

vManage:シングルサインオンの確認と確認方法

内容

[概要](#)

[用語](#)

[機能とは何ですか。](#)

[vManageで有効にする方法](#)

[ワークフローとは](#)

[vManageはTwo-Factor Authenticationをサポートしていますか。また、SSOとどのように異なりますか。](#)

[ソリューションの一部として役割はいくつありますか。](#)

[どのIdPsをサポートしますか。](#)

[SAMLアサートのユーザグループメンバーシップを示す方法](#)

[SSOが動作するかどうかを有効または確認する方法](#)

[SAML Tracer](#)

[サンプルSAMLメッセージ](#)

[SSO対応vManageにログインする方法](#)

[どの暗号化アルゴリズムが使用されますか。](#)

[関連情報](#)

概要

このドキュメントでは、vManageでシングルサインオン(SSO)を有効にするための基本と、この機能が有効になっている場合にvManageで確認/確認する方法について説明します。vManageは18.3.0からSSOをサポートします。SSOを使用すると、外部IDプロバイダー(IP)に対して認証を行うことでvManageにログインできます。この機能は、SSOのSAML 2.0仕様をサポートしています。

著者 : Cisco TACエンジニア、Shankar Vemulapalli

用語

Security Assertion Markup Language(SAML)は、特にIDプロバイダーとサービスプロバイダ。その名前が示すように、SAMLはセキュリティアサーション用のXMLベースのマークアップ言語です (サービスプロバイダーがアクセス制御の決定に使用するステートメント)。

アイデンティティプロバイダー(IdP)は、「シングルサインオン(SSO)を使用して他のWebサイトにアクセスできる信頼できるプロバイダー」です。潜在的な攻撃対象を減らし、セキュリティを向上させます。

サービスプロバイダー- SAMLのSSOプロファイルと組み合わせて認証アサーションを受け取り、受け入れるシステムエンティティです。

機能とは何ですか。

- SAML2.0のみがサポートされています
- サポート対象：シングルテナント（スタンドアロンおよびクラスタ）、マルチテナント（プロバイダーレベルおよびテナントレベルの両方）、マルチテナント展開もデフォルトではクラスタです。Provider-as-tenantは該当しません。
- IDPがSAML 2.0仕様に従っている限り、各テナントは独自のIDプロバイダーを持つことができます。
- ファイルのアップロード、プレーンテキストコピー、およびvManageメタデータのダウンロードによるIDPメタデータの設定をサポートします。
- ブラウザベースのSSOだけがサポートされます。
- vmanageメタデータに使用される証明書は、このリリースでは設定できません。
これは自己署名証明書であり、SSOを初めて有効にするときに作成され、次のパラメータを使用します。

文字列CN = <TenantName>、DefaultTenant

文字列OU = <組織名>
 文字列O = <Sp組織名>
 文字列L = "San Jose";
 文字列ST = "CA";
 文字列C = "USA";
 文字列の有効性= 5yrs;
 証明書署名アルゴリズム：SHA256WithRSA
 キーペア生成アルゴリズム：RSA

- シングルログイン：SPが開始し、IDPがサポートされる
- シングルログアウト：SPが開始のみ

vManageで有効にする方法

vManage NMSのシングルサインオン(SSO)を有効にして、外部IDプロバイダーを使用してユーザーを認証できるようにするには、次の手順を実行します。

1. vManage NMSでNTPが有効になっていることを確認します。
2. IdPで設定されたURLを使用してvManage GUIに接続します
(例：vmanage-112233.viptela.netおよび使用しないIPアドレス。このURL情報はSAMLメタデータに含まれているため)
3. [Identity Provider Settings]バーの右側にある[Edit]ボタンをクリックします。
4. [Enable Identity Provider]フィールドで、[Enabled]をクリックします。
5. [Upload Identity Provider Metadata]ボックスに、アイデンティティプロバイダーのメタデータをコピーして貼り付けます。または、[ファイルの選択(Select a File)]をクリックして、アイデンティティプロバイダーメタデータファイルをアップロードします。
6. [Save] をクリックします。

ワークフローとは

1. ユーザーは、アイデンティティプロバイダーのメタデータをアップロードして、[Administration] > [Settings]ページからSSOを有効にします。
2. 次に、IDプロバイダーにアップロードする対応するvManageテナントメタデータをダウンロードします([Must be done to generate vManage metadata])。

どのIdPsをサポートしますか。

- 岡田
- PingID
- ADFS

お客様は他のIdPsを使用して、動作していると見なすことができます。これは「ベストエフォート」の下にあります

たとえば、MSFT Azure AD is NOT SUPPORTED IDP (まだ)です。ただし、注意が必要な場合もあります。

その他： Oracle Access Manager、F5 Networks

注：vManageでサポートされている最新のIdPsについては、シスコの最新のマニュアルを参照してください

SAMLアサートのユーザグループメンバーシップを示す方法

SAML IdPvManage

SAMLRBAC

この問題は、IDPの不適切な設定が原因で発生します。ここで重要なのは、認証中にIDPから送信される情報には、xmlの属性として「Username」と「Groups」を含める必要があることです。「グループ」の代わりに他の文字列を使用する場合、ユーザグループはデフォルトで「基本」になります。「基本」ユーザは、基本ダッシュボードにのみアクセスできます。

IDPが「UserId/role」ではなく「Username/Groups」をvManageに送信していることを確認します。

/var/log/nms/vmanage-server.logファイルに表示される例を次に示します。

動作しない例：

「UserId/role」がIdPによって送信され、ユーザーが基本グループにマップされています。

```
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]
```

動作例：

この例では「Username/Groups」と表示され、ユーザはnetadminグループにマッピングされています。

```
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)
```

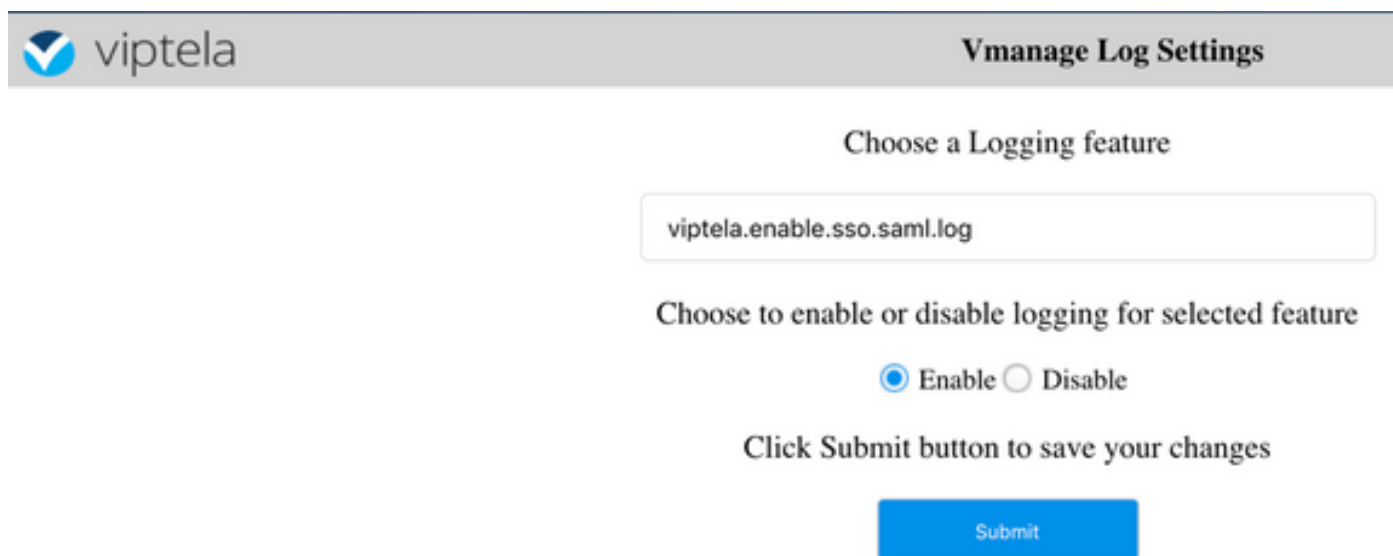
```
|default| AttributeMap: {UserName=[Tester@Example.MFA.com], Groups=[netadmin]}
05-Mar-2019 21:35:55,766 UTC INFO [vManage] [SAMLAuthenticationProvider] (default task-90)
|default| Roles: [netadmin]
```

SSOが動作するかどうかを有効または確認する方法

SSO機能のデバッグロギングは、次のように有効にできます。

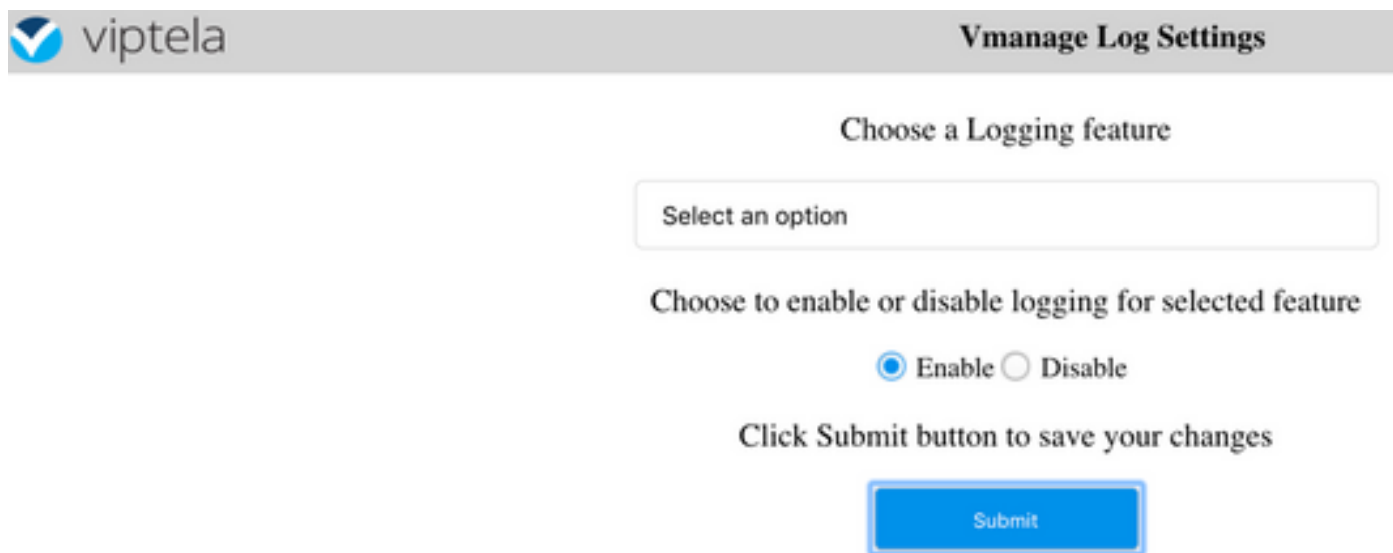
1. https://<vManage_ip_addr:port>/logsettings.html

2. SSOロギングを選択し、図のように有効にします。



The screenshot shows the 'Vmanage Log Settings' page. At the top left is the 'viptela' logo. The page title is 'Vmanage Log Settings'. Below the title, it says 'Choose a Logging feature'. A text input field contains 'viptela.enable.sso.saml.log'. Below this, it says 'Choose to enable or disable logging for selected feature'. There are two radio buttons: 'Enable' (which is selected) and 'Disable'. Below the radio buttons, it says 'Click Submit button to save your changes'. At the bottom, there is a blue 'Submit' button.

3. Enabledになったら、Submitボタンを押します。



This screenshot is identical to the previous one, showing the 'Vmanage Log Settings' page with the 'Enable' radio button selected and the 'Submit' button visible.

List of Logging features updated

viptela.enable.sso.saml.log:	true
------------------------------	------

- SSO関連のログがvManageログファイル/var/log/nms/vmanage-server.logに保存されます。特に、IDP認証の「グループ」設定が対象です。一致しない場合、ユーザはデフォルトで「Basic」グループに設定され、読み取り専用アクセス権が付与されます。

ファイルにSHA1アルゴリズムで署名し、IdPsはこれを受け入れる必要があります。 SHA256のサポートは今後のリリースで提供される予定ですが、現在はサポートされていません。

関連情報

シングルサインオンの構成

: <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の作業ログを参照としてケースに添付。