vManager: Inschakelen en controleren van één teken

Inhoud

Inleiding

In dit document worden de basisbeginselen beschreven om Single Sign On (SSO) op vManager mogelijk te maken en om op vManager te controleren/controleren, wanneer deze optie is ingeschakeld. Om te beginnen met 18.3.0 ondersteunt vManager SSO. SSO biedt een gebruiker de mogelijkheid om in te loggen op vManager door verificatie tegen een externe Identity Provider (IP). Deze optie ondersteunt SAML 2.0 specificatie voor SSO.

Bijgedragen door Shankar Vemulapalli, Cisco TAC Engineer.

Terminologie

Security Assertion Markup Language (SAML) is een open standaard voor het uitwisselen van gegevens over authenticatie en autorisatie tussen partijen, met name tussen een identiteitsaanbieder en een dienstverlener. Zoals de naam al zegt, is SAML een op XML gebaseerde markup-taal voor veiligheidsbeweringen (verklaringen die dienstverleners gebruiken om beslissingen te nemen over toegangscontrole).

Een Identity Provider (IDP) is "een vertrouwde provider die u één aanmelding (SSO) kunt gebruiken om toegang te krijgen tot andere websites." SSO vermindert de wachtwoordvermoeidheid en verbetert de bruikbaarheid. Het vermindert het potentiële oppervlak van de aanval en biedt betere beveiliging.

Serviceprovider - Het is een systeementiteit die in combinatie met een SSO-profiel van het SAML verificatiebeweringen ontvangt en accepteert.

Wat zijn de mogelijkheden?

- Alleen SAML2.0 wordt ondersteund
- Ondersteund voor - één-huurslang (standalone en cluster), multi-Tenant (zowel op het niveau van de leverancier als op huurniveau), ook, multiTenant implementaties zijn per default cluster. Als huurder van de leverancier is niet van toepassing.
- Elke huurder kan zijn eigen unieke identiteitsverschaffer hebben, zolang de idp zich houdt aan SAML 2.0.
- Ondersteunt configuratie van IDP-metagegevens via het uploaden van bestanden evenals onbewerkte tekst en het downloaden van vManager-metagegevens.
- Alleen op een browser gebaseerde SSO wordt ondersteund.
- Certificaten die worden gebruikt voor metagegevens zijn niet Configureerbaar in deze release. het is een zelfgetekend certificaat, dat is gemaakt wanneer u SSO voor het eerst instelt, met de volgende parameters:

  String CN = <tenantName>, DefaultTenant

  String OU = <naam van OCR>
  String O = <p org naam>
  String L = "San Jose";
  String ST = "CA";
  String C = "USA";
  String-geldigheid = 5 jaar;
  Algoritme voor certificatie: SHA256W met RSA
  KeyPair Generation-algoritme: RSA

- Single Login - SP geïnitieerd en IDP geïnitieerd
- Enkelvoudige aanmelding - alleen SP geïnitieerd

Hoe kan het op vManager inschakelen?

Om één aanmelding (SSO) voor vManager-NMS mogelijk te maken zodat gebruikers gewaarmerkt kunnen worden met behulp van een externe identiteit provider:

1. Zorg ervoor dat u NTP op vManager NMS hebt ingeschakeld.
2. Sluit aan op vManager GUI met de URL die op IDP is ingesteld (bv. vmanagement-112233.viptela.net en gebruik geen IP-adres, omdat deze URL-informatie in SAML-metagegevens is opgenomen)
3. Klik op de knop Bewerken rechts van de balk Instellingen voor Identity Provider.
4. Klik in het veld Identity Provider inschakelen op Ingeschakeld.
5. Kopieer en plak de metagegevens van de identiteitskaart in het vakje Upload Identity Provider. Of klik op Selecteer een bestand om het metagegevensbestand van de identiteit te uploaden.
6. Klik op Opslaan.

Wat is de werkstroom?

1. Gebruiker stelt SSO in via de pagina Instellingen beheer->door de metagegevens van de

identiteitsprovider te uploaden.
2. Gebruiker downloads vervolgens de corresponderende vManager-metagegevens die op de identiteit provider moeten worden geüpload (dit moet minimaal één keer gebeuren om metagegevens voor vManager te genereren).
3. Gebruiker kan metadata indien nodig op elk moment uitschakelen of bijwerken.

Steekproef vManager Meta

Ondersteunt vManager tweedelige verificatie en hoe deze verschilt van SSO?

Two-Factor Authentication (ook bekend als2FA) is een type of subset van multifactor authenticatie (MFA). Het is een methode om de beweerde identiteit van gebruikers te bevestigen door gebruik te maken van een combinatie van twee verschillende factoren: 1) iets wat ze weten, 2) iets wat ze hebben, of 3) iets wat ze zijn.

Voorbeeld: Google GMail (Wachtwoord met Wachtwoord voor één keer (OTP)

2FA is iets dat op de SSO-server zal worden geleverd. Het is vergelijkbaar met de manier waarop we inloggen op de interne website van Cisco.

Het wijst u terug naar Cisco SSO, waar u wordt gevraagd voor PingID / DUO 2FA.

Hoeveel rollen zijn er als onderdeel van de oplossing?

We hebben drie rollen; basis, exploitant, netadmin.

Gebruikerstoegang en -verificatie configureren

Welke ID's steunen we?

- Okta
- PingID
- ADFS

Klanten kunnen andere IDs gebruiken en kunnen dit bekijken. Dit zou onder de "best inspanning" vallen

Een voorbeeld hiervan is MSFT KRI AD (nog). Maar het kan werken, gegeven sommige uitzonderingen.

Andere omvatten: Oracle Access Manager F5-netwerken

> **Opmerking:** Controleer de nieuwste Cisco-documentatie voor de nieuwste IDs die worden ondersteund door vManager

Hoe wordt het lidmaatschap van de gebruikersgroep in SAML aangegeven?

Probleem: voorkant het vManager met een SAML IDP. Wanneer de gebruiker voor authentiek is verklaard, is het enige wat de gebruiker kan hebben het dashboard.

Is er een manier om de gebruiker meer toegang te geven (via gebruikersgroep RBAC) wanneer de gebruiker geauthentiseerd is via SAML?

Dit probleem wordt veroorzaakt door een onjuiste configuratie van de IDP. De sleutel is dat de informatie die door IDP tijdens de authenticatie wordt verzonden "Gebruikersnaam" en "Groepen" als eigenschappen in de xml moet bevatten. Als andere strings worden gebruikt in plaats van "Groepen", dan is de gebruikersgroep standaard op "Basic". "Basisgebruikers hebben alleen toegang tot het basisdashboard.

Zorg ervoor dat IDP "Naam/groepen", in plaats van "GebruikerID/rol" naar vManager verstuurt. Hieronder zie je een voorbeeld in het /var/log/nms/vmanage-server.log-bestand:

Niet-werkbaar voorbeeld:

We zien dat "User ID/role" door IDP is verzonden en de gebruiker is in kaart gebracht in de *basisgroep*.

```
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]
```

Werkvoorbeeld:

Hierin ziet u "Gebruikersnaam/Groepen" en de gebruiker is in kaart gebracht in de netadmin groep.

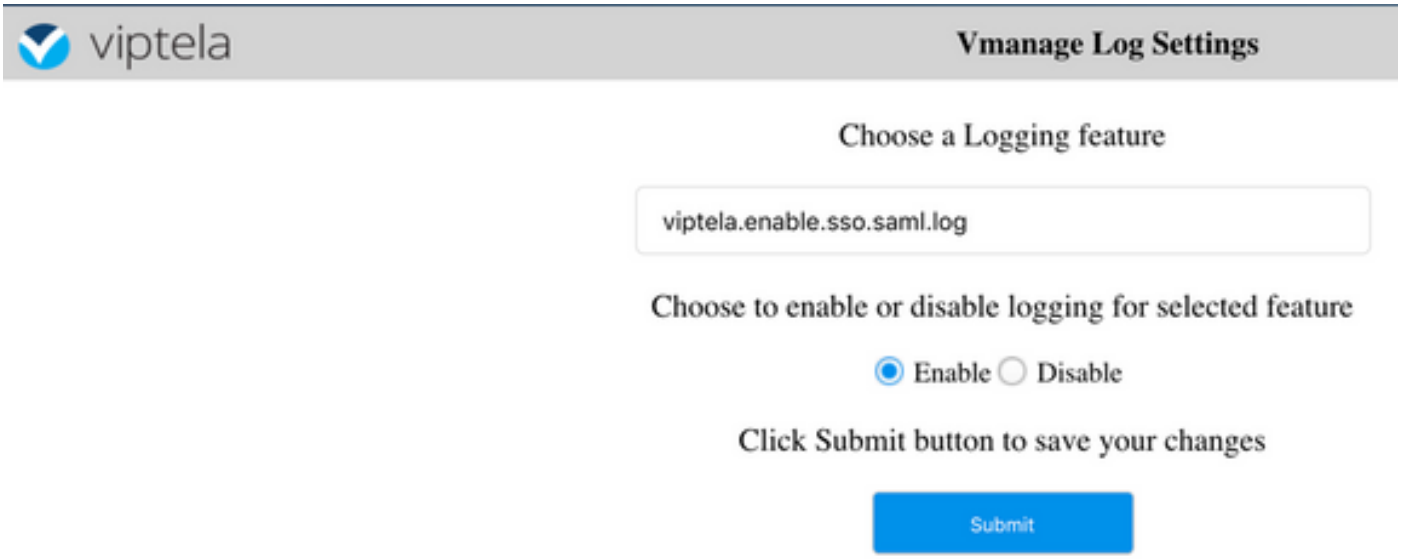
```
05-Mar-2019 21:35:55,766 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-90)
|default| AttributeMap: {UserName=[Tester@Example.MFA.com], Groups=[netadmin]}
05-Mar-2019 21:35:55,766 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-90)
|default| AttributeMap: {UserName=[Tester@Example.MFA.com],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

Hoe kan de SSO worden ingeschakeld of gecontroleerd?

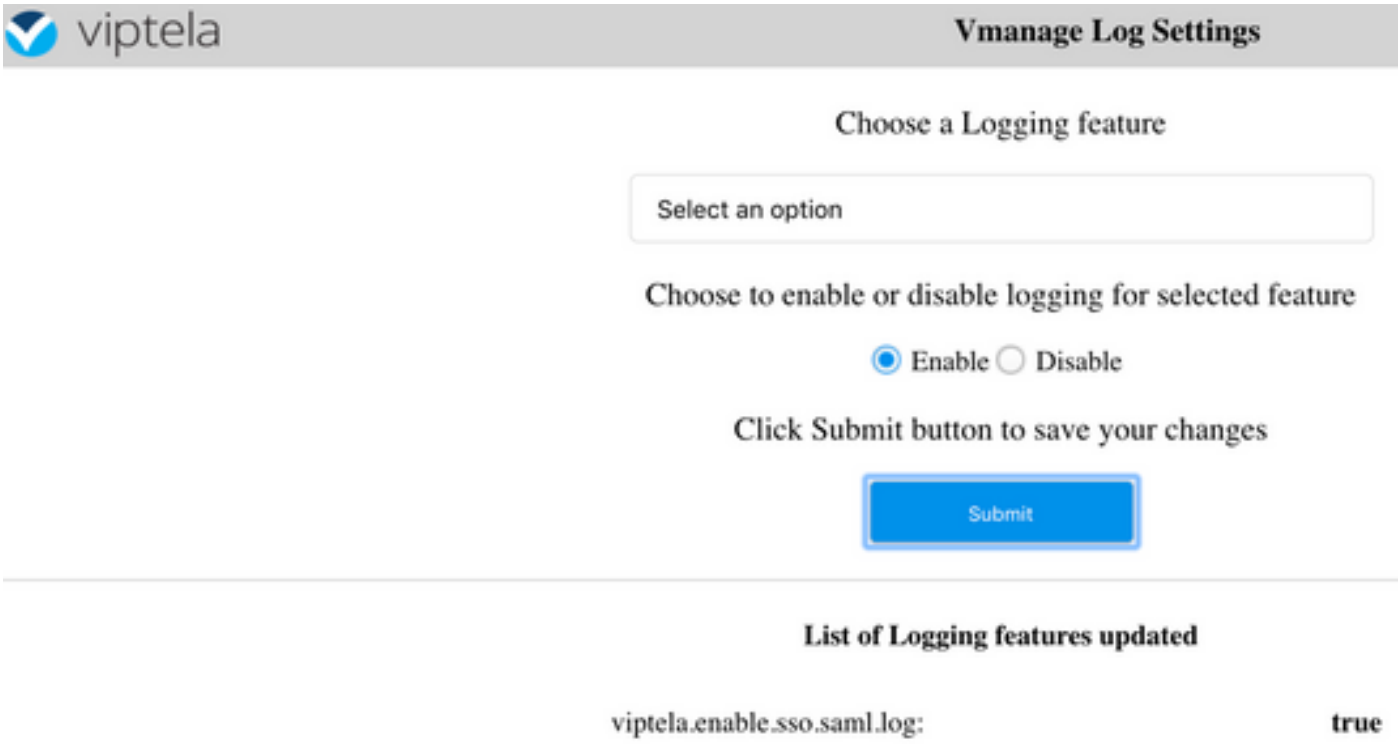
U kunt de volgende functies voor debug loggen inschakelen:

1. Navigeren naar **https://<vManager_ip_addr:poort>/logsettings.html**

2. Selecteer de SSO-vastlegging en schakelt u deze in zoals in de afbeelding.



3. Eenmaal ingeschakeld, drukt u op de knop **Indienen**.



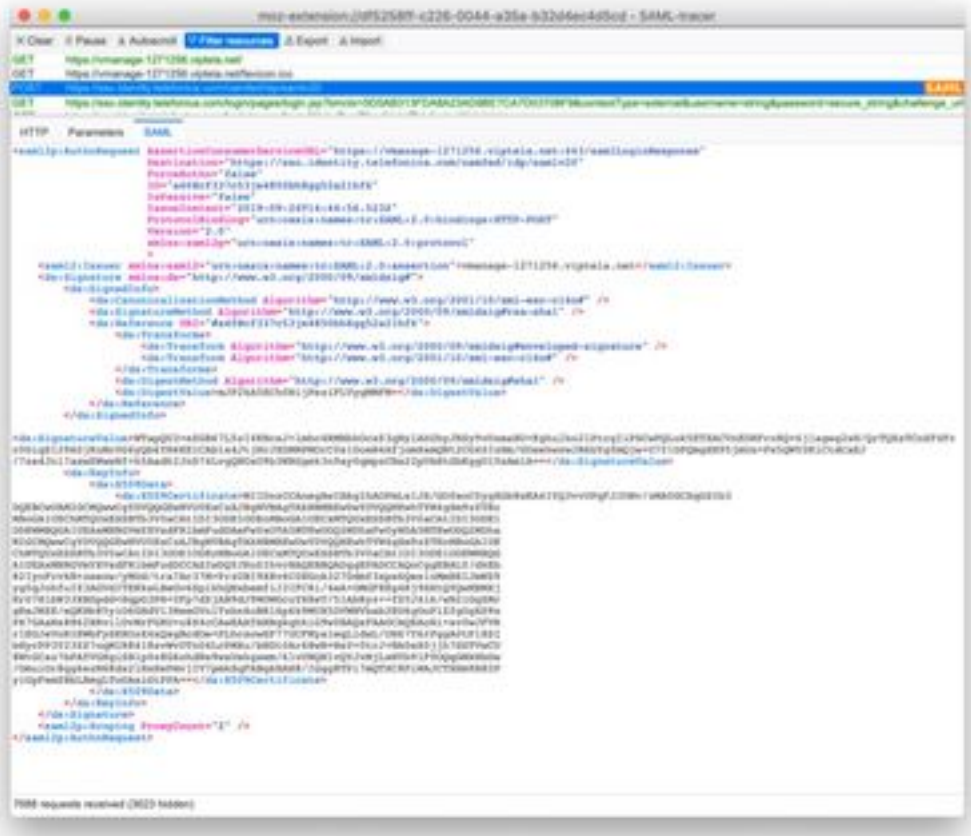
- De met SSO samenhangende logbestanden worden nu opgeslagen in het vManager-logbestand **/var/log/nms/vmanage-server.log** van bijzonder belang is de "Groepen"-instelling voor IDP-toestemming. Als er geen match is, zal de gebruiker in gebreke blijven op "Basic" groep, die alleen-lezen toegang heeft;
- Controleer het logbestand en zoek naar een string "SamlUserGroup" om het probleem van de toegangsrechten op te lossen. Wat volgt is dat een lijst van snaren van groepsnamen zou moeten zijn. Eén ervan moet overeenkomen met de groepsinstellingen op vManager. Als geen overeenkomst wordt gevonden, is de gebruiker standaard onderworpen aan de "Basic" groep.

SAML Tracer

Een hulpmiddel om de SAML- en WS-Federatie-berichten te bekijken die door de browser worden verstuurd tijdens één aanmelding en één logout.

FireFox SAML-Tracer add-on

Chroom SAML-Tracer-uitbreiding



staal SAML-bericht

Hoe inlogt u in op SSO-enabled vManager?

SSO is alleen voor aanmelding door browser. U kunt vManager handmatig rechtstreeks naar de traditionele inlogpagina en de SSO omzeilen, zodat u alleen de gebruikersnaam en het wachtwoord kunt gebruiken: **https://<beheer>:8443/login.html.**

Welk Encryptiealgoritme wordt gebruikt?

Momenteel ondersteunen we SHA1 als encryptie-algoritme. vManager zal het SAML meta-bestand met SHA1-algoritme ondertekenen dat IDs het moeten accepteren. De ondersteuning van SHA256 komt in toekomstige releases, die we momenteel niet hebben.

Gerelateerde informatie

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

OKTA Login / Logout werkdocumenten toegevoegd aan de case als referentie.