vManage:단일 사인온 확인 및 확인 방법

목차

[소개](#)
[용어](#)
[기능 기능이란 무엇입니까?](#)
[vManage에서 활성화하는 방법](#)
[워크플로란 무엇입니까?](#)
[vManage는 2단계 인증을 지원하고 SSO와 어떻게 다릅니까?](#)
[솔루션의 일부로 몇 개의 역할이 있습니까?](#)
[어떤 IdPs를 지원합니까?](#)
[SAML 어설션에서 사용자 그룹 멤버십을 나타내는 방법](#)
[SSO의 작동 여부를 활성화/확인하는 방법](#)
[SAML 추적기](#)
[샘플 SAML 메시지](#)
[SSO가 활성화된 vManage에 로그인하는 방법](#)
[어떤 암호화 알고리즘을 사용합니까?](#)
[관련 정보](#)

소개

이 문서에서는 vManage에서 SSO(Single Sign On)를 활성화하기 위한 기본 사항과 이 기능이 활성화된 경우 vManage에서 확인/확인하는 방법에 대해 설명합니다. 18.3.0부터 vManage는 SSO를 지원합니다. SSO를 사용하면 사용자가 외부 IP(Identity Provider)에 대해 인증하여 vManage에 로그인할 수 있습니다. 이 기능은 SSO용 SAML 2.0 사양을 지원합니다.

기고자: Shankar Vemulapalli, Cisco TAC 엔지니어.

용어

SAML(Security Assertion Markup Language)은 당사자 간, 특히 ID 제공자와 ID 공급자 간에 인증 및 권한 부여 데이터를 교환하기 위한 개방형 표준입니다 서비스 제공자입니다.이름에서 알 수 있듯이 SAML은 보안 어설션을 위한 XML 기반 마크업 언어입니다 (통신 사업자가 액세스 제어 결정을 내리는 데 사용하는 설명)

IdP(Identity Provider)는 "다른 웹 사이트에 액세스하기 위해 SSO(Single Sign-On)를 사용할 수 있는 신뢰할 수 있는 공급자"입니다."SSO는 비밀번호 피로를 줄이고 사용 편의성을 향상시킵니다.잠재적 공격 표면을 줄이고 더 나은 보안을 제공합니다.

통신 사업자 - SAML의 SSO 프로파일과 함께 인증 어설션을 수신하고 수락하는 시스템 엔티티입니다.

기능 기능이란 무엇입니까?

- SAML2.0만 지원됩니다.
- 지원 대상 - 단일 테넌트(독립형 및 클러스터), 다중 테넌트(공급자 레벨 및 테넌트 레벨 모두), 멀티 테넌트 구축도 기본적으로 클러스터입니다.Provider-as-tenant는 적용할 수 없습니다.
- idp가 SAML 2.0 사양을 따르는 경우 각 테넌트에는 고유한 ID 공급자가 있을 수 있습니다.
- 파일 업로드를 통한 IDP 메타데이터 컨피그레이션, 일반 텍스트 복사, vManage 메타데이터 다운로드를 지원합니다.
- 브라우저 기반 SSO만 지원됩니다.
- vmanage 메타데이터에 사용되는 인증서는 이 릴리스에서 구성할 수 없습니다.
  SSO를 처음 활성화할 때 생성되는 자체 서명 인증서이며 다음 매개변수를 사용합니다.

    문자열 CN = <TenantName>, DefaultTenant

    문자열 OU = <Org Name>
    문자열 O = <SP 조직 이름>
    문자열 L = "산호세";
    문자열 ST = "CA";
    문자열 C = "USA";
    문자열 유효성 = 5년;
    인증서 서명 알고리즘:SHA256WithRSA
    키 쌍 생성 알고리즘:RSA

- 단일 로그인 - SP 시작 및 IDP 시작 지원
- 단일 로그아웃 - SP만 시작

vManage에서 활성화하는 방법

vManage NMS에 대해 SSO(Single Sign-On)를 활성화하여 사용자가 외부 ID 제공자를 사용하여 인증할 수 있도록 하려면 다음을 수행합니다.

1. vManage NMS에서 NTP를 활성화했는지 확인합니다.
2. IdP에 구성된 URL을 사용하여 vManage GUI에 연결
   (예: vmanage-112233.viptela.net, 이 URL 정보는 SAML 메타데이터에 포함되어 있으므로 IP 주소를 사용하지 않음)
3. ID 제공자 설정 표시줄 오른쪽의 편집 버튼을 클릭합니다.
4. Enable Identity Provider(ID 제공자 활성화) 필드에서 Enabled(활성화됨)를 클릭합니다.
5. ID 제공자 메타데이터 업로드 상자에 ID 제공자 메타데이터를 복사하여 붙여넣습니다.또는 Select a File(파일 선택)을 클릭하여 ID 제공자 메타데이터 파일을 업로드합니다.
6. 저장을 클릭합니다.

워크플로란 무엇입니까?

1. 사용자는 ID 제공자 메타데이터를 업로드하여 Administration->Settings 페이지를 통해 SSO를 활성화합니다.
2. 그런 다음 사용자는 ID 공급자에 업로드할 해당 vManage 테넌트 메타데이터를 다운로드합니다(vManage 메타데이터를 생성하려면 적어도 한 번 이상 수행해야 함).
3. 필요한 경우 언제든지 메타데이터를 비활성화하거나 업데이트할 수 있습니다.

샘플 vManage 메타

vManage는 2단계 인증을 지원하고 SSO와 어떻게 다릅니까?

Two-Factor Authentication(2FA라고도 함)은 MFA(Multi-Factor Authentication)의 유형 또는 하위 집합입니다. 이는 다음과 같은 두 가지 요소를 조합하여 사용자의 청구 ID를 확인하는 방법입니다.1) 아는 것 2) 가진 것 3) 있는 것

예: Google GMail(비밀번호(OTP(일회용 비밀번호)))

2FA는 SSO 서버에서 제공될 것입니다.내부 Cisco 웹 사이트에 로그인하는 방식과 유사합니다.

그러면 Cisco SSO로 리디렉션되며 PingID/DUO 2FA를 입력하라는 메시지가 표시됩니다.

솔루션의 일부로 몇 개의 역할이 있습니까?

3롤이 있습니다.기본, 운영자, netadmin.

사용자 액세스 및 인증 구성

어떤 IdPs를 지원합니까?

- 옥타

- PingID
- ADFS

고객은 다른 IdP를 사용할 수 있으며, 작동 중인 것으로 보일 수 있습니다.이것은 '최선의 노력'이 될 것이다.

예를 들어 MSFT Azure AD는 아직 IDP가 지원되지 않습니다. 그러나 몇 가지 주의 사항을 고려할 때 그것은 효과가 있을 수도 있다.

기타 구성 요소는 다음과 같습니다. Oracle Access Manager, F5 네트워크

> **참고:**vManage에서 지원하는 최신 IdPs는 최신 Cisco 설명서를 참조하십시오.

SAML 어설션에서 사용자 그룹 멤버십을 나타내는 방법

/:SAML IdP vManage . .

SAML RBAC ?

이 문제는 IDP의 잘못된 컨피그레이션으로 인해 발생합니다.여기서 핵심은 인증 중에 IDP가 전송한 정보는 xml의 특성으로 "Username" 및 "Groups"를 포함해야 한다는 것입니다."그룹" 대신 다른 문자열을 사용하는 경우 사용자 그룹은 기본적으로 "기본"입니다."기본" 사용자는 기본 대시보드에만 액세스할 수 있습니다.

IDP가 "UserId/role" 대신 "Username/Groups"를 vManage로 전송해야 합니다.
다음은 /var/log/nms/vmanage-server.log 파일에 표시된 예입니다.

비작동 예:

"UserId/role"이 IdP에 의해 전송되고 사용자가 *기본* 그룹에 매핑되는 것을 볼 수 있습니다.

```
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]
```

작업 예:

여기서 "Username/Groups(사용자 이름/그룹)"가 표시되고 사용자는 netadmin 그룹에 매핑됩니다.

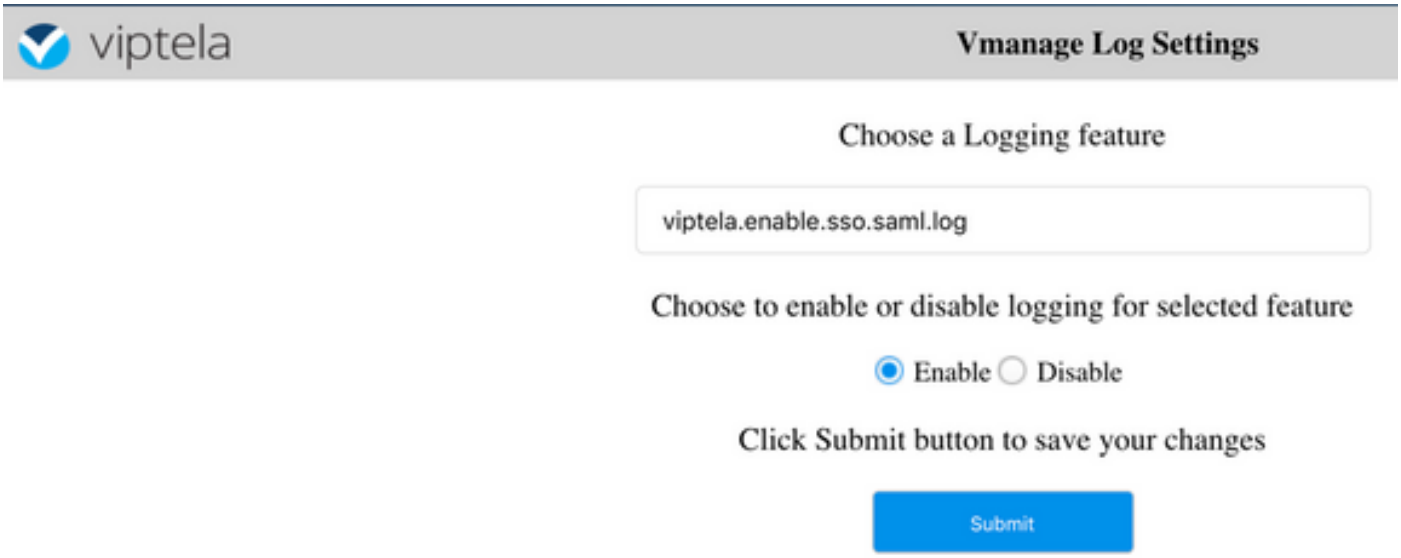
```
05-Mar-2019 21:35:55,766 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-90)
|default| AttributeMap: {UserName=[Tester@Example.MFA.com], Groups=[netadmin]}
05-Mar-2019 21:35:55,766 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-90)
|default| AttributeMap: {UserName=[Tester@Example.MFA.com],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

SSO의 작동 여부를 활성화/확인하는 방법

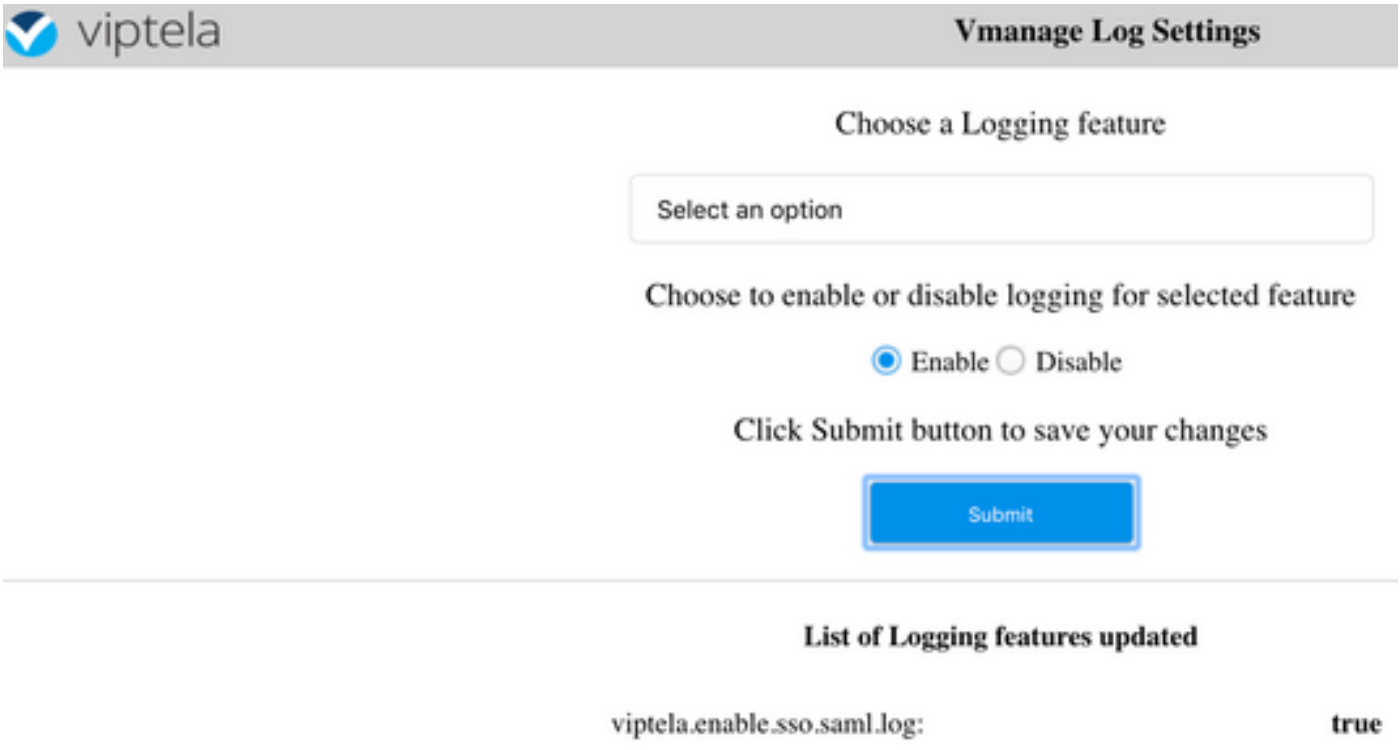
SSO 기능 디버그 로깅은 다음과 같이 활성화할 수 있습니다.

1. https://<vManage_ip_addr:port>/logsettings.html으로 이동합니다.

2. SSO 로깅을 선택하고 이미지에 표시된 대로 활성화합니다.



3. 활성화되면 **Submit** 버튼을 누릅니다.



- 이제 SSO 관련 로그가 vManage 로그 파일에 저장됩니다. /var/log/nms/vmanage-server.log에 특히 관심이 있는 것은 IDP 권한 부여에 대한 "Groups" 설정입니다.일치하는 항목이 없으면 사용자는 기본적으로 "Basic" 그룹으로 설정되며, 이 그룹은 읽기 전용 액세스 권한을 가집니다.
- 액세스 권한 문제를 디버깅하려면 로그 파일을 확인하고 문자열 "SamlUserGroups"를 찾습니다. 다음은 그룹 이름의 문자열 목록입니다.그 중 하나가 vManage의 그룹 설정과 일치해야 합니다.일치하는 항목이 없으면 기본적으로 "Basic(기본)" 그룹으로 설정됩니다.

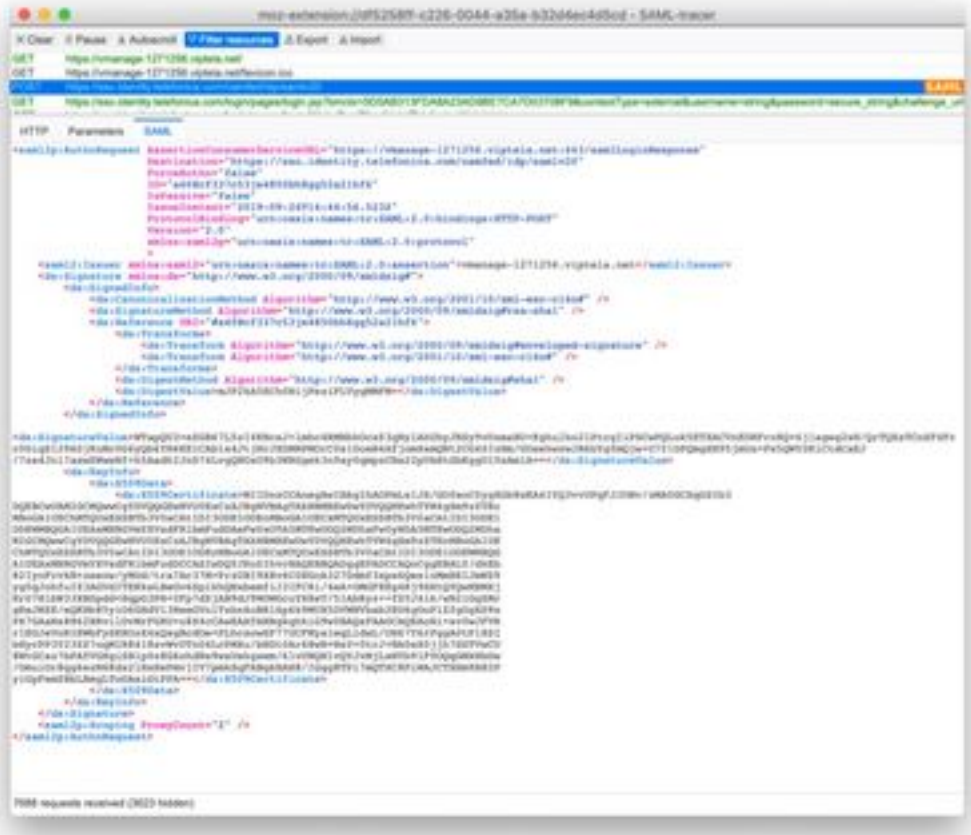
SAML 추적기

단일 로그인 및 단일 로그아웃 중에 브라우저를 통해 전송된 SAML 및 WS-Federation 메시지를 보

는 도구입니다.

FireFox SAML-Tracer 애드온

Chrome SAML-Tracer 확장



샘플 SAML 메시지

SSO가 활성화된 vManage에 로그인하는 방법

SSO는 브라우저 로그인에만 사용됩니다.사용자 이름 및 비밀번호만 사용하려면 수동으로 vManage를 기존 로그인 페이지에 연결하고 SSO를 우회하여 https://**<vmanage>:8443/login.html을 사용할 수 있습니다.**

어떤 암호화 알고리즘을 사용합니까?

현재 암호화 알고리즘으로 SHA1을 지원합니다. vManage는 IdPs가 수락해야 하는 SHA1 알고리즘을 사용하여 SAML 메타데이터 파일에 서명합니다. SHA256에 대한 지원은 향후 릴리스에서 제공될 예정이며 현재 지원되지 않습니다.

관련 정보

단일 로그인 구성: 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 작업 로그를 참조로 케이스에 첨부합니다.