

ASA和ACS的RSA令牌伺服器 and SDI 協定使用情況

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[理論](#)

[通過RADIUS的RSA](#)

[通過SDI的RSA](#)

[SDI協定](#)

[組態](#)

[ACS上的SDI](#)

[ASA上的SDI](#)

[疑難排解](#)

[RSA上沒有代理配置](#)

[損壞的金鑰節點](#)

[處於掛起模式的節點](#)

[帳戶已鎖定](#)

[最大過渡單元\(MTU\)問題和分段](#)

[ACS的資料包和調試](#)

[相關資訊](#)

簡介

本文檔介紹RSA Authentication Manager(可與思科自適應安全裝置(ASA)和思科安全訪問控制伺服器(ACS)整合)的故障排除過程。

RSA Authentication Manager是一個提供一次性密碼(OTP)進行身份驗證的解決方案。該密碼每60秒更改一次，且只能使用一次。它同時支援硬體和軟體令牌。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- Cisco ASA CLI配置
- Cisco ACS配置

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco ASA軟體8.4版及更高版本
- Cisco Secure ACS 5.3版及更高版本

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。

理論

可以使用RADIUS或專有的RSA協定訪問RSA伺服器：SDI。ASA和ACS都可以使用這兩種協定（RADIUS、SDI）來訪問RSA。

請記住，使用軟體令牌時，RSA可以與Cisco AnyConnect安全移動客戶端整合。本文檔僅重點介紹ASA和ACS整合。有關AnyConnect的詳細資訊，請參閱[Cisco AnyConnect安全移動客戶端管理員指南3.1版](#)中的[使用SDI身份驗證](#)部分。

通過RADIUS的RSA

與SDI相比，RADIUS有一個很大的優勢。在RSA上，可以將特定配置檔案（在ACS上稱為組）分配給使用者。這些配置檔案定義了特定的RADIUS屬性。身份驗證成功後，從RSA返回的RADIUS-Accept消息包含這些屬性。ACS根據這些屬性做出其他決定。最常見的情況是決定使用ACS組對映將與RSA上的配置檔案相關的特定RADIUS屬性對映到ACS上的特定組。使用此邏輯，可以將整個授權過程從RSA移動到ACS，並且仍然可以保持精細的邏輯，如RSA上的邏輯。

通過SDI的RSA

相較於RADIUS，SDI有兩個主要優勢。第一個是整個作業階段已加密。第二個是SDI代理提供的有趣選項：可以確定建立失敗是因為身份驗證或授權失敗還是因為未找到使用者。

ACS在操作中使用此資訊獲取身份。例如，它可以繼續執行「未找到使用者」操作，但拒絕「身份驗證失敗」操作。

RADIUS和SDI之間還有一個差異。當ASA等網路接入裝置使用SDI時，ACS僅執行身份驗證。使用RADIUS時，ACS會執行驗證、授權、記帳(AAA)。不過，這並不是什麼大區別。可以配置SDI進行身份驗證，RADIUS進行相同會話的記帳。

SDI協定

預設情況下，SDI使用使用者資料包協定(UDP)5500。SDI使用與RADIUS金鑰類似的對稱加密金鑰來加密會話。該金鑰儲存在節點金鑰檔案中，並且對於每個SDI客戶端都是不同的。該檔案可手動或自動部署。

附註：ACS/ASA不支援手動部署。

對於自動部署節點，在第一次成功身份驗證之後自動下載機密檔案。使用從使用者的密碼和其它資訊匯出的金鑰加密節點金鑰。這會產生一些可能的安全問題，因此第一次身份驗證應該在本機執行，並使用加密協定（Secure Shell [SSH]，而不是telnet），以確保攻擊者無法攔截和解密該檔案。

組態

附註：

使用[命令查詢工具](#)(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

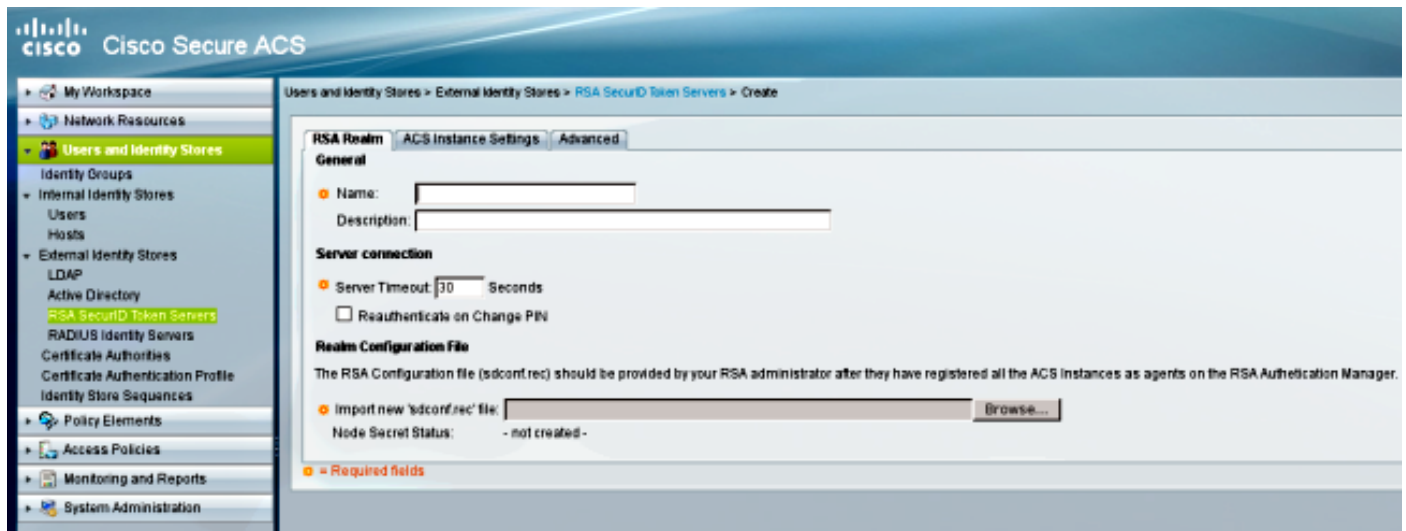
[輸出直譯器工具](#)(僅供已註冊客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸出的分析。

使用 debug 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

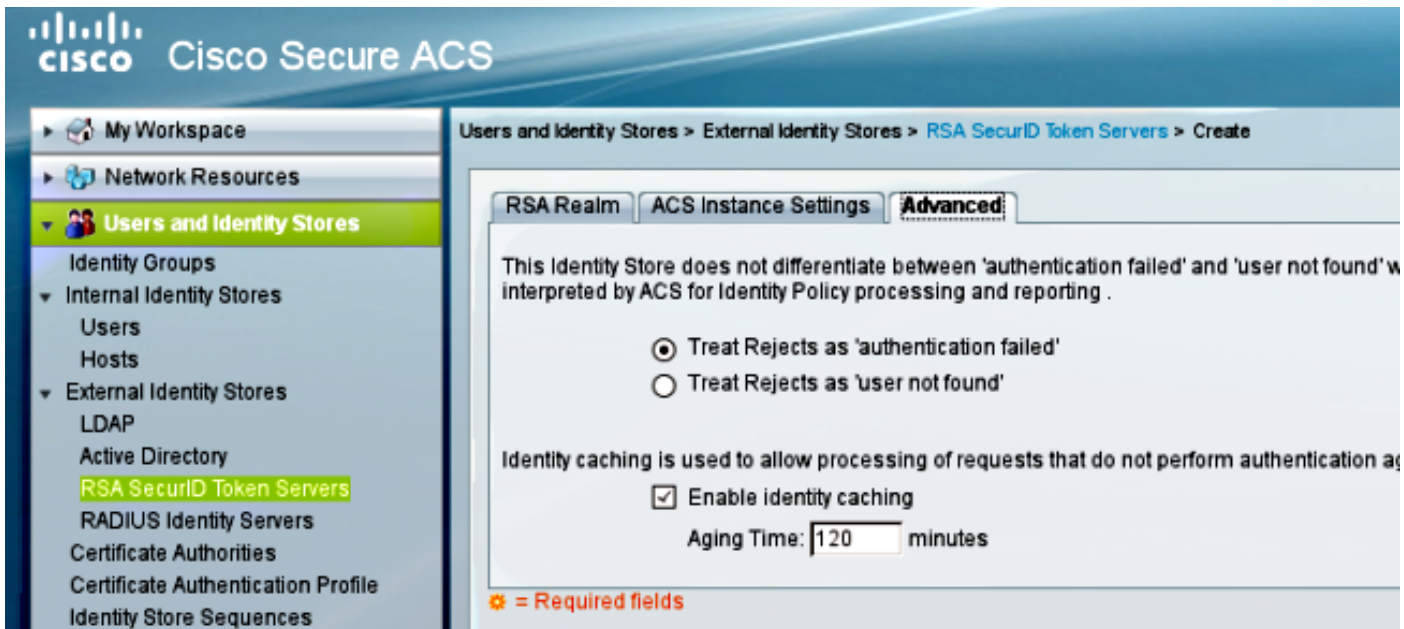
ACS上的SDI

在Users and Identity Stores > External Identity Store > RSA Secure ID Token Servers中配置。

RSA有多個副本伺服器，例如ACS的輔助伺服器。不需要將所有地址都放在此處，只需輸入RSA管理員提供的sdconf.rec檔案。此檔案包括主RSA伺服器的IP地址。在第一個成功的身份驗證節點之後，會隨所有RSA複製副本的IP地址一起下載機密檔案。



若要區分「未找到使用者」和「身份驗證失敗」，請在Advanced頁籤中選擇設定：



還可以在多個RSA伺服器（主伺服器和複製副本）之間更改預設路由（負載平衡）機制。使用RSA管理員提供的sdopts.rec檔案更改它。在ACS中，它會上傳到**使用者和身份庫>外部身份庫>RSA安全ID令牌伺服器>ACS例項設定**中。

對於群集部署，應複製配置。第一次成功身份驗證後，每個ACS節點使用從主RSA伺服器下載的自己的節點金鑰。請務必記住為群集中的所有ACS節點配置RSA。

ASA上的SDI

ASA不允許上傳sdconf.rec檔案。與ACS一樣，它僅允許自動部署。需要手動配置ASA以指向主RSA伺服器。不需要密碼。在第一個成功的身份驗證節點之後，將安裝金鑰檔案（快閃記憶體上的.sdi檔案），並且保護其他身份驗證會話。另外，還會下載其他RSA伺服器的IP地址。

以下是範例：

```
aaa-server SDI protocol sdi
aaa-server SDI (backbone) host 1.1.1.1
debug sdi 255
test aaa auth SDI host 1.1.1.1 user test pass 321321321
```

身份驗證成功後，**show aaa-server protocol sdi**或**show aaa-server <aaa-server-group>**命令會顯示所有RSA伺服器（如果有多個伺服器），而**show run**命令僅顯示主IP地址：

```
bsns-asa5510-17# show aaa-server RSA
Server Group: RSA
Server Protocol: sdi
Server Address: 10.0.0.101
Server port: 5500
Server status: ACTIVE (admin initiated), Last transaction at
10:13:55 UTC Sat Jul 27 2013
Number of pending requests 0
Average round trip time 706ms
Number of authentication requests 4
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
```

Number of accepts	1
Number of rejects	3
Number of challenges	0
Number of malformed responses	0
Number of bad authenticators	0
Number of timeouts	0
Number of unrecognized responses	0

SDI Server List:

Active Address:	10.0.0.101	
Server Address:	10.0.0.101	
Server port:	5500	
Priority:	0	
Proximity:	2	
Status:	OK	
Number of accepts		0
Number of rejects		0
Number of bad next token codes		0
Number of bad new pins sent		0
Number of retries		0
Number of timeouts		0
Active Address:	10.0.0.102	
Server Address:	10.0.0.102	
Server port:	5500	
Priority:	8	
Proximity:	2	
Status:	OK	
Number of accepts		1
Number of rejects		0
Number of bad next token codes		0
Number of bad new pins sent		0
Number of retries		0
Number of timeouts		0

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

RSA上沒有代理配置

在許多情況下，安裝新的ASA或更改ASA IP地址後，很容易忘記在RSA上進行同樣的更改。需要為所有訪問RSA的客戶端更新RSA上的代理IP地址。然後，生成新的節點金鑰。這同樣適用於ACS，尤其是輔助節點，因為它們具有不同的IP地址，RSA需要信任它們。

損壞的金鑰節點

有時ASA或RSA上的加密節點檔案會損壞。然後，最好刪除RSA上的代理配置並再次新增。您還需要在ASA/ACS上執行相同的流程 — 再次刪除和新增配置。此外，刪除快閃記憶體中的.sdi檔案，以便在下次身份驗證時安裝新的.sdi檔案。一旦完成自動節點金鑰部署，應立即進行。

處於掛起模式的節點

有時某個節點處於掛起模式，這是因為該伺服器沒有響應造成的：

```
asa# show aaa-server RSA
<.....output ommited"
SDI Server List:
Active Address: 10.0.0.101
Server Address: 10.0.0.101
Server port: 5500
Priority: 0
Proximity: 2
Status: SUSPENDED
```

在掛起模式下，ASA不會嘗試向該節點傳送任何資料包；它需要具有OK狀態。在失效計時器之後，故障伺服器再次進入活動狀態。有關詳細資訊，請參閱[Cisco ASA系列命令參考 9.1指南中的 reactivation-mode命令](#)部分。

在這種情況下，最好刪除並新增該組的AAA伺服器配置，以便再次將該伺服器觸發到活動模式。

帳戶已鎖定

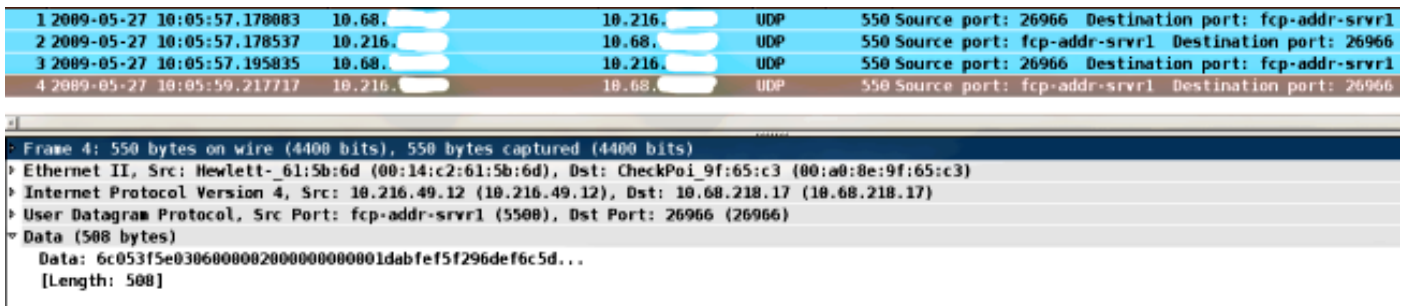
多次重試後，RSA可能會鎖定該帳戶。它很容易通過報告在RSA上檢查。在ASA/ACS上，報告僅顯示「身份驗證失敗」。

最大過渡單元(MTU)問題和分段

SDI使用UDP作為傳輸，而不是MTU路徑發現。此外，UDP流量預設未設定「不分段(DF)」位元。有時對於較大的資料包，可能存在分段問題。很容易在RSA上嗅探流量（裝置和虛擬機器[VM]都使用Windows並使用Wireshark）。在ASA/ACS上完成相同的過程並進行比較。此外，在RSA上測試RADIUS或WebAuthentication，以便將其與SDI進行比較（以便縮小問題範圍）。

ACS的資料包和調試

由於SDI負載已加密，因此排除捕獲故障的唯一方法是比較響應的大小。如果小於200位元組，則可能存在問題。典型的SDI交換涉及四個資料包，每個資料包為550個位元組，但這種情況可能會隨RSA伺服器版本而改變：



```
1 2009-05-27 10:05:57.178083 10.68.  10.216.  UDP 550 Source port: 26966 Destination port: fcp-addr-srvr1
2 2009-05-27 10:05:57.178537 10.216.  10.68.  UDP 550 Source port: fcp-addr-srvr1 Destination port: 26966
3 2009-05-27 10:05:57.195835 10.68.  10.216.  UDP 550 Source port: 26966 Destination port: fcp-addr-srvr1
4 2009-05-27 10:05:59.217717 10.216.  10.68.  UDP 550 Source port: fcp-addr-srvr1 Destination port: 26966

Frame 4: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits)
  Ethernet II, Src: Hewlett-61:5b:6d (00:14:c2:61:5b:6d), Dst: CheckPoi_9f:65:c3 (00:a0:8e:9f:65:c3)
  Internet Protocol Version 4, Src: 10.216.49.12 (10.216.49.12), Dst: 10.68.218.17 (10.68.218.17)
  User Datagram Protocol, Src Port: fcp-addr-srvr1 (5500), Dst Port: 26966 (26966)
  Data (508 bytes)
    Data: 6c053f5e03060000200000000001dabfe15f296def6c5d...
    [Length: 508]
```

發生問題時，交換的資料包通常多於四個且大小較小：

- [技術支援與文件 - Cisco Systems](#)