Configurazione e risoluzione dei problemi di sincronizzazione dello stato della postura

Sommario

Introduzione

Questo documento descrive la configurazione e l'utilizzo della sincronizzazione dello stato della postura introdotta nella versione 3.1 di Cisco Identity Service Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Posture flow su Cisco ISE
- Configurazione dei componenti di postura su Cisco ISE

Si suppone che abbiate una configurazione di postura al posto di qualsiasi tipo.

Per comprendere meglio i concetti descritti più avanti, si consiglia di esaminare:

- Guida dell'amministratore di Cisco Identity Services Engine, versione 3.1
- Confronta le versioni precedenti di ISE con ISE Posture Flow in ISE 2.2
- Gestione e postura delle sessioni ISE

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE versione 3.1
- Cisco Secure Client 5.0.00556

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

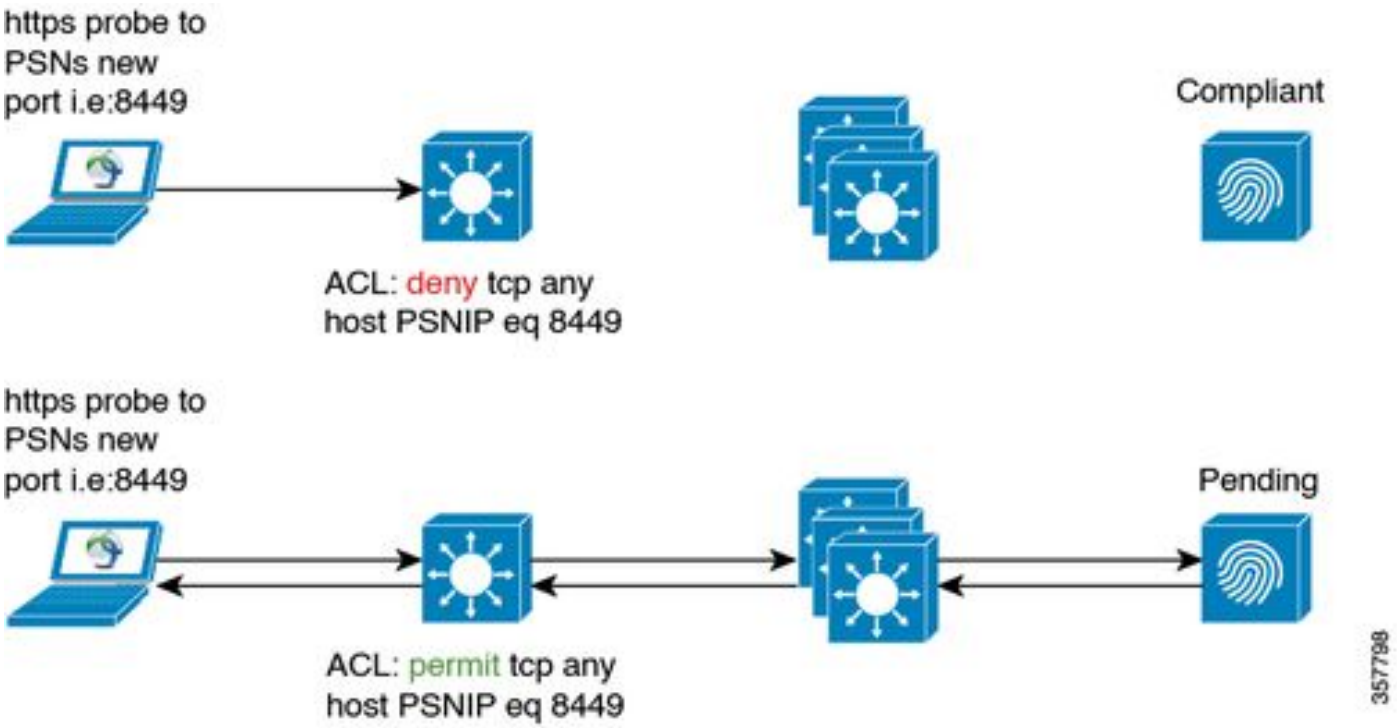
Il flusso ISE Posture in genere non consente di aggiornare lo stato della postura sul client dall'ISE. Il modulo Cisco Secure Client Posture viene usato per valutare lo stato della postura dell'endpoint e lo mantiene fino alla modifica della rete, alla rivalutazione periodica o ad altri trigger sul lato client. Se lo stato di postura dell'endpoint cambia in ISE a causa della terminazione di una sessione o per altri motivi, il modulo Secure Client Posture potrebbe non essere a conoscenza della modifica, quindi l'endpoint rimane in stato di postura sconosciuta con accesso limitato alla rete fino a quando non si verifica uno dei trigger lato client.

Questo documento è incentrato su una nuova funzione - Sincronizzazione dello stato della postura, che è stata sviluppata per risolvere questo tipo di problema e consentire ad ISE di fornire un feedback al Secure Client Posture Module sullo stato corrente della postura dell'endpoint.

Configurazione

La porta probe dello stato della postura è stata introdotta su ciascun nodo PSN ISE quando la sincronizzazione dello stato della postura è abilitata - TCP 8449 per impostazione predefinita. Deve essere raggiungibile dall'endpoint se lo stato della postura dell'endpoint è Sconosciuto o In sospeso e non raggiungibile se lo stato dell'endpoint è Conforme.

Esempio di rete



Configurazioni

La configurazione della feature Sincronizzazione stato postura (Posture State Synchronization) è costituita da due parti:

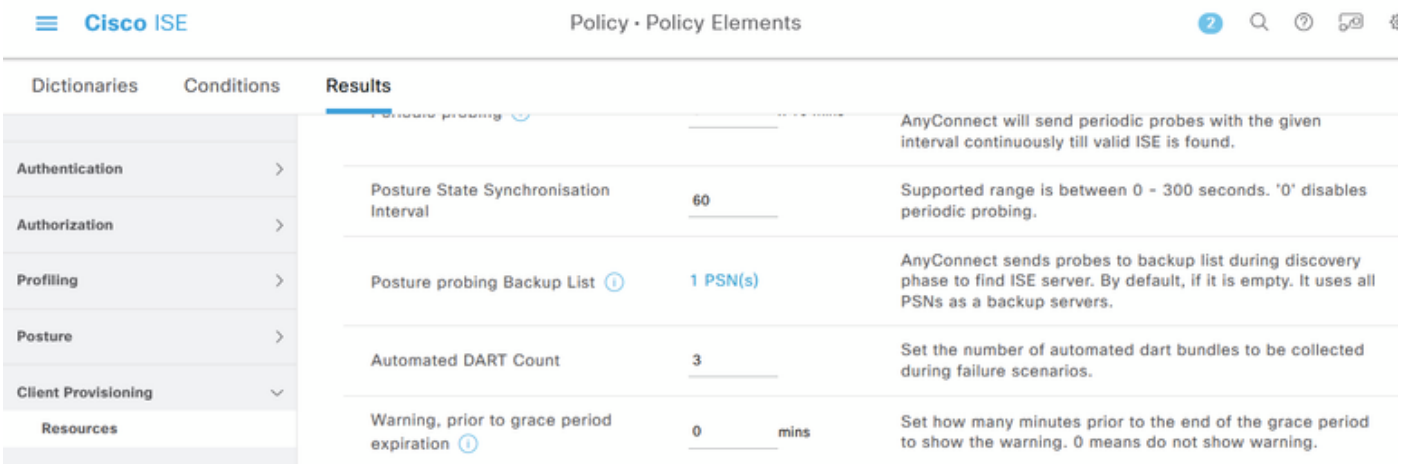
1. Configurazione del profilo di postura di AnyConnect

1.1 Nell'interfaccia utente di Cisco ISE, selezionare Policy > Policy Elements > Results > Client Provisioning > Resources (Policy > Elementi della policy > Risultati > Provisioning client > Risorse).

1.2 Selezionare il profilo di postura di AnyConnect già in uso o crearne uno nuovo.

1.3 Nell'area Comportamento agente, configurare l'intervallo di sincronizzazione dello stato della postura su un valore compreso tra 1 e 300 secondi, 0 - disattiva la sincronizzazione dello stato della postura

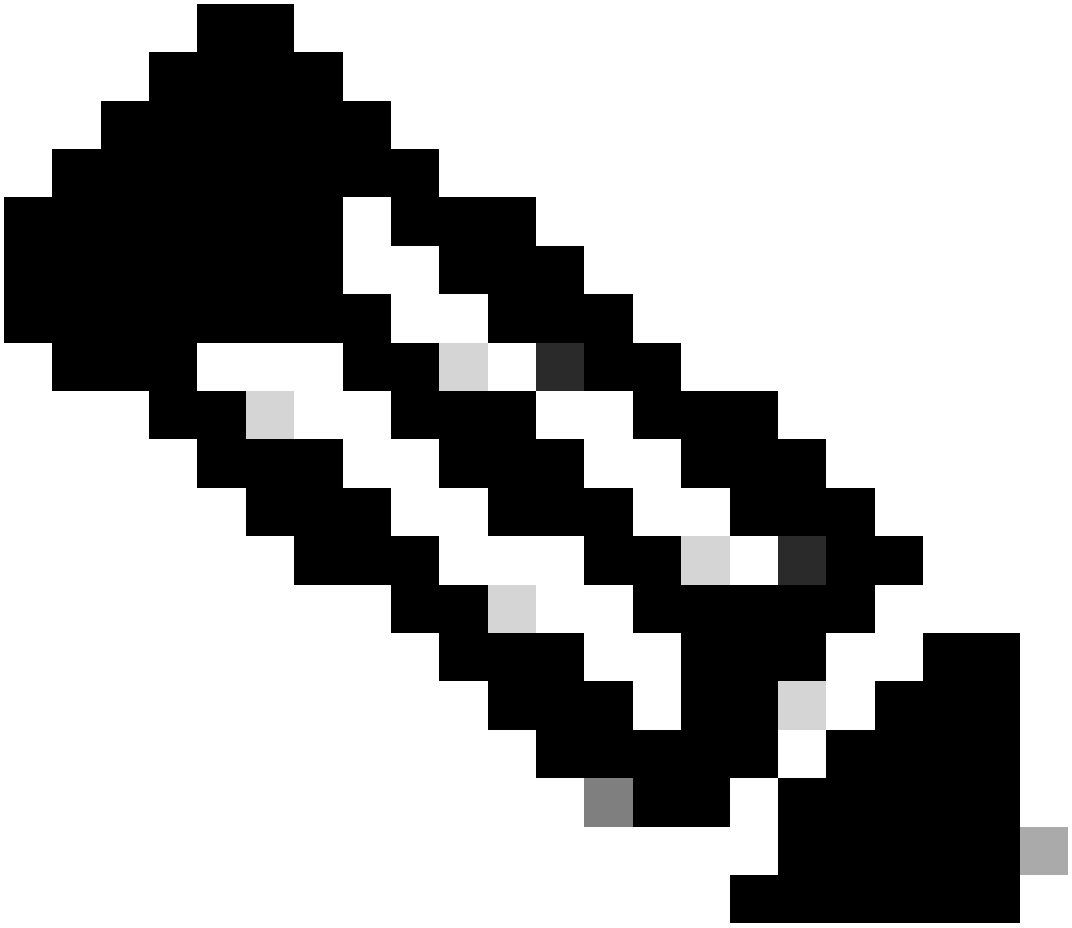
1.4 È possibile configurare l'elenco di backup di verifica della postura. Secure Client utilizza questo elenco per controllare lo stato della postura sui nomi di servizio (PSN) selezionati. Se non si sceglie un PSN, il PSN connesso e i due server di backup vengono utilizzati come backup per la sincronizzazione dello stato di postura.



2. Configurazione di un ACL (dACL) scaricabile per bloccare l'accesso alla porta di sincronizzazione dello stato della postura su Cisco ISE quando lo stato della postura del client è Conforme o Non conforme. Per limitare l'accesso alla porta di sincronizzazione dello stato della postura se lo stato dell'endpoint è noto, è necessario aggiungere la voce di rifiuto del controllo di accesso con la porta di sincronizzazione dello stato della postura per ogni PSN nella parte superiore degli ACL utilizzati per gli endpoint conformi, ad esempio:

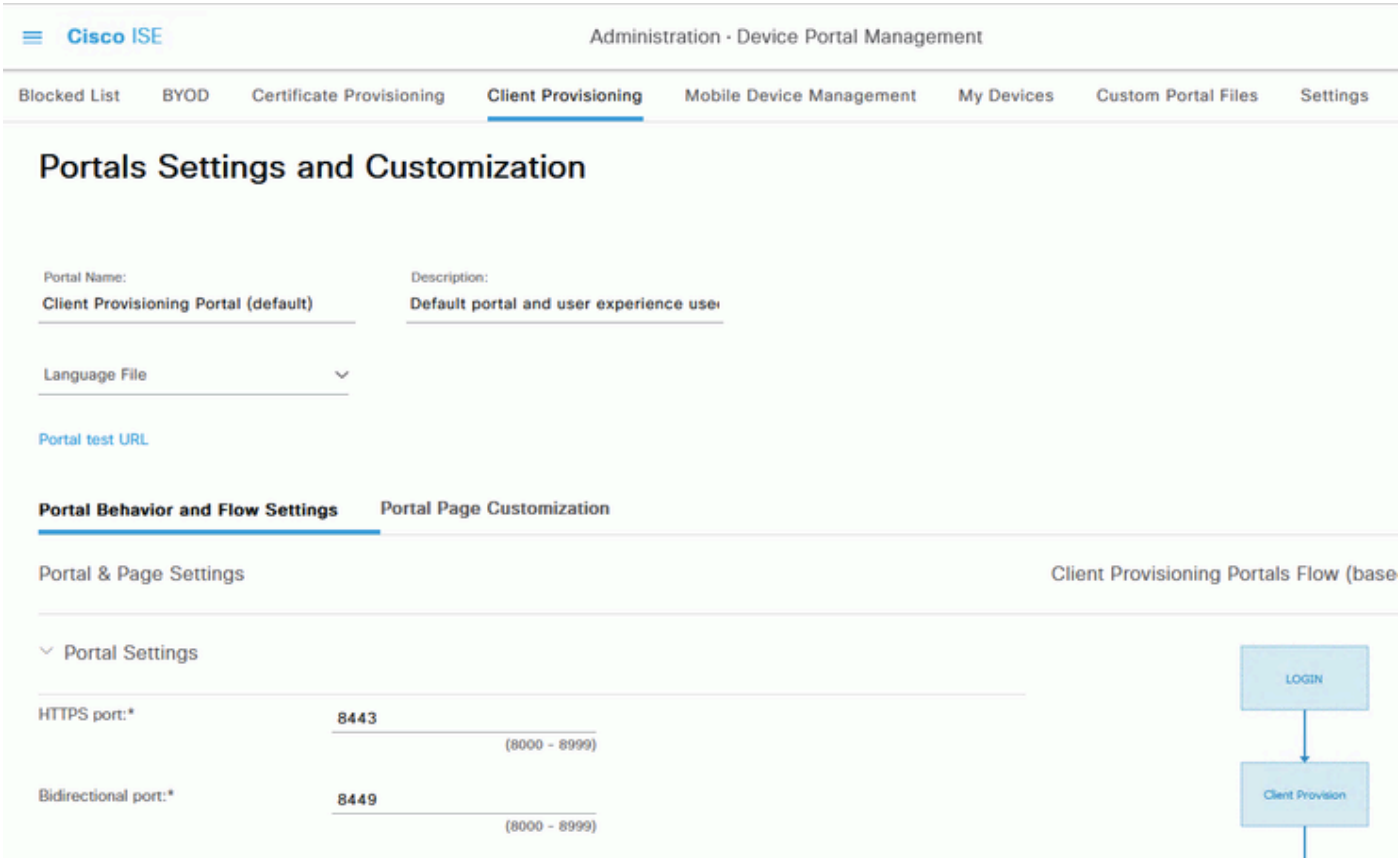
```
deny tcp any host PSN1-IP-ADDRESS eq 8449
deny tcp any host PSN2-IP-ADDRESS eq 8449
permit ip any any
```

allow ip any any non è obbligatorio, è possibile sostituirlo con qualsiasi set di regole in base alle proprie esigenze.



Nota: se non è configurata la voce deny in dACL, viene attivato l'allarme di rilevamento della configurazione della postura sul dashboard di Cisco ISE e la sincronizzazione dello stato della postura viene disabilitata sull'endpoint finché Cisco Secure Client non viene riavviato.

La porta di sincronizzazione dello stato della postura (porta bidirezionale) può essere modificata nella pagina di configurazione del portale di provisioning client. Passare a Amministrazione > Gestione portale dispositivi > Provisioning client > Selezionare il portale desiderato > Impostazioni comportamento portale e flusso e aprire Impostazioni portale. Impossibile modificare la porta di sincronizzazione stato postura per il portale di provisioning client predefinito.



Verifica

Da pacchetto DART

La sincronizzazione dello stato della postura può essere verificata dal lato client esaminando i log di Cisco Secure Client Posture Module (AnyConnect_ISEPosture.txt) dal bundle DART:

1. Valutazione della postura completata. Lo stato della postura è Conforme.

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

2. Il probe di sincronizzazione dello stato della postura è stato avviato.

```
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. È stata avviata la connessione HTTPS a ISE PSN sulla porta di sincronizzazione dello stato della postura (8449).

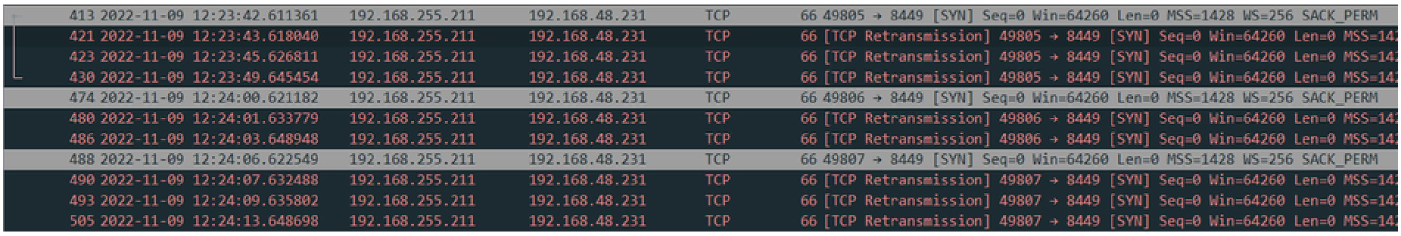
```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:22:47 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x296C Fi
```

4. Timeout per il probe di sincronizzazione dello stato della postura.

```
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
```

Da acquisizione pacchetti sul client

L'acquisizione dei pacchetti sul client mostra i pacchetti SYN inviati al nodo PSN ISE sulla porta di sincronizzazione dello stato della postura (8449) senza risposta SYN-ACK da PSN ISE:



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

ISE

Impossibile verificare la configurazione corretta della sincronizzazione dello stato della postura dal lato ISE perché la connessione sulla porta di sincronizzazione dello stato della postura (8449) dovrebbe avere esito negativo.

Riavvio della postura alla modifica dello stato della postura

1) ISE ha ricevuto informazioni sullo stato della sessione con stato postura "Sconosciuto" mentre Cisco Secure Client è in stato "Conforme".

```
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_http
```

2) Cisco Secure Client riconosce la modifica dello stato della postura e riavvia il rilevamento della postura:

```
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) Cisco Secure Client interrompe la sincronizzazione dello stato della postura finché non viene eseguita la valutazione della postura:

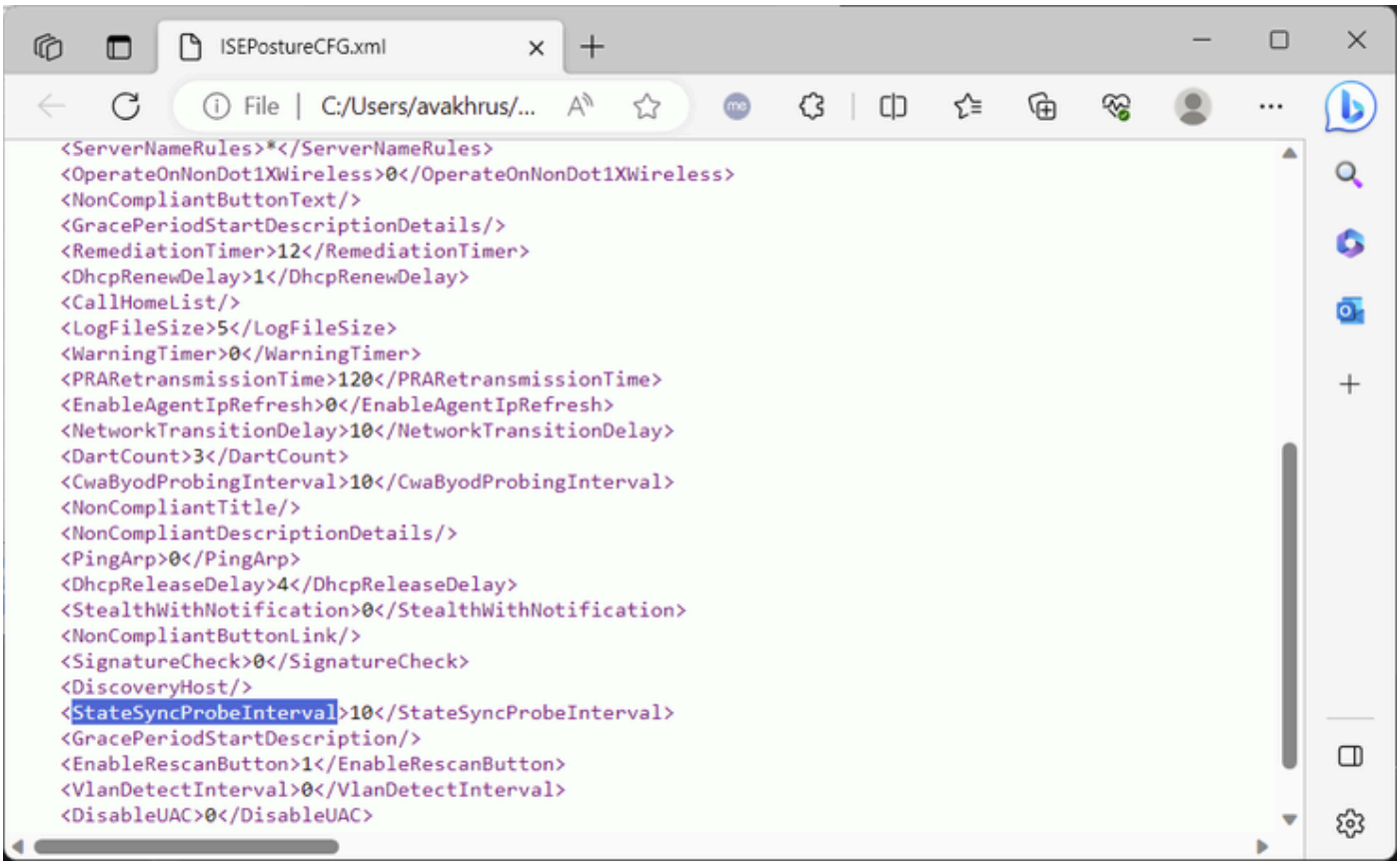
```
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::processMessage Thread Id: 0xC60
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery 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
```

Risoluzione dei problemi

Sincronizzazione stato postura non avviata

Se non viene indicato l'avvio di Sincronizzazione stato postura nel file di log AnyConnect_ISEPosture.txt e il client non tenta di stabilire una connessione con il nodo PSN ISE sulla porta di sincronizzazione stato postura (8449), controllare il file di configurazione postura ISEPostureCFG.xml dal bundle DART o direttamente sul computer client: "%ProgramData%\Cisco\Cisco Secure Client\ISE Posture\" per un PC Windows.

Il parametro responsabile per la sincronizzazione dello stato della postura è "StateSyncProbeInterval", che deve essere impostato con un valore superiore a 0:



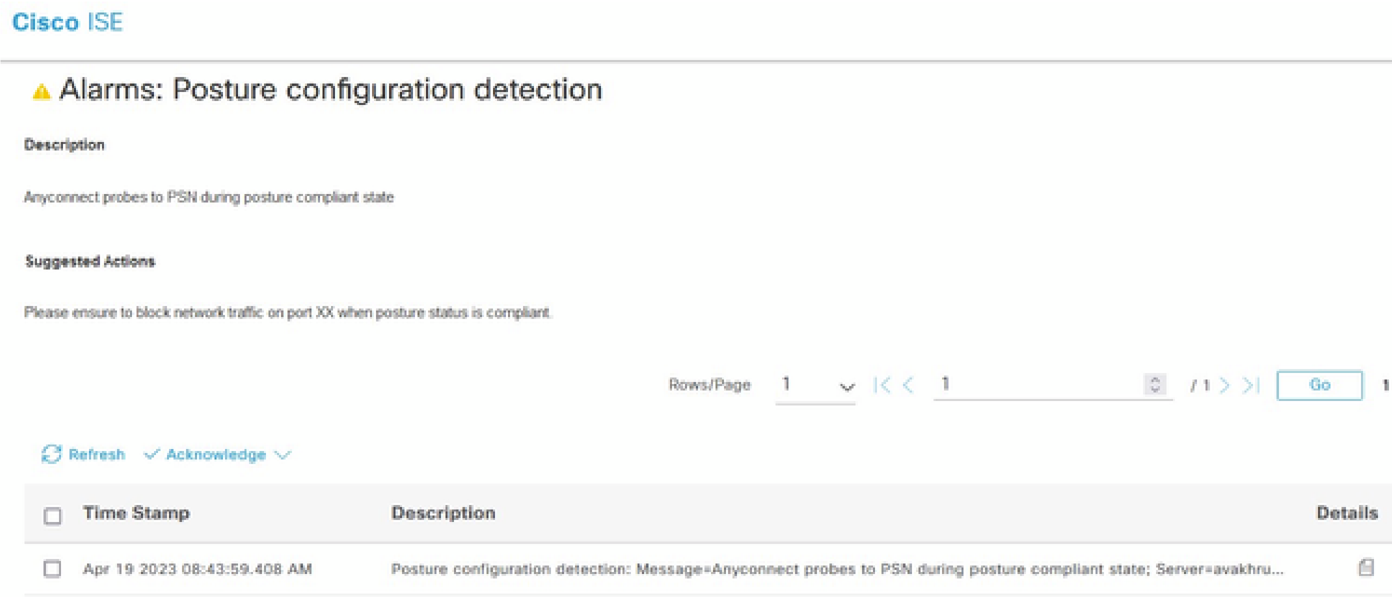
L'assenza di "StateSyncProbeInterval" o il valore "0" indica che la sincronizzazione dello stato della postura è disabilitata.

Se "Intervallo di sincronizzazione stato postura" è impostato in Profilo postura su ISE ma non è riflesso in un file di configurazione sul client, è necessario indagare sul provisioning postura.

Sincronizzazione dello stato della postura non riuscita con allarme sul dashboard ISE

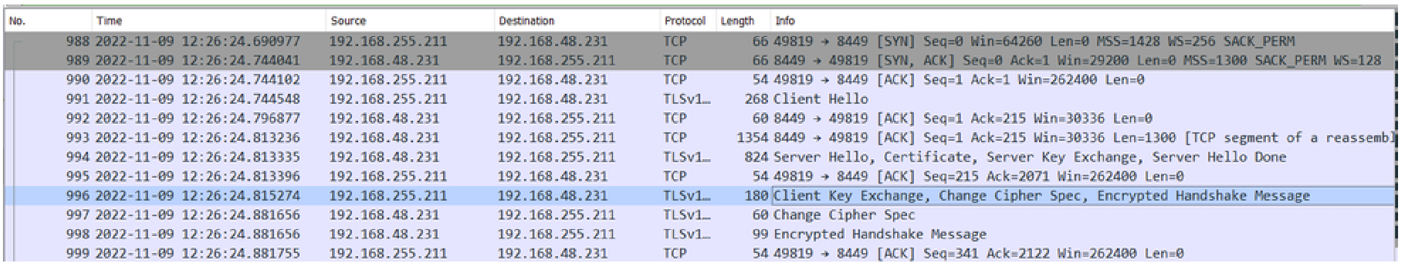
Se la sincronizzazione dello stato della postura non riesce con l'allarme su ISE, Cisco Secure Client è riuscito a raggiungere ISE sulla porta di sincronizzazione dello stato della postura (8449) e ha richiesto uno stato per la sessione con stato "Conforme".

- Allarme nell'interfaccia grafica di ISE:



- Convalida dall'acquisizione pacchetti

La connessione TCP sulla porta di sincronizzazione dello stato della postura (8449) è stabilita:



- Convalida dal log di Cisco Secure Client Posture Module

Controllare AnyConnect_ISEPosture.txt dal bundle DART:

1) Viene avviata la connessione HTTPS a ISE PSN sulla porta di sincronizzazione dello stato della postura (8449).

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

2) ISE ha inviato informazioni sullo stato della sessione con lo stato della postura "Conforme".

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

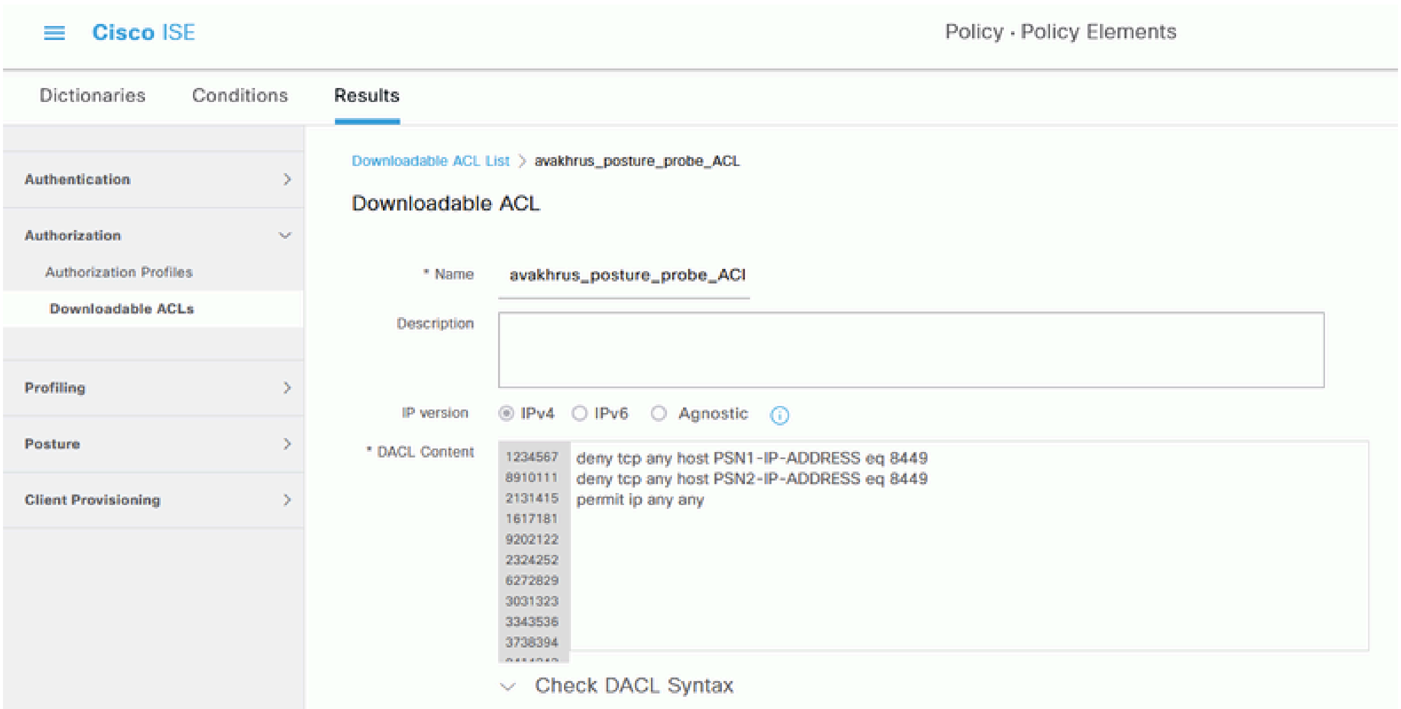
3) La sincronizzazione dello stato della postura si interrompe a causa del rilevamento di una configurazione errata:

```
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
```

Impossibile riavviare Sincronizzazione stato postura dall'interfaccia utente di Cisco Secure Client riavviando la valutazione della postura o una modifica di rete. Al contrario, è necessario riavviare Cisco Secure Client per consentire il riavvio della sincronizzazione dello stato della postura.

Verifica dACL configurato per il profilo di autorizzazione "Conforme" della postura

1. Verificare che il dACL corretto sia configurato per il profilo di autorizzazione "Conforme" della postura:



2. Convalida che l'ACL del report di autenticazione dettagliato è stato inviato correttamente come risultato dell'autenticazione dell'endpoint "conforme".

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. Verificare che dACL sia applicato correttamente su un dispositivo di accesso alla rete:

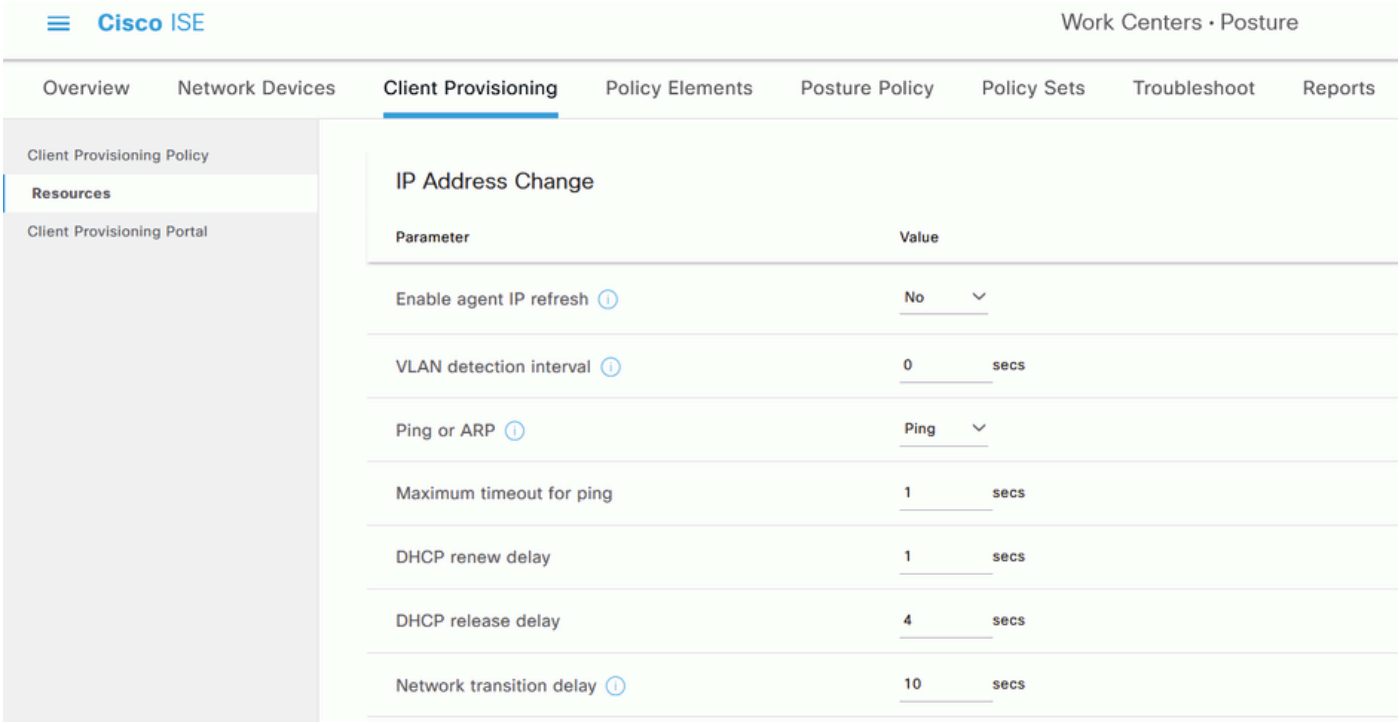
```
avakhrus_3560C#sh authe sess int fa0/12 det
            Interface:  FastEthernet0/12
          MAC Address:  0050.56a8.be02
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.255.193
            User-Name:  TRAINING\bob
               Status:  Authorized
               Domain:  DATA
       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
```

Problemi noti

Sincronizzazione stato postura non riuscita con allarme su ISE

La sincronizzazione dello stato della postura può non riuscire con un allarme su ISE anche se un corretto dACL viene applicato su un dispositivo di accesso alla rete all'endpoint del client. Questo si verifica se la sonda di sincronizzazione dello stato della postura viene eseguita più rapidamente di quanto sia stato applicato dACL o se la sonda di sincronizzazione dello stato della postura è già in corso quando dACL è applicato. Il problema è stato esaminato con l'ID bug Cisco CSCwd58316 . Per risolvere questo problema, è necessario impostare il "ritardo di transizione della rete" su 10 secondi nel profilo Anyconnect Posture (impostazioni del profilo ISE Posture Agent).



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).