

Secure Access Control Server (ACS 3.x and 4.x) Troubleshooting

Document ID: 99449

Contents

Introduction

Prerequisites

Requirements

Components Used

Conventions

Problem: Resources needed by the CiscoSecure Install are locked

Solution

Problem: Cannot Delete AAA Server, AAA Server is a Synchronization Partner

Solution

Problem: 127.0.0.1 is a reserved address

Solution

Problem: Authentication failure for Nexus Switch

Solution

Problem: ACS 1113 SE – Unable to Assign Static IP Address

Solution

Problem: Primary Server is not Preempt

Solution

Problem: Cannot Set New NIC Configuration

Solution

Problem: ACS Folder is Locked by Another Application

Solution 1

Solution 2

Problem: Event Error

Solution

Problem: Bad request from NAS

Solution

Problem: Unable to install ACS version 3.3.3 on ACS 1113

Solution

Problem: Reason: is currently being edited elsewhere

Solution

Problem: Remote agent service will not start

Solution

Problem: "Error:Auth type not supported by External DB" during user authentication

Solution

Problem: Unable to enable ping to ACS

Solution

Problem: "Appliance upgrade in progress" message is shown even after the ACS upgrade is complete.

Solution

Problem : Password Reset after Replication

Solution

Problem: DST Issue on ACS

Solution

Problem: "Error: Failed to get NIC configuration: (null) (FFFFFFFF)" on ACS appliance

Solution

Problem: Unable to disable SSHv1 enable only SSHv2 on the ACS appliance

Solution

Problem: Unable to Reset ACS Appliance to Factory Default

Solution

Problem: Failed TACACS+ Authentication with ACS with the NDG Issue

Solution

Problem: Windows External Database not Operational

Solution

Problem: External DB user invalid or bad password

Solution

Problem: Error on ACS when accessed using IE8

Solution

Problem: Error "eap_peap type not configured"

Solution

Problem: Failure Reason : 24428 Connection related error has occurred in either LRPC, LDAP or KERBEROS

Solution

Problem: Unable to do local logging on Cisco Secure ACS Solution Engine instead of using the remote logging capability of the Cisco Secure ACS remote agent

Solution

Problem: How do you generate the complete list of all the users along with their current method of password authentication?

Solution

Problem: ACS is unable to control the delimiter of the mac-address

Solution

Problem : "Failed to export user database. Please check there is sufficient disk space then rerun setup. Set up will now exit."

Solution

Problem: ACS is unable to join the Active Directory domain and User unable to Authenticate

Solution

Problem: Could not generate valid password to perform the Auth test

Solution

Problem: Cannot login to Cisco ACS, All Administration ports are currently in use

Solution

Problem: ODBC operation failed with following information: message=[Sybase][ODBC Driver][Adaptive Server Anywhere].....

Solution

Problem: Unable to integrate ACS with Active Directory

Solution

Problem: CSCOacs_Internal_Operations_Diagnostics ERROR Could not start message bus

Solution

Problem: 13017 Received TACACS+ packet from unknown Network Device or AAA Client

Solution

Problem: Unable to delete Authentication History (RADIUS Successes or Failures) and the syslogs from the ACS

Solution

Problem: Management process in not running and shows "running (HTTP is nonresponsive)"

Solution

Problem: Can I use a secure ID token with SFTP to backup the ACS database?

Solution

Problem: Unable to filter the reports using Interactive Viewer

Solution

Problem: Authentication prompt appears only for the first connection and not for subsequent connections

Solution

Problem: Authorization prompt appears when using Apple devices with ACS

Solution

Problem: ACS Error Message – Not all user Active Directory groups are retrieved successfully...

Solution

Problem: ACS does not log proxy authentication requests

Solution

Problem: ACS loses the configuration when repository is created from the GUI

Solution

Problem: Unable to use an SSH session for the RADIUS IETF attribute "Login-Service"

Solution

Problem: Error "value too long (ACS Server Name,TacacsAuthentication), Alarm details is "Please see the collector log for details""

Solution

Problem: ACS 4.x local user password change does not work with IOS devices running SSH v1

Solution

Problem: Remote logging is not working for ACS 4.2

Solution

Related Information

Introduction

This document describes how to troubleshoot Cisco Secure Access Control Server (ACS) and resolve error messages.

For information on how to troubleshoot Cisco Secure Access Control System (ACS 5.x and later), refer to Secure Access Control System (ACS 5.x and later) Troubleshooting.

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) version 3.3 and 4.x.

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.

Problem: Resources needed by the CiscoSecure Install are locked

You can experience this problem when you upgrade your ACS server.

Solution

If you have too many old log files, you need to clear the "Local Logging Configuration" logs.

Modify the logging of ACS to keep the last three files.

1. On the ACS GUI, choose **System Configuration > Service Control**. Check the **Manage Directory** box and select to keep only the last three files. Then restart ACS and test the upgrade.
2. If option #1 does not work, you can try to manually remove some log files.

You must always copy the files to a dedicated folder before you delete them.

- a. On the local drive of the Windows server, where ACS for Windows is installed, choose Program Files > Cisco Secure ACS folder.

- b. Delete all the logs under each of these folders:

- ◇ * CSAuth
- ◇ * CSLog
- ◇ * CSDbsync
- ◇ * CSAdmin
- ◇ * CSRADIUS
- ◇ * CSTacacs
- ◇ * CSMon

- c. Restart the PC and retest the upgrade.

Problem: Cannot Delete AAA Server, AAA Server is a Synchronization Partner

The Cannot Delete AAA Server, AAA Server is a Synchronization Partner error message can appear when you delete the entry under **Network Configuration**.

Solution

Complete these steps in order resolve this issue:

1. Choose **Interface Configuration**, and check the **RDBMS Synchronization** check box
2. Choose **System Configuration > RDBMS Synchronization** and remove the AAA server that cannot be deleted from the AAA group that is on the Synchronization Partner
3. You can now delete the AAA server group.

Problem: 127.0.0.1 is a reserved address

You have two units of ACS SE 1113 and want to replicate the internal database from primary to secondary, but you notice this error message in the secondary unit:

```
Inbound database replication from ACS <secondary ACS unit name> denied - shared
secret mismatch
```

When you try to modify the key of AAA Server **Self** under **Network Configuration** the error message is returned.

AAA Server Setup for Self	
AAA Server IP Address	127.0.0.1
Key	new/any
<input type="checkbox"/> Log Handling/Watching Profiles from this remote AAA Server	
AAA Server Type	Radius ACS
Traffic Type	inbound/outbound
AAA Server RADIUS Authentication Port	1644
AAA Server RADIUS Accounting Port	1645
<input type="button" value="Submit"/> <input type="button" value="Submit & Apply"/> <input type="button" value="Cancel"/>	

AAA Client Update Errors	
Number	Error
1	127.0.0.1 is a reserved address

127.0.0.1 is a reserved address

Solution

In order to resolve the 127.0.0.1 self problem, you can backup and restore the .DMP files on a fresh installation of ACS for Windows 4.2 and modify the 127.0.0.1 entry with the desired IP address.

Note: Cisco bug ID CSCso36620 (registered customers only) states that the **toggle nic** command changes the AAA server IP address to **127.0.0.1** in the GUI. In order to restore the original IP address on the appliance, issue the **set ip** command.

Problem: Authentication failure for Nexus Switch

Nexus 5010 authentication does not work with TACACS+. This error message can also appear:

```
Message-Type : Authen failed
Authen-Failure-Code : Key Mismatch
```

Solution

The shared secret defined under the NDG takes precedence over the individually configured device. Look at the shared secret configured under the NDG **Century PROD FSW**, and make sure it matches with the one configured on Nexus switch.

Problem: ACS 1113 SE – Unable to Assign Static IP Address

This issue occurs when you are unable to configure the static IP address on ACS 1113 SE.

Solution

In order to resolve this issue, install the applACS-4.1-set-ip-CSCsm73656-Patch.zip patch, which is available from Cisco Downloads (registered customers only). The patch suits all ACS SE 4.1 versions.

Problem: Primary Server is not Preempt

When the primary ACS servers goes down, you authenticate users with the secondary server. When the primary is up again, your users are still authenticated against the secondary, even though the primary is running again.

Solution

By default, the ASA works in depletion mode. Change it to timed mode so that when the primary ACS server becomes active you can return the authentication to the primary.

You can use:

```
host(config)# aaa-server <tag> protocol radius
host(config)# reactivation mode timed
host(config)# aaa-server acsgroup deadtime 0
```

Optional: Specify the amount of time in minutes with the deadtime, between zero and 1440, that elapses between when the last server in the group is disabled and when all the servers are re-enabled. The default is ten minutes.

Problem: Cannot Set New NIC Configuration

This issue occurs when you configure the static IP address on ACS 1113 SE.

Solution

In order to resolve this issue, try to reimage the software.

Problem: ACS Folder is Locked by Another Application

The ACS Folder is Locked by Another Application error message appears during an ACS software upgrade, such as the upgrade from version 3.3 to 4.0

Use these solutions in order to solve the problem.

Solution 1

Complete these steps:

1. In the ACS Window, check the **System Configuration > Service Control > Check the Manage Directory** check box.
2. Enter a value, such as **3**, in the **Keep only the last __ files** box.
3. Restart. The upgrade is likely to work.

Services Log File Configuration	
Level of detail	
<input type="radio"/>	None
<input checked="" type="radio"/>	Low
<input type="radio"/>	Full
Generate New File	
<input type="radio"/>	Every day
<input type="radio"/>	Every week
<input type="radio"/>	Every month
<input checked="" type="radio"/>	When size is greater than <input type="text" value="10240"/> KB
<input checked="" type="checkbox"/>	Manage Directory
<input checked="" type="radio"/>	Keep only the last <input type="text" value="3"/> files
<input type="radio"/>	Delete files older than <input type="text" value="7"/> days

Solution 2

If Solution 1 does not resolve the issue, complete these steps:

1. Backup the current ACS database.

Refer to the *Cisco Secure ACS Backup* section of User Guide for Cisco Secure ACS for Windows Server for more information on how to perform the backup of the ACS database.

2. Run the **clean.exe** file in order to uninstall ACS 3.3 (or your existing version). This file is located on the CD under ACS Utilities/support/clean.
3. Reinstall ACS 3.3 from the CD.
4. Restore your database from the file that you saved in Step 1.

Refer to the *Cisco Secure ACS System Restore* section of User Guide for Cisco Secure ACS for Windows Server for more information on how to restore the ACS database.

5. Upgrade the ACS to version 4.0.

Refer to Installation Guide for Cisco Secure ACS for Windows Server Version 4.0 for more information on upgrade procedures.

Problem: Event Error

During startup, the ACS SE receives the At least one service or driver failed during startup. use event viewer to examine the event log for details error message.

Solution

This error on the ACS SE does not affect any of the ACS functionalities. It is a Microsoft Windows error . This error appears because the monitor, mouse and keyboard cannot be used on the appliance and are disabled by default.

The ACS appliance is a hardened, locked-down system and is designed with security in mind. The appliance

uses windows strengthen image, which has all *redundant* services and connections stopped. It is made to keep all viruses, worms, and DDOS attackers out. Hence there is no VNC, DOS prompt, or any other way to reach the windows configuration. Services like the mouse, keyboard and monitor are closed.

On rare occasions, it indicates that something is corrupted on the appliance image. If you re-image the appliance, it fixes the issue in the majority of instances. You can try to re-image the ACS as well.

Problem: Bad request from NAS

This error message appears:

```
Bad request from NAS
OR
Authen-Failure-Code=Invalid message authenticator in EAP request
```

Solution

This error message usually appears because of a mismatch in the shared secret key or like in this case NDG defined with a key overriding the AAA client key.

Problem: Unable to install ACS version 3.3.3 on ACS 1113

Unable to install images earlier than version 4.0 on ACS SE 1113.

Solution

Only ACS 4.0 and later can run on ACS SE 1113. Refer to Upgrading and Migrating to Cisco Secure ACS Solution Engine for more information on how to upgrade ACS SE.

Problem: Reason: is currently being edited elsewhere

When you open the ACS page, you can receive this error: Reason: is currently being edited elsewhere..

Solution

Restart the ACS services in order to resolve this issue.

Problem: Remote agent service will not start

The user is not able to run the remote agent service.

Solution

The user must be a local admin user for the service to start.

Problem:"Error:Auth type not supported by External DB" during user authentication

The Auth type not supported by External DB error appears during user authentication.

Solution

This error appears because the CHAP Authentication protocol is not supported on the Microsoft Windows database Active Directory (AD) when you use ACS version 3.3. In order to resolve this issue, use PAP instead of CHAP. Refer to Authentication Protocol–Database Compatibility for more information on Protocol–Database Compatibility for ACS version 3.3.

Problem: Unable to enable ping to ACS

Unable to ping ACS SE.

Solution

Turn off the CSA Agent in **System Configuration** --> **Appliance Configuration** in order to enable ping response on ACS SE versions earlier to 4.2. For ACS versions 4.2 and later download and install the patch available from Cisco.com. Refer to Turning Ping On and Off for more information.

Problem: "Appliance upgrade in progress" message is shown even after the ACS upgrade is complete.

The `Appliance upgrade in progress` message appears, even after the ACS upgrade is complete.

Solution

ACS is struck after upgrade and cannot start or stop any services.

In order to resolve this issue, complete these steps:

1. Log into the ACS Appliance with a different Admin account.
2. On the Appliance Upgrade present under the System Configuration tab, press the **Refresh** or the **Download** button.

Refer to Cisco bug ID CSCsg89042 (registered customers only) for more information.

If you are unable to use the GUI, try to reboot the ACS appliance in order to resolve the issue.

Problem : Password Reset after Replication

After the replication, the new password gets reset to the old password.

Solution

This issue occurs because users do not authenticate to the primary ACS. Once the replication occurs, the primary pushes its policies to the secondary ACS because the replication is not bidirectional. This causes the password to be reset to the old password.

In order to resolve this issue, authenticate the user to the primary ACS, if possible.

Problem: DST Issue on ACS

DST issues are seen on ACS.

Solution

In order to resolve the Daylight Saving Time (DST) issue with ACS, download and install these patches:

1. applAcs-4.1.4.13.7-CSUpdate.zip
2. applAcs-4.1.4.13.7.zip

Note: Apply the **csupdate** patch first. Then install the cumulative patch.

Problem: "Error: Failed to get NIC configuration: (null) (FFFFFFFF)" on ACS appliance

The **Error: Failed to get NIC configuration: (null) (FFFFFFFF)** error appears on the ACS appliance.

Solution

This error usually appears if the right version of the ACS image is not used on ACS appliance. It is more of a compatibility issue. Re-image the ACS appliance in order to resolve this issue.

Refer to [Re-Imaging the Appliance Hard Drive](#) for more information on how to re-image the ACS appliance.

Problem: Unable to disable SSHv1 enable only SSHv2 on the ACS appliance

Unable to disable SSHv1 and leave only the SSHv2 enabled on the ACS appliance.

Solution

Right now it is not possible to disable SSHv1 and leave only SSHv2 enabled. Both SSHv1 and SSHv2 are enabled together and cannot be disabled individually.

Problem: Unable to Reset ACS Appliance to Factory Default

This section details what to do if you are unable to reset the ACS appliance to factory default settings.

Solution

The **acs reset-config** command includes an option to reset the configuration that, when issued, resets all ACS configuration information, but retains the appliance settings such as network configuration. If you want it to look exactly like the factory default, you need to re-image the appliance.

Problem: Failed TACACS+ Authentication with ACS with the NDG Issue

This section explains why authentication fails with TACACS+ when a Network Device Group (NDG) is configured..

Solution

The same AAA client is mapped to two different NDGs, one as a RADIUS client and the other as a TACACS client, and NDG level external database authentication is enabled for the NDG with the RADIUS client.

TACACS+ users are configured in the ACS internal database. When the TACACS+ authentication request comes, ACS looks in the NDG, where the same client is configured as RADIUS.

In order to avoid this problem, remove the external database authentication check box from the RADIUS NDG.

Problem: Windows External Database not Operational

This section explains why some user authentication fails with external a database not operational error.

Solution

Here is a list of possible causes and their solutions:

- The Remote Agent (RA) version does not match the ACS version. Install the correct version of RA.
- The Remote Agent services are stopped. Restart the RA services.
- Upgrade the ACS to the latest available version.

Problem: External DB user invalid or bad password

This section explains why you receive the External DB user invalid or bad password error for authentication on ACS.

Solution

Review these troubleshooting tips in order to resolve this issue:

- If any changes related to the AD membership or the system name are made on the ACS server, make sure to reboot it for changes to take effect.
- Check the connectivity between the ACS and the Domain Server.
- Security policies on the Domain Server must allow the ACS to Query Username on the Active Directory.
- Make sure that there is a two-way trust that exists between the ACS and the Domain Server.
- Make sure that the ACS is installed on a server that has Local and DomainAdmin Privileges.
- Make sure the username and password is correct.

Problem: Error on ACS when accessed using IE8

```
The faultCode:Server.Error.Request faultString:'HTTP request error'  
faultDetail:'Error: [IOErrorEvent type="ioError" bubbles=false  
cancelable=false eventPhase=2 text="Error #2032"]'. URL:  
/acsview/LoadAuthenticationTrendsPortlet.do' error occurs on the ACS when the ACS is  
accessed using Internet Explorer 8 (IE8).
```

Solution

This error occurs because IE8 is not supported by ACS. Use another browser in order to resolve this issue.

Problem: Error "eap_peap type not configured"

The `eap_peap type not configured` error occurs on the ACS when you attempt to perform a wireless authentication.

Solution

This error occurs on the ACS due to one of these reasons:

1. The supplicant requesting for EAP-PEAP authentication is not configured on the ACS. Enable EAP-MSCHAPv2 and EAP-GTC from the Global Authentication page, and disable NAP on the primary server in order to resolve the issue.
2. When a wireless user tries to authenticate through the ACS server, the login fails and the error message is **EAP_PEAP Type not configured**. This occurs when authenticating with a user configured in the Microsoft Windows AD database, as well as when authenticating with a user in the local ACS database.
3. When the WLC uses key-wrap for FIPS, but the ACS has not been configured for the same. Configure the same on the ACS in order to resolve the issue.

Problem: Failure Reason : 24428 Connection related error has occurred in either LRPC, LDAP or KERBEROS

This error message is received on the ACS:

```
Failure Reason : 24428 Connection related error has occurred in either
LRPC, LDAP or KERBEROS This RPC connection problem may be because the
stub received incorrect data
```

Solution

In order to resolve this issue, upgrade the ACS to version 5.2.

Problem: Unable to do local logging on Cisco Secure ACS Solution Engine instead of using the remote logging capability of the Cisco Secure ACS remote agent

The issue is the inability to perform local logging on the Cisco Secure ACS Solution Engine instead of using the remote logging capability of the Cisco Secure ACS remote agent.

Solution

It is possible to perform local logging on the Cisco Secure ACS Solution Engine instead of using the remote logging capability of the Cisco Secure ACS remote agent. However, local logging on the Cisco Secure ACS Solution Engine is constrained in size. This forces log files to be recycled after seven days. The Cisco Secure ACS remote agent provides full, unconstrained logging capability to a remote server.

Problem: How do you generate the complete list of all the users along with their current method of password authentication?

With ACS 4.2, the users are authenticated by different methods such as Windows/LDAP/OTP. Is there a way to prepare a complete list of the users with their password authentication methods?

Solution

This is time-consuming if performed manually. There is a way to perform this automatically with ACS release 4.2.1.15.

Complete these steps:

1. Take the backup of the ACS internal database.
2. Run the **CSUtil.exe -dumpUSERS** command.

This generates a text file "userauditinfo.txt" that contains the password authentication method used for all the available users.

Problem: ACS is unable to control the delimiter of the mac-address

The ACS is unable to control the delimiter of the mac-address. The delimiter cannot be changed or added.

Solution

The ACS is not designed to control the delimiter of the mac-address and it cannot change or add delimiter. The client or the WLC controls the delimiter.

Problem : "Failed to export user database. Please check there is sufficient disk space then rerun setup. Set up will now exit."

The problem is the backup database cannot be restored when upgrading the ACS for Windows. An insufficient disk space error message is received.

Solution

Complete this workaround:

1. Collect a backup from your database.
2. Uninstall the ACS software by using the clean utility which is available on the FULL packages of the installation files of the ACS version.
3. Reinstall the software with the same version.
4. Perform a restore of the database.
5. Upgrade the ACS version again.

Problem: ACS is unable to join the Active Directory domain and User unable to Authenticate

The ACS cannot join the Active Directory domain and the user cannot authenticate. A clock skew error is received.

Solution

This issue can be resolved by changing the time–zone and time on the ACS to match the time–zone and time on the Active Directory.

Problem: Could not generate valid password to perform the Auth test

The Could not generate valid password to perform the Auth test error message appears on the ACS.

Solution

In order to resolve this issue, go to **System Configuration** and click **Local Password Management**. Make sure the password length is not more than 9 characters. If it is then make sure to change the length to between 4 and 8 characters.

Problem: Cannot login to Cisco ACS, All Administration ports are currently in use

When authenticating as an administrator, a successful message is received. Then, you are quickly forwarded to a page that shows `Cannot login to CiscoSecure ACS, all Administration ports are currently in use`. Contact the System Administrator for more details. This occurs in ACS 4.X.

Solution

This error message indicates that the range of ports allocated for GUI auto redirect are totally reserved and being used by others. In order to resolve this, complete this procedure:

1. Stop the `csadmin` service and then try to login.
2. Verify the HTTP port allocation policy for the Administrator. The complete path is shown here:

Administration Control > Access Policy > HTTP port Allocation > Restrict Administration Sessions to the following port range From Port n to Port n

3. Increase the range of the ports as per the requirement. For more information, refer to HTTP Configuration.
4. Specify a lesser *Session idle–time–out* in the *Session Policy*. The complete path is shown here:

Administration Control > Session Policy > Session idle timeout

For more information, refer to Session Policy.

5. Sometimes, reloading the ACS can also help to resolve this issue.

Problem: ODBC operation failed with following information: message=[Sybase][ODBC Driver][Adaptive Server Anywhere].....

This error is received on ACS version 4.X: ODBC operation failed with following information: message=[Sybase][ODBC Driver][Adaptive Server Anywhere].....

Solution

ACS version 4.0 does not install properly if the Sybase server is installed on the same machine. In certain cases, when CiscoWorks and the ACS are used on the same machine, this error message appears and ACS installation problems arise. This occurs because CiscoWorks uses the Sybase for a database. In order to avoid this error, you need to ensure there is no other application that uses SQL Anywhere on that PC in order to successfully install the software. Refer to the Notes section in Preparation for Install or Upgrade ACS for more information.

Problem: Unable to integrate ACS with Active Directory

Unable to integrate ACS with Active Directory, and the Samba Port Status Error error message is received.

Solution

In order to resolve this problem, make sure these ports are open to support Active Directory functionality:

- Samba Port – TCP 445
- LDAP – TCP 389
- LDAP – UDP 389
- KDC – TCP 88
- kpasswd – TCP 464
- NTP– UDP 123
- Global catalogue – TCP – 3268
- DNS – UDP 53

ACS needs to be able to reach all the DCs in the domain in order for the ACS–AD integration to be complete. Even if one of the DCs is not reachable from the ACS, the integration would not happen. Refer to Cisco bug ID CSCte92062 (registered customers only) for more information.

Problem: CSCOacs_Internal_Operations_Diagnostics ERROR Could not start message bus

Why do I receive the CSCOacs_Internal_Operations_Diagnostics ERROR Could not start message bus error message on ACS?

Solution

This is a cosmetic error and it is not a serious problem as long as none of the authentication/authorizations/ACS performance is affected and it only indicates that the internal message bus connection is being re-established.

Problem: 13017 Received TACACS+ packet from unknown Network Device or AAA Client

Why do I receive the 13017 Received TACACS+ packet from unknown Network Device or AAA Client error message on ACS?

Solution

This error usually comes up when either the right interface is not configured as the AAA client on ACS, or when the IP address configured on ACS is getting natted. In other words, the right IP address is not contacting ACS which is causing this error. This can also come up if the **ip tacacs source-interface <interface-name/id>** command is issued on the router, but some other IP address is used on ACS as the AAA client address. Also, disabling single-connect on IOS might help resolve this problem.

Problem: Unable to delete Authentication History (RADIUS Successes or Failures) and the syslogs from the ACS

Unable to delete Authentication History (RADIUS Successes or Failures) and the syslogs from the ACS.

Solution

It is not possible to delete the Authentication History from the ACS. Also, the logs that are sent as syslogs to the ACS itself cannot be deleted.

Problem: Management process in not running and shows "running (HTTP is nonresponsive)"

The management process is not running and the management process shows `running (HTTP is nonresponsive)`.

Solution

This issue can be resolved by restoring an older backup of the configuration followed by reimaging and reloading the ACS.

Problem: Can I use a secure ID token with SFTP to backup the ACS database?

Solution

No, this is not possible. SFTP needs a static user name/password. When using a secure ID, it cannot provide a static user name/password.

Problem: Unable to filter the reports using Interactive Viewer

When trying to filter ACS reports using the Interactive Viewer; all the buttons are greyed out and the

right-click menu options are not populated properly. Internet Explorer 8 is the browser used.

Solution

This could be a browser related problem. Try other browsers like Firefox in order to get this to work. You could also try to enable the "Compatibility View" on IE8 to make things appear properly.

Problem: Authentication prompt appears only for the first connection and not for subsequent connections

When a Windows XP host sends across an 802.1x requests to the ACS via a 3750G switch, there is an authentication prompt only the first time the device attempts to connect to the switch. All subsequent connections are made without an authentication. Why does this happen and how can the authentication prompt be made to appear each time a connection is made?

Solution

In order to resolve the issue, go to **Network Connections > Local Area Connection > Properties > Authentication**, and make sure the **Cache user information for subsequent connections to this network** option is unchecked.

Problem: Authorization prompt appears when using Apple devices with ACS

Why does an Authorization prompt to validate the certificate appear while using Apple devices with ACS? Can I stop this authorization prompt from appearing?

Solution

The Authorization prompt is generated by Apple iDevices and not the ACS. There is no way to configure the ACS in such a way that the Apple device will stop showing the Authorization prompt.

Problem: ACS Error Message – Not all user Active Directory groups are retrieved successfully...

Why is the Not all user Active Directory groups are retrieved successfully. One or more of the group's canonical name was not retrieved error message seen on ACS?

Solution

This issue occurs because unicode characters are used in the group name on AD. Since ACS sees AD groups as ASCII text, the unicode characters are not translated correctly. As a result, the group membership is not retrieved. Remove the unicode character from the AD configuration in order to resolve this issue.

Problem: ACS does not log proxy authentication requests

ACS does not log proxy authentication requests even though Radius proxying has been enabled.

Solution

ACS does not log proxy authentication requests. ACS only takes the request and forwards it to the proxy server. The logs will only be visible on the proxy radius server. ACS does not contribute anything to the processing of authentication/accounting of the packet. As a result, no messages are logged on ACS for proxied packets.

Problem: ACS loses the configuration when repository is created from the GUI

ACS loses the configuration when repository is created from the GUI after modifications are done on the CLI.

Solution

If you create the repository from the GUI, after modifications are done using CLI, ACS loses the configuration and this is the expected behavior. When you stop and start ACS, the repository will be recreated based on the configuration stored by the GUI. The modifications made on the CLI to a repository created by the GUI will not be transported to the ACS application configuration.

Problem: Unable to use an SSH session for the RADIUS IETF attribute "Login-Service"

Unable to use an SSH session for the RADIUS IETF attribute "Login-Service".

Solution

It is not possible to use an SSH session for the RADIUS IETF attribute "Login-Service" as ACS IETF attributes are a per-RFC standard and there is no way any changes can be made in it.

Problem: Error "value too long (ACS Server Name,TacacsAuthentication), Alarm details is "Please see the collector log for details""

The value too long (<ACS Server Name>,TacacsAuthentication), Alarm details is "Please see the collector log for details" error message is received.

Solution

Check each of these items in order to resolve this problem:

- Verify that the console port of the ACS has a cable connected to it.
- Remove any unnecessary cables.
- Reseat the cable if it is connected to a terminal server.

Problem: ACS 4.x local user password change does not work with IOS devices running SSH v1

When a user connects with SSH to the system and uses an expired TACACS password, they are prompted to change their password. However, this password change is not working correctly.

Solution

In order to fix this issue, you need to have SSH v2 with "Keyboard interactive" authentication for the SSH v2 set. Cisco bug ID CSCin91851 (registered customers only) discusses this behavior.

Problem: Remote logging is not working for ACS 4.2

ACS Remote Agent is unable to log messages from the ACS Solution Engine, and this error message is received:

```
CSLogAgent - Can't get max number of connections maxNumberOfConnections  
using default 32
```

Solution

Try to un-install the Remote Agent from the member server, and re-install it with the domain user account.

Related Information

- [Cisco Secure Access Control Server for Windows Support Page](#)
- [Configuration Guide for Cisco Secure ACS 4.1](#)
- [Cisco Secure ACS Online Troubleshooting Guide, 4.1](#)
- [Technical Support & Documentation – Cisco Systems](#)

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

© 2011 – 2012 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 21, 2012

Document ID: 99449
