

vManage : Vérification et vérification de l'authentification unique

Contenu

[Introduction](#)

[Terminologie](#)

[Quelles sont les fonctionnalités ?](#)

[Comment l'activer sur vManage ?](#)

[Quel est le workflow ?](#)

[Est-ce que vManage prend en charge l'authentification à deux facteurs et en quoi elle est différente de SSO ?](#)

[Combien de rôles y a-t-il dans la solution ?](#)

[Quels IDPs prenons-nous en charge ?](#)

[Comment indiquer l'appartenance à un groupe d'utilisateurs dans l'assertion SAML ?](#)

[Comment activer/vérifier si SSO fonctionne ?](#)

[SAML Tracer](#)

[exemple de message SAML](#)

[Comment se connecter à SSO enabled vManage ?](#)

[Quel algorithme de chiffrement est utilisé ?](#)

[Informations connexes](#)

Introduction

Ce document décrit les éléments de base afin d'activer l'authentification unique (SSO) sur vManage et comment vérifier/vérifier sur vManage, lorsque cette fonctionnalité est activée. À partir de 18.3.0, vManage prend en charge SSO. SSO permet à un utilisateur de se connecter à vManage en s'authentifiant auprès d'un fournisseur d'identité externe (IP). Cette fonctionnalité prend en charge la spécification SAML 2.0 pour SSO.

Contribué par Shankar Vemulapalli, ingénieur TAC Cisco.

Terminologie

Le langage SAML (Security Assertion Markup Language) est une norme ouverte permettant l'échange de données d'authentification et d'autorisation entre les parties, en particulier entre un fournisseur d'identité et un prestataire de services. Comme son nom l'indique, SAML est un langage de balisage XML pour les assertions de sécurité (instructions utilisées par les fournisseurs de services pour prendre des décisions de contrôle d'accès).

Un fournisseur d'identité (IdP) est “ un fournisseur de confiance qui vous permet d'utiliser l'authentification unique (SSO) afin d'accéder à d'autres sites Web. ” SSO réduit la fatigue des mots de passe et améliore la convivialité. Elle réduit la surface d'attaque potentielle et améliore la sécurité.

Fournisseur de services - Il s'agit d'une entité système qui reçoit et accepte des assertions

d'authentification en conjonction avec un profil SSO du SAML.

Quelles sont les fonctionnalités ?

- Seul SAML2.0 est pris en charge
- Pris en charge pour - le service partagé unique (autonome et cluster), le service partagé (au niveau du fournisseur et du client), ainsi que les déploiements multilocataire sont regroupés par défaut. Provider-as-locataire n'est pas applicable.
- Chaque locataire peut avoir son propre fournisseur d'identité unique tant que le idp respecte la spécification SAML 2.0.
- Prend en charge la configuration des métadonnées IDP via le téléchargement de fichiers ainsi que la copie de texte brut et le téléchargement des métadonnées vManage.
- Seule l'authentification unique basée sur navigateur est prise en charge.
- Les certificats utilisés pour les métadonnées vmanage ne sont pas configurables dans cette version.

il s'agit d'un certificat auto-signé, créé la première fois que vous activez SSO, avec les paramètres suivants :

Chaîne CN = <NomClient>, DefaultTenant

OU de chaîne = <Nom de l'organisation>

Chaîne O = <Nom De L'Organisation Sp>

Chaîne L = « San Jose »;

Chaîne ST = « CA »;

Chaîne C = « États-Unis »;

Validité de la chaîne = 5 ans ;

Algorithme de signature de certificat : SHA256AvecRSA

Algorithme de génération de paire de clés : RSA

- Connexion unique - Prise en charge par SP et IDP
- Déconnexion unique - Initié par SP uniquement

Comment l'activer sur vManage ?

Pour activer l'authentification unique (SSO) pour le NMS vManage afin de permettre l'authentification des utilisateurs à l'aide d'un fournisseur d'identité externe :

1. Assurez-vous que vous avez activé NTP sur vManage NMS.
2. se connecter à l'interface utilisateur graphique vManage avec l'URL configurée sur IdP (par exemple vmanage-112233.viptela.net et n'utilisez pas d'adresse IP, car ces informations d'URL sont incluses dans les métadonnées SAML)
3. Cliquez sur le bouton Modifier à droite de la barre Paramètres du fournisseur d'identité.
4. Dans le champ Enable Identity Provider, cliquez sur Enabled,
5. Copiez et collez les métadonnées du fournisseur d'identité dans la zone Upload Identity Provider Metadata. Ou cliquez sur Sélectionner un fichier pour télécharger le fichier de métadonnées du fournisseur d'identité.
6. Click Save.

Quel est le workflow ?

1. L'utilisateur active SSO via la page Administration->Paramètres en téléchargeant les métadonnées du fournisseur d'identité.
2. L'utilisateur télécharge ensuite les métadonnées de locataire vManage correspondantes à télécharger sur le fournisseur d'identité (il doit être effectué au moins une fois pour générer les métadonnées vManage).
3. L'utilisateur peut désactiver ou mettre à jour les métadonnées à tout moment si nécessaire.

Exemple de méta vManage

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?><md xmlns="urn:ietf:params:xml:ns:md" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:ietf:params:xml:ns:md http://www.w3.org/2001/XMLSchema-instance" ><id>1</id><name>vManage</name><type>vManage</type><url>https://vmanage.cisco.com</url><logo>https://vmanage.cisco.com/images/logo.png</logo><description>vManage</description><authn><type>SAML2</type><url>https://vmanage.cisco.com/saml/</url><spid>vmanage</spid><spurl>https://vmanage.cisco.com/</spurl><acspurl>https://vmanage.cisco.com/</acspurl><assertionurl>https://vmanage.cisco.com/</assertionurl></authn><idp><name>vManage</name><url>https://vmanage.cisco.com/</url><entityid>https://vmanage.cisco.com/</entityid></idp></md></pre>
```

Est-ce que vManage prend en charge l'authentification à deux facteurs et en quoi elle est différente de SSO ?

L'authentification à deux facteurs (également appelée 2FA) est un type, ou sous-ensemble, d'authentification multifactor (MFA). Il s'agit d'une méthode de confirmation des identités revendiquées par les utilisateurs en combinant deux facteurs différents : 1) quelque chose qu'ils savent, 2) quelque chose qu'ils ont, ou 3) quelque chose qu'ils sont.

Exemple : Google GMail (Mot de passe avec mot de passe unique)

2FA est un élément qui sera fourni sur le serveur SSO. Il est similaire à la façon dont nous nous

connectons au site Web interne de Cisco.

Il vous redirige vers Cisco SSO, où vous serez invité à entrer PingID / DUO 2FA.

Combien de rôles y a-t-il dans la solution ?

Nous avons 3 rouleaux ; basic, opérateur, netadmin.

[Configuration de l'accès et de l'authentification des utilisateurs](#)

Quels IDPs prenons-nous en charge ?

- Okta
- PingID
- ADFS

Les clients peuvent utiliser d'autres IdPs et le voir fonctionner. Cela passerait par le 'meilleur effort'

Un exemple de ceci serait MSFT Azure AD n'est PAS pris en charge IDP (pour le moment). Mais cela pourrait fonctionner, compte tenu de certaines des mises en garde.

Autres : Oracle Access Manager, F5 Networks

Note: Veuillez consulter la dernière documentation Cisco pour connaître les derniers IdPs pris en charge par vManage

Comment indiquer l'appartenance à un groupe d'utilisateurs dans l'assertion SAML ?

Problème : frontal du vManage avec un IDP SAML. Lorsque l'utilisateur est authentifié avec succès, la seule chose à laquelle il peut accéder est le tableau de bord.

Existe-t-il un moyen de donner à l'utilisateur plus d'accès (via le groupe d'utilisateurs RBAC) lorsque l'utilisateur est authentifié via SAML ?

Ce problème est dû à une configuration incorrecte du PCI. La clé ici est que les informations envoyées par IDP lors de l'authentification doivent contenir « Nom d'utilisateur » et « Groupes » comme attributs dans le xml. Si d'autres chaînes sont utilisées à la place de « Groupes », alors le groupe d'utilisateurs est par défaut défini sur « Basic ». Les utilisateurs de base n'ont accès qu'au tableau de bord de base.

Assurez-vous que IDP envoie « Nom d'utilisateur/Groupes » au lieu de « ID d'utilisateur/rôle » à vManage.

Vous trouverez ci-dessous un exemple de ce qui se passe dans le fichier /var/log/nms/vmanage-server.log :

Exemple de non-travail :

Nous voyons que « UserId/role » a été envoyé par IdP et que l'utilisateur est mappé au groupe de

base.

```
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]
```

Exemple de travail :

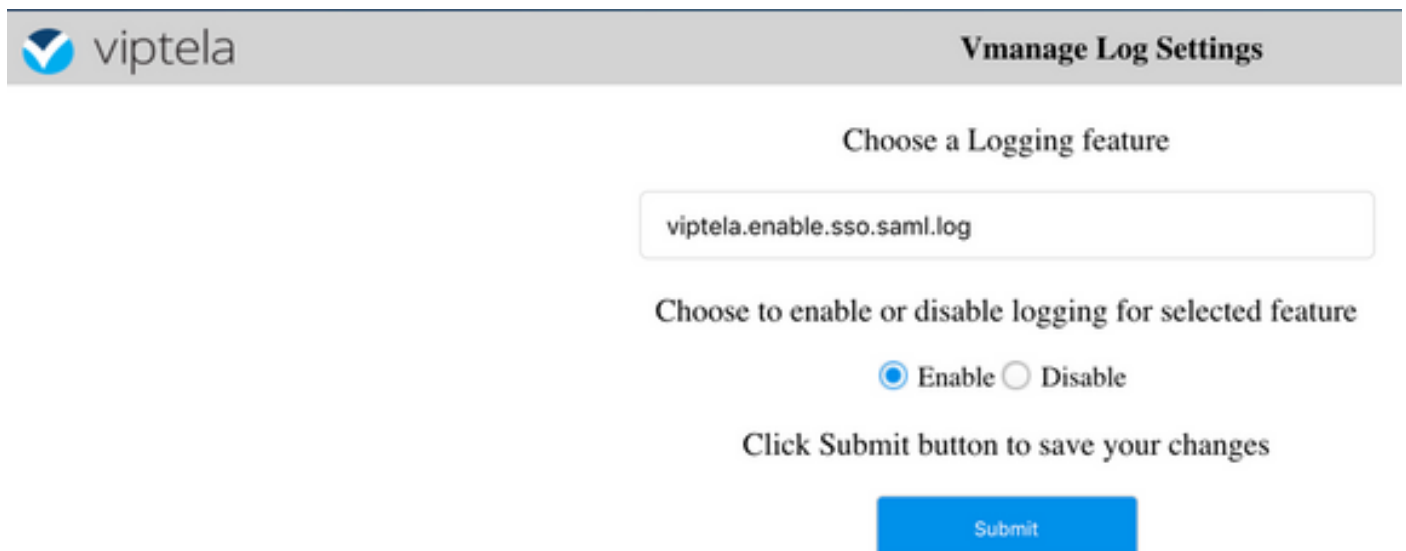
Dans cette section, vous voyez « Nom d'utilisateur/Groupes » et l'utilisateur est mappé au groupe netadmin.

```
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]
```

Comment activer/vérifier si SSO fonctionne ?

La journalisation de débogage de fonctionnalité SSO peut être activée comme suit :

1. Accédez à https://<vManage_ip_addr:port>/logsettings.html
2. Sélectionnez la journalisation SSO et activez-la comme indiqué dans l'image.



The screenshot shows the 'Vmanage Log Settings' interface. At the top left is the Viptela logo. The title 'Vmanage Log Settings' is on the right. Below the title is the heading 'Choose a Logging feature'. A text input field contains 'viptela.enable.sso.saml.log'. Below this is the heading 'Choose to enable or disable logging for selected feature'. There are two radio buttons: 'Enable' (selected) and 'Disable'. Below the radio buttons is the instruction 'Click Submit button to save your changes'. At the bottom is a blue 'Submit' button.

3. Une fois Activé, cliquez sur le bouton **Soumettre**.

Choose a Logging feature

Select an option

Choose to enable or disable logging for selected feature

Enable Disable

Click Submit button to save your changes

Submit

List of Logging features updated

viptela.enable.sso.saml.log: true

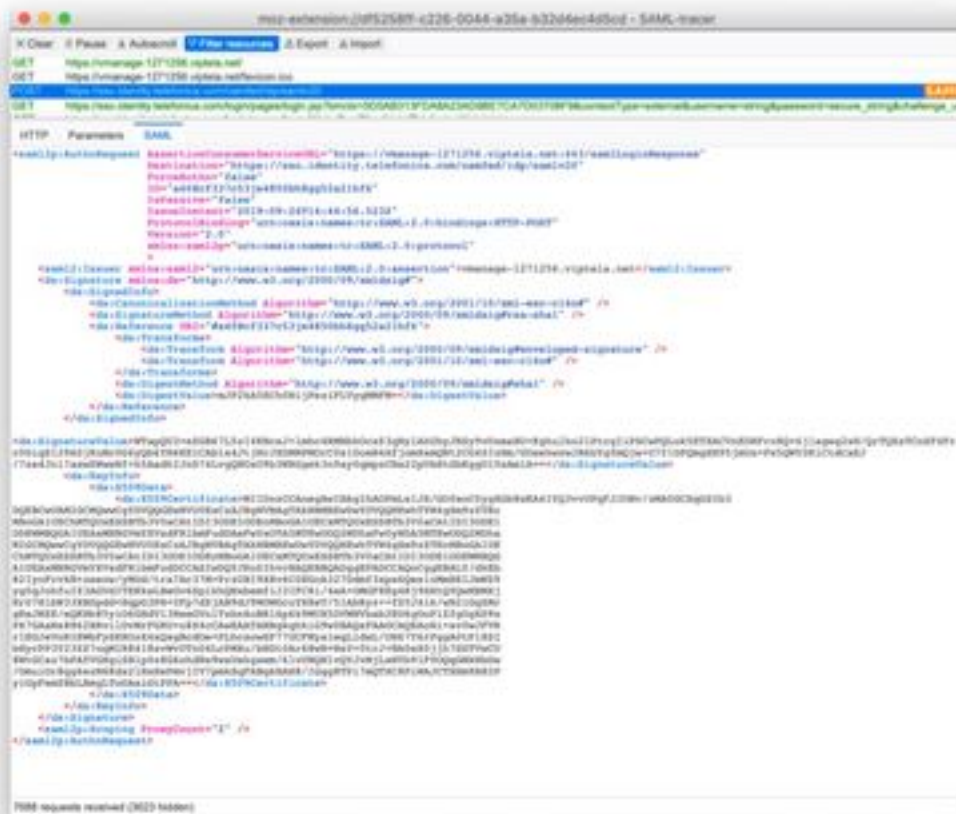
- Les journaux liés à SSO seront maintenant enregistrés dans le fichier journal vManage `/var/log/nms/vmanage-server.log` qui présente un intérêt particulier est le paramètre « Groupes » pour l'autorisation de PCI. S'il n'y a pas de correspondance, l'utilisateur utilisera par défaut le groupe « Basic », qui dispose d'un accès en lecture seule ;
- Afin de déboguer la question de privilège d'accès, vérifiez le fichier journal et recherchez la chaîne « SamlUserGroups ». Ce qui suit devrait être une liste de chaînes de noms de groupe. L'un d'eux doit correspondre aux paramètres de groupe sur vManage. Si aucune correspondance n'est trouvée, l'utilisateur a utilisé le groupe « Basic » par défaut.

SAML Tracer

Outil permettant d'afficher les messages SAML et WS-Federation envoyés via le navigateur lors de la connexion unique et de la déconnexion unique.

[Module complémentaire FireFox SAML-Tracer](#)

[Extension Chrome SAML-Tracer](#)



exemple de

message SAML

Comment se connecter à SSO enabled vManage ?

SSO est réservé à la connexion au navigateur. Vous pouvez diriger manuellement vManage vers la page de connexion traditionnelle et contourner SSO afin d'utiliser uniquement le nom d'utilisateur et le mot de passe : <https://<vmanage>:8443/login.html>.

Quel algorithme de chiffrement est utilisé ?

Actuellement, nous prenons en charge SHA1 en tant qu'algorithme de chiffrement. vManage signera le fichier de métadonnées SAML avec l'algorithme SHA1 que les IdPs doivent accepter. La prise en charge de SHA256 est prévue dans les versions futures, que nous n'avons pas actuellement.

Informations connexes

Configurer l'authentification unique :

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-16/security-book-xe/configure-ss.html>

Journaux de travail de connexion/déconnexion OKTA joints au dossier comme référence.