تنفيذ وضع ISE غير القابل لإعادة التوجيه

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

Connectiondata.xml

قائمة الاتصال بالمنزل

تصميم

التكوين

مجموعات أجهزة الشبكة (اختياري)

جهاز الشبكة

إدارة العميل

الإدارة اليدوية (قبل النشر)

مدخل توفير العميل (نشر عبر الويب)

نهج توفير العميل

الاعتماد

ملف تعريف التخويل

سياسة التخويل

استكشاف الأخطاء وإصلاحها

توافق مع Cisco Secure Client و Posture غير قابل للتطبيق (معلق) على ISE

جلسات عمل بسيطة/مهيمنة

التعرف على

الحل

الأداء

التعرف على

الحل

الحسابات

معلومات ذات صلة

المقدمة

يصف هذا المستند إستخدام وتكوين تلميحات أستكشاف المشكلات وإصلاحها الخاصة بتدفق الوضع دون إعادة التوجيه.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تدفق Posture على ISE
- تكوين مكونات الوضع على ISE
- إعادة التوجيه إلى بوابات ISE

من أجل فهم أفضل للمفاهيم الموصوفة لاحقا، يوصى بالمرور بما يلي:

[مقارنة تدفق إعادة توجيه ISE Posture (وضعية محرك خدمات الهوية (ISE)) بتدفق غير قابل لإعادة التوجيه من ISE]
[استكشاف أخطاء إدارة جلسة ISE ووضعية محرك خدمات الهوية (ISE) وإصلاحها]

المكونات المستخدمة

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

- ISE الإصدار 3.3 من Cisco
- Cisco Secure Client 5.0.01242

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

يتكون تدفق ISE Posture (وضعية محرك خدمات الهوية (ISE)) من الخطوات التالية:

0. المصادقة/التخويل. يتم بشكل عام مباشرة قبل بدء تدفق الوضع ولكن يمكن تجاوزه في حالات إستخدام معينة مثل إعادة تقييم الوضع (PRA).

بما أن المصادقة نفسها لا تطلق اكتشاف الوضع، فإن هذا لا يعتبر ضروريا لكل تدفق وضعية.

1. الاكتشاف. تم إجراء العملية بواسطة وحدة وضع ISE للعميل الآمن للعثور على مالك PSN لجلسة العمل النشطة الحالية.
2. إمداد العميل. تم إجراء العملية بواسطة ISE لتوفير العميل باستخدام وحدة وضع ISE النمطية المتوافقة مع Cisco Secure Client (المعروفة سابقا باسم AnyConnect) وإصدارات وحدة التوافق النمطية. في هذه الخطوة، يتم أيضا دفع النسخة المحلية من ملف تعريف الوضع الموجود في PSN المعين والموقع منه إلى العميل.
3. فحص النظام. يتم تقييم سياسات الوضع التي تم تكوينها على ISE بواسطة وحدة التوافق النمطية.
4. الإصلاح (إختياري). يتم تنفيذه في حالة عدم توافق أي نهج وضعية.
5. CoA. يعد إعادة التفويض أمرا ضروريا لمنح حق الوصول النهائي إلى الشبكة (متوافق أو غير متوافق).

يركز هذا المستند على عملية اكتشاف تدفق وضعية ISE.

cisco يوصي أن يستعمل redirection ل الإكتشاف عملية، ومع ذلك، هناك حالات معينة حيث ال يمكن إعادة التوجيه أن ينفذ مثل إستخدام طرف ثالث شبكة أداة حيث إعادة التوجيه غير

مدعوم. يهدف هذا المستند إلى توفير توجيه عام وأفضل الممارسات لتنفيذ الوضعية التي لا تحتاج إلى إعادة توجيه في هذه البيئات واستكشاف أخطائها وإصلاحها.

يتم وصف الوصف الكامل للتدفق عديم الإتجاه في تدفق إعادة توجيه وضع ISE للمقارنة إلى وضع ISE لتدفق لا يحتاج إلى توجيه

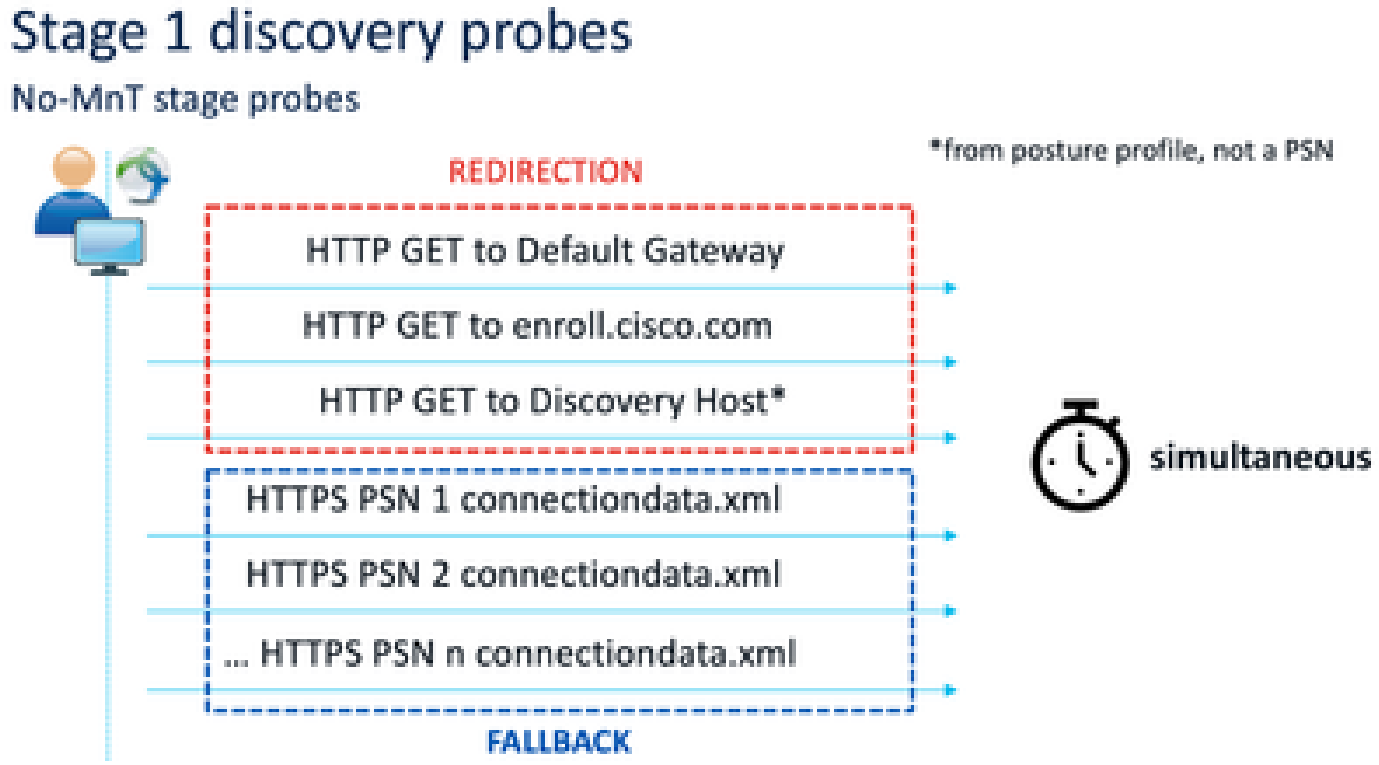
هناك نوعان من مستكشفات الوضع التي لا تستخدم إعادة التوجيه:

1. Connectiondata.xml
2. قائمة الاتصال بالمنزل

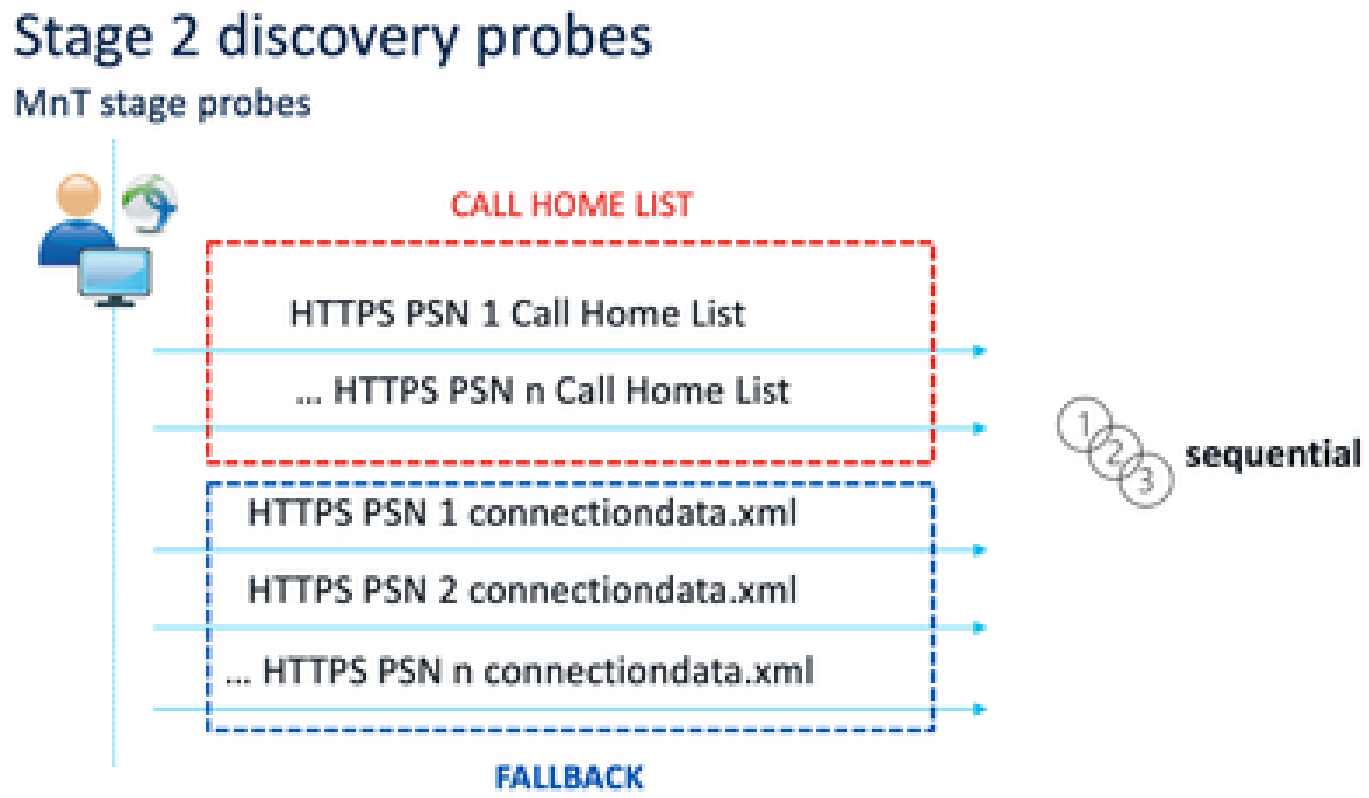
Connectiondata.xml

ConnectionData.xml هو ملف تم إنشاؤه وصيانته تلقائيا بواسطة Cisco Secure Client. وهو يتكون من قائمة بشبكات PSN التي نجح العميل في الاتصال بها للوضعية، وبالتالي، هذا هو الملف المحلي فقط ومحتوياته غير ثابتة عبر جميع نقاط النهاية.

والغرض الرئيسي من ConnectionData.xml هو العمل كآلية نسخ إحتياطي لكل من عمليات أستكشاف المرحلة الأولى والثانية. في حالة تعذر العثور على مستكشفات Redirection أو Call Home List على PSN جلسة عمل نشطة، يرسل Cisco Secure Client طلبا مباشرا إلى كل خادم من الخوادم المدرجة في ConnectionData.xml.



مستكشفات المرحلة 1



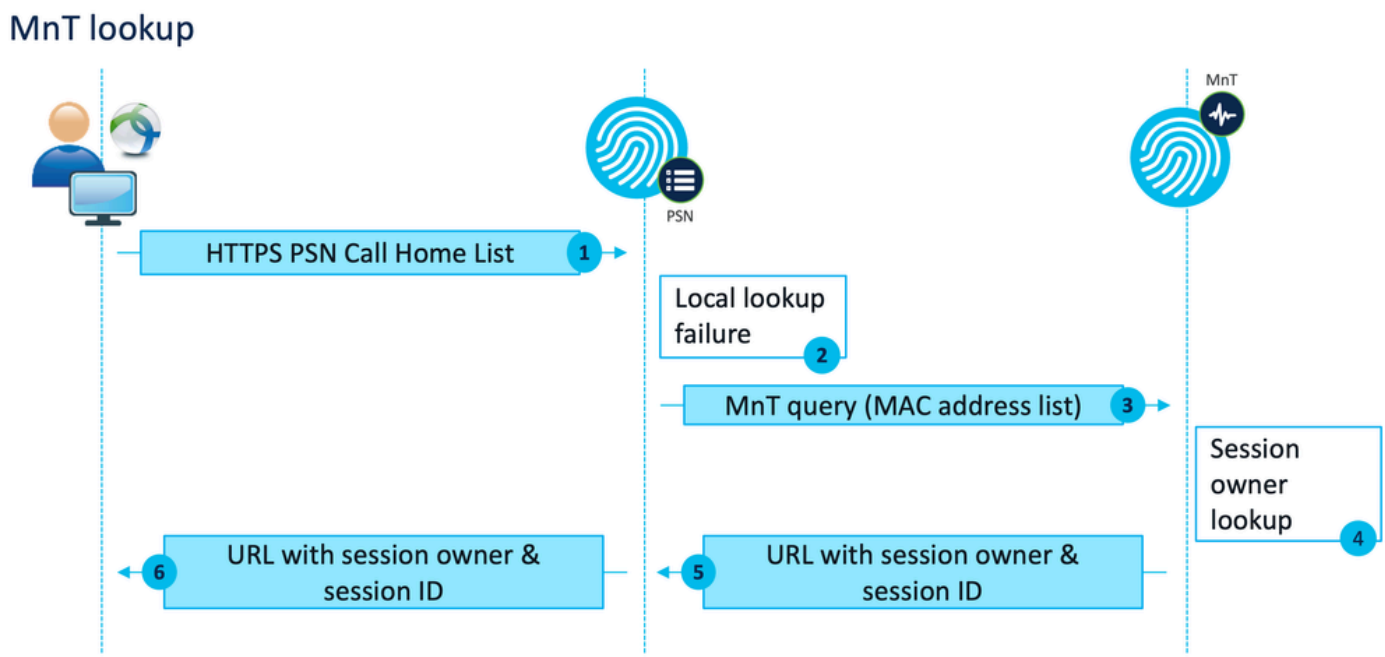
مستكشفات المرحلة 2

هناك مشكلة شائعة ناجمة عن إستخدام إختبارات ConnectionData.xml وهي الحمل الزائد لنشر ISE بسبب وجود عدد كبير من طلبات HTTPS التي تم إرسالها بواسطة نقاط النهاية. من المهم إعتبار أنه في حين أن ConnectionData.xml فعال كآلية نسخ إحتياطي لتجنب حالات انتهاء الصلاحية الكاملة لكل من آليات إعادة التوجيه والوضعية غير القابلة لإعادة التوجيه، فإنه ليس حل مستدام لبيئة الوضع، وبالتالي، من الضروري تشخيص مشاكل التصميم والتكوين التي تتسبب في فشل إختبارات الاكتشاف الرئيسية والتي ينتج عنها مشاكل في الاكتشاف وحلها.

قائمة الاتصال بالمنزل

Call Home List هو قسم من ملف تعريف الوضع حيث تم تحديد قائمة من PSNs ليتم إستخدامها للوضع. وعلى عكس ConnectionData.xml، يتم إنشاء هذا الإجراء وصيانته بواسطة مسؤول ISE ويمكن أن يتطلب مرحلة تصميم للحصول على التكوين الأمثل. تطابق قائمة شبكات PSN في "قائمة الاتصال بالمنزل" قائمة خوادم المصادقة والمحاسبة التي تم تكوينها في جهاز الشبكة أو موازن التحميل ل RADIUS.

يمكن Call Home List Probe إستخدام بحث MnT أثناء البحث في جلسة العمل النشطة في حالة فشل البحث المحلي في PSN. وتمتد الوظيفة نفسها إلى مسار ConnectionData.xml فقط عند إستخدامها أثناء اكتشاف المرحلة 2. ولهذا السبب، يشار أيضا إلى جميع مستكشفات المرحلة 2 باسم مستكشفات الجيل الجديد.



تدفق بحث MNt

تصميم

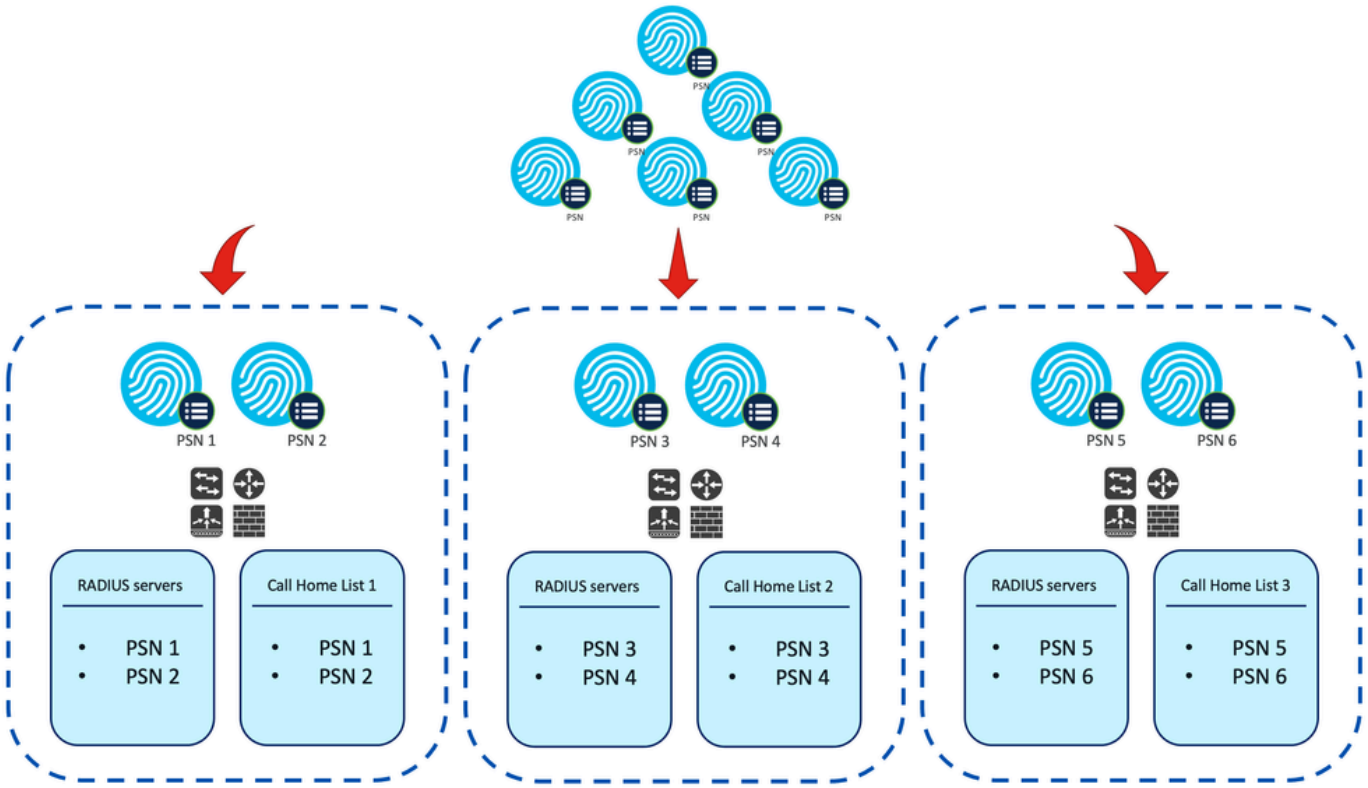
ونظرا لأن عملية الاكتشاف دون توجيه غالبا ما تستلزم تدفقا أكثر تعقيدا وكمية أكبر من المعالجة على شبكات PSN وشبكة MnT مقارنة بتدفق إعادة التوجيه، فهناك تحديان مشتركان يمكن أن يظهرا أثناء التنفيذ:

1. اكتشاف فعال
2. أداء نشر ISE

للتعامل مع هذه التحديات، يوصى بتصميم قائمة الاتصال بالمنزل للحد من عدد شبكات PSN التي يمكن لنقطة نهاية معينة إستخدامها للوضع. بالنسبة لعمليات النشر المتوسطة والكبيرة، من الضروري توزيع النشر لإنشاء قوائم المكالمات الرئيسية المتعددة ذات عدد أقل من شبكات PSN، وبالتالي يمكن تقييد قائمة شبكات PSN المستخدمة لمصادقة RADIUS لجهاز شبكة معين بنفس الطريقة لمطابقة قائمة المكالمات الرئيسية المقابلة.

ويمكن أخذ هذه الجوانب بعين الاعتبار عند تطوير إستراتيجية توزيع الشبكات الخاصة لتحديد الحد الأقصى لعدد الشبكات الخاصة في كل قائمة "الاتصال بالمنزل":

- عدد شبكات PSN في النشر
- مواصفات أجهزة PSN وعقد MNt
- الحد الأقصى لعدد جلسات عمل الوضع المتزامن في النشر
- عدد أجهزة الشبكة
- البيئات المختلطة (إعادة التوجيه المتزامن وتنفيذ الوضع دون إعادة التوجيه)
- عدد المهايئات التي تستخدمها نقاط النهاية
- موقع أجهزة الشبكة وشبكات PSN
- أنواع اتصال الشبكة المستخدمة للوضع (سلكي، لاسلكي، VPN)



مثال: توزيع PSN لوضعية غير قابلة لإعادة التوجيه

تلميح: أستخدم مجموعات أجهزة الشبكة لتصنيف أجهزة الشبكة وفقا للتصميم.

التكوين

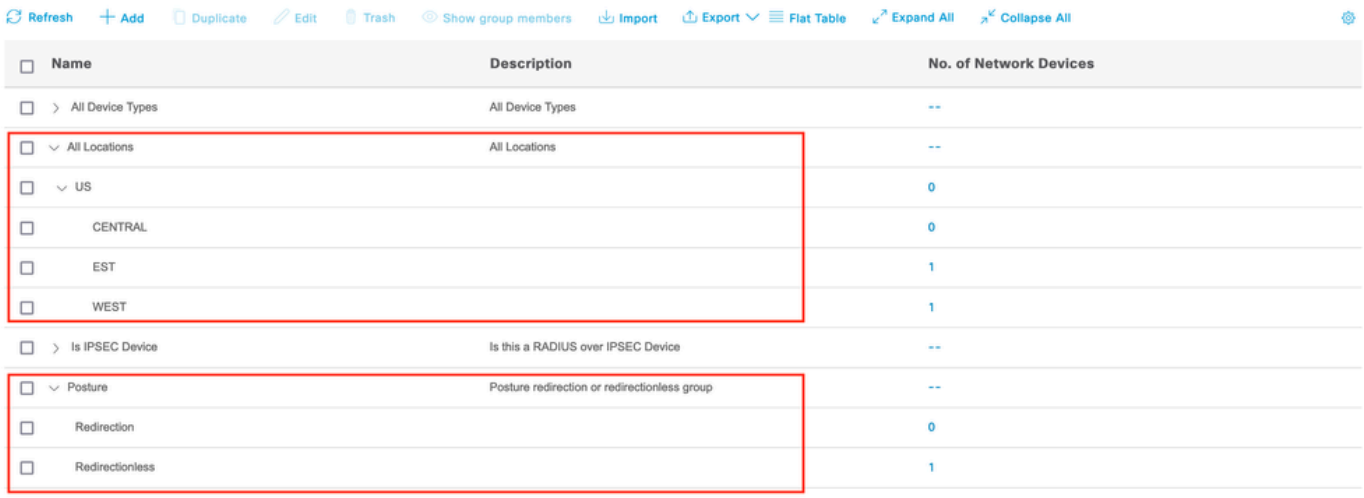
مجموعات أجهزة الشبكة (إختياري)

يمكن إستخدام مجموعات أجهزة الشبكة للتعرف على أجهزة الشبكة ومطابقتها باستخدام قائمة خوادم RADIUS المطابقة لها وقائمة الاتصال بالمنزل. في حالة البيئات المختلطة، يمكن إستخدامها أيضا لتحديد الأجهزة التي تدعم إعادة التوجيه من الأجهزة التي لا تدعم.

إذا كانت إستراتيجية التوزيع التي تم تطويرها أثناء مرحلة التصميم تعتمد على مجموعات أجهزة الشبكة، فاتبع الخطوات التالية لتكوينها على ISE:

1. انتقل إلى إدارة > مجموعات موارد شبكة موارد الشبكة.
2. انقر فوق إضافة لإضافة مجموعة جديدة، قم بتوفير اسم وحدد المجموعة الأصلية ، إذا كان ذلك ممكنا.
3. كرر الخطوة 2 لإنشاء كافة المجموعات الضرورية.

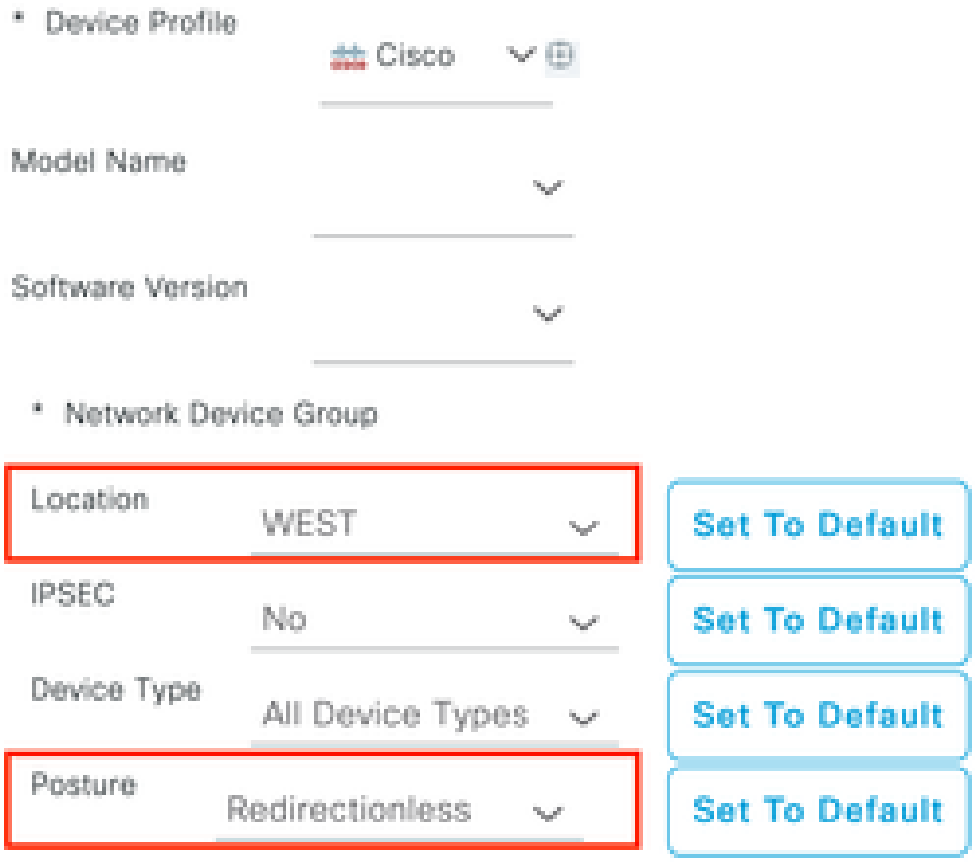
في الأمثلة المستخدمة في هذا الدليل، يتم إستخدام مجموعة أجهزة تحديد الموقع لتحديد قائمة خوادم RADIUS وقائمة الاتصال بالمنزل، ويتم إستخدام مجموعة أجهزة الوضع المخصص لتعريف إعادة التوجيه من أجهزة الوضع غير القابلة لإعادة التوجيه.

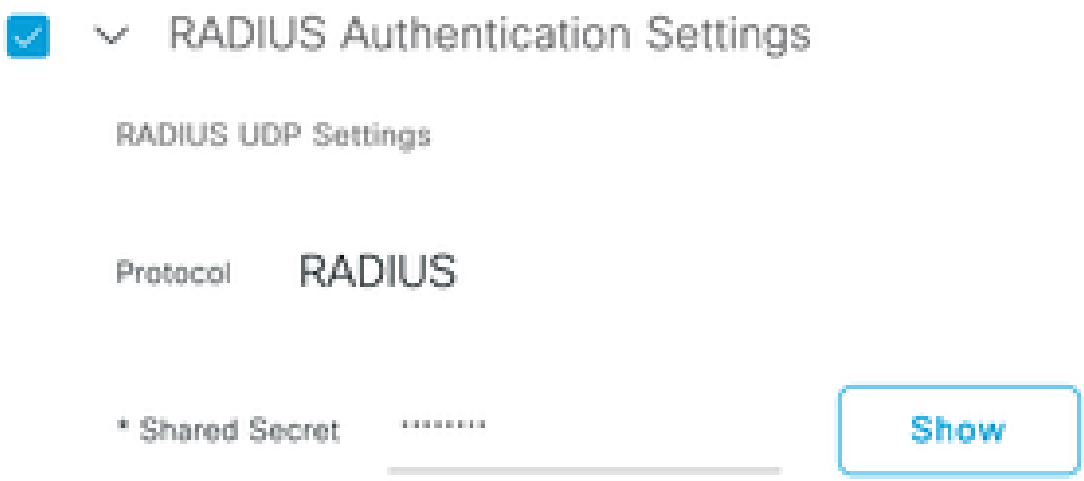


مجموعات أجهزة الشبكة

جهاز الشبكة

1. يمكن تكوين جهاز الشبكة لمصادقة RADIUS والتخويل والمحاسبة. ارجع إلى كل وثائق المورد لخطوات التكوين. قم بتكوين قائمة خوادم RADIUS وفقا لقائمة الاتصال الرئيسية المقابلة.
2. على ISE، انتقل إلى إدارة > موارد الشبكة>أجهزة الشبكة وانقر فوق إضافة. قم بتكوين مجموعات أجهزة الشبكة وفقا للتصميم وتمكين إعدادات مصادقة RADIUS لتكوين السر المشترك.





تكوين جهاز الشبكة

إمداد العميل

هناك طريقتان لتزويد العميل بالبرنامج المناسب وملف التعريف المناسب لأداء الوضعية في بيئة غير قابلة لإعادة التوجيه:

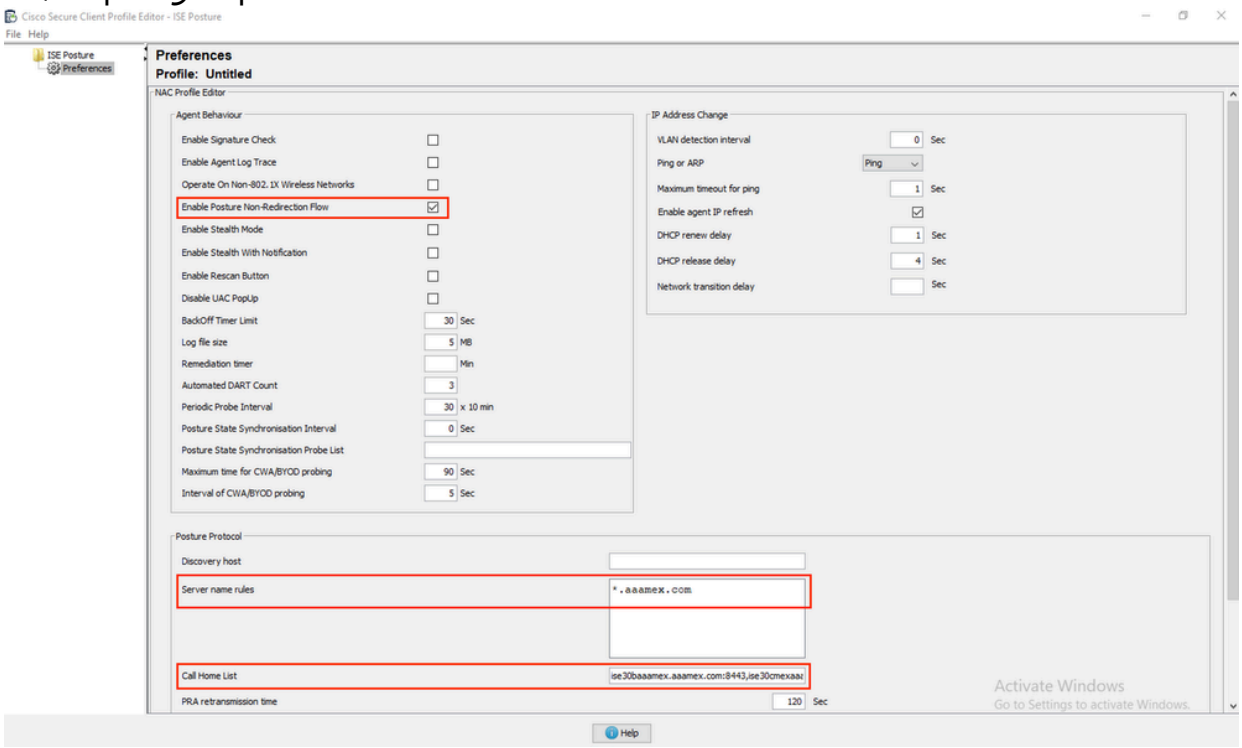
1. الإمداد اليدوي (قبل النشر)
2. مدخل توفير العميل (نشر عبر الويب)

الإمداد اليدوي (قبل النشر)

1. تنزيل Cisco Secure Client Profile Editor من [تنزيل برنامج Cisco Software](#).

   حزمة محرر ملف التعريف

2. افتح محرر ملف تعريف ISE Posture (وضعية محرك خدمات الهوية (ISE)):
   - تأكد من تمكين تمكين تدفق عدم إعادة التوجيه للوضع.
   - قم بتكوين قواعد اسم الخادم مفصولة بفواصل. أختر أحد هذه التكوينات:
     - نجمة واحدة * للسماح بالاتصال بأي PSN.
     - قيم أحرف البدل (على سبيل المثال، *.aaamex.com) للسماح بالاتصال بأي PSN في مجالات معينة.
     - قائمة PSN FQDNs، مفصولة بفاصلة، لتقييد الاتصال بشبكات PSN معينة. في حالة إستخدامها، يجب أن تطابق هذه القائمة قائمة "الاتصال بالمنزل".
   - قم بتكوين قائمة "الاتصال بالمنزل" لتحديد قائمة PSNs التي تم فصلها بفاصلة. تأكد من إضافة منفذ بوابة إمداد العميل باستخدام التنسيق FQDN:port أو IP:port.

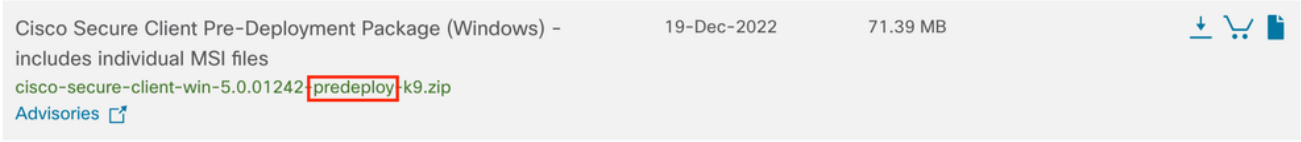


   تشكيل توصيف وضعي باستخدام محرر ملف التعريف

   > ملاحظة: ارجع إلى الخطوة 4 من قسم سياسة إمداد العميل للحصول على تعليمات حول كيفية التحقق من منفذ بوابة إمداد العميل إذا لزم الأمر.

3. احفظ ملف التعريف على هيئة ISEPostureCFG.xml.
4. كرر الخطوات 2 و 3 لإنشاء ملف تعريف وضعية جديد لكل قائمة "الاتصال بالمنزل" قيد الاستخدام.

5. تنزيل حزمة النشر المسبق ل Cisco Secure Client من تنزيل برامج Cisco.



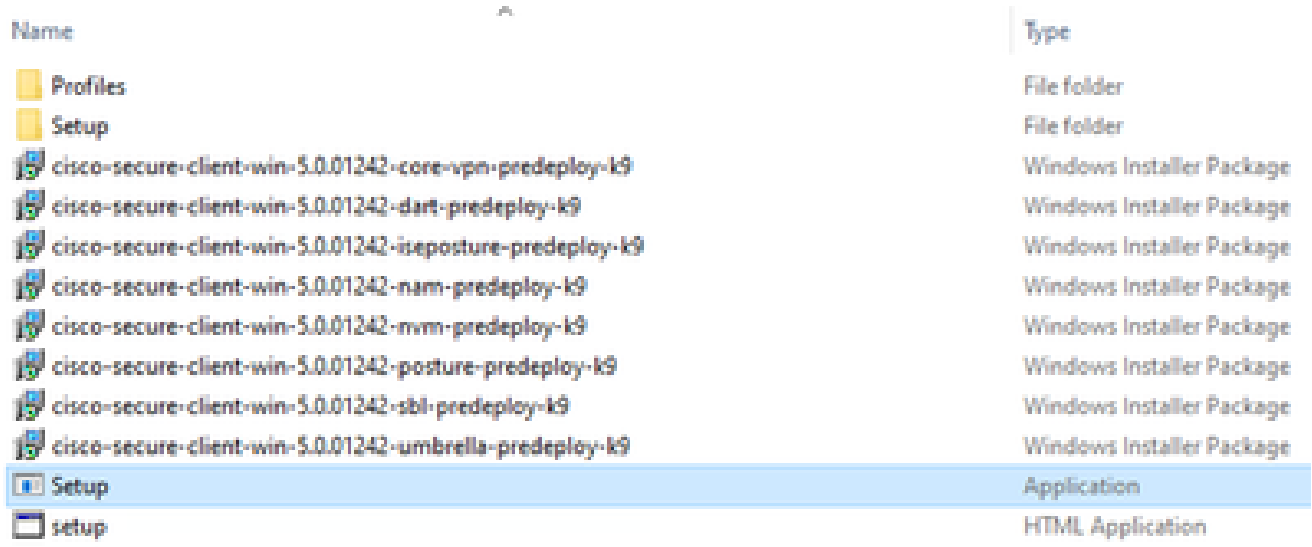
حزمة النشر المسبق ل Cisco Secure Client

6. قم بتوزيع ملف التخصيص وملفات التثبيت في ملف أرشيف، أو انسخ الملفات إلى العملاء.

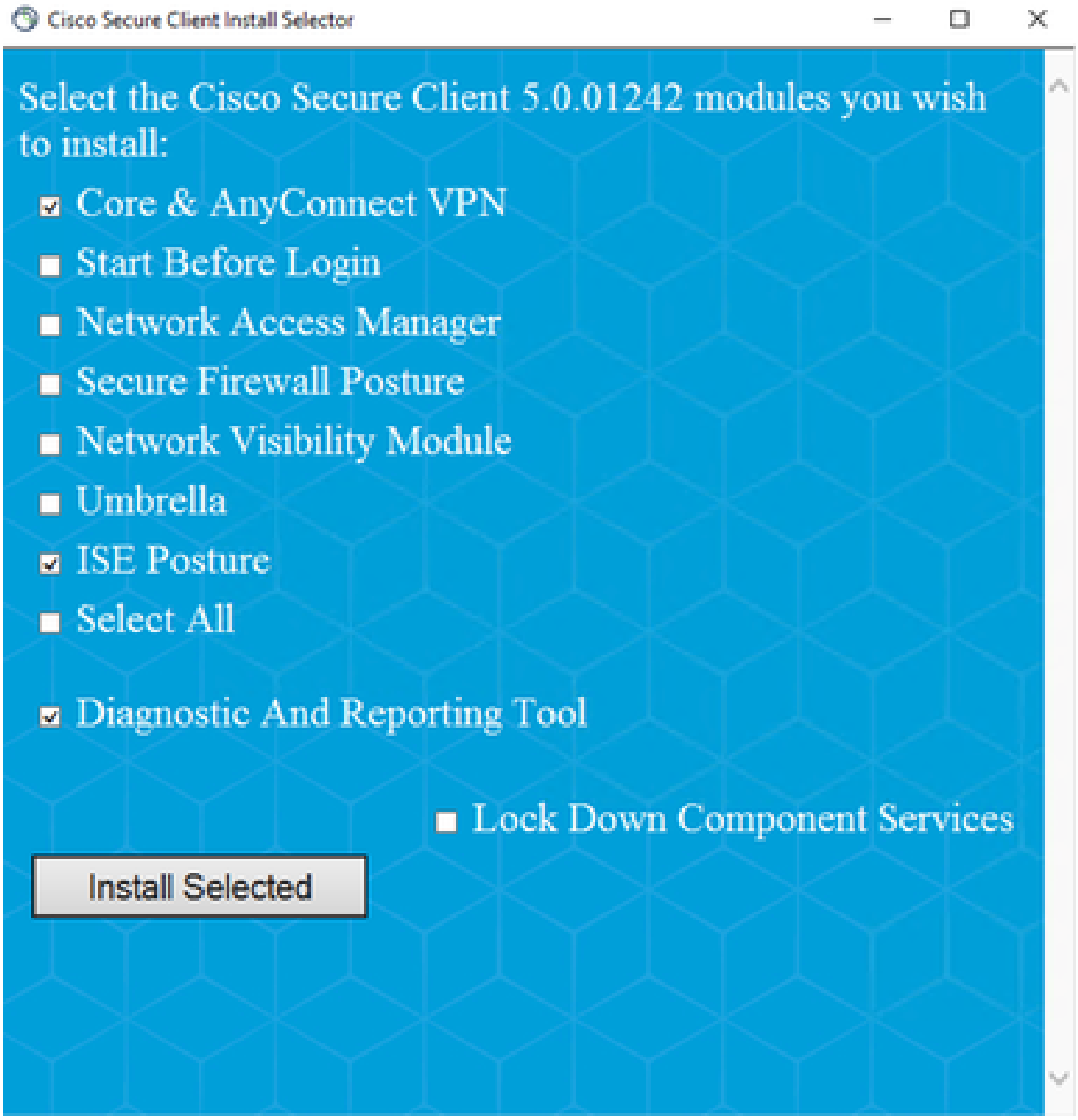
تحذير: تأكد من أن نفس ملفات Cisco Secure Client موجودة أيضا على المنافذ التي تخطط للاتصال بها: جدار الحماية الآمن ASA و ISE وهكذا. حتى عند إستخدام الإمداد اليدوي، يجب تكوين ISE لتوفير العميل باستخدام إصدار البرنامج المطابق. ارجع إلى قسم تكوين سياسة تزويد العميل للحصول على تعليمات تفصيلية.

---

7. على العميل، افتح ملف zip وشغل Setup لتثبيت الوحدات النمطية Core و ISE Posture (وضعية محرك خدمات الهوية (ISE)). بدل من ذلك، يمكن إستخدام ملفات msi الفردية لتثبيت كل وحدة نمطية، في هذه الحالة، يجب التأكد من تثبيت وحدة Core-VPN النمطية أولا.



محتويات حزمة النشر المسبق ل Cisco Secure Client



مثبت العميل الآمن من Cisco

تلميح: تثبيت "أداة التشخيص وإعداد التقارير" التي سيتم إستخدامها لأغراض أستكشاف الأخطاء وإصلاحها.

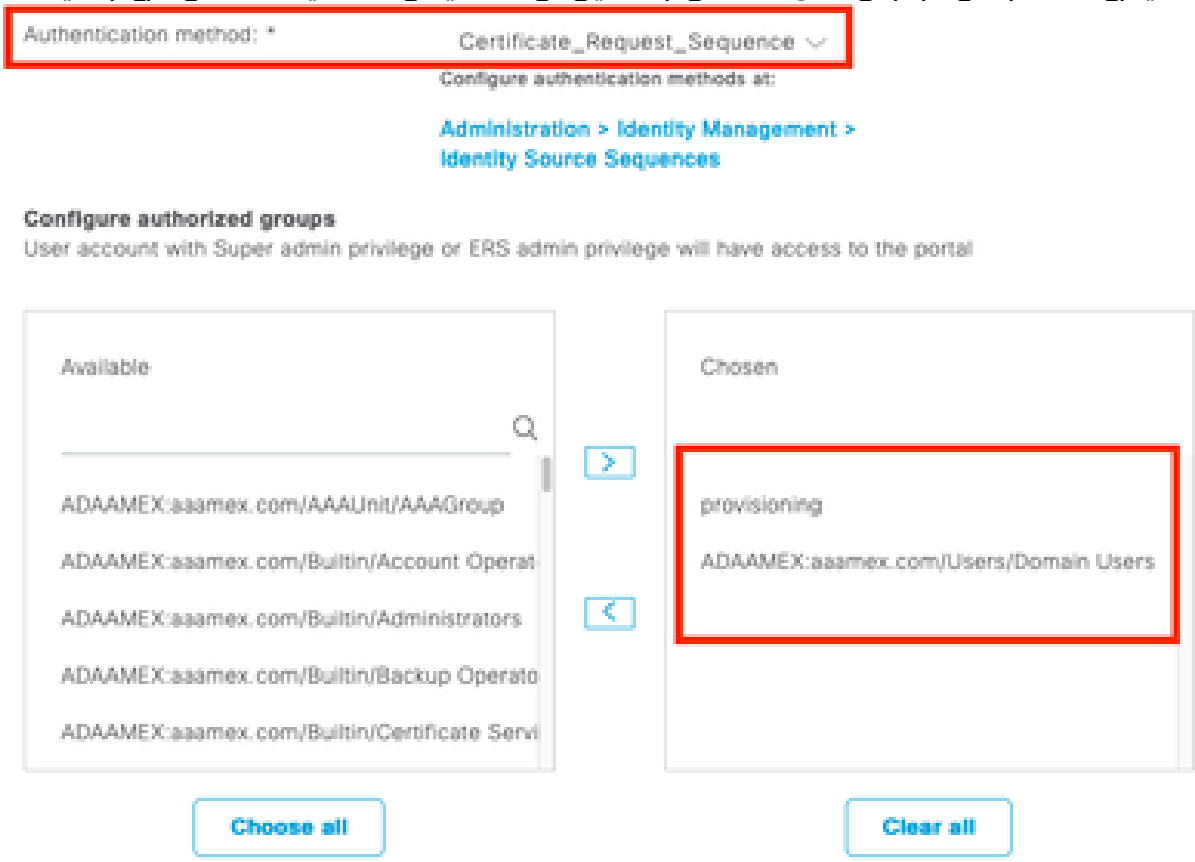
8. بمجرد اكتمال التثبيت، انسخ ملف تعريف الوضع xml إلى هذه المواقع:
   - Windows: %ProgramData%\Cisco\Cisco\Secure Client\ISE Posture
   - نظام التشغيل MacOS: /opt/cisco/secureclient/iseposture/

مدخل توفير العميل (نشر عبر الويب)

يمكن إستخدام مدخل إمداد عميل ISE لتثبيت وحدة Cisco Secure Client ISE Posture Module وملف تعريف الوضع من ISE، كما يمكن إستخدامه لدفع ملف تعريف الوضع وحده إذا كان

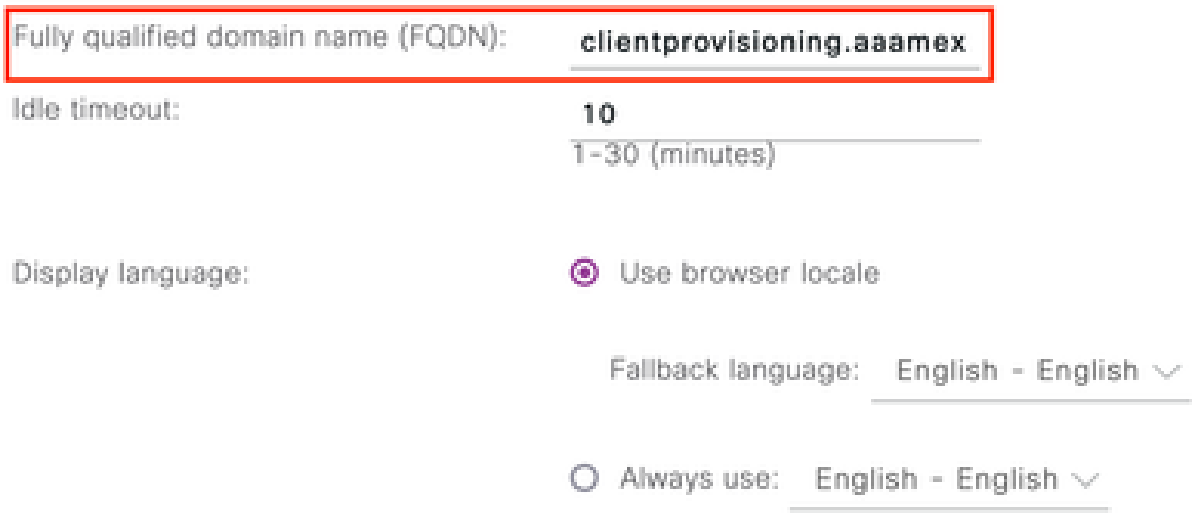
وحدة ISE Posture المنصة مثبتة بالفعل على العميل.

1. انتقل إلى مركز العمل> الوضع> إمداد العميل>بوابة إمداد العميل لفتح تكوين البوابة. قم بتوسيع قسم إعدادات المدخل وحدد موقع حقل طريقة المصادقة، وحدد تسلسل مصدر الهوية الذي سيتم إستخدامه للمصادقة في المدخل.
2. تكوين مجموعات الهوية الداخلية والخارجية المخولة لاستخدام مدخل إمداد العميل.



أسلوب المصادقة والمجموعات المعتمدة في إعدادات المدخل

3. في حقل اسم المجال المؤهل بالكامل (FQDN)، قم بتكوين عنوان URL الذي يتم إستخدامه من قبل العملاء للوصول إلى البوابة. لتكوين شبكات FQDN متعددة، أدخل القيم المفصولة بفواصل.



4. قم بتكوين خادم (خوادم) DNS لحل عنوان URL الخاص بالمدخل إلى شبكات PSN

الخاصة بقائمة Call Home List المقابلة.

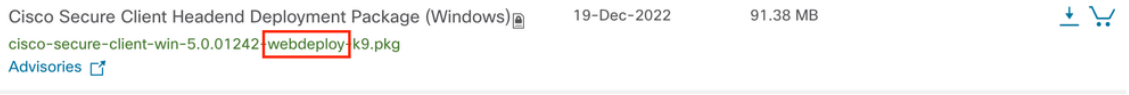
5. قم بتوفير FQDN للمستخدمين النهائيين للوصول إلى البوابة لتثبيت برنامج ISE Posture (وضعية محرك خدمات الهوية (ISE)).

ملاحظة: لاستخدام FQDN الخاص بالمدخل، يجب أن يحتوي العملاء على سلسلة شهادات مسؤول PSN بالإضافة إلى سلسلة شهادات المدخل المثبتة في المخزن الموثوق به، كما يجب أن تحتوي شهادة المسؤول على FQDN الخاص بالمدخل في حقل شبكة التخزين (SAN).

نهج توفير العميل

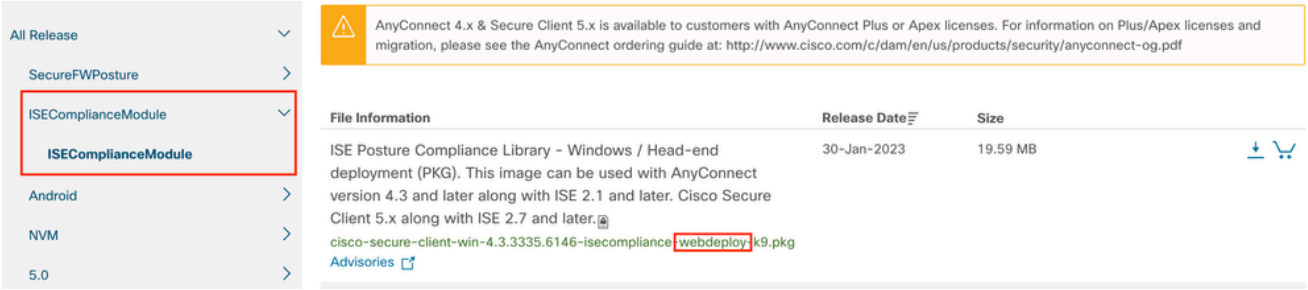
يجب تكوين إمداد العميل على ISE بغض النظر عن نوع الإمداد (النشر المسبق أو النشر عبر الويب) الذي يتم إستخدامه لتثبيت Cisco Secure Client على نقاط النهاية.

1. تنزيل حزمة نشر وحدة الاستقبال والبث الخاصة ب Cisco Secure Client من تنزيل برامج Cisco.



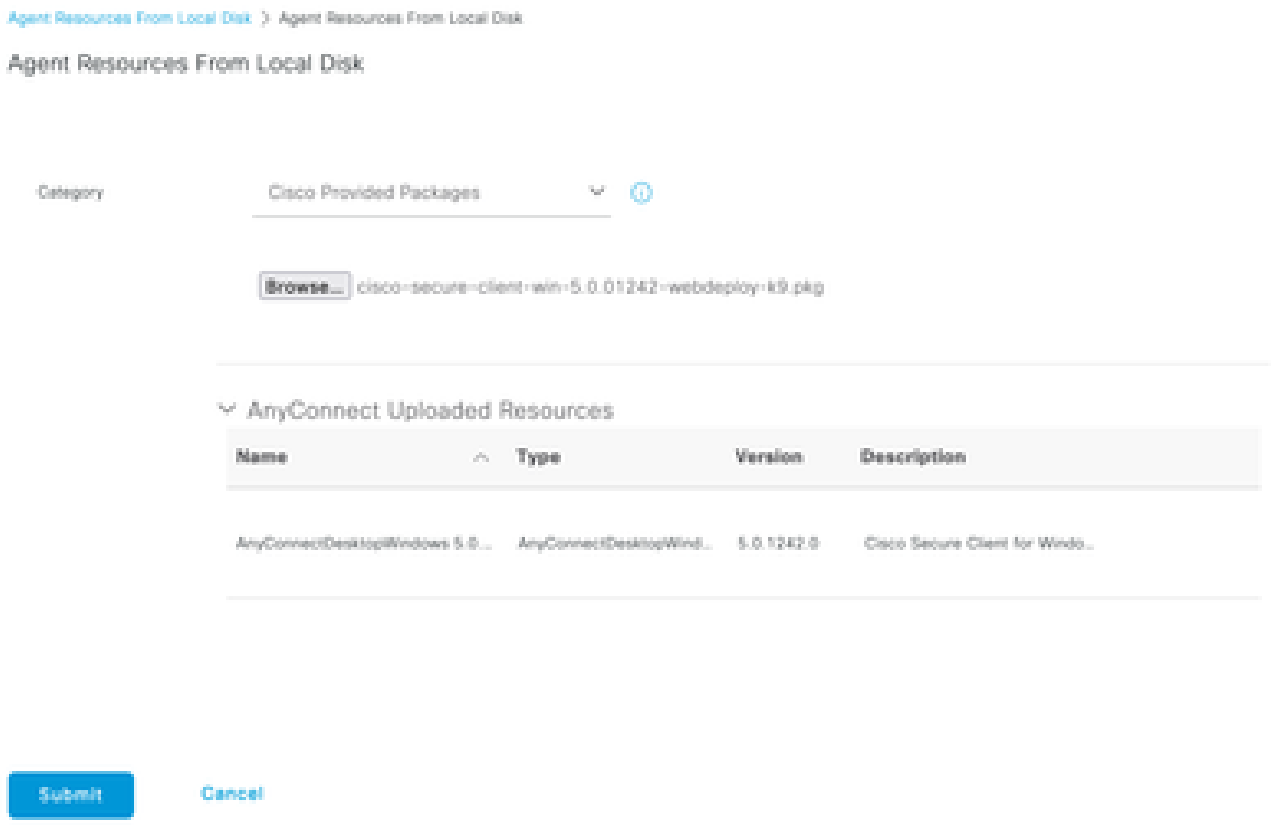
حزمة Cisco Secure Client Webdeployment

2. قم بتنزيل أحدث وحدة توافق مع معيار ISE حزمة نشر على الويب من تنزيل برامج Cisco.



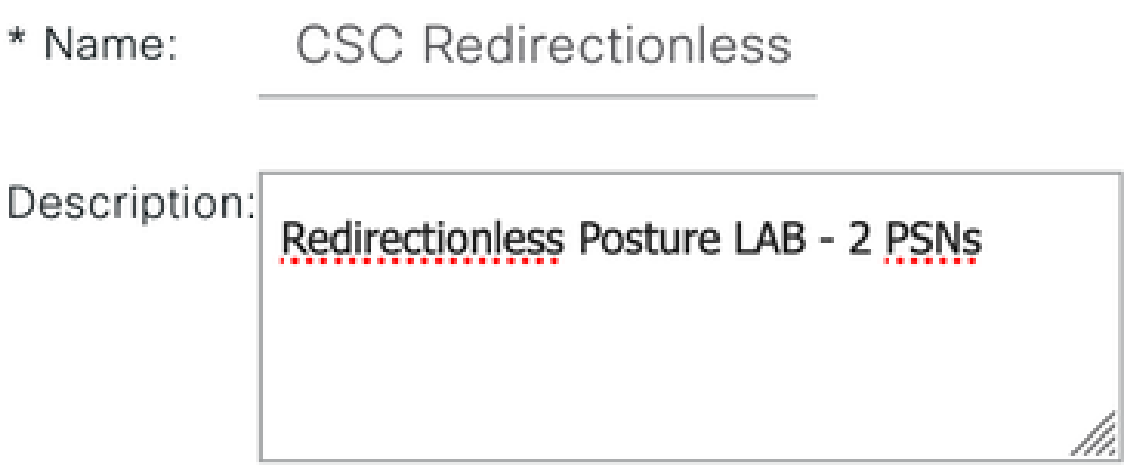
حزمة النشر عبر الويب لوحدة ISE Compliance Module

3. على ISE، انتقل إلى مركز العمل>Posture> Client Provisioning>الموارد وانقر فوق إضافة >موارد الوكيل من القرص المحلي. حدد حزم Cisco المقدمة من القائمة المنسدلة الفئة وقم بتحميل حزمة نشر وحدة الاستقبال والبث الخاصة بالعميل الآمن من Cisco التي تم تنزيلها مسبقا. كرر نفس العملية لتحميل وحدة التوافق النمطية.

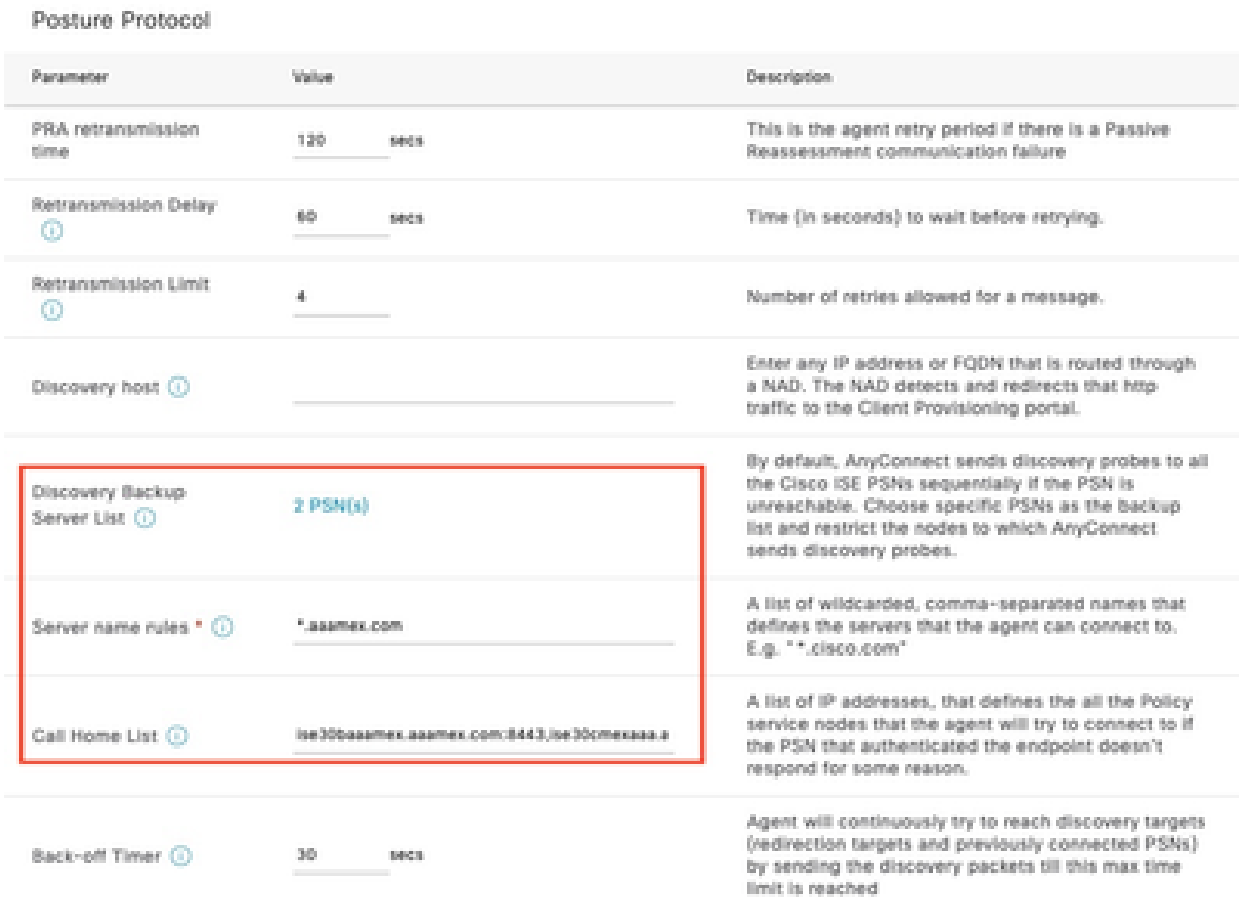


تحميل الحزم المقدمة من Cisco إلى ISE

4. في علامة التبويب موارد، انقر فوق إضافة > ملف تعريف وضعية العميل. في التوصيف:
   - قم بتكوين اسم يمكن إستخدامه لتحديد ملف التعريف وقائمة الاتصال بالمنزل داخل ISE.
   - تأكد من أن تمكين المسابير الإضافية بحيث يمكن أن يعمل التدفق غير إعادة التوجيه تم ضبطه على نعم.
   - قم بتكوين قائمة خادم النسخ الاحتياطي للاكتشاف. حدد شبكات PSN التي تطابق قائمة "الاتصال بالمنزل" التي يتم تكوينها.
     هذه هي قائمة شبكات PSN التي يتم حفظها في ConnectionData.xml بعد أول اتصال.
   - قم بتكوين قواعد اسم الخادم مفصولة بفواصل. أختر أحد هذه التكوينات:
     - نجمة واحدة * للسماح بالاتصال بأي PSN.
     - قيم أحرف البدل (على سبيل المثال، *.aaamex.com) للسماح بالاتصال بأي PSN في مجالات معينة.
     - قائمة بروتوكولات PSN FQDNs، مفصولة بفاصلة، لتقييد الاتصال بشبكات PSN معينة. في حالة إستخدامها، يجب أن تتطابق هذه القائمة مع قائمة "الاتصال بالمنزل".
   - قم بتكوين قائمة "الاتصال بالمنزل" لتحديد قائمة PSNs التي تم فصلها بفاصلة. تأكد من إضافة منفذ بوابة إمداد العميل باستخدام التنسيق FQDN:port أو IP:port.
     للعثور على منفذ CPP أو تعديله، انتقل إلى مركز العمل > الوضع > إمداد العميل> مدخل إمداد العميل، حدد المدخل قيد الاستخدام، وتوسع إعدادات المدخل، وابحث عن منفذ HTTP.



تكوين ملف تعريف وضع الوكيل



Posture Protocol

Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Number of retries allowed for a message.
Discovery host		Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List	2 PSN(s)	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules *	*.aaamex.com	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List	ise30baaamex.aaamex.com:8443,ise30cmexaaa.a	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

تكوين بروتوكول الوضع في ملف تعريف وضعية العميل

5. في علامة التبويب المواراد، انقر فوق إضافة>تكوين الوكيل. حدد حزمة Cisco Secure Client ووحدة التوافق النمطية التي سيتم إستخدامها.

⚠ تحذير: إذا تم نشر Cisco Secure Client مسبقا على العملاء، فتأكد من تطابق الإصدار الموجود على ISE مع الإصدار الموجود على نقاط النهاية. إذا تم إستخدام ASA أو FTD لنشر الويب، يمكن أن يتطابق الإصدار الموجود على هذا الجهاز كذلك.

---

6. قم بالتمرير لأسفل إلى قسم تحديد الوضع وحدد ملف التعريف الذي تم إنشاؤه في الخطوة 1. انقر فوق إرسال في أسفل الصفحة لحفظ التكوين.

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1.2.042

* Configuration Name:

SecureClient Configuration Redirectionless

Description:

Redirectionless Lab Call Home List 1

Description Value Notes

* Compliance Module CiscoSecureClientComplianceModuleWindows

Cisco Secure Client Module Selection

ISE Posture ☑

VPN ☑

Zero Trust Access ☐

Network Access Manager ☐

Secure Firewall Posture ☐

Network Visibility ☐

Umbrella ☐

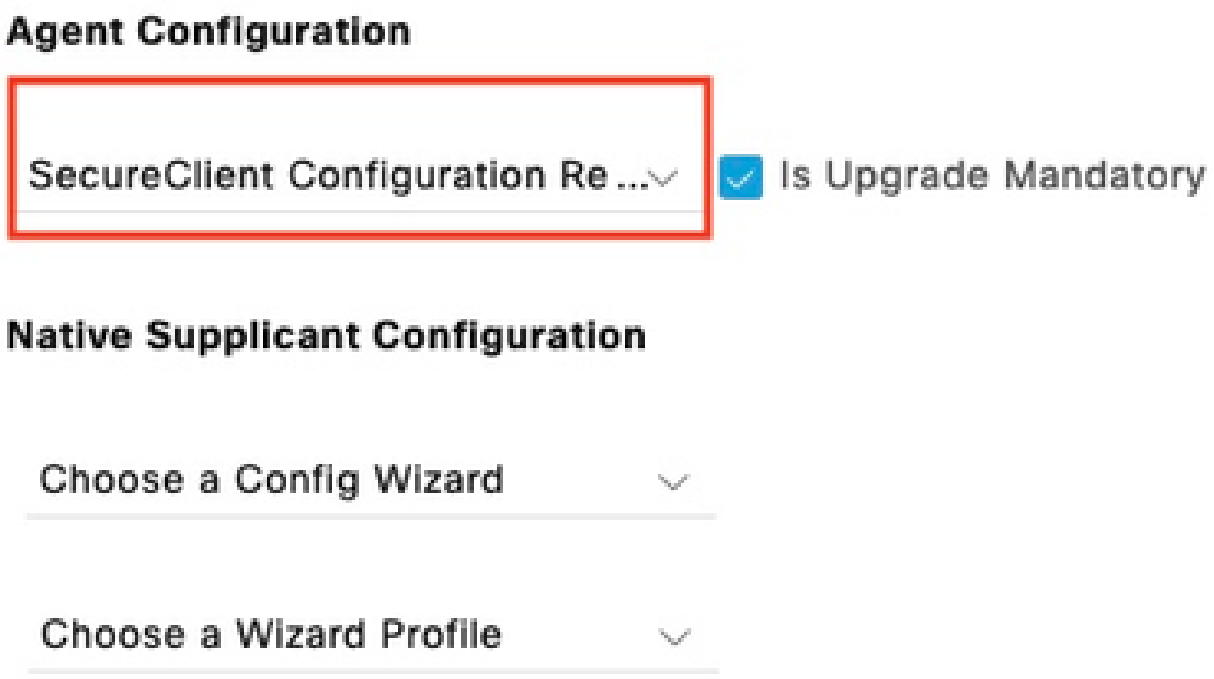
Start Before Logon ☐

Diagnostic

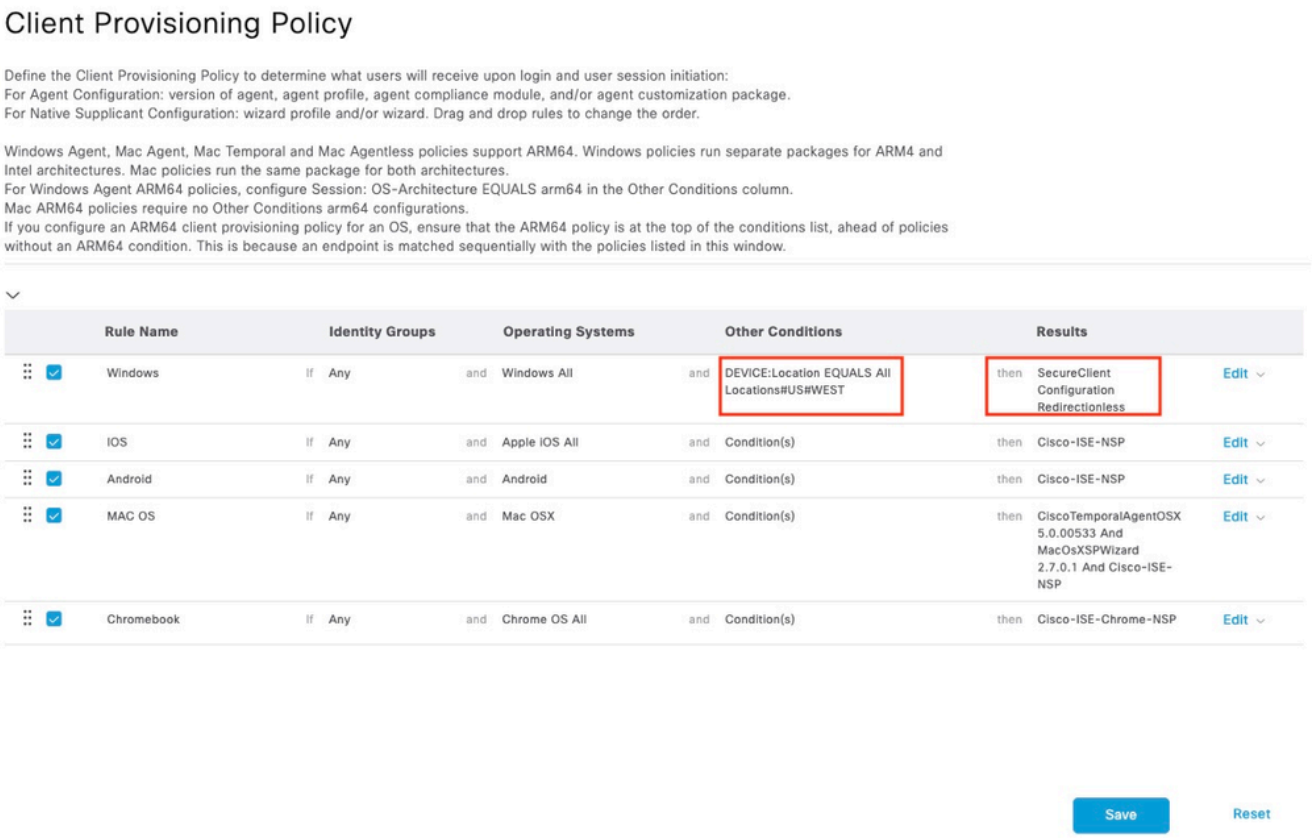
7. انتقل إلى مركز العمل> الوضع > إمداد العميل
>نهج إمداد العميل. حدد موقع النهج المستخدم في نظام التشغيل المطلوب وانقر فوق تحرير. انقر فوق علامة + في عمود النتائج وحدد التكوين للوكيل من الخطوة 5 أسفل قسم تكوين الوكيل". انقر فوق حفظ في الجزء السفلي من الصفحة.

ملاحظة: في حالة قوائم "الاتصال بالمنزل" المتعددة، أستخدم حقل الشروط الأخرى لدفع ملف التعريف الصحيح إلى العملاء المتفقين. في هذا المثال، يتم إستخدام "مجموعة مواقع الأجهزة" لتحديد ملف تعريف الوضع الذي يتم دفعه في النهج.

تلميح: إذا تم تكوين سياسات توفير عملاء متعددة لنفس نظام التشغيل، فمن المستحسن أن تكون هذه السياسات خاصة بشكل متبادل، أي أن العميل المحدد يمكنه فقط تنفيذ سياسة واحدة في كل مرة. يمكن إستخدام سمات RADIUS تحت عمود شروط أخرى للتمييز بين سياسة وأخرى.



تكوين الوكيل في نهج توفير العميل



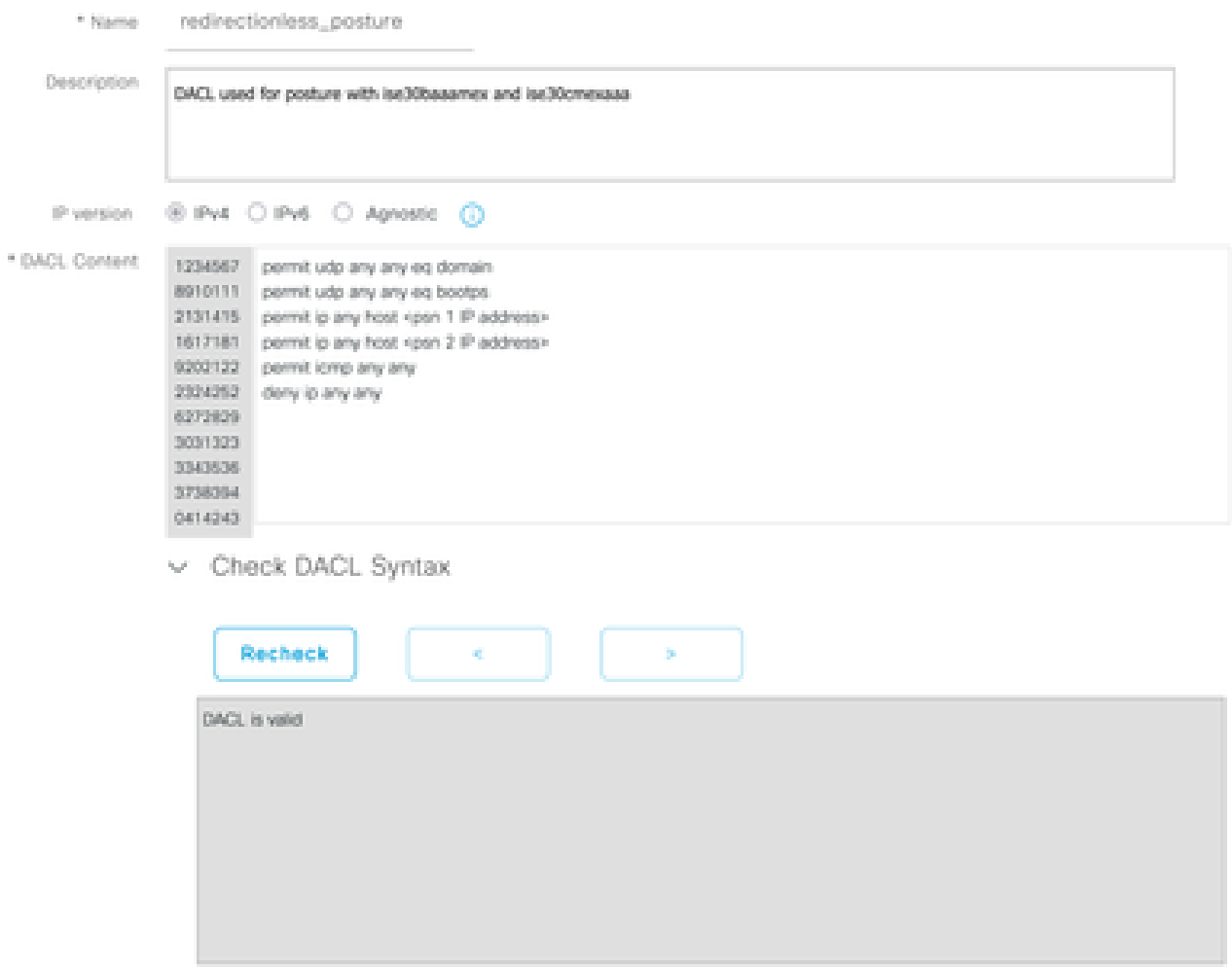
نهج توفير العميل

8. كرر الخطوات من 4 إلى 7 لكل قائمة "الاتصال بالمنزل" وملف تعريف الوضع المتوافق قيد الاستخدام. للبيئات المختلطة، يمكن إستخدام نفس التوصيفات لعملاء إعادة التوجيه.

الاعتماد

ملف تعريف التخويل

1. انتقل إلى السياسة >عناصر السياسة>النتائج>التفويض > قوائم التحكم في الوصول (ACL) القابلة للتنزيل وانقر فوق إضافة.
2. قم بإنشاء قائمة تحكم في الوصول إلى البنية الأساسية (DACL) للسماح بحركة المرور إلى DNS و DHCP (إذا تم إستخدامها) و ISE PSNs وحظر حركة المرور الأخرى. تأكد من السماح لأي حركة مرور أخرى ضرورية للوصول قبل الوصول المتوافق النهائي.



تهيئة DACL

permit udp any any eq domain
permit udp any any eq bootps
permit ip any host

permit ip any host

deny ip any any

⚠ تحذير: لا يمكن لبعض أجهزة الطرف الثالث دعم قوائم التحكم في الوصول إلى النقل (DACLs)، في مثل هذه الحالات من الضروري إستخدام معرف عامل التصفية

⚠ أو سمات المورد المحددة الأخرى. راجع وثائق المورد للحصول على مزيد من المعلومات. إذا لم يتم إستخدام قوائم التحكم في الوصول للبنية الأساسية (DACL)، فتأكد من تكوين قائمة التحكم في الوصول (ACL) المطابقة في جهاز الشبكة.

3. انتقل إلى السياسة>عناصر السياسة>النتائج>التفويض>ملفات تعريف التفويض وانقر فوق إضافة. إعطاء اسم لملف تعريف التخويل وتحديد اسم قائمة التحكم بالوصول (DACL) من المهام المشتركة. من القائمة المنسدلة، حدد قائمة التحكم في الوصول الخاصة بالمنفذ (DACL) التي تم إنشاؤها في الخطوة 2.

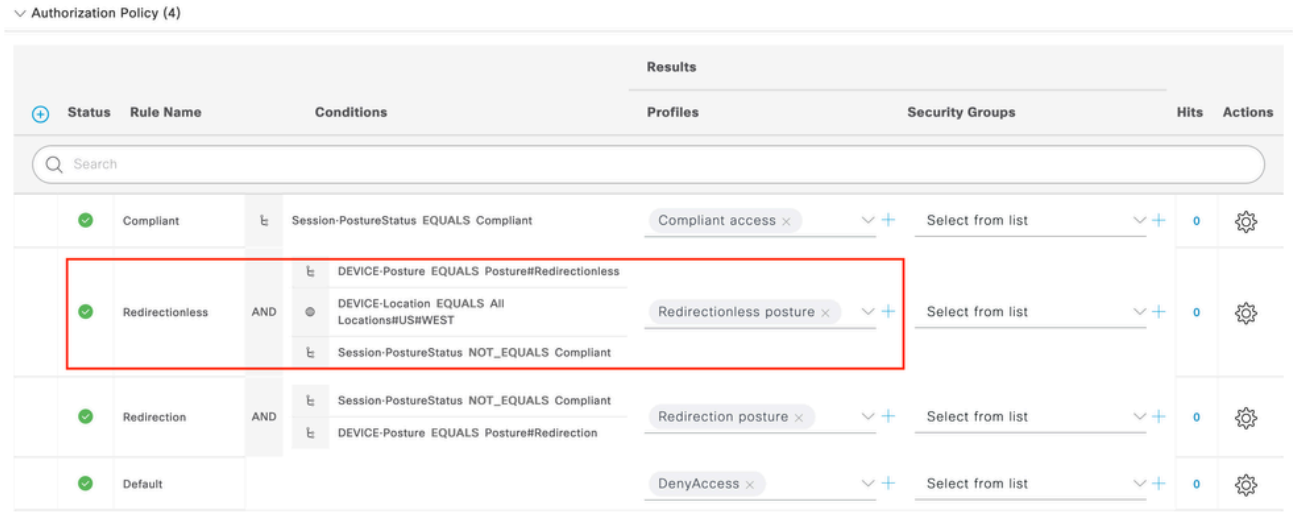
ملف تعريف التخويل

ملاحظة: إذا لم يتم إستخدام قوائم التحكم في الوصول الخاصة بالمنفذ (DACL)، فاستخدم Filter-ID من المهام المشتركة أو إعدادات السمة المتقدمة للضغط على اسم قائمة التحكم في الوصول (ACL) المقابل.

4. كرر الخطوات من 1 إلى 3 لكل قائمة "الاتصال بالمنزل" قيد الاستخدام. بالنسبة للبيئات المختلطة، يكون من الضروري وجود توصيف تخويل واحد فقط لإعادة التوجيه. تكوين ملف تعريف التخويل لإعادة التوجيه خارج نطاق هذا المستند.

سياسة التخويل

1. انتقل إلى النهج >مجموعات النهج وافتح مجموعة السياسات قيد الاستخدام أو قم بإنشاء مجموعة جديدة.
2. قم بالتمرير لأسفل إلى قسم نهج التخويل. قم بإنشاء سياسة تخويل باستخدام Session PostureStatus NOT_EQUALS متوافق وحدد ملف تعريف التخويل الذي تم إنشاؤه في القسم السابق.



سياسات التخويل

3. كرر الخطوة 2 لكل ملف تعريف تخويل مع إستخدام قائمة "الاتصال بالمنزل" المقابلة لها. بالنسبة للبيئات المختلطة، يلزم وجود سياسة تخويل واحدة فقط

لإعادة التوجيه.

استكشاف الأخطاء وإصلاحها

متوافق مع Cisco Secure Client و Posture غير قابل للتطبيق (معلق) على ISE

جلسات عمل بسيطة/وهمية

يمكن أن يؤدي وجود جلسات عمل وهمية في النشر إلى إنشاء حالات فشل متقطعة وعشوائية على ما يبدو مع اكتشاف الوضع غير القابل لإعادة التوجيه مما يؤدي إلى إحتجاز المستخدمين في وضع غير معروف/غير قابل للتطبيق على ISE بينما تظهر واجهة مستخدم Cisco Secure Client وصول متوافق.

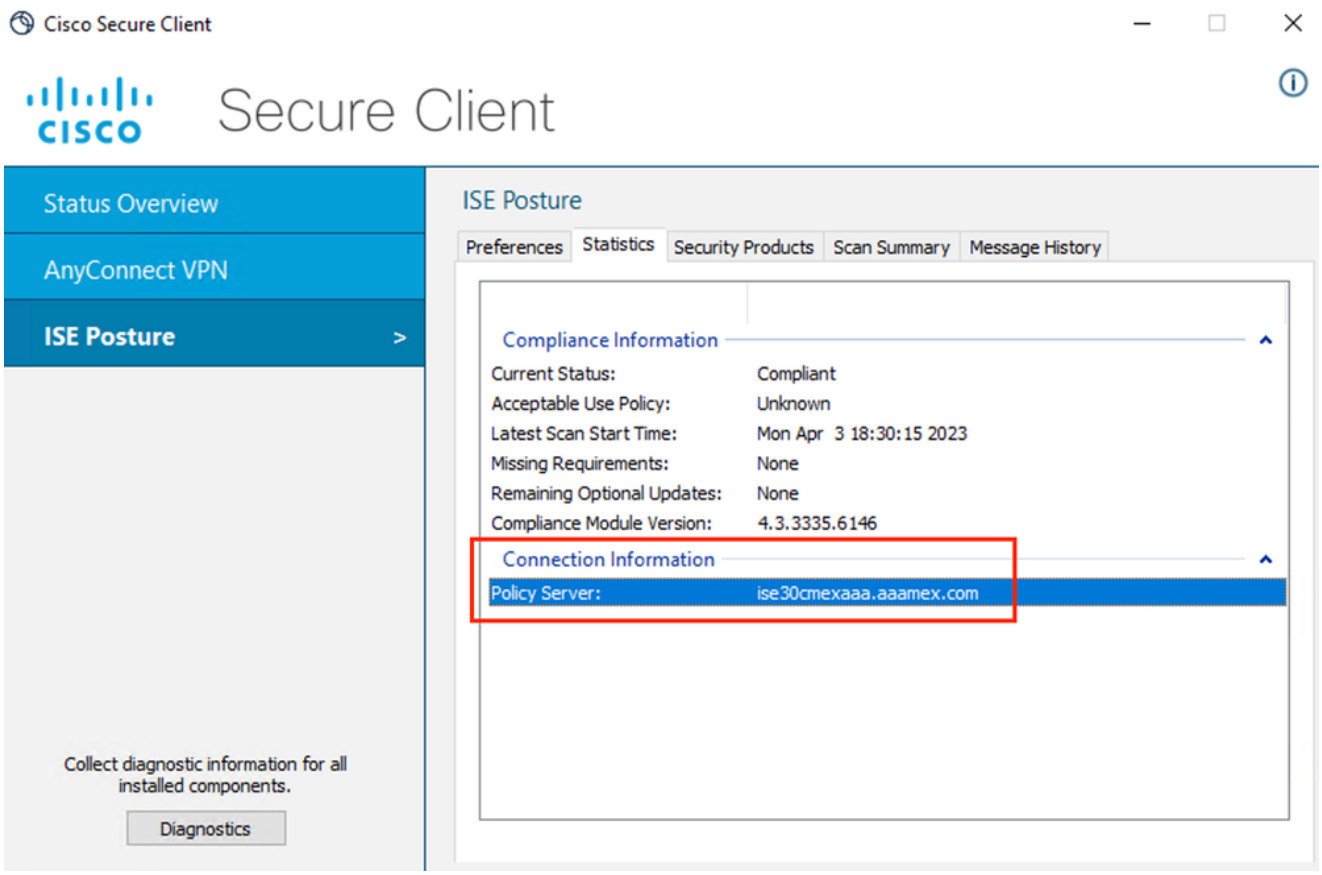
جلسات العمل القديمة هي جلسات قديمة لم تعد نشطة. يتم إنشاؤها بواسطة طلب مصادقة وبداية محاسبة، ولكن لا يتم تلقي أي توقف محاسبي على PSN لمسح الجلسة.

الجلسات الوهمية هي جلسات لم تكن نشطة في الواقع في شبكة PSN معينة. يتم إنشاؤها بواسطة تحديث مؤقت للمحاسبة، ولكن لا يتم تلقي أي توقف محاسبي على PSN لمسح الجلسة.

التعرف على

لتحديد مشكلة في جلسة عمل وهمية/وهمية، تحقق من PSN المستخدم في مسح النظام على العميل وقارن مع PSN الذي يقوم بتنفيذ المصادقة:

1. في واجهة مستخدم العميل الآمن من Cisco، انقر فوق رمز التروس في الركن الأيسر السفلي. من القائمة اليسرى، افتح قسم وضعية محرك خدمات الهوية (ISE) وانتقل إلى علامة تبويب الإحصائيات. لاحظ خادم النهج في "معلومات الاتصال".



Policy Server ل ISE Posture (وضعية محرك خدمات الهوية (ISE)) في Cisco Secure Client

2. في سجلات ISE RADIUS المباشرة، لاحظ ما يلي:
   - تغيير في حالة الوضع
   - تغيير في الخادم
   - لا يوجد تغيير في سياسة التخويل وملف تعريف التخويل
   - لا يوجد سجل CoA مباشر

Time	Status	Details	Repea...	Identity	Endpoint...	Authorization Policy	Server	Posture Status	Authorization Profiles
Apr 03, 2023 07:32:52.3...			0	redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30cmexaaa	Compliant	Redirectionless posture
Apr 03, 2023 07:32:40.7...				#ACSACL#-IP-...			ise30baaamex		
Apr 03, 2023 07:32:40.6...				redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30baaamex	NotApplicable	Redirectionless posture

السجلات الحية لجلسة العمل السطحية/الوهمية

3. افتح جلسة عمل Live أو آخر تفاصيل سجل حي للمصادقة. انتبه إلى خادم النهج، إذا كان مختلفا عن الخادم الملاحظ في الخطوة 1، فإن ذلك يشير إلى وجود مشكلة في جلسات العمل البسيطة/الوهمية.

Overview

Event	5200 Authentication succeeded
Username	redirectionless
Endpoint Id	00:50:56:B3:3E:0E
Endpoint Profile	Windows10-Workstation
Authentication Policy	Posture Lab >> Default
Authorization Policy	Posture Lab >> Redirectionless
Authorization Result	Redirectionless posture

Authentication Details

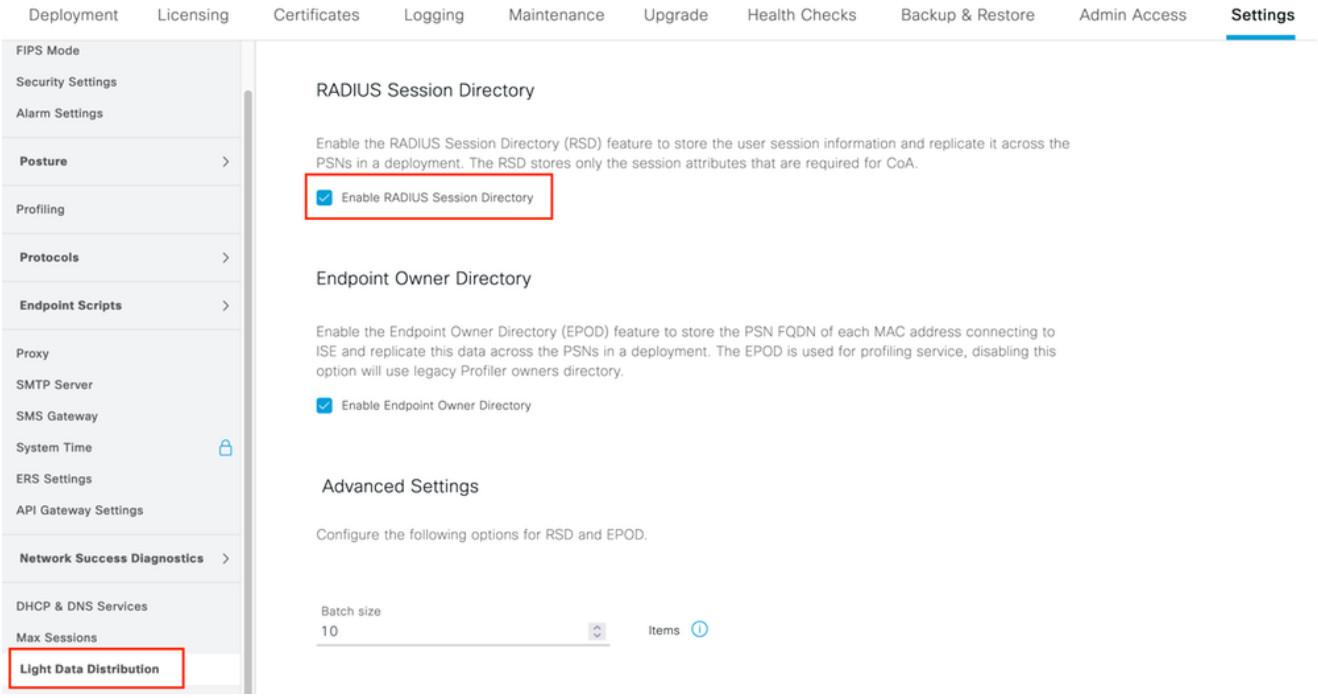
Source Timestamp	2023-04-03 19:32:40.691
Received Timestamp	2023-04-03 19:32:40.691
Policy Server	ise30baaamex
Event	5200 Authentication succeeded
Username	redirectionless

خادم النهج الموجود في تفاصيل السجل المباشر

الحل

تقوم إصدارات ISE بعد تصحيح ISE 2.6 و 2.7 تصحيح 3 بتطبيق دليل جلسة RADIUS كحل لسيناريو جلسة العمل البسيطة/الوهمية في تدفق تموضع بدون إتجاه.

1. انتقل إلى إدارة>نظام> إعدادات>توزيع بيانات ضوئي وتحقق من تمكين خانة الاختيار تمكين دليل جلسة عمل RADIUS.



تمكين دليل جلسة RADIUS

2. من واجهة سطر أوامر (CLI) ISE، تحقق من أن خدمة مراسلة ISE قيد التشغيل على جميع شبكات PSN من خلال تشغيل الأمر show application status ise.

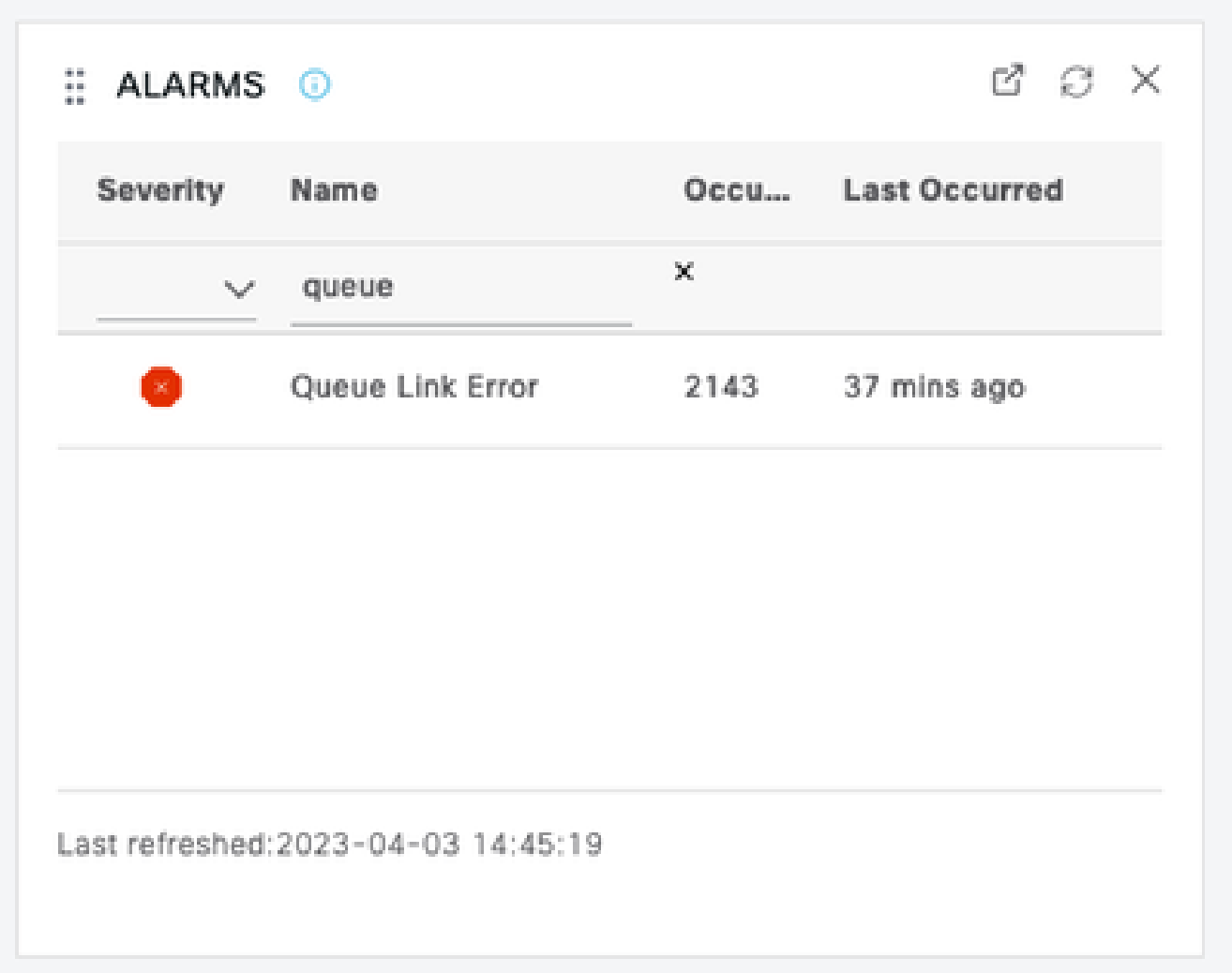
```
ise30cmexaaa/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          12434
Database Server                        running          112 PROCESSES
Application Server                     running          33093
Profiler Database                      running          19622
ISE Indexing Engine                    running          42923
AD Connector                           running          60317
M&T Session Database                   running          19361
M&T Log Processor                      running          33283
Certificate Authority Service          disabled
EST Service                            disabled
SXP Engine Service                     disabled
Docker Daemon                          running          14791
TC-NAC MongoDB Container               running          18594
TC-NAC Core Engine Container           running          18981
VA Database                            running          53465
VA Service                             running          53906
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID WMI Service                  running          55480
PassiveID Syslog Service               running          56312
PassiveID API Service                  running          57153
PassiveID Agent Service                running          58079
PassiveID Endpoint Service             running          59138
PassiveID SPAN Service                 running          60059
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          16526
ISE API Gateway Database Service       running          18463
ISE API Gateway Service                running          23052
```

خدمة مراسلة ISE قيد التشغيل

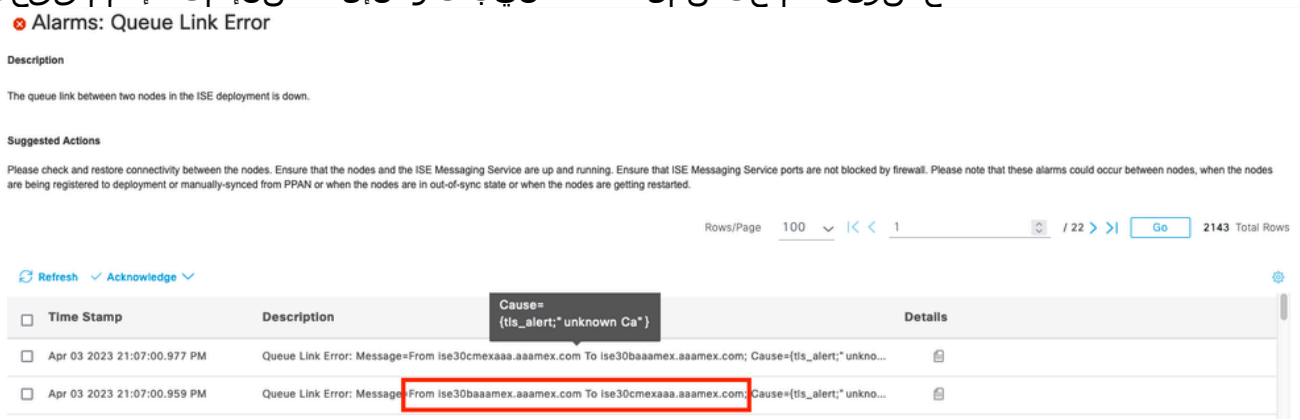
> ملاحظة: تشير هذه الخدمة إلى طريقة الاتصال التي يتم إستخدامها ل RSD بين شبكات PSN ويمكن تشغيلها بغض النظر عن حالة إعداد خدمة ISE Messaging ل syslog التي يمكن تعييناها من واجهة مستخدم ISE.

3. انتقل إلى لوحة معلومات ISE وحدد موقع dashlet Alarm. تحقق من وجود أي تنبيهات خطأ لارتباط قائمة الانتظار. انقر اسم المنبه لترى المزيد من التفاصيل.



تنبيهات خطأ ارتباط قائمة الانتظار

4. تحقق مما إذا تم إنشاء الإنذارات بين PSNs المستخدمة للوضع.



تفاصيل تنبيه خطأ ارتباط قائمة الانتظار

5. قم بالمرور فوق وصف التنبيه للاطلاع على التفاصيل الكاملة والإحاطة علما بحقل السبب. السببان الأكثر شيوعا لخطأ ارتباط قائمة الانتظار هما:
   - المهلة: تشير إلى أنه لا تتم الاستجابة للطلبات التي يتم إرسالها بواسطة عقدة إلى عقدة أخرى على المنفذ 8671 داخل الحد. للإصلاح، تحقق من السماح بمنفذ TCP 8671 بين العقد.
   - مرجع مصدق غير معروف: تشير إلى أن سلسلة الشهادات التي توقع شهادة ISE

Messaging غير صالحة أو غير مكتملة. لتصحيح هذا الخطأ:

a. انتقل إلى الإدارة > النظام > الشهادات>طلبات توقيع الشهادات.
b. انقر فوق إنشاء طلبات توقيع الشهادات (CSR).
c. من القائمة المنسدلة، حدد ISE Root CA وانقر فوق إستبدال سلسلة شهادات ISE Root CA.
إذا لم يتوفر ISE Root CA، انتقل إلى المرجع المصدق>إعدادات CA الداخلية وانقر فوق تمكين مرجع الشهادة، ثم عد إلى CSR وأعد إنشاء المرجع المصدق الجذر.
d. قم بإنشاء CSR جديد وحدد خدمة مراسلة ISE من القائمة المنسدلة.
e. حدد جميع العقد من النشر وأعد إنشاء الشهادة.

ملاحظة: من المتوقع مراقبة عمليات التنبيه بخطأ إرتباط قائمة الانتظار التي تتسبب في رفض CA أو Econnrejected غير معروف أثناء إعادة إنشاء الشهادات. مراقبة التنبيهات بعد إنشاء الشهادة لتأكيد حل المشكلة.

الأداء

التعرف على

قد تؤثر مشاكل الأداء مثل الاستخدام العالي لوحدة المعالجة المركزية (CPU) ومتوسط الحمل المرتفع المرتبط بوضعية عدم التوجيه على PSN وكذلك عقد MnT، وغالبا ما تكون مصحوبة أو مسبوقة بهذه الأحداث:

- عشوائي أو متقطع، لم يكتشف أي خادم نهج أخطاء، في Cisco Secure Client.
- وصل الحد الأقصى للموارد إلى تقارير تجمع مؤشرات الترابط لخدمة المدخل إلى أحداث قيمة الحد. انتقل إلى العمليات> تقارير > تقارير > تدقيق > تدقيق العمليات لعرض التقارير.
- Posture Query إلى البحث عن MNT وه عالي التنبيه. يتم إنشاء هذه التنبيهات فقط على ISE 3.1 والإصدارات الأحدث.

الحل

وإذا تأثر أداء النشر بوضعية عدم التوجيه، فإن ذلك غالبا ما يدل على عدم فعالية التنفيذ. ويوصى بتنقيح هذه الجوانب:

- عدد شبكات PSN المستخدمة لكل قائمة "الاتصال بالمنزل". فكر في تقليل عدد شبكات PSN التي يمكن إستخدامها للوضع لكل نقطة نهاية أو جهاز شبكة وفقا للتصميم.
- منفذ مدخل تزويد العميل في قائمة الاتصال الرئيسية. تأكد من تضمين رقم منفذ المدخل بعد IP أو FQDN لكل عقدة.

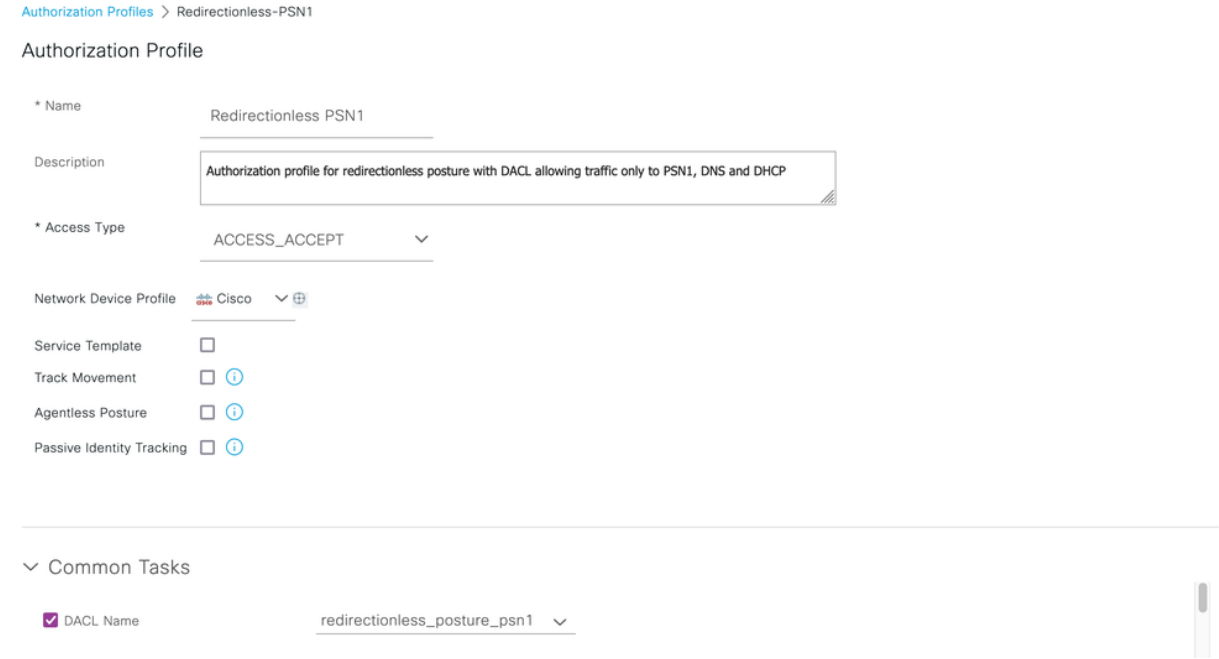
للتخفيف من التأثير:

1. قم بمسح ConnectionData.xml من نقاط النهاية من خلال إزالة الملف من مجلد Cisco

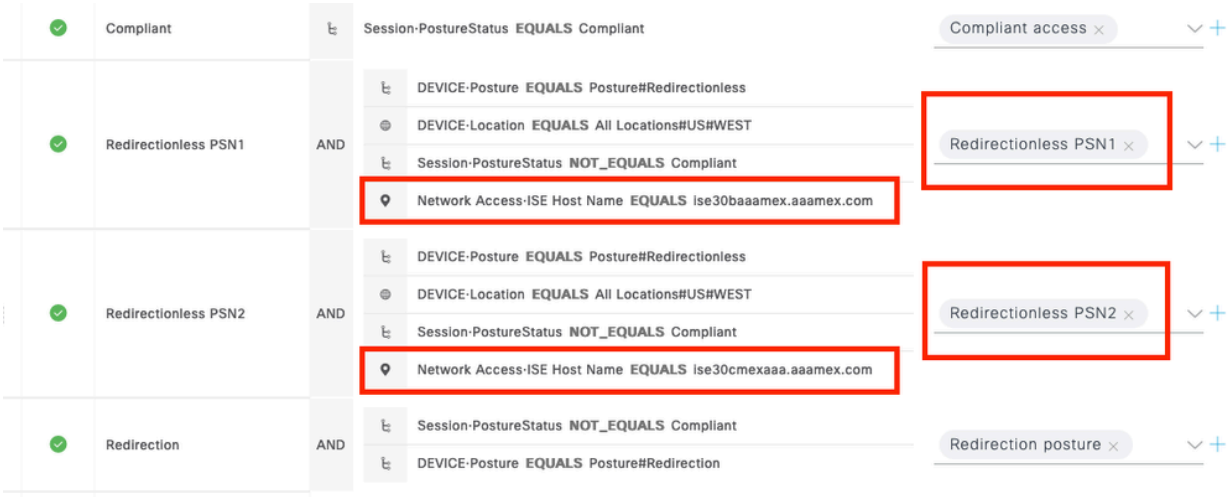
Secure Client وإعادة تشغيل خدمة ISE Posture (وضعية محرك خدمات الهوية (ISE)) أو Cisco Secure Client. في حالة عدم إعادة تشغيل الخدمات، يتم إعادة إنشاء الملف القديم والتي يتم تفعيل التغييرات. يمكن تنفيذ هذا الإجراء أيضا بعد مراجعة قوائم الاتصال بالمنزل وتعديلها.

2. إستخدام قوائم التحكم في الوصول الخاصة بالمنفذ (DACL) أو قوائم التحكم في الوصول الأخرى لحظر حركة المرور إلى شبكات ISE PSN لاتصالات الشبكة حيث لا تكون ذات صلة:

- بالنسبة للاتصالات التي لا يتم فرض الوضع فيها في سياسات التخويل، ولكن يتم تطبيق ذلك على نقاط النهاية مع وحدة Cisco Secure Client ISE Posture Module المثبتة، قم بحظر حركة مرور البيانات من العملاء إلى جميع شبكات ISE PSN لمنافذ TCP 8905 ومنفذ بوابة إمداد العميل. يوصى بهذا الإجراء للوضع مع تنفيذ إعادة التوجيه أيضا.
- بالنسبة للاتصالات التي يتم فرض الوضع فيها في سياسات التخويل، السماح بحركة مرور البيانات من العملاء إلى PSN المصادق ومنع حركة مرور البيانات إلى PSN الأخرى في النشر. يمكن تنفيذ هذا الإجراء بشكل مؤقت أثناء مراجعة التصميم.



ملف تعريف التخويل مع DACL ل PSN واحد



نهج التخويل لكل PSN

الحسابات

تعد عملية محاسبة RADIUS ضرورية لإدارة جلسات العمل على ISE. نظرا لأن الوضع يعتمد على جلسة عمل نشطة ليتم تنفيذها، فإن التكوين المحاسبي غير الصحيح أو عدم تكوينه يمكن أن يؤثر أيضا على اكتشاف الوضع وأداء ISE. من المهم التحقق من تكوين عملية المحاسبة بشكل صحيح على جهاز الشبكة لإرسال طلبات المصادقة وبدء عملية المحاسبة وتوقف عملية المحاسبة وتحديثات عملية المحاسبة إلى PSN واحد لكل جلسة عمل.

للتحقق من الحزم المحاسبية المستلمة على ISE، انتقل إلى العمليات > تقارير > تقارير > نقاط النهاية والمستخدمين > محاسبة RADIUS.

معلومات ذات صلة

- الدعم الفني والتنزيلات من Cisco

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 دائماً إلى المستند الإنجليزي الأصلي (الرابط متوفر).