配置狀態狀態同步並對其進行故障排除

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

設定

- 網路圖表
- 組態

驗證

- 從DART捆綁包
- 從客戶端上的資料包捕獲
- 從ISE
- 狀態狀態更改時狀態重新啟動

疑難排解

- 狀況狀態同步無法啟動
- 安全評估狀態同步失敗，ISE控制台上出現警報
  - 驗證為狀態「相容」授權配置檔案配置的dACL
- 已知的問題
  - 狀態狀態同步失敗，ISE上出現警報

簡介

本文檔介紹在Cisco Identity Service Engine(ISE) 3.1版本中引入的狀態狀態同步的配置與使用。

必要條件

需求

思科建議您瞭解以下主題：

- 思科ISE上的狀態流
- 在Cisco ISE上配置終端安全評估元件

假設您有狀態配置來代替任何型別。

為了更好地理解稍後介紹的概念，建議進行以下操作：

- 思科身份服務引擎管理員指南3.1版
- 比較早期ISE版本與ISE 2.2中的ISE終端安全評估流程
- ISE會話管理和安全評估

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE版本3.1
- 思科安全使用者端5.0.00556

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

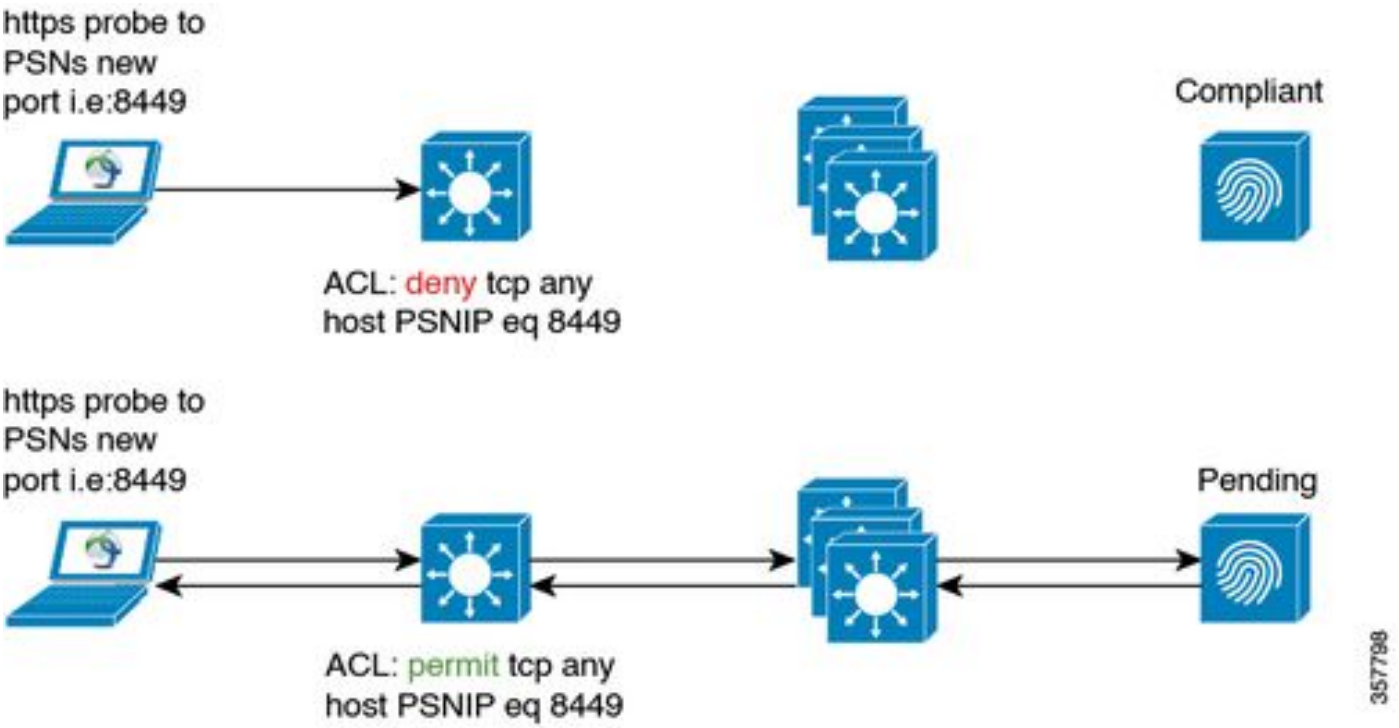
ISE終端安全評估流程通常不允許在客戶端上從ISE更新終端安全評估狀態。思科安全客戶端安全評估模組用於評估終端的安全評估狀態，並將其保留到網路更改、定期重新評估或其他客戶端觸發事件之前。如果終端安全評估狀態由於會話終止或其他原因在ISE上發生更改，安全客戶端安全評估模組可能不知道該更改，因此終端將處於安全評估未知狀態，網路訪問受限，直到某個客戶端觸發事件發生。

本文檔重點介紹一項新功能- Posture Status Synchronization，該功能旨在解決此類問題，並允許ISE向安全客戶端狀態模組提供有關終端當前狀態的反饋。

設定

啟用終端安全評估狀態同步時，每個ISE PSN節點上都會引入終端安全評估狀態探測埠-預設情況下為TCP 8449。如果Endpoint Posture狀態為Unknown或Pending，且如果Endpoint狀態為Compliant，則應該可從終端訪問它。

網路圖表



組態

狀態狀態同步功能配置包括兩部分：

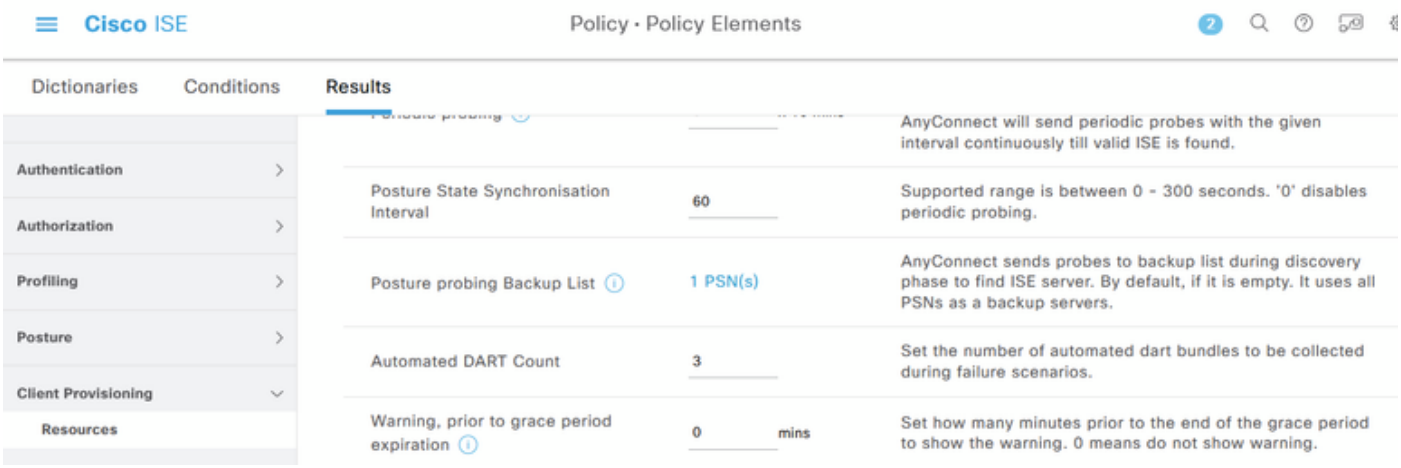
1. AnyConnect終端安全評估配置檔案配置

1.1在Cisco ISE GUI中，導航到策略>策略元素>結果>客戶端調配>資源。

1.2選擇您已使用的AnyConnect終端安全評估配置檔案，或建立新配置檔案。

1.3在「Agent Behavior」區域，將Posture State Synchronization Interval配置為介於1和300秒之間的任意值，0表示停用狀態同步

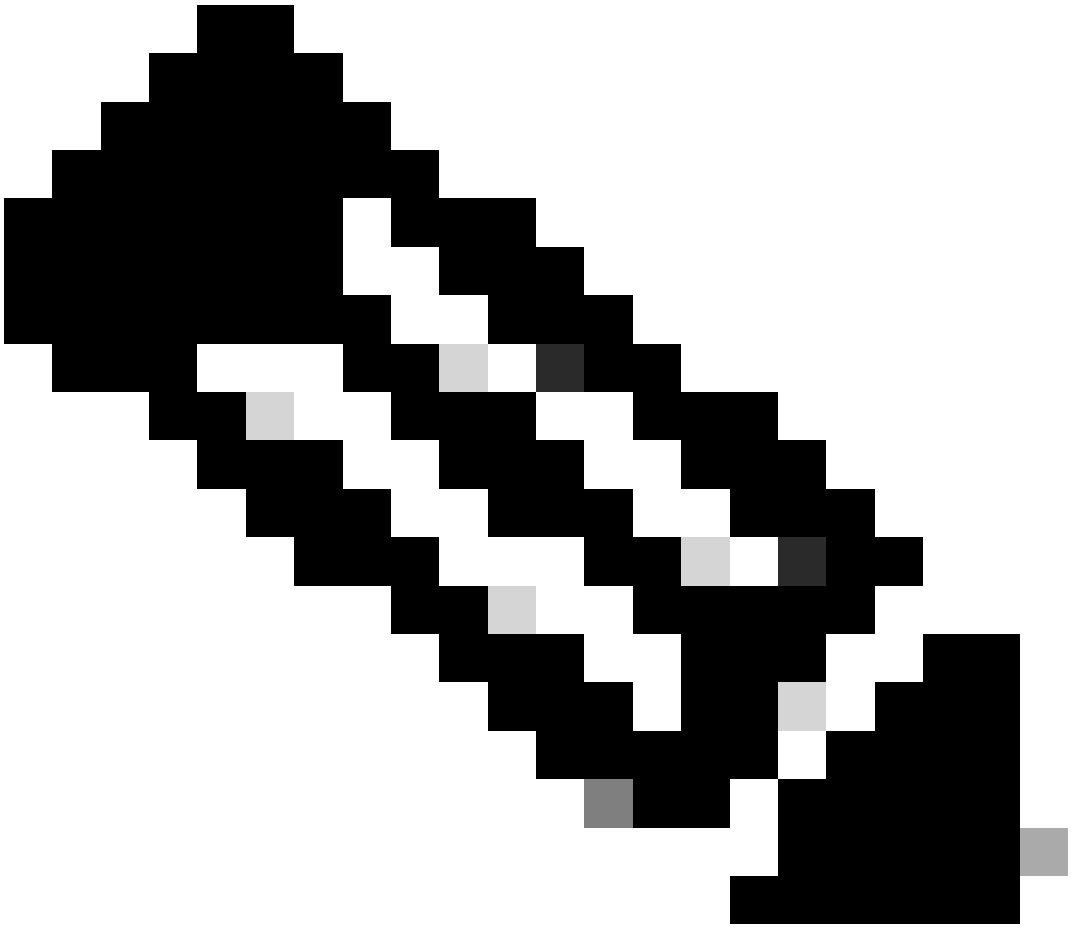
1.4 您可以配置終端安全評估探測備份清單-安全客戶端使用此清單檢查所選PSN上的終端安全評估狀態。如果不選擇任何PSN，則連線的PSN和任意兩台備份伺服器用作狀態同步的備份。



2. 配置可下載ACL(dACL)，在客戶端狀態為合規或不合規時阻止對思科ISE上的安全評估狀態同步埠的訪問。如果終端狀態為已知，您需要為用於合規終端的ACL頂部的每個PSN增加具有狀態狀態狀態同步埠的訪問控制拒絕條目，以限制對狀態狀態同步埠的訪問，例如：

```
deny tcp any host PSN1-IP-ADDRESS eq 8449
deny tcp any host PSN2-IP-ADDRESS eq 8449
permit ip any any
```

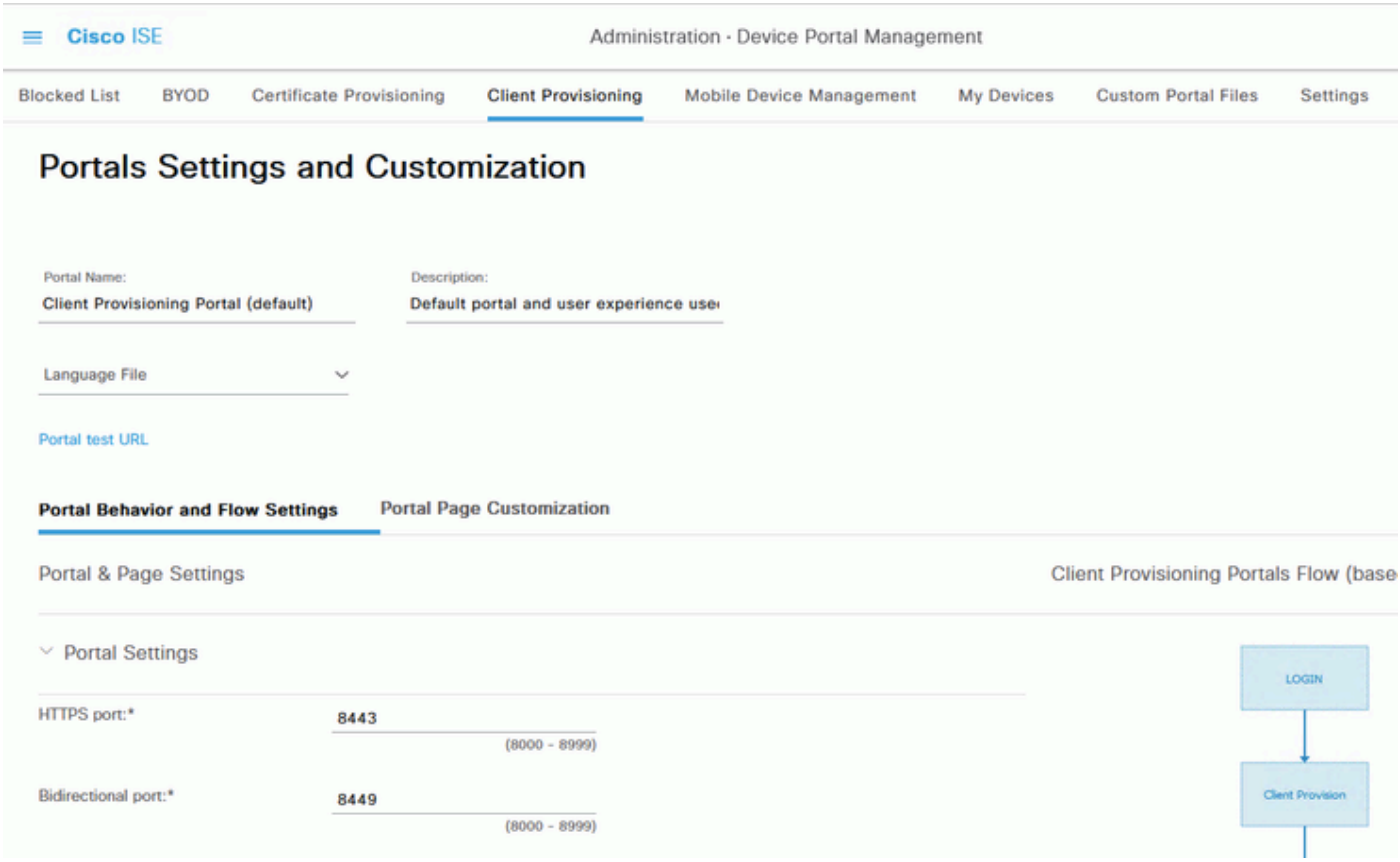
permit ip any any不是必需的，您可以根據需要用任何規則集替換它。



> 注意：如果未配置dACL中的deny條目，則在Cisco ISE控制台上觸發狀態配置檢測警報(Posture Configuration Detection Alarm)並在終端上停用狀態同步(Posture State Synchronization)，直到Cisco Secure Client重新啟動。

可以在Client Provisioning Portal configuration頁面上更改狀態狀態同步埠（雙向埠）。導航到管理

>裝置門戶管理>客戶端調配>選擇所需門戶>門戶行為和流設定，然後打開門戶設定。無法更改預設客戶端調配門戶的終端安全評估狀態同步埠。



驗證

從DART捆綁包

透過檢視DART捆綁包中的思科安全客戶端狀態模組日誌(AnyConnect_ISEPosture.txt)，可從客戶端驗證狀態同步：

1. 狀態評估已完成，狀態狀態為「合規」。

```
2022/11/09 12:22:47 [Information] aciseagent Function: Authenticator::sendUIStatus Thread Id: 0xC60 Fil
```

2. 狀態同步探測已啟動。

```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
```

3. 在狀態狀態同步埠(8449)上啟動到ISE PSN的HTTPS連線。

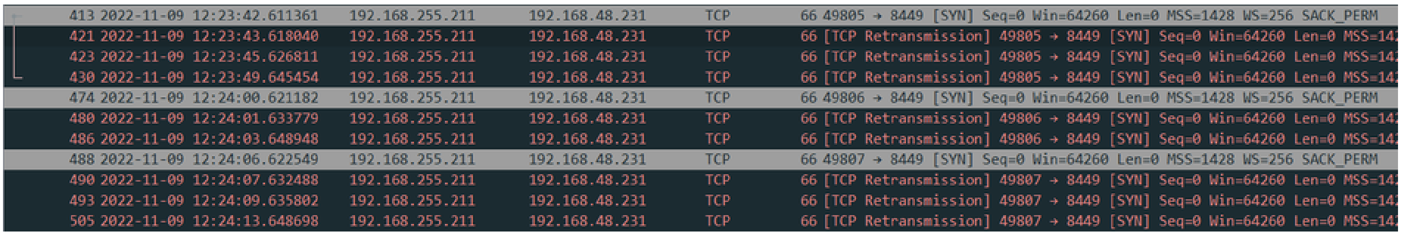
```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:22:47 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x296C Fi
```

4. 狀態狀態同步探測超時。

```
2022/11/09 12:22:54 [Information] aciseagent Function: hs_transport_winhttp_post Thread Id: 0x296C File
2022/11/09 12:22:54 [Information] aciseagent Function: hs_transport_post Thread Id: 0x296C File: hs_tra
2022/11/09 12:22:54 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
```

從客戶端上的資料包捕獲

在客戶端上捕獲的資料包顯示，在沒有ISE PSN的SYN-ACK響應的情況下，在終端安全評估狀態同步埠(8449)上向ISE PSN節點傳送了SYN資料包：



413	2022-11-09 12:23:42.611361	192.168.255.211	192.168.48.231	TCP	66	49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
421	2022-11-09 12:23:43.618040	192.168.255.211	192.168.48.231	TCP	66	[TCP Retransmission] 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
423	2022-11-09 12:23:45.626811	192.168.255.211	192.168.48.231	TCP	66	[TCP Retransmission] 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
430	2022-11-09 12:23:49.645454	192.168.255.211	192.168.48.231	TCP	66	[TCP Retransmission] 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
474	2022-11-09 12:24:00.621182	192.168.255.211	192.168.48.231	TCP	66	49806 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
480	2022-11-09 12:24:01.633779	192.168.255.211	192.168.48.231	TCP	66	[TCP Retransmission] 49806 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
486	2022-11-09 12:24:03.648948	192.168.255.211	192.168.48.231	TCP	66	[TCP Retransmission] 49806 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
488	2022-11-09 12:24:06.622549	192.168.255.211	192.168.48.231	TCP	66	49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
490	2022-11-09 12:24:07.632488	192.168.255.211	192.168.48.231	TCP	66	[TCP Retransmission] 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
493	2022-11-09 12:24:09.635802	192.168.255.211	192.168.48.231	TCP	66	[TCP Retransmission] 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
505	2022-11-09 12:24:13.648698	192.168.255.211	192.168.48.231	TCP	66	[TCP Retransmission] 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14

從ISE

無法從ISE端驗證正確的終端安全評估狀態同步配置，因為終端安全評估狀態同步埠(8449)上的連線應該失敗。

狀態狀態更改時狀態重新啟動

1)當思科安全客戶端處於「相容」狀態時，從ISE收到的會話狀態資訊保安評估狀態為「未知」。

```
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
```

2)思科安全客戶端確認安全評估狀態更改並重新啟動安全評估發現：

```
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
```

3)思科安全客戶端停止狀態同步，直到執行狀態評估：

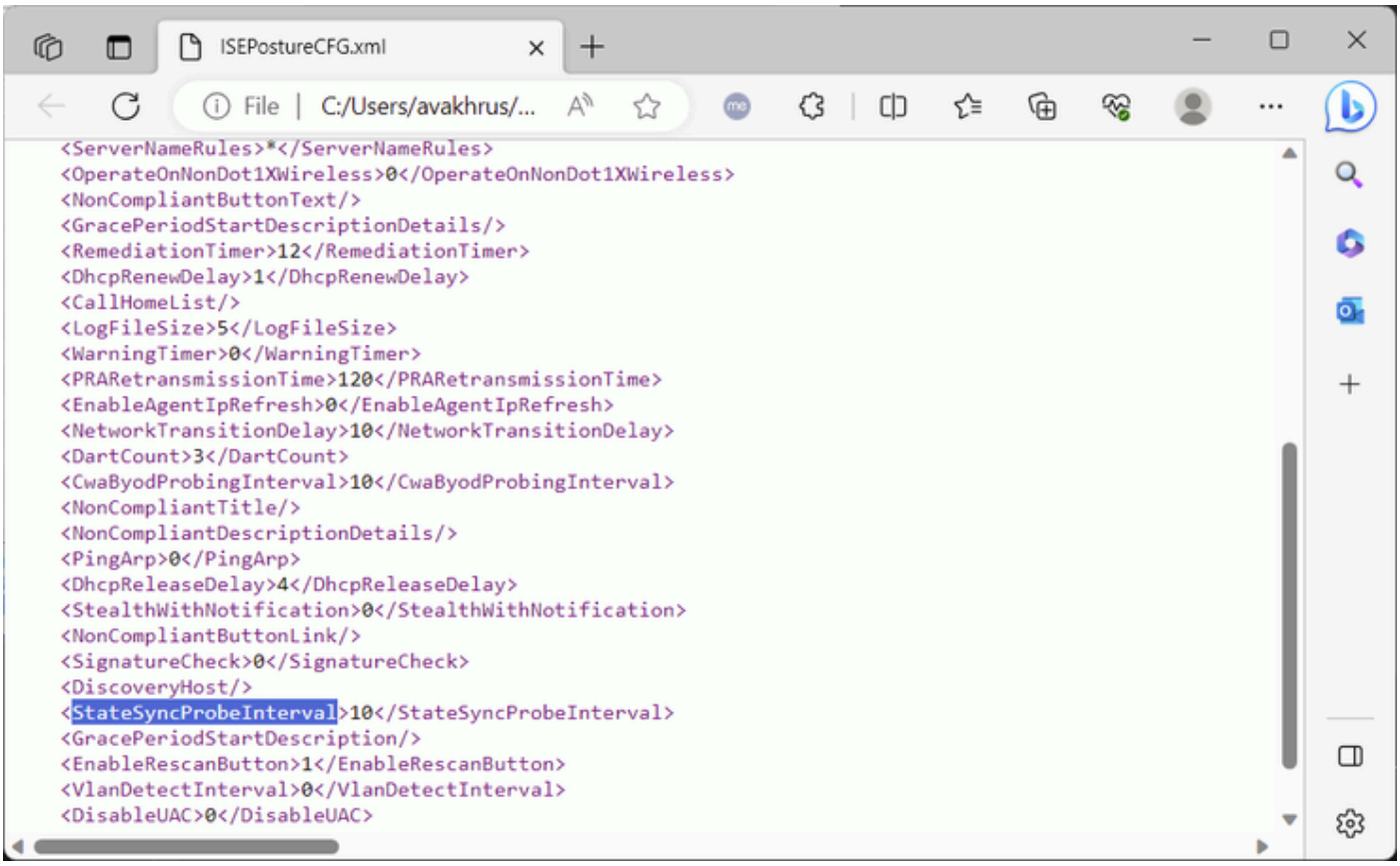
```
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::processMessage Thread Id: 0xC60
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
2022/11/09 12:26:24 [Information] aciseagent Function: hs_transport_free Thread Id: 0xC60 File: hs_tran
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
```

疑難排解

狀況狀態同步無法啟動

如果AnyConnect_ISEPosture.txt日誌檔案中沒有指示狀態同步啟動，並且客戶端未嘗試與狀態同步埠(8449)上的ISE PSN節點建立連線，請從DART捆綁包或直接在客戶端電腦上檢查狀態配置檔案ISEPostureCFG.xml：「%ProgramData%\Cisco\Cisco Secure Client\ISE Posture\」（適用於Windows PC）。

負責狀態同步的引數是「StateSyncProbeInterval」，應使用大於0的值進行設定：



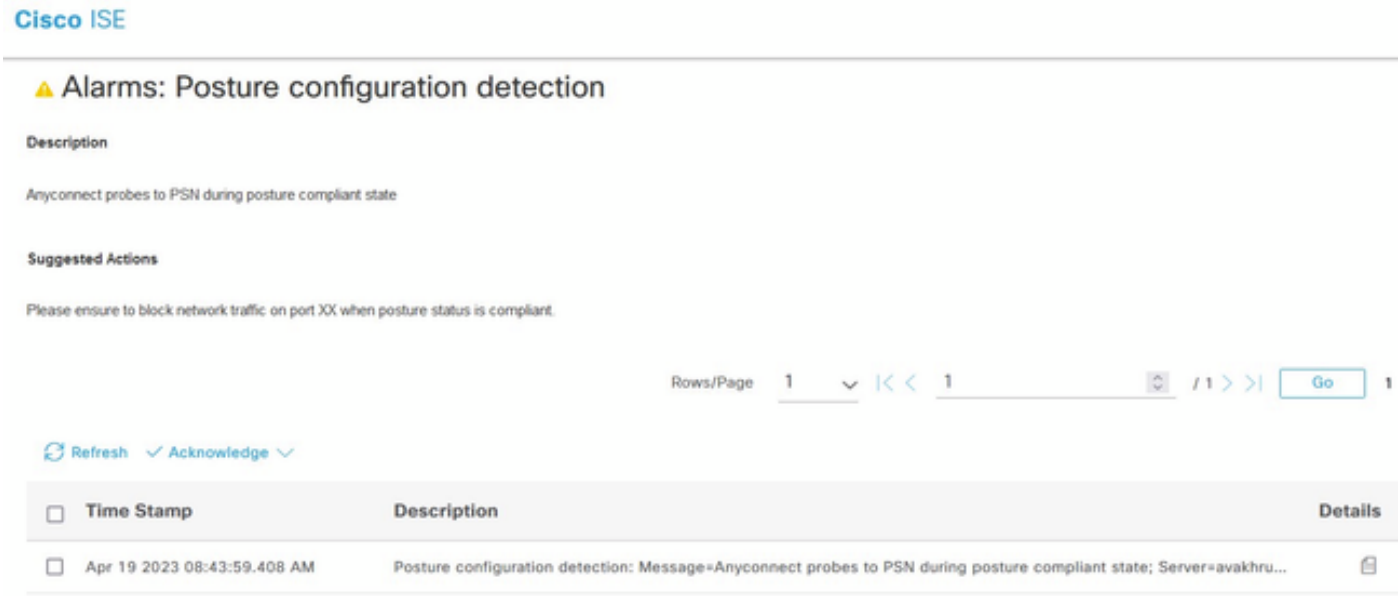
缺少「StateSyncProbeInterval」或值為「0」表示狀態同步被停用。

如果在ISE的終端安全評估配置檔案中設定了「終端安全評估狀態同步時間間隔」，但它沒有反映在客戶端的配置檔案中，則需要調查終端安全評估調配。

安全評估狀態同步失敗，ISE控制台上出現警報

如果ISE上的安全狀態同步失敗並發出警報，則意味著思科安全客戶端能夠在安全狀態同步埠(8449)上訪問ISE，並請求會話的狀態為「相容」(Compliant)。

- ISE GUI中的警報：



- 驗證資料包捕獲

在狀態狀態同步埠(8449)上建立TCP連線：

No.	Time	Source	Destination	Protocol	Length	Info
988	2022-11-09 12:26:24.690977	192.168.255.211	192.168.48.231	TCP	66	49819 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
989	2022-11-09 12:26:24.744041	192.168.48.231	192.168.255.211	TCP	66	8449 → 49819 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1300 SACK_PERM WS=128
990	2022-11-09 12:26:24.744102	192.168.255.211	192.168.48.231	TCP	54	49819 → 8449 [ACK] Seq=1 Ack=1 Win=262400 Len=0
991	2022-11-09 12:26:24.744548	192.168.255.211	192.168.48.231	TLSv1…	268	Client Hello
992	2022-11-09 12:26:24.796877	192.168.48.231	192.168.255.211	TCP	60	8449 → 49819 [ACK] Seq=1 Ack=215 Win=30336 Len=0
993	2022-11-09 12:26:24.813236	192.168.48.231	192.168.255.211	TCP	1354	8449 → 49819 [ACK] Seq=1 Ack=215 Win=30336 Len=1300 [TCP segment of a reassembl
994	2022-11-09 12:26:24.813335	192.168.48.231	192.168.255.211	TLSv1…	824	Server Hello, Certificate, Server Key Exchange, Server Hello Done
995	2022-11-09 12:26:24.813396	192.168.255.211	192.168.48.231	TCP	54	49819 → 8449 [ACK] Seq=215 Ack=2071 Win=262400 Len=0
996	2022-11-09 12:26:24.815274	192.168.255.211	192.168.48.231	TLSv1…	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
997	2022-11-09 12:26:24.881656	192.168.48.231	192.168.255.211	TLSv1…	60	Change Cipher Spec
998	2022-11-09 12:26:24.881656	192.168.48.231	192.168.255.211	TLSv1…	99	Encrypted Handshake Message
999	2022-11-09 12:26:24.881755	192.168.255.211	192.168.48.231	TCP	54	49819 → 8449 [ACK] Seq=341 Ack=2122 Win=262400 Len=0

- 從思科安全客戶端狀態模組日誌進行驗證

從DART捆綁包檢查AnyConnect_ISEPosture.txt：

1)在終端安全評估狀態同步埠(8449)上啟動到ISE PSN的HTTPS連線。

```
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x275
```

2)從ISE收到的會話狀態資訊保安評估狀態為「相容」。

```
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
```

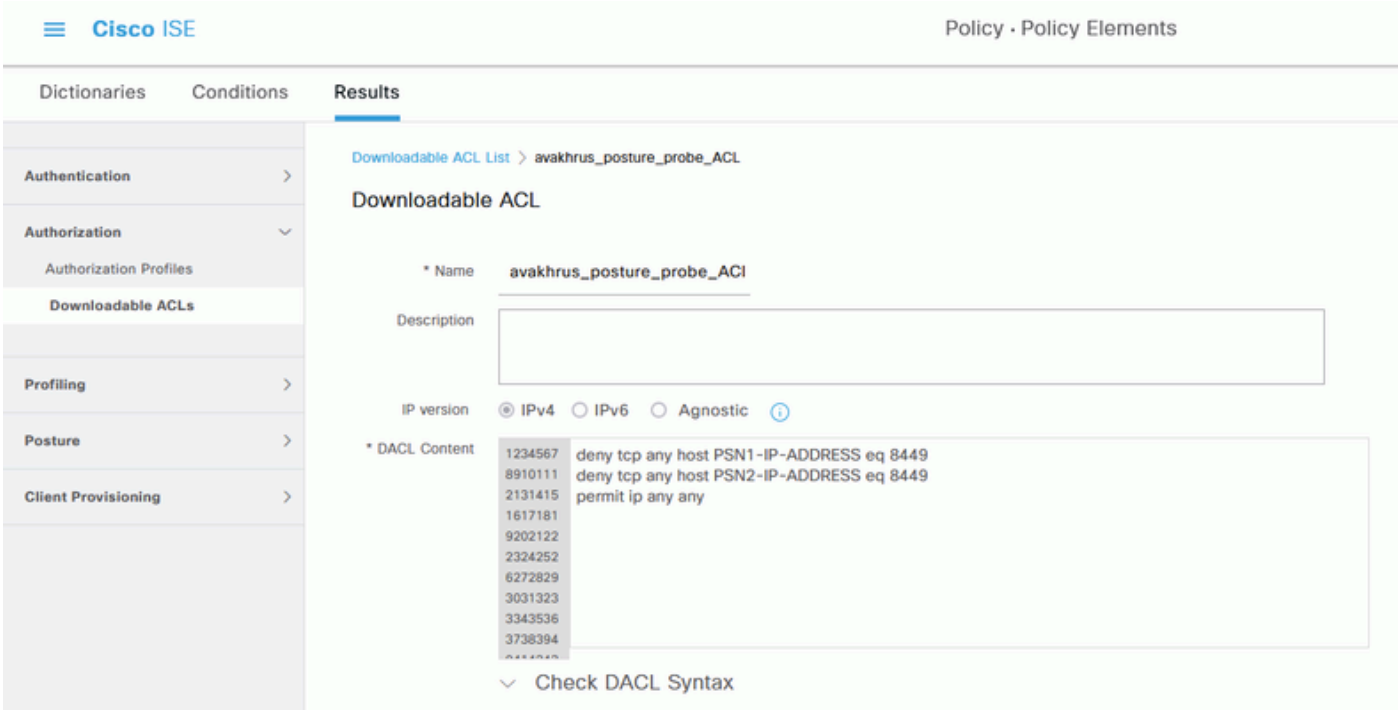
3)由於檢測到不正確的配置，Posture State Synchronization停止：

```
2022/11/09 12:26:34 [Error] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x2750 File
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x275
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
```

無法通過重新啟動狀態評估或網路更改從思科安全客戶端GUI中重新啟動狀態狀態同步。相反，需要重新啟動Cisco Secure Client才能使狀態同步重新工作。

驗證為狀態「相容」授權配置檔案配置的dACL

1. 驗證為安全狀態「相容」授權配置檔案配置了正確的dACL：



2. 驗證詳細身份驗證報告dACL作為「相容」端點的身份驗證結果是否正確傳送。

CPMSessionID	c0a830e7lFjmLTxwC_6BfWNqU3RwKrGfaDTw5krqr1QOzEm/ej0
CiscoAVPair	aaa:service=ip_admission,aaa:event=acl-download

Result

Class	CACS:c0a830e7lFjmLTxwC_6BfWNqU3RwKrGfaDTw5krqr1QOzEm/ej0:ISE-PSN-FQDN/482174459/480
cisco-av-pair	ip:inacl#1=deny tcp any host PSN1-IP-ADDRESS eq 8449
cisco-av-pair	ip:inacl#2=deny tcp any host PSN2-IP-ADDRESS eq 8449
cisco-av-pair	ip:inacl#3=permit ip any any

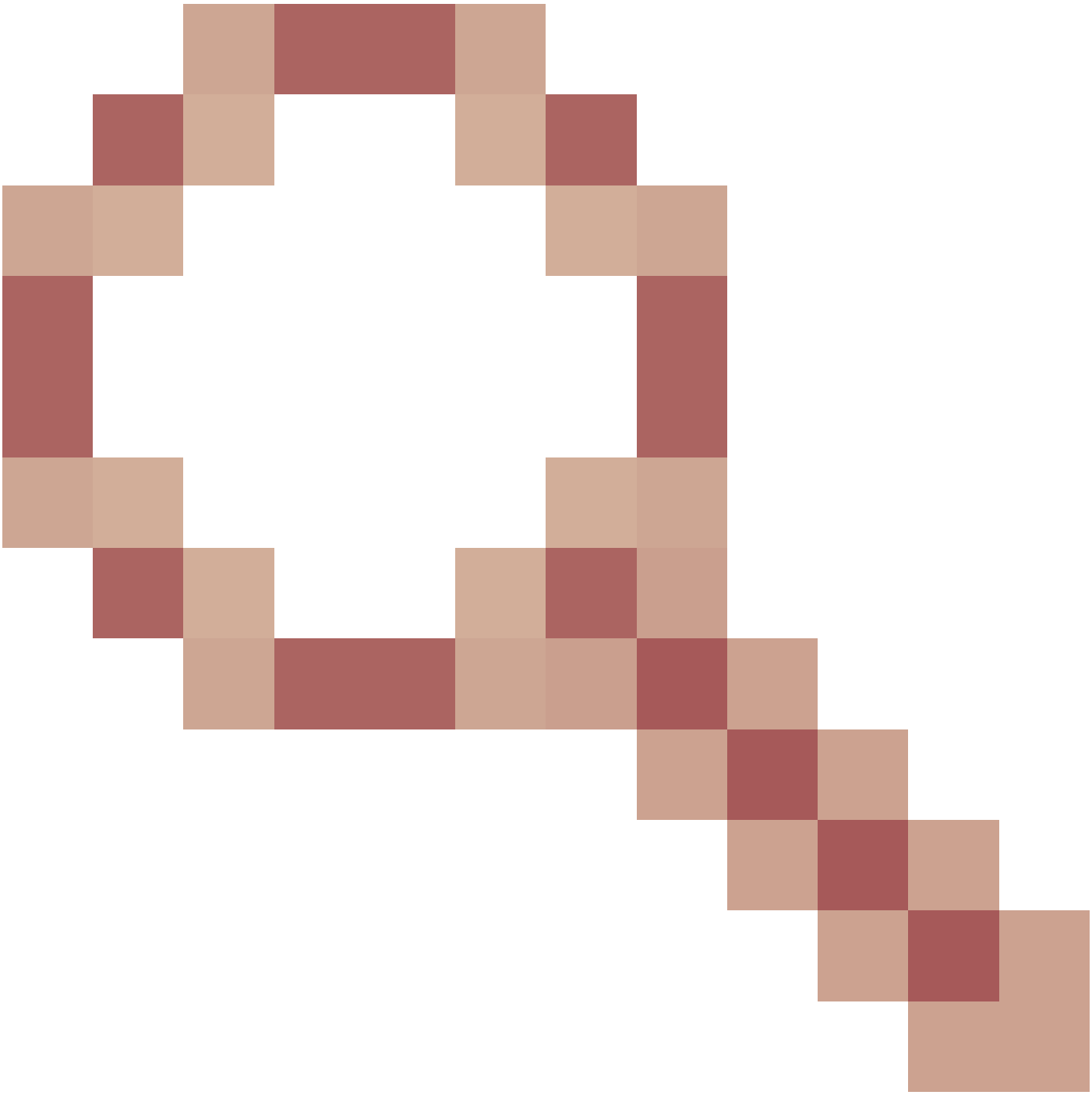
3. 驗證dACL是否正確應用於網路訪問裝置：

```
avakhrus_3560C#sh authe sess int fa0/12 det
            Interface:  FastEthernet0/12
          MAC Address:  0050.56a8.be02
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.255.193
            User-Name:  TRAINING\bob
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  172800s (local), Remaining: 92111s
       Session Uptime:  1515s
    Common Session ID:  C0A8FF0C00000012679EAF14
      Acct Session ID:  0x00000012
               Handle:  0x5D000005
       Current Policy:  POLICY_Fa0/12

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
             ACS ACL:  xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac

Method status list:
       Method           State

       mab              Stopped
       dot1x            Authc Success

avakhrus_3560C#sh access-lists | s  xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac
Extended IP access list xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac (per-user)
    1 deny tcp any host PSN1-IP-ADDRESS eq 8449
    2 deny tcp any host PSN2-IP-ADDRESS eq 8449
    3 permit ip any any
```

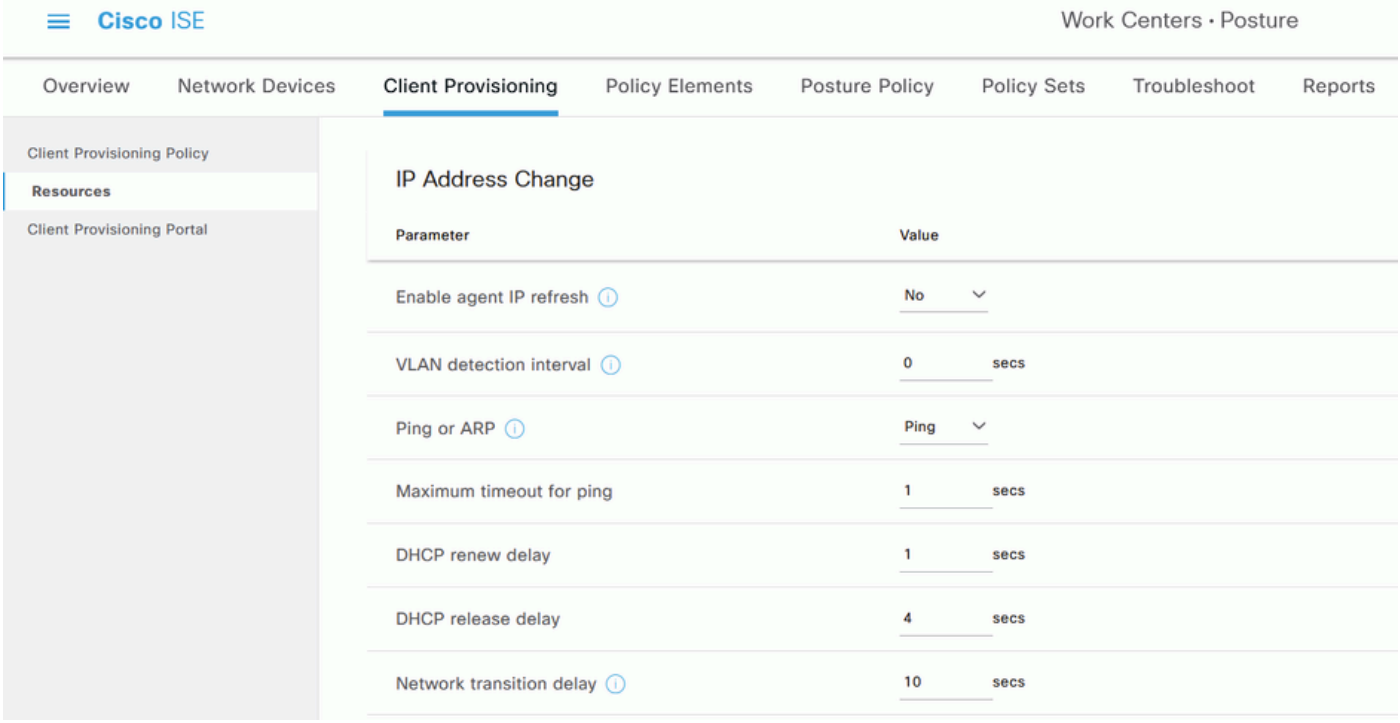
已知的問題

狀態狀態同步失敗，ISE上出現警報

即使在網路訪問裝置上對客戶端終端應用了正確的dACL，狀態同步也可能因ISE上的警報而失敗。如果Posture State Synchronization Probe的執行速度快於應用dACL的速度，或者如果Posture State Synchronization Probe在應用dACL時已在進行中，則會發生這種情況。思科漏洞ID CSCwd58316中調查了此問題



.解決方法是，您需要在Anyconnect終端安全評估配置檔案（ISE終端安全評估代理配置檔案設定）中將「網路轉換延遲」設定為10秒。


Cisco ISE
Work Centers · Posture
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Client Provisioning Policy
Resources
Client Provisioning Portal
IP Address Change
Parameter
Value
Enable agent IP refresh
No
VLAN detection interval
0
secs
Ping or ARP
Ping
Maximum timeout for ping
1
secs
DHCP renew delay
1
secs
DHCP release delay
4
secs
Network transition delay
10
secs

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）。