Secure Access Control System (ACS 5.x and later) Troubleshooting

Document ID: 113485

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Problem: "Error: Saved the running configuration to startup successfully % Manifest file not found in the bundle" on ACS appliance during appliance upgrade
Solution
Problem: Unable to Restart ACS Server 5.x from GUI
Solution
Problem: Issue setting up Active Directory authentication with ACS 5.2
Solution
Problem: Cannot view more than 100 pages in the accounting report
Solution
Problem: Unable to generate pass/fail authentication report for a group of devices
Solution
Problem: The monitoring and reports database is currently unavailable. Attempting to reconnect in 5 seconds.
Solution

Problem: 22056 Subject not found in the applicable identity store(s)
Solution
Problem: Unable to integrate ACS with Active Directory
Solution
Problem: Unable to integrate ACS with LDAP
Solution
Problem: "csco acs_internal_operations_diagnostics error: could not write to local storage file" Error Message
Solution
Problem: Unable to integrate the ACS 5.1 with Active Directory
Solution
Problem: Unable to configure ACS 5.x to recognize regular expressions in the service selection rules
Solution
Problem: SFTP backup is not working when using Cisco Works as the SFTP server
Solution
Problem: "Invalid EAP payload dropped"
Solution
Problem: "ACS runtime process is not running on this instance at this time."
Solution
Problem: Unable to export the users with the Password
Solution
Problem: ACS internal users are disabled intermittently
Solution
Problem: "TACACS+ authentication request ended with error"

Solution

Problem: "Radius Authentication Request Rejected due to critical logging error"

Solution

Problem: ACS View interface shows "Data Upgrade Failed" at the top of the page when ACS is upgraded from 5.2 to 5.3

Solution

Problem: Issue with "change password on next login acs" on Cisco ACS 5.0

Solution

Problem: "% Application upgrade failed, Error − −999. Please check ADE logs for details, or re−run with − debug application install − enabled" on ACS appliance during upgrade

Solution

Problem: Error "Authentication failed : 12308 Client sent Result TLV indicating failure"

Solution

Problem: Error "24495 Active Directory servers are not available"

Solution

Problem: Error "5411 EAP session timed out"

Solution

Problem: 802.1x authentication does not work if logon restrictions is configured on the Active Directory

Solution

Problem: Error: "You are not authorized to view the requested page" when ACS 5.x admin with ChangeUserPassword role changes the password

Solution

Problem: Getting error on ACS 5.x for failed authentication "24495 Active Directory servers are not available."

Solution

Problem: Unable to connect to the ACS appliance using BMC

Solution

Problem: A warning alarm "delete 20000 sessions" with cause "active sessions are over limit", appear in the monitor and report general dashboard.

Solution

Problem: ACS 5.x error "11013 RADIUS packet already in the process"

Solution

Problem: RADIUS authentication failed with error "11012 RADIUS packet contains invalid header"

Solution

Problem: RADIUS/TACACS+ authentication failed with error "11007 Could not locate Network Device or AAA Client"

Solution

Problem: RADIUS authentication failed with error "11050 RADIUS request dropped due to system overload".

Solution

Problem: RADIUS authentication failed with error "11309 Incorrect RADIUS MS−CHAP v2 attribute."

Solution

Problem: ACS reports memory usage over 90%. Alarm

Solution

Problem: error:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Failed to link nodes

Solution

Problem: error:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Failed to link nodes

Solution

Problem: error 11026 The requested dACL is not found

Solution

Problem: error 11025 The Access−Request for the requested dACL is missing a cisco−av−pair attribute with the value aaa:event=acl−download. The request is rejected

Solution
Problem: error 11023 The requested dACL is not found. This is an unknown dACL name
Solution
Problem: Administrator authentication failed with error 10001 Internal error. Incorrect configuration version
Solution
Problem: Administrator authentication failed with error 10002 Internal error: Failure to load appropriate service
Solution
Problem: Administrator authentication failed with error 10003 Internal error: Administrator authentication received blank Administrator name
Solution
Problem: Failure Reason : 24428 Connection related error has occurred in either LRPC, LDAP or KERBEROS
Solution
Problem: TACACS+ Auth−Proxy authentication is not working on a router running IOS 15.x from ACS 5.x server
Solution
Problem: Getting error message Store failure (acs−xxx, TacacsAccounting) from ACS 5.x
Solution
Problem: User authentication failed with error "11036 The Message−Authenticator RADIUS attribute is invalid."
Solution
Problem: RADIUS accounting failed with error "11037 Dropped accounting request received via unsupported port."
Solution
Problem: RADIUS accounting failed with error "11038 RADIUS Accounting−Request header contains invalid Authenticator field."
Error: "24493 ACS has problems communicating with Active Directory using its machine credentials."
Solution
Problem: "When creating Shell Profile names with special characters like "ê", ACS may crash."
Solution
Problem: Getting "Parse error at line 2: not well−formed (invalid token)" while running "show run" on the ACS 5.x CLI.
Solution
Problem: ACS 5.x /opt partition fills up very quickly
Solution
Problem: Querying the desired domain
Solution
Problem: Parent and child domains at the same time
Solution
Problem: Logging to Remote Database
Solution
Problem: VMWare Support
Solution
Problem: Disk Space Requirements
Solution
Problem: "24401 Could not establish connection with ACS Active Directory agent."
Solution
Problem: "Runtime" process shows "Execution Failed" state
Solution
Problem: Failed ACS authentication when the UCS forces re−authentication
Solution

Problem: "24444 Active Directory operation has failed because of an unspecified error in the ACS"
Solution
Problem: Unable to authenticate ACS 5.1 users with AD 2008 R2 Server
Solution
Error: 22056 Subject not found in the applicable identity store(s).
Solution
Problem: ipt_connlimit: Oops: Invalid ct state ?
Solution
Problem:ACs 5.x / ISE does not see radius calling−station−id attribute in a RADIUS request from Cisco IOS Software Release 15.x NAS
Solution
Problem: User accounts gets locked at first instance of wrong credentials even if configured for 3 attempts
Solution
Problem: Unbale to save back up from ACS
Solution
Related Information

Introduction

This document provides information on how to troubleshoot Cisco Secure Access Control System (ACS) and how to resolve error messages.

For information on how to troubleshoot Cisco Secure ACS 3.x and 4.x, refer to Secure Access Control Server (ACS 3.x and 4.x) 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 System version 5.x and 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.

Problem: "Error: Saved the running configuration to startup successfully % Manifest file not found in the bundle" on ACS appliance during appliance upgrade

The `Error: Saved the running configuration to startup successfully % Manifest file not found in the bundle` error appears when an attempt is made to upgrade ACS Express from 5.0 to 5.0.1.

Solution

Complete these steps in order to upgrade the ACS appliance without any issue:

1. Download patch 9 (5−0−0−21−9.tar.gpg) and ADE−OS (ACS_5.0.0.21_ADE_OS_1.2_upgrade.tar.gpg) from: **Cisco.com > support > download software > Security > Cisco Secure Access Control System 5.0 > Secure Access Control System Software > 5.0.0.21**
2. After you install the two files, install the ACS 5.1 upgrade ACS_5.1.0.44.tar.gz. This is available from the same path from previous step.
3. Use this command in order to install the upgrade:

```
application upgrade <application−bundle> remote−repository−name
```

This completes the upgrade procedure.

Refer to Upgrading an ACS Server from 5.0 to 5.1 for more information on how to upgrade the ACS appliance.

Problem: Unable to Restart ACS Server 5.x from GUI

This section explains why you cannot restart the ACS server version 5.x from the GUI.

Solution

There is no option available to restart the ACS 5.x server from the GUI. The ACS can only be restarted from the CLI.

Problem: Issue setting up Active Directory authentication with ACS 5.2

When setting up Active Directory (AD) authentication for a new 5.2 ACS service, this error message is received:

```
Unexpected RPC Error: Access Denied due to unexpected configuration or
network error. Please try the −−verbose option or run "adinfo −−diag".
```

Solution

The ACS needs to write permissions in order to authenticate with the AD. In order to resolve this issue, provide temporary write permissions to the service account.

Problem: Cannot view more than 100 pages in the accounting report

When attempting to generate a custom AAA accounting report with ACS version 5.1, you cannot view more than 100 pages. This does not cover several older reports. How do you change this setting to see all the pages?

Solution

You cannot change the number of pages on the ACS because the maximum number of pages displayed is only 100 by default. In order to overcome this limitation and view older statistics, you need to change the filtering options so that more specific matches can be made. For example, if you try to generate the report for the last thirty days, it contains a large volume and the last 100 pages might show the activity for only the last hour. Here, using the filtering options is advised. Taking the filtering option as a user ID and specifying the time−range will yield much older reports.

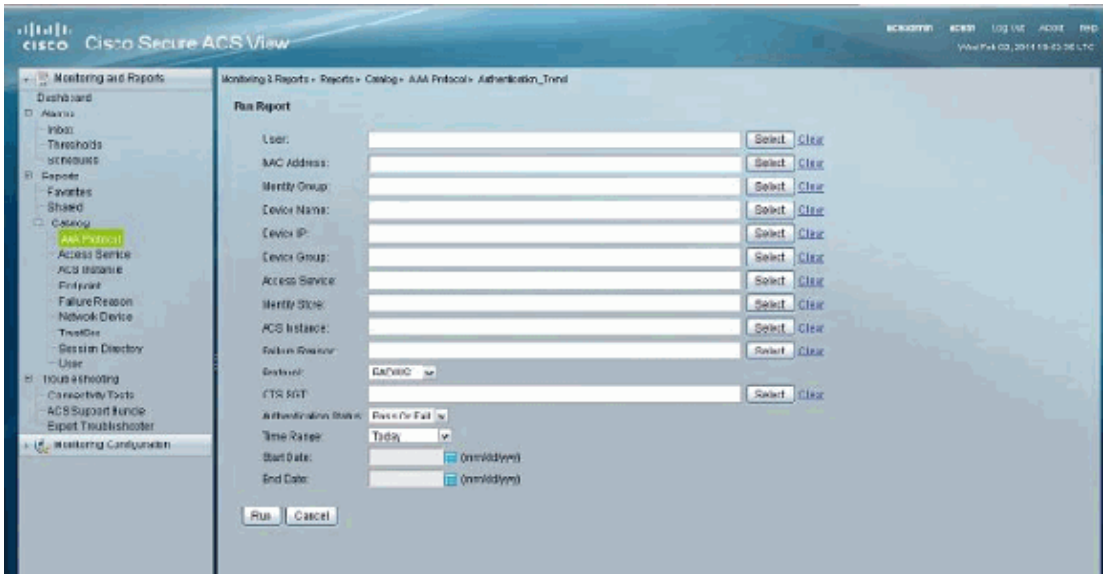
Problem: Unable to generate pass/fail authentication report for a group of devices

This issue occurs when attempting to generate the authentication report only for a group of six routers/switches, not for all the devices. ACS version 4.x is used.

Solution

This is not possible with ACS 4.x. You need to migrate to ACS 5.x because this feature is available with that version. You can extract reports for the specific group of devices by generating the Catalog Reports.

Refer to this image for a better understanding:



Problem: The monitoring and reports database is currently unavailable. Attempting to reconnect in 5 seconds.

When you click the Launch Monitoring and Report Viewer from ACS 5.x, this error message is received: `The monitoring and reports database is currently unavailable. Attempting to reconnect in 5 seconds. If problem persist, please contact your ACS administrator.`

Solution

Perform one of these workarounds in order to resolve this issue:

- Restart the ACS services from CLI by issuing these commands:

```
application stop acs
application start acs
```

- Upgrade to the latest available patch. Refer to Applying Upgrade Patches for more information about this.

Problem: 22056 Subject not found in the applicable identity store(s)

AD users do not get authenticated with ACS version 5.x and receive this error message: `22056 Subject not found in the applicable identity store(s).`

Solution

This error message occurs when the ACS failed to find the user in the first listed database that is configured in the Identity store sequence. This is an informational message and does not affect the performance of the ACS. The way that ACS 5.x performs the authentication for internal or external users is different than the previous 4.x version. With the 5.x version, there is an option called Identity Store Sequence to define the sequence of user databases to be authenticated. For more information, refer to Configuring Identity Store Sequences.

If you receive this error when you are using the ACS to authenticate requests against a Child Domain, then you have to add a UPN suffix or NETBIOS prefix to the username. For more information, refer to the Notes in the Microsoft AD section.

Problem: Unable to integrate ACS with Active Directory

Users cannot 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

The ACS needs 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 does not happen. Refer to Cisco bug ID CSCte92062 (registered customers only) for more information.

Problem: Unable to integrate ACS with LDAP

In this document, ACS 5.2 is used as an AAA RADIUS server for 802.1X implementation. 802.1X can be successfully used with ACS using the internal user store, but there are issues integrating ACS and LDAP. This error message is displayed:

```
Radius authentication failed for USER: example MAC:
UU-VV-WW-XX-YY-ZZ AUTHTYPE: PEAP(EAP-MSCHAPv2)
EAP session timed out : 5411 EAP session timed out
```

Solution

In this instance, LDAP is being used with the PEAP and the internal authentication method used is eap−mschap v2. This will fail because LDAP is not supported for PEAP (eap−mschap v2). It is recommended to use eap−tls or the AD.

Problem: "csco acs_internal_operations_diagnostics error: could not write to local storage file" Error Message

During replication of the ACS, the primary ACS does not replicate properly and displays this error message:

```
csco acs_internal_operations_diagnostics error: could
         not write to local storage file
```

Solution

Restart the ACS services and make sure critical logging is disabled. For more information, refer to Cisco bug ID CSCth66302 (registered customers only) . If this does not help, contact Cisco TAC in order to get the latest ACS patch suitable to resolve this problem.

Problem: Unable to integrate the ACS 5.1 with Active Directory

When trying to implement AD integration, this error message is received:

```
Error while configuring Active Directory:Using writable
         domain controller:test1.test.pvt Authentication error due unexpect
         configuration or network error. Please try the --verbose option or run 'adinfo
         -diag' to diagnose the problem. Join to domain 'test.pvt', zone 'null'
         failed.
```

Solution

Complete this workaround in order to fix this problem:

1. Delete the existing machine account on AD.
2. Create a new OU.
3. Go to Properties of the OU and uncheck **inherit permissions**.
4. Create a new machine account for the ACS in the new OU.
5. Allow the AD to replicate.
6. Try to join the AD from the ACS GUI.

In some cases, it is also helpful if you contact Microsoft and apply the Hot Fix .

Problem: Unable to configure ACS 5.x to recognize regular expressions in the service selection rules

Solution

This is not possible because it is not yet supported in ACS 5.x.

Problem: SFTP backup is not working when using Cisco Works as the SFTP server

When the network resource is on the CiscoWorks server, the backup scheduler works fine with other SFTP clients, but not ACS 5.2. Specifically, when trying to connect to the SFTP server from the ACS, the `Unable to negotiate a key exchange method` error message is received.

Solution

In this case, the SFTP server is not a FIPS compliant device using the DH 14 group. ACS only supports servers with DH 14 support as it is FIPS compliant. For more information about this issue, refer to Known Limitations in ACS 5.2.

Problem: "Invalid EAP payload dropped"

The `Error: Invalid EAP payload dropped` error message is received while authenticating the wireless users to ACS 5.0 patch 7.

Solution

This is an observed behavior and addressed in Cisco bug IDs CSCsz54975 (registered customers only) and CSCsy46036 (registered customers only) .

In order to resolve this issue, upgrade to ACS 5.0 patch 9, which is required as part of the upgrade to 5.1 or 5.2. Refer to Upgrading the Database for complete details. This also includes the information on how to upgrade to patch 9.

Problem: "ACS runtime process is not running on this instance at this time."

Users cannot login to the ACS GUI and this error message is received:

```
"The ACS runtime process is not running on this instance at this time. Changes can be made to the ACS configuration (these will be saved in the database), but changes will not take effect until the runtime process is restarted."
```

Solution

Manually restarting the runtime process from the CLI and rebooting the appliance resolves this issue. This is a minor issue and does not create any performance issue for the ACS. There are two minor bugs filed to observe this behavior. For more information, refer to Cisco bug IDs CSCtb99448 (registered customers only) and CSCtc75323 (registered customers only) .

In order to restart the runtime processes manually, issue these commands from the ACS CLI:

- **acs stop runtime**
- **acs start runtime**

Problem: Unable to export the users with the Password

You can export and import the user database to another ACS 5.x with a CSV file, but it does not include the user password field (appears blank). How do you move a local user's Identity store from one ACS to another that includes the password information?

Solution

This is not possible as this will become a security breach. In this case, one workaround is to perform a backup and restore procedure. However, the limitation to this workaround is that the backup and restore only works for another ACS with a similar configuration.

Problem: ACS internal users are disabled intermittently

ACS users are disabled intermittently with a `Password expired` message. The password expiration policy is set for 60 days, but these users must be manually enabled in order for them to get access.

Solution

This behavior is observed and filed in Cisco bug ID CSCtf06311 (registered customers only) . This issue can be resolved by applying patch 3 to ACS 5.1. In order to view all resolved issues under patch 3, refer to Resolved Issues in Cumulative Patch ACS 5.1.0.44.3. For related information on how to upgrade the patch, refer to Applying Upgrade Patches.

Problem: "TACACS+ authentication request ended with error"

The ACS authentication report shows the `TACACS+ authentication request ended with error` error message.

Solution

This occurs when the TACACS authentication has the Service Type set to PPP. Refer to Cisco bug ID CSCte16911 (registered customers only) for more information.

Problem: "Radius Authentication Request Rejected due to critical logging error"

Radius authentication is rejected with the `Radius Authentication Request Rejected due to critical logging error` error message.

Solution

This error is detailed in Cisco bug ID CSCth66302 (registered customers only) .

Problem: ACS View interface shows "Data Upgrade Failed" at the top of the page when ACS is upgraded from 5.2 to 5.3

The ACS View interface shows `Data Upgrade Failed` at the top of the page when the ACS is upgraded from 5.2 to 5.3.

Solution

This error is detailed in Cisco bug ID CSCtu15651 (registered customers only) .

Problem: Issue with "change password on next login acs" on Cisco ACS 5.0

Solution

In ACS 5.0, the password expiration function (user must change password on next logon) on the local user ID Store is selectable, but does not work. Enhancement request CSCtc31598 fixes the issue in ACS version 5.1.

Problem: "% Application upgrade failed, Error − −999. Please check ADE logs for details, or re−run with − debug application install − enabled" on ACS appliance during upgrade

The `% Application upgrade failed, Error − −999. Please check ADE logs for details, or re−run with − debug application install − enabled` error appears when an attempt is made to upgrade an ACS Express from 5.0 to 5.0.1.

Solution

This error occurs when the repository used is TFTP and the file size is greater than 32MB. ACS Express cannot handle files greater than 32MB. Use FTP as repository in order to resolve this issue even if the file size is more than 32MB.

Problem: Error "Authentication failed : 12308 Client sent Result TLV indicating failure"

The `Authentication failed : 12308 Client sent Result TLV indicating failure` error occurs on the ACS when you try to authenticate for the first time. Authentication works fine the second time.

Solution

This error can be resolved when you disable **Fast Reconnect**. An upgrade to **patch 2 of ACS version 5.2** helps to resolve the issue without the Fast Reconnect being disabled.

This error can also be resolved when you disable **Forced cryptobinding** on the supplicant. Refer to Cisco bug ID CSCtj31281 (registered customers only) for more information.

Problem: Error "24495 Active Directory servers are not available"

Authentication starts failing with this error: `24495 Active Directory servers are not available.` in the ACS 5.3 logs.

Solution

Check the ACSADAgent.log file through the CLI of the ACS 5.x for messages such as:`Mar 11 00:06:06 xlpacs01 adclient[30401]: INFO <bg:bindingRefresh> base.bind.healing Lost connection to xxxxxxxx. Running in disconnected mode: unlatch`. If you see the `Running in disconnected mode: unlatch` error message, this means the ACS 5.3 cannot maintain a stable connection with Active Directory. The workaround is to either switch to LDAP or downgrade the ACS to 5.2 version. Refer to Cisco bug ID CSCtx71254 (registered customers only) for more information.

Problem: Error "5411 EAP session timed out"

`5411 EAP session timed out` error messages are received on ACS 5.x.

Solution

EAP session timeouts are quite common with PEAP where the supplicant restarts authentication after the initial packet goes out to the RADIUS server and, most of the time, are not indicative of a problem.

The flow that is commonly seen is:

```
Supplicant ------------- Authenticator -------------- ACS
Connect
<------------------Request for Identity
----------------------> Response Identity ------------->
<--------------   EAP Challenge <-----------------
EAPOL-Start ------------->
normal flow ending in successful authentication.......
```

In the end the authentication is successful. However, there is a thread left open on the ACS due to the abrupt restart of the EAP session from the supplicant which causes a successful authentication followed by the EAP session timeout message. Many times this is due to the driver level of the machine. Make sure that the NIC/Wireless drivers are up to date on the client machine. You can capture on the client and filter on EAP || EAPOL in order to see what the client receives or sends when connecting.

Problem: 802.1x authentication does not work if logon restrictions is configured on the Active Directory

802.1x authentication does not work if the users have logon restrictions configured on the Active Directory.

Solution

If you have logon restrictions set Active Directory for a single machine and attempt an 802.1x authentication. The authentication fails because in the perspective of Active Directory that authentication is coming from the ACS, not the machine that the logon restriction is set to. For the authentication to be successful, the logon restrictions can be set to include the ACS machine accounts.

Problem: Error: "You are not authorized to view the requested page" when ACS 5.x admin with ChangeUserPassword role changes the password

ACS 5.x GUI admin user with the **ChangeUserPassword** role cannot change the password of the AAA user stored in the internal database. After changing the password, the user receives this pop−up error message: `You are not authorized to view the requested page`.

Solution

This can occur when the ACS 5.x database is migrated from ACS 4.x. Use the **SuperAdmin** privilege in order to change the user password. Refer to Cisco bug ID CSCty91045 (registered customers only) for more information.

Problem: Getting error on ACS 5.x for failed authentication "24495 Active Directory servers are not available."

Solution

You need to verify the Active Directory integration with ACS 5.x. If it is a distributed setup, ensure both the primary and secondary ACS 5.x in the setup are properly integrated with Active Directory.

Problem: Unable to connect to the ACS appliance using BMC

When the BMC client (a hardware level tool) is used to get into the ACS 1121 IBM servers, it is observed that the BMC client has two IP addresses.

Solution

This behavior has been identified and logged in Cisco bug ID CSCtj81255 (registered customers only) . In order to resolve this, you need to disable the BMC DHCP client on the ACS 1121.

Problem: A warning alarm "delete 20000 sessions" with cause "active sessions are over limit", appear in the monitor and report general dashboard.

There is a limit to the number of records that a session directory can hold. Because the probing requests are heavy in the customer's setup, the limit is reached fast. After reaching the limit, by design, ACS−View deletes a certain number of records (for example, 20k) from the session directory and sends an alert. You can increase this limit, but it does not help much except to prolong the alert.

Solution

In order to resolve this, perform the following:

- It is suggested to disable logging in order to view the database.

1. Go to **Cisco Secure ACS > System Administration > Configuration > Log Configuration > Logging Categories > Global > "Passed Authentications" > Remote Syslog Target** and remove **LogCollector** from Selected Targets.
2. Go to **Cisco Secure ACS > System Administration > Configuration > Log Configuration > Logging Categories > Global > "Failed Attempts" > Remote Syslog Target** and remove **LogCollector** from Selected Targets.
3. Go to **Cisco Secure ACS > System Administration > Configuration > Log Configuration > Logging Categories > Global > Edit: "RADIUS Accounting" > Remote Syslog Target** and remove **LogCollector** from Selected Targets.

- You can ignore the probing authentication requests becasue these are not real authentication requests. Perform the following:

  Go to **Cisco Secure ACS > Monitoring Configuration > System Configuration > Add Filter** and create the filter. Creating the filter based on *user name* is more appropriate because the probing requests are understood to be sent with a dummy user name. If you create a separate access policy in ACS to process these probing requests, then filters can be created based on *Access Service* as well.

Problem: ACS 5.x error "11013 RADIUS packet already in the process"

In an ACS 5.3 deployment, users fail dot1x authentication. The database used is an Active Directory. The RADIUS failure code is shown here:

```
RADIUS Request dropped: 11013 RADIUS packet already in the process
```

Solution

The ACS has ignored this request because it is a duplicate of another packet that is currently being processed. This can occur because of any of these:

- The Average RADIUS Request Latency statistic is close to or exceeds the client RADIUS request timeout of the client.
- External identity store can be very slow.
- The ACS has been overloaded.

Perform these steps in order to resolve:

1. Increase the client RADIUS request timeout of the client.
2. Use a faster or additional external identity store.
3. Follow the ways to reduce the overload on ACS.

Problem: RADIUS authentication failed with error "11012 RADIUS packet contains invalid header"

Solution

The header of the incoming RADIUS packet did not parse correctly. In order to resolve this, verify the following:

- Check the network device or AAA Client for hardware problems.
- Check the network that connects the device to the ACS for hardware problems.

- Check whether the network device or AAA Client has any known RADIUS compatibility issues.

Problem: RADIUS/TACACS+ authentication failed with error "11007 Could not locate Network Device or AAA Client"

This error message is received on the ACS when an ASA sends a radius access−request message:

```
11007 Could not locate Network Device or AAA Client
```

Solution

This occurs because there is a mismatch between the IP of the ACS client and the interface IP that actually sends the request. Sometimes the firewall performs an address translation to this AAA client. Verify if the AAA client is properly configured with the correct translated IP address at this path:

Network Resources > Network Devices and AAA Clients

Problem: RADIUS authentication failed with error "11050 RADIUS request dropped due to system overload".

Users cannot access the network because of the authentication failures. This error message from the ACS is received:

```
11050 RADIUS request dropped due to system overload
```

Solution

Cisco ACS drops these authentication requests because of overload. This can be caused by the replication of many parallel auhentication requests. In order to avoid this, perform any of these:

- Modify the **Network Device/AAA Client** settings so that it uses the **Legacy TACACS+ Single Connection Support** option. With this, the client will re−use the same session for all requests instead of creating many sessions.
- Refrain the users from invoking new authentication requests for some point of time.
- Restart the ACS server.

Problem: RADIUS authentication failed with error "11309 Incorrect RADIUS MS−CHAP v2 attribute."

Solution

This error occurs due to the invalid length or incorrect value from one of the MSCHAP v2 attributes (MS−CHAP−Challenge, MS−CHAP−Response, MS−CHAP−CPW−2, or MS−CHAP−NT−Enc−PW) in the received RADIUS access−request packet.

Problem: ACS reports memory usage over 90%. Alarm

ACS reports memory usage over 90%.Alarm such as the following: `Cisco Secure ACS − Alarm NotificationSeverity: Critical Alarm Name ACS − System`

`HealthCause/Trigger Alarm caused by ACS − System Health thresholdAlarm Details ACS Instance CPU Utilization (%) Memory Utilization (%) Disk I/O Utilization (%) Disk Space Used /opt (%) Disk Space Used /localdisk: (%) Disk Space Used / (%) KOM−AAA02 0.41 90.14 0.02 9.57 5.21 25.51`

Solution

This issue is usually seen on ACS 5.2. In order to fix this issue, reload the ACS in order to free the memory or upgrade to ACS 5.2 patch 7 or later. Refer to Cisco bug ID CSCtk52607 (registered customers only) for more information.

Problem: error:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Failed to link nodes

In a distributed setup after a maintenance task (joining to a primary, force full replication, patching), ACS instance A reports ACS instance B as offline in the distributed deployment screen, while B is really online and reports instance A as online. In the management logs, you see `error:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Failed to link nodes`.

Solution

This can occur if a previous instance of the replication management service is still bound to port 2030 when the new instance comes up and tries to bind to that port. From the CLI of ACS instance B, run:sho acs−logs file ACSManagement. `log | i Replication service`. You will see messages such as `Replication service failed.:Port already in use: 2030`. Currently, the workaround is to restart the ACS instance B (the one that reports the other as online). Refer to Cisco bug ID CSCtx56129 (registered customers only) for more information.

Problem: error:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Failed to link nodes

In a distributed setup after a maintenance task (joining to a primary, force full replication, patching), ACS instance A reports ACS instance B as offline in the distributed deployment screen, while B is really online and reports instance A as online. In the management logs, you see `error:com.cisco.nm.acs.mgmt.msgbus.FatalBusException: Failed to link nodes`.

Solution

Upgrade to ACS 5.2 patch 6 or later in order to fix this issue. Refer to Cisco bug ID CSCto47203 (registered customers only) for more information.

Note: The viewDB backup will fail once the ""/opt"" usage exceeds 30%. It is required to configure NFS staging to perform a backup when ""/opt"" exceeds 30% usage.

Problem: error 11026 The requested dACL is not found

RADIUS authentication fails with this error message: `11026 The requested dACL is not found`.

Solution

The request is rejected because the version of the Downloadable ACL requested in the RADIUS Access−Request is not found. The request for the Downloadable ACL occurred long after the original Access−Request. Because of this, the version of the Downloadable ACL was no longer available. Find the reason for this delay in the request for the Downloadable ACL from the RADIUS client.

Problem: error 11025 The Access−Request for the requested dACL is missing a cisco−av−pair attribute with the value aaa:event=acl−download. The request is rejected

RADIUS authentication fails with this error message: `11025 The Access−Request for the requested dACL is missing a cisco−av−pair attribute with the value aaa:event=acl−download. The request is rejected`.

Solution

Every Access−Request for the Downloadable ACL must have a `cisco−av−pair attribute` with the value `aaa:event=acl−download`. In this case, that attribute is missing the request and the ACS failed the request. Check whether the network device or AAA client has any known RADIUS compatibility issues.

Problem: error 11023 The requested dACL is not found. This is an unknown dACL name

RADIUS authentication fails with this error message: `11023 The requested dACL is not found. This is an unknown dACL name`.

Solution

Check the ACS configuration to verify that the Downloadable ACL specified in the Authorization Profile exists in the list of Downloadable ACLs. This is an ACS side misconfiguration.

Problem: Administrator authentication failed with error 10001 Internal error. Incorrect configuration version

Administrator authentication fails with this error: `10001 Internal error. Incorrect configuration version`.

Solution

This error can be caused by a corrupt ACS database, or by a problem in the underlying configuration data. Contact Cisco TAC (registered customers only) for more information.

Problem: Administrator authentication failed with error 10002 Internal error: Failure to load appropriate service

Administrator authentication fails with this error: `10002 Internal error: Failure to load appropriate service`.

Solution

ACS 5.x cannot load the AAC configuration service. This can be caused by a corrupt ACS database, or by a problem in the underlying configuration data. It can also occur when the system resources are exhausted. Contact Cisco TAC (registered customers only) for more information.

Problem: Administrator authentication failed with error 10003 Internal error: Administrator authentication received blank Administrator name

Administrator authentication fails with this error: `10003 Internal error: Administrator authentication received blank Administrator name`.

Solution

When accessing the GUI of the ACS 5.x, ACS receives a blank user name. Check the validity of the user name transmitted to the ACS. If it is valid, contact Cisco TAC (registered customers only) for more information.

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: TACACS+ Auth−Proxy authentication is not working on a router running IOS 15.x from ACS 5.x server

TACACS+ Auth−Proxy authentication is not working on a router that runs Cisco IOS Software Release 15.x from an ACS 5.x server.

Solution

TACACS+ Auth−Proxy is only supported after ACS 5.3 patch 5. Upgrade your ACS 5.x, or use RADIUS for Auth−Proxy.

Problem: Getting error message Store failure (acs−xxx, TacacsAccounting) from ACS 5.x

Solution

The ACS 5.1 TACACS accounting report misses a few attributes such as username, privilege level, and Request−Type when it receives a malformed accounting packet from the client. In some cases, this leads to the generation of "Store failure (acs−xxx, TacacsAccounting)" alarm in View. In order to resolve this, verify the following:

- Accounting packet sent by the client has a malformed TACACS argument (for example, mismatch in length and value of any of the argument sent by AAA client).
- Ensure that the client sends a valid accounting packet with proper length and value for the arguments.

Refer to Cisco bug ID CSCte88357 (registered customers only) for more information.

Problem: User authentication failed with error "11036 The Message−Authenticator RADIUS attribute is invalid."

Solution

Verify the following:

- Check whether the Shared secrets on the AAA client and ACS server match.
- Ensure that the AAA client and the network device have no hardware problems or problems with RADIUS compatibility.
- Ensure that the network that connects the device to the ACS has no hardware problems.

Problem: RADIUS accounting failed with error "11037 Dropped accounting request received via unsupported port."

Solution

Accounting request was dropped because it was received via an unsupported UDP port number. Verify the following:

- Ensure that the accounting port number configuration on the AAA client and on the ACS server match.
- Ensure that the AAA client has no hardware problems or problems with RADIUS compatibility.

Problem: RADIUS accounting failed with error "11038 RADIUS Accounting−Request header contains invalid Authenticator field."

The ACS cannot validate the Authenticator field in the header of the RADIUS Accounting−Request packet. The Authenticator field must not be confused with the Message−Authenticator RADIUS attribute. Ensure that the RADIUS Shared Secret configured on the AAA client matches that configured for the selected Network

Device on the ACS server. Also, ensure that the AAA client has no hardware problems or problems with RADIUS compatibility.

Error: "24493 ACS has problems communicating with Active Directory using its machine credentials."

Solution

Check the ACS for AD connectivity, and ensure that the ACS machine account is still present in the AD.

Problem: "When creating Shell Profile names with special characters like "ê", ACS may crash."

Solution

This behavior has been identified and logged in Cisco bug ID CSCts17763 (registered customers only) . You need to upgrade to 5.3.40 patch 1 or 5.2.26 patch 7.

Problem: Getting "Parse error at line 2: not well−formed (invalid token)" while running "show run" on the ACS 5.x CLI.

Solution

Make sure that the SNMP community configured on the ACS has valid characters. Only alphanumeric characters (letters and numbers only) are allowed to be used in the community name.

Problem: ACS 5.x /opt partition fills up very quickly

Solution

ACS 5.x runs out of disk space because of insufficient space in the */opt* partition. This occurs because of the high number of logging data flooding the ACS View. As a workaround, you need to replace the View database often. Because ACS View cannot cope with gigabytes of data every day, you need to organize the logging data. When you need all the logs, use an external syslog server instead of the ACS View. When you need to use only a part of the logging data, use *System Administration > Configuration > Log Configuration > Logging Categories > Global* in order to send only the required logs to the ACS View log−collector.

Problem: Querying the desired domain

Can ACS 5.x query desired Domain Controllers (DCs) when joining an Active Directory Domain?

Solution

No. Currently, the ACS queries the DNS with the domain in order to get a list of all the DCs in the domain. Then, it tries to communicate with all of them. If the connection to even one DC fails, then the ACS connection to the domain is declared as failed.

Problem: Parent and child domains at the same time

Is there a way to set up ACS 5.x in both parent and child domains at the same time?

Solution

No. Currently, ACS 5.x can only be a part of one domain. However, ACS 5.x can authenticate users/machines from multiple trusted domains.

Problem: Logging to Remote Database

Can I log the ACS 5.x View data to a remote database?

Solution

Yes, ACS 5.x allows you to log the ACS View data to Microsoft SQL servers and Oracle SQL servers.

Problem: VMWare Support

Solution

ACS 5.x can be installed on a Virtual Machine. The latest version, ACS 5.3, can be installed on these VMWare versions:

- VMWare ESX 3.5
- VMWare ESX 4.0
- VMWare ESX i4.1
- VMWare ESX 5.0

Problem: Disk Space Requirements

What are the disk space requirements for the ACS 5.x evaluation version?

Solution

A minimum of 60 GB disk space is required for the evaluation version. 500 GB is required for the production installation.

Problem: "24401 Could not establish connection with ACS Active Directory agent."

Solution

In order to resolve this error, verify the following:

- Check if the ACS machine is joined to the Active Directory domain.
- Check the connectivity status between the ACS machine and Active Directory server.
- Check if the ACS Active Directory agent is running.

Refer to Cisco bug ID CSCtx71254 (registered customers only) for more information.

Problem: "Runtime" process shows "Execution Failed" state

When updating the Cisco ACS with a patch, the Runtime process gets stuck in "Execution Failed" state and this message is logged:

```
"local0 err err 83 2012−06−12T12:11:08+0200 192.168.150.74 ACS ACS
logforward ERROR: /opt/CSCOacs/runtime/bin/run−logforward.sh: line 18:
7097 Segmentation fault (core dumped) ./$daemon −b −f $logfile"
```

Solution

This can be an issue with the MD5 patch of the last patch. Verify the MD5 checksum of the last patch applied to the Cisco ACS. Download that again, then apply it properly.

Problem: Failed ACS authentication when the UCS forces re−authentication

The UCS server is configured to authenticate a Java Client from the Cisco ACS. The authentication process involves the use of RSA Token server. The first authentication passes. However, when the UCS refreshes and forces the Java Client to re−authenticate, it fails because RSA does not allow to re−use any token. Therefore, the authentication fails.

Solution

This is a limitation from the persepective of the UCS Server, but not from Cisco ACS. The UCS Server follows a two−factor authentication which is an unsupported feature for Cisco ACS when used with RSA Tokens. Currently, it is not supported. As a workaround, you are advised to use any database server, such as AD or LDAP, other than the RSA Token server.

Problem: "24444 Active Directory operation has failed because of an unspecified error in the ACS"

Solution

An unmapped error has occurred in an AD related operation. Refer to ACS 5.x Integration with Microsoft AD Configuration Example and configure the AD integration with the ACS properly. If everything is configured properly as per the document, then contact Cisco TAC for further troubleshooting.

Problem: Unable to authenticate ACS 5.1 users with AD 2008 R2 Server

Solution

This occurs because of incompatibility issues. AD 2008 R2 integration is supported from ACS 5.2 version only. Upgrade your ACS to 5.2 or later. Refer to Cisco bug ID CSCtg12399 (registered customers only) for more information.

Error: 22056 Subject not found in the applicable identity store(s).

When the SSL VPN users are trying to get authenticated from an RSA appliance, this error message is received from the Cisco ACS Server:

```
Failure Reason: 22056 Subject not found in the applicable identity
store(s).
```

Solution

Check whether the user is present in the database where the ACS is pointed to look for. In case of RSA and RADIUS Identity Store, ensure that the **Treat Reject** option is selected as **authentication failed**. This is under the Advanced tab of the Identity Store configuration.

Problem: ipt_connlimit: Oops: Invalid ct state ?

The `ipt_connlimit: Oops: Invalid ct state ?` error message appears on the console when ACS 5.x runs on VMWare.

Solution

This is a cosmetic message. Refer to Cisco bug ID CSCth25712 (registered customers only) for more information.

Problem:ACs 5.x / ISE does not see radius calling−station−id attribute in a RADIUS request from Cisco IOS Software Release 15.x NAS

ACs 5.x / ISE does not see `radius calling−station−id` attribute in a RADIUS request from Cisco IOS Software Release 15.x NAS.

Solution

Use the **radius−server attribute 31 send nas−port−detail** command on Cisco IOS Software Release 15.x in order to enable sending the attribute.

Problem: User accounts gets locked at first instance of wrong credentials even if configured for 3 attempts

When ACS 5.3 is integrated with Active Directory at a Windows 2008 R2 functional level, user accounts that are set with lockout parameters (3 incorrect attempts) are lockouted prematurely after the user enters the wrong credentials just once.

Solution

Refer to Cisco bug ID CSCtz03211 (registered customers only) for more information.

Problem: Unbale to save back up from ACS

During an attempt to save a backup from the ACS, the `Cause: Incremental Backup Not Configured− Details: Incremental backup is not configured.Configuring incremental backup is necessary to make the database purge successful. This will help to avoid disk space issues. View database Size is 0.08GB and size it occupies on the harddisk is 0.08GB` warning appears.

Solution

You cannot concurrently run an incremental backup, full back up, and data purge. If any of these jobs are running, you must wait for a period of 90 minutes before you can begin the next job.

Related Information

- **Cisco Secure Access Control System Support Page**
- **Cisco Secure Access Control System End−User Guides**
- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 29, 2012 Document ID: 113485