

Secure Access Control Server (ACS) Database Migration

Document ID: 98760

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

ACS Database Migration

- Migrate the ACS Database for Windows to ACS Solution Engine

- Migrate the ACS Database for Windows to Another Windows Server

Verify

Troubleshoot

Related Information

Introduction

This document describes how to migrate the database from an Access Control Server (ACS) that runs on a Windows server to a Cisco ACS Solution Engine (ACS SE) or another Windows server.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Secure Access Control Server (ACS) that runs software version 3.x or later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

ACS Database Migration

Migrate the ACS Database for Windows to ACS Solution Engine

Migration from ACS for Windows to ACS Solution Engine uses the ACS backup and restore features. ACS for Windows produces backup files that are compatible with ACS Solution Engine, provided that both use the same version of the ACS software.

The migration process depends on which version of ACS for Windows you use and the operating system on which it runs. For example, if ACS runs on Windows NT 4.0, the procedure in this section advises you when it is necessary to upgrade to Windows 2000 Server. Because the use of the backup and restore features is supported only between ACS applications of the same version, you must use ACS for Windows version 4.0 in order to transfer data from ACS for Windows to ACS Solution Engine. ACS for Windows version 4.0 supports Windows 2000 Server and Windows Server 2003, but not Windows NT 4.0.

Note: Before you upgrade or transfer data, back up your original ACS and save the backup file in a location on a drive that is not local to the computer that runs ACS.

Complete these steps in order to migrate from a Windows version of ACS to ACS Solution Engine:

1. Complete the steps in the Installation and Setup Guide for Cisco Secure ACS Solution Engine 4.0 in order to set up the appliance.
2. Upgrade ACS for Windows to version 4.0.
 - ◆ If you do not have a license for version 4.0, you can use the trial version, which is available from Cisco Software Download (registered customers only).
 - ◆ If you run ACS on Windows NT 4.0, upgrade to ACS version 3.0, and then migrate to Windows 2000 Server before you upgrade to ACS version 4.0. ACS version 4.0 does not support Windows NT 4.0. ACS version 3.0 is the most recent version of ACS that supports Windows NT 4.0. For information about how to upgrade to ACS version 3.0 and how to migrate to Windows 2000 Server, see *Installing Cisco Secure ACS 3.0 for Windows 2000/NT Servers*. You can download the trial version from Cisco Software Download (registered customers only).
3. In the HTML interface of ACS for Windows version 4.0, use the ACS Backup feature in order to back up the database. For more information, refer to the ACS Backup section of the *User Guide for Cisco Secure ACS for Windows 4.0*.
4. Copy the backup file from the computer that runs ACS for Windows version 4.0 to a directory on an FTP server. The directory must be accessible from the FTP root directory. ACS Solution Engine must be able to contact the FTP server. Any gateway devices must permit FTP communication between the appliance and the FTP server.
5. In the HTML interface of ACS Solution Engine, use the ACS Restore feature in order to restore the database. For more information, refer to the ACS System Restore section of the *User Guide for Cisco Secure ACS Solution Engine 4.0*.

The ACS Solution Engine contains the original configuration of the Windows version of ACS from which you migrated.

6. In the HTML interface of the ACS Solution Engine, verify the settings are correct for the (Default) entry in the Proxy Distribution Table. Choose **Network Configuration > (Default)**, and ensure that the Forward To list contains the entry for the appliance.
7. If you want to replace the computer that runs ACS for Windows with ACS Solution Engine, you must change the IP address of the appliance to the IP address of the computer that runs ACS for Windows.

Note: If you do not change the IP address of the ACS Solution Engine to the address of the computer that runs ACS for Windows, you must reconfigure all AAA clients to use the IP address of the ACS Solution Engine.

In order to change the IP address of the ACS Solution Engine, complete these steps:

- a. Record the IP address of the computer that runs ACS for Windows.
- b. Change the IP address of the computer that runs ACS with Windows to a different IP address.
- c. Change the IP address of the ACS Solution Engine to the IP address previously used by the computer that runs ACS for Windows. This is the IP address that you recorded in the step **a**.

Migrate the ACS Database for Windows to Another Windows Server

In this procedure, you migrate the database of ACS 3.0.4 that runs on Windows NT Server to another ACS 3.3.3 that runs on Windows 2003 Server.

1. In the HTML interface of ACS for Windows version 3.0.4, use the ACS Backup feature in order to back up the database.
2. Copy the backup file from the server that runs ACS for Windows version 3.0.4 to a directory on an FTP server. The directory must be accessible from the FTP root directory. ACS 3.3.3 for Windows must be able to contact the FTP server. Any gateway devices must permit FTP communication between the appliance and the FTP server.
3. Upgrade the operating system (OS) from Windows NT to Windows 2000 SP4 on this machine.
4. Install again ACS 3.0.4 on this machine.
5. Restore the backup configuration on this Windows 2000 machine.
6. Upgrade to ACS 3.3.3 on the same server. Ensure you check the **keep the existing configuration** option.
7. After you upgrade to ACS 3.3.3 on this server, backup again the current configuration.
8. If you have the exact version of ACS 3.3.3 running on the other server, restore the backup on the new server.

Note: In order to backup and restore data, both servers must run the same version of ACS.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

- If you want the ACS SE to use an external database, such as Microsoft Windows database or Active Directory (AD), in order to authenticate user access to AAA clients, such as routers, switches, and security appliances, install the ACS remote agent in the AD server and enable group mapping through the ACS.

For more information about how to install the remote agent, refer to Installing Cisco Secure ACS Remote Agent for Windows section of the Installation and Configuration Guide for Cisco Secure ACS Remote Agents 4.1.

For more information about how to configure group mapping, refer to the User Group Mapping and Specification section of the User Guide for Cisco Secure Access Control Server 4.1.

Note: The software version on the ACS server and the remote agent must be the same. For example, if your ACS SE runs software version 4.1, then you must use the remote agent version 4.1 in the AD. If the software versions are not the same, the configuration will not work, and you may receive this error message: *External DB user invalid or bad password*.

- **Problem:** Remote agent cannot authenticate Windows users accounts. You receive this error message in remote agent log:

```
NTLIB: Windows authentication FAILED (error 6L)
```

Cause: Insufficient privileges for the remote agent to perform authentication.

Resolution: Remote agent must be given the right permissions (select local admin rights) in order to communicate with ACS. In most cases, you can install the remote agent in the member server instead of the domain controller in order to resolve this issue.

Related Information

- [Cisco Secure Access Control Server for Windows Support Page](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 24, 2007

Document ID: 98760
