

vManage: Come controllare e verificare Single Sign-On

Sommario

[Introduzione](#)

[Terminologia](#)

[Che cosa sono le funzionalità?](#)

[Come attivarlo su vManage?](#)

[Che cos'è il flusso di lavoro?](#)

[vManage supporta l'autenticazione a due fattori e in che modo è diversa dall'SSO?](#)

[Quanti ruoli sono presenti nella soluzione?](#)

[Quali provider di identità supportiamo?](#)

[Come indicare l'appartenenza al gruppo di utenti nell'asserzione SAML?](#)

[Come attivare/verificare il funzionamento di SSO?](#)

[Tracer SAML](#)

[messaggio SAML di esempio](#)

[Come accedere a vManage abilitato per SSO?](#)

[Quale algoritmo di crittografia viene utilizzato?](#)

[Informazioni correlate](#)

Introduzione

In questo documento vengono descritte le nozioni di base per abilitare Single Sign On (SSO) su vManage e per verificare su vManage quando questa funzionalità è abilitata. A partire dalla versione 18.3.0, vManage supporta l'SSO. L'SSO consente a un utente di accedere a vManage tramite l'autenticazione tramite un provider di identità (IP) esterno. Questa funzionalità supporta la specifica SAML 2.0 per SSO.

Contributo di Shankar Vemulapalli, Cisco TAC Engineer.

Terminologia

Security Assertion Markup Language (SAML) è uno standard aperto per lo scambio di dati di autenticazione e autorizzazione tra parti, in particolare tra un provider di identità e un fornitore di servizi. Come indica il nome, SAML è un linguaggio di markup basato su XML per le asserzioni di protezione (istruzioni utilizzate dai provider di servizi per prendere decisioni sul controllo dell'accesso).

Un provider di identità (IdP) è "un provider attendibile che consente di utilizzare Single Sign-On (SSO) per accedere ad altri siti Web". L'SSO riduce l'usura della password e migliora la fruibilità. Diminuisce la superficie di attacco potenziale e fornisce una migliore sicurezza.

Provider di servizi - Si tratta di un'entità di sistema che riceve e accetta asserzioni di autenticazione insieme a un profilo SSO del SAML.

Che cosa sono le funzionalità?

- È supportato solo SAML2.0
- Supportato per: tenant singolo (standalone e cluster), multi tenant (sia a livello di provider che a livello di tenant). Inoltre, le distribuzioni multi tenant sono cluster per impostazione predefinita. Provider-as-tenant non applicabile.
- Ogni tenant può avere il proprio provider di identità univoco se l'idp segue la specifica SAML 2.0.
- Supporta la configurazione dei metadati IDP tramite il caricamento di file, la copia in testo normale e il download di metadati vManage.
- È supportato solo l'SSO basato su browser.
- In questa release non è possibile configurare i certificati utilizzati per gestire i metadati. Si tratta di un certificato autofirmato, creato la prima volta che si abilita SSO, con i seguenti parametri:

Stringa CN = <TenantName>, DefaultTenant

Stringa OU = <Nome organizzazione>

Stringa O = <Nome Organizzazione Sp>

Stringa L = "San Jose";

Stringa ST = "CA";

Stringa C = "USA";

Validità stringa = 5 anni;

Algoritmo di firma del certificato: SHA256ConRSA

Algoritmo di generazione della coppia di chiavi: RSA

- Accesso singolo - Supporto di SP avviato e IDP avviato
- Disconnessione singola - Solo SP avviato

Come attivarlo su vManage?

Per abilitare Single Sign-On (SSO) per vManage NMS per consentire l'autenticazione degli utenti tramite un provider di identità esterno:

1. Assicurarsi di aver abilitato NTP su vManage NMS.
2. connettersi alla GUI vManage con l'URL configurato su IdP
(ad esempio, vmanage-112233.viptela.net e non utilizzare IP-Address, perché queste informazioni sull'URL sono incluse nei metadati SAML)
3. Fare clic sul pulsante Modifica a destra della barra Impostazioni provider di identità.
4. Nel campo Attiva provider di identità fare clic su Attivato,
5. Copiare e incollare i metadati del provider di identità nella casella Carica metadati provider di identità. In alternativa, fare clic su Selezionare un file per caricare il file di metadati del provider di identità.
6. Fare clic su Salva.

Che cos'è il flusso di lavoro?

1. L'utente abilita l'SSO tramite la pagina Amministrazione->Impostazioni caricando i metadati

del provider di identità.

2. L'utente scarica quindi i metadati del tenant vManage corrispondenti da caricare nel provider di identità (operazione da eseguire almeno una volta per generare i metadati vManage).
3. Se necessario, l'utente può disabilitare o aggiornare i metadati in qualsiasi momento.

Esempio di metadati vManage

```
...<!--></pre></div><div data-bbox="57 655 920 705" data-label="Section-Header"><h2>vManage supporta l'autenticazione a due fattori e in che modo è diversa dall'SSO?</h2></div><div data-bbox="57 725 940 795" data-label="Text"><p>L'autenticazione a due fattori (nota anche come 2FA) è un tipo, o sottoinsieme, di autenticazione a più fattori (MFA). Si tratta di un metodo per confermare le identità dichiarate dagli utenti utilizzando una combinazione di due fattori diversi: 1) qualcosa che sanno, 2) qualcosa che hanno, o 3) qualcosa che sono.</p></div><div data-bbox="57 810 670 830" data-label="Text"><p>Esempio: Google GMail (password con password monouso (OTP))</p></div><div data-bbox="57 845 850 880" data-label="Text"><p>2FA viene fornito sul server SSO. La procedura di accesso è simile a quella utilizzata per accedere al sito Web interno di Cisco.</p></div><div data-bbox="57 895 900 915" data-label="Text"><p>Viene quindi reindirizzato all'SSO Cisco, dove viene richiesto di immettere PingID / DUO 2FA.</p></div></html>
```

Quanti ruoli sono presenti nella soluzione?

Abbiamo 3 rulli. basic, operator, netadmin.

[Configurazione dell'accesso utente e dell'autenticazione](#)

Quali provider di identità supportiamo?

- Okta
- IDping
- ADFS

I clienti possono utilizzare altri IdP e vedere se funziona. Ciò rientrerebbe nel "massimo sforzo"

Ad esempio, Microsoft Azure AD NON è ancora supportato dall'IDP. Ma potrebbe funzionare, date alcune riserve.

Altri sono: Oracle Access Manager, F5 Networks

Nota: Per gli IdP più recenti supportati da vManage, consultare la documentazione Cisco più recente

Come indicare l'appartenenza al gruppo di utenti nell'asserzione SAML?

Problema: front-end di vManage con un provider di identità SAML. Quando l'utente viene autenticato correttamente, l'unica cosa a cui può accedere è il dashboard.

È possibile concedere all'utente maggiore accesso (tramite il gruppo di utenti RBAC) quando l'utente viene autenticato tramite SAML?

Questo problema è causato da una configurazione non corretta di IDP. La chiave è che le informazioni inviate da IDP durante l'autenticazione devono contenere "Username" e "Groups" come attributi nel file xml. Se invece di "Gruppi" vengono utilizzate altre stringhe, per impostazione predefinita il gruppo utenti sarà "Base". Gli utenti di base hanno accesso solo al dashboard di base.

Accertarsi che IDP invii a vManage "Nome utente/Gruppi" anziché "ID utente/ruolo".

Di seguito è riportato un esempio come mostrato nel file /var/log/nms/vmanage-server.log:

Esempio non lavorativo:

Viene visualizzato il messaggio "UserId/role" inviato da IdP e l'utente è mappato al gruppo di *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]

Esempio:

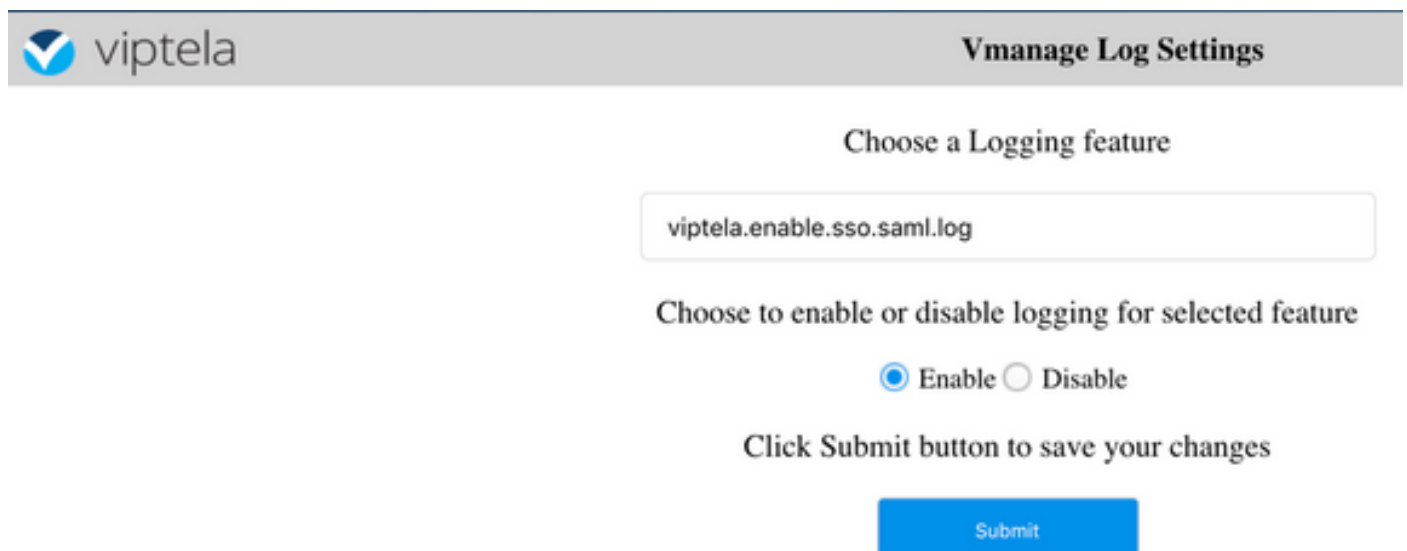
In questa schermata viene visualizzato "Nome utente/Gruppi" e l'utente è mappato al gruppo netadmin.

```
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]
```

Come attivare/verificare il funzionamento di SSO?

La registrazione debug delle funzionalità SSO può essere abilitata nel modo seguente:

1. Passare a https://<vManage_ip_addr:port>/logsettings.html
2. Selezionare la registrazione SSO e abilitarla come mostrato nell'immagine.



The screenshot shows the 'Vmanage Log Settings' interface. At the top left is the Viptela logo. The page title is 'Vmanage Log Settings'. Below the title, there is a section titled 'Choose a Logging feature' with a text input field containing 'viptela.enable.sso.saml.log'. Underneath, there is a section titled 'Choose to enable or disable logging for selected feature' with two radio buttons: 'Enable' (which is selected) and 'Disable'. Below this, there is a text instruction: 'Click Submit button to save your changes' and a blue 'Submit' button.

3. Una volta abilitato, fare clic sul pulsante **Sottometti**.

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

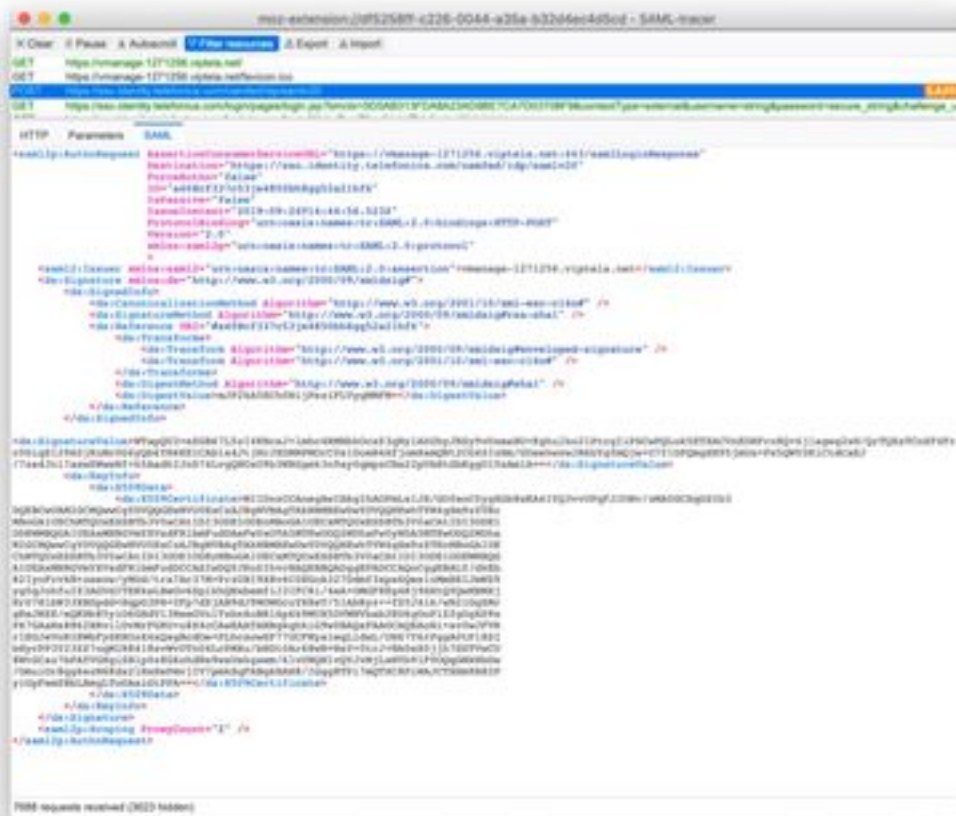
- I log relativi all'SSO verranno ora salvati nel file di log di vManage `/var/log/nms/vmanage-server.log` di particolare interesse è l'impostazione "Groups" per l'autorizzazione IDP. Se non vi sono corrispondenze, l'utente utilizzerà il gruppo "Basic", che dispone di accesso in sola lettura;
- Per eseguire il debug del problema relativo ai privilegi di accesso, controllare il file di log e cercare la stringa "SamlUserGroups". Segue un elenco di stringhe di nomi di gruppi. Una di esse deve corrispondere alle impostazioni di gruppo in vManage. Se non viene trovata alcuna corrispondenza, l'utente ha utilizzato il gruppo "Basic" come impostazione predefinita.

Tracer SAML

Strumento per la visualizzazione dei messaggi SAML e WS-Federation inviati tramite il browser durante l'accesso singolo e la disconnessione singola.

[Componente aggiuntivo FireFox SAML-Tracer](#)

[Estensione Chrome SAML-Tracer](#)



messaggio

SAML di esempio

Come accedere a vManage abilitato per SSO?

SSO è disponibile solo per l'accesso tramite browser. È possibile indirizzare manualmente vManage alla pagina di accesso tradizionale e ignorare l'SSO per utilizzare solo il nome utente e la password: <https://<vmanage>:8443/login.html>.

Quale algoritmo di crittografia viene utilizzato?

Attualmente è supportato SHA1 come algoritmo di crittografia. vManage firmerà il file di metadati SAML con l'algoritmo SHA1 che gli IdP devono accettare. Il supporto per SHA256 sarà disponibile nelle versioni future, ma attualmente non è disponibile.

Informazioni correlate

Configurare Single Sign-On:

<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-16/security-book-xe/configure-ss0.html>

OKTA LogIn/Logout log di lavoro collegati alla richiesta come riferimento.