安全訪問控制系統5.x及更高版本常見問題

目錄

簡介

本文回答與思科安全存取控制系統(ACS)5.x及更新版本相關的最常見問題(FAQ)。

驗證相關問題

問：能否將ACS 5.x內部資料庫的少數使用者/組從使用者密碼策略（系統管理>使用者>身份驗證設定）中排除？

A.默認情況下，每個內部資料庫使用者必須遵守使用者密碼策略。目前，無法排除ACS 5.x內部資料庫的使用者/組。

問：是否可以從管理使用者密碼策略（系統管理>管理員>設定>身份驗證）中排除幾個ACS 5.x的GUI管理員？

答：預設情況下，每個GUI管理使用者都必須遵守管理使用者密碼策略。目前，無法排除ACS 5.x的管理使用者。

問：ACS 5.x是否支援VMWare工具？

答：否。目前，ACS 5.x版不支援VMWare工具。如需詳細資訊，請參閱Cisco錯誤ID CSCtg50048(僅限註冊客戶)。

問：將LDAP配置為身份庫時，ACS 5.x支援哪些EAP身份驗證協定？

A.將LDAP用作身份庫時，ACS 5.2僅支援PEAP-GTC、EAP-FAST-GTC和EAP-TLS協定。它不支援EAP-FAST MSCHAPv2、PEAP EAP-MSCHAPv2和EAP-MD5。有關詳細資訊，請參閱身份驗證協定和使用者資料庫相容性。

問：在ACS上使用RADIUS的WLC身份驗證為什麼失敗？為什麼ACS未顯示任何失敗的嘗試？

答：在修補程式4之前，**ACS 5.0和WLC的互操作性存在問**題。請下載修補程式8，然後在CLI上應用該修補程式。請勿使用TFTP解決此問題。

問：為什麼我無法還原在ACS 5.2中使用backup-log命令備份的tar.gz檔案？

A.無法還原使用backup-log命令備份的日誌文件。您只能恢復為ACS配置和ADE-OS備份的檔案。如需詳細資訊，請參閱思科安全存取控制系統5.1的CLI參考指南中的backup和backup-logs命令。

問：是否可以限制ACS 5.2上密碼嘗試失敗次數？

答：否。此功能在ACS 5.2上不可用，但預計將在ACS 5.3中整合。有關詳細資訊，請參閱Cisco安全訪問控制系統5.2發行說明的「不支援的功能」部分。

問：我無法使用該選項在ACS 5.0中更改內部使用者的下次登入密碼。如何解決此問題？

答：ACS 5.0不支援在下次登入時更改密碼的選項。ACS 5.1及更高版本提供對此功能的支援。

ACS上的警報表示什麼意思？

```
Cisco Secure ACS - Alarm Notification
Severity: Warning
Alarm Name delete 20000 sessions
Cause/Trigger active sessions are over limit
Alarm Details session is over 250000
```

A.此錯誤表示當ACS檢視達到250,000個會話的限制時，它會發出警報以刪除20,000個會話。ACS檢視資料庫儲存所有先前的身份驗證會話，當達到250,000時，它會發出警報以清除快取並刪除20,000個會話。

問：如何解決此錯誤消息：24407Active Directory?

A.當SDI身份驗證期間的密碼管理出現問題時，將顯示此錯誤消息。ACS 5.x用作Radius代理，且使用者必須由RSA伺服器進行身份驗證。RSA的Radius代理只有在沒有密碼管理的情況下才能運行。原因是OTP值必須由Radius伺服器恢復，才能將密碼值代理到RSA伺服器。在隧道組中啟用密碼管理後，會使用MS-CHAPv2屬性傳送Radius請求。RSA不支援MS-0CHAPv2;它僅支援PAP。

為了解決此問題，請禁用密碼管理。如需更多資訊，請參閱Cisco錯誤ID CSCsx47423(僅限註冊客戶)。

問：是否可以限制ACS管理員僅管理ACS 5.1中的某些裝置？

答：不，不能限制ACS管理員僅管理ACS 5.1中的某些裝置。

問：ACS是否支援身份驗證中的QoS，以便可以將RADIUS優先於TACACS?

答：不，ACS不支援身份驗證中的QoS。ACS不會通過TACACS或通過RADIUS確定RADIUS身份驗證請求的優先順序。

問：ACS 5.x是否可以代理其他TACACS或RADIUS伺服器的TACACS和RADIUS身份驗證？

答：是，所有ACS 5.x版本均可將RADIUS身份驗證代理到其他RADIUS伺服器。ACS 5.3及更高版本可以將TACACS身份驗證代理到其他TACACS伺服器。

問：ACS 5.x是否可以檢查Active Directory使用者的撥入屬性以授予訪問許可權？

答：是，在ACS 5.3及更高版本中，您可以允許、拒絕和控制對使用者的撥入許可權的訪問。從Active Directory進行身份驗證或查詢時檢查許可權。它設定在Active Directory專用字典上。

問：ACS 5.x是否支援TACACS的CHAP或MSCHAP身份驗證型別+?

答：是，ACS 5.3及更新版本支援TACACS+ CHAP和MSCHAP身份驗證型別。

問：是否可以將ACS內部使用者的密碼型別設定為任何外部資料庫？

答：是，在ACS 5.3及更高版本中，您可以設定ACS內部使用者的密碼型別。ACS 4.x提供此功能。

問：是否可以根據在ACS內部身份庫中建立使用者的時間，通過/拒絕身份驗證？

答：是，在ACS 5.3及更高版本中，可以使用「自使用者建立以來的小**時**」屬性來建立策略。此屬性包含從使用者在Internal Identity Store中建立到當前身份驗證請求為止的小時數。

問：是否可以使用萬用字元在ACS內部資料庫中新增新主機條目？

答：是，ACS 5.3及更高版本允許您在內部身份庫中新增新主機時使用萬用字元。它還允許您輸入萬用字元（在輸入前三個八位元後），以指定來自已標識製造商的所有裝置。

問：是否可在ACS 5.x上配置IP地址池並從ACS分配它們？

答：否，目前無法在ACS 5.x上建立IP地址池。

問：是否可以在「FAILED AUTHENTICATION」報告中看到請求來自的AAA客戶端的IP地址？

答：不，無法檢視請求來自哪裡的AAA客戶端的IP地址。

問：什麼是ACS 5.3中的檢視日誌消息恢復？

答：ACS 5.3提供了一項新功能，可恢復檢視關閉時丟失的任何日誌。ACS會收集這些丟失的日誌並將其儲存在資料庫中。使用此功能，您可以在備份檢視後從ACS資料庫將丟失的日誌檢索到檢視資料庫。為了使用此功能，您必須將日誌消息恢復配置設定為**on**。有關配置檢視日誌消息恢復的詳細資訊，請參閱監視和報告檢視器系統操作。

問：是否可以從解決方案引擎CLI發出database-compress命令壓縮ACS 5.x資料庫？ACS 4.x提供此功能。

答：是，在ACS 5.3及更高版本中，**database-compress命令通過刪除ACS事務表的選項來減小ACS資料庫大小。ACS管理員可以發出此命令來減小資料庫大小。**這有助於減少資料庫大小，以及進行維護所需的備份和完全同步所需的時間。

問：我是否可以根據某個AAA客戶端的IP地址搜尋該條目？

答：是，ACS 5.3及更高版本允許您使用其IP地址搜尋網路裝置。您還可以使用萬用字元和範圍來搜尋一組特定的網路裝置。

問：是否可以根據在ACS內部身份庫中建立使用者的時間建立條件？

答：是，在ACS 5.3及更高版本中，可以使用「自使用者建立以來的小時數」屬性，該屬性允許您根據在ACS內部身份儲存庫中建立使用者的時間，配置策略規則條件。例如：如果**group=HelpDesk&NumberOfHoursSinceUserCreation>48，則**拒絕。此屬性包含從使用者在Internal Identity Store中建立到當前身份驗證請求為止的小時數。

問：我是否可以在服務策略的「授權」部分中籤入對使用者進行身份驗證的身份庫？

答：是，在ACS 5.3及更高版本中，可以使用**Authentication Identity Store屬性，該屬性使您能夠根據Authentication Identity Store配置策略規則條件。**例如：如果**AuthenticationIdentityStore=LDAP_NY**，則拒絕。此屬性包含使用的身份儲存庫的名稱，在身份驗證成功後，將用相關的身份儲存庫名稱更新此屬性。

問：ACS何時轉至身份庫序列中定義的下一個身份庫？

A.在以下情況下，ACS將轉至身份庫序列中定義的下一個身份庫：

- 在第一個身份儲存中找不到使用者
- 序列中沒有身份庫

問： ACS 5.3中的帳戶停用策略是什麼？

答：帳戶禁用策略允許您在配置日期超過允許日期、配置的天數超過允許天數，或連續不成功登入嘗試次數超過閾值時禁用內部身份儲存的用戶。日期超過的預設值為自當前日期起30天。天數的預設值不應超過自當前日期起的60天。失敗嘗試的預設值為5。

問：是否可以通過telnet更改ACS的內部資料庫使用者的口令？

答：是，您允許通過telnet使用TACACS+更改內部資料庫使用者的密碼。您需要在**ACS 5.x上的密碼更改控制**下選擇**Enable TELNET Change Password**。

問：主ACS 5.x例項是否定期自動更新備份例項，或者僅在配置發生更改時才更新？

答：每當在主ACS上進行更改時，ACS 5.x將立即複製到輔助ACS。此外，如果您沒有對主ACS進行任何更改，它將每15分鐘執行一次強制複製。此時，沒有控制計時器的選項，因此ACS可以在特定時間後複製資訊。

問：是否可以檢視/匯出當前從不同NAS客戶端上的ACS登入和驗證的所有使用者的ACS 5.x報告？

是的，這是可能的。RADIUS和TACACS+有兩個獨立的報告。您可以在Monitoring & Reports > Reports > Catalog > **Session Directory** > **RADIUS Active Sessions**和TACACS Active Sessions下找到它們。這兩個報告都基於NAS客戶端的記帳資訊，因為它允許您跟蹤使用者連線和註銷的時間。會話歷史記錄甚至允許您在特定日期從開始和停止消息獲取資訊。

相關資訊

- 思科安全存取控制系統支援頁面
- 技術支援與文件 - Cisco Systems