Configurar e Solucionar Problemas de Sincronização de Estado de Postura

Contents

Introdução

Este documento descreve a configuração e o uso da sincronização de estado de postura introduzida na versão 3.1 do Cisco Identity Service Engine (ISE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Fluxo de postura no Cisco ISE
- Configuração de componentes de postura no Cisco ISE

Supõe-se que você tenha uma configuração Posture no lugar de qualquer tipo.

Para entender melhor os conceitos descritos mais adiante, é recomendável passar por:

- Guia do Administrador do Cisco Identity Services Engine, Versão 3.1
- Comparar versões anteriores do ISE com o fluxo de postura do ISE no ISE 2.2
- Postura e gerenciamento de sessões do ISE

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE versão 3.1
- Cisco Secure Client 5.0.00556

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

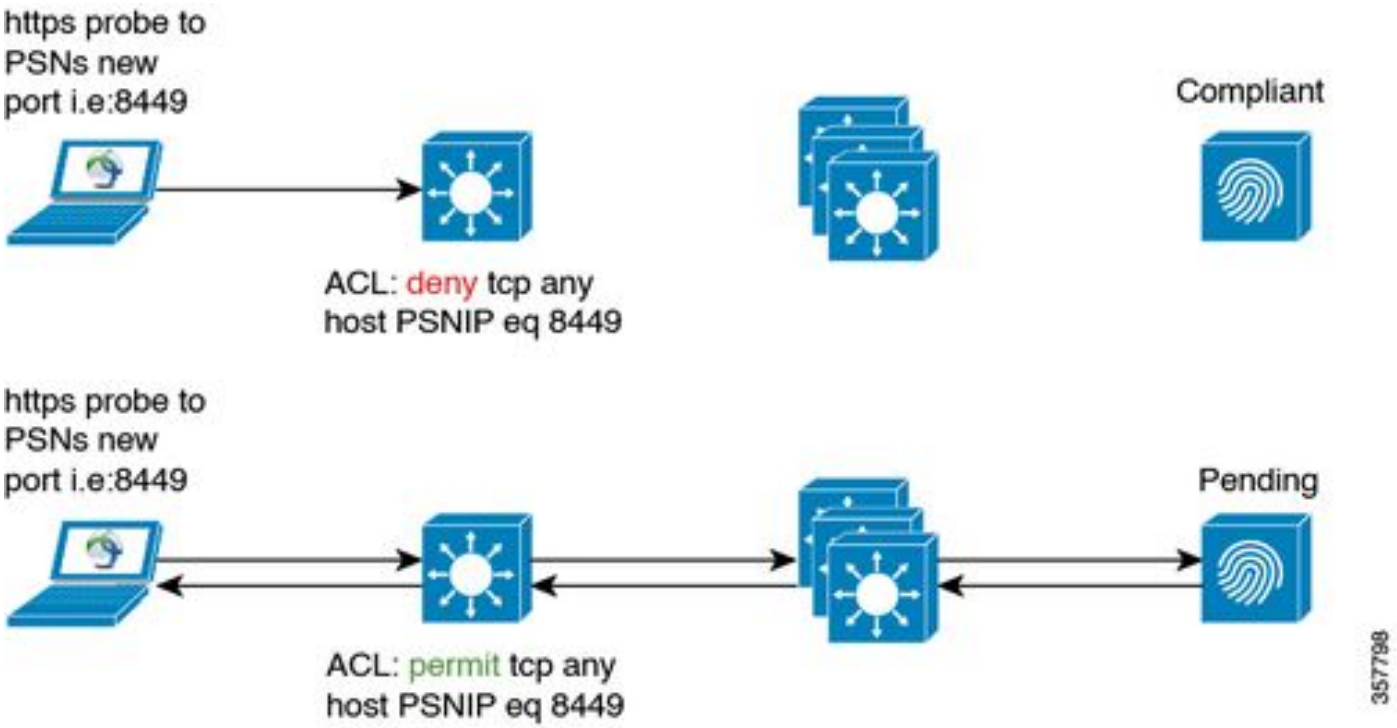
O fluxo de postura do ISE geralmente não permite que o status de postura seja atualizado no cliente a partir do ISE. O Cisco Secure Client Posture Module é usado para avaliar o status de postura do endpoint e o mantém até que a rede altere, reavalie periodicamente ou outros acionadores do lado do cliente. Se o status da postura do endpoint mudar no ISE devido ao encerramento de uma sessão ou por outros motivos, o Módulo de postura do cliente seguro pode não estar ciente dessa mudança, de modo que o endpoint permanece no estado Postura desconhecida com acesso limitado à rede até que um dos acionadores do lado do cliente aconteça.

Este documento se concentra em um novo recurso - a Sincronização de Status de Postura, que foi desenvolvida para tratar desse tipo de problema e permitir que o ISE forneça feedback ao Módulo de Postura de Cliente Seguro sobre o Status de Postura atual do endpoint.

Configurar

A porta de investigação de status de Postura foi introduzida em cada nó PSN do ISE quando a Sincronização de Estado de Postura está habilitada - TCP 8449 por padrão. Ele deve estar acessível do ponto final se o status da postura do ponto final for Desconhecido ou Pendente e inacessível se o status do ponto final for Compatível.

Diagrama de Rede



Configurações

A configuração do recurso Sincronização de Estado de Postura consiste em duas partes:

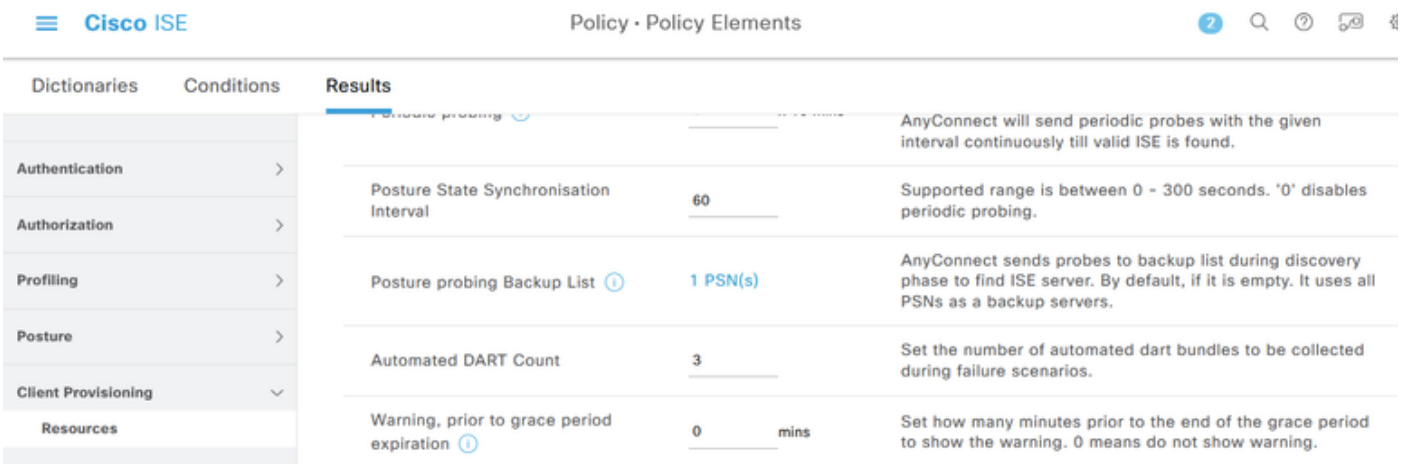
1. Configuração de perfil de postura do AnyConnect

   1.1 Na GUI do Cisco ISE, navegue para Policy > Policy Elements > Results > Client Provisioning > Resources.

   1.2 Selecione o Perfil de postura do AnyConnect que você já usa ou crie um novo.

   1.3 Na área Agent Behavior, configure o Posture State Synchronization Interval com qualquer valor entre 1 e 300 segundos, 0 - desabilita a Sincronização de Estado de Situação

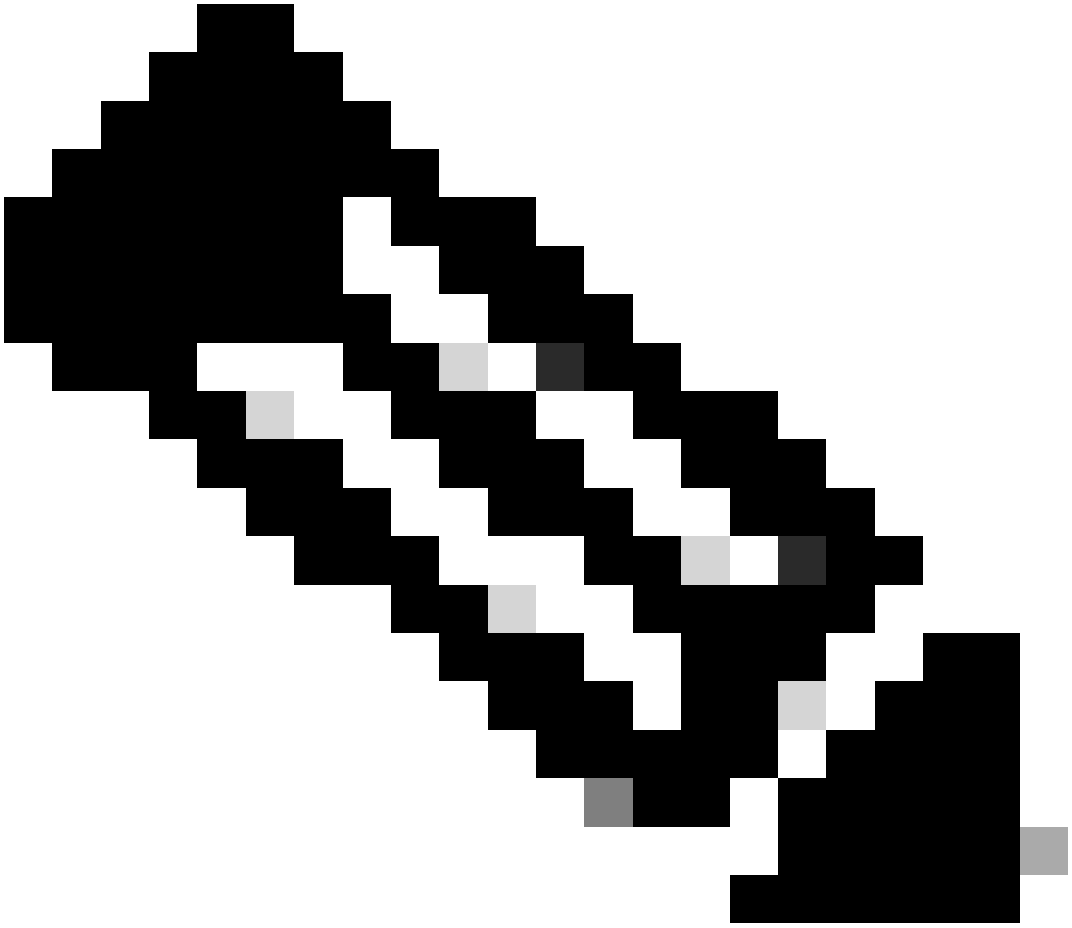
   1.4 Você pode configurar a Lista de backup de sondagem de postura - O Secure Client usa essa lista para verificar o estado de postura em PSNs selecionadas. Se você não escolher nenhuma PSN, a PSN conectada e dois servidores de backup serão usados como backups para sincronização de estado de postura.



2. Configuração de uma ACL(dACL) para download para bloquear o acesso à porta de sincronização de estado de postura no Cisco ISE quando o status da postura do cliente for Compatível ou Não Compatível. Você precisa adicionar a entrada de negação de controle de acesso com a porta de Sincronização de Estado de Postura para cada PSN na parte superior das ACLs usadas para pontos de extremidade Compatíveis para restringir o acesso à porta de Sincronização de Estado de Postura se o status do ponto de extremidade for conhecido, por exemplo:

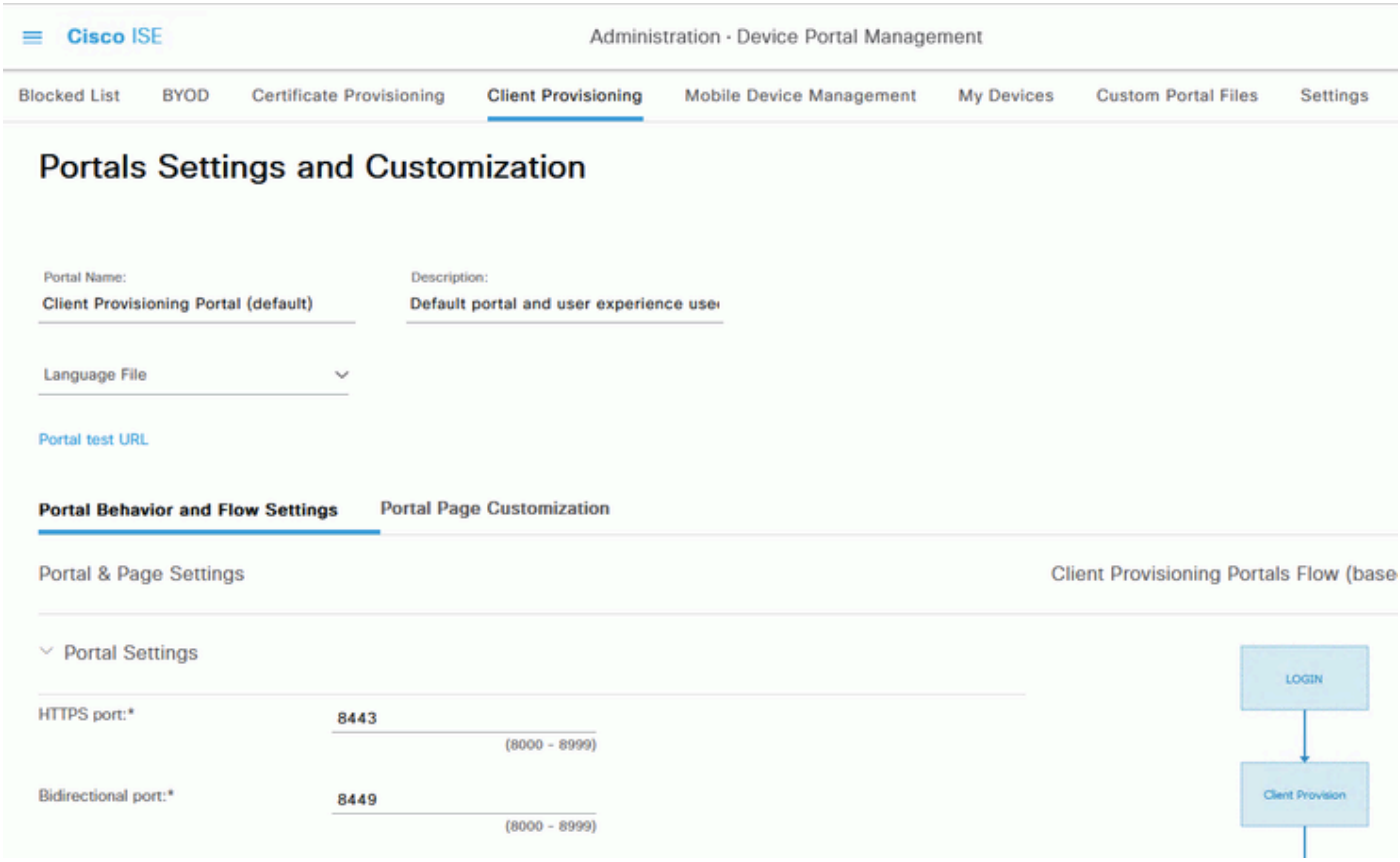
```
deny tcp any host PSN1-IP-ADDRESS eq 8449
deny tcp any host PSN2-IP-ADDRESS eq 8449
permit ip any any
```

permit ip any any não é obrigatório, você pode substituí-lo por qualquer conjunto de regras de acordo com suas necessidades.



Observação: se a entrada deny no dACL não estiver configurada, o alarme Posture Configuration Detection será acionado no painel do Cisco ISE e a Sincronização de estado Posture será desativada no endpoint até que o Cisco Secure Client seja reiniciado.

A porta de sincronização de estado de postura (porta bidirecional) pode ser alterada na página de configuração do Portal de provisionamento do cliente. Navegue até Administração > Gerenciamento do portal de dispositivos > Provisionamento do cliente > Selecione o portal desejado > Configurações de comportamento e fluxo do portal e abra Configurações do portal. A porta de Sincronização de Estado de Situação do Portal de Provisionamento de Cliente padrão não pode ser alterada.



Verificar

Do pacote DART

A Sincronização de status de postura pode ser verificada no lado do cliente, examinando os logs do Cisco Secure Client Posture Module (AnyConnect_ISEPosture.txt) do pacote DART:

1. A avaliação da postura foi concluída, o status da postura é Compatível.

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

2. Sondagem de Sincronização de Status da Postura iniciada.

```
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. A conexão HTTPS com o ISE PSN na porta de Sincronização de Estado de Postura (8449) é iniciada.

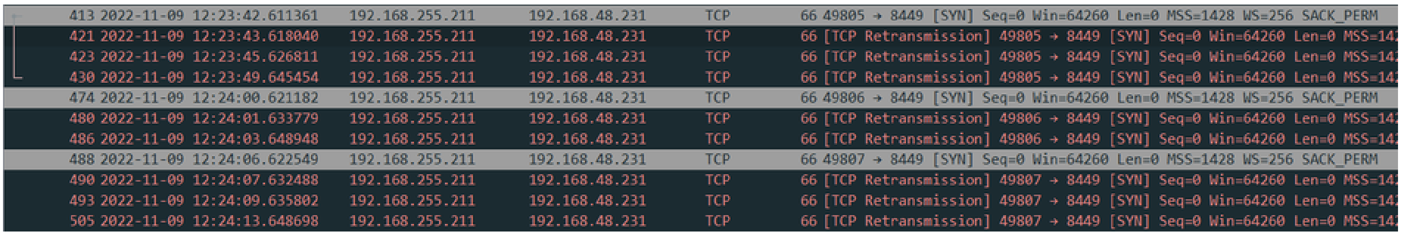
```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:22:47 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x296C Fi
```

4. Tempo limite para sondagem de Sincronização de Status de 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
```

A partir da captura de pacotes no cliente

A captura de pacote realizada no cliente mostra pacotes SYN enviados para o nó PSN do ISE na porta de sincronização de estado de postura (8449) sem resposta SYN-ACK do PSN do 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

Do ISE

A configuração de Sincronização de Status de Situação Correta não pode ser verificada do lado do ISE, pois a conexão na porta de Sincronização de Estado de Situação (8449) deve falhar.

Postura Reiniciar ao Alterar Status da Postura

1) As informações de estado da sessão foram recebidas do ISE com Status de postura "Desconhecido" enquanto o Cisco Secure Client está em um estado "Compatível".

```
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) O Cisco Secure Client confirma a alteração do status da postura e reinicia a descoberta de 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) O Cisco Secure Client interrompe a Sincronização do Status da Situação até que a avaliação da Situação seja realizada:

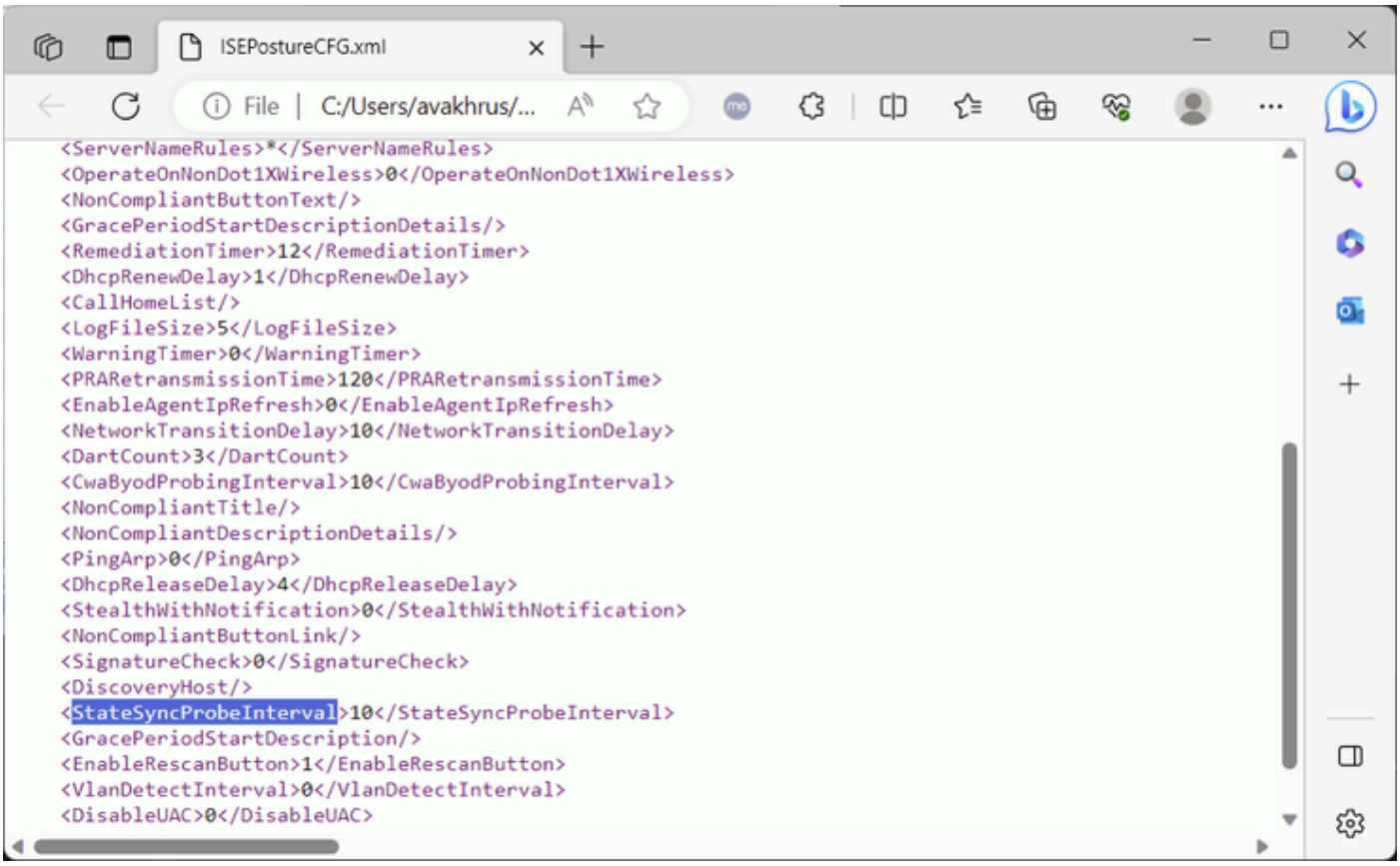
```
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::processMessage Thread Id: 0xC60
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery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

Troubleshooting

A Sincronização de Status da Postura não é Iniciada

Se não houver indicação de que a sincronização de status de postura começa no arquivo de log AnyConnect_ISEPosture.txt e o cliente não tentar estabelecer uma conexão com o nó ISE PSN na porta de sincronização de estado de postura (8449), verifique o arquivo de configuração de postura ISEPostureCFG.xml do pacote DART ou diretamente na máquina do cliente: "%ProgramData%\Cisco\Cisco Secure Client\ISE Posture\" para um PC com Windows.

O parâmetro responsável pela Sincronização de Status de Postura é "StateSyncProbeInterval", ele deve ser definido com um valor superior a 0:



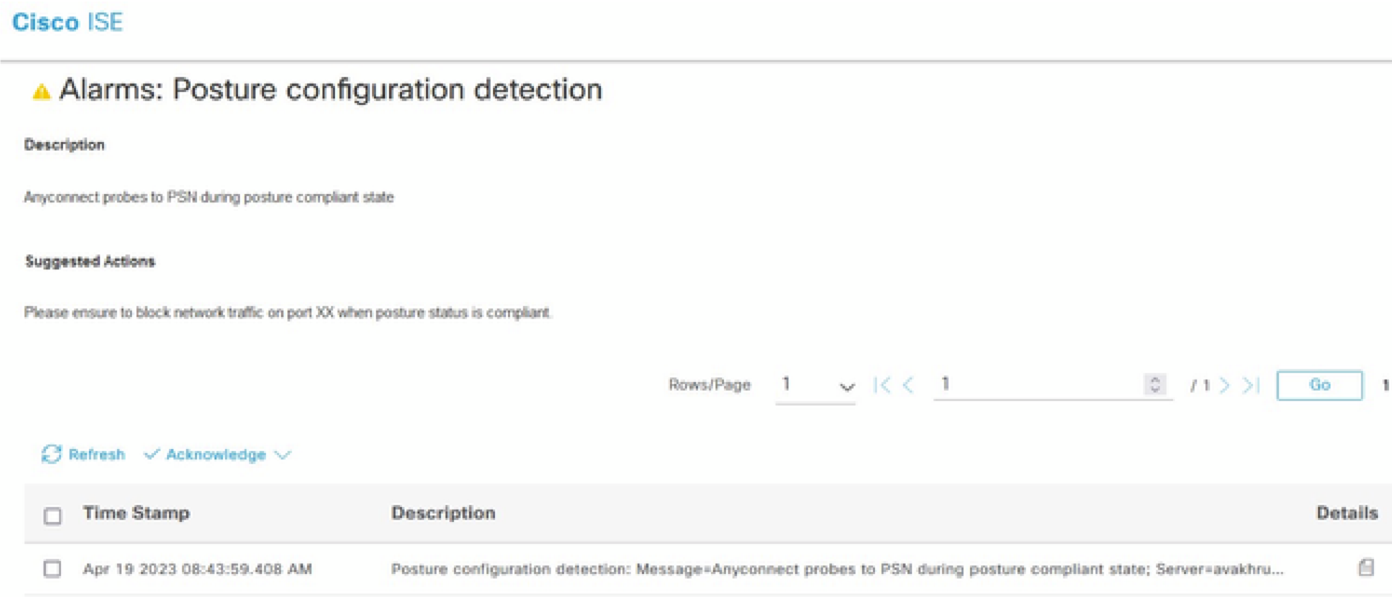
A ausência de "StateSyncProbeInterval" ou um valor de "0" significa que a Sincronização de Status da Postura está desabilitada.

Se "Intervalo de sincronização de estado de postura" estiver definido no perfil de postura no ISE, mas não estiver refletido em um arquivo de configuração no cliente, o provisionamento de postura precisará ser investigado.

A sincronização do status da postura falha com o alarme no painel do ISE

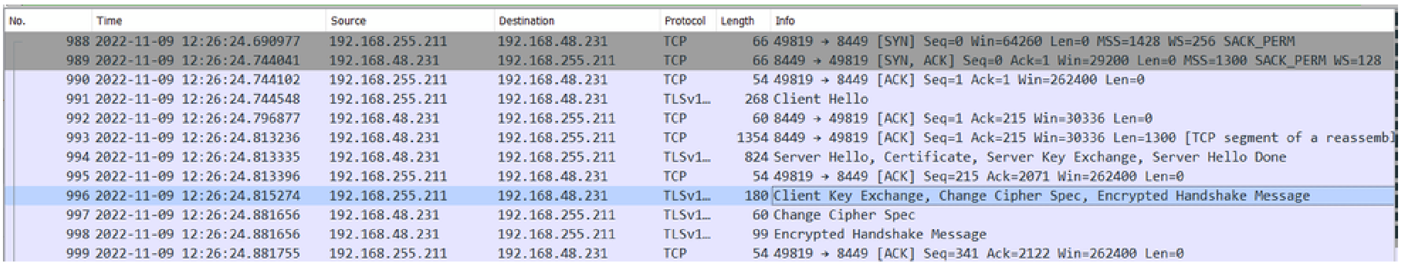
Se a Sincronização de estado de postura falhar com o alarme no ISE, isso significa que o Cisco Secure Client conseguiu acessar o ISE na porta de Sincronização de estado de postura (8449) e solicitou um status para a sessão com o status "Compatível".

- Alarme na GUI do ISE:



- Validar a partir da captura de pacotes

A conexão TCP na porta de Sincronização de Estado de Postura (8449) foi estabelecida:



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

- Validar a partir do log do Cisco Secure Client Posture Module

Verifique o AnyConnect_ISEPosture.txt do pacote DART:

1) A conexão HTTPS com o ISE PSN na porta de sincronização de estado de postura (8449) é iniciada.

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

2) As informações de estado da sessão foram recebidas do ISE com o status de postura "Compatível".

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

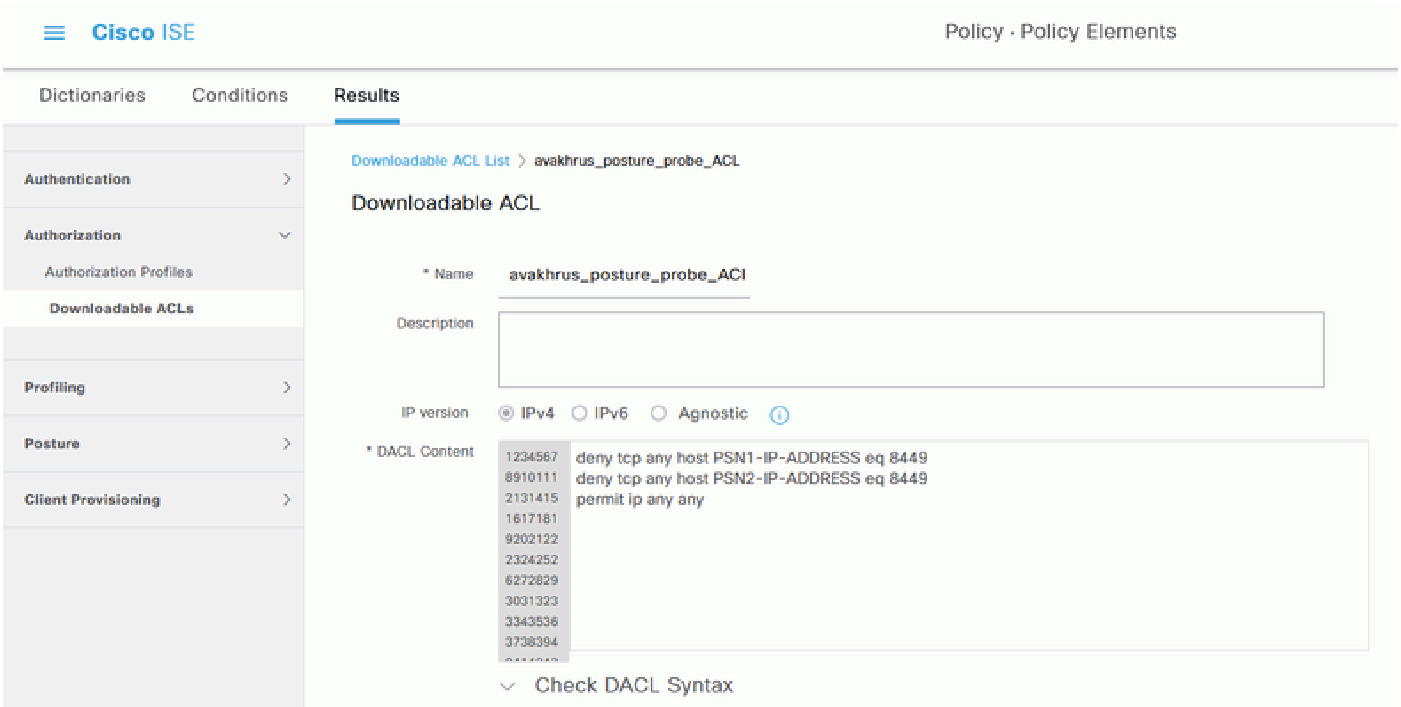
3) A Sincronização de Estado de Postura é interrompida devido à detecção de uma configuração incorreta:

```
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
```

A sincronização de estado de postura não pode ser reiniciada na GUI do Cisco Secure Client reiniciando a avaliação de postura ou uma alteração na rede. Em vez disso, o Cisco Secure Client precisa ser reiniciado para que a Sincronização de Estado de Postura funcione novamente.

Verificar o dACL configurado para o perfil de autorização "Compatível" com a postura

1. Valide se o dACL apropriado está configurado para o perfil de autorização "Compatível" com Postura:



2. Validar relatório de autenticação detalhado dACL enviado corretamente como resultado da autenticação do ponto final "Compatível".

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. Valide se o dACL está corretamente aplicado em um dispositivo de acesso à rede:

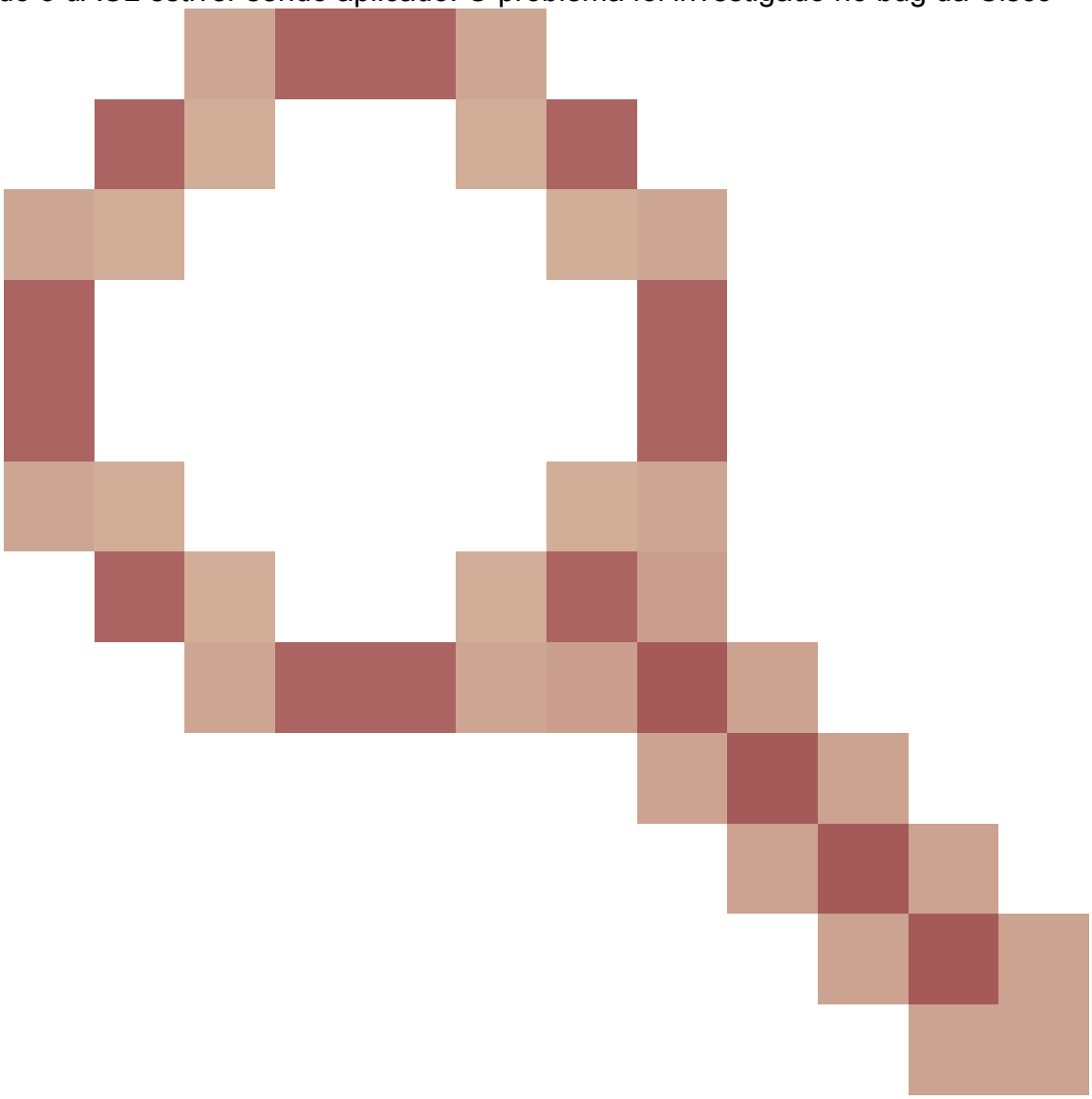
```
avakhrus_3560C#sh authe sess int fa0/12 det
            Interface:  FastEthernet0/12
          MAC Address:  0050.56a8.be02
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.255.193
            User-Name:  TRAINING\bob
               Status:  Authorized
               Domain:  DATA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

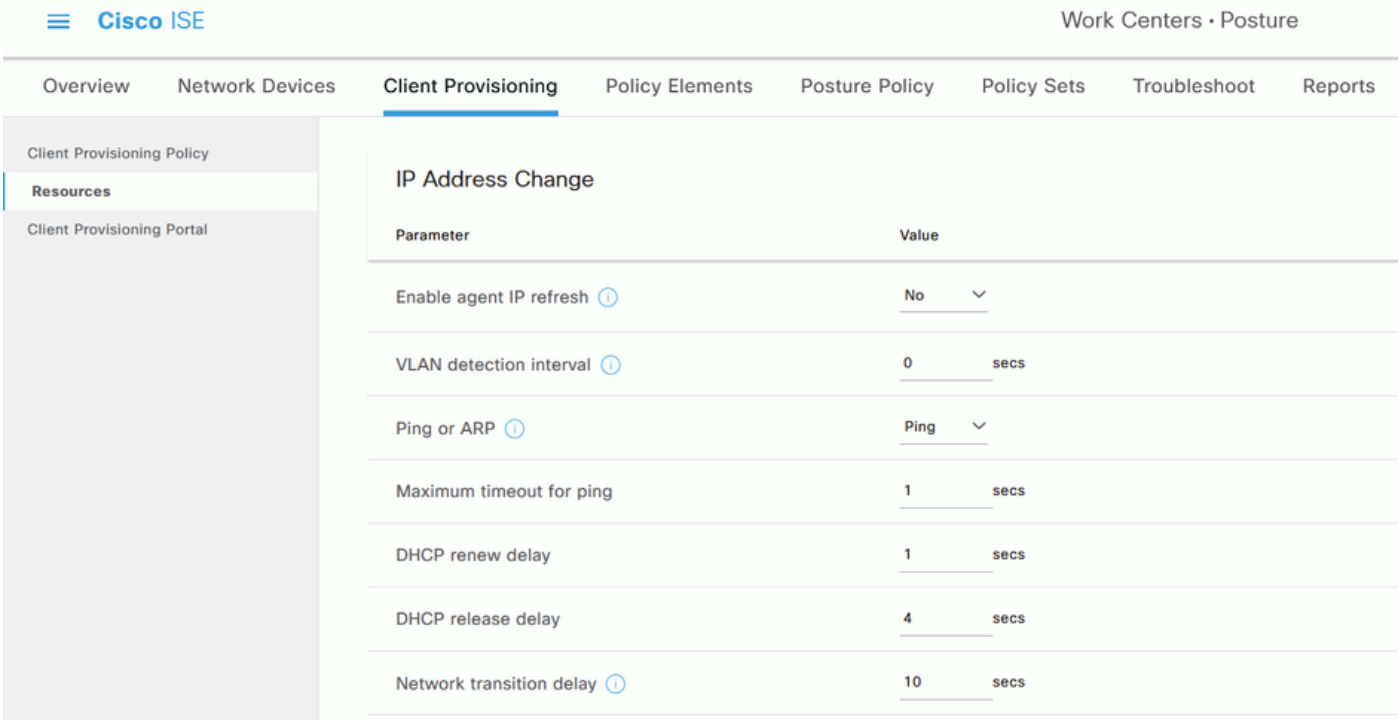
Problemas conhecidos

A sincronização de estado de postura falha com alarme no ISE

A sincronização de estado de postura pode falhar com alarme no ISE, mesmo se o dACL apropriado for aplicado em um dispositivo de acesso à rede para o endpoint do cliente. Isso acontece se a Sonda de sincronização de estado de postura for executada mais rapidamente do que o dACL for aplicado ou se a Sonda de sincronização de estado de postura já estiver em andamento quando o dACL estiver sendo aplicado. O problema foi investigado no bug da Cisco



ID CSCwd58316
. Como solução alternativa, você precisa definir o "atraso de transição da rede" como 10 segundos no perfil de postura do Anyconnect (Configurações de perfil do agente de postura do ISE).


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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.