8. See Installing the ACS Server, page 2, for more information on installing the ACS server.

You should also consider having the servers send logs to both a Monitoring and Report server and a generic syslog server. The addition of the generic syslog server provides a backup if the Monitoring and Report server goes down.

Note: ACS 5.8 does not support large deployments with more than 22 ACS instances.

Figure 4 Large ACS Deployment



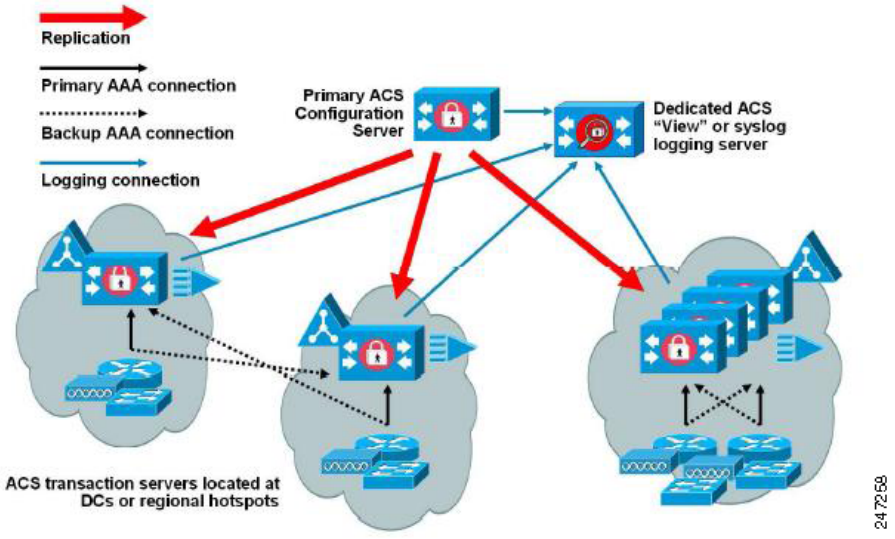
Dispersed ACS Deployment

A dispersed ACS deployment is useful for organizations that have campuses located throughout the world. There may be a home campus where the primary network resides, but there may be additional LANs, sized from small to large, in campuses in different regions.

To optimize AAA performance, each of these remote campuses should have its own AAA infrastructure. See Figure 5 on page 4. The centralized management model should still be used to maintain a consistent, synchronized AAA policy.

A centralized-configuration, primary ACS server and a separate Monitoring and Report server should still be used. However, each of the remote campuses will have unique requirements.

Figure 5 Dispersed ACS Deployment



Some of the factors to consider when planning a network with remote sites are:

- Check whether there is a central or external database (Microsoft Active Directory [AD] or Lightweight Directory Access Protocol [LDAP]) in use. For the purposes of optimization, each remote site should have a synchronized instance of the external database available for ACS to access.

- The location of the AAA clients is also a major consideration. You should place your ACS servers as close as possible to the AAA clients to reduce the effects of network latency and the possibility of loss of access caused by WAN failure.
- ACS has console access for some functions, such as backup. Consider using a terminal at each site. This allows for secure console access outside of network access to each server.
- If small, remote sites are in close proximity and have reliable WAN connectivity to other sites, you may consider using an ACS server in a nearby site as a backup server for the local site for redundant configuration.
- DNS should be properly configured on all ACS nodes to ensure access to the external databases.

Understanding the ACS Server Setup

This section briefly describes the roles of various ACS servers and how to configure them. For more information on assigning a role to a server and configuring it, see the *User Guide for Cisco Secure Access Control System 5.8.*

This section contains:

- Primary Server, page 5
- Secondary Server, page 5
- Logging Server, page 6

The installation procedure is similar for any ACS server.

See Installing and Configuring the Cisco Secure Access Control System with CSACS-1121, page 1 for installing ACS with the CSACS-1121 appliance, Installing and Configuring the Secure Access Control System with the Cisco SNS-3415 and Cisco SNS-3495, page 1 for installing ACS with the Cisco SNS-3415 appliance, or Installing ACS in a VMware Virtual Machine, page 1 for installing ACS with VMware ESX. In an ACS deployment, ensure that you first install a primary server.

Primary Server

In an ACS deployment, only one instance serves as an ACS primary, which provides the configuration capabilities and serves as the source for replication.

On an ACS primary server, you can set up all the system configurations that are required for an ACS deployment. However you must configure licenses and local certificates individually for each ACS secondary server.

Secondary Server

Except the primary server, all the other instances function as a secondary server.

A secondary ACS server receives all the system configurations from the primary server, except that you need to configure the following on each secondary server:

- License—Install a unique base license for each of the ACS secondary servers in the deployment.
- New local certificates—You can either configure the local certificates on the secondary servers or import the local certificates from the primary server.
- Logging server—You can configure either the primary server or the secondary server to be the logging server for ACS. Cisco recommends that you configure a secondary ACS server as the logging server.

Note: You cannot translate a network address between the primary and secondary servers when selecting the installation location for the secondary server.

The secondary server must be activated to join the ACS environment. The administrator can either activate a secondary server or set up automatic activation. By default, the activation is set to Automatic.

After the secondary server is activated, it is synchronized with the configuration and replication updates from the primary server.

Logging Server

Either a primary server or one of the secondary servers can function as a logging server.

The logging server receives the logs from the primary server and all the ACS secondary servers in the deployment. Cisco recommends that you allocate one of the ACS secondary servers as the Monitoring and Report server and exclude this particular secondary server from the AAA activities.

The three main logging categories are Audit, Accounting, and Diagnostics.

For more details on logging categories and configuration, see the *User Guide for Cisco Secure Access Control System 5.8*.