

vManage: Cómo verificar y verificar el inicio de sesión único

Contenido

[Introducción](#)

[Terminology](#)

[¿Qué son las funciones?](#)

[¿Cómo se activa en vManage?](#)

[¿Cuál es el flujo de trabajo?](#)

[¿vManage admite la autenticación de dos factores y cómo es diferente de SSO?](#)

[¿Cuántos roles hay como parte de la solución?](#)

[¿Qué IdPs admite?](#)

[¿Cómo se indica la pertenencia al grupo de usuarios en SAML assert?](#)

[¿Cómo se habilita/verifica si SSO funciona?](#)

[SAML Tracer](#)

[ejemplo de mensaje SAML](#)

[¿Cómo iniciar sesión en vManage habilitado para SSO?](#)

[¿Qué algoritmo de cifrado se utiliza?](#)

[Información Relacionada](#)

Introducción

Este documento describe los fundamentos para habilitar el inicio de sesión único (SSO) en vManage y cómo verificar en vManage, cuando esta función está habilitada. A partir de 18.3.0, vManage admite SSO. SSO permite al usuario iniciar sesión en vManage mediante la autenticación con un proveedor de identidad externo (IP). Esta función admite la especificación SAML 2.0 para SSO.

Colaborado por Shankar Vemulapalli, ingeniero del TAC de Cisco.

Terminology

El Lenguaje de marcado de aserción de seguridad (SAML) es un estándar abierto para el intercambio de datos de autenticación y autorización entre partes, en particular entre un proveedor de identidad y un proveedor de servicios. Como su nombre implica, SAML es un lenguaje de marcado basado en XML para las aserciones de seguridad (instrucciones que utilizan los proveedores de servicios para tomar decisiones de control de acceso).

Un proveedor de identidad (IdP) es "un proveedor de confianza que le permite utilizar el inicio de sesión único (SSO) para acceder a otros sitios web". SSO reduce la fatiga de las contraseñas y mejora la facilidad de uso. Reduce la superficie de ataque potencial y proporciona una mejor seguridad.

Proveedor de servicios - Es una entidad del sistema que recibe y acepta aserciones de autenticación junto con un perfil SSO de SAML.

¿Qué son las funciones?

- Solo se admite SAML2.0
- Compatible con: arrendatario único (independiente y de clúster), arrendatario múltiple (tanto a nivel de proveedor como de arrendatario). Además, las implementaciones de arrendatarios múltiples se agrupan de forma predeterminada. El proveedor como arrendatario no es aplicable.
- Cada arrendatario puede tener su propio proveedor de identidad único siempre y cuando el idp siga las especificaciones de SAML 2.0.
- Admite la configuración de los metadatos IDP mediante la carga de archivos, así como la copia de texto sin formato y la descarga de los metadatos de vManage.
- Solo se admite SSO basado en navegador.
- Los certificados utilizados para administrar metadatos no se pueden configurar en esta versión.

es un certificado autofirmado, creado la primera vez que habilita SSO, con los siguientes parámetros:

Cadena CN = <NombreArrendatario>, InquilinoPredeterminado

Cadena OU = <Org Name>

Cadena O = <Sp Org Name>

Cadena L = "San José";

Cadena ST = "CA";

Cadena C = "USA";

Validez de cadena = 5 años;

Algoritmo de firma de certificado: SHA256WithRSA

Algoritmo de generación de par de claves: RSA

- Inicio de sesión único: SP iniciado y IDP iniciado admitido
- Cierre de sesión único: solo SP iniciado

¿Cómo se activa en vManage?

Para habilitar el inicio de sesión único (SSO) para vManage NMS para permitir que los usuarios se autenticuen mediante un proveedor de identidad externo:

1. Asegúrese de haber habilitado NTP en el vManage NMS.
2. conexión a la GUI de vManage con la URL configurada en IdP (por ejemplo, vmanage-112233.viptela.net y no use IP-Address, porque esta información de URL se incluye en los metadatos SAML)
3. Haga clic en el botón Edit (Editar) situado a la derecha de la barra Identity Provider Settings (Parámetros del proveedor de identidad).
4. En el campo Enable Identity Provider (Activar proveedor de identidad), haga clic en Enabled (Activado),
5. Copie y pegue los metadatos del proveedor de identidad en el cuadro Cargar metadatos del proveedor de identidad. O bien haga clic en Seleccionar un archivo para cargar el archivo de metadatos del proveedor de identidad.
6. Click Save.

2FA es algo que se proporcionará en el servidor SSO. Es similar a cómo iniciamos sesión en el sitio web interno de Cisco.

Le redirige a Cisco SSO, donde se le solicitará PingID / DUO 2FA.

¿Cuántos roles hay como parte de la solución?

Tenemos 3 rollos; básico, operador, netadmin.

[Configuración del acceso de usuario y la autenticación](#)

¿Qué IdPs admite?

- Okta
- PingID
- ADFS

Los clientes pueden utilizar otros IdPs y pueden verlo funcionar. Esto se encuadra en el "mejor esfuerzo"

Un ejemplo de esto sería MSFT Azure AD NO es compatible con IDP (todavía). Pero puede funcionar, dadas algunas de las advertencias.

Otros incluyen: Oracle Access Manager, F5 Networks

Nota: Consulte la documentación más reciente de Cisco para ver los últimos IdPs admitidos por vManage

¿Cómo se indica la pertenencia al grupo de usuarios en SAML assert?

Problema: final frontal del vManage con un IDP de SAML. Cuando el usuario se autentica correctamente, lo único al que puede acceder es el panel.

¿Hay alguna manera de dar al usuario más acceso (a través del grupo de usuarios RBAC) cuando el usuario se autentica a través de SAML?

Este problema se debe a una configuración inadecuada de los desplazados internos. La clave aquí es que la información enviada por IDP durante la autenticación debe contener "Nombre de usuario" y "Grupos" como atributos en el xml. Si se utilizan otras cadenas en lugar de "Grupos", el grupo de usuarios es de forma predeterminada "Básico". Los usuarios "básicos" solo tienen acceso al panel básico.

Asegúrese de que IDP envíe "Nombre de usuario/Grupos", en lugar de "ID de usuario/rol" a vManage.

A continuación se muestra un ejemplo, como se muestra en el archivo /var/log/nms/vmanage-server.log:

Ejemplo no laborable:

Vemos que IdUsuario/rol ha sido enviado por IdP y el usuario está asignado al grupo *básico*.

```
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]
```

Ejemplo de trabajo:

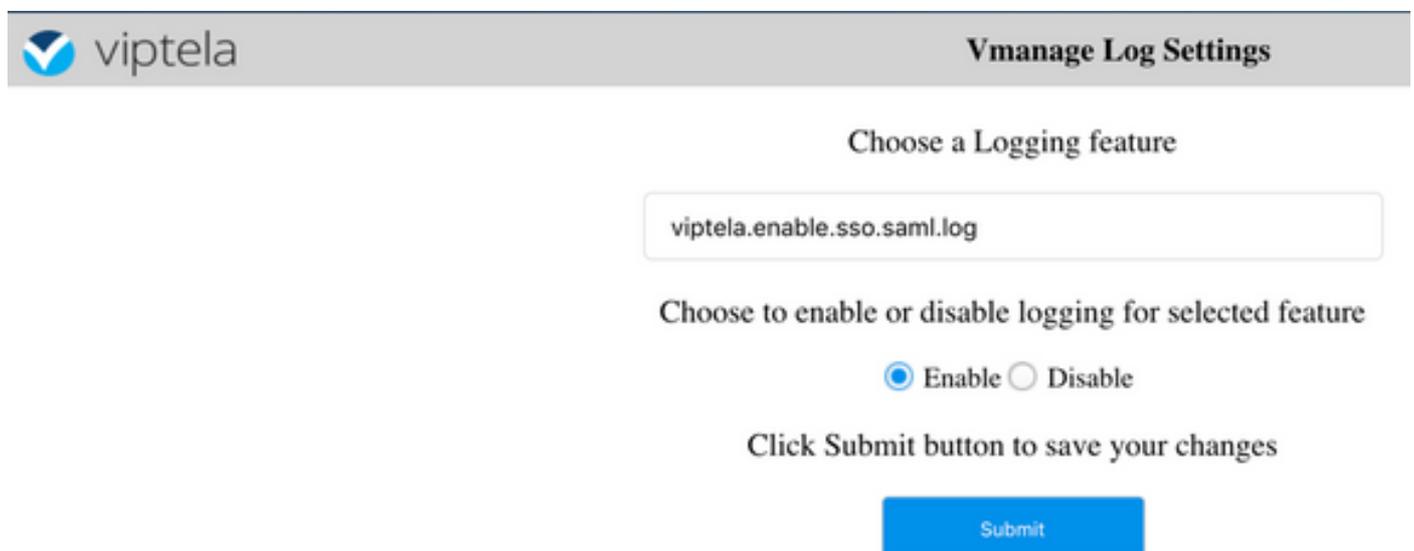
En esto verá "Username/Groups" (Nombre de usuario/Grupos) y el usuario se asignará al grupo netadmin.

```
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]
```

¿Cómo se habilita/verifica si SSO funciona?

El registro de depuración de funciones SSO se puede habilitar de la siguiente manera:

1. Vaya a https://<vManage_ip_addr:port>/logsettings.html
2. Seleccione el registro SSO y habilite el registro como se muestra en la imagen.



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'. Underneath is the heading 'Choose to enable or disable logging for selected feature'. There are two radio buttons: 'Enable' (which is selected) and 'Disable'. Below this is the instruction 'Click Submit button to save your changes'. At the bottom is a blue 'Submit' button.

3. Una vez habilitado, pulse el botón **Enviar**.

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

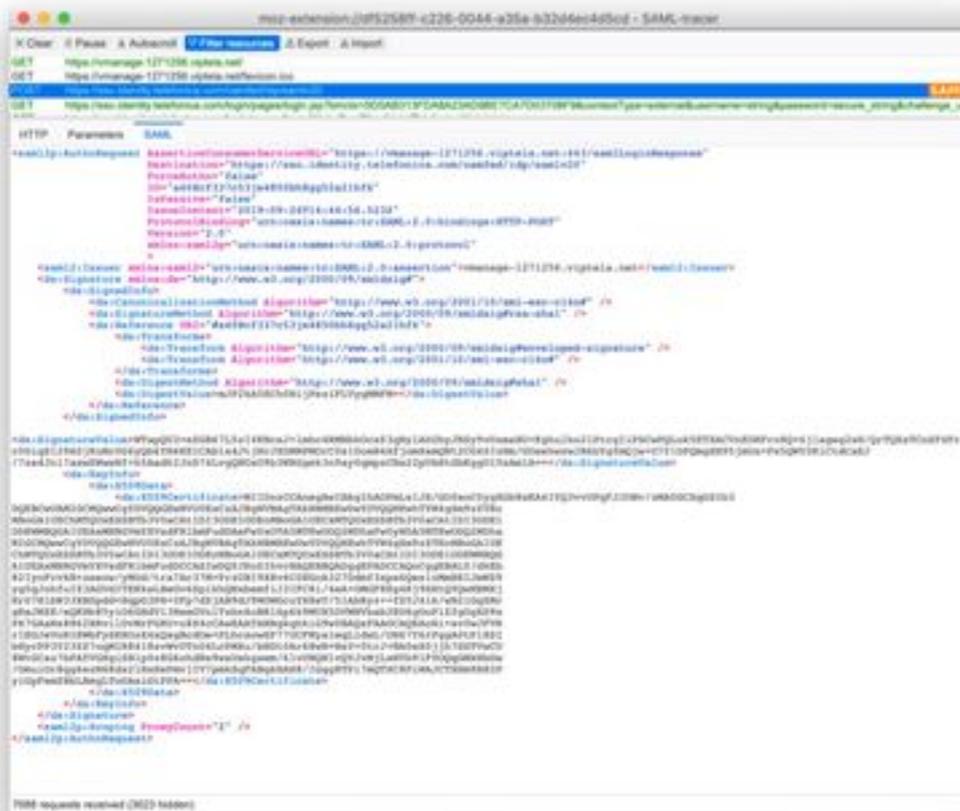
- Los registros relacionados con SSO se guardarán ahora en el archivo de registro vManage `/var/log/nms/vmanage-server.log` de particular interés es la configuración de "Grupos" para la autorización de IDP. Si no hay ninguna coincidencia, el usuario utilizará de forma predeterminada el grupo "Básico", que tiene acceso de sólo lectura;
- Para depurar el problema de privilegios de acceso, verifique el archivo de registro y busque la cadena "SamlUserGroups". A continuación, se muestra una lista de cadenas de nombres de grupo. Uno de ellos debe coincidir con la configuración del grupo en vManage. Si no se encuentra ninguna coincidencia, el usuario ha seleccionado de forma predeterminada el grupo "Básico".

SAML Tracer

Herramienta para ver mensajes SAML y WS-Federation enviados a través del navegador durante el inicio de sesión único y el cierre de sesión único.

[Complemento FireFox SAML-Tracer](#)

[Extensión cromada SAML-Tracer](#)



ejemplo de

mensaje SAML

¿Cómo iniciar sesión en vManage habilitado para SSO?

SSO es solo para el inicio de sesión en el navegador. Puede dirigir manualmente vManage a la página de inicio de sesión tradicional y omitir SSO para utilizar solamente el nombre de usuario y la contraseña: <https://<vmanage>:8443/login.html>.

¿Qué algoritmo de cifrado se utiliza?

Actualmente, es compatible con SHA1 como algoritmo de cifrado. vManage firmará el archivo de metadatos SAML con el algoritmo SHA1 que los IdPs deben aceptar. El soporte para SHA256 está llegando en futuras versiones, que actualmente no tenemos el soporte.

Información Relacionada

Configurar el inicio de sesión único:

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

Registros de trabajo de inicio/cierre de sesión de OKTA asociados al caso como referencia.