vManage: كيفية التحقق من تسجيل الدخول الأحادي والتحقق من صحته

المحتويات

المقدمة

يصف هذا المستند الأساسيات لتمكين تسجيل الدخول الأحادي (SSO) على vManage وكيفية التحقق/التحقق من صحة vManage، عند تمكين هذه الميزة. وبدءا من الإصدار 18.3.0، يدعم تقنية vManage برنامج SSO. يسمح SSO للمستخدم بتسجيل الدخول إلى vManage عن طريق المصادقة مقابل موفر هوية خارجي (IP). تدعم هذه الميزة مواصفات SAML 2.0 ل SSO.

تمت المساهمة من قبل شانكار فيمولاباللي، مهندس TAC من Cisco.

مصطلحات

لغة ترميز أتكيد الأمان (SAML) هي معيار مفتوح لتبادل بيانات المصادقة والتفويض بين الأطراف، وخاصة بين موفر الهوية و موزع الخدمة. كما يشير اسمها ضمنا، فإن SAML هي لغة ترميز قائمة على XML لتأكيدات الأمان (البيانات التي يستخدمها موفر الخدمة لاتخاذ قرارات التحكم في الوصول).

موفر الهوية (IDp) هو "موفر موثوق به يتيح لك إستخدام تسجيل الدخول الأحادي (SSO) للوصول إلى مواقع الويب الأخرى." يقلل SSO من إرهاق كلمة المرور ويعزز إمكانية الاستخدام. كما أنها تقلل من سطح الهجوم المحتمل وتوفر مستوى أمان أفضل.

موزع الخدمة - وهو كيان نظام يتلقى ويقبل تأكيدات المصادقة بالاقتران مع ملف تعريف SSO الخاص ب SAML.

ما هي إمكانات المميزات؟

- يتم دعم SAML2.0 فقط
- مدعوم من أجل - مستأجر واحد (مستقل وعنقود) ومستأجر متعدد (على مستوى المزود ومستوى المستأجر)، كما أن عمليات النشر متعددة المستأجرين يتم تجميعها بشكل افتراضي. المورد كمستأجر غير قابل للتطبيق.
- يمكن أن يكون لكل مستأجر مورد هوية فريد خاص به طالما أن المشرفين داخليا يتبعون مواصفات SAML 2.0.
- يدعم تكوين بيانات تعريف IDP عبر تحميل الملفات وكذلك نسخ النص العادي وتنزيل بيانات تعريف vManage.
- يتم دعم SSO المستند إلى المستعرض فقط.
- الشهادات المستخدمة لبيانات تعريف vManage غير قابلة للتكوين في هذا الإصدار. هي "شهادة موقعة ذاتيا"، تم إنشاؤها في أول مرة تقوم فيها بتمكين SSO، باستخدام المعلمات التالية:

  String CN = <TenantName>، DefaultTenant

  String OU = <اسم المؤسسة>
  السلسلة O = <sp org name>
  السلسلة L = "سان خوسيه"؛
  String ST = "CA"؛
  السلسلة C = "الولايات المتحدة الأمريكية"؛
  صلاحية السلسلة = 5 سنوات؛
  خوارزمية توقيع الشهادة: SHA256WithRSA
  خوارزمية إنشاء KeyPair: RSA

- تسجيل دخول أحادي - بدء تشغيل SP وبدء تشغيل النازحين داخليا
- تسجيل خروج أحادي - تم بدء SP فقط

كيف يمكنك تمكينها على vManage؟

لتمكين تسجيل الدخول الأحادي (SSO) ل vManage NMS للسماح للمستخدمين بالمصادقة باستخدام مورد هوية خارجي:

1. تأكد من تمكين بروتوكول NTP على نظام vManage NMS.
2. الاتصال ب vManage GUI باستخدام URL الذي تم تكوينه على IdP (على سبيل المثال، vmanage-112233.viptela.net والا تستخدم عنوان IP، لأن معلومات عنوان URL هذه مضمنة في بيانات SAML الأولية)
3. انقر زر التحرير الموجود على يمين شريط إعدادات مورد الهوية.
4. في حقل تمكين مزود الهوية، انقر على تمكين،
5. قم بنسخ ولصق بيانات تعريف مورد الهوية في مربع بيانات تعريف تحميل مورد الهوية. أو انقر فوق تحديد ملف لتحميل ملف بيانات تعريف مورد الهوية.
6. انقر حفظ.

ما هو سير العمل؟

1. يقوم المستخدم بتمكين SSO عبر صفحة الإدارة->الإعدادات عن طريق تحميل بيانات تعريف مورد الهوية.

2. يقوم المستخدم بعد ذلك بتنزيل بيانات تعريف المستأجر vManage المطابقة لإنشاء الطلب وتحميلها على موفر الهوية (يجب القيام به مرة واحدة على الأقل بيانات تعريف vManage).
3. يمكن للمستخدم تعطيل بيانات التعريف أو تحديثها في أي وقت إذا لزم الأمر.

نموذج التعريف vManage

هل تدعم تقنية vManage مصادقة ثنائية العوامل وكيف تختلف عن SSO؟

المصادقة ثنائية العوامل (تعرف أيضا باسم2FA) هي نوع المصادقة متعددة العوامل (MFA) وأ مجموعة فرعية منها. وهي طريقة لتأكيد هويات المستخدمين المزعومة باستخدام مجموعة من عوامل مختلفة: 1) شيء يعرفونه، 2) شيء ما يمتلكونه، و3) شيء ما.

مثال: Google GmAil (كلمة السر مع كلمة مرور المرة الواحدة (OTP))

2FA هو شيء سيتم توفيره على خادم SSO. وهو مماثل إلى كيف نحن login إلى الداخلي cisco موقع.

إنه يعيد توجيهك إلى Cisco SSO، حيث سيتم مطالبتك ب PingID / Duo 2FA.

كم عدد الأدوار الموجودة كجزء من الحل؟

لديان 3 لفائف، أساسي، مشغل، netadmin.

تكوين وصول المستخدم والمصادقة

ما هي المعرفات التي ندعمها؟

- أوكتا
- PingID
- نظام الملفات الموزعة

قد يستخدم العملاء معرفات أخرى وقد يروناها تعمل. وهذا سيكون ضمن "أفضل جهد"

مثال على ذلك هو MSFT Azure AD الذي لم يتم دعمه لـ IDP (حتى الآن). ولكن هذا قد يتجح، انظر لبعض المحاذير.

ومن بين الشبكات الأخرى: Oracle Access Manager و F5 Networks

> **ملاحظة**: يرجى التحقق من أحدث وثائق Cisco للحصول على أحدث معرفات IdPs التي يدعمها vManage

كيف تشير إلى تأكيد عضوية مجموعة المستخدمين في SAML؟

المشكلة: إدارة vManage في المقدمة باستخدام معرف SAML IDp. عندما تتم مصادقة المستخدم بنجاح، فإن الشيء الوحيد الذي يمكن للمستخدم الوصول إليه هو لوحة المعلومات.

هل هناك طريقة لمنح المستخدم إمكانية وصول أكبر (عبر مجموعة المستخدمين RBAC) عند مصادقة المستخدم عبر SAML؟

وهذه المشكلة ناجمة عن التكوين غير السليم للمشرفين داخليا. المفتاح هنا هو أن المعلومات المرسلة من قبل IDP أثناء المصادقة يجب أن تحتوي على "اسم المستخدم" و"المجموعات" كسمات في xml. إذا تم إستخدام سلاسل أخرى بدلا من "المجموعات"، فإن مجموعة المستخدمين تكون افتراضية لـ "basic". المستخدمون "الأساسيون" لديهم حق الوصول إلى لوحة المعلومات الأساسية فقط.

تأكد من أن IDP يرسل "اسم المستخدم/المجموعات"، بدلا من "UserId/Role" إلى vManage. فيما يلي مثال على ذلك كما هو موضح في الملف /var/log/nms/vmanage-server.log:

مثال غير عامل:

نرى "UserId/Role" تم إرساله بواسطة IdP وتم تعيين المستخدم إلى مجموعة *أساسية*.

```
01-Mar-2019 15:23:50,797 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-227)
|default| AttributeMap: {role=[netadmin], UserId=[Tester@Example.MFA.com]}
01-Mar-2019 15:23:50,797 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-227)
|default| AttributeMap: {role=[netadmin], UserId=[Tester@Example.MFA.com]}
01-Mar-2019 15:23:50,797 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-227)
|default| Roles: [Basic]
```

مثال عمل:

في هذا ترى "اسم المستخدم/المجموعات" وتم تعيين المستخدم على مجموعة NetAdmin.

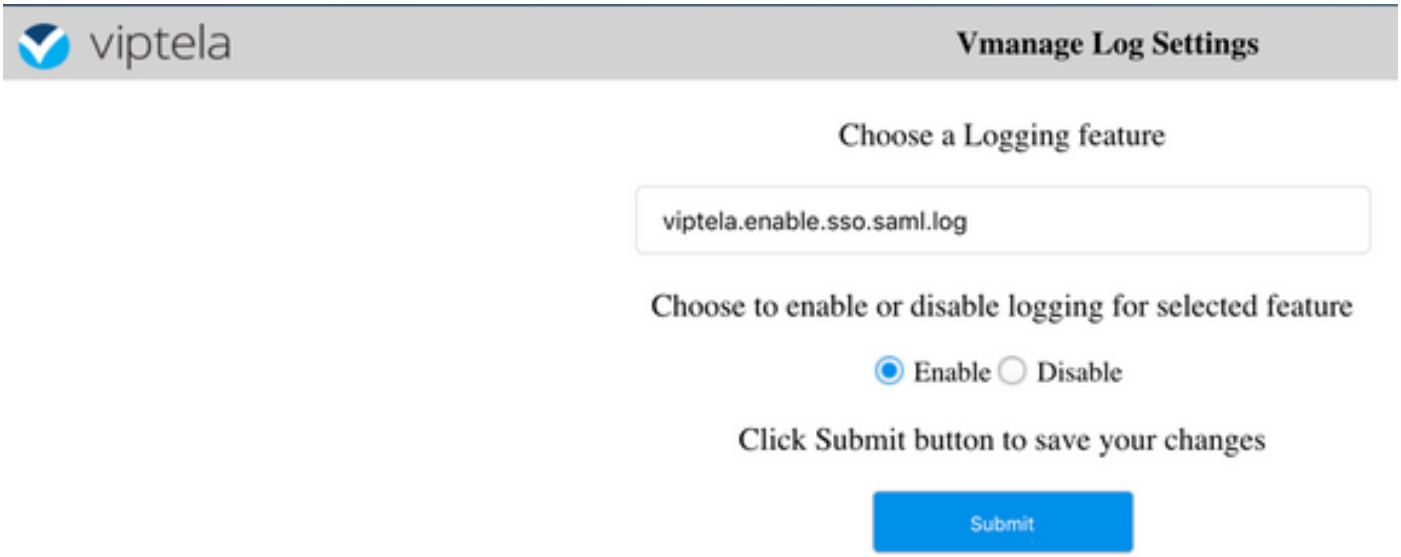
```
05-Mar-2019 21:35:55,766 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-90)
|default| AttributeMap: {UserName=[Tester@Example.MFA.com], Groups=[netadmin]}
05-Mar-2019 21:35:55,766 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-90)
|default| AttributeMap: {UserName=[Tester@Example.MFA.com], Groups=[netadmin]}
05-Mar-2019 21:35:55,766 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-90)
|default| Roles: [netadmin]
```

كيفية تمكين/التحقق مما إذا كان SSO يعمل؟

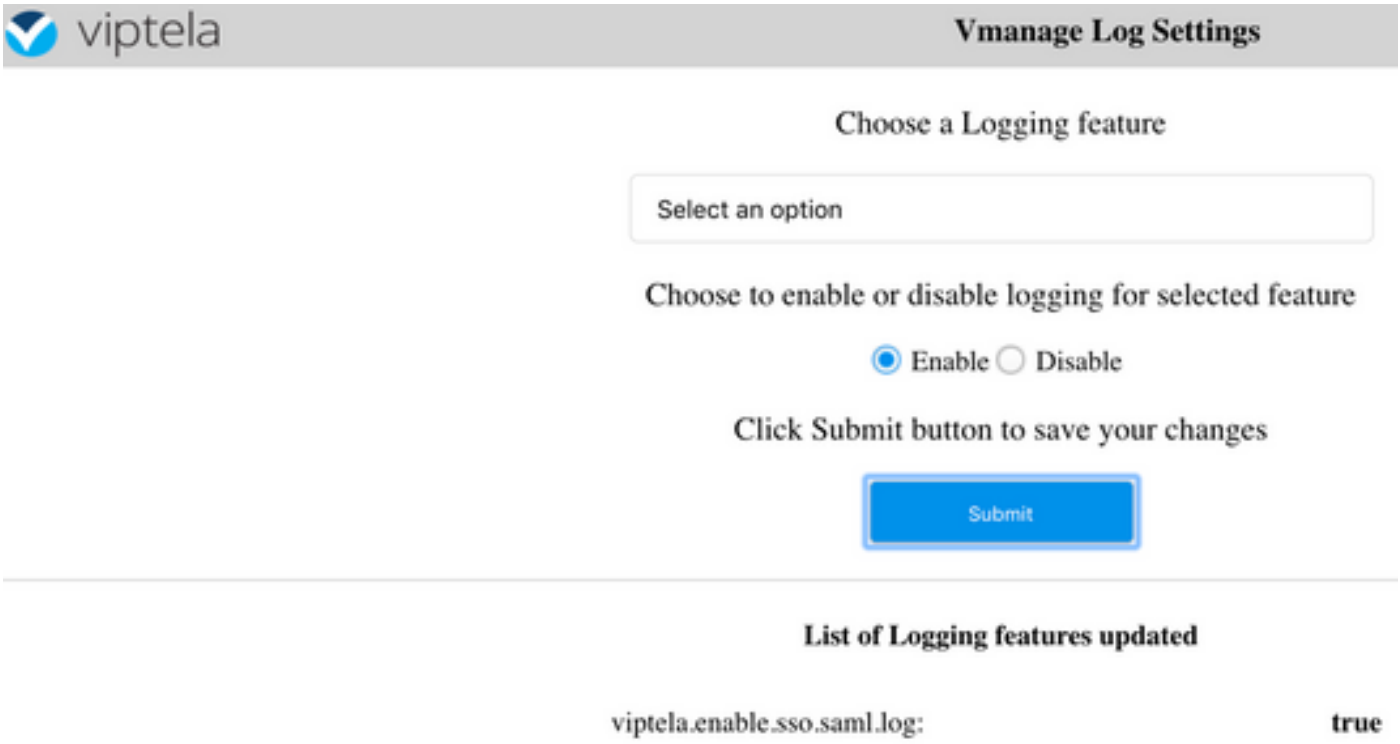
يمكن تمكين تسجيل تصحيح أخطاء ميزة SSO كما يلي:

1. انتقل إلى **https://<vManage_ip_addr:port>/logsettings.html**

2. حدد تسجيل SSO وقم بتمكينه كما هو موضح في الصورة.



3. بمجرد تمكينها، اضغط على الزر **إرسال**.



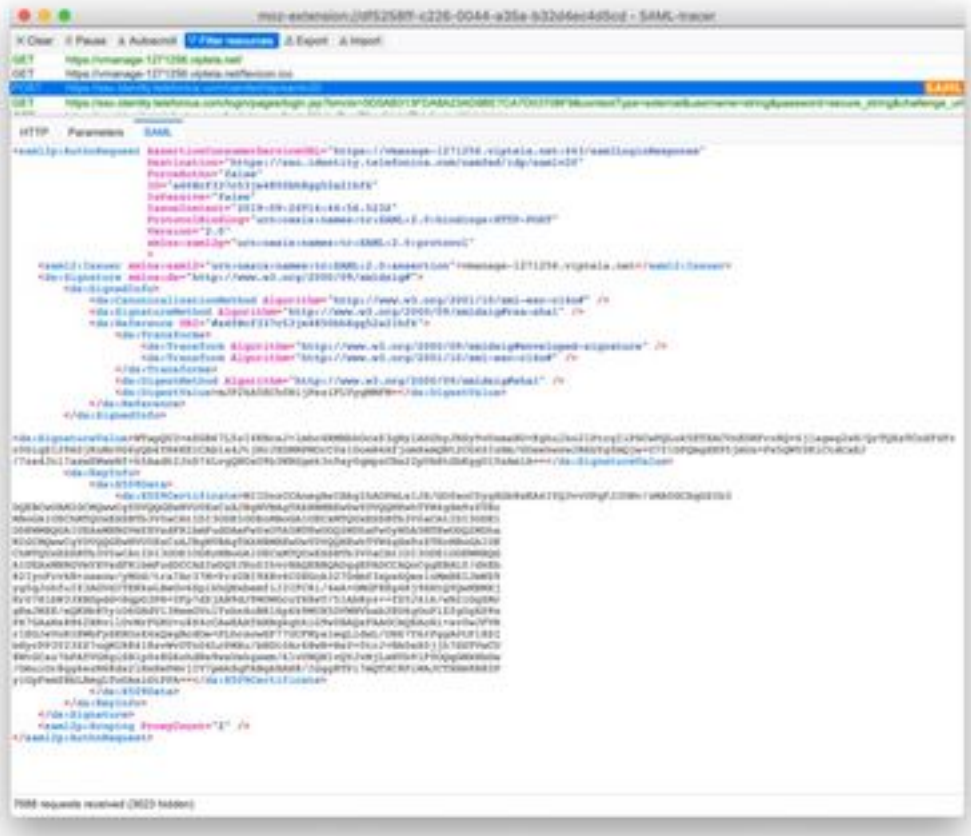
- سيتم الآن حفظ السجلات المرتبطة بالموجه المستقل (SSO) في ملف سجل vManage /var/log/nms/vmanage-server.log في الأهمية الخاصة في إعداد "المجموعات" الخاص بتفويض IDP. إذا لم يكن هناك تطابق، فسيعمل المستخدم افتراضي على مجموعة "Basic"، والتي لها وصول للقراءة فقط؛
- لتصحيح أخطاء مشكلة امتياز الوصول، تحقق من ملف السجل وابحث عن السلسلة "SamlUserGroups". ما يلي ذلك ينبغي أن يكون قائمة سالس من أسماء المجموعات. يجب أن يطابق أحدها إعدادات المجموعة في vManage. إذا لم يتم العثور على تطابق، يكون المستخدم قد قام بالتقصير إلى المجموعة "أساسي".

سامل تريكر

أداة لعرض رسائل SAML و WS-Federation المرسلة من خلال المستعرض أثناء تسجيل الدخول الأحادي وتسجيل الخروج الأحادي.

الأداة الإضافية FireFOX SAML-Tracer

امتداد Chrome SAML-Tracer



نموذج

رسالة SAML

كيف يمكنك تسجيل الدخول إلى برنامج vManage الذي يدعم SSO؟

يتم تسجيل الدخول إلى المستعرض فقط. يمكنك توجيه vManage يدويا إلى صفحة تسجيل الدخول التقليدية وتجاوز SSO لاستخدام اسم المستخدم وكلمة المرور فقط: https://<vmanage>:8443/login.html.

ما هي خوارزمية التشفير المستخدمة ؟

حاليا ندعم SHA1 كخوارزمية تشفير. سيقوم vManage بتوقيع ملف بيانات التعريف SAML باستخدام خوارزمية SHA1 التي يجب على IdPs قبولها. سيتوفر الدعم ل SHA256 في الإصدارات المستقبلية، التي لا نتوفر على الدعم حاليا.

معلومات ذات صلة

تكوين الدخول الأحادي:
https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-16/security-book-xe/configure-sso.html

تسجيل الدخول إلى OKTA / تسجيل الخروج من سجلات العمل المرفقة بالحالة كمرجع.

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).