

排除ISE會話管理和狀態故障

目錄

[簡介](#)

[背景資訊](#)

[問題](#)

[終端使用者體驗](#)

[ISE管理員體驗](#)

[常見問題場景](#)

[陳舊/幻像會話問題](#)

[ISE會話管理邏輯](#)

[MNT和作業階段管理](#)

[PSN和會話管理](#)

簡介

本文檔描述常見身份服務引擎(ISE)終端安全評估服務問題：「AnyConnect ISE終端安全評估模組顯示合規性.....」

背景資訊

本文檔描述常見身份服務引擎(ISE)終端安全評估服務問題 — AnyConnect ISE終端安全評估模組在ISE上的會話狀態為掛起時顯示合規性。

雖然症狀始終相同，但此問題可能有多個根本原因。

通常，對此類問題進行故障排除會非常耗時，從而造成嚴重影響。

本檔案將說明：

- 從終端使用者和ISE管理員的角度顯示問題。
- 常見問題場景。
- 觸發問題的ISE、AnyConnect和網路操作背後的理論。
- 快速問題識別演算法。
- 常見問題情景的經典解決方案。
- 通過Radius會話目錄進行狀態共用。

如需稍後介紹的概念的更詳細說明，請參閱：

[ISE終端安全評估樣式比較，用於前期和後期2.2](#)

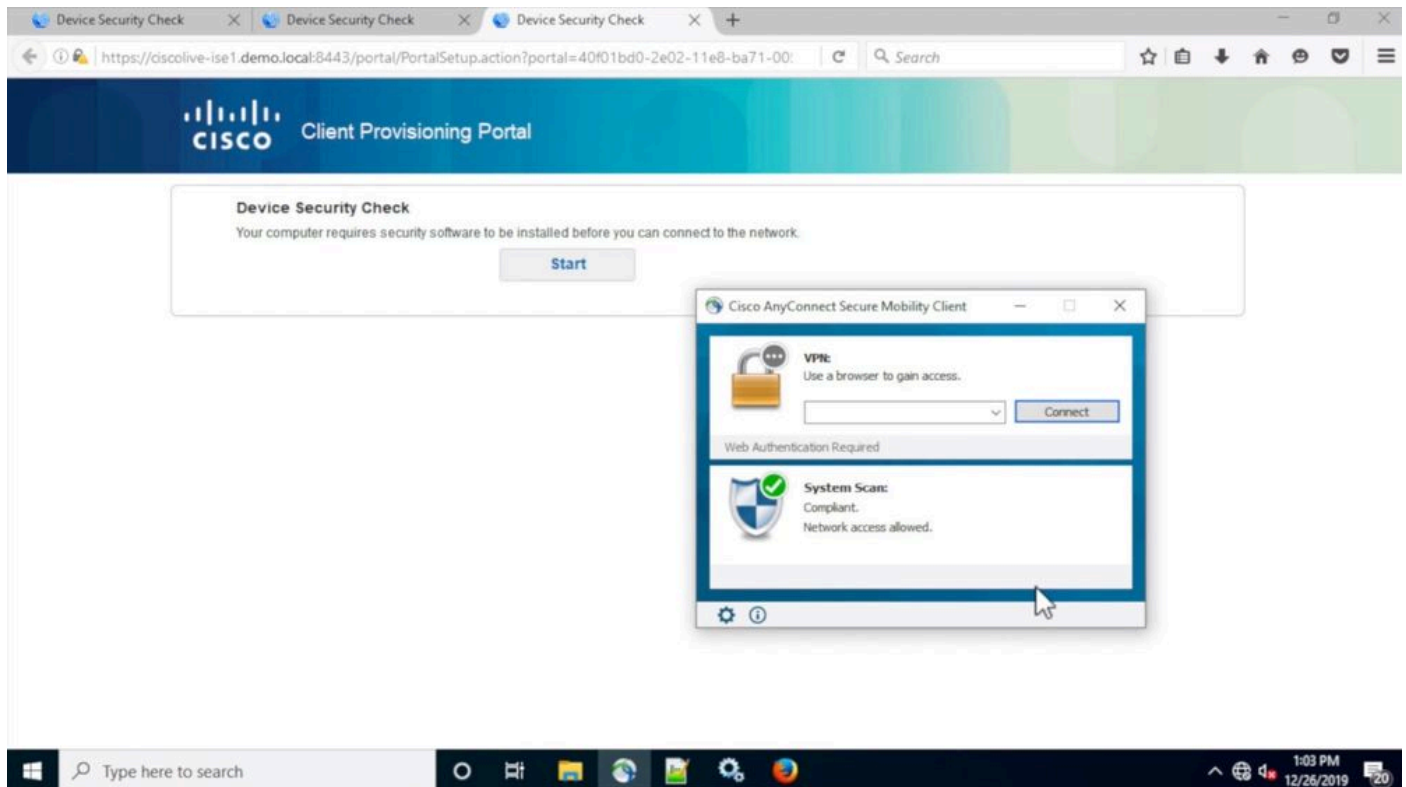
[放大鏡下的ISE。如何排除ISE故障 — BRKSEC-3229](#)

問題

終端使用者體驗

此問題通常表現為瀏覽器中沒有網路訪問或經常重定向到ISE客戶端調配門戶，同時AnyConnect ISE終端安全評估模組將終端安全評估狀態顯示為Compliant。

典型的終端使用者體驗：



ISE管理員體驗


通常，在此問題的初始分類中，ISE管理員執行Radius Live日誌調查以確保有一個實際身份驗證到達ISE。

在此階段發現的第一個症狀表示終端和ISE之間的狀態不匹配，如在即時日誌中或Radius身份驗證報告終端上次成功身份驗證顯示Pending狀態狀態。

典型的ISE管理員體驗：

Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication ...	Authorization Policy	Network Device	Device Port	Identity Group	Posture St...
			Identity	Endpoint ID	Endpoint Profile	Authentication Poli	Authorization Policy	Network Device	Device Port	Identity Group	Posture Status
			alice	C0-4A-00-1F-6B-39	Microsoft-Workstation	Default -> Dot1X	Default -> DEMO-OPP-POLICY				Compliant
			alice	C0-4A-00-1F-6B-39	Microsoft-Workstation	Default -> Dot1X	Default -> DEMO-OPP-POLICY	DEMO-WLC		RegisteredDevices	Pending

- Alice的上次成功身份驗證。
- 會話的狀態為Pending。
- Alice的最後一個會話事件。
- 會話事件將狀態顯示為Compliant。

 注意：當描述的問題清單出現時，活動日誌並不總是顯示c.和d.。狀態為符合的作業階段事件更常見於由過期或虛擬作業階段造成的情況，本檔案稍後將對此進行說明。

常見問題場景

此問題通常出現在兩個有問題的場景中，並且每個場景都有多個根本原因。場景：

- AnyConnect ISE終端安全評估模組在終端安全評估過程中被策略服務節點(PSN)錯誤告知，導致顯示錯誤的終端安全評估狀態。在這種情況下，我們通常處理PSN會話快取中的過時或幻像會話。
- AnyConnect ISE顯示上一個發現週期的狀態為當前身份驗證未觸發發現進程。AnyConnect中的ISE終端安全評估模組具有有限數量的事件，這些事件會觸發發現進程，並且可能會在身份驗證或重新身份驗證期間未檢測到這些事件。

陳舊/幻像會話問題

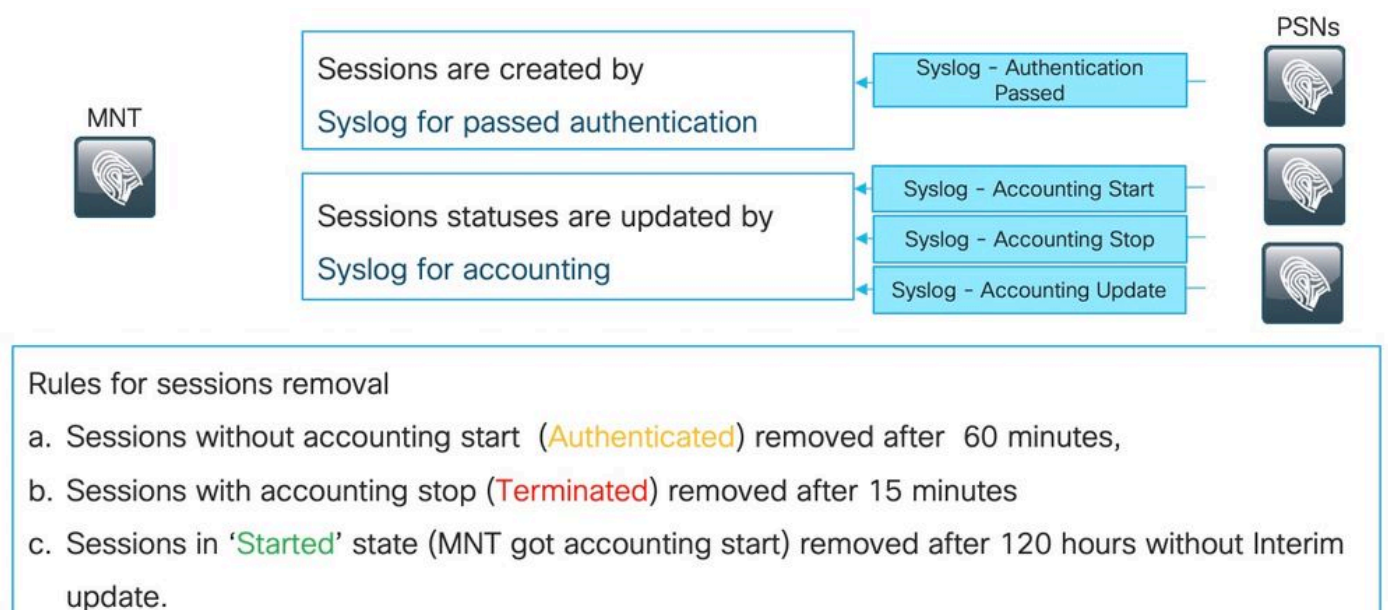
為了更好地瞭解問題，請調查所需的ISE會話管理邏輯和AnyConnect發現流程。

ISE會話管理邏輯

在ISE部署中，有兩個人員負責會話管理流程：PSN和監控節點(MNT)。

要正確排除故障並確定此問題，請務必瞭解兩個角色上的會話管理理論。

MNT和作業階段管理



如本圖所述，MNT節點根據來自PSN的經過身份驗證的系統日誌消息建立季節。

系統日誌可以更新後續會話狀態以進行記帳。

MNT上的會話刪除在3種情況下發生：

- 未計帳的作業階段在建立後約60分鐘就已移除。每5分鐘執行一次cron作業以檢查會話狀態和清除。
- 已終止的會話在被同一cron作業處理記帳停止後約15分鐘刪除。

- 每次執行上的相同cron都會刪除已處於「Started」狀態超過5天 (120小時) 的會話。已啟動狀態表示MNT節點已處理身份驗證和計費，以啟動會話的系統日誌。

來自PSN的系統日誌消息示例。當runtime-aaa元件啟用到DEBUG時，這些消息將登入到prrt-server.log。粗體部分可用於構建搜尋正規表示式。

通過身份驗證：

```
<#root>
```

```
AcsLogs
```

```
,  
2020-04-07 10:07:29,202  
,DEBUG,0x7fa0ada91700,cntx=0000629480,sesn=skuchere-ise26-1/375283310/10872,CPMSessionID=0A3E946C000000  
5200 NOTICE Passed-Authentication: Authentication succeeded  
, ConfigVersionId=87, Device IP Address=10.62.148.108, DestinationIPAddress=192.168.43.26, DestinationP  
bob@example.com  
, NAS-IP-Address=10.62.148.108, NAS-Port=50105, Service-Type=Framed, Framed-IP-Address=192.168.255.205,  
0A3E946C00000073559C0123  
\;42SessionID=skuchere-ise26-1/375283310/10872\;, Calling-Station-ID=  
00-50-56-B6-0B-C6  
, NAS-Port-Type=Ethernet, NAS-Port-Id=GigabitEthernet1/0/5, EAP-Key-Name=, cisco-av-pair=service-type=F
```

記帳開始：

```
<#root>
```

```
AcsLogs
```

```
,  
2020-04-07 10:07:30,202  
,DEBUG,0x7fa0ad68d700,cntx=0000561096,sesn=skuchere-ise26-1/375283310/10211,CPMSessionID=0A3E946C000000  
3000 NOTICE Radius-Accounting: RADIUS Accounting start request  
, ConfigVersionId=87, Device IP Address=10.62.148.108, UserName=  
bob@example.com  
, RequestLatency=7, NetworkDeviceName=3850-1-BB, User-Name=bob@example.com, NAS-IP-Address=10.62.148.10  
0A3E946C00000073559C0123  
:skuchere-ise26-1/375283310/10210, Called-Station-ID=00-E1-6D-D1-4F-05, Calling-Station-ID=  
00-50-56-B6-0B-C6  
, Acct-Status-Type=Start, Acct-Delay-Time=0, Acct-Session-Id=00000041, Acct-Authentic=Remote, Event-Tim
```

中期會計更新：

<#root>

AcsLogs,2020-04-07 22:57:48,642,

DEBUG,0x7fa0adb92700,cntx=0000629843,sesn=skuchere-ise26-1/375283310/10877,CPMSessionID=0A3E946C0000007

3002 NOTICE Radius-Accounting: RADIUS Accounting watchdog update

, ConfigVersionId=87, Device IP Address=10.62.148.108, UserName=

bob@example.com

, RequestLatency=8, NetworkDeviceName=3850-1-BB, User-Name=bob@example.com, NAS-IP-Address=10.62.148.10

00-50-56-B6-0B-C6

, Acct-Status-Type=Interim-Update, Acct-Delay-Time=0, Acct-Input-Octets=2293926, Acct-Output-Octets=0, A

0A3E946C00000073559C0123

, cisco-av-pair=method=dot1x, AcsSessionID=skuchere-ise26-1/375283310/10877, SelectedAccessService=Defa

記帳停止：

<#root>

AcsLogs,2020-04-08 11:43:22,356

,DEBUG,0x7fa0ad68d700,cntx=0000696242,sesn=skuchere-ise26-1/375283310/11515,CPMSessionID=0A3E946C0000007

3001 NOTICE Radius-Accounting: RADIUS Accounting stop request

, ConfigVersionId=88, Device IP Address=10.62.148.108, UserName=

bob@example.com

, RequestLatency=12, NetworkDeviceName=3850-1-BB, User-Name=bob@example.com, NAS-IP-Address=10.62.148.10

00-50-56-B6-0B-C6

, Acct-Status-Type=Stop, Acct-Delay-Time=0, Acct-Input-Octets=4147916, Acct-Output-Octets=0, Acct-Sessi

0A3E946C00000073559C0123

, cisco-av-pair=method=dot1x, AcsSessionID=skuchere-ise26-1/375283310/11515, SelectedAccessService=Defa

PSN和會話管理

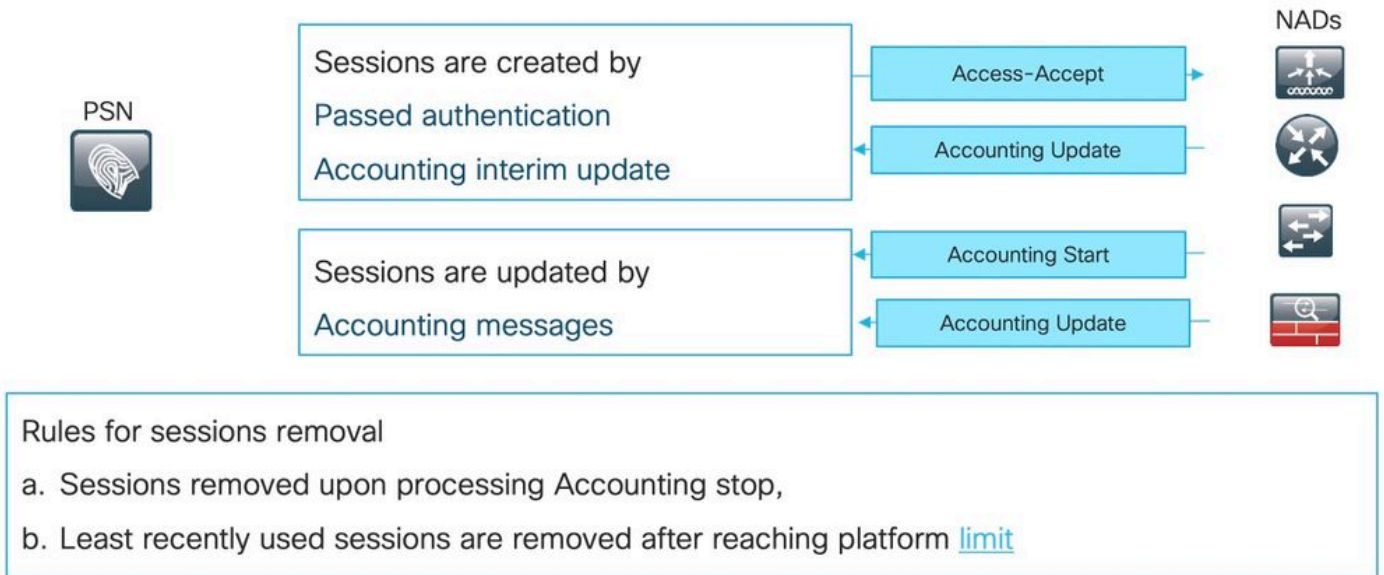
什麼是PSN會話快取？

儲存特定PSN的所有活動會話的記憶體中資料庫。會話快取始終是節點本地的，而且ISE中沒有任何機制可以執行從一個節點到另一個節點的完整會話狀態複製。

對於每個活動會話ID，PSN儲存身份驗證/授權階段收集的所有屬性，如內部/外部使用者組、網路接入裝置(NAD)屬性、證書屬性等。PSN使用這些屬性來選擇不同的策略型別，如身份驗證、授權、客戶端調配、狀態。

當節點或節點自身上的服務重新啟動時，會話快取被完全刪除。

Who is responsible for session management in ISE deployment?



當前會話處理邏輯在兩個場景中在會話快取中建立一個新條目，以後對現有會話的詳細資訊可以從來自NAD的記帳消息進行更新：

- 會話已在PSN上成功通過身份驗證。
- PSN獲取會話的記帳臨時更新，該更新在會話快取中不存在。

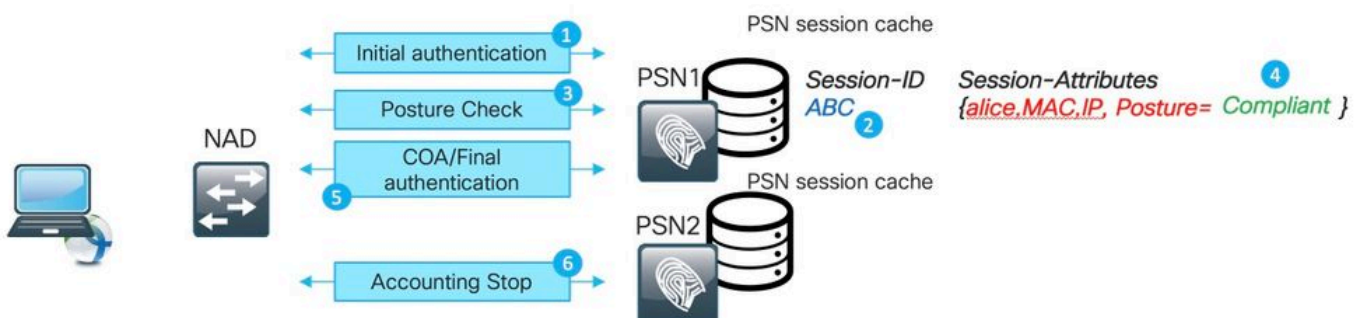
在會話刪除方面，PSN將實現以下邏輯：

- 處理記帳停止消息後立即刪除會話快取條目。
- 當節點達到活動會話數的1000時，PSN開始刪除最近最少使用的會話。

PSN上的過時會話

在ISE部署中，未執行實際身份驗證的PSN已處理現有會話的記帳停止：

陳舊會話示例：



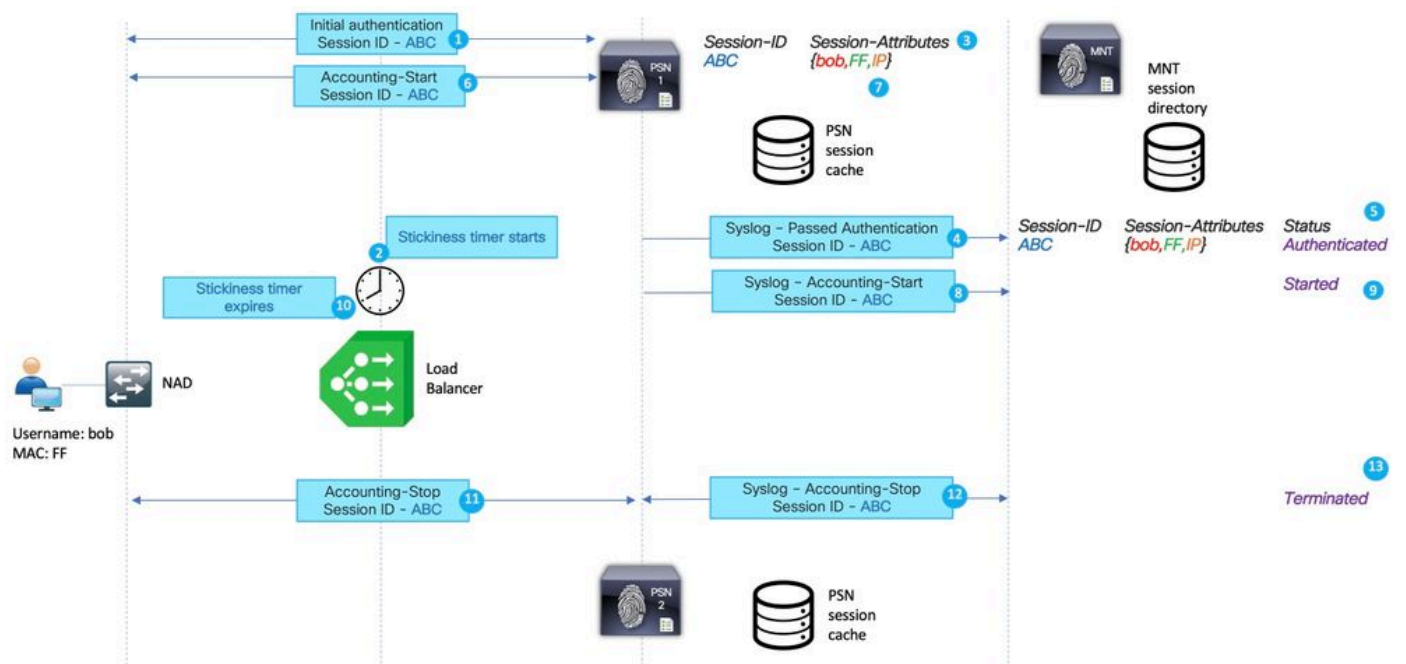
- 1.在PSN上對會話ABC成功進行身份驗證。
2. PSN在會話快取中建立條目。
- 3.進行狀態評估。
- 4.標籤為符合的會話。
- 5.狀態更改觸發的授權更改(COA)導致終端重新身份驗證以應用下一個訪問級別。
- 6.會話ABC的記帳停止將到達PSN2。

在步驟6會話之後，ABC在PSN1上停滯在陳舊狀態，因為此PSN上不會處理會計停止消息以將其刪除。如果部署未遇到大量身份驗證嘗試，則會長時間刪除會話。

在以下情況下，過時會話將顯示在PSN會話快取中：

- 由於負載平衡器上的粘性計時器過期，記帳停止到達錯誤的PSN。
- NAD上的錯誤配置與為身份驗證和記帳配置的PSN不同。
- 網路路徑上的臨時連線問題，導致NAD故障切換到下一個PSN。

負載平衡器(LB)環境中過時會話的示例：



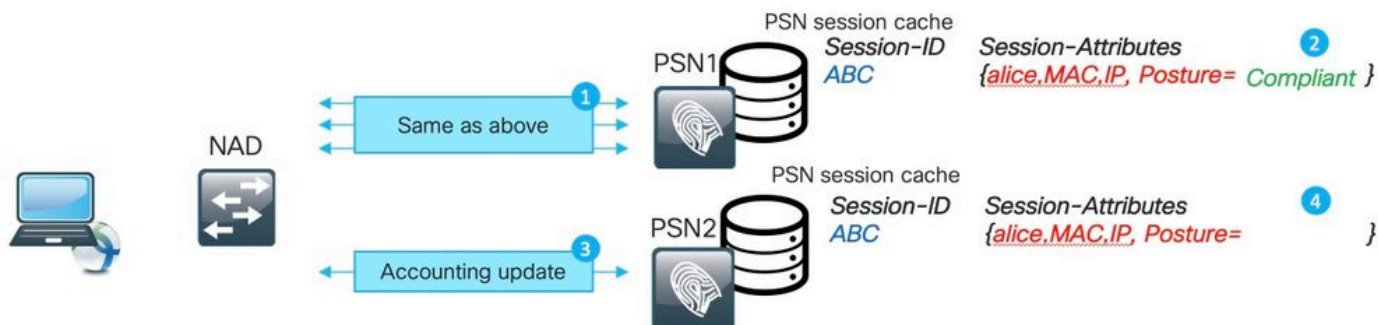
- 1.由PSN 1執行的會話ABC的初始身份驗證。
- 2.此身份驗證會在負載平衡器上啟動粘性計時器。
3. PSN 1在本地快取中為會話ABC建立條目。
- 4.已傳遞身份驗證的系統日誌消息已傳輸到MNT節點。

- 5.在MNT會話目錄中建立的會話ABC的條目，狀態為Authenticated。
- 6.會話ABC的記帳開始消息位於PSN 1上。
- 7.會話ABC的會話快取條目已使用Accounting-Start中的資訊更新。
8. Accounting-Start的系統日誌消息已傳輸到MNT節點。
- 9.會話狀態更新為已啟動。
- 10.負載均衡器上的粘性計時器過期。
- 11.負載平衡器向PSN 2轉發的會話ABC的記帳停止。
12. PSN 2將記帳停止的系統日誌消息轉發到MNT。
- 13.在MNT上標籤為終止的會話ABC。

PSN上的虛擬會話

幻像會話是指當記帳臨時更新到達未對此特定會話執行身份驗證的PSN時的場景。在此方案中，在PSN會話快取中建立一個新條目，如果PSN沒有收到該會話的記帳停止消息，則不會刪除該條目，除非PSN達到活動會話的限制。

虛擬會話示例：



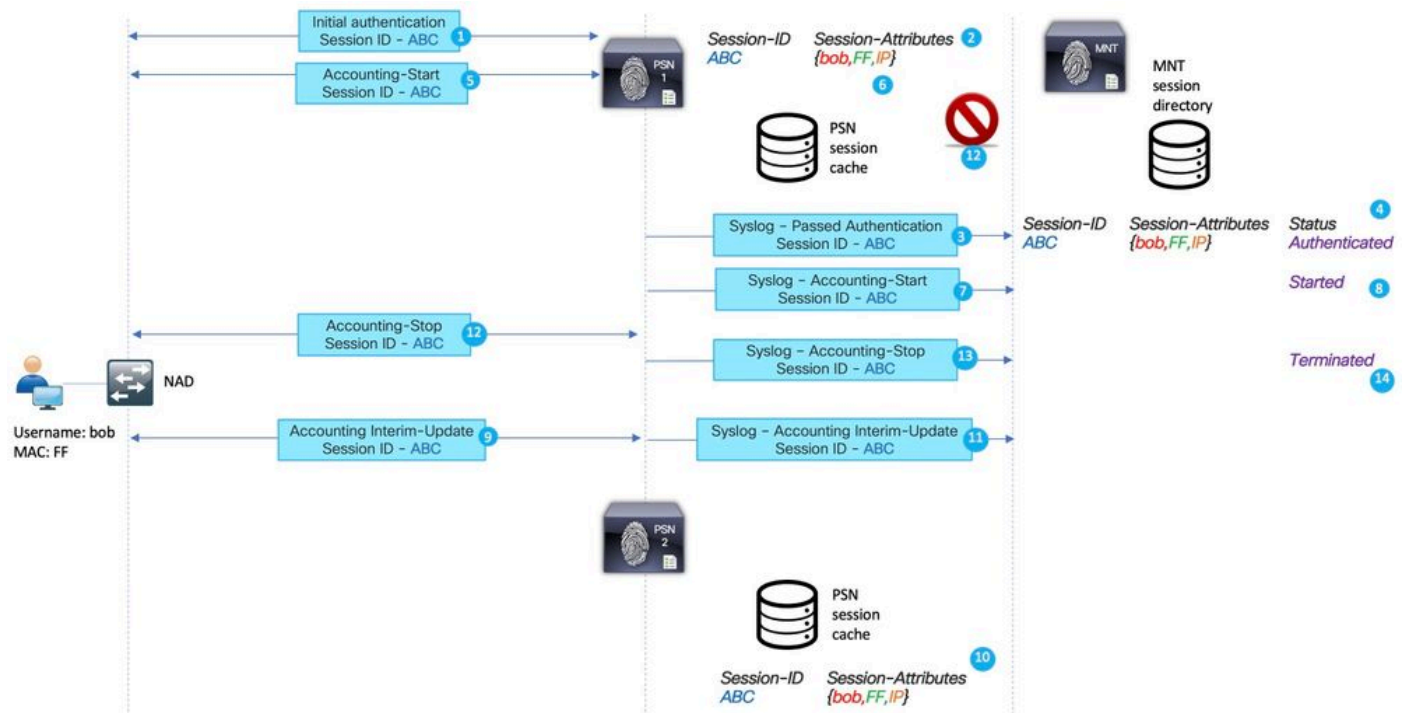
- 1.在PSN1上為會話ABC執行與過時會話示例中所述相同的步驟。
- 2.會話ABC在PSN1會話快取中的狀態為Compliant。
- 3.會話ABC的會計臨時更新命中PSN2。

4.在PSN2上建立的會話ABC的會話條目。由於會話條目是從記帳消息建立的，因此其屬性數量有限。例如，狀態狀態不可用於會話ABC。還缺少使用者組和其他授權特定屬性等內容。

在以下情況下，虛擬會話出現在PSN會話快取中：

- 網路傳輸中的短期中斷。
- 網路訪問裝置的不行為。
- 負載平衡器上的行為錯誤或配置錯誤。

通向PSN1的網路路徑上出現臨時問題的方案的虛擬會話示例：



- 1.由PSN執行的會話ABC的初始身份驗證。
2. PSN1在本地快取中為會話ABC建立條目。
- 3.已傳遞身份驗證的系統日誌消息已傳輸到MNT節點。
- 4.在TimesTen DB中建立的會話ABC的條目，狀態為Authenticated。
- 5.會話ABC的記帳開始消息位於PSN 1上。
- 6.會話ABC的會話快取條目已使用Accounting-Start中的資訊更新。
7. Accounting-Start的系統日誌消息已傳輸到MNT節點。

8. 會話狀態更新為已啟動。

9. 會話ABC的臨時會計更新已轉發到PSN2。

10. PSN2在本地快取中為會話ABC建立條目。

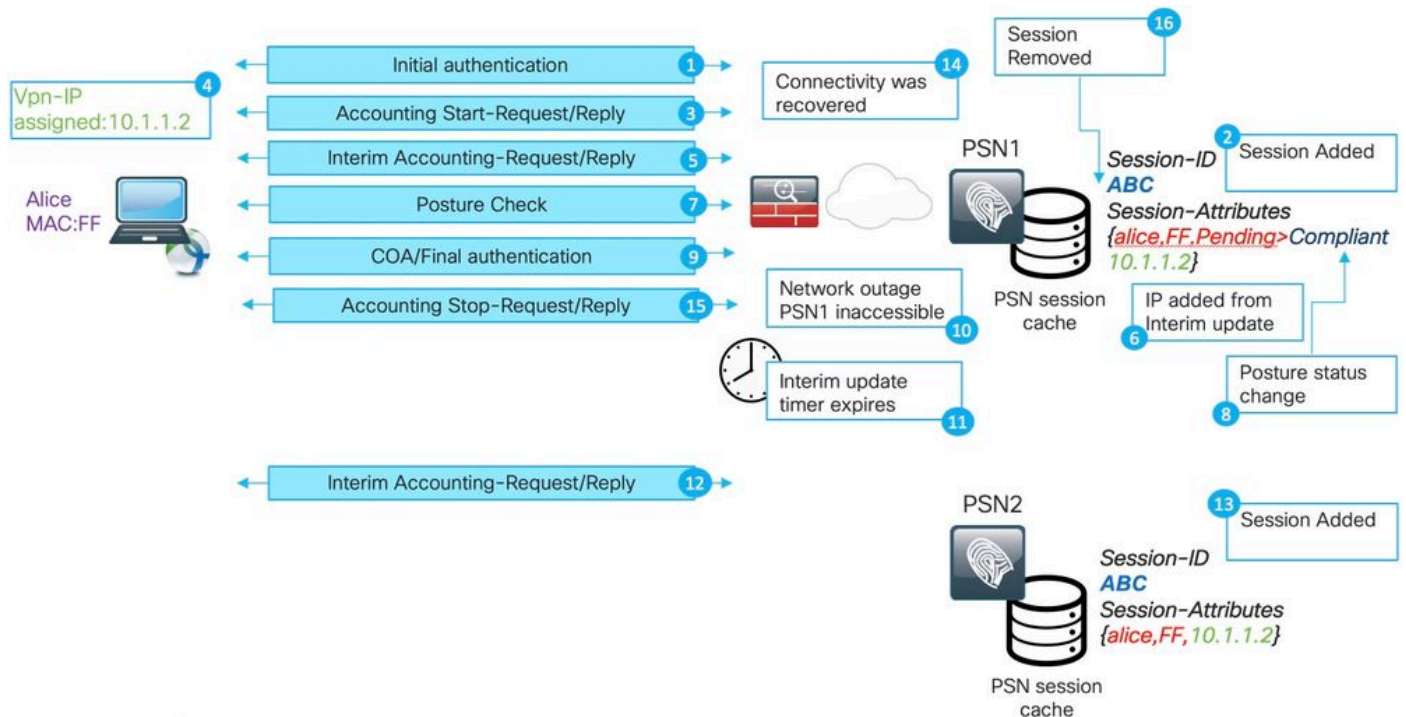
11. 將會話ABC轉發到PSN1的記帳停止。

12. 會話ABC的條目已從PSN1上的會話快取中刪除。

13. PSN 1將記帳停止的系統日誌消息轉發到MNT。

14. 在MNT上標籤為終止的會話ABC。

為長壽VPN連線建立的虛擬會話場景：



1. PSN1上的初始身份驗證。

2. 在會話快取中建立的會話ABC。

3. 記帳會啟動PSN處理的消息。

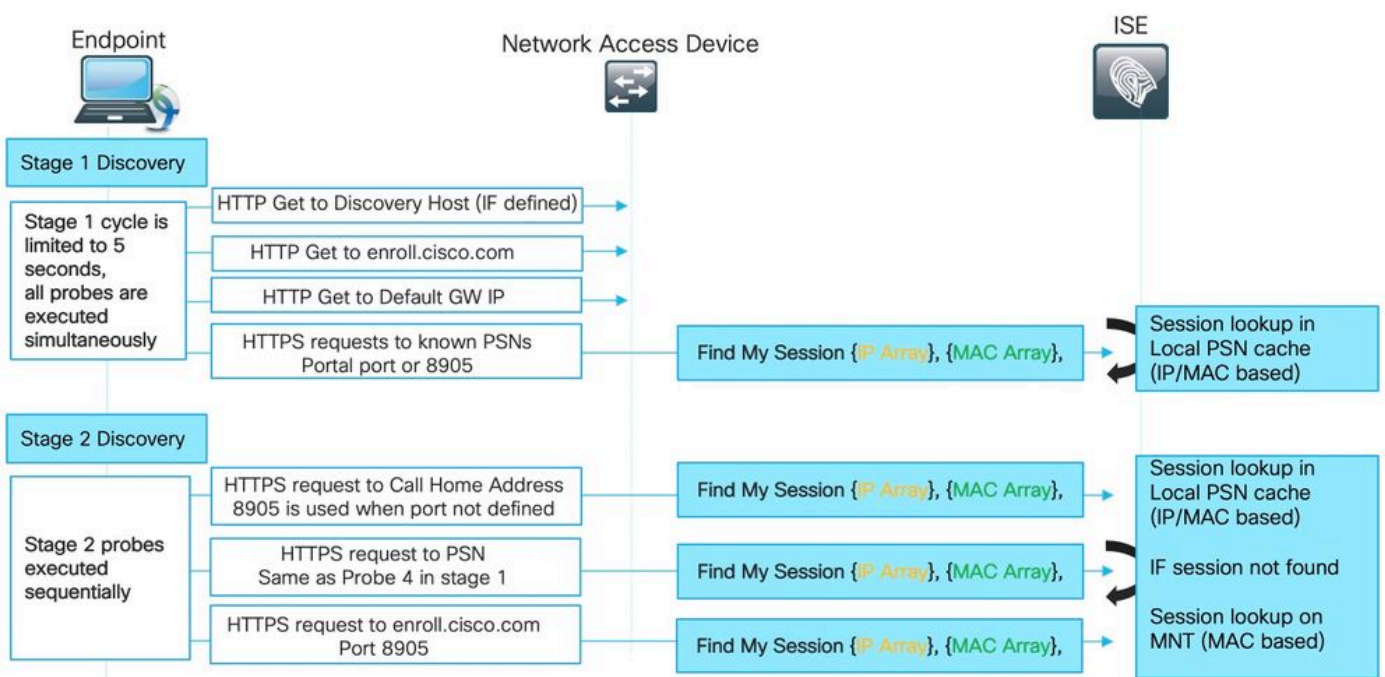
4. 分配給虛擬專用網路(VPN)介面卡的新IP地址。

5. IP地址資訊臨時會計更新位於PSN上。
- 6.新增到會話快取的IP地址資訊。
- 7.對PSN1進行狀態評估。
- 8.會話中更新的状态狀態。
9. ISE執行的COA推送，這將觸發要分配的新訪問級別。
- 10.使PSN1無法訪問的網路路徑中斷。
- 11.在臨時更新間隔過期後，ASA/FTD檢測到無法訪問PSN1。
12. PSN2將更新中期會計資訊。
- 13.在PSN2會話快取中建立的虛擬會話。

如果之後的PSN1變得可訪問(14)，則所有後續的記帳消息都在這裡轉發(15,16)，並且這會在PSN2會話快取中保留會話ABC一段未定義的時間。

陳舊會話和虛擬會話如何中斷狀態進程？

要瞭解陳舊會話和虛擬會話如何中斷狀態，您可以檢視AnyConnect ISE狀態模組發現流程：



階段1發現：

在此階段，ISE終端安全評估模組執行4個同時問題以定位對終端執行身份驗證的PSN。

首先，圖中的3個探測器基於重定向（預設GW IP）。發現主機IP（如果已定義）和 enroll.cisco.com IP — 這些探測功能始終將代理指向正確的PSN，因為重定向URL是從NAD本身獲取的。

探查號4將傳送到ConnectionData.xml檔案中顯示的所有主服務器。如果客戶端在PSN之間遷移，則可在第一次成功安全評估嘗試之後建立此檔案，並在以後更新檔案內容。在Windows系統上，檔案位置為 — C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\。

由於所有階段1探測都同時執行，因此僅當所有其他3個探測失敗或ISE終端安全評估模組在5秒內無法與重定向URL中返回的PSN建立正確通訊時，才會使用探測器4的結果。

當探測器4位於PSN上時，它包含在終端上發現的有效IP和MAC地址清單。PSN使用此資料在本地快取中查詢此終結點的會話。如果PSN的端點有一個陳舊或幻像會話，則可能導致在客戶端稍後顯示錯誤的狀態狀態。

當代理獲得探測4的多個應答時(ConnectionData.xml可以包含多個主PSN)，將始終使用最快的應答。

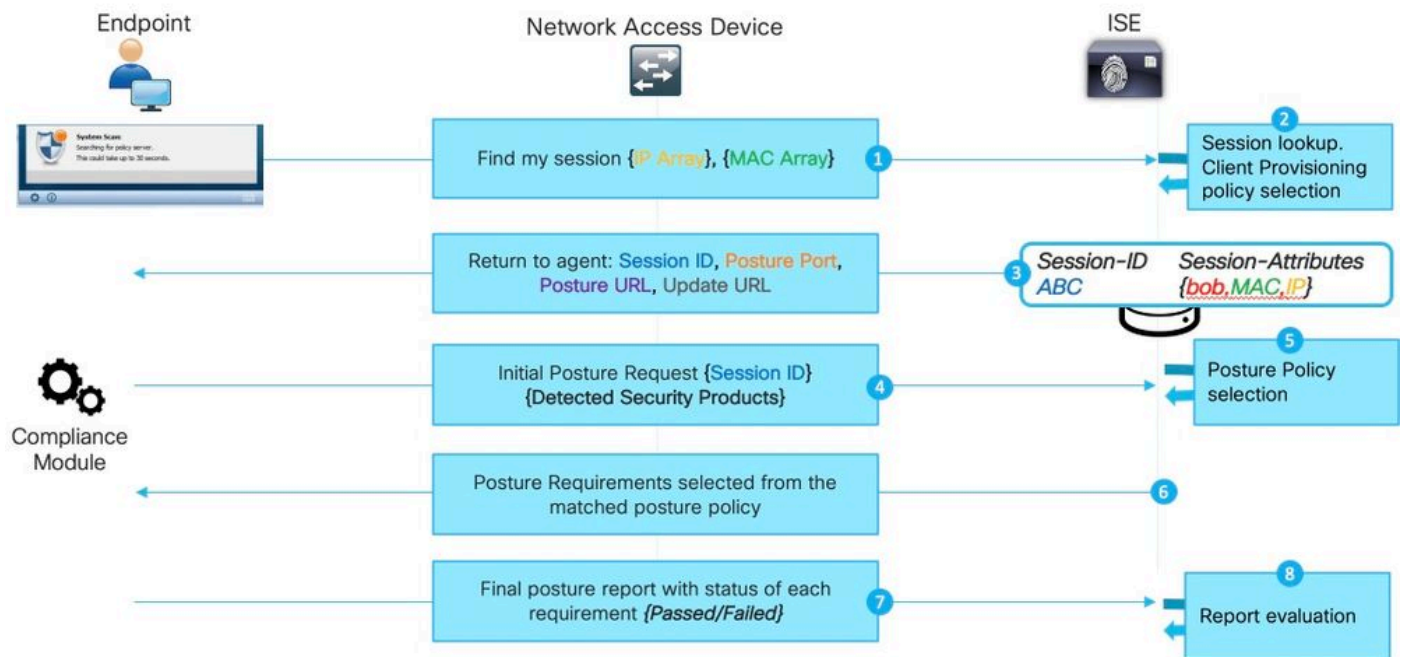
階段2發現：


所有階段2發現探測都無重定向，這意味著每個探測都會觸發目標PSN上的會話查詢。如果PSN無法在本地會話快取中找到會話，則必須執行MNT查詢（僅基於MAC地址）以查詢會話所有者並將所有者名稱返回給代理。

由於所有探測都會觸發會話查詢，因此階段2的發現可能更容易受到由於過時或幻像會話而導致的問題。


如果PSN進入第2階段，會話快取中存在的發現探測將為同一端點建立一個過時或幻像條目。這會導致錯誤的安全狀態返回給終端使用者。

此示例顯示了當PSN保留過時會話或虛擬會話時如何執行安全狀態：



 注意：必須記住，僅當所有基於重定向的發現探測失敗或實施非重定向狀態時才會顯示此問題。

1. ISE終端安全評估模組發出的任何查詢我的會話探測器(Find my session probe)。
2. PSN在會話快取中執行會話查詢。如果要找到該會話，則會發生陳舊或幻像會話問題。
3. PSN運行客戶端調配策略選擇。如果虛擬會話缺少身份驗證/授權屬性，並且客戶配置的所有策略都非常具體（例如，為特定Active Directory組建立策略），則PSN無法分配正確的客戶端調配策略。這可能顯示在錯誤消息「Bypassing AnyConnect scan your network is configured to use Cisco NAC Agent（繞過AnyConnect掃描您的網路配置為使用Cisco NAC代理）」中。
 - 如果客戶端調配策略是通用的（虛擬會話中可用的屬性足以將策略與AnyConnect配置相匹配），則PSN將回覆評估過程繼續所需的詳細資訊。
 - 在此步驟中，當我們可以處理過時的會話時，PSN會立即回覆安全評估狀態Compliant，並且不會執行所有後續步驟。PSN不會傳送COA，因為它認為會話已經合規。在Radius Live日誌中，沒有顯示狀態為Compliant的會話事件。
- 4.對於幻像會話場景，ISE終端安全評估模組將繼續執行初始終端安全評估請求。此請求包含關於終結點上檢測到的所有安全和修補程式管理產品的資訊。
5. PSN使用來自請求和會話屬性的資訊來匹配正確的狀態策略。由於幻像會話此時缺少屬性，因此沒有要匹配的策略。在這種情況下，PSN會回復到符合策略的端點，因為在安全狀態策略不匹配的情況下，這是預設的ISE行為。


 注意：當存在可從虛擬會話屬性中選擇的通用策略時，我們繼續執行步驟6。

6. PSN將選定的狀態策略返回給代理。

 注意：當無法選擇任何策略時，PSN將返回相容狀態。

- 7.代理返回每個策略/需求通過或失敗的狀態。

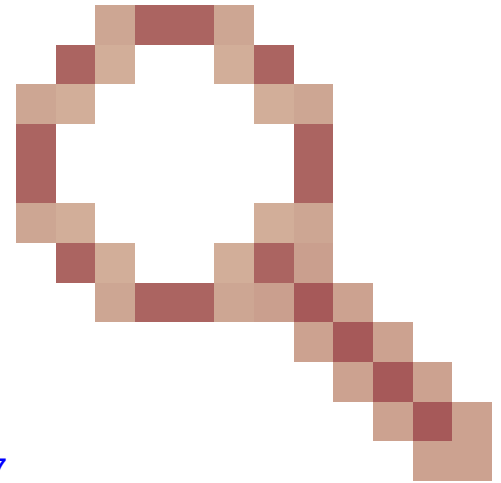
- 8.對ISE進行報告評估，會話狀態更改為合規。

 注意：如果出現由虛擬會話引起的終端安全評估問題，ISE管理員可能會注意到一些失敗的終端安全評估COA，因為在這種情況下，從錯誤的PSN執行了COA請求，並且使用了錯誤的會話ID。

發現進程不會在新身份驗證嘗試時啟動

ISE終端安全評估模組旨在監控終端上有限數量的事件以觸發發現流程。觸發發現的事件的清單：

- 初始ISE狀態模組安裝。
- 使用者登入。
- 電源事件。
- 介面狀態更改。
- 作業系統在睡眠後恢復。
- 預設網關(DG)更改。



- 狀態重新評估(PRA)失敗，請參閱思科錯誤ID [CSCvo69557](#)

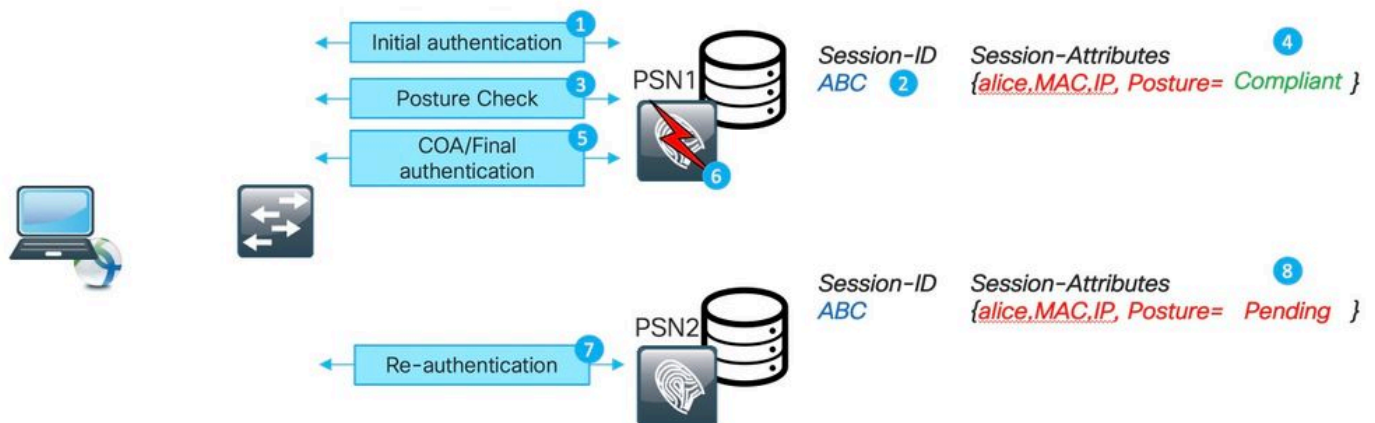
ISE終端安全評估模組未檢測到新的dot1x身份驗證、PC解鎖、IP地址更改。

在這些情況下，ISE終端安全評估模組無法檢測新的身份驗證或重新身份驗證嘗試：

- 重新身份驗證命中不同的PSN (由於LB決策或原始PSN的問題)。
- NAD在重新身份驗證時生成新的會話ID。

不同PSN上的重新身份驗證

由於原始PSN中斷而在不同PSN上重新身份驗證的示例。具有負載平衡器的情況看起來非常相似。在LB的情況下，由於粘性計時器過期，將重新認證定向到不同的PSN。

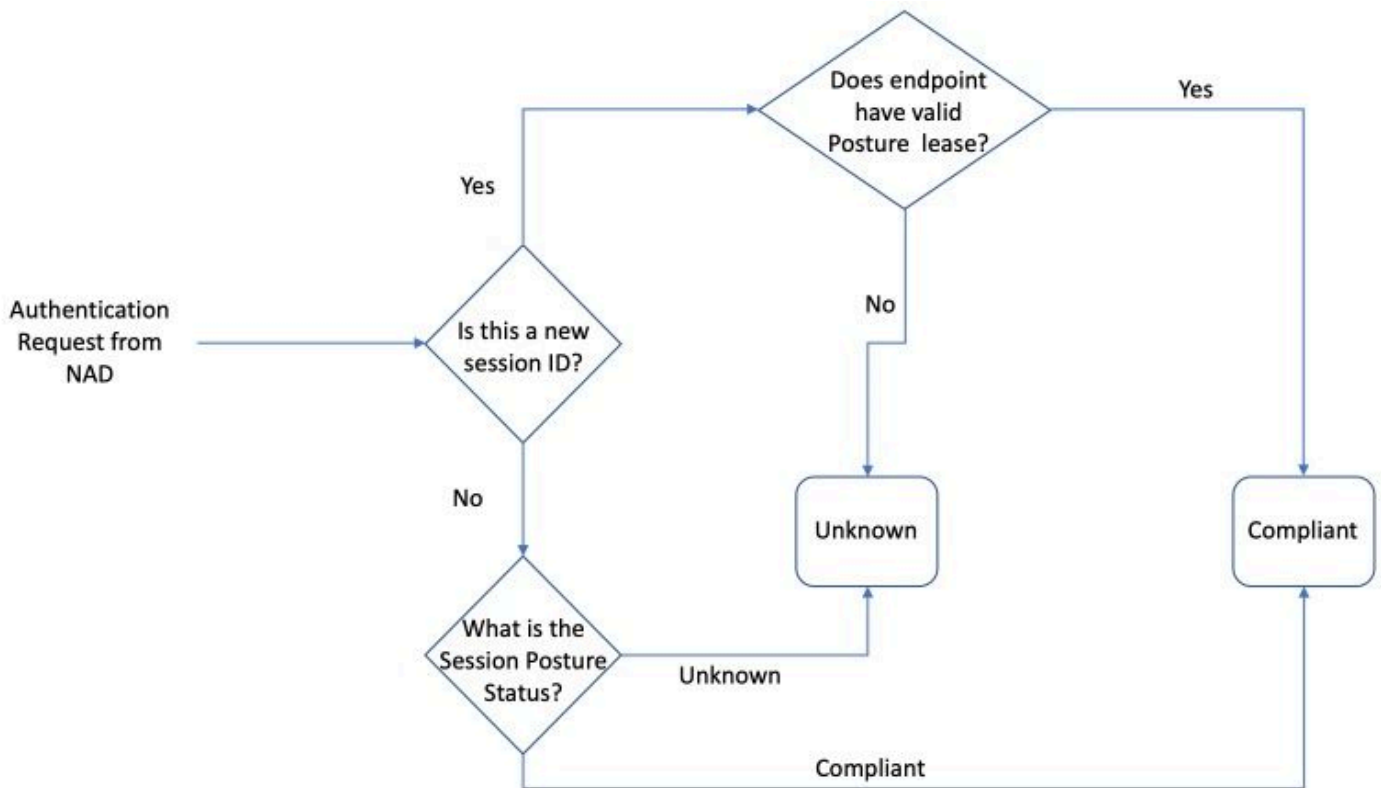



1. PSN1上的初始身份驗證。
2. 在PSN1會話快取中建立的會話ABC。
3. 使用PSN1執行的狀態評估。
4. 會話ABS安全評估狀態將移至「合規」。
5. 狀態更改觸發的COA導致重新驗證終端以應用下一個訪問級別。
6. PSN1變為不可用。

7. 會話ABC的重新身份驗證命中PSN2。

8. 由於會話是PSN2狀態的新會話，因此該會話的狀態變為「待定」。

PSN分配給會話的初始狀態狀態：



 注意：狀態機僅描述狀態狀態的初始選擇。最初標籤為Unknown的每個會話均可根據ISE終端安全評估模組收到的報告，隨後變為Compliant或Not Compliant。

NAD在重新身份驗證時生成新的會話ID

這種情況可能發生在兩種最常見的情形中：

- ISE端重新身份驗證配置不正確。此問題的解決方案將在本文檔的後面部分介紹。
- NAD端的不當行為 — 在重新身份驗證嘗試期間，NAD通常保持相同的會話ID。如果您發現NAD在重新身份驗證時更改了會話ID，則這是一個潛在的錯誤行為，需要在NAD本身上進行調查。

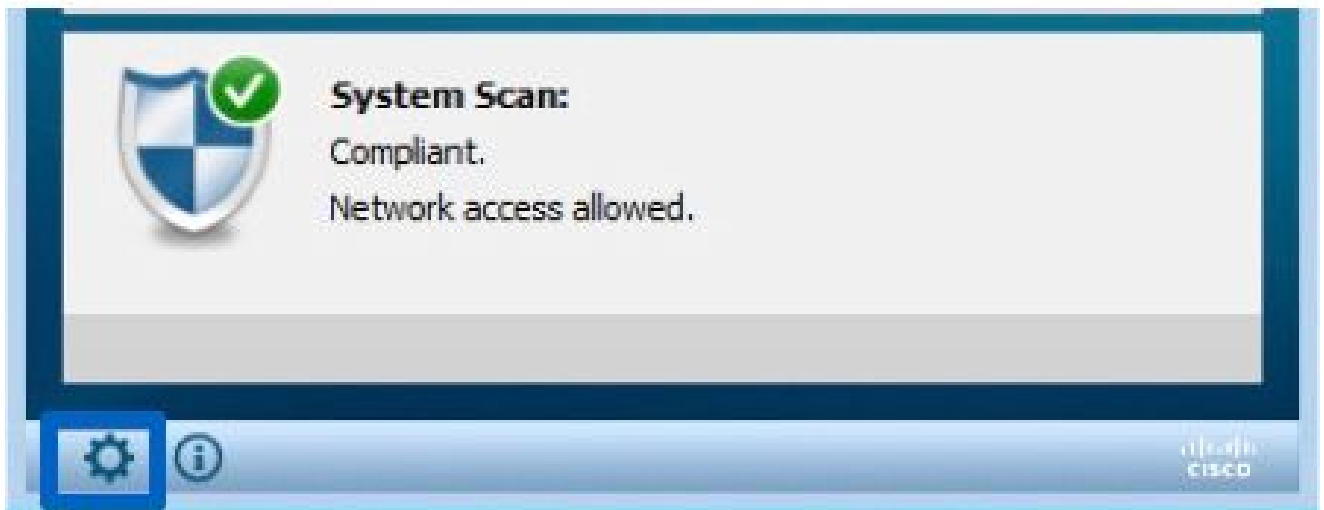
新的會話ID可以在其它某些角落場景中生成。例如，在某些情況下，無線漫遊可能是其原因。這裡的主要問題是，ISE PSN始終將新會話置於posture Pending狀態，除非配置了終端安全評估租用。安全狀態租期將在本文檔的後續部分進行說明。

快速確定問題何時由陳舊/幻像會話引起

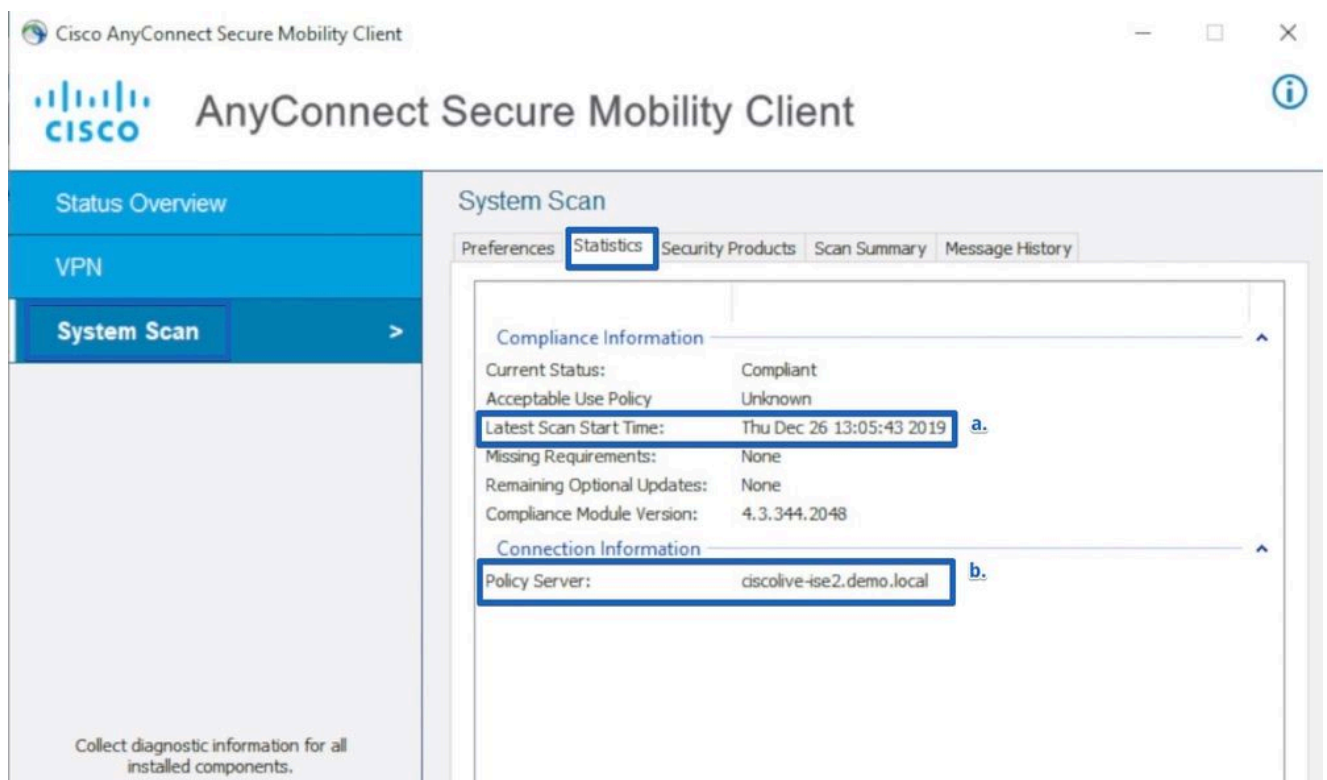
要確定AnyConnect處於重定向狀態時是否顯示合規是由過期/幻像會話引起的，我們需要在終端處於有問題的狀態時獲得對終端的訪問許可權。

1. 調查系統掃描詳細資訊：

1.按AnyConnect UI中的齒輪圖示



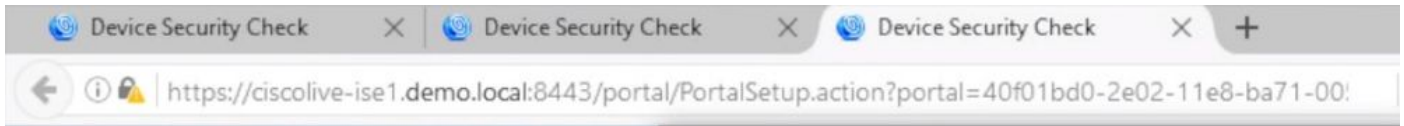
2.在新視窗中，定位至「系統掃描」標籤和「統計資訊」子標籤



在此，請注意以下兩個因素：

- Latest Scan Start Time — 此處的時間戳必須接近發現問題的時間。
- Policy Server — 此欄位指示對終端執行狀態評估的策略伺服器的名稱。此處的FQDN需要與來自Redirect-URL的FQDN（用於重定向基礎狀態）或來自上次身份驗證嘗試的PSN名稱（用於無重定向狀態）進行比較。

2. 將系統掃描統計資訊中的策略伺服器FQDN與對終端進行身份驗證的節點名稱進行比較：



在給定的示例中，名稱不匹配，表示名為ciscolive-ise2的PSN保留此終結點的過時或幻像會話。

此演示顯示了問題識別所需步驟的記錄：

陳舊/幻像會話高級故障排除

上例是將過時或幻像會話問題與未啟動的發現進程問題區分開來。同時，我們需要確定觸發問題的實際會話，以便更好地瞭解它究竟如何變成陳舊或幻像會話問題。

但在某些情況下，無法避免陳舊和幻像會話。由於某些未實施的最佳實踐，我們需要確保環境中不會建立陳舊/幻像會話。

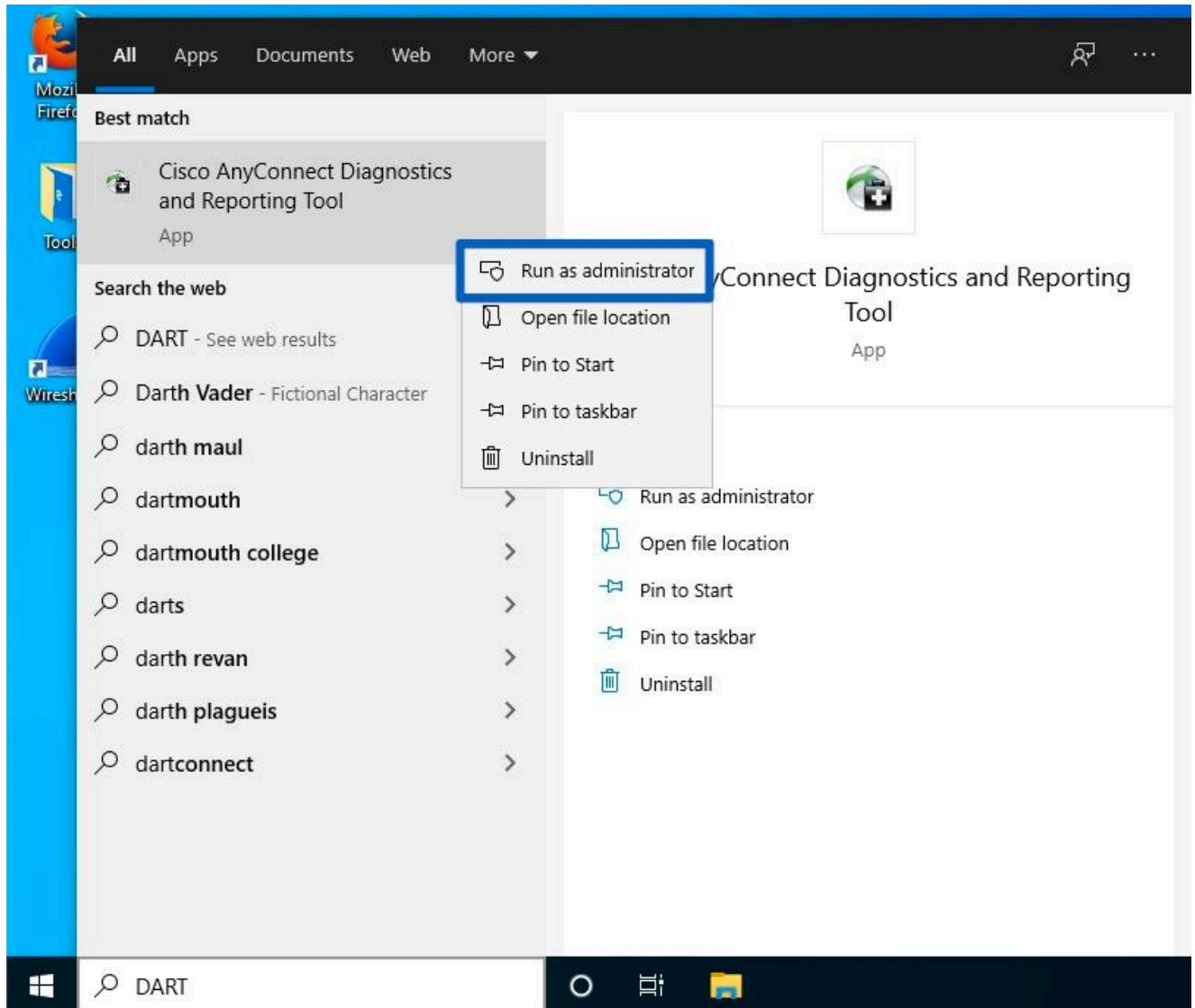
DART捆綁包集合

分析從重現問題的終端獲取的DART捆綁包。

- 在DART中僅保留重要日誌。建議在重現問題之前清除日誌。

為此，需要以管理員身份啟動DART捆綁工具並執行日誌清除。

1. 在Windows上，導航到「開始」並開始鍵入DART，按一下右鍵並選擇「以管理員身份運行」



2. 在第一個嚮導螢幕上，按「下一步」

Cisco Diagnostic and Reporting Tool (DART)



DART is a tool that helps to bundle the appropriate log files and diagnostic information that can be used for analyzing and debugging the AnyConnect client connections.

This wizard will guide you through the steps required to create the diagnostic bundle. To continue, click Next.

3. 在下一個嚮導螢幕上，按「清除所有日誌」

Bundle Creation Option



Select "Default" to include the typical log files and diagnostic information in the bundle. Select "Custom" to choose the list of log files and diagnostic information to be included in the bundle.

Default (Bundle will be saved to Desktop)

Custom

Clear All Logs

Back

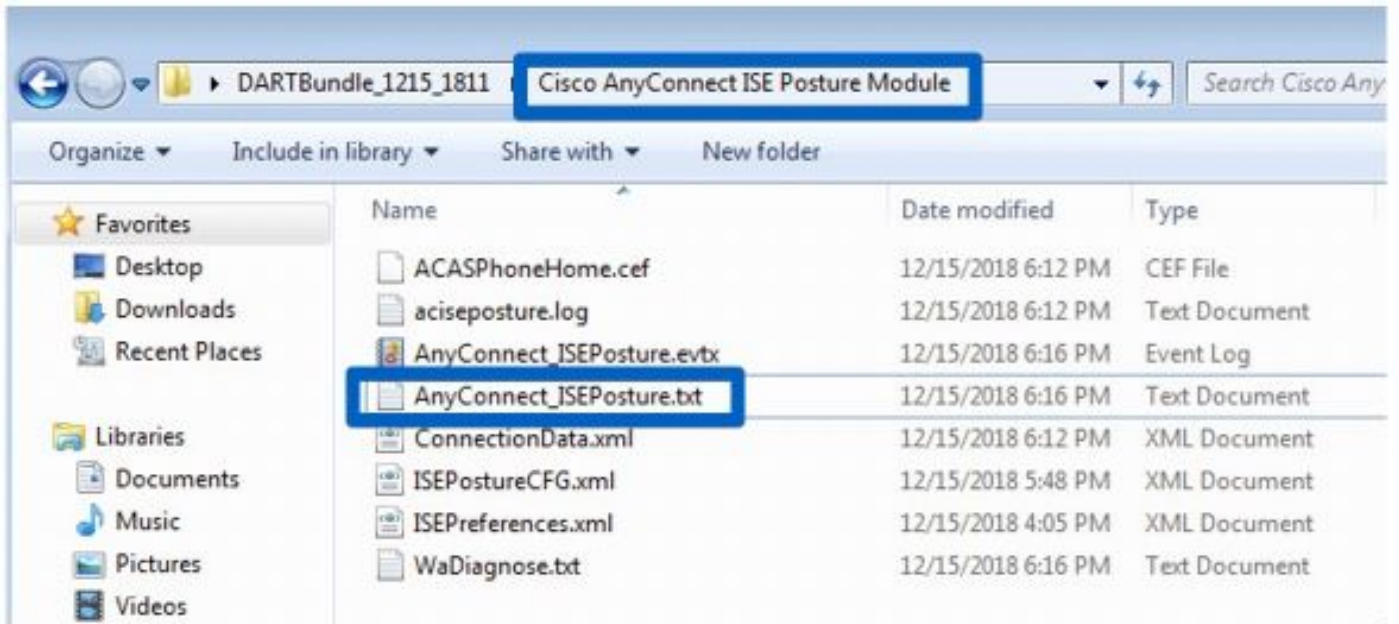
Next

Cancel

4. 重現問題後，可從此處收集DART；按下一步。

DART捆綁包分析

收集DART捆綁包後，我們需要將其取消歸檔，並集中處理Cisco AnyConnect ISE終端安全評估模組資料夾中的AnyConnect_ISEPosture.txt檔案。此檔案包含所有與發現相關的事件。



1.開始故障排除並確定發現重啟的所有時刻。要搜尋的關鍵字是重新啟動發現或HTTP發現。在這裡，導航到在問題時刻重新啟動發現的行：

```
Line 3575: 2018/12/15 17:48:08      1251 Level: info  Restarting Discovery.
Line 3840: 2018/12/15 17:48:59      1251 Level: info  Restarting Discovery.
Line 3991: 2018/12/15 17:50:24      1251 Level: info  Restarting Discovery.
Line 4214: 2018/12/15 18:00:54      1251 Level: info  Restarting Discovery.
Line 4308: 2018/12/15 18:01:14      1251 Level: info  Restarting Discovery.
Line 4530: 2018/12/15 18:11:45      1251 Level: info  Restarting Discovery.
Line 4642: 2018/12/15 18:12:01      1251 Level: info  Restarting Discovery.
```

<output omitted>

2.在發現重新啟動後的幾行中，您會看到一條包含 — 探測無MNT階段目標的行。這是第1階段發現開始的一個指標：

```
SwiftHttpRunner::collectNoMntTargets Thread Id: 0x1340 File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\ise\libswift\SwiftHttpRunner.cpp Line: 1157 Level: debug Probing no MNT stage targets (#5):
Redirection target 192.168.255.1, Redirection target enroll.cisco.com,
Auth-Status target ciscolive-ise2.demo.local with path /auth/status,
Auth-Status target ciscolive-ise1.demo.local with path /auth/status,
```

建議突出顯示具有相同顏色的所有基於重定向的探測器，而以前從ConnectionData.xml (身份驗證狀態目標) 獲取的PSN需要以不同顏色突出顯示，因為通常PSN FQDN非常相似，很難發現差異。

3.讀取日誌檔案，檢視每個單次探測的結果。前面已經說過，在由於過時/幻像會話導致的問題中，所有基於重定向的探測器都必須失敗。以下是失敗探測結果的示例：

```
2018/12/15 18:12:01 [Information] aciseagent Function: Target::Probe Thread Id: 0x1130
File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\ise\libnacommon\Target.cpp Line: 200 Level: debug Status of Redirection target enroll.cisco.com is 6 <Not Reachable.>
```

4.在檔案內第1階段或第2階段的發現重新啟動後，您會看到來自一個或多個PSN的成功回覆：

```
Target::fetchPostureStatus Thread Id: 0xBF0 File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\ise\libnaccommon
\Target.cpp Line: 401 Level: debug POST request to URL (
https://ciscolive-ise2.demo.local:8443/auth/ng-discovery), returned status 0
<Operation Success.>
```

5.幾行之後，有一行帶有關鍵字MSG_NS_SWISS_NEW_SESSION。此行包含PSN在查詢會話後選擇的實際會話ID。使用此會話ID對ISE進行進一步調查，瞭解此會話如何變成陳舊/幻像：

```
SwiftHttpRunner::invokePosture Thread Id: 0x1340 File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\ise\libswift\SwiftHttpRunner.cpp Line: 1407 Level: debug MSG_NS_SWISS_NEW_SESSION,
{{ise_fqdn="ciscolive-ise2.demo.local"}, {posture_port="8443"},
{posture_path="/auth/perfigo_validate.jsp"},
{posture_domain="posture_domain"}, {posture_status="Compliant"},
{session_id="0a3e949c000002585cf00588"},
{config_uri="/auth/anyconnect?uuid=f62337c2-7f2e-4b7f-a89a-3508d761173c"},
{acpack_uri="/auth/provisioning/download/066ac0d6-2df9-4a2c-a129-fabf1ace36aa"},
{acpack_port="8443"}, {acpack_ver="4.6.3049.0"}, {pra_enabled=0}}.
```

ISE日誌調查

在clientwebapp元件啟用到DEBUG的guest.log中，可以看到使用過時/幻像會話進行回覆的PSN。

PSN從ISE終端安全評估代理獲取請求。由於User-Agent值，您可以看到這是來自AnyConnect的請求：

```
<#root>
```

```
cisco.cpm.client.posture.PostureStatusServlet -:-
```

```
Got http request from 192.168.255.228 user agent is: Mozilla/4.0 (compatible; WINDOWS; 1.2.1.6.1.48; Any
```

```
cisco.cpm.client.posture.PostureStatusServlet -:-
```

```
mac_list
```

```
from http request ==> C0:4A:00:1F:6B:39
```

```
cisco.cpm.client.posture.PostureStatusServlet -:-
```

```
iplist
```

```
from http request ==> 192.168.255.228
```

```
cisco.cpm.client.posture.PostureStatusServlet -:-
```

```
Session id from http request -
```

```
req.getParameter
```

```
(  
sessionId  
) ==> null
```

請求包含IP地址和MAC地址的陣列。在此特定示例中，每個陣列僅包含一個值。此外，日誌顯示請求的會話ID為Null，這表示這是來自非重定向型探測器的請求。

稍後，您可以看到如何使用陣列的值來定位會話ID:

<#root>

```
cpm.client.provisioning.utils.ProvisioningUtil --:- the input ipAddress from the list currently processed  
cpm.client.provisioning.utils.ProvisioningUtil --:- the ipAddress that matched the http request remote IP  
cpm.client.provisioning.utils.ProvisioningUtil --:- the clientMac from the macarray list for the for loop  
cisco.cpm.client.posture.PostureStatusServlet --:- Found Client IP matching the remote IP 192.168.255.228  
cpm.client.provisioning.utils.ProvisioningUtil --:-  
Session = 0a3e949c000000495c216240
```

在包含關鍵字Sent http response的行之後，您可以檢視實際回覆中的內容：

<#root>

```
cisco.cpm.client.posture.PostureStatusServlet --:- Sent an http response to 192.168.255.228 with X-ISE-AC-STATUS_PATH  
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-PDP value is clemea19-ise1.demo.local  
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-POSTURE value is /auth/perfigo_validate  
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-POSTURE_PORT value is 8443  
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-AC_PKG_PORT value is 8443  
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-GUESTFLOW value is false  
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-AC_CONFIG_URL value is https://clemea19-ise1.demo.local  
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-AC_CONFIG_URI value is /auth/anyconnect  
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-AC_PKG_URL value is https://clemea19-ise1.demo.local  
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-AC_PKG_URI value is /auth/provisioning  
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-AC_PKG_VER value is 4.6.3049.0  
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-STATUS_PATH value is /auth/status  
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-BACKUP_SERVERS value is clemea19-ise2.
```

```
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-SessionId value is 0a3e949c00000495c2
cpm.client.provisioning.utils.ProvisioningUtil --:- header X-ISE-PostureDomain value is posture_domain
cpm.client.provisioning.utils.ProvisioningUtil --:-
header X-ISE-POSTURE_STATUS value is Unknown
```

ISE報告調查

知道過期/幻像會話的ID後，您可以調查Radius記帳報告，以便更好地瞭解導致此會話過期/幻像的原因：

- 導航到Operations > Reports > Endpoints and Users > Radius Accounting報告，然後運行此報告7天。使用終端ID作為過濾器金鑰。

顯示如何在ciscolive-ise2上保留過時會話的報告的示例：

2019-05-30 16:42:13.36	3 Stop	alice	C0:4A:00:1F:6B:39	0a3e949c000002585cf00588	DEMO-WLC	ciscolive-ise1
2019-05-30 16:32:20.819	2 Interim-Update	alice	C0:4A:00:1F:6B:39	0a3e949c000002585cf00588	DEMO-WLC	ciscolive-ise2
2019-05-30 16:32:16.263	1 Start	alice	C0:4A:00:1F:6B:39	0a3e949c000002585cf00588	DEMO-WLC	ciscolive-ise2

1. PSN ciscolive-ise2開始進行會話記帳
2. 已在同一PSN上處理會話的臨時更新。
3. 有問題的會話ID的記帳停止消息到達不同的PSN(ciscolive-ise1)。

一種快速方法，可確定問題何時由未重新啟動發現導致

此處適用的邏輯與上一期相同。唯一的區別是您需要關注最新的掃描開始時間。對於此類問題，上次掃描的時間戳位於過去某個位置。

一般情況下，當終端使用者發現問題時，會看到一段時間前發生的掃描。在ISE Radius Live日誌中，會看到有問題的終端最近的身份驗證嘗試。

此演示顯示了問題識別所需步驟的記錄：

高級故障排除：發現無法重新啟動

這裡的方法非常類似於「高級故障排除陳舊/幻像會話」部分。主要故障排除要素是DART捆綁調查。在DART捆綁包中，您可以搜尋發現重新啟動（如針對前一問題顯示的內容），並確認報告問題時沒有發現重新啟動。

在ISE端，關注Radius Live Logs/ Radius身份驗證報告，以確認PSN之間出現故障切換，或者由NAD生成新的會話ID。

解決方案

傳統方法 — 問題避免

過去，ISE沒有可以解決本文檔中描述問題的功能，因此唯一的方法是依靠在網路和ISE端實施的一組最佳實踐，將風險降至最低。

可以將ISE部署中的陳舊或幻像會話數量降至最低的最佳實踐

儘可能始終實施基於重定向的終端安全評估

此建議的一個常見反論是使用者體驗不佳，因為在OS或瀏覽器中看到彈出視窗，指示重新導向，而後台的AnyConnect ISE終端安全評估模組執行評估流程。

作為解決方案，可以僅重定向ISE終端安全評估模組發現探測並選擇性地允許所有其他流量。

範例顯示重新導向ACL，其設計目的僅是將HTTP要求重新導向到探索主機（本範例中為10.1.1.1）和enroll.cisco.com(172.16.1.80):

```
ip access-list extended REDIRECT-DH-ENROLL  
  
permit tcp any host 10.1.1.1 eq www  
  
permit tcp any host 172.16.1.80  
  
deny ip any any
```

為了保持可接受的安全級別，此類重定向ACL可以與ISE分配的DACL結合使用。

掛起狀態僅允許連線到終端經過身份驗證的PSN

此方法對不支援url重定向的環境（例如第三方NAD的實施）很有用。

作為解決方案，您需要實施多個PosturePending授權策略（每個PSN一個）。每個策略都需要包含進行身份驗證的PSN名稱作為條件之一。在分配給每個策略的授權配置檔案中，必須阻止對所有PSN的訪問（進行身份驗證的節點除外）。

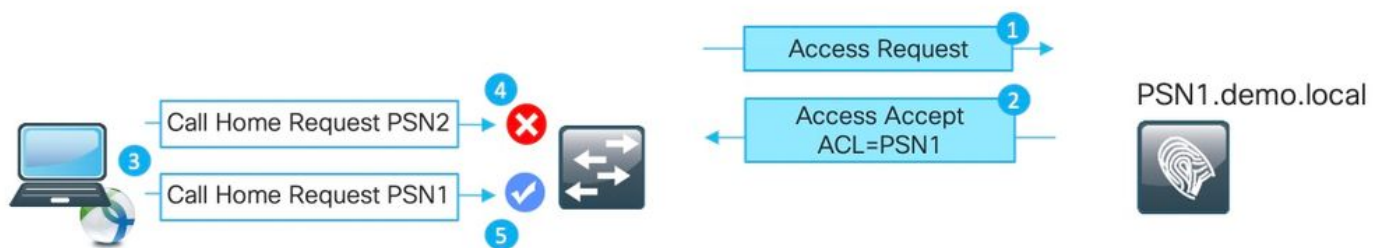
為2個節點部署建立授權策略：

The screenshot displays the configuration for three authorization policies in ISE:

- Any-PSN-Compliant (7):** Session PostureStatus EQUALS Compliant. Action: PermitAccess.
- PS2-Posture-Pending (4):** AND condition. Session PostureStatus EQUALS Unknown (5). Network Access-ISE Host Name EQUALS PSN2 (6). Action: Probes-to-PSN2.
- PS1-Posture-Pending (1):** AND condition. Session PostureStatus EQUALS Unknown (5). Network Access-ISE Host Name EQUALS PSN1 (2). Action: Probes-to-PSN1 (3).

1. PSN1的狀態掛起策略。
- 2.用作策略中條件的PSN1名稱。
- 3.具有ACL的授權配置檔案，阻止對除PSN1以外的所有PSN的訪問。
4. PSN2的狀態掛起策略。
- 5.用作策略中條件的PSN2名稱。
- 6.具有ACL的授權配置檔案，阻止對除PSN2以外的所有PSN的訪問。
- 7.安全狀態「合規」授權策略。

圖中說明了此方法的運作方式：



- 1.身份驗證命中PSN1。
- 2.由於配置了授權策略，PSN1會分配阻止對PSN1以外的所有其他節點進行訪問的授權配置檔案。
3. AnyConnect ISE終端安全評估模組重新啟動發現過程。
- 4.探測被NAD阻止的PSN2 (如之前分配的ACL) 。
- 5.在NAD上分配的ACL允許探測到PSN1。

負載平衡器最佳實踐

- 在LB上啟用粘性，以呼叫站ID作為粘性金鑰進行身份驗證和記帳。有關ISE的LB最佳實踐的詳細資訊，請[此處](#)。
- 使用比平均工作日更長的粘性計時器來覆蓋PC進入睡眠的時間 (例如10小時而不是8小時) 。
- 如果已實施重新身份驗證，請使用重新身份驗證計時器略低於粘性計時器 (例如，如果粘性配置為10小時，則使用8小時) 。這可確保通過重新驗證來延長粘滯間隔。

Posture Over VPN使用案例

- 確保accounting-interim更新間隔大於或等於vpn-session-timeout。這樣可以防止長存VPN會話上PSN之間的記帳抖動。

此示例顯示為20小時配置的臨時記帳更新間隔。這不會阻止初始臨時更新，該更新攜帶分配給終端的IP地址。

```
aaa-server ISE protocol radius
interim-accounting-update periodic 20
group-policy SSL-VPN attributes
vpn-idle-timeout 1200
vpn-session-timeout 1200
```

可以實施最佳實踐，以最大程度降低未進行ISE終端安全評估模組發現重啟的影響

啟用狀態租用

這是ISE上的一個功能，它將終端標籤為符合規定的時間段（1-365天）。終端安全評估租賃值是終端屬性，這意味著它是ISE DB儲存的。在ISE部署中的所有節點上複製包括狀態租賃的所有終端屬性。

當PSN獲得終端安全評估租約的新會話時，可利用此會話立即標籤為Compliant。

為了做出此決定，PSN使用3個值。這些值為：

- 在ISE設定中為終端安全評估租賃定義的天數：導航到Administration > System > Posture > General Settings:

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The left sidebar shows the navigation tree with 'Posture' expanded to 'General Settings'. The main content area is titled 'Posture General Settings' and contains the following configuration options:

- Remediation Timer: 4 Minutes
- Network Transition Delay: 3 Seconds
- Default Posture Status: Compliant
- Automatically Close Login Success Screen After: 0 Seconds (unchecked)
- Continuous Monitoring Interval: 5 Minutes (checked)
- Acceptable Use Policy in Stealth Mode: Block
- Posture Lease:
 - Perform posture assessment every time a user connects to the network (unchecked)
 - Perform posture assessment every 1 Days (selected and highlighted with a blue box)
- Cache Last Known Posture Compliant Status: checked
- Last Known Posture Compliant State: 7 Days

Buttons for 'Save' and 'Reset' are located at the bottom of the configuration area.

- PostureExpiry屬性的值 — 這是包含紀元時間戳的實際端點屬性。在ISE管理員啟用終端安全評估租約後，終端首次成功安全評估嘗試時初始填充PostureExpiry值。稍後，此值在租約到期後進行的下一次成功狀態嘗試時更新。

開啟其中一個姿勢端點時，您可在「情景可視性」>「端點」中看到PostureExpiry:

PostureExpiry

1586332942236

PostureOS

Windows 10 Professional 64-bit

此值可以轉換為人類可讀的時間戳，例如<https://www.epochconverter.com/>

Convert epoch to human-readable date and vice versa

1586332942236

Timestamp to Human date

[batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

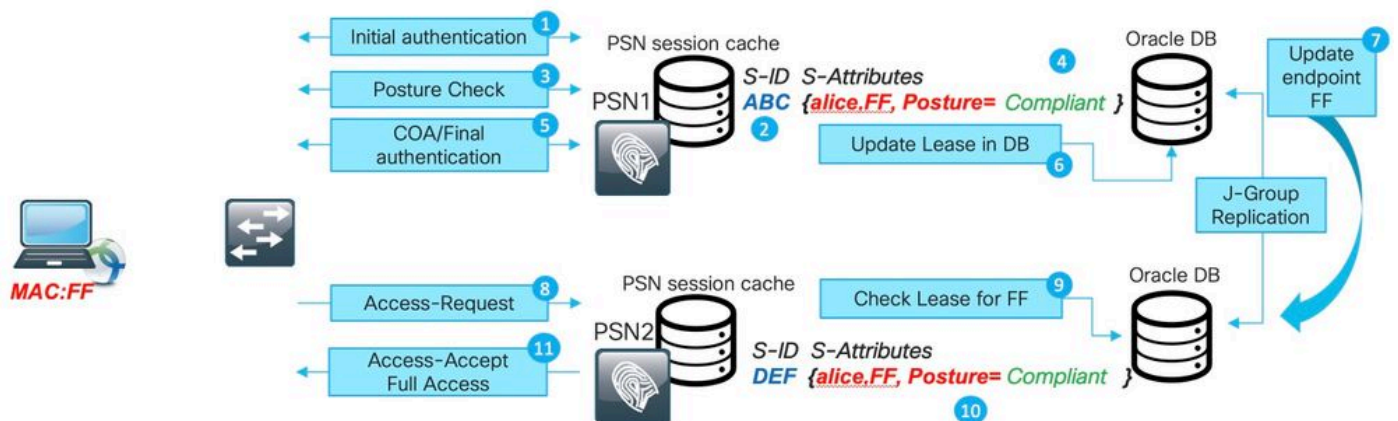
Assuming that this timestamp is in **milliseconds**:

GMT: Wednesday, 8 April 2020 r., 8:02:22.236

- 進行新身份驗證時的PSN系統時間

當具有安全狀態租約的終端身份驗證到達PSN時，它使用PostureExpiry和系統日期獲取上次成功安全狀態檢查的天數。如果結果值在設定中定義的狀態租用間隔內，則會話將獲得Compliant狀態。如果結果值大於租用值，則會話將獲得Unknown狀態。這將觸發再次執行安全評估並且可儲存新的PostureExpiry值。

圖中說明了發生故障切換時的過程：

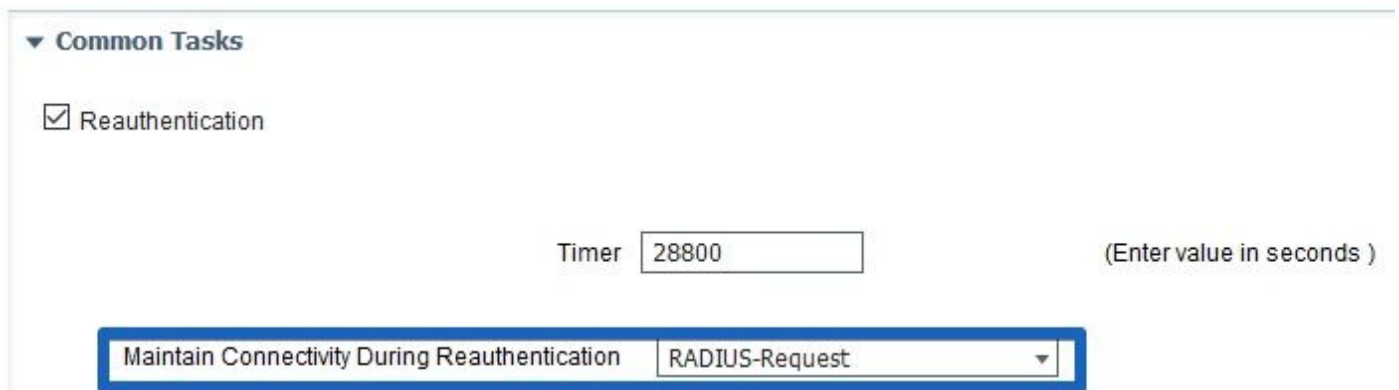


- 1.對PSN1進行初始身份驗證。
- 2.在會話快取中建立的會話ABC。
- 3.進行狀態評估。
- 4.會話狀態更改為「合規」
- 5.狀態更改觸發的COA導致重新驗證終端以應用下一個訪問級別。

6. 終結點中儲存的postureExpiry值。
7. 跨部署複製的終端資料。
8. 下一個身份驗證命中PSN2。
9. PSN2檢查終端是否處於有效的終端安全評估租約中。
11. 會話已新增到會話快取中，並為Compliant。
12. 由於有效租約，因此建立的會話的狀態為Compliant。

重新驗證實施

在Maintain Connectivity During Reauthentication中選擇RADIUS-Request時，始終從ISE推送重新身份驗證計時器。此設定可確保NAD在重新身份驗證時保持相同的會話ID。



▼ Common Tasks

Reauthentication

Timer (Enter value in seconds)

Maintain Connectivity During Reauthentication

具有負載平衡器的環境

可以實施在過時/幻像會話一節中介紹的同一組最佳做法。

不同的子網可用於掛起狀態和合規狀態

當網路設計提供使用不同子網Pending和Compliant狀態時，此方法可以確保狀態狀態的每次更改都會導致預設網關的變化。

與重新身份驗證計時器相同的時間間隔內使用的狀態評估

可以使用等於重新驗證計時器的時間間隔啟用狀態評估。在這種情況下，當原始PSN變得不可用時，PRA故障將重新啟動發現過程。

現代方法 — 狀態共用

作為已實施的增強功能的一部分，思科漏洞ID [CSCvi35647](#) 補丁6 for ISE 2.6中介紹了一項新功能，該功能實現了在ISE部署中的所有節點間共用會話狀態狀態。此增強功能整合到未來版本中：ISE 2.7補丁2和ISE 3.0。

此新功能基於ISE 2.6中引入的輕量級會話目錄(LSD)機制。在較新版本中，此功能已重新命名為輕

量資料分發(LDD)Radius會話目錄。 預設情況下，輕量級資料分發已啟用，並允許在ISE節點之間共用有限的會話上下文。 在PSN之間沒有完整會話上下文複製這樣的東西，每個會話只共用有限數量的屬性。

Light Session Directory的主要思想是在部署中的一個節點必須確定誰是當前會話所有者時，消除對MNT執行資源昂貴API呼叫的需要。 啟動COA流時，通常需要查詢所有者。 使用LDD，每個PSN可以從本地Radius會話目錄快取中找到會話的實際所有者。

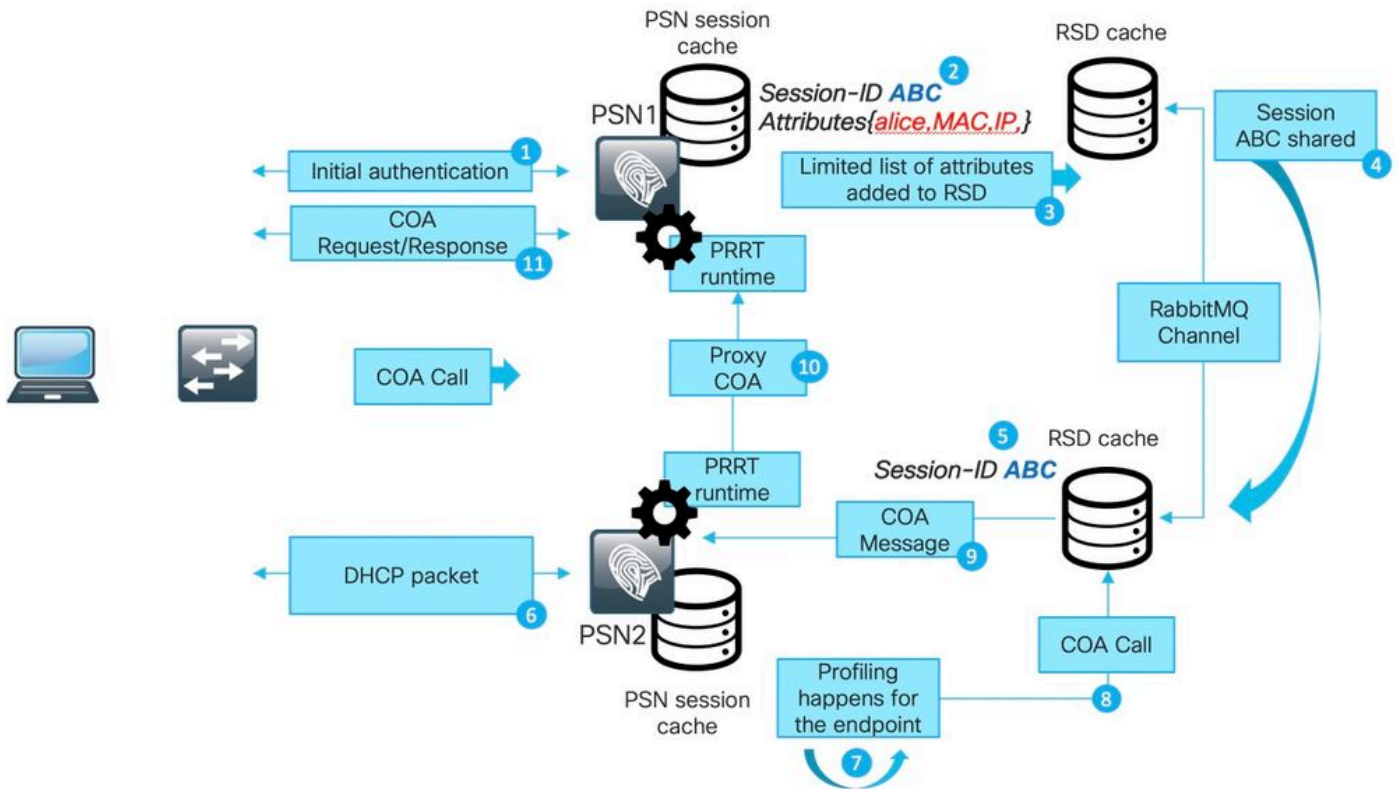
輕量型資料發佈架構

此功能包含以下元素：

- Radius會話目錄(RSD)快取 — 此快取存在於每個ISE節點上並儲存ISE部署中顯示的所有活動會話。 每個會話在快取中的屬性數量有限。 每個會話儲存在Radius會話目錄中的屬性示例：
 - 會話ID。
 - 終端MAC。
 - CallingStationID。
 - 終端IP。
 - PSN IP — 進行身份驗證的PSN。
 - PSN FQDN — 與上面相同。
 - NAS-IP-Address。
 - NAS-IPv6-Address。
 - 狀態 — 已驗證、已啟動、已停止。
- RabbitMQ交換 — 在ISE部署的每個節點上形成一個交換，其中發佈者、相關隊列和消費者呈現。 這確保在所有ISE節點之間形成全網狀拓撲。
- 發佈者 — Radius會話目錄在此處表示發佈者。 在PSN會話快取中建立由PSN處理的新身份驗證成功後，將建立新會話。 對於此會話，將一組有限的屬性放入Radius會話目錄中。
- 使用者 — 在所有其他節點上，Radius會話目錄代表使用者。

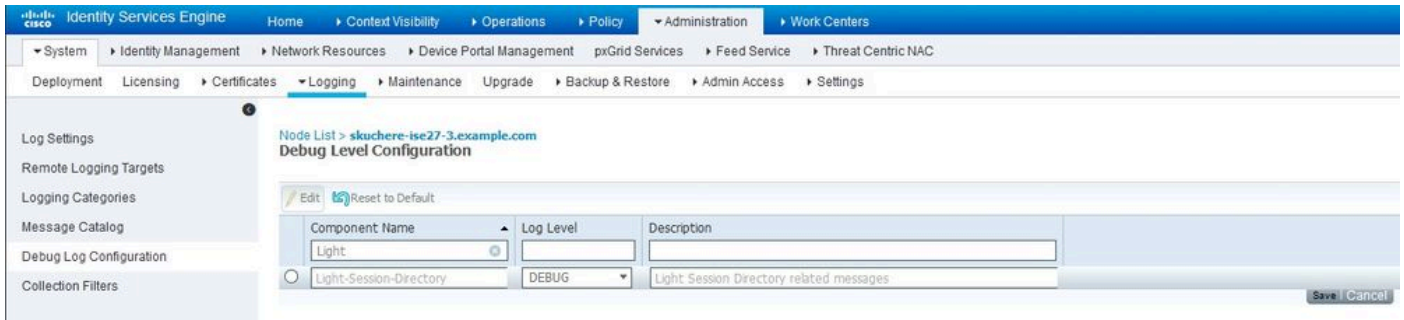
注意：常規RabbitMQ術語和體系結構不在本文檔範圍之內。

圖中解釋了COA流如何與RSD快取配合：



- 1.對PSN1進行初始身份驗證。
- 2.在會話快取中建立的會話ABC。
- 3.將所需的屬性儲存到RSD中。
- 4.通過RabbitMQ與所有其他ISE節點共用會話。
- 5.在所有ISE節點的RSD快取中建立會話。
- 6.新的配置檔案資料到達PSN2。
- 7.重新歸檔端點，如果發生需要執行COA的更改，PSN2將繼續執行下一步。
- 8.向RSD快取提交內部API呼叫以執行COA。
- 9.來自RSD快取的資料用於準備代理COA消息（從一個ISE節點到另一個ISE節點的COA，它包含目標節點可用於向NAD發回CAO請求的所有詳細資訊）。COA消息首先在內部傳輸到PRRT運行時（ISE內的實際AAA伺服器）。
10. PSN2向PSN1傳送COA消息。
11. PSN1向NAD傳送COA消息。

要排除通過ISE上的LDD通訊故障，可以將Light Session Director元件啟用為DEBUG:



來自lsd.log檔案的調試消息示例，用於在原始PSN上建立和發佈會話：

```
DEBUG [pool-45-thread-6][ ] cisco.cpm.lsd.service.LSDRedisClient -::::- Mapping Session ID 0a3e94980000
```

```
DEBUG [PrRTEvents-Executor-2][ ] cisco.cpm.lsd.service.LSDNetAccessEventListener -::::- Publishing sess
```

```
DEBUG [PrRTEvents-Executor-2][ ] cisco.cpm.lsd.service.SessionPublisher -::::- Forwarding session 07a26
```

在所有其他ISE節點上，您可以看到會話的使用方式：

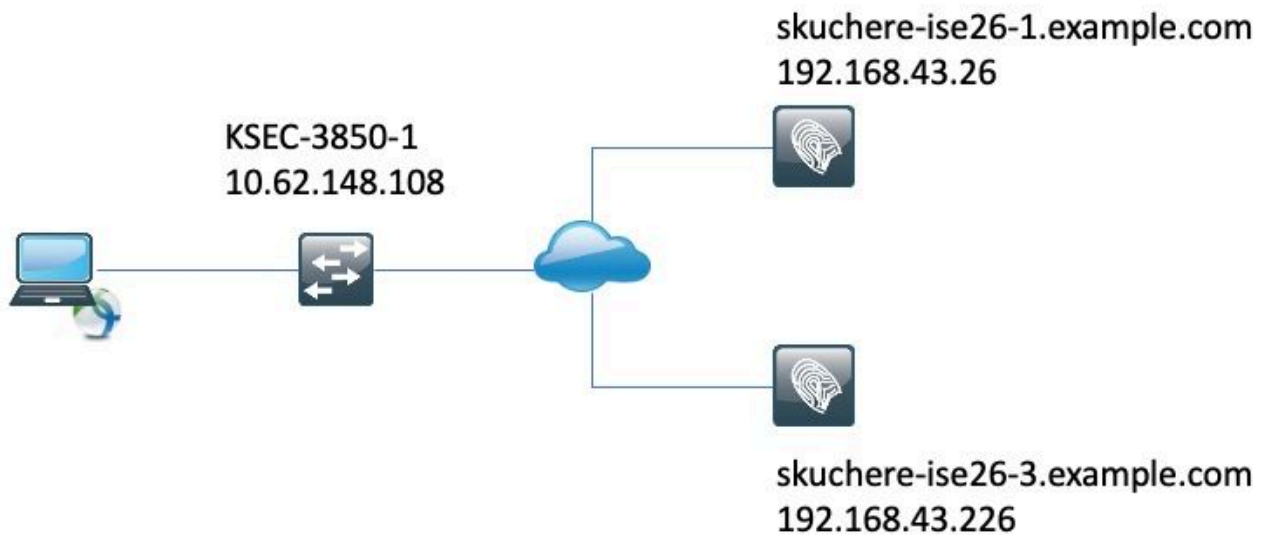
```
[pool-35-thread-38][ ] cisco.cpm.lsd.service.SessionConsumer -::::- Consumer is processing : sessionId:[
```

透過RSD進行狀態共用

當根本原因為Stale/Phantom session或Re-authentication on different PSN with the original session ID not trigger discovery restart時，節點之間的終端安全評估狀態共用可解決出現以下症狀的問題：「AnyConnect ISE終端安全評估模組顯示合規性，而ISE上的會話狀態為掛起」。只要會話符合要求，此資訊就會放到會話RSD中，以後它就可以由部署中的每個PSN使用。

還有一些其它角點的情況是所述特徵無法解決的。例如，當NAD在同一個PSN上使用不同的會話ID運行重新身份驗證時的場景。可使用本文檔中所述的最佳實踐處理此類情景。

圖中演示了用於測試狀態共用狀態的拓撲：



通過RSD進行狀態共用 — 陳舊/幻像會話

要建立陳舊會話身份驗證，最初在skuchere-ise26-1上執行，之後的NAD已重新配置為將記帳傳送到skuchere-ise26-3。在將一條記帳消息轉發到錯誤的PSN之後，再次重新配置了NAD以將記帳傳送回skuchere-ise26-1。

圖中顯示了一個會計報告，它證明了在skuchere-ise26-3上存在幻像會話：

Stop	3.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-1	0A3E946C0000007D5B679296
Interim-Update	2.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-3	0A3E946C0000007D5B679296
Start	1.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-1	0A3E946C0000007D5B679296

1. skuchere-ise26-1處理的Accounting-Start消息。
2. Skuchere-ise處理的同一會話的臨時會計更新26-3。
3. 稍後在skuchere-ise26-1上完成會話。

一段時間後，終端再次連線到網路，但重定向不再有效。在PSN的guest.log - skuchere-ise26-3中，您可以看到以下日誌消息，並且在DEBUG中啟用了client-webapp元件：

```
2020-04-08 13:30:48,217 DEBUG [https-jsse-nio-192.168.43.226-8443-exec-4][] cisco.cpm.client.posture.Ut
```

當PSN檢測到它保留終結點的陳舊/幻像會話時，它不會回覆ISE終端安全評估模組，這允許我們從發生最新身份驗證的PSN獲取正確答案。

作為當前會話查詢時已過期/幻像會話問題的解決方案，PSN會檢查RSD中是否存在該終端的任何新會話。如果RSD包含的會話ID與本地會話快取中的PSN不同，則假定會話快取中顯示的會話已過時。

。

通過RSD進行狀態共用 — PSN之間的故障轉移

為了重現此場景，在分配給符合狀態的終端的授權配置檔案中，已經啟用了一個短的重新身份驗證計時器。之後，NAD被重新配置為將身份驗證和記帳傳送到另一個PSN(skuchere-ise26-3)。重新驗證計時器到期後，同一會話在不同的PSN上未進行驗證。

圖中顯示了一個身份驗證報告，其中顯示了從skuchere-ise26-1到skuchere-ise26-3的sane會話的故障切換：

✓	4.	bob@example.com	00:50:56:B6:0B:C6	Compliant-Wired	skuchere-ise26-3	0A3E946C000000896011D045
✓	3.	bob@example.com	00:50:56:B6:0B:C6	Compliant-Wired	skuchere-ise26-1	0A3E946C000000896011D045
✓	2.		00:50:56:B6:0B:C6		skuchere-ise26-1	0A3E946C000000896011D045
✓		#ACSACL#IP-PERMIT_ALL_IPV4_TRAF...			skuchere-ise26-1	
✓	1.	bob@example.com	00:50:56:B6:0B:C6	CPP-Wired	skuchere-ise26-1	0A3E946C000000896011D045

1. 在skuchere-ise26-1上進行身份驗證，分配具有重定向的授權配置檔案。
2. 成功進行狀態評估後的COA。
3. 分配符合狀態的授權配置檔案時的下一個身份驗證。
4. 身份驗證到達不同的PSN，但它仍然獲取合規狀態的授權配置檔案。

在ise-psc.log中啟用了epm-pip和nsf-session元件的DEBUG中進行故障轉移後，會話在新PSN上獲得合規狀態：

<#root>

```
2020-04-09 11:06:42,176 DEBUG [Thread-7979] [] cpm.nsf.session.impl.SessionCache -::::-
```

```
Looking up session 0A3E946C000000896011D045 for attribute Session.Session.PostureStatus
```

```
2020-04-09 11:06:42,176 DEBUG [Thread-7979] [] cpm.nsf.session.api.ExecutionContext -::::- Execution con
```

```
2020-04-09 11:06:42,176 DEBUG [Thread-7979] [] cpm.nsf.session.impl.PIPManager -::::- Returning a PIP co
```

```
2020-04-09 11:06:42,176 DEBUG [Thread-7979] [] cpm.nsf.session.api.ExecutionContext -::::- Execution con
```

```
2020-04-09 11:06:42,176 DEBUG [Thread-7979] [] cpm.nsf.session.impl.SessionCache -::::- Looking up sessi
```

```
2020-04-09 11:06:42,176 DEBUG [SessionLifecycleNotifier] [] cpm.nsf.session.internal.LRUagingAlgorithm -
```

```
2020-04-09 11:06:42,176 DEBUG [Thread-7979] [] cpm.nsf.session.impl.SessionCache -::::- Returning for se
```

```
IndexValues: {}
```

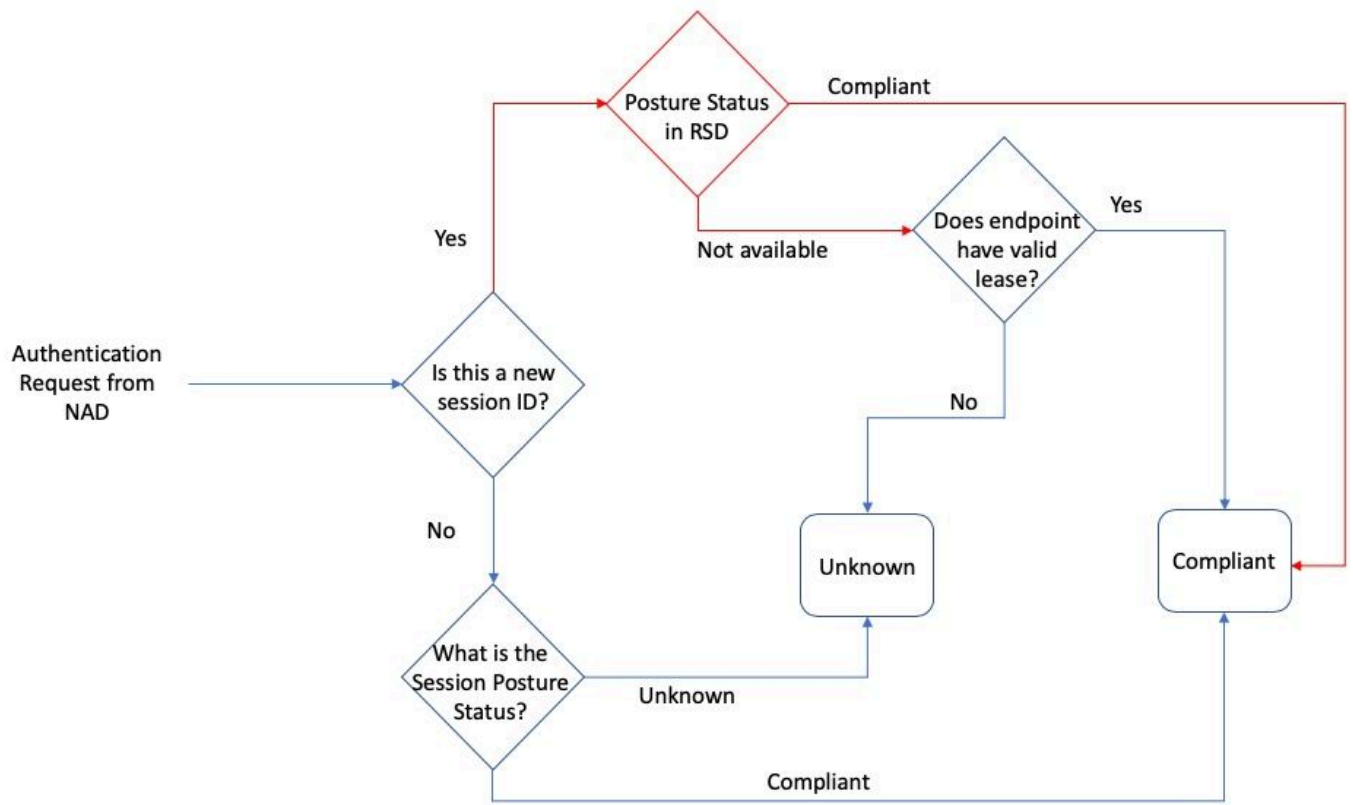
```
2020-04-09 11:06:42,177 DEBUG [Thread-7979] [] cisco.cpm.posture.pip.PostureStatusPIP -::::-
```

```
set postureStatus based on posture LSD dictionary: Compliant
```

```
2020-04-09 11:06:42,177 DEBUG [Thread-7979] [] cisco.cpm.posture.pip.PostureStatusPIP -::::-
```

```
PostureStatusPIP for mac 00-50-56-B6-0B-C6 - Attribute Session.Session.PostureStatus value is Compliant
```

通過在姿勢狀態選擇過程中新增額外邏輯，解決了原始問題。圖中顯示了已更改的內容（以紅色突出顯示的更改）：



關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。