vManage: Como verificar o login único

Contents

Introduction

Este documento descreve os conceitos básicos para habilitar o SSO (Single Sign On, logon único) no vManage e como verificar/verificar no vManage, quando esse recurso estiver habilitado. Começando com 18.3.0, o vManage suporta SSO. O SSO permite que um usuário faça login no vManage autenticando em um provedor de identidade externo (IP). Este recurso suporta a especificação SAML 2.0 para SSO.

Contribuído por Shankar Vemulapalli, Engenheiro do TAC da Cisco.

Terminology

O SAML (Security Assertion Markup Language) é um padrão aberto para a troca de dados de autenticação e autorização entre as partes, em particular entre um provedor de identidade e um provedor de serviços. Como o nome indica, SAML é uma linguagem de marcação baseada em XML para asserções de segurança (declarações que os provedores de serviços usam para tomar decisões de controle de acesso).

Um provedor de identidade (IdP) é "um provedor confiável que permite usar o login único (SSO) para acessar outros sites." O SSO reduz a fadiga de senha e aumenta a usabilidade. Ela diminui a superfície de ataque potencial e oferece melhor segurança.

Provedor de serviços - É uma entidade de sistema que recebe e aceita asserções de autenticação juntamente com um perfil SSO do SAML.

Quais são os recursos?

- Somente SAML2.0 é suportado
- Suportado para - Locatário único (autônomo e cluster), Multilocatário (tanto no nível do provedor quanto no nível do locatário); além disso, as implantações multilocatário são agrupadas por padrão. O provedor como locatário não é aplicável.
- Cada espaço pode ter seu próprio provedor de identidade exclusivo, desde que o idp siga a especificação SAML 2.0.
- Suporta a configuração de metadados IDP através de upload de arquivos, bem como cópia de texto simples e download de metadados vManage.
- Somente SSO baseado em navegador é suportado.
- Os certificados usados para metadados vmanage não são configuráveis nesta versão.
  éum certificado autoassinado, criado na primeira vez que você ativa o SSO, com os seguintes parâmetros:

  String CN = <TenantName>, DefaultTenant

  OU da cadeia de caracteres = <Nome da empresa>
  String O = <Nome Da Empresa Sp>
  String L = "San Jose";
  String ST = "CA";
  String C = "EUA";
  Validade da string = 5 anos;
  Algoritmo de assinatura de certificado: SHA256Com RSA
  Algoritmo de geração de pares de chaves: RSA

- Login único - SP iniciado e IDP iniciado suportado
- Logoff único - SP iniciado somente

Como ativá-lo no vManage?

Para ativar o login único (SSO) para o vManage NMS para permitir que os usuários sejam autenticados usando um provedor de identidade externo:

1. Certifique-se de ter ativado o NTP no vManage NMS.
2. conectar-se à GUI do vManage com o URL configurado no IdP
   (por exemplo, vmanage-112233.viptela.net e não usar endereço IP, pois essas informações de URL estão incluídas em metadados SAML)
3. Clique no botão Editar à direita da barra Configurações do provedor de identidade.
4. No campo Ativar provedor de identidade, clique em Ativado,
5. Copie e cole os metadados do provedor de identidade na caixa Carregar metadados do provedor de identidade. Ou clique em Selecionar um arquivo para carregar o arquivo de metadados do provedor de identidade.
6. Click Save.

Qual é o fluxo de trabalho?

1. O usuário ativa SSO através da página Administration->Settings carregando os metadados do provedor de identidade.
2. Em seguida, o usuário faz o download dos metadados de espaço correspondentes do vManage a serem carregados no provedor de identidade (deve ser feito pelo menos uma

vez para gerar metadados do vManage).

3. O usuário pode desativar ou atualizar metadados a qualquer momento, se necessário.

Exemplo de meta do vManage

O vManage oferece suporte à Autenticação de dois fatores e como ela é diferente do SSO?

Autenticação de dois fatores (também conhecida como2FA) é um tipo, ou subconjunto, de autenticação de vários fatores (MFA). Trata-se de um método de confirmação das identidades reivindicadas pelos utilizadores, utilizando uma combinação de dois fatores diferentes: 1) algo que eles sabem, 2) algo que eles têm ou 3) algo que eles são.

Exemplo: Google GMail (Senha com senha única (OTP))

2FA é algo que será fornecido no Servidor SSO. É semelhante ao modo como fazemos login no site interno da Cisco.

Ele o redireciona para o Cisco SSO, onde será solicitado que você insira PingID / DUO 2FA.

Quantas funções fazem parte da solução?

Temos 3 rolos. básico, operador, netadmin.

Configurando o acesso de usuário e a autenticação

Com quais IDs oferecemos suporte?

- Okta
- PingID
- ADFS

Os clientes podem usar outros IdPs e vê-los funcionando. Isso seria feito sob o "melhor esforço"

Um exemplo disso seria o IDP do MSFT Azure AD NÃO suportado (ainda). Mas pode funcionar, dadas algumas das advertências.

Outros incluem: Oracle Access Manager, F5 Networks

> **Note**: Verifique a documentação mais recente da Cisco para obter os IdPs mais recentes suportados pelo vManage

Como indicar a associação ao grupo de usuários na asserção SAML?

Problema: o vManage com um ID de SAML IdP é encerrado pela frente. Quando o usuário é autenticado com êxito, a única coisa que o usuário pode acessar é o painel.

Há uma maneira de dar ao usuário mais acesso (através do grupo de usuários RBAC) quando o usuário é autenticado via SAML?

Esse problema é causado pela configuração incorreta do IDP. A chave aqui é que as informações enviadas pelo IDP durante a autenticação devem conter "Nome de usuário" e "Grupos" como atributos no xml. Se outras strings forem usadas no lugar de "Grupos", o grupo de usuários será padrão como "Básico". Os usuários "básicos" só têm acesso ao painel básico.

Certifique-se de que o IDP envie "Nome de usuário/grupos", em vez de "ID de usuário/função" para o vManage.
Veja abaixo um exemplo, como visto no arquivo /var/log/nms/vmanage-server.log:

Exemplo não funcional:

Vemos que "UserId/role" foi enviado pelo IdP e o usuário está mapeado para o 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]
```

Exemplo de trabalho:

Nesse caso, você verá "Nome de usuário/Grupos" e o usuário será mapeado para o grupo netadmin.

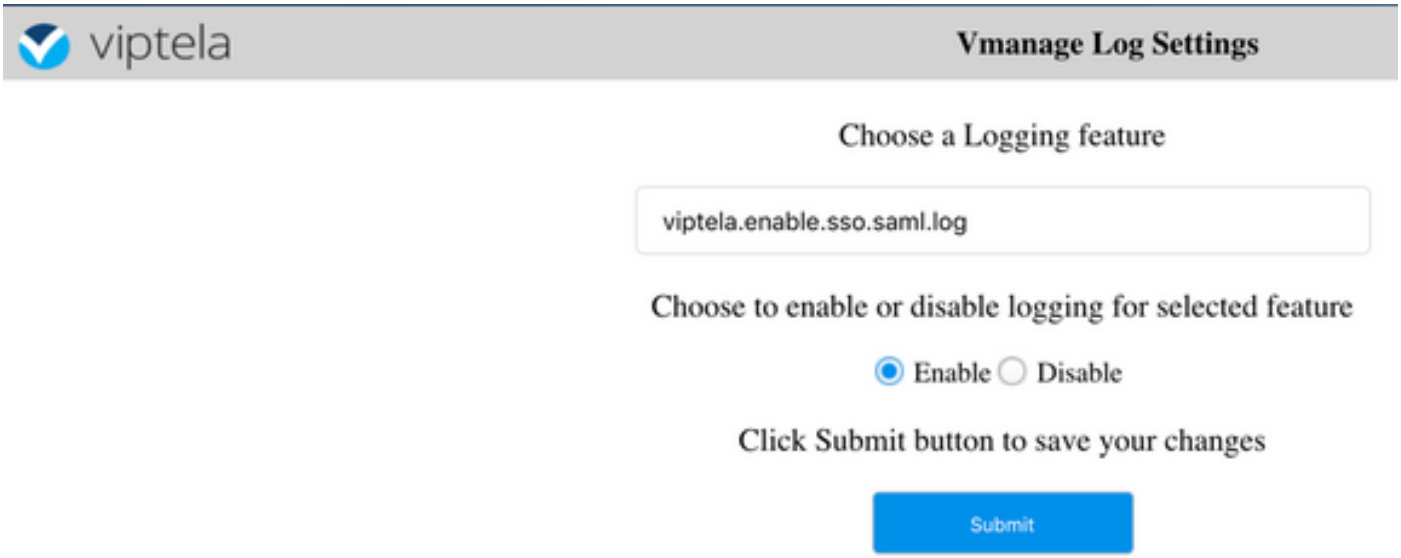
```
05-Mar-2019 21:35:55,766 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-90)
|default| AttributeMap: {UserName=[Tester@Example.MFA.com], Groups=[netadmin]}
05-Mar-2019 21:35:55,766 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-90)
|default| AttributeMap: {UserName=[Tester@Example.MFA.com],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

Como ativar/verificar se o SSO funciona?

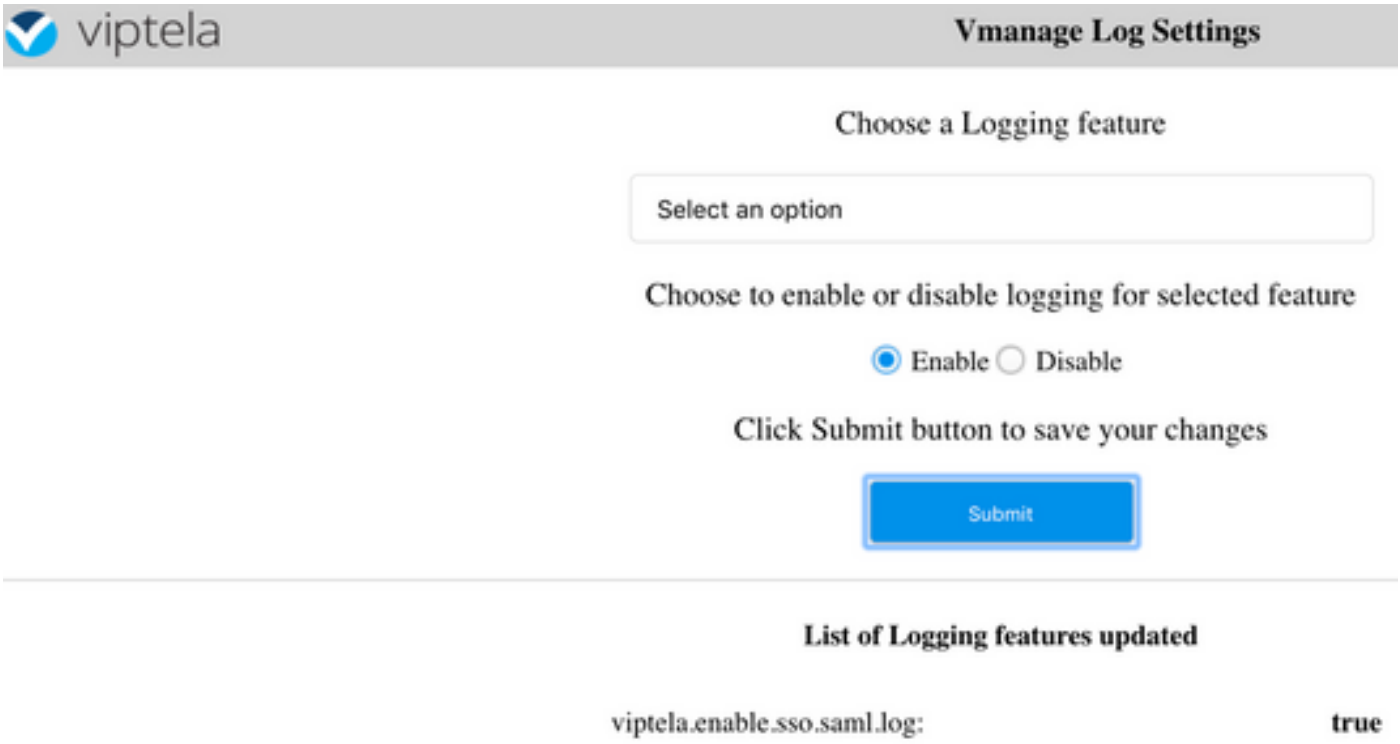
O log de depuração do recurso SSO pode ser ativado da seguinte maneira:

1. Navegue até **https://<vManage_ip_addr:port>/logsettings.html**

2. Selecione o registro SSO e ative-o como mostrado na imagem.



3. Depois de Habilitado, pressione o botão **Submit (Enviar)**.



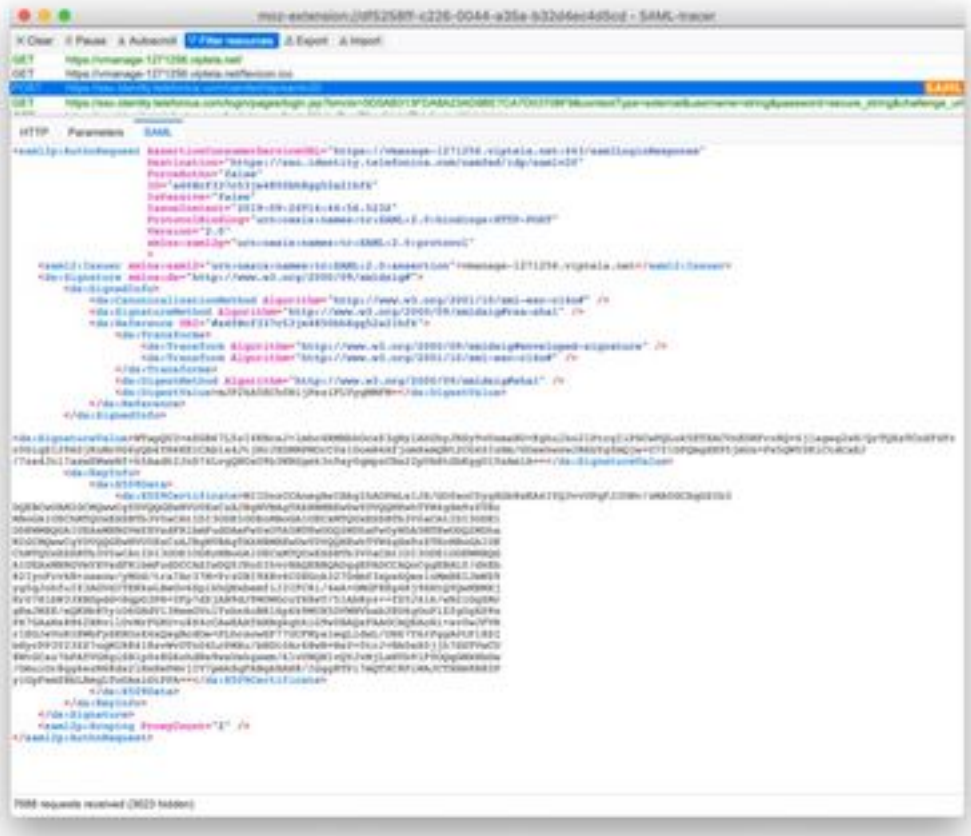
- Os registros relacionados ao SSO serão salvos no arquivo de log do vManage **/var/log/nms/vmanage-server.log** de particular interesse é a configuração "Grupos" para autorização do IDP. Se não houver correspondência, o usuário usará como padrão o grupo "Básico", que tem acesso somente leitura;
- Para depurar o problema de privilégio de acesso, verifique o arquivo de log e procure a string "SamlUserGroups". O que se segue deve ser uma lista de strings de nomes de grupos. Um deles deve corresponder às configurações de grupo no vManage. Se não for encontrada nenhuma correspondência, o usuário assume como padrão o grupo "Básico".

SAML Tracer

Uma ferramenta para exibir mensagens SAML e WS-Federation enviadas pelo navegador durante logon único e logoff único.

Complemento FireFox SAML-Tracer

Chrome SAML-Tracer Extension



exemplo de mensagem SAML

Como fazer login no vManage habilitado para SSO?

SSO é apenas para login do navegador. Você pode direcionar manualmente o vManage para a página de login tradicional e ignorar SSO para usar somente o nome de usuário e a senha: **https://<vmanage>:8443/login.html.**

Que algoritmo de criptografia é usado?

Atualmente, oferecemos suporte a SHA1 como algoritmo de criptografia. O vManage assinará o arquivo de metadados SAML com algoritmo SHA1 que os IdPs precisam aceitar. O suporte para SHA256 está chegando em versões futuras, que não temos suporte atualmente.

Informações Relacionadas

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

Login OKTA / Logoff dos logs de trabalho anexados ao caso como referência.