تكوين مزامنة حالة الوضع واستكشاف أخطائها وإصلاحها

المحتويات

المقدمة

يصف هذا المستند تكوين مزامنة حالة الوضع واستخدامها الذي تم تقديمه في إصدار Cisco Identity Service Engine(ISE) 3.1.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تدفق Posture على Cisco ISE
- تكوين مكونات الوضع على Cisco ISE

من المفترض أن يكون لديك تكوين Posture (وضعية) بدلا من أي نوع.

ولفهم المفاهيم الموصوفة لاحقا على نحو أفضل، يوصى بالمرور بما يلي:

- دليل مسؤول محرك خدمات الهوية من Cisco، الإصدار 3.1
- مقارنة إصدارات ISE السابقة بتدفق وضعية ISE في ISE 2.2
- إدارة جلسة ISE ووضعها

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ISE الإصدار 3.1 من Cisco
- Cisco Secure Client 5.0.00556

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

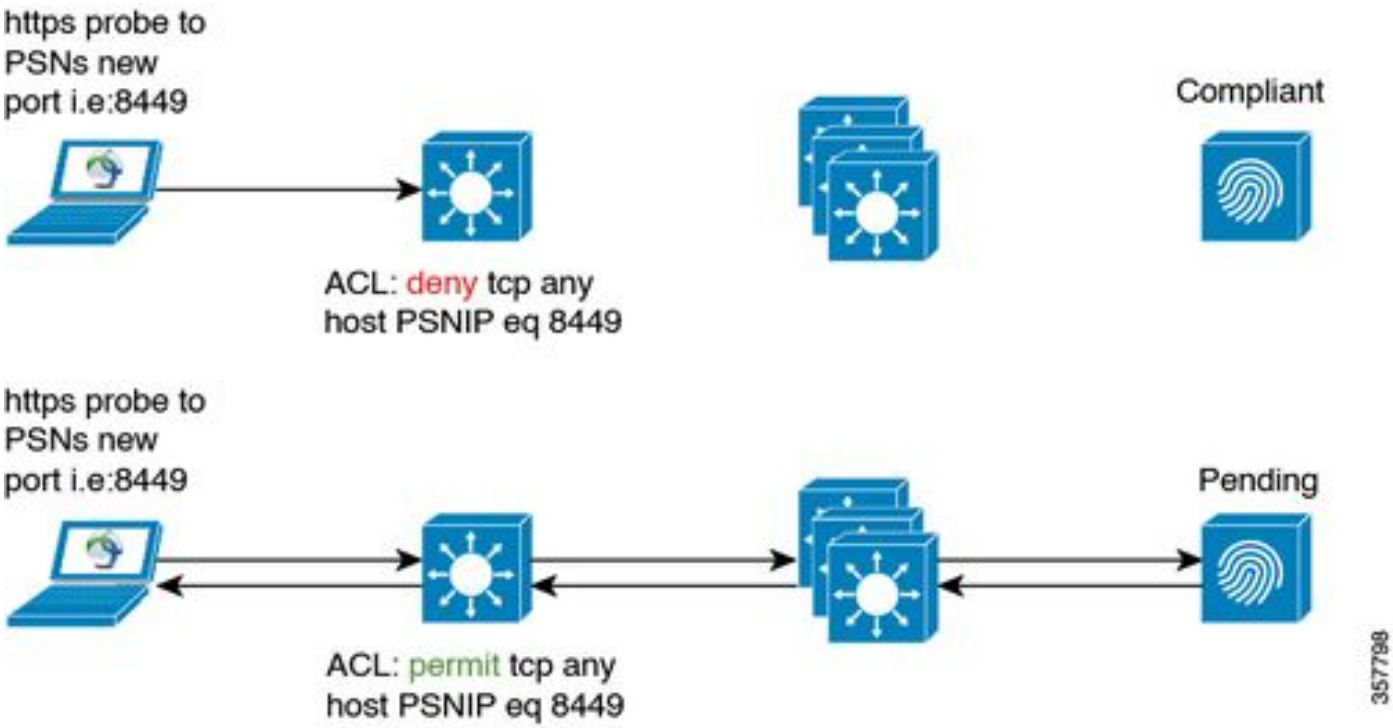
يسمح تدفق ISE Posture (وضعية محرك خدمات الهوية (ISE)) لعادة بتحديث حالة Posture على العميل من ISE. يتم إستخدام الوحدة النمطية Cisco Secure Client Posture (وضعية العميل) لتقييم حالة نقطة النهاية وإبقائها حتى تغيير الشبكة أو إعادة التقييم الدورية أو المشغلات من جانب العميل الأخرى. إذا تم تغيير حالة حالة نقطة النهاية على ISE بسبب إنهاء جلسة عمل أو أسباب أخرى، فقد تكون الوحدة النمطية "وضع العميل الآمن" غير مدركة لهذا التغيير، لذلك ظلت نقطة النهاية في حالة Posture Unknown مع وصول محدود إلى الشبكة حتى يحدث أحد مشغلات جانب العميل.

يركز هذا المستند على ميزة جديدة - مزامنة حالة الوضع، التي تم تطويرها لمعالجة هذا النوع من المشاكل والسماح لـ ISE بتوفير ملاحظات إلى الوحدة النمطية "وضع العميل الآمن" على حالة الوضع الحالية لنقطة النهاية.

التكوين

تم إدخال منفذ تحقيق حالة Posture على كل عقدة ISE PSN عند تمكين مزامنة حالة الوضع - TCP 8449 بشكل افتراضي. من المفترض أن يكون من الممكن الوصول إليه من نقطة النهاية إذا كانت حالة "وضع النقطة الطرفية" غير معروفة أو معلقة ولا يمكن الوصول إليها إذا كانت حالة نقطة النهاية متوافقة.

الرسم التخطيطي للشبكة



التكوينات

يتكون تكوين ميزة مزامنة حالة الوضع من جزئين:

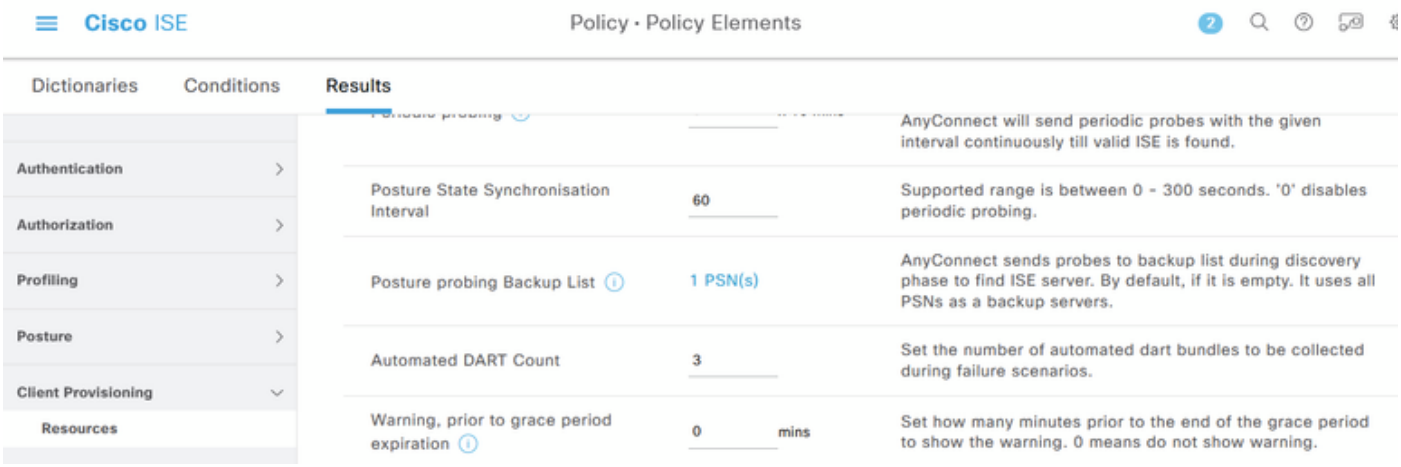
1. تكوين ملف تعريف AnyConnect Posture

1.1 في واجهة المستخدم الرسومية Cisco ISE، انتقل إلى السياسة > عناصر السياسة > النتائج > إمداد العميل > الموارد.

1.2 حدد ملف تعريف AnyConnect Posture الذي تستخدمه بالفعل أو قم بإنشاء ملف تعريف جديد.

1.3 في منطقة "سلوك الوكيل"، قم بتكوين الفاصل الزمني لمزامنة حالة الوضع إلى أي قيمة تتراوح بين 1 و 300 ثانية، 0 - تعطيل مزامنة حالة الوضع

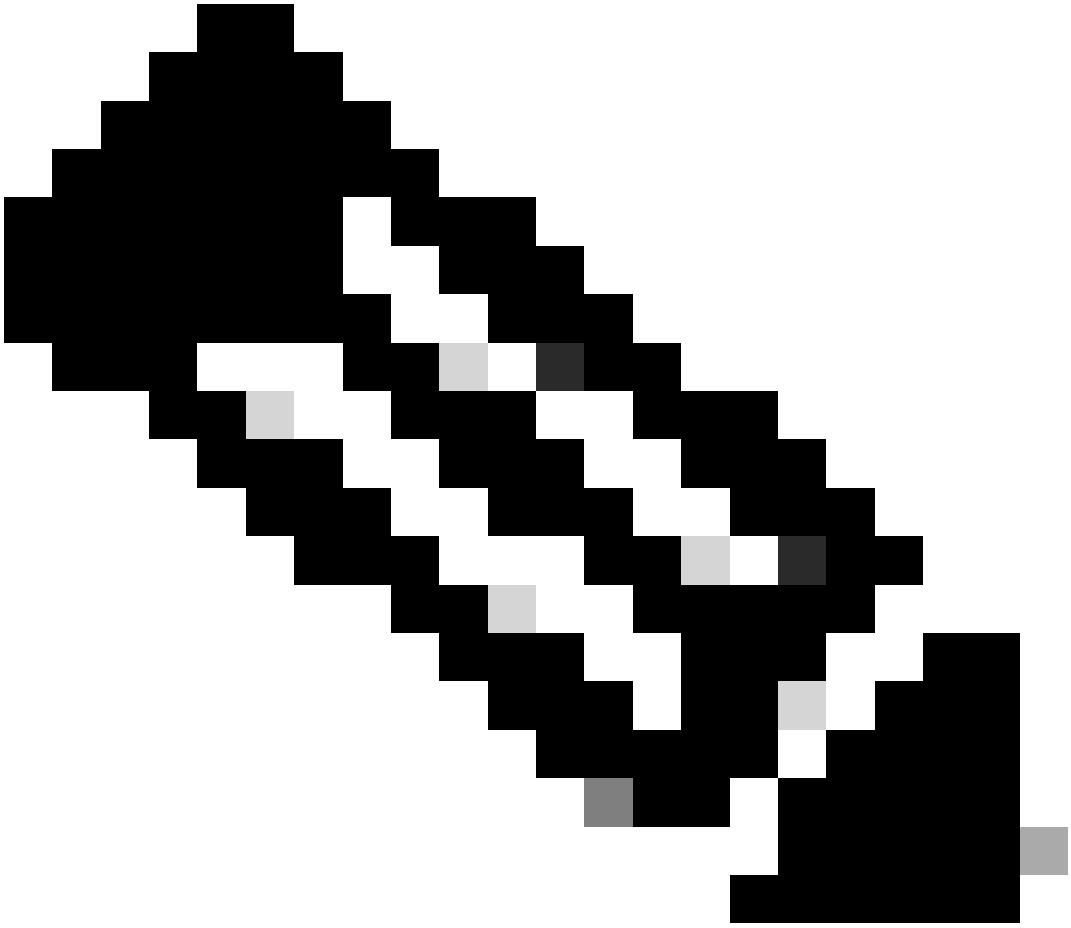
1.4 يمكنك تكوين قائمة النسخ الاحتياطي لاختبار الوضع - يستخدم العميل الآمن هذه القائمة للتحقق من حالة الوضع على شبكات PSN المحددة. إذا لم تقم باختيار أي PSN، فسيتم استخدام PSN المتصل وأي خادمين للنسخ الاحتياطي كنسخ إحتياطية لمزامنة حالة الوضع.



2. تكوين قائمة تحكم في الوصول (dACL) قابلة للتنزيل لحظر الوصول إلى منفذ مزامنة حالة الوضع على Cisco ISE عندما تكون حالة وضع العميل متوافقة وأ غير متوافقة. تحتاج إلى إضافة إدخال رفض التحكم بالوصول باستخدام منفذ مزامنة حالة الوضع لكل PSN في أعلى قوائم التحكم في الوصول المستخدمة لنقاط النهاية المتوافقة لتقييد الوصول إلى منفذ مزامنة حالة الوضع إذا كانت حالة نقطة النهاية معروفة، على سبيل المثال:

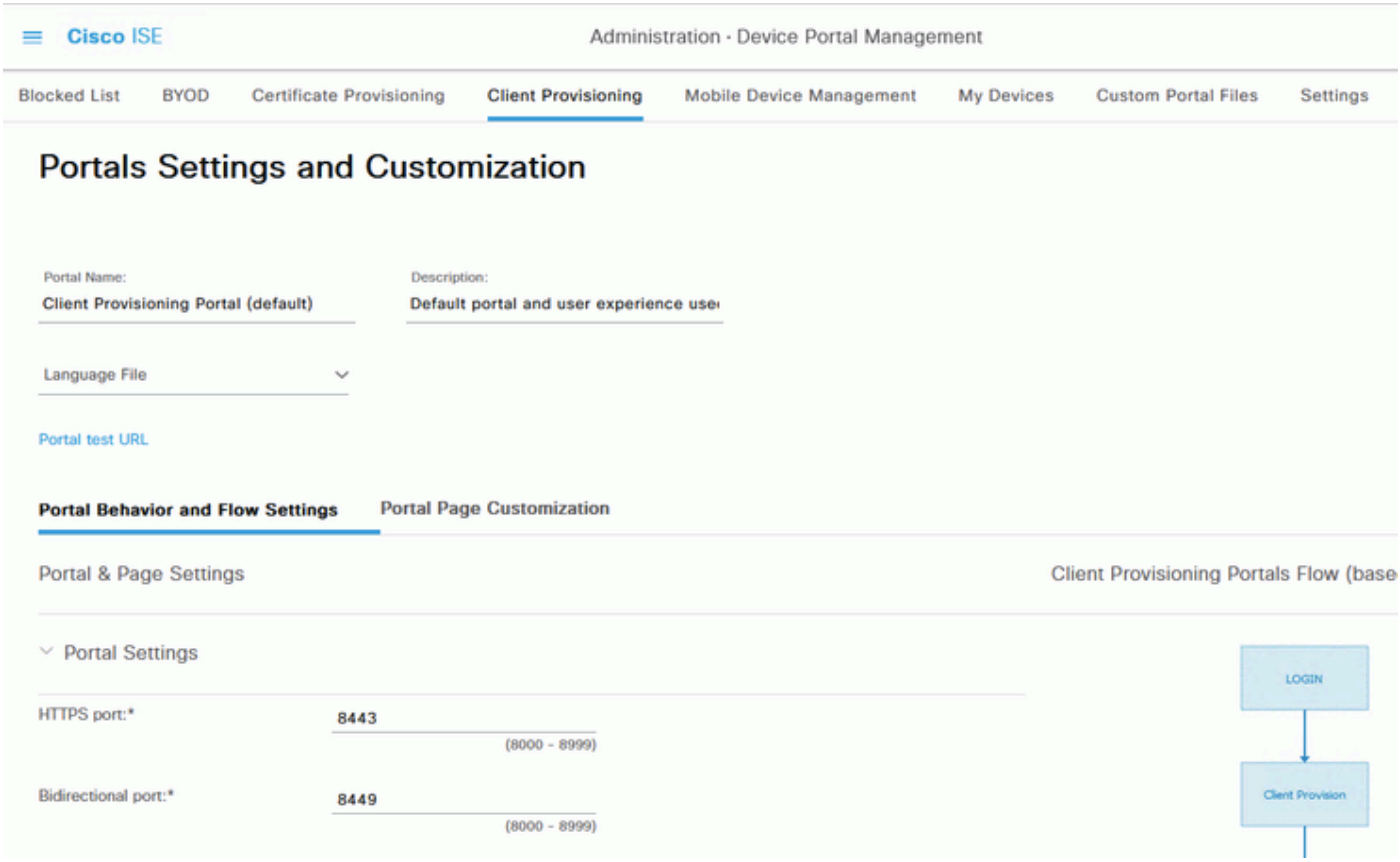
```
deny tcp any host PSN1-IP-ADDRESS eq 8449
deny tcp any host PSN2-IP-ADDRESS eq 8449
permit ip any any
```

ال يكون السماح ب ip أي أمرا إلزاميا، يمكنك إستبداله بأي مجموعة من القواعد وفقا لاحتياجاتك.



ملاحظة: في حالة عدم تكوين إدخال الرفض في قائمة التحكم في الوصول إلى البنية الأساسية (dACL)، يتم تشغيل تنبيه اكتشاف تكوين الوضع على لوحة معلومات Cisco ISE ويتم تعطيل مزامنة حالة الوضع على نقطة النهاية حتى يتم إعادة بدء تشغيل عميل Cisco الآمن.

يمكن تغيير منفذ مزامنة حالة الوضع (منفذ ثنائي الإتجاه) في صفحة تكوين مدخل إمداد العميل. انتقل إلى إدارة > إدارة مدخل الأجهزة > إمداد العميل > تحديد المدخل المطلوب > سلوك المدخل وإعدادات التدفق وإعدادات المدخل المفتوح. لا يمكن تغيير منفذ مزامنة حالة الوضع لبوابة إمداد العميل الافتراضية.



التحقق من الصحة

من DART Bundle

يمكن التحقق من مزامنة حالة الوضع من جانب العميل من خلال النظر في سجلات وحدة وضع العميل الآمنة من Cisco (AnyConnect_ISEPosture.txt) من حزمة DART:

1. انتهى تقييم الوضع، وكانت حالة الوضع متوافقة.

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

2. تم بدء التحقق من مزامنة حالة الوضع.

```
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. يتم بدء اتصال HTTPS بـ ISE PSN على منفذ مزامنة حالة الوضع (8449).

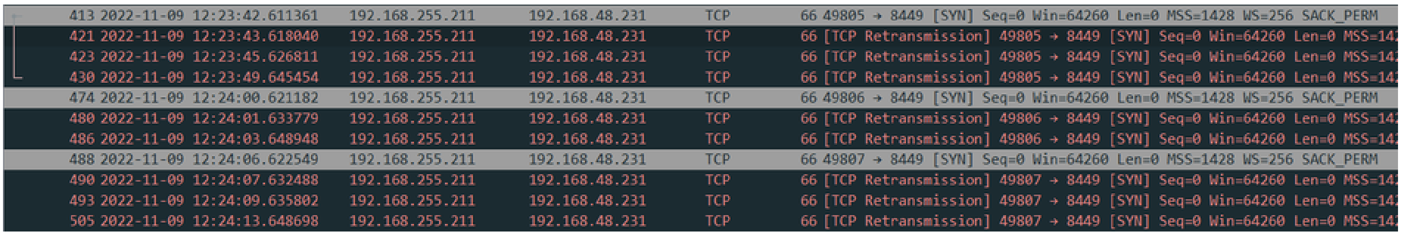
```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:22:47 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x296C Fi
```

4. مهلة تدقيق مزامنة حالة الوضع.

```
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
```

من التقاط الحزمة على العميل

يظهر التقاط الحزم المأخوذ على العميل حزم SYN المرسلة نحو عقدة ISE PSN على منفذ مزامنة حالة الوضع (8449) بدون إستجابة SYN-ACK من ISE PSN:



من ISE

لا يمكن التحقق من صحة تكوين مزامنة حالة الوضع من جانب ISE حيث من المفترض أن يفشل الاتصال بمنفذ مزامنة حالة الوضع (8449).

إعادة تشغيل الوضع عند تغيير حالة الوضع

1) تم تلقي معلومات حالة جلسة العمل من ISE مع وضع "غير معروف" بينما يكون Cisco Secure Client في حالة "متوافق".

```
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) فرعتي Cisco Secure Client على تغيير حالة الوضع ويعيد تشغيل اكتشاف الوضع:

```
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) فقوت Cisco Secure Client مزامنة حالة الوضع حتى يتم إجراء تقييم الوضع:

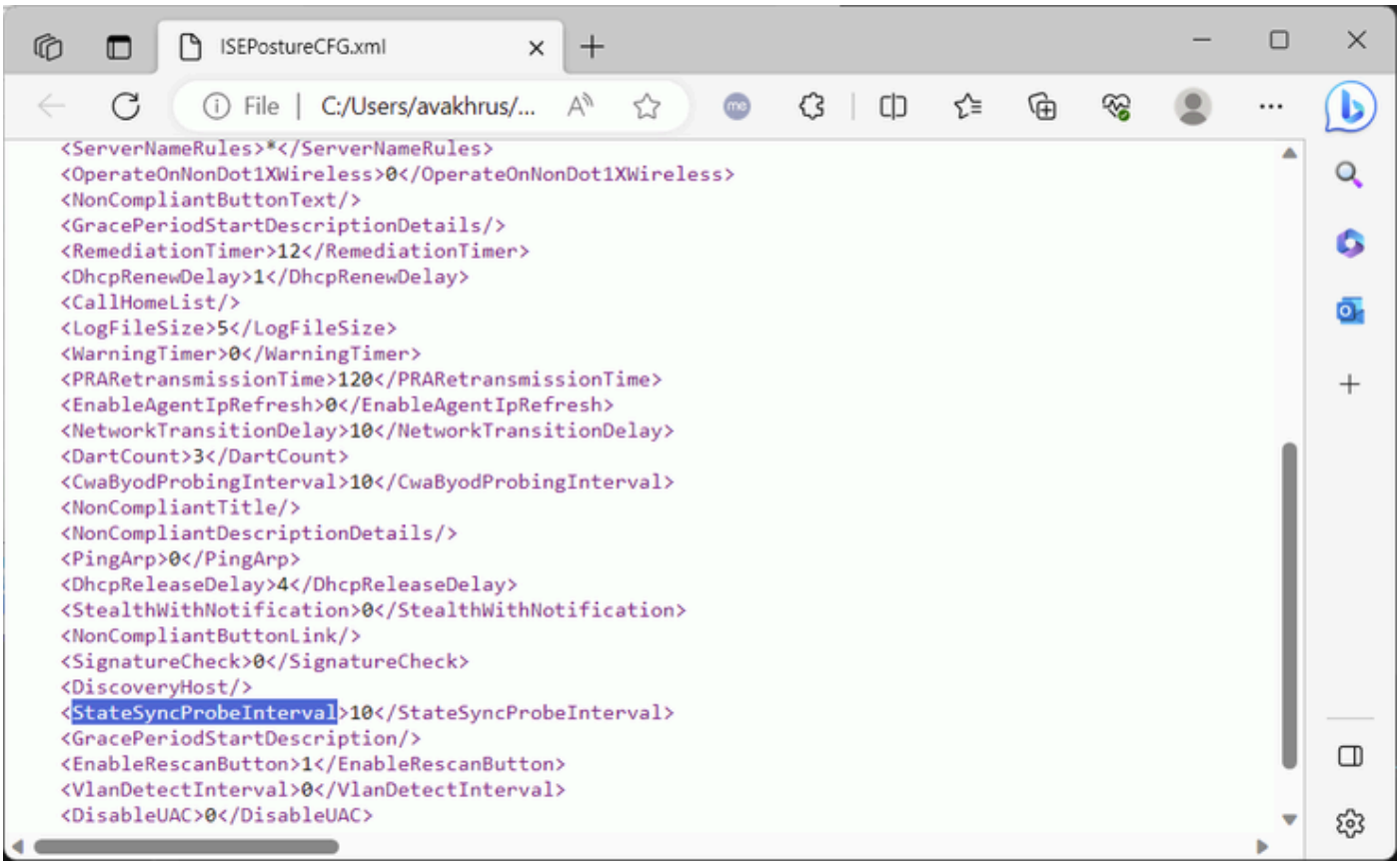
```
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::processMessage Thread Id: 0xC60
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery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

استكشاف الأخطاء وإصلاحها

لا يتم بدء مزامنة حالة الوضع

لجسلا فلم يف عضولا ةلاح ةنمازم ءدب ىلإ ةراشإ دوجو مدع ةلاح يف AnyConnect_ISEPosture.txt الو لواحي ليمعلا إنشاء اتصال مع عقدة ISE PSN يف ذفنم DART ةمزح نم ISEPostureCFG.xml عضولا نيوكت فلم نم ققحت ،(8449) عضولا ةلاح ةنمازم ليمعلا: "%ProgramData%\Cisco\Cisco Secure Client\ISE Posture\" زاهج ىلع زاهج ةرشابم وأ رتويبمك Windows.

ةملعملا ةلوؤسملا نع مزامنة حالة الوضع يه StateSyncProbeInterval"، نمو ضرتفملا نم ىلعأ ةميقب اهنييعت 0:



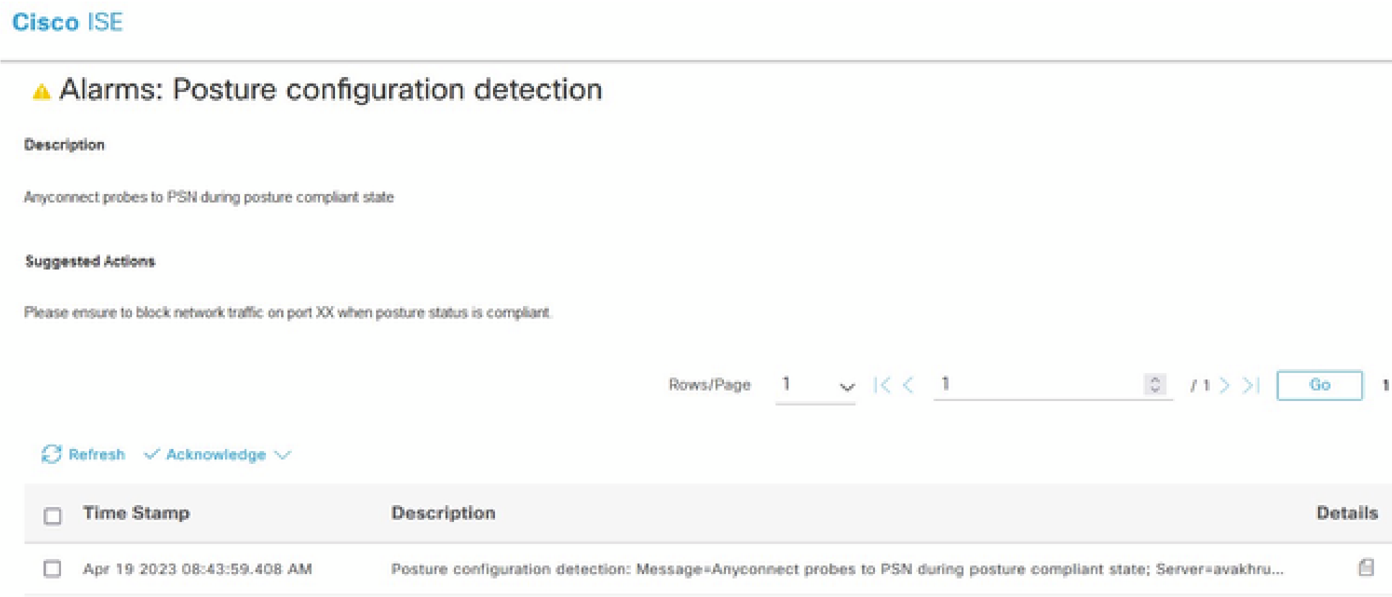
يعني غياب StateSyncProbeInterval" أو قيمة "0" أن مزامنة حالة الوضع معطلة.

في حالة تعيين "الفاصل الزمني لمزامنة حالة الوضع" في ملف تعريف Posture على ISE ولكن لا يتم عكسه في ملف تكوين على العميل، يلزم عندئذ التحقق من إعداد Posture.

فشل مزامنة حالة الوضع مع التنبيه على لوحة معلومات ISE

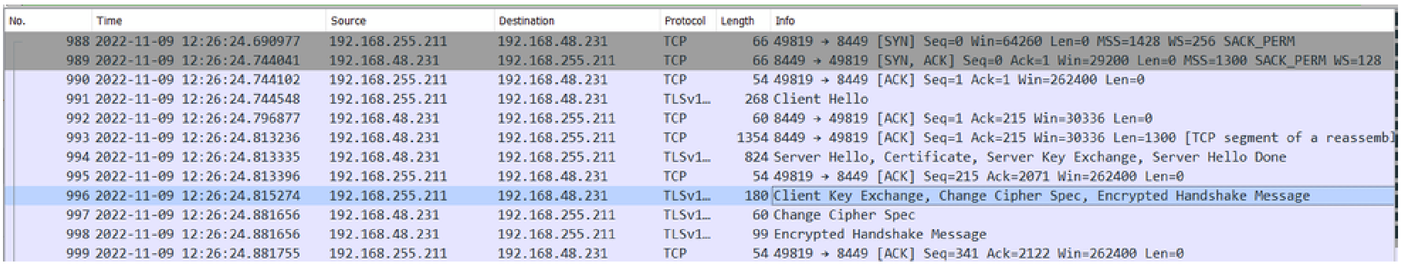
إذا فشلت مزامنة حالة الوضع مع التنبيه على ISE، فهذا يعني أن Cisco Secure Client كان قادرا على الوصول إلى ISE على منفذ مزامنة حالة الوضع (8449) وطلب حالة لجلسة العمل بحالة "متوافق".

- الإنذار في واجهة المستخدم الرسومية (ISE):



- التحقق من التقاط الحزمة

تم إنشاء اتصال TCP على منفذ مزامنة حالة الوضع (8449):



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 reassemb]
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

- التحقق من الصحة من سجل وحدة وضع العميل الآمن من Cisco

تحقق من AnyConnect_ISEPosture.txt من حزمة DART:

1) تم بدء اتصال HTTPS ب ISE PSN على منفذ مزامنة حالة الوضع (8449).

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

2) تم تلقي معلومات حالة جلسة العمل من ISE مع حالة Posture "متوافق".

```
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
```

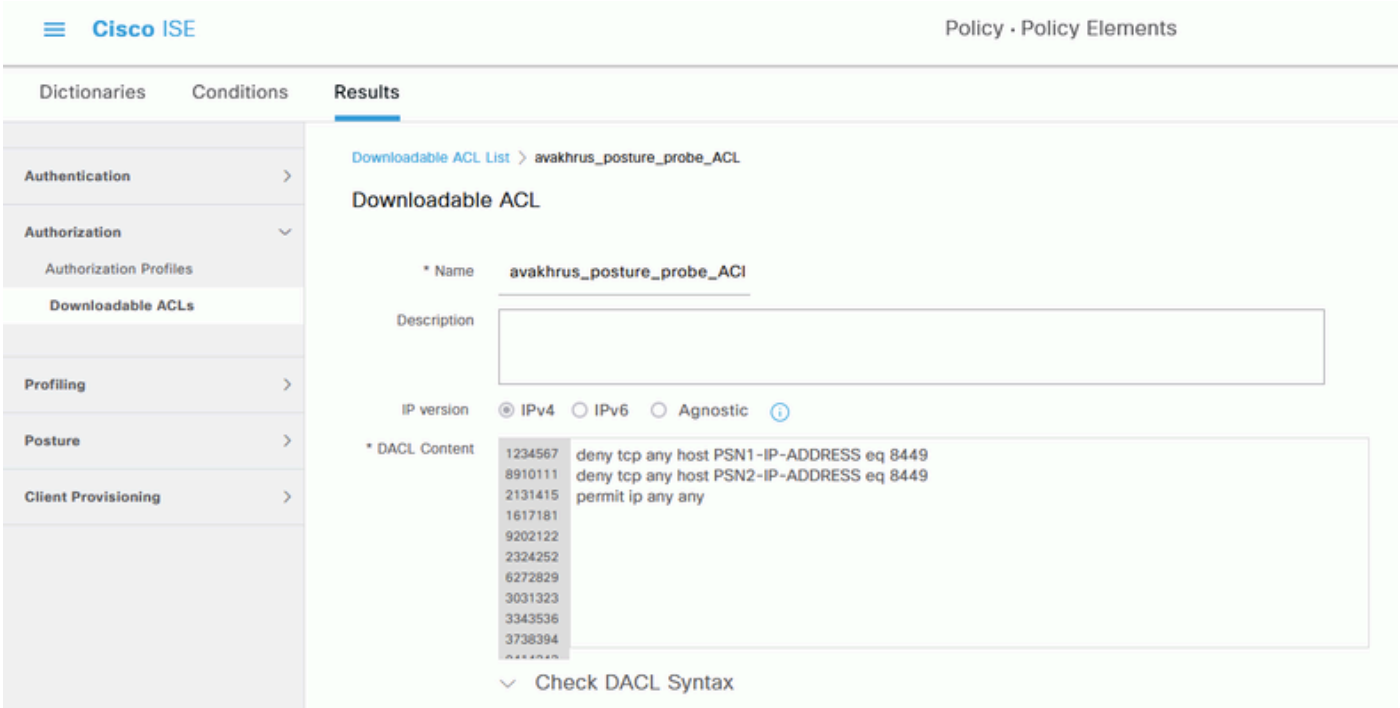
3) توقفات مزامنة حالة الوضع بسبب اكتشاف تكوين غير صحيح:

```
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
```

الا يمكن إعادة تشغيل مزامنة حالة الوضع من واجهة المستخدم الرسومية (GUI) لـ Cisco Secure Client عن طريق إعادة تشغيل تقييم الوضع أو تغيير الشبكة. بدلا من ذلك، يلزم إعادة تشغيل "العميل الآمن من Cisco" من أجل مزامنة حالة الوضع للعمل مرة أخرى.

التحقق من تكوين قائمة التحكم في الوصول للبنية الأساسية (dACL) لملف تعريف تفويض "متوافق" للوضع

1. التحقق من تكوين قائمة التحكم في الوصول للبنية الأساسية (dACL) المناسبة لملف تعريف تخويل "متوافق" للوضع:



2. التحقق من صحة إرسال تقرير المصادقة التفصيلي إلى قائمة التحكم في الوصول (dACL) بشكل صحيح تتيجة لمصادقة نقطة النهاية "متوافق".

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. تحقق من تطبيق قائمة التحكم في الوصول للبنية الأساسية (dACL) بشكل صحيح على جهاز الوصول إلى الشبكة:

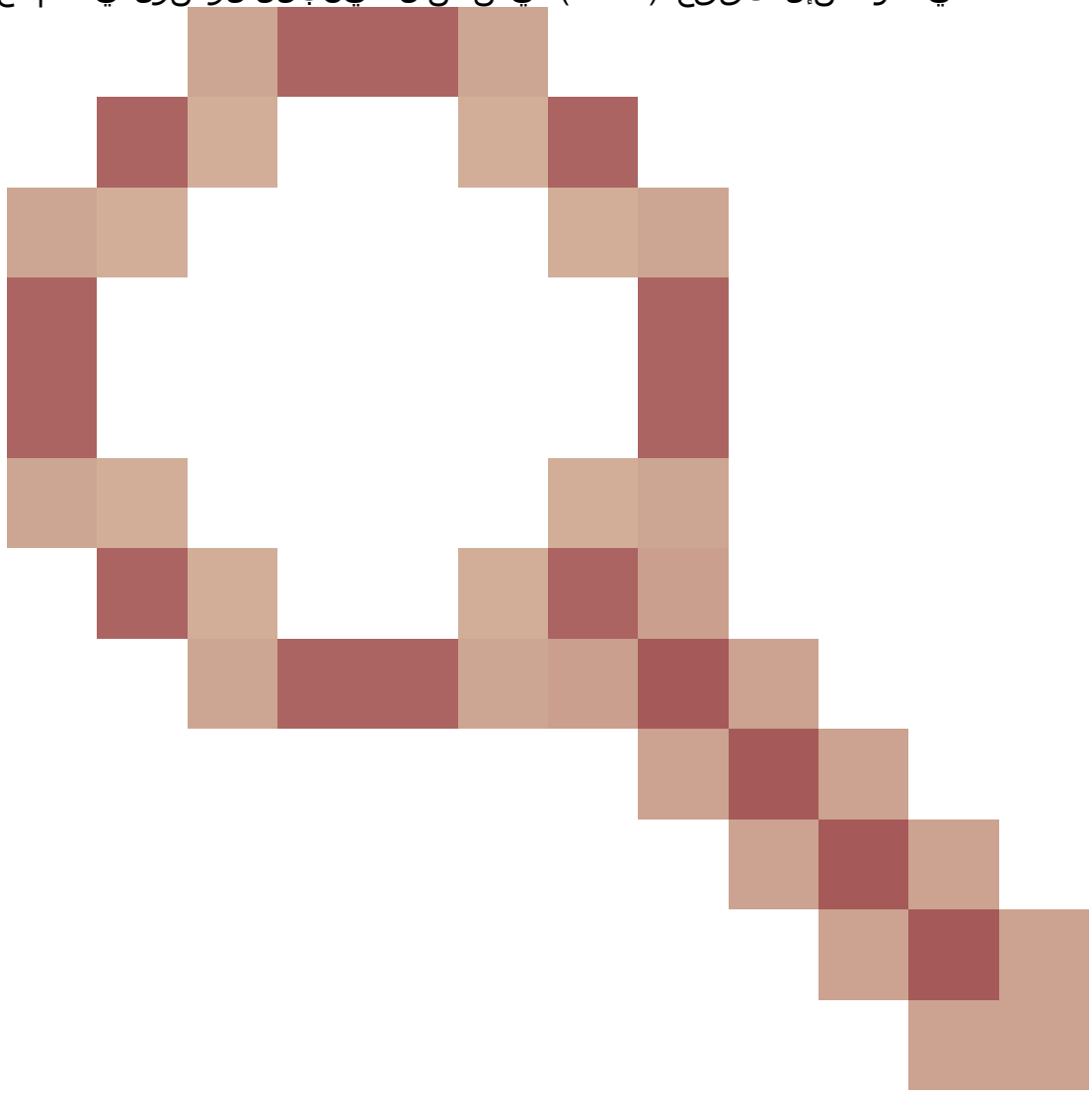
```
avakhrus_3560C#sh authe sess int fa0/12 det
            Interface:  FastEthernet0/12
          MAC Address:  0050.56a8.be02
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.255.193
            User-Name:  TRAINING\bob
               Status:  Authorized
               Domain:  DATA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

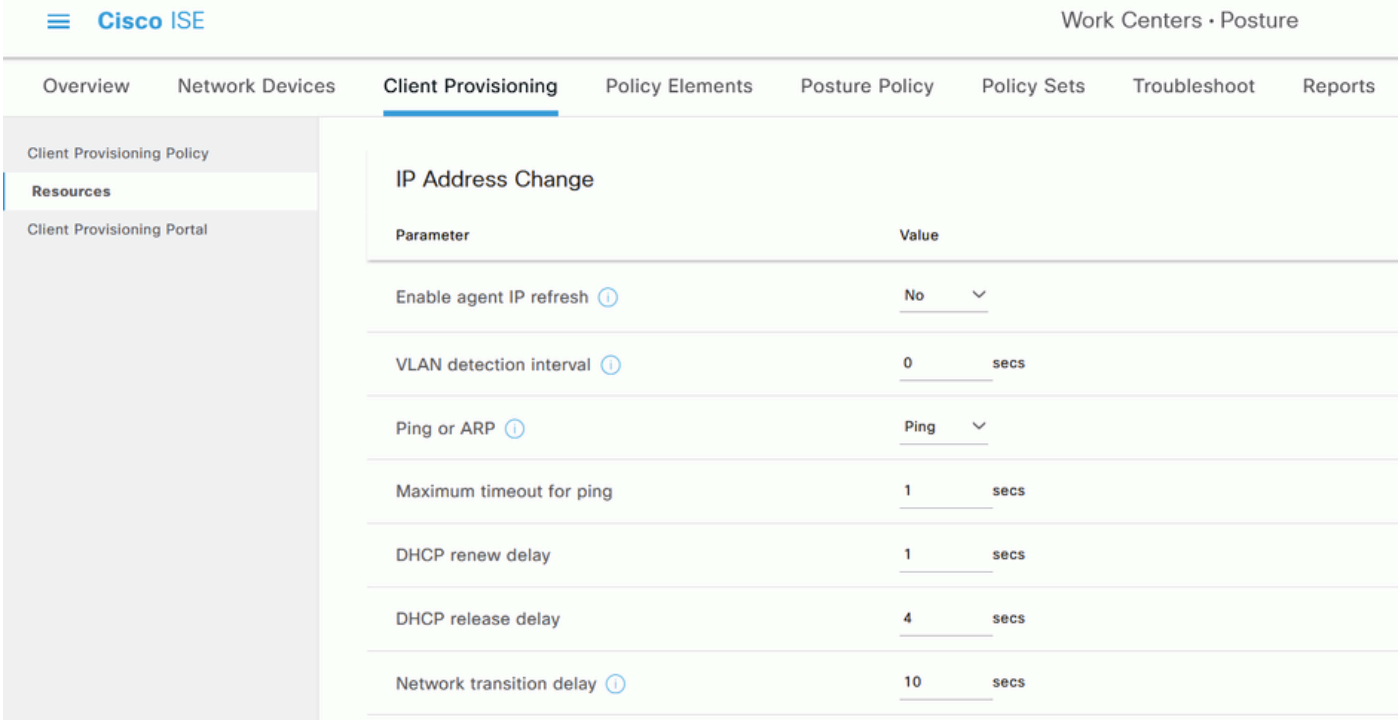
مشكلات معروفة

فشل مزامنة حالة الوضع مع ظهور تنبيه على ISE

يمكن أن تفشل مزامنة حالة الوضع مع التنبيه على ISE حتى إذا تم تطبيق قائمة التحكم في الوصول (dACL) المناسبة على جهاز وصول الشبكة إلى نقطة نهاية العميل. يحدث ذلك إذا تم تنفيذ Posture State Synchronization Probe أسرع من تطبيق قائمة التحكم في الوصول (dACL) أو إذا كان Posture State Synchronization Probe قيد التقدم بالفعل عندما يتم تطبيق قائمة التحكم في الوصول للبنية الأساسية (dACL). حققت الإصدار في cisco



بق id CSCwd58316
. كحل بديل، يلزمك تعيين "تأخر انتقال الشبكة" على 10 ثوان في ملف تعريف AnyConnect Posture (إعدادات ملف تعريف وكيل ISE Posture).


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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).