

ACS 5.x及更高版本 — 安全ACS故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[問題："錯誤：在裝置升級期間，已儲存運行配置以成功啟動% Manifest file not found in the bundle" on ACS appliance](#)

[解決方案](#)

[問題：無法從GUI重新啟動ACS伺服器5.x](#)

[解決方案](#)

[問題：使用ACS 5.2設定Active Directory身份驗證時出現問題](#)

[解決方案](#)

[問題：在會計報表中不能檢視超過100頁](#)

[解決方案](#)

[問題：無法為一組裝置生成通過/失敗身份驗證報告](#)

[解決方案](#)

[問題：監控和報告資料庫當前不可用。嘗試在5秒後重新連線。](#)

[解決方案](#)

[問題：22056在適用的標識儲存中找不到主題](#)

[解決方案](#)

[問題：無法將ACS與Active Directory整合](#)

[解決方案](#)

[問題：無法將ACS與LDAP整合](#)

[解決方案](#)

[問題："cisco acs internal operations diagnostics錯誤：無法寫入本地儲存檔案「」錯誤消息](#)

[解決方案](#)

[問題：無法將ACS 5.1與Active Directory整合](#)

[解決方案](#)

[問題：無法將ACS 5.x配置為識別服務選擇規則中的正規表示式](#)

[解決方案](#)

[問題：使用Cisco Works作為SFTP伺服器時，SFTP備份無法正常工作](#)

[解決方案](#)

[問題："無效的EAP負載已丟棄"](#)

[解決方案](#)

[問題："此時，ACS運行時進程未在此例項上運行。"](#)

[解決方案](#)

[問題：無法使用密碼匯出使用者](#)

[解決方案](#)

[問題：ACS內部使用者被間歇性禁用](#)

[解決方案](#)

[問題："TACACS+身份驗證請求因錯誤而結束"](#)

[解決方案](#)

[問題："由於嚴重日誌記錄錯誤，Radius身份驗證請求被拒絕"](#)

[解決方案](#)

[問題：ACS從5.2升級到5.3時，ACS檢視介面頁面頂部顯示「Data Upgrade Failed」（資料升級失敗）](#)

[解決方案](#)

[問題：在Cisco ACS 5.0上發出「在下次登入acs時更改密碼」問題](#)

[解決方案](#)

[問題："% Application upgrade failed， Error —999.請檢視ADE日誌以瞭解詳細資訊，或在升級期間在ACS裝置上重新運行為 — debug application install - enabled"](#)

[解決方案](#)

[問題：錯誤「身份驗證失敗：12308 Client sent Result TLV indicating failure（客戶端傳送的結果TLV指示失敗）」](#)

[解決方案](#)

[問題：錯誤「24495 Active Directory伺服器不可用」](#)

[解決方案](#)

[問題：錯誤「5411 EAP會話超時」](#)

[解決方案](#)

[問題：如果在Active Directory上配置了登入限制，則802.1x身份驗證不起作用](#)

[解決方案](#)

[問題：錯誤：具有ChangeUserPassword角色的ACS 5.x管理員更改密碼時「您無權檢視請求的頁面」](#)

[解決方案](#)

[問題：在ACS 5.x上獲取身份驗證失敗的錯誤「24495 Active Directory伺服器不可用」。](#)

[解決方案](#)

[問題：無法使用BMC連線到ACS裝置](#)

[解決方案](#)

[問題：監控和報告常規儀20000板中出現警告警報「刪除活動會話」，其原因為「活動會話超出限制」。](#)

[解決方案](#)

[問題：ACS 5.x錯誤「11013 RADIUS資料包已在進程中」](#)

[解決方案](#)

[問題：RADIUS驗證失敗，錯誤為「11012 RADIUS封包包含無效標頭」](#)

[解決方案](#)

[問題：RADIUS/TACACS+驗證失敗，錯誤為「11007找不到網路裝置或AAA客戶端」](#)

[解決方案](#)

[問題：RADIUS驗證失敗，錯誤為「11050 RADIUS request dropped due to system overload」。](#)

[解決方案](#)

[問題：RADIUS身份驗證失敗，錯誤為「11309 Incorrect RADIUS MS-CHAP v2屬性」。](#)

[解決方案](#)

[問題：ACS報告記憶體使用率超過90%。警報](#)

[解決方案](#)

[問題：錯誤：com.cisco.nm.acs.mgmt.msgbus.FatalBusException:無法連結節點](#)

解決方案

問題：錯誤：com.cisco.nm.acs.mgmt.msgbus.FatalBusException:無法連結節點

解決方案

問題：錯誤11026未找到請求的dACL

解決方案

問題：錯誤11025請求的dACL的Access-Request缺少值為aaa:event=acl-download的cisco-av-pair屬性。請求被拒絕

解決方案

問題：錯誤11023未找到請求的dACL。這是未知的dACL名稱

解決方案

問題：管理員身份驗證失敗，錯誤為10001內部錯誤。配置版本不正確

解決方案

問題：管理員身份驗證失敗，錯誤為10002內部錯誤：無法載入適當的服務

解決方案

問題：管理員身份驗證失敗，錯誤為10003內部錯誤：管理員身份驗證收到空管理員名稱

解決方案

問題：失敗原因：24428 LRPC、LDAP或KERBEROS中發生連線相關錯誤

解決方案

問題：從ACS 5.x伺服器運行IOS 15.x的路由器上，TACACS+身份驗證代理無法正常工作

解決方案

問題：從ACS 5.x獲取錯誤消息Store failure(acs-xxx, TacacsAccounting)

解決方案

問題：使用者身份驗證失敗，錯11036為「The Message-Authenticator RADIUS attribute is invalid.」。

解決方案

問題：RADIUS記賬失敗，錯誤為「11037 Dropped accounting request received via unsupported port」。

解決方案

問題：RADIUS記帳失敗，錯誤為「11038 Accounting-Request header contains invalid Authenticator field」。

錯誤："ACS24493使用其電腦憑據與Active Directory通訊時出現問題。"

解決方案

問題："使用特殊字元(如"è")建立外殼配置檔名稱時，ACS可能崩潰。"

解決方案

問題：在第2行獲取「分析錯誤：在ACS 5.x CLI上運行「show run」時，格式不正確（無效令牌）。

解決方案

問題：ACS 5.x /opt分割槽很快滿

解決方案

問題：正在查詢所需域

解決方案

問題：同時存在父域和子域

解決方案

問題：記錄到遠端資料庫

解決方案

問題：VMWare支援

[解決方案](#)

[問題：磁碟空間要求](#)

[解決方案](#)

[問題："24401法與ACS Active Directory代理建立連線。"](#)

[解決方案](#)

[問題：「運行時」進程顯示「執行失敗」狀態](#)

[解決方案](#)

[問題：UCS強制重新身份驗證時ACS身份驗證失敗](#)

[解決方案](#)

[問題："24444 Active Directory操作因ACS中發生未指定的錯誤而失敗"](#)

[解決方案](#)

[問題：無法使用AD 2008 R2伺服器驗證ACS 5.1使用者](#)

[解決方案](#)

[錯誤：22056在適用的標識儲存中找不到主題。](#)

[解決方案](#)

[問題：ipt_connlimit:哎呀：無效的ct狀態？](#)

[解決方案](#)

[問題：AC 5.x/ISE在來自Cisco IOS軟體版本15.x NAS的RADIUS請求中看不到radius calling-station-id屬性](#)

[解決方案](#)

[問題：使用者帳戶在第一次出現錯誤憑據時鎖定，即使配置了3次嘗試](#)

[解決方案](#)

[問題：無法從ACS儲存備份](#)

[解決方案](#)

[相關資訊](#)

簡介

本文提供如何對思科安全存取控制系統(ACS)進行疑難排解以及如何解決錯誤訊息的相關資訊。

有關如何對Cisco Secure ACS 3.x和4.x進行故障排除的資訊，請參閱[安全訪問控制伺服器 \(ACS 3.x和4.x \) 故障排除](#)。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據思科安全存取控制系統5.x版及更新版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

問題："錯誤：在裝置升級期間，已儲存運行配置以成功啟動% Manifest file not found in the bundle" on ACS appliance

%ACS Express從5.0升級到5.0.1時，將出現捆綁包中未找到清單檔案錯誤。

解決方案

完成以下步驟，升級ACS裝置，沒有任何問題：

1. 從以下位置下載修補程式9([5-0-0-21-9.tar.gpg](#))和ADE-OS([ACS_5.0.0.21_ADE_OS_1.2_upgrade.tar.gpg](#)):[Cisco.com](#) > [支援](#) > [下載軟體](#) > [安全](#) > [思科安全訪問控制系統5.0](#) > [安全訪問控制系統軟體](#) > 5.0.0.21
2. 安裝這兩個檔案後，安裝ACS 5.1升級[ACS_5.1.0.44.tar.gz](#)。可從上一步的同一路徑中獲得。
3. 使用以下命令以安裝升級：

[application upgrade](#)

升級程式到此結束。

有關如何升級ACS裝置的詳細資訊，請參閱[將ACS伺服器從5.0升級到5.1](#)。

問題：無法從GUI重新啟動ACS伺服器5.x

本節介紹無法從GUI重新啟動ACS伺服器5.x版的原因。

解決方案

沒有從GUI重新啟動ACS 5.x伺服器的選項。ACS只能從CLI重新啟動。

問題：使用ACS 5.2設定Active Directory身份驗證時出現問題

為新的5.2 ACS服務設定Active Directory(AD)身份驗證時，收到以下錯誤消息：

```
RPC - verboseadinfo -diag
```

解決方案

ACS需要寫入許可權才能使用AD進行身份驗證。為了解決此問題，請為服務帳戶提供臨時寫入許可權。

問題：在會計報表中不能檢視超過100頁

嘗試使用ACS 5.1版生成自定義AAA記帳報告時，不能檢視100頁以上。這不包括幾個較舊的報告。

如何更改此設定以檢視所有頁面？

解決方案

您無法更改ACS上的頁數，因為預設情況下顯示的最大頁數僅為100。為了克服此限制並檢視較早的統計資訊，您需要更改篩選選項，以便可以進行更具體的匹配。例如，如果您嘗試生成最近30天的報告，該報告將包含很大的卷，而最後100頁可能只顯示最近一小時的活動。建議在此處使用過濾選項。將篩選選項作為使用者ID並指定時間範圍將生成較舊的報告。

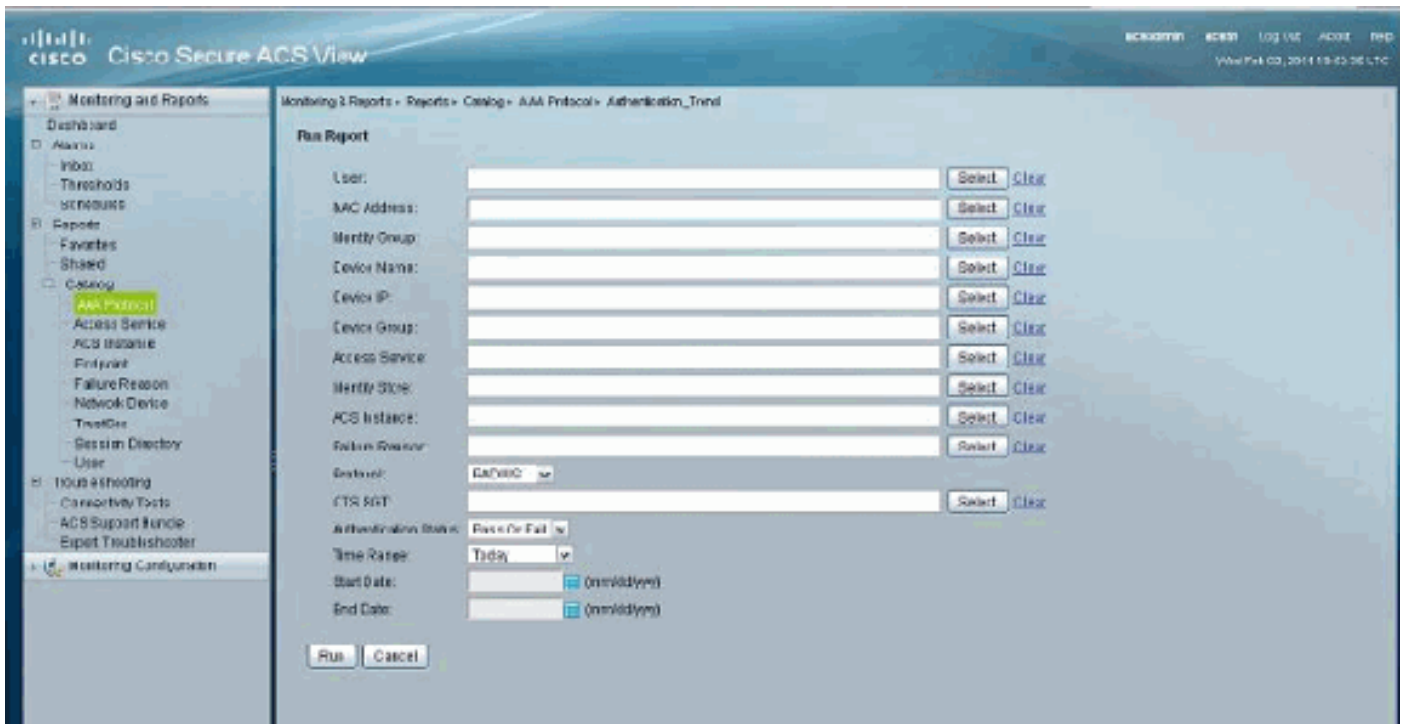
問題：無法為一組裝置生成通過/失敗身份驗證報告

當嘗試只為六台路由器/交換機組生成身份驗證報告，而不是為所有裝置生成身份驗證報告時，會出現此問題。使用ACS 4.x版。

解決方案

在ACS 4.x中無法實現此功能。您需要遷移到ACS 5.x，因為該版本提供此功能。您可以通過生成目錄報告來提取特定裝置組的報告。

如需進一步的瞭解，請參閱以下映像：



問題：監控和報告資料庫當前不可用。嘗試在5秒後重新連線。

當您從ACS 5.x中按一下啟動監控和報告檢視器時，收到以下錯誤消息：5ACS

解決方案

執行以下解決方法之一以解決此問題：

- 發出以下命令，從CLI重新啟動ACS服務：

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

- 升級到最新的可用修補程式。有關此問題的詳細資訊，請參閱[應用升級修補程式](#)。

問題：22056在適用的標識儲存中找不到主題

AD使用者未使用ACS 5.x版進行身份驗證，並收到以下錯誤消息：22056

解決方案

當ACS在身份庫序列中配置的第一個列出的資料庫中找不到使用者時，會出現此錯誤消息。這只是一條資訊性消息，不會影響ACS的效能。ACS 5.x對內部或外部使用者執行身份驗證的方式與先前的4.x版本不同。在5.x版本中，有一個名為Identity Store Sequence的選項用於定義要驗證的使用者資料庫的序列。有關詳細資訊，請參閱[配置身份儲存序列](#)。

如果在使用ACS對子域請求進行身份驗證時收到此錯誤，則必須向使用者名稱新增UPN字尾或NETBIOS字首。有關詳細資訊，請參閱[Microsoft AD](#)部分中的[註釋](#)。

問題：無法將ACS與Active Directory整合

使用者無法將ACS與Active Directory整合，並收到Samba Port Status Error錯誤消息。

解決方案

為了解決此問題，請確保這些埠是開放的，以支援Active Directory功能：

- Samba埠 — TCP 445
- LDAP - TCP 389
- LDAP - UDP 389
- KDC - TCP 88
- kpasswd - TCP 464
- NTP - UDP 123
- 全域性編錄 — TCP - 3268
- DNS - UDP 53

ACS需要到達域中的所有DC，才能完成ACS-AD整合。即使無法從ACS訪問其中一個DC，也不會進行整合。如需詳細資訊，請參閱Cisco錯誤ID [CSCte92062](#)(僅限[註冊](#)客戶)。

問題：無法將ACS與LDAP整合

在本文檔中，ACS 5.2用作802.1X實施的AAA RADIUS伺服器。802.1X可以使用內部使用者儲存成功用於ACS，但存在整合ACS和LDAP的問題。系統會顯示以下錯誤消息：

```
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
```

解決方案

在此例項中，LDAP正與PEAP一起使用，使用的內部身份驗證方法是eap-mschap v2。這將失敗，因為PEAP(eap-mschap v2)不支援LDAP。建議使用eap-tls或AD。

[問題："cisco acs internal operations diagnostics"錯誤：無法寫入本地儲存檔案「」錯誤消息](#)

在ACS複製期間，主ACS不能正確複製並顯示以下錯誤消息：

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

[解決方案](#)

重新啟動ACS服務，並確保禁用關鍵日誌記錄。如需更多資訊，請參閱Cisco錯誤ID [CSCth66302](#)(僅限註冊客戶)。如果這不起作用，請聯絡[Cisco TAC](#)以獲取適用於解決此問題的最新ACS修補程式。

[問題：無法將ACS 5.1與Active Directory整合](#)

嘗試實施AD整合時，收到以下錯誤消息：

```
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
-diaq' to diagnose the problem. Join to domain 'test.pvt', zone 'null'
failed.
```

[解決方案](#)

完成以下解決方法即可解決此問題：

1. 刪除AD上的現有電腦帳戶。
2. 建立新的OU。
3. 轉到OU的屬性並取消選中繼承許可權。
4. 為新OU中的ACS建立新電腦帳戶。
5. 允許AD複製。
6. 嘗試從ACS GUI加入AD。

在某些情況下，如果您與Microsoft聯絡並應用[Hot Fix](#)，也會很有用。

[問題：無法將ACS 5.x配置為識別服務選擇規則中的正規表示式](#)

[解決方案](#)

這是不可能的，因為ACS 5.x尚不支援它。

[問題：使用Cisco Works作為SFTP伺服器時，SFTP備份無法正常工作](#)

當網路資源位於CiscoWorks伺服器上時，備份排程器可以順利與其他SFTP使用者端協同工作，但無法與ACS 5.2協同工作。具體來說，當嘗試從ACS連線到SFTP伺服器時，會收到「Unable to negotiate a key exchange method」錯誤訊息。

解決方案

在這種情況下，SFTP伺服器不是使用DH 14組的FIPS相容裝置。ACS僅支援具有DH 14支援的伺服器，因為它與FIPS相容。有關此問題的詳細資訊，請參閱[ACS 5.2中的已知限制](#)。

問題："無效的EAP負載已丟棄"

ACS 5.07驗證無線使用者時，收到無效的EAP負載丟棄錯誤消息。

解決方案

這是一個已觀察到的行為，在Cisco錯誤ID [CSCsz54975](#)(僅限註冊客戶)和[CSCsy46036](#)(僅限註冊客戶)中進行了解決。

要解決此問題，請升級到ACS 5.0補丁9，這是升級到5.1或5.2所必需的。有關詳細資訊，請參閱[升級資料庫](#)。還包括有關如何升級到修補程式9的資訊。

問題："此時，ACS運行時進程未在此例項上運行。"

使用者無法登入到ACS GUI，收到以下錯誤消息：

ACSACS

解決方案

從CLI手動重新啟動運行時進程並重新啟動裝置可解決此問題。這是一個次要問題，不會給ACS帶來任何效能問題。存在兩個用於觀察此行為的次要錯誤。如需更多資訊，請參閱Cisco錯誤ID [CSCtb99448](#)(僅限註冊客戶)和[CSCtc75323](#)(僅限註冊客戶)。

若要手動重新啟動運行時進程，請從ACS CLI發出以下命令：

- **acs**停止運行時
- **acs**啟動運行時

問題：無法使用密碼匯出使用者

您可以使用CSV檔案將使用者資料庫匯出並匯入到另一個ACS 5.x，但它不包括使用者密碼欄位（顯示為空白）。如何將本地使用者的身份儲存庫從一個ACS移動到另一個包含密碼資訊的ACS？

解決方案

這是不可能的，因為這將成為安全漏洞。在這種情況下，一種解決方法是執行備份和還原過程。但是，此解決方法的限制是備份和還原僅對具有相似配置的其他ACS有效。

[問題：ACS內部使用者被間歇性禁用](#)

ACS使用者被間歇性禁用，並出現消息。密碼過期策略設定為60天，但必須手動啟用這些使用者才能獲得訪問許可權。

[解決方案](#)

觀察到此行為並在Cisco錯誤ID [CSCtf06311](#)(僅限[註冊](#)客戶)中存檔。此問題可以通過將補丁3應用於ACS 5.1來解決。要檢視補丁3下的所有已解決問題，請參閱[累積補丁ACS 5.1.0.44.3中已解決的問題](#)。有關如何升級補丁的相關資訊，請參閱[應用升級補丁](#)。

[問題："TACACS+身份驗證請求因錯誤而結束"](#)

ACS身份驗證報告顯示TACACS+誤消息。

[解決方案](#)

當TACACS身份驗證的「服務型別」設定為PPP時，會發生這種情況。如需詳細資訊，請參閱Cisco錯誤ID [CSCte16911](#)(僅限[註冊](#)客戶)。

[問題："由於嚴重日誌記錄錯誤，Radius身份驗證請求被拒絕"](#)

由於出現嚴重日誌記錄錯誤，RadiusRadius被拒絕。

[解決方案](#)

此錯誤在Cisco錯誤ID [CSCth66302](#)(僅限[註冊](#)客戶)中詳細說明。

[問題：ACS從5.2升級到5.3時，ACS檢視介面頁面頂部顯示「Data Upgrade Failed」（資料升級失敗）](#)

當ACS從5.2升級到5.3時，ACS檢視介面頁面頂部顯示Data Upgrade Failed。

[解決方案](#)

此錯誤在Cisco錯誤ID [CSCtu15651](#)(僅限[註冊](#)客戶)中詳細說明。

[問題：在Cisco ACS 5.0上發出「在下次登入acs時更改密碼」問題](#)

[解決方案](#)

在ACS 5.0中，本地使用者ID儲存中的密碼過期功能（使用者下次登入時必須更改密碼）是可選擇的，但不起作用。增強請求[CSCtc31598](#)修復了ACS 5.1版中的問題。

[問題："% Application upgrade failed， Error —999.請檢視ADE日](#)

誌以瞭解詳細資訊，或在升級期間在ACS裝置上重新運行為 — debug application install - enabled"

% Application upgrade failed Error -999ADEACS Express5.05.0.1以 — debug application install - enabled重新運行的錯誤。

解決方案

當使用的資料庫是TFTP且檔案大小大於32MB時，會發生此錯誤。ACS Express無法處理大於32MB的檔案。使用FTP作為儲存庫可解決此問題，即使檔案大小超過32MB。

問題：錯誤「身份驗證失敗：12308 Client sent Result TLV indicating failure (客戶端傳送的结果TLV指示失敗)」

12308 Client sent Result TLV(TLV)，指示ACS首次嘗試進行身份驗證時出現故障。第二次驗證工作正常。

解決方案

禁用Fast Reconnect時，可以解決此錯誤。升級到ACS 5.2版的Patch 2有助於解決此問題，同時不會禁用「快速重新連線」。

在請求方上禁用Forced cryptobinding時，也可以解決此錯誤。如需詳細資訊，請參閱Cisco錯誤ID [CSCtj31281](#)(僅限註冊客戶)。

問題：錯誤「24495 Active Directory伺服器不可用」

身份驗證開始失敗，出現以下錯誤：24495 Active Directory在ACS 5.3日誌中。

解決方案

通過ACS 5.x的CLI檢查ACSADAgent.log檔案，查詢以下消息：Mar 11 00:06:06 xlpacs01 adclient[30401]:INFO <bg:bindingRefresh> base.bind.healingxxxxxxxx。如果您看到unlatch錯誤消息，這意味著ACS 5.3無法與Active Directory保持穩定的連線。解決方法是切換到LDAP或將ACS降級到5.2版本。如需詳細資訊，請參閱Cisco錯誤ID [CSCtx71254](#)(僅限註冊客戶)。

問題：錯誤「5411 EAP會話超時」

ACS 5.x到5411 EAP會話超時錯誤消息。

解決方案

EAP會話超時在PEAP中非常常見，其中請求方在初始資料包傳出RADIUS伺服器後重新啟動身份驗證，在大多數情況下，不會指示問題。

常見的流程是：

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

最後，身份驗證成功。但是，由於請求方突然重新啟動EAP會話，導致EAP會話超時消息後成功進行身份驗證，因此ACS上有一個執行緒保持開啟狀態。很多時候，這是由於電腦的驅動程式級別造成的。確保客戶機上的網絡卡/無線驅動程式是最新的。您可以在客戶端上捕獲並過濾EAP || EAPOL，以檢視連線時客戶端接收或傳送的内容。

問題：如果在Active Directory上配置了登入限制，則802.1x身份驗證不起作用

如果使用者在Active Directory上配置了登入限制，則802.1x身份驗證不起作用。

解決方案

如果您有登入限制，請為一台電腦設定Active Directory並嘗試802.1x身份驗證。身份驗證失敗，因為Active Directory認為身份驗證來自ACS，而不是登入限制設定為的電腦。要使身份驗證成功，可將登入限制設定為包括ACS電腦帳戶。

問題：錯誤：具有ChangeUserPassword角色的ACS 5.x管理員更改密碼時「您無權檢視請求的頁面」

具有ChangeUserPassword角色的ACS 5.x GUI管理員使用者無法更改儲存在內部資料庫中的AAA使用者的密碼。變更密碼後，使用者會收到以下快顯錯誤訊息：

解決方案

從ACS 4.x遷移ACS 5.x資料庫時，可能會發生這種情況。使用SuperAdmin許可權更改使用者密碼。如需詳細資訊，請參閱Cisco錯誤ID [CSCty91045](#)(僅限註冊客戶)。

問題：在ACS 5.x上獲取身份驗證失敗的錯誤「24495 Active Directory伺服器不可用」。

解決方案

您需要驗證Active Directory與ACS 5.x的整合。如果是分散式設定，請確保設定中的主ACS 5.x和輔助ACS 5.x與Active Directory正確整合。

問題：無法使用BMC連線到ACS裝置

在使用BMC客戶端(硬體級工具)進入ACS 1121 IBM伺服器時，可以發現BMC客戶端有兩個IP地

址。

解決方案

已識別此行為並記錄在Cisco錯誤ID [CSCtj81255](#)(僅限註冊客戶)。為了解決此問題，您需要禁用ACS 1121上的BMC DHCP客戶端。

問題：監控和報告常規儀20000板中出現警告警報「刪除活動會話」，其原因為「活動會話超出限制」。

會話目錄可以保留的記錄數量有限。由於客戶設定中的探測請求數量很大，因此可以快速達到限制。達到限制後，ACS-View會從會話目錄中刪除一定數量的記錄（例如20k）並傳送警報。您可以增加此限制，但除了延長警報外，它無濟於事。

解決方案

要解決此問題，請執行以下操作：

- 建議禁用日誌記錄以檢視資料庫。轉至Cisco Secure ACS > System Administration > Configuration > Log Configuration > Logging Categories > Global > "Passed Authentications" > Remote Syslog Target並從所選目標中刪除LogCollector。轉至Cisco Secure ACS > System Administration > Configuration > Log Configuration > Logging Categories > Global > "Failed Attempts" > Remote Syslog Target並從所選目標中刪除LogCollector。轉至Cisco Secure ACS >系統管理>配置>日誌配置>日誌記錄類別>全域性>編輯：「RADIUS記帳」>遠端系統日誌目標，並從選定目標中刪除LogCollector。
- 您可以忽略探測身份驗證請求，因為這些請求不是真正的身份驗證請求。執行以下操作：轉到Cisco Secure ACS > Monitoring Configuration > System Configuration > Add Filter並建立過濾器。根據使用者名稱建立過濾器更為適合，因為探測請求被理解為使用虛擬使用者名稱傳送。如果您在ACS中建立單獨的訪問策略來處理這些探測請求，則還可以根據訪問服務建立過濾器。

問題：ACS 5.x錯誤「11013 RADIUS資料包已在進程中」

在ACS 5.3部署中，使用者無法通過dot1x身份驗證。使用的資料庫是Active Directory。RADIUS故障代碼如下所示：

```
RADIUS11013 RADIUS
```

解決方案

ACS已忽略此請求，因為它是當前正在處理的另一個資料包的副本。發生這種情況的原因可能有以下任一情況：

- 「平均RADIUS請求延遲」統計資訊接近或超過客戶端的客戶端RADIUS請求超時。
- 外部身份儲存可能非常慢。
- ACS已過載。

執行以下步驟以解決：

1. 增加客戶端的客戶端RADIUS請求超時。
2. 使用速度更快或額外的外部身份庫。
3. 按照以下方法減少ACS上的過載。

問題：RADIUS驗證失敗，錯誤為「11012 RADIUS封包包含無效標頭」

解決方案

傳入RADIUS資料包的報頭分析不正確。為了解決此問題，請驗證以下內容：

- 檢查網路裝置或AAA客戶端是否有硬體問題。
- 檢查將裝置連線到ACS的網路是否有硬體問題。
- 檢查網路裝置或AAA客戶端是否有任何已知RADIUS相容性問題。

問題：RADIUS/TACACS+驗證失敗，錯誤為「11007找不到網路裝置或AAA客戶端」

當ASA傳送radius訪問請求消息時，ACS上會收到以下錯誤消息：

```
11007AAA
```

解決方案

發生這種情況的原因是ACS客戶端的IP與實際傳送請求的介面IP不匹配。有時，防火牆會執行到此AAA客戶端的地址轉換。驗證AAA客戶端是否正確配置了以下路徑上正確的轉換IP地址：

網路資源>網路裝置和AAA客戶端

問題：RADIUS驗證失敗，錯誤為「11050 RADIUS request dropped due to system overload」。

由於身份驗證失敗，使用者無法訪問網路。收到來自ACS的以下錯誤消息：

```
11050 RADIUS
```

解決方案

Cisco ACS由於過載而丟棄這些身份驗證請求。這可能是由許多並行驗證請求的複製引起的。為了避免此問題，請執行以下任一操作：

- 修改Network Device/AAA Client設定，使其使用Legacy TACACS+ Single Connection Support選項。這樣，客戶端會對所有請求重複使用同一會話，而不是建立多個會話。
- 在某一時間點，避免使用者呼叫新的身份驗證請求。
- 重新啟動ACS伺服器。

問題：RADIUS身份驗證失敗，錯誤為「11309 Incorrect RADIUS MS-CHAP v2屬性」。

解決方案

之所以出現此錯誤，是因為收到的RADIUS訪問請求資料包中的一個MSCHAP v2屬性 (MS-CHAP-Challenge、MS-CHAP-Response、MS-CHAP-CPW-2或MS-CHAP-NT-Enc-PW) 的長度無效或值不正確。

問題：ACS報告記憶體使用率超過90%。警報

ACS報告記憶體使用率超過90%。警報如下所示：`Cisco Secure ACS - ACS - ACS/ - ACSCPU(%) (%) I/O (%) (%) /opt(%) /localdisk:(%) / (%)KOM-AAA02 0.41 90.14 0.02 9.57 5.21 25.51`

解決方案

ACS 5.2上通常出現此問題。要解決此問題，請重新載入ACS以釋放記憶體或升級到ACS 5.2補丁7或更高版本。如需詳細資訊，請參閱Cisco錯誤ID [CSCtk52607](#)(僅限註冊客戶)。

問題：錯誤

: com.cisco.nm.acs.mgmt.msgbus.FatalBusException:無法連結節點

在維護任務 (加入主、強制完全複製、打補丁) 之後的分散式設定中，ACS例項A在分散式部署螢幕中報告ACS例項B為離線，而B實際上處於聯機狀態，且報告例項A為聯機。在管理日誌中，您會看到`com.cisco.nm.acs.mgmt.msgbus.FatalBusException:。`

解決方案

如果在新例項啟動並嘗試繫結到埠2030時，複製管理服務的上一個例項仍繫結到該埠，則會發生這種情況。從ACS例項B的CLI運行：`sho acs-logs file ACSMmanagement.log | i。` 您將看到類似復制服2030。目前，解決方法是重新啟動ACS例項B (將另一個例項報告為聯機的)。如需詳細資訊，請參閱Cisco錯誤ID [CSCtx56129](#)(僅限註冊客戶)。

問題：錯誤

: com.cisco.nm.acs.mgmt.msgbus.FatalBusException:無法連結節點

在維護任務 (加入主、強制完全複製、打補丁) 之後的分散式設定中，ACS例項A在分散式部署螢幕中報告ACS例項B為離線，而B實際上處於聯機狀態，且報告例項A為聯機。在管理日誌中，您會看到`com.cisco.nm.acs.mgmt.msgbus.FatalBusException:。`

解決方案

升級到ACS 5.2補丁6或更高版本以解決此問題。如需詳細資訊，請參閱Cisco錯誤ID

[CSCto47203](#)(僅限[註冊](#)客戶)。

注意：當「/opt」使用率超過30%時，viewDB備份將失敗。當「」/opt「」使用率超過30%時，需要配置NFS轉儲以執行備份。

問題：錯誤11026未找到請求的dACL

RADIUS驗證失敗，錯誤消息如下：11026dACL。

解決方案

由於未找到RADIUS Access-Request中請求的可下載ACL的版本，因此請求被拒絕。對可下載ACL的請求在原始Access-Request之後很長時間才發生。因此，可下載ACL的版本不再可用。從RADIUS使用者端要求可下載ACL時，尋找此延遲的原因。

問題：錯誤11025請求的dACL的Access-Request缺少值為aaa:event=acl-download的cisco-av-pair屬性。請求被拒絕

RADIUS驗證失敗，錯誤消息如下：11025dACLAccess-Requestaaa:event=acl-downloadcisco-av-pair。

解決方案

可下載ACL的每個Access-Request都必須具有值為aaa:event=acl-download的cisco-av-pair屬性。在這種情況下，該屬性缺少請求，ACS未能通過請求。檢查網路裝置或AAA客戶端是否有任何已知RADIUS相容性問題。

問題：錯誤11023未找到請求的dACL。這是未知的dACL名稱

RADIUS驗證失敗，錯誤消息如下：11023dACLdACL。

解決方案

檢查ACS配置，驗證授權配置檔案中指定的可下載ACL是否存在於可下載ACL清單中。這是ACS端配置錯誤。

問題：管理員身份驗證失敗，錯誤為10001內部錯誤。配置版本不正確

管理員身份驗證失敗，錯誤為：10001。

解決方案

此錯誤可能是由於ACS資料庫損壞或基礎配置資料出現問題。如需詳細資訊，請聯絡[Cisco TAC](#)(僅限[註冊](#)客戶)。

問題：管理員身份驗證失敗，錯誤為10002內部錯誤：無法載入適當的服務

管理員身份驗證失敗，錯誤為：10002。

解決方案

ACS 5.x無法載入AAC配置服務。這可能是由於ACS資料庫損壞或基礎配置資料出現問題。當系統資源耗盡時也可能發生這種情況。如需詳細資訊，請聯絡[Cisco TAC](#)(僅限[註冊](#)客戶)。

問題：管理員身份驗證失敗，錯誤為10003內部錯誤：管理員身份驗證收到空管理員名稱

管理員身份驗證失敗，錯誤為：10003稱。

解決方案

訪問ACS 5.x的GUI時，ACS收到空白使用者名稱。檢查傳輸到ACS的使用者名稱的有效性。如果有效，請聯絡[Cisco TAC](#)(僅限[註冊](#)客戶)瞭解詳細資訊。

問題：失敗原因：24428 LRPC、LDAP或KERBEROS中發生連線相關錯誤

ACS上收到此錯誤消息：

```
24428LRPCLDAPKERBEROSRPC
```

解決方案

為了解決此問題，請將ACS升級到5.2版。

問題：從ACS 5.x伺服器運行IOS 15.x的路由器上，TACACS+身份驗證代理無法正常工作

從ACS 5.x伺服器運行Cisco IOS軟體版本15.x的路由器上，TACACS+身份驗證代理無法正常工作。

解決方案

只有ACS 5.3補丁5支援TACACS+身份驗證代理。請升級ACS 5.x，或使用RADIUS進行身份驗證代理。

問題：從ACS 5.x獲取錯誤消息Store failure(acs-xxx, TacacsAccounting)

解決方案

ACS 5.1 TACACS記帳報告從客戶端收到格式錯誤的記帳資料包時，遺漏了幾個屬性，例如使用者名稱、許可權級別和請求型別。在某些情況下，這會導致「檢視」中生成「儲存故障(acs-xxx、TacacsAccounting)」警報。為了解決此問題，請驗證以下內容：

- 客戶端傳送的記帳資料包具有格式錯誤的TACACS引數（例如，AAA客戶端傳送的任何引數的長度和值不匹配）。
- 確保客戶端傳送一個有效的記帳資料包，該資料包具有適當的引數長度和值。

如需詳細資訊，請參閱Cisco錯誤ID [CSCte88357](#)(僅限[註冊](#)客戶)。

問題：使用者身份驗證失敗，錯誤11036為「The Message-Authenticator RADIUS attribute is invalid。」

解決方案

驗證以下內容：

- 檢查AAA客戶端和ACS伺服器上的共用金鑰是否匹配。
- 確保AAA客戶端和網路裝置沒有硬體問題或RADIUS相容性問題。
- 確保將裝置連線到ACS的網路沒有硬體問題。

問題：RADIUS記帳失敗，錯誤為「11037 Dropped accounting request received via unsupported port」。

解決方案

記帳請求被丟棄，因為它是通過不受支援的UDP埠號接收的。驗證以下內容：

- 確保AAA客戶端和ACS伺服器上的記帳埠號配置匹配。
- 確保AAA客戶端沒有硬體問題或RADIUS相容性問題。

問題：RADIUS記帳失敗，錯誤為「11038 Accounting-Request header contains invalid Authenticator field」。

ACS無法驗證RADIUS Accounting-Request資料包報頭中的Authenticator欄位。Authenticator欄位不得與Message-Authenticator RADIUS屬性相混淆。確保AAA客戶端上配置的RADIUS共用金鑰與為ACS伺服器上的選定網路裝置配置的金鑰匹配。此外，請確保AAA客戶端沒有硬體問題或RADIUS相容性問題。

錯誤："ACS24493使用其電腦憑據與Active Directory通訊時出現問題。"

解決方案

檢查ACS的AD連線，並確保ACS電腦帳戶仍在AD中。

問題："使用特殊字元(如"ê")建立外殼配置檔名稱時，ACS可能崩潰。"

解決方案

已識別此行為並記錄在Cisco錯誤ID [CSCts17763](#)(僅限註冊客戶)。您需要升級到5.3.40 patch 1或5.2.26 patch 7。

問題：在第2行獲取「分析錯誤：在ACS 5.x CLI上運行「show run」時，格式不正確（無效令牌）。

解決方案

確保ACS上配置的SNMP社群具有有效字元。社群名稱中只允許使用字母數字字元（僅限字母和數字）。

問題：ACS 5.x /opt分割槽很快滿

解決方案

ACS 5.x磁碟空間不足，因為/opt分割槽空間不足。出現這種情況是因為大量日誌記錄資料泛洪ACS檢視。作為解決方法，您需要經常替換View資料庫。因為ACS View無法每天處理數GB的資料，您需要組織日誌記錄資料。當您需要所有日誌時，請使用外部系統日誌伺服器而不是ACS檢視。當只需要使用部分日誌記錄資料時，請使用系統管理>配置>日誌配置>日誌記錄類別>全域性以僅將所需的日誌傳送到ACS檢視日誌收集器。

問題：正在查詢所需域

加入Active Directory域時，ACS 5.x是否可以查詢所需的域控制器(DC)?

解決方案

否。目前，ACS會通過域查詢DNS，以獲取域中所有DC的清單。然後，它嘗試與所有使用者進行通訊。如果連到一個DC的連線都失敗，則與域的ACS連線將宣告為失敗。

問題：同時存在父域和子域

是否可以在父域和子域中同時設定ACS 5.x?

解決方案

不能。目前，ACS 5.x只能是一個域的一部分。但是，ACS 5.x可以對來自多個受信任域的使用者/電腦進行身份驗證。

問題：記錄到遠端資料庫

是否可以將ACS 5.x檢視資料記錄到遠端資料庫？

解決方案

是，ACS 5.x允許您將ACS檢視資料記錄到Microsoft SQL伺服器 and Oracle SQL伺服器。

問題：VMWare支援

解決方案

可以在虛擬機器上安裝ACS 5.x。以下這些VMWare版本中可以安裝最新版本ACS 5.3:

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

問題：磁碟空間要求

ACS 5.x評估版本的磁碟空間要求是什麼？

解決方案

評估版本至少需要60 GB磁碟空間。生產安裝需要500 GB。

問題："24401法與ACS Active Directory代理建立連線。"

解決方案

若要解決此錯誤，請驗證以下內容：

- 檢查ACS電腦是否已加入Active Directory域。
- 檢查ACS電腦和Active Directory伺服器之間的連線狀態。
- 檢查ACS Active Directory代理是否正在運行。

如需詳細資訊，請參閱Cisco錯誤ID [CSCtx71254](#)(僅限註冊客戶)。

問題：「運行時」進程顯示「執行失敗」狀態

使用修補程式更新Cisco ACS時，運行時進程將停滯在「執行失敗」狀態，並且會記錄以下消息：

```
"local0 err err 83 2012-06-12T12:11:08+0200 192.168.150.74 ACS ACS/opt/CSCOacs/runtime/bin/run-  
logforward.sh:187097/$daemon -b -f $logfile
```

解決方案

這可能是最後一個修補程式的MD5修補程式的問題。驗證應用於Cisco ACS的最後一個補丁的MD5校驗和。重新下載，然後正確應用。

[問題：UCS強制重新身份驗證時ACS身份驗證失敗](#)

UCS伺服器配置為從Cisco ACS對Java客戶端進行身份驗證。身份驗證過程包括使用RSA令牌伺服器。第一個身份驗證通過。但是，當UCS刷新並強制Java客戶端重新驗證時，由於RSA不允許重複使用任何令牌，UCS將失敗。因此，身份驗證失敗。

[解決方案](#)

從UCS伺服器的角度來看，這是限制，但從Cisco ACS的角度來看則不是。UCS伺服器遵循雙因素身份驗證，該功能在與RSA令牌一起使用時不受思科ACS支援。目前不支援。作為解決方法，建議您使用除RSA令牌伺服器之外的任何資料庫伺服器（如AD或LDAP）。

[問題："24444 Active Directory操作因ACS中發生未指定的錯誤而失敗"](#)

[解決方案](#)

AD相關操作中出現未對映錯誤。請參閱[ACS 5.x與Microsoft AD整合配置示例](#)，並正確配置ACS與AD的整合。如果所有內容都已根據文檔正確配置，請聯絡Cisco TAC進行進一步的故障排除。

[問題：無法使用AD 2008 R2伺服器驗證ACS 5.1使用者](#)

[解決方案](#)

出現這種情況是因為存在不相容問題。僅ACS 5.2版本支援AD 2008 R2整合。將ACS升級到5.2或更高版本。如需詳細資訊，請參閱Cisco錯誤ID [CSCtg12399](#)(僅限註冊客戶)。

[錯誤：22056在適用的標識儲存中找不到主題。](#)

當SSL VPN使用者嘗試從RSA裝置獲得身份驗證時，從Cisco ACS伺服器收到以下錯誤消息：

22056

[解決方案](#)

檢查該使用者是否存在於指向ACS查詢的資料庫中。對於RSA和RADIUS身份庫，請確保選擇Treat Reject選項作為身份驗證失敗。它位於Identity Store配置的Advanced頁籤下。

[問題：ipt_connlimit:哎呀：無效的ct狀態？](#)

ipt_connlimit:ct當ACS 5.x在VMWare上運行時，控制檯上會顯示錯誤消息。

[解決方案](#)

這是一個裝腔作勢的資訊。如需詳細資訊，請參閱Cisco錯誤ID [CSCth25712](#)(僅限[註冊](#)客戶)。

問題：AC 5.x/ISE在來自Cisco IOS軟體版本15.x NAS的RADIUS請求中看不到radius calling-station-id屬性

AC 5.x / ISE在Cisco IOS軟體版本15.x NAS的RADIUS請求中看不到radius calling-station-id屬性。

解決方案

在Cisco IOS軟體版本15.x上使用[radius-server attribute 31 send nas-port-detail](#) 命令以啟用傳送屬性。

問題：使用者帳戶在第一次出現錯誤憑據時鎖定，即使配置了3次嘗試

當ACS 5.3在Windows 2008 R2功能級別與Active Directory整合時，在使用者僅輸入錯誤憑證一次後，使用鎖定引數設定的使用者帳戶（3次不正確的嘗試）會過早鎖定。

解決方案

如需詳細資訊，請參閱Cisco錯誤ID [CSCtz03211](#)(僅限[註冊](#)客戶)。

問題：無法從ACS儲存備份

嘗試從ACS儲存備份時， - 0.08GB0.08GB」警告。

解決方案

不能同時運行增量備份、完全備份和資料清除。如果其中任何一個作業正在運行，則必須等待90分鐘，才能開始下一個作業。

相關資訊

- [思科安全存取控制系統支援頁面](#)
- [思科安全存取控制系統終端使用者指南](#)
- [技術支援與文件 - Cisco Systems](#)