# vManage:如何检查和验证单点登录

### 目录

<u>简介</u> <u>术语</u> <u>哪些功能?</u> <u>如何在vManage上启用它?</u> <u>工作流程是什么?</u> <u>vManage是否支持双因素身份验证,以及它与SSO有何不同?</u> <u>作为解决方案的一部分,有多少角色?</u> <u>我们支持哪个IdP?</u> <u>如何在SAML断言中指示用户组成员?</u> <u>如何在SAML断言中指示用户组成员?</u> <u>如何启用/检查SSO是否有效?</u> <u>SAML Tracer</u> <u>示例SAML消息</u> <u>如何登录启用SSO的vManage?</u> <u>使用什么加密算法?</u> 相关信息

## 简介

本文档介绍在vManage上启用单点登录(SSO)的基本知识,以及启用此功能后如何在vManage上检查/验证。从18.3.0开始,vManage支持SSO。SSO允许用户通过对外部身份提供程序(IP)进行身份 验证来登录vManage。此功能支持SSO的SAML 2.0规范。

作者:Shankar Vemulapalli, Cisco TAC工程师。

## 术语

安全断言标记语言(SAML)是一种开放标准,用于在各方之间,特别是在身份提供者和 服务提供商 。正如其名称所暗示的,SAML是一种基于XML的安全断言标记语言 (服务提供商用于制定访问控 制决策的语句)。

身份提供程序(IdP)是"可以使用单点登录(SSO)访问其他网站的受信任提供程序"。SSO可减少密码 疲劳并增强可用性。它降低了潜在攻击面并提供更好的安全性。

服务提供商-它是一个系统实体,与SAML的SSO配置文件一起接收和接受身份验证断言。

### 哪些功能?

- 仅支持SAML2.0
- 支持 单租户(独立和集群)、多租户(提供商级和租户级),此外,多租户部署默认为集群。
   。提供商即租户不适用。
- •只要idp遵循SAML 2.0规范,每个租户都可以拥有自己的唯一身份提供程序。

- 支持通过文件上传以及纯文本复制和vManage元数据下载来配置IDP元数据。
- 仅支持基于浏览器的SSO。
- 此版本中不能配置用于vmanage元数据的证书。
   它是自签名证书,首次启用SSO时创建,其参数如下:
   字符串CN = <TenantName>. DefaultTenant

```
字符串OU = <组织名称>
字符串O = <SP组织名称>
字符串L ="圣何塞";
字符串ST ="CA";
字符串C ="USA";
字符串有效性= 5年;
证书签名算法:SHA256WithRSA
密钥对生成算法:RSA
```

- 单次登录 支持SP发起和IDP发起
- 单次注销 仅SP启动

### 如何在vManage上启用它?

要为vManage NMS启用单点登录(SSO),以允许使用外部身份提供程序对用户进行身份验证:

- 1. 确保已在vManage NMS上启用NTP。
- 使用在IdP上配置的URL连接到vManage GUI (例如vmanage-112233.viptela.net,不使用IP-Address,因为此URL信息包含在SAML元数据 中)
- 3. 点击身份提供程序设置栏右侧的编辑按钮。
- 4. 在启用身份提供程序(Enable Identity Provider)字段中,点击启用(Enabled),
- 5. 在上传身份提供程序元数据框中复制并粘贴身份提供程序元数据。或点击选择文件以上传身份 提供程序元数据文件。
- 6. Click Save.

#### 工作流程是什么?

- 1. 用户通过上传身份提供程序元数据,通过"管理"(Administration)->"设置"(Settings)页面启用 SSO。
- 然后,用户下载要上传到身份提供程序的相应vManage租户元数据(必须至少完成一次才能生成vManage元数据)。
- 3. 用户可以根据需要随时禁用或更新元数据。

vManage元示例

sed dettingfereringter interiet/unitationalistaneeristations, 10-10.46.40.40.40.40.40.40.40.40.40.40.40.40.40.	
shall get fair with a drift by the state of	
<pre>contraction[int]int[interved.4]got[intervetp(//www.eb.org/DWI/D4/wel-enc-chewP/h</pre>	
relu-11grad-uselfected: Alger:1994m/1994gr.//www.adl.org/2006/09/wr0de1gd/maceba01/11	
tako Barteraman Millor Mila. Ak. 2014 r	
<ul> <li>Statistics</li> <li>Statis</li> <li>Statisting</li> <li>Statisting</li>     &lt;</ul>	
AND THE PART AND THE THE ADDRESS AND ADDRESS AND ADDRESS AND ADDRESS ADDRE ADDRESS ADDRESS ADD	
vite: Transferen	
nde strigendfieldeni útgenstelkes/histors/view.ed. ang/1008/04/indexighted////	
sis Toper relate by (Helder all) of DRI (1997) is Toper (Helder	
4 YES /R File (a) A	
HIS TO PERSONNAL AND AND ADDRESS OF THE ADDRESS OF	
References and the second s	
DISPATISED CONTRACTOR (Experimentation)	
All And I Mark	
where the information of the processing lines in a factor of the proceeding of the processing of the processing lines of the p	
ECHICAL UNIVERSITATION FOR VERY TO VERY TO ALL LOCATION OF THE VERY VERY TO VERY VERY VERY TO VERY VERY VERY VERY VERY VERY VERY VERY	
ExPERSION THEN DEPARTMENT OF THE ADDRESS OF A DEPARTMENT	
TOTAL DEVICES AND ADDRESS AND ADDRESS AND ADDRESS ADDR	
The Theorem Theorem is a more in the theorem and the second in the secon	
Kontral Michiga (Problem) and a finite Anna Canada and Anna Anna Anna Anna Anna Anna	
accession (weight construct and the first construction) (weight accession) and the construction of the con	
eC11e-Weirreiter (herrich) geware et al Weirreit (herrich) and an	
Control de la	
Reserve a Problem of Audio Contractor ( March and Audio Contractor ( Audio Contra	
ephotexehineDrutesDvHz-tapRetexee4080F80790Pepy48F02F91904a0206e1020a8F	
RECEIVE AND CONTRACT OF TAXABLE AND A DEPARTMENT OF A DEPARTMENT OF TAXABLE AND A DEPARTMENT OF TAXABL	
PUP / 1204 (2004) 2004 (2004) (2004) (2004 (20))))))))))))))))))))))))))))))))))))	
1/2/2/2019/9/1/2/	
1. Table of any Star Free Star Star Star Star Star Star Star Star	
<ul> <li>A text chapter turks</li> </ul>	
and dependence in the providence of the providen	
<ul> <li>Non-independent and a start of the start (start of the start (start of the start of the start of the start (start of the start (start of the start of the start (start of the start of the</li></ul>	
daulaetta-	
101200001011511212121210100000000000000	
PERIOD AND COMPACT AND TRANSPORTED AND ADDRESS OF THE DATA	
Conservations of the comparison of the region of the conservation of the conservationo	
EPERATURE INFORMATION OF THE ADDRESS	
FTWTB/FIRM-TEPRETER/LIMANELIZATE/MIRE/PUT/CHAP KLAP (#DEL/ALL #007/04/21	
Frankel Billerung (Predictional geschletter) (Predictional State) (Predictional Predictional Pre	
Benderschutz (PP) wir hat (PP) wir and (PP) wir hat (PP)	
Charles (200 / Purchash and a control of control and a control of the control of	
IP/INSUSSING/OFFICE/IP/INSUS/INSUS/IP/INSUSSING/ALP/INS	
Refer Teampers and an environmental and a second state and a second s	
Construction of Construction (Construction) and Constructio	
Note of control of the first of	
NUM PROF VERY VERY VERY VERY VERY VERY VERY VERY	
A REPORT AND A	
Lives many limited	
contraction of the second seco	
calculate to New York (Construction of Construction) and an approximation of Construction of Const	
Add : 100 MIC M1 8-	
x46 (2000) (x11) T11444-91 (2000) (342) (x11) (360) (371) (360) (371) (360) (371)	
And the second	
AND TYVE TRANSPORT OF A DEVICE A DEVIC	
NUMPER PRODUCTION AND A DESCRIPTION AND A	
REAL PLANNED AND A DELEVATION OF A DELEVATIONO OF A DELEVATION OF A	
Number of the second	
V West Physics (Rev Hest Rev Article 1) (V West Rev Article 1) (Rev Figure 1) (Physics 1) (Rev Article 1) (	
E3x485x80.xxX2x8x231740x81xxxx2x8xxx810xxxxxxx810xxxxxxxxxxxxx	
excepted/dived/games/second/fill/second/fill/second/games/and/and/and/	
Digital Constraints and a second se	
The second state of the se	
KOLD REVENUE VRAME PROVIDED VOLD REVENUE VRAME REVENUE VRAME REVENUE VRAME REVENUE VRAME	
x00;r81X60/y8x9a/W14x64;j349;j365849930/Y7X81g8Qxagstall.cls(3bars.cls)z40ars;j15castar	
1. Sec. 2007 Sec.	
A real devices of the second second	
rect Single Lager Deriver Mindings" errored in termenter (444, 1), it bit high of The And Inter", (acard and "Wetter / 754, 54, 55, 57, 58, 58, 59, 58, 51, 59, 58, 51, 59, 58, 51, 51, 52, 52, 53, 54, 54, 55, 55, 55, 55, 55, 55, 55, 55	
HAR CONSTRUCTOR REACTOR FOR CONSTRUCTIONS (C.D. REACTOR (C.D. REACTOR (TTP-0057) Loss Conv (REQUIDED AND ADDRESS (C.D. REACTOR (	
rand time (Director) and a supervision (DBL-1). To supervise Formal Landson of Formal Contents of the Content of States of Content of Content of States of Content o	
The function of the second structure of the State of Parity of Parity of the State	
And Research Funders and the research of the second of the research of the res	
indel Name (1) Prome Environment for EUR (n) - (1) manual of Prome Environment in Name (1) Prome Environment in	
and described an and entropy decision to characterized and an analyzed of the PROPE Constraint (Property) (CLACAE) and Capital Analyzed and an analyzed of the Constraint (Property) and Constraint (	
A real of a constraint of the second se	

## vManage是否支持双因素身份验证,以及它与SSO有何不同?

双因素身份验证(也称为2FA)是多因素身份验证(MFA)的类型或子集。 它是通过两种不同因素的 组合来确认用户所声明的身份的方法:1)他们知道的东西,2)他们拥有的东西,或3)他们是什么。

示例: Google GMail(密码,带一次性密码(OTP))

2FA是SSO服务器上将提供的内容。它类似于我们登录思科内部网站的方式。

它将您重定向到Cisco SSO,系统会提示您输入PingID/DUO 2FA。

## 作为解决方案的一部分,有多少角色?

我们有3卷卷;基本、操作员、netadmin。

配置用户访问和身份验证

#### 我们支持哪个IdP?

- 奥克塔
- PingID

ADFS

客户可能会使用其他IdP,并可能会看到其正常运行。这将属于"尽力而为"

例如,MSFT Azure AD不支持IDP(目前)。 但考虑到一些警告,这可能会奏效。

其他包括: Oracle Access Manager、F5网络

注意:请查看最新的思科文档,了解vManage支持的最新IdP

#### 如何在SAML断言中指示用户组成员?

#### SAML IdPvManage

#### SAMLRBAC

此问题是由IDP配置不正确引起的。此处的关键是,IDP在身份验证期间发送的信息应包含"用户名 "和"组"作为xml中的属性。如果使用其他字符串代替"组",则用户组默认为"基本"。"基本"用户只能访 问基本控制面板。

确保IDP将"用户名/组"而不是"用户ID/角色"发送到vManage。 以下是/var/log/nms/vmanage-server.log文件中所示的示例:

非工作示例:

我们看到IdP发送了"UserId/role",用户被映射到基本组。

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] **工作示例**:

在此中,您将看到"Username/Groups",并且用户已映射到netadmin组。

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]

#### 如何启用/检查SSO是否有效?

SSO功能调试日志记录可以启用,如下所示:

1.导航至https://<vManage\_ip\_addr:port>/logsettings.html

2.选择SSO日志记录并启用它,如图所示。



Choose a Logging feature



viptela.enable.sso.saml.log:

true

- •现在,SSO相关日志将保存到vManage日志文件/var/log/nms/vmanage-server.log中,其特别 关注的是IDP授权的"组"设置。如果没有匹配项,用户将默认为具有只读访问权限的"基本"组;
- 要调试访问权限问题,请检查日志文件并查找字符串"SamlUserGroups"。后面应是组名字符串 列表。其中一个应与vManage上的组设置匹配。如果未找到匹配项,则用户已默认为"基本"组。

#### SAML Tracer

一种工具,用于查看在单点登录和单次注销期间通过浏览器发送的SAML和WS-Federation消息。

<u>FireFox SAML-Tracer插件</u>

<u>Chrome SAML-Tracer扩展</u>



示例

#### SAML消息

## 如何登录启用SSO的vManage?

SSO仅用于浏览器登录。您可以手动将vManage定向到传统登录页并绕过SSO,以便仅使用用户名和密码:https://<vmanage>:8443/login.html。

### 使用什么加密算法?

目前我们支持SHA1作为加密算法。 vManage将使用SHA1算法对SAML元数据文件进行签名,IdP需要接受该文件。 SHA256的支持将来会推出,目前我们尚未获得支持。

### 相关信息

配置单点登录:<u>https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-</u> 16/security-book-xe/configure-sso.html

OKTA登录/注销附加到案例的工作日志作为参考。