4.0 رادصإلا AnyConnect ليكو رهظي ال ISE ءاطخأ أشاكتسأ ليلد يف NAC ةيعضوو اهحالصإو

المحتويات

المقدمة

يوفر محرك خدمات الهوية (ISE) إمكانات إعادة الوضع التي تتطلب إستخدام عميل التحكم في الدخول إلى الشبكة (NAC) (لنظام التشغيل Microsoft Windows أو Macintosh أو عبر وحدة التحكم) أو AnyConnect الإصدار 4.0. تعمل الوحدة النمطية AnyConnect Version 4.0 ISE Posture Module تماما مثل وكيل NAC، وبالتالي تتم الإشارة إليها باسم وكيل NAC في هذا المستند. من أكثر الأعراض شيوعا لفشل الوضع للعميل هو أن عامل NAC لا يظهر لأن سيناريو العمل يتسبب دائما في ظهور نافذة عميل NAC وتحليلها على الكمبيوتر. يساعدك هذا المستند على تضييق الأسباب المتعددة التي يمكن أن تؤدي إلى فشل الوضعية، مما يعني أن وكيل NAC لا يظهر. ليس المقصود منه أن يكون شاملا لأن سجلات عوامل NAC يمكن فك ترميزها فقط بواسطة مركز المساعدة التقنية (TAC) من Cisco، ولأن الأسباب الجذرية المحتملة عديدة؛ ومع ذلك، فإنه يهدف إلى توضيح الحالة وتحديد المشكلة بشكل أكبر من مجرد "لا يظهر العميل مع تحليل الوضع" وربما يساعدك على حل الأسباب الأكثر شيوعا.

المتطلبات الأساسية

المتطلبات

تتم كتابة السيناريوهات والأعراض والخطوات المدرجة في هذا المستند لك لاستكشاف المشاكل وإصلاحها بعد اكتمال الإعداد الأولي بالفعل. للحصول على التكوين الأولي، ارجع إلى Posture Services في دليل تكوين Cisco ISE على Cisco.com.

المكونات المستخدمة

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

- ISE الإصدار x.1.2
- وكيل NAC ل ISE، الإصدار x.4.9
- AnyConnect، الإصدار 4.0

ملاحظة: ينبغي أن تكون المعلومات قابلة للتطبيق أيضا على إصدارات أخرى من التصنيف التصويري الموحد (ISE) ما لم تشير ملاحظات الإصدار إلى تغييرات سلوكية رئيسية.

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

منهجية أستكشاف الأخطاء وإصلاحها

ما الذي يجعل العميل يظهر؟

يظهر العميل عندما يكتشف عقدة ISE. إذا شعر العميل بأنه لا يتمتع بحق الوصول الكامل إلى الشبكة وهو في سيناريو إعادة توجيه الوضع، فإنه يبحث باستمرار عن عقدة ISE.

هناك مستند Cisco.com يشرح تفاصيل عملية اكتشاف الوكيل: عملية اكتشاف عميل التحكم في الدخول إلى الشبكة (NAC) لمحرك خدمات الهوية. لتجنب تكرار المحتوى، يناقش هذا المستند فقط النقطة الأساسية.

عندما يتصل عميل، فإنه يخضع لمصادقة RADIUS (تصفية MAC أو 802.1x) في نهايتها، ويقوم ISE بإرجاع قائمة التحكم في الوصول (ACL) لإعادة التوجيه وعنوان URL لإعادة التوجيه إلى جهاز الشبكة (المحول أو جهاز الأمان القابل للتكيف (ASA) أو وحدة التحكم اللاسلكية) لتقييد حركة مرور العميل للسماح له فقط بالحصول على حلول عنوان IP وخادم اسم المجال (DNS). تتم إعادة توجيه جميع حركة مرور HTTP(s) التي تأتي من العميل إلى URL فريد على ISE ينتهي ب CPP (وضع العميل والإمداد)، باستثناء حركة المرور الموجهة إلى مدخل ISE نفسه. يرسل وكيل NAC حزمة HTTP GET عادية إلى البوابة الافتراضية. إذا لم يتلقى العميل أي إجابة أو أي إجابة أخرى غير إعادة توجيه CPP، فإنه يعتبر نفسه أن لديه اتصال كامل ولا يتابع الحالة. إذا كان يستلم إستجابة HTTP التي هي إعادة توجيه إلى عنوان URL ل CPP في نهاية عقدة ISE معينة، فإنه يواصل عملية الوضع وجهات الاتصال التي تقوم ب ISE العقدة. يظهر فقط ويبدأ التحليل عندما يستلم بنجاح تفاصيل الوضع من عقدة ISE تلك.

يصل عامل NAC أيضا إلى عنوان IP لمضيف الاكتشاف الذي تم تكوينه (لا يتوقع أن يتم تكوين أكثر من واحد). هو يتوقع أن يتم إعادة توجيهه هناك أيضا من أجل الحصول على عنوان URL لإعادة التوجيه باستخدام معرف الجلسة. إذا كان عنوان IP للاكتشاف عبارة عن عقدة ISE، فلا يتم متابعته لأنه ينتظر إعادة التوجيه للحصول على معرف الجلسة الصحيح. لذلك لا يكون مضيف الاكتشاف عادة ضروريا، ولكن يمكن أن يكون مفيدا عند ضبطه على أنه أي عنوان IP في نطاق قائمة التحكم في الوصول لإعادة التوجيه لتشغيل إعادة التوجيه (مثل سيناريوهات VPN، على سبيل المثال).

الأسباب المحتملة

إعادة التوجيه لا يحدث

وهذا هو السبب الأكثر شيوعا حتى الآن. للتحقق من الصحة أو الإبطال، افتح مستعرض على الكمبيوتر الشخصي حيث لا يظهر الوكيل، ثم راجع ما إذا تم إعادة توجيهك إلى صفحة تنزيل عامل الوضع عند كتابة أي عنوان URL. يمكنك أيضا كتابة عنوان IP عشوائي مثل http://1.2.3.4 لتجنب مشكلة DNS المحتملة (إذا تم إعادة توجيه عنوان IP ولكن اسم موقع ويب لا، يمكنك النظر إلى DNS).

إن يحصل أنت أعدت، أنت ينبغي جمعت الوكيل سجل دعم حزمة (مع الوضع ووحدة سويسرية أن يضبط أسلوب) اتصل cisco TAC. وهذا يشير إلى أن العامل يكتشف عقدة ISE ولكن يفشل شيء ما أثناء العملية للحصول على بيانات الوضع.

إذا لم يحدث أي إعادة توجيه، لديك السبب الأول، الذي لا يزال يتطلب المزيد من التحقيق في السبب الجذري. تتمثل البداية الجيدة في التحقق من التكوين الموجود على جهاز الوصول إلى الشبكة (وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) أو المحول) والانتقال إلى العنصر التالي في هذا المستند.

لم يتم تثبيت السمات على جهاز الشبكة

هذا إصدار حالة فرعية من **ال redirection لا يقع** سيناريو. إذا لم يحدث إعادة التوجيه، فإن الأمر الأول هو التحقق من (حيث تحدث المشكلة على عميل معين) وضع العميل بشكل صحيح في الحالة الصحيحة بواسطة المحول أو طبقة الوصول اللاسلكية.

وفيما يلي مثال على إخراج الأمر **show access-session interface <interface number>** detail (قد تحتاج إلى إضافة **تفاصيل** في النهاية على بعض الأنظمة الأساسية) على المحول حيث يتم توصيل العميل. يجب التحقق من أن الحالة هي "نجاح المصادقة"، وأن قائمة التحكم بالوصول (ACL) الخاصة بإعادة توجيه URL تشير بشكل صحيح إلى قائمة التحكم بالوصول (ACL) المخصصة لإعادة التوجيه، وأن إعادة توجيه URL يشير إلى عقدة ISE المتوقعة مع **CPP** في نهاية URL. حقل قائمة التحكم بالوصول (ACL) إلى ACS غير إلزامي لأنه يظهر فقط إذا قمت بتكوين قائمة وصول قابلة للتنزيل على ملف تعريف التخويل على ISE. ومع ذلك، من المهم النظر إليها والتحقق من عدم وجود تعارض مع قائمة التحكم في الوصول (ACL) المعاد توجيهها (راجع المستندات حول تكوين الوضع في حالة الشك).

```
01-SW3750-access#show access-sess gi1/0/12 det
                 Interface: GigabitEthernet1/0/12
                    MAC Address:  000f.b049.5c4b
                IP Address:  192.168.33.201
             User-Name:  00-0F-B0-49-5C-4B
                 Status:  Authz Success
                          Domain:  DATA
              Security Policy:  Should Secure
                   Security Status:  Unsecure
             Oper host mode:  single-host
                          Oper control dir:  both
          Authorized By:  Authentication Server
                           Vlan Policy:  N/A
                ACS ACL:  xACSACLx-IP-myDACL-51519b43
                           URL Redirect ACL:  redirect
?URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway
                sessionId=C0A82102000002D8489E0E84&action=cpp
                           Session timeout:  N/A
                           Idle timeout:  N/A
          Common Session ID:  C0A82102000002D8489E0E84
                     Acct Session ID:  0x000002FA
                     Handle:  0xF60002D9

                                :Runnable methods list

                                  Method   State
                               mab      Authc Success
```

دخلت in order to تحريت WLC أن يركض AireOS، **أبديت زبون تفصيل <mac address>**وأدخل **عرض زبون لاسلكي ماك عنوان <mac address> تفصيل** in order to تحريت WLC أن يركض cisco IOS-XE. بيانات مماثلة تعرض ويجب عليك التحقق من عنوان URL المعاد توجيهه وقوائم التحكم في الوصول (ACL) وإذا كان العميل في حالة "POSTURE_REQD" أو ما شابه (يختلف حسب إصدار البرنامج).

إذا لم تكن السمات موجودة، فيجب عليك فتح تفاصيل المصادقة في ISE الخاصة بالعميل الذي كنت تستكشف أخطائه (انتقل إلى **العمليات > المصادقة**) وتحقق في قسم النتائج من أن سمات إعادة التوجيه قد تم إرسالها. إذا لم يتم

إرسالها، يجب مراجعة سياسة التخويل لفهم سبب عدم إرجاع السمات لهذا العميل المعين. وعلى الأرجح أن إحدى هذه الحالات لم تكن متطابقة، لذا فهي فكرة طيبة أن نستكشف أخطائها وإصلاحها واحدا تلو الآخر.

تذكر أنه، فيما يتعلق بقوائم التحكم في الوصول (ACL) المعاد توجيهها من Cisco IOS®على عبارات الترخيص (لذلك يجب رفض عناوين ISE و DNS IP) بينما يقوم AireOS على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بإعادة التوجيه على عبارات الرفض (لذلك مسموح به ل ISE و DNS).

السمات في مكانها ولكن جهاز الشبكة لا يعيد التوجيه

السبب الرئيسي في هذه الحالة هو مشكلة تكوين. يجب مراجعة تكوين جهاز الشبكة مقابل دليل التكوين وأمثلة التكوين على Cisco.com. إن يكون هذا هو الحالة، المشكلة يتواجد عادة في كل ميناء أو منفذ نقطة (APs) من الشبكة أداة. إن لا، المشكلة أمكن وقعت فقط على بعض switchports أو بعض APs. إن يكون هذا هو الحالة، أنت ينبغي قارنت التشكيل من أن حيث المشكلة يقع بالمقارنة مع الميناء أو APs حيث الوضع يعمل جيد.

تكون نقاط الوصول من FlexConnect حساسة لأنه يمكن أن يكون لكل منها تكوين فريد ومن السهل إرتكاب خطأ في قائمة التحكم في الوصول أو شبكة VLAN في بعض نقاط الوصول وليس غيرها.

مشكلة أخرى شائعة هي أن شبكة VLAN الخاصة بالعميل لا تحتوي على SVI. يطبق هذا فقط إلى مفتاح ويناقش بالتفصيل في ISE حركة مرور redirection على المادة حفازة 3750 sery مفتاح. قد يبدو كل شيء جيدا من منظور السمات.

التدخل في قائمة الوصول القابلة للتنزيل (DACL)

إذا قمت بدفع قائمة التحكم في الوصول إلى البنية الأساسية (DACL) مرة أخرى إلى المحول (أو Airespace-ACL لوحدة التحكم اللاسلكية)، في نفس الوقت الذي يتم فيه دفع سمات إعادة التوجيه، فقد تقوم بحظر إعادة التوجيه. يتم تطبيق قائمة التحكم في الوصول للبنية الأساسية (DACL) أولا، كما تحدد ما يتم إسقاطه بالكامل وما يحدث ليتم معالجته. ثم يتم تطبيق قائمة التحكم في الوصول (ACL) المعاد توجيهها وتحديد ما يتم إعادة توجيهه.

ما يعنيه هذا بشكل ملموس هو أنه في معظم الوقت، سترغب في السماح بجميع حركات مرور HTTP و HTTPS في قائمة التحكم في الوصول الخاصة بك. إذا قمت بحظره، فلن يتم إعادة توجيهه لأنه سيتم إسقاطه قبل ذلك. إنها ليست مشكلة أمنية، نظرا لأنه سيتم إعادة توجيه حركة المرور غالبا على قائمة التحكم في الوصول (ACL) المعاد توجيهها بعد ذلك، لذلك فهي غير مسموح بها حقا على الشبكة؛ ومع ذلك، يلزمك السماح لهذين النوعين من حركة المرور في قائمة التحكم في الوصول الخاصة بالمنفذ (DACL) حتى تتوفر لهم الفرصة للوصول إلى قائمة التحكم في الوصول (ACL) المعاد توجيهها بعد ذلك مباشرة.

إصدار وكيل NAC غير صحيح

من السهل نسيان أنه تم التحقق من صحة إصدارات وكيل NAC المحددة مقابل إصدارات محددة من ISE. يقوم العديد من المسؤولين بترقية مجموعة ISE الخاصة بهم ونسيان تحميل إصدار وكيل NAC ذي الصلة في قاعدة بيانات نتائج توفير العميل.

إذا كنت تستخدم إصدار عميل NAC قديم لرمز ISE الخاص بك، فاعلم أنه قد يعمل ولكن قد لا يعمل أيضا. لذلك ليس مدهشا ان يعمل بعض الزبائن فيما لا يعمل الآخرون. إحدى طرق التحقق من ذلك هي الانتقال إلى قسم التنزيل في Cisco.com الخاص بإصدار ISE الخاص بك والتحقق من إصدارات وكيل NAC الموجودة. عادة، يتم دعم العديد من إصدارات ISE لكل إصدار. تجمع صفحة الويب هذه جميع المصفوفات: معلومات توافق Cisco ISE.

وكيل ويب HTTP قيد الاستخدام بواسطة العملاء

ومفهوم وكيل ويب HTTP هو أن العملاء لا يحلون عناوين IP الخاصة بموقع DNS على الويب بأنفسهم أو يتصلون بالمواقع مباشرة؛ بل يرسلون طلبهم ببساطة إلى الخادم الوكيل، الذي يتولى الأمر. المشكلة النموذجية التي تتعلق بالتكوين المعتاد هي أن العميل يقوم بحل موقع ويب (مثل www.cisco.com) من خلال إرسال HTTP GET

الخاص به مباشرة إلى الوكيل، والذي يتم اعتراضه وإعادة توجيهه بشكل صحيح إلى بوابة ISE. ومع ذلك، بدلا من إرسال HTTP التالي إلى عنوان IP لمدخل ISE، يستمر العميل في إرسال هذا الطلب إلى الوكيل.

في حالة ما إذا قررت عدم إعادة توجيه حركة مرور HTTP الموجهة إلى الوكيل، فسيتمتع المستخدمون لديك بحق الوصول المباشر إلى الإنترنت بالكامل (نظرا لأن جميع حركة المرور تمر عبر الوكيل) دون المصادقة أو إعادة الوضع. يكمن الحل في تعديل إعدادات مستعرض العملاء بالفعل وإضافة إستثناء لعنوان ISE IP في إعدادات الوكيل. وبهذه الطريقة، عندما يتعين على العميل الوصول إلى ISE، فإنه يرسل الطلب مباشرة إلى ISE وليس إلى الوكيل. يؤدي هذا إلى تجنب التكرار غير المحدود حيث يتم إعادة توجيه العميل بشكل مستمر ولكن لا يرى صفحة تسجيل الدخول أبدا.

لاحظ أن وكيل NAC لا يتأثر بإعدادات الوكيل التي تم إدخالها في النظام ولا يزال يعمل بشكل طبيعي. هذا يعني أنه إذا كنت تستخدم وكيل ويب، فلن يمكنك على حد سواء أن يعمل اكتشاف عميل NAC (لأنه يستخدم المنفذ 80) وأن يضطر المستخدمون إلى تثبيت العميل ذاتيا بمجرد إعادة توجيههم إلى صفحة الوضع عند الاستعراض (نظرا لأن ذلك يستخدم منفذ الوكيل ولا يمكن للمحولات النموذجية إعادة التوجيه على منافذ متعددة).

تم تكوين مضيفات الاستكشاف في وكيل NAC

خاصة بعد ISE الإصدار 1.2، يوصى بعدم تكوين أي مضيف اكتشاف على وكيل NAC ما لم تكن لديك خبرة فيما يقوم به وما لا يقوم به. من المفترض أن يكتشف وكيل NAC عقدة ISE التي صادقت جهاز العميل من خلال اكتشاف HTTP. إذا كنت تعتمد على مضيفات الاكتشاف، فقد يكون لديك عميل NAC يتصل بعقدة ISE أخرى أكثر من تلك التي صادقت الجهاز والتي لا تعمل. يرفض ISE Version 1.2 وكيلا يكتشف العقدة من خلال عملية مضيف الاكتشاف لأنه يريد أن يحصل عميل NAC على معرف الجلسة من عنوان URL المعاد توجيهه، لذلك يتم إحباط هذه الطريقة.

في بعض الحالات، قد ترغب في تكوين مضيف اكتشاف. بعد ذلك يجب تكوينها باستخدام أي عنوان IP (حتى إذا لم يكن موجودا) سيتم إعادة توجيهه بواسطة قائمة التحكم في الوصول (ACL) المعاد توجيهها، ويجب أن لا تكون بشكل مثالي في الشبكة الفرعية نفسها الخاصة بالعميل (وإلا فإن العميل سيقوم ARP إلى أجل غير مسمى لها ولن يرسل أبدا حزمة اكتشاف HTTP).

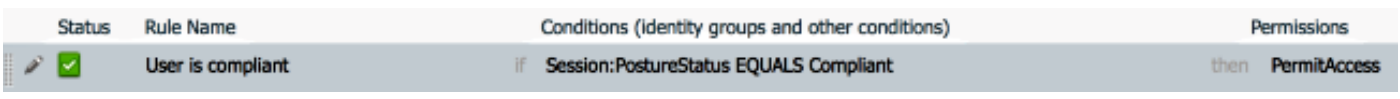
وكيل NAC لا يظهر في بعض الأحيان

عندما تكون المشكلة متقطعة بشكل أكبر وتجعلها إجراءات مثل إلغاء توصيل/نسخ اتصال الكبل/WiFi تعمل، فإنها تكون مشكلة أكثر دقة. قد تكون هناك مشكلة في معرفات جلسات RADIUS حيث يتم حذف معرف الجلسة على ISE by RADIUS Accounting (تعطيل المحاسبة لمعرفة ما إذا كانت تغير شيئا).

إذا كنت تستخدم ISE Version 1.2، فإن هناك إمكانية أخرى هي أن يرسل العميل العديد من حزم HTTP حتى لا يأتي أي منها من مستعرض أو وكيل NAC. يقوم ISE الإصدار 1.2 بمسح حقل وكيل المستخدم في حزم HTTP لمعرفة ما إذا كان يأتي من وكيل NAC أو متصفح، ولكن تقوم العديد من التطبيقات الأخرى بإرسال حركة مرور HTTP باستخدام حقل وكيل المستخدم ولا تذكر أي نظام تشغيل أو معلومات مفيدة. يرسل ISE الإصدار 1.2 بعد ذلك تغييرا في التفويض لقطع اتصال العميل. لا تتأثر الإصدار 1.3 من ISE بهذه المشكلة لأنها تعمل بطريقة مختلفة. الحل هو إما الترقية إلى الإصدار 1.3 أو السماح لجميع التطبيقات المكتشفة في قائمة التحكم في الوصول (ACL) المعاد توجيهها حتى لا يتم إعادة توجيهها إلى ISE.

عكس المشكلة: يظهر الوكيل بشكل متكرر

وقد تظهر مشكلة معاكسة عندما يظهر العميل فجأة، ويقوم بتحليل الوضع، ويتحقق من صحة العميل، ثم يظهر مرة أخرى بعد فترة قصيرة بدلا من السماح بتوصيل الشبكة والبقاء صامتا. يحدث هذا لأنه، حتى بعد الوضع الناجح، ما تزال حركة مرور HTTP تتم إعادة توجيهها إلى مدخل CPP على ISE. ومن الأفضل بعد ذلك المرور عبر سياسة تفويض ISE والتحقق من أن لديك قاعدة ترسل حق الوصول المسموح به (أو قاعدة مماثلة مع قوائم التحكم في الوصول والشبكات المحلية الظاهرية (VLANs) المحتملة) عندما ترى عميلا متوافقا وليس إعادة توجيه CPP مرة أخرى.



معلومات ذات صلة

- Posture Services على دليل تكوين Cisco ISE
- عملية اكتشاف وكيل NAC ل ISE
- إعادة توجيه حركة مرور ISE على المحول Catalyst 3750 Series Switch
- الدعم التقني والمستندات - Cisco Systems

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).