دمج Cisco ACS 5.x مع خادم الرموز المميز RSA SecureID

المحتويات

المقدمة

يوضح هذا المستند كيفية دمج الإصدار x.5 من نظام التحكم في الوصول (ACS) من Cisco مع تقنية مصادقة RSA SecureID.

معلومات أساسية

يدعم "مصدر المحتوى الإضافي الآمن من Cisco" خادم RSA SecureID كقاعدة بيانات خارجية.

تتكون مصادقة RSA SecureID ثنائية العوامل من رقم التعريف الشخصي للمستخدم (PIN) ورمز RSA SecureID مسجل بشكل فردي والذي يقوم بإنشاء أكواد الرمز المميز للاستخدام الأحادي استنادا إلى خوارزمية الرمز الزمني.

يتم إنشاء رمز مميز مختلف على فواصل زمنية ثابتة، عادة كل 30 أو 60 ثانية. يقوم خادم RSA SecureID بالتحقق من صحة رمز المصادقة الديناميكي هذا. كل رمز مميز RSA SecurID فريد، ولا يمكن التنبؤ بقيمة رمز مميز في المستقبل استنادا إلى الرموز المميزة السابقة.

وبالتالي، عندما يتم توفير رمز رمز مميز صحيح مع رقم تعريف شخصي (PIN)، هناك درجة عالية من اليقين بأن الشخص هو مستخدم صالح. وبالتالي، توفر خوادم RSA SecureID آلية مصادقة أكثر موثوقية من كلمات المرور التقليدية القابلة لإعادة الاستخدام.

يمكنك تكامل Cisco ACS 5.x مع تقنية مصادقة RSA SecureID بهذه الطرق:

- عامل SecureID ل RSA - تتم مصادقة المستخدمين باستخدام اسم المستخدم ورمز المرور من خلال بروتوكول RSA الأصلي.
- بروتوكول RADIUS - تتم مصادقة المستخدمين باستخدام اسم المستخدم ورمز المرور من خلال بروتوكول RADIUS.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- أمان RSA
- نظام التحكم في الوصول الآمن (ACS) من Cisco

المكونات المستخدمة

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

- نظام التحكم بالوصول الآمن (ACS) من Cisco، الإصدار x.5
- خادم الرمز المميز SecureID ل RSA

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

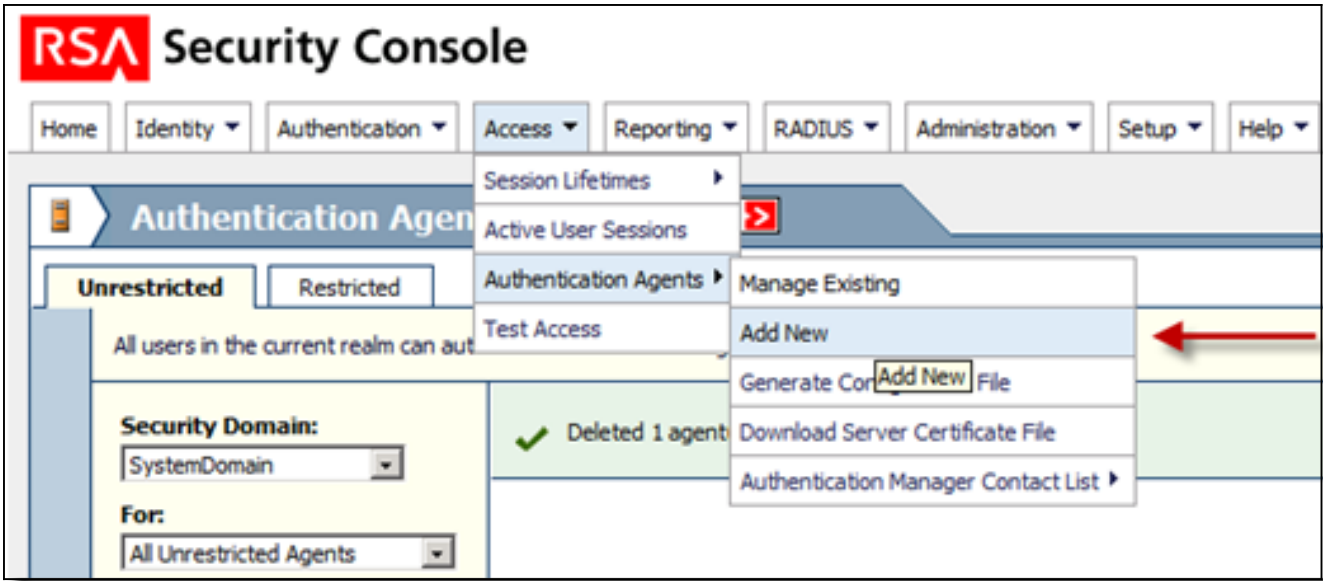
التكوينات

خادم RSA

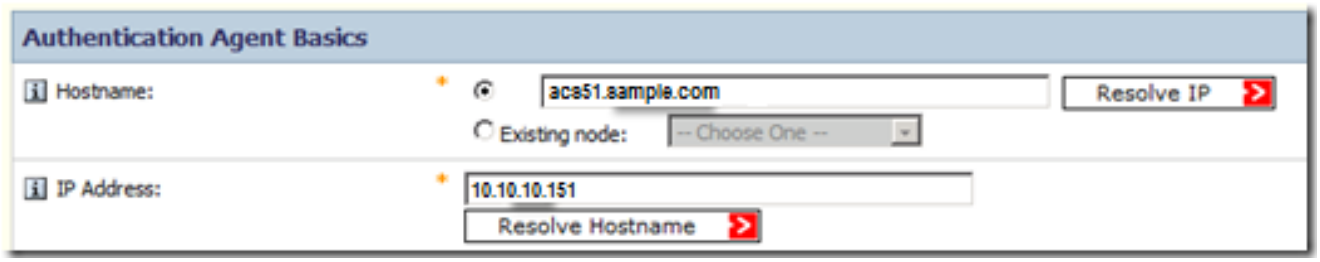
يوضح هذا الإجراء كيفية قيام مسؤول خادم RSA SecureID بإنشاء وكلاء مصادقة وملف تكوين. عامل المصادقة هو بشكل أساسي اسم خادم اسم المجال (DNS) وعنوان IP لجهاز أو برنامج أو خدمة لها حقوق الوصول إلى قاعدة بيانات RSA. يصف ملف التكوين بشكل أساسي مخطط RSA والاتصال.

في هذا المثال، يجب على مسؤول RSA إنشاء وكيلين لمثيلي ACS.

1. في وحدة تحكم أمان RSA، انتقل إلى **الوصول > وكلاء المصادقة > إضافة جديد**:

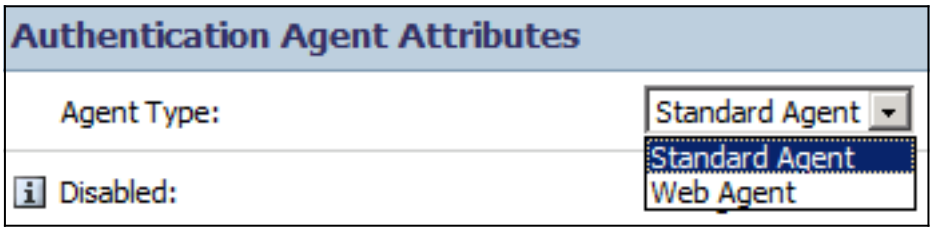


2. في نافذة إضافة عامل مصادقة جديد، قم بتعريف اسم المضيف وعنوان IP لكل من الوكلاء:

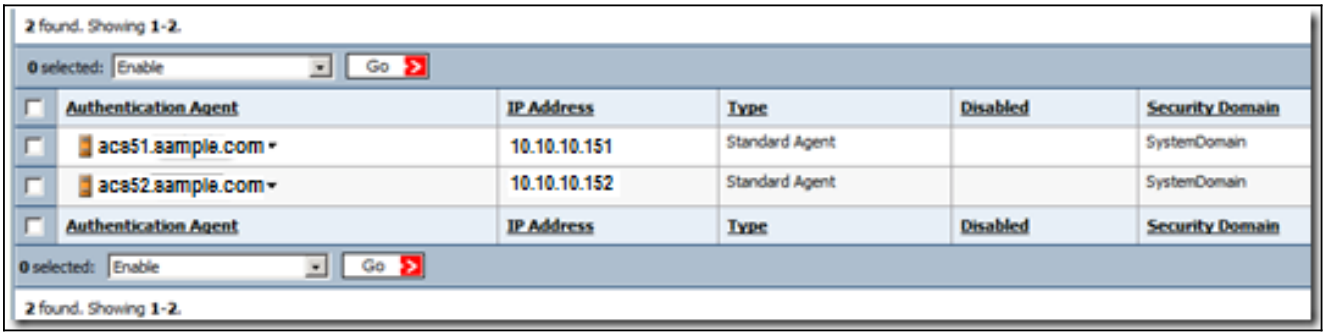


يجب أن تعمل كل من عمليات البحث عن DNS للأمام والعكس لعملاء ACS.

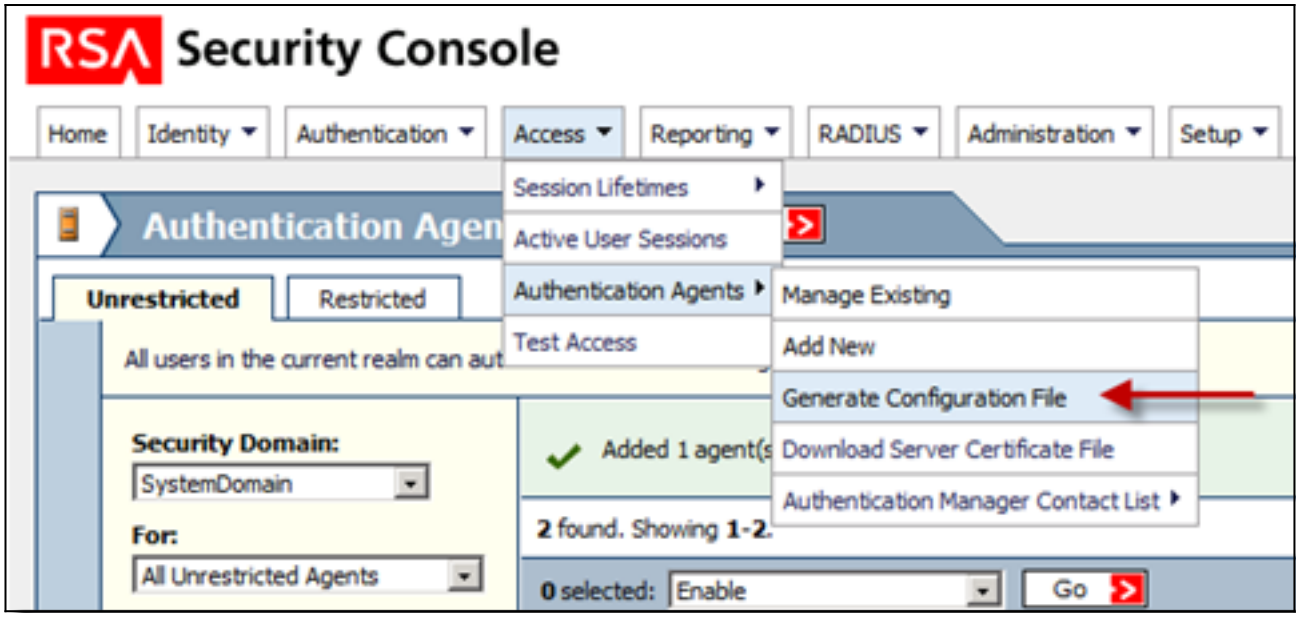
3. تعريف نوع العامل كعامل قياسي:



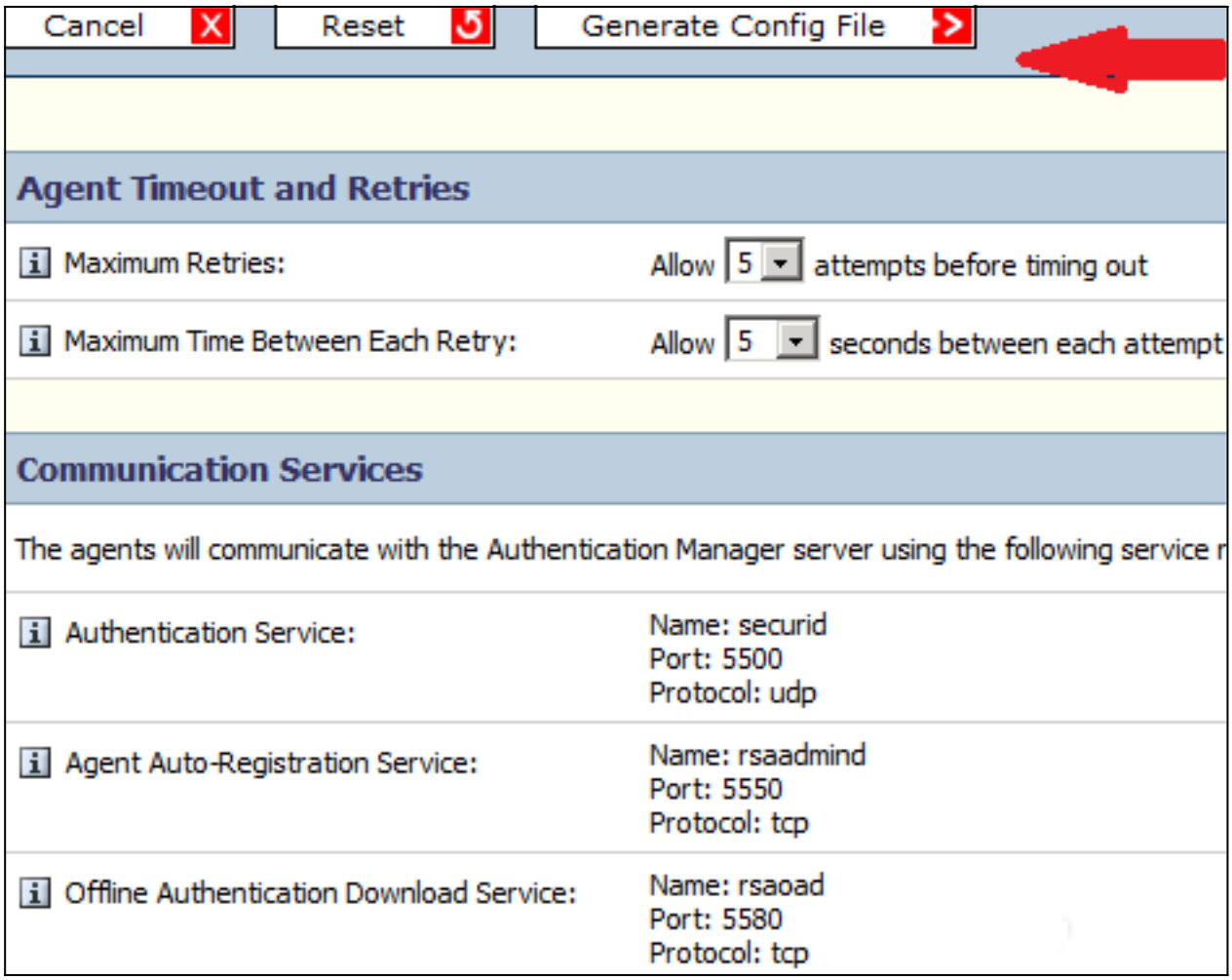
هذا مثال على المعلومات التي تراها بمجرد إضافة الوكلاء:



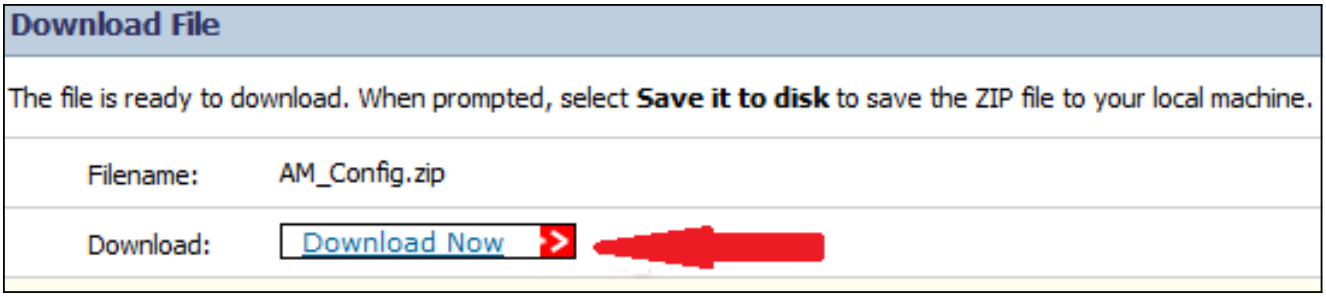
4. في وحدة تحكم أمان RSA، انتقل إلى **الوصول** > **وكلاء المصادقة** > **إنشاء ملف التكوين** لإنشاء ملف تكوين sdconf.rec:



5. أستخدم القيم الافتراضية للحد الأقصى من عمليات إعادة المحاولة والحد الأقصى للوقت بين كل محاولة:



6. قم بتنزيل ملف التكوين:

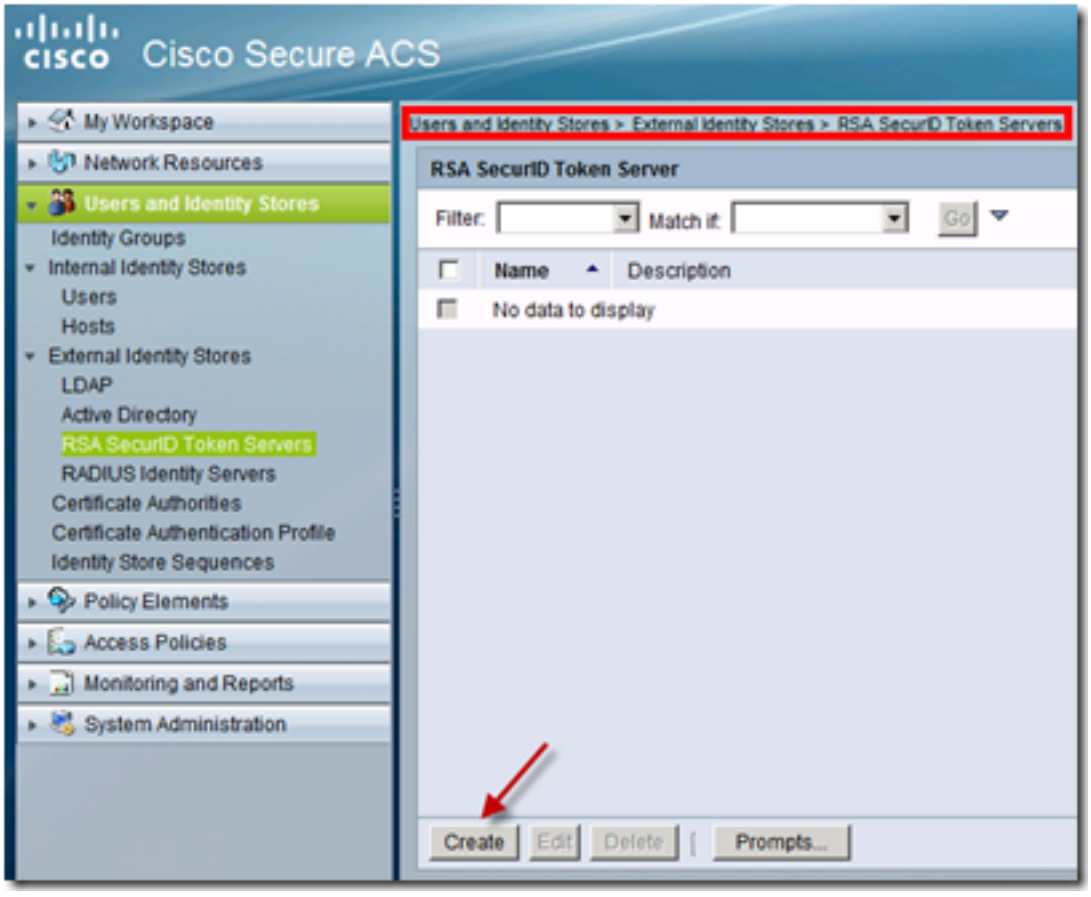


يحتوي ملف .zip على ملف sdconf.rec للتكوين الفعلي، والذي يحتاج إليه مسؤول ACS لإكمال مهام التكوين.

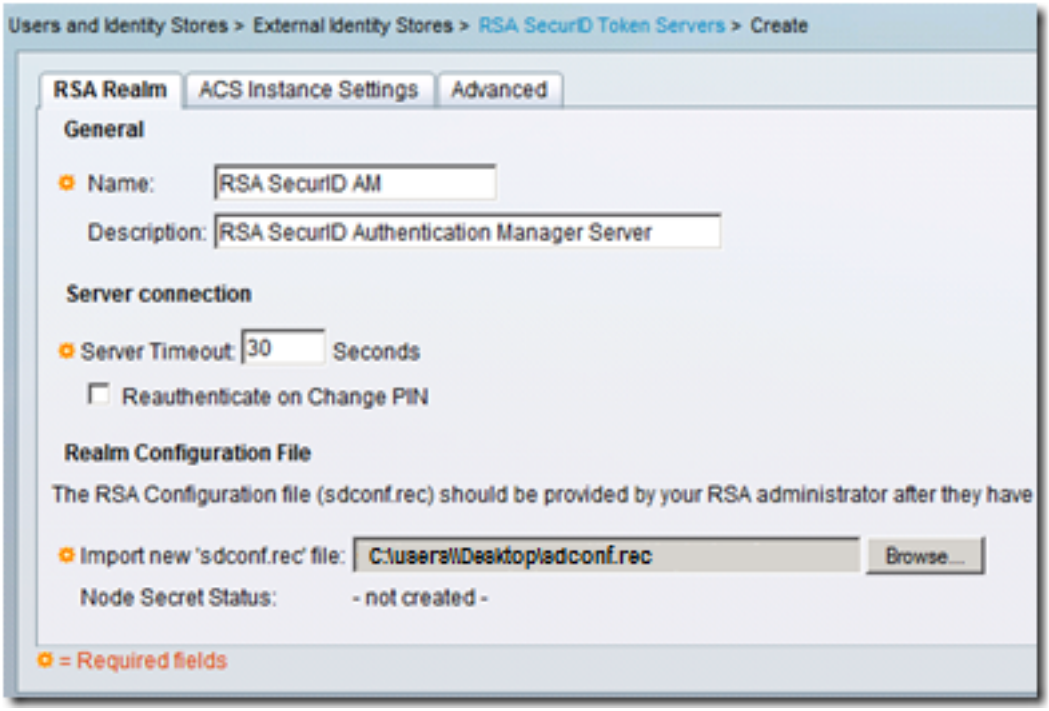
خادم ACS الإصدار x.5

يوضح هذا الإجراء كيفية إسترداد مسؤول ACS لملف التكوين وإرساله.

في وحدة تحكم الإصدار x.5 من Cisco الآمن ل ACS، انتقل إلى **المستخدمين ومخازن الهوية > مخازن الهوية الخارجية > خوادم RSA SecureID المميزة**، وانقر فوق **إنشاء**:



2. أدخل اسم خادم RSA، واستعرض إلى ملف sdconf.rec الذي تم تنزيله من خادم RSA:



3. حدد الملف، وانقر **إرسال**.

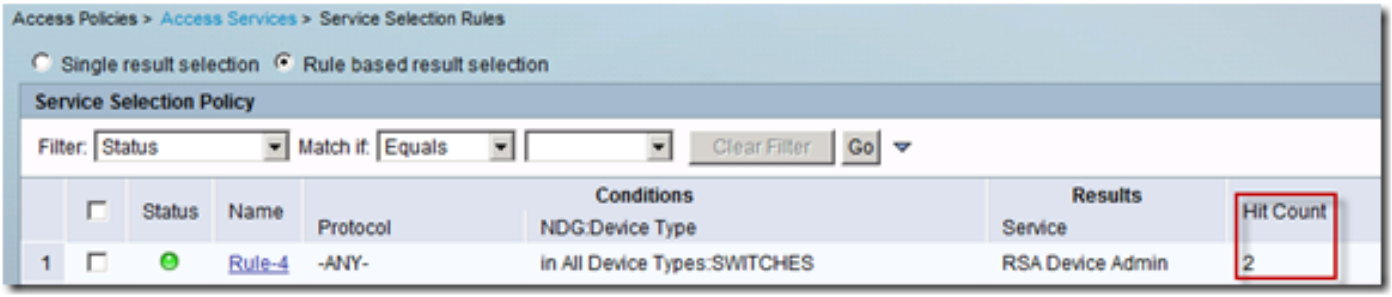
ملاحظة: في المرة الأولى التي يتصل فيها ACS بخادم الرمز المميز، يتم إنشاء ملف آخر، يسمى الملف السري للعقدة، لوكيل ACS على مدير مصادقة RSA ويتم تنزيله إلى ACS. يتم إستخدام هذا الملف للاتصالات المشفرة.

التحقق من الصحة

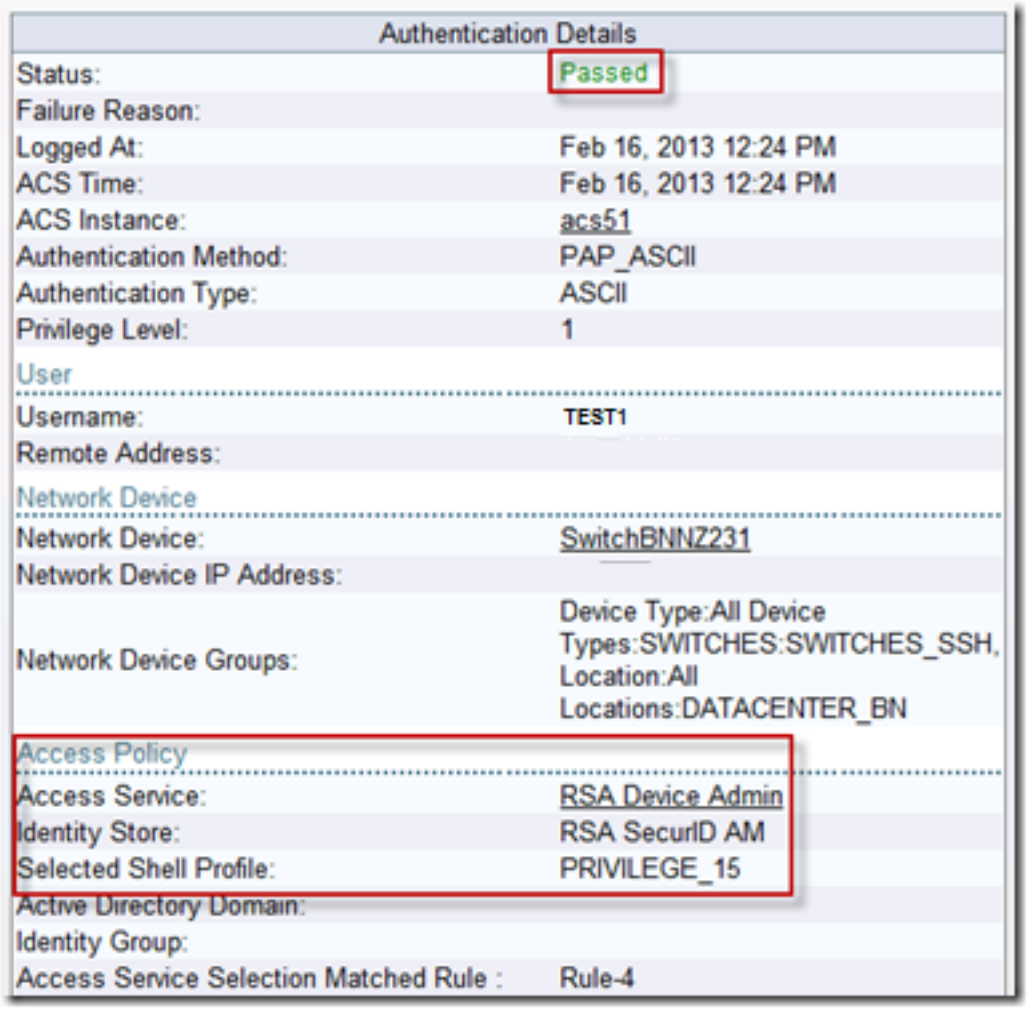
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

خادم ACS الإصدار x.5

للتحقق من تسجيل دخول ناجح، انتقل إلى وحدة تحكم ACS، وراجع عدد مرات الوصول:



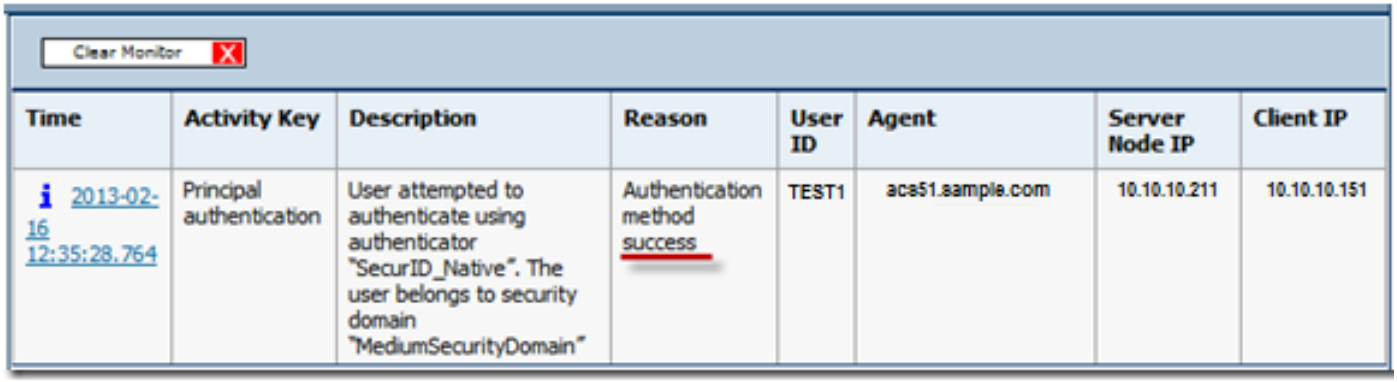
يمكنك أيضا مراجعة تفاصيل المصادقة من سجلات ACS:



Authentication Details	
Status:	Passed
Failure Reason:	
Logged At:	Feb 16, 2013 12:24 PM
ACS Time:	Feb 16, 2013 12:24 PM
ACS Instance:	acs51
Authentication Method:	PAP_ASCII
Authentication Type:	ASCII
Privilege Level:	1
User	
Username:	TEST1
Remote Address:	
Network Device	
Network Device:	SwitchBNNZ231
Network Device IP Address:	
Network Device Groups:	Device Type:All Device Types:SWITCHES:SWITCHES_SSH, Location:All Locations:DATACENTER_BN
Access Policy	
Access Service:	RSA Device Admin
Identity Store:	RSA SecurID AM
Selected Shell Profile:	PRIVILEGE_15
Active Directory Domain:	
Identity Group:	
Access Service Selection Matched Rule :	Rule-4

خادم RSA

للتحقق من المصادقة الناجحة، انتقل إلى وحدة تحكم RSA، وراجع السجلات:



Clear Monitor

Time	Activity Key	Description	Reason	User ID	Agent	Server Node IP	Client IP
2013-02-16 12:35:28.764	Principal authentication	User attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "MediumSecurityDomain"	Authentication method success	TEST1	acs51.sample.com	10.10.10.211	10.10.10.151

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

إنشاء سجل عميل (sdconf.rec)

من أجل تكوين خادم رمز RSA SecureID المميز في الإصدار 5.3 من ACS، يجب أن يحتوي مسؤول ACS على ملف sdconf.rec. ملف sdconf.rec هو ملف سجل تكوين يحدد كيفية اتصال وكيل RSA مع نطاق خادم RSA SecureID.

لإنشاء ملف sdconf.rec، يجب على مسؤول RSA إضافة مضيف ACS كمضيف وكيل على خادم RSA SecureID وإنشاء ملف تكوين لمضيف الوكيل هذا.

إعادة تعيين سر العقدة (معرف الأمان)

بعد أن يتصل العميل في البداية بخادم RSA SecurID، يوفر الخادم للوكيل ملف سري لعقدة يسمى SecurityID. يعتمد الاتصال اللاحق بين الخادم والوكيل على تبادل سر العقدة للتحقق من صحة الآخر.

وفي بعض الأحيان، قد يضطر المسؤولون إلى إعادة تعيين سر العقدة:

1. يجب على مسؤول RSA إلغاء تحديد خانة الاختيار "سر العقدة" الذي تم إنشاؤه في سجل "مضيف الوكيل" في خادم RSA SecureID.
2. يجب على مسؤول ACS إزالة ملف معرف الأمان من ACS.

تجاوز الموازنة التلقائية للأحمال

يقوم عميل SecureID ل RSA تلقائيا بموازنة الأحمال المطلوبة على خوادم RSA SecureID في النطاق. على أي حال، لديك الخيار أن توازن الحمل يدويا. يمكنك تحديد الخادم المستخدم من قبل كل مضيف من البيئات المضيفة الوكيل. يمكنك تعيين أولوية لكل خادم بحيث يقوم مضيف الوكيل بتوجيه طلبات المصادقة إلى بعض الخوادم بشكل أكثر تواترا من غيرها.

يجب عليك تحديد إعدادات الأولوية في ملف نصي، وحفظه على هيئة sdopts.rec، وتحميله إلى ACS.

التدخل يدويا لإزالة خادم RSA SecureID لأسفل

عندما يكون خادم RSA SecureID معطلا، لا تعمل آلية الاستبعاد التلقائية دائما بسرعة. قم بإزالة ملف sdstatus.12 من ACS لتسريع هذه العملية.

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).