啟用並驗證vManage的單點登入

目錄

簡介

本文檔介紹在vManage上啟用和驗證單一登入(SSO)的基本資訊。

技術

安全斷言標籤語言(SAML)是一種開放標準，用於在各方之間，特別是在身份提供者和服務提供商之間交換身份驗證和授權資料。顧名思義，SAML是一種基於XML的安全宣告（服務提供商用來作出訪問控制決策的語句）標籤語言。

身份提供程式(IdP)是「一個受信任的提供程式，它允許你使用單一登入(SSO)來訪問其他網站。」SSO減少了密碼疲勞，增強了可用性。它減少了潛在攻擊面，提供了更好的安全性。

服務提供商 — 它是與SAML的SSO配置檔案一起接收並接受身份驗證斷言的系統實體。

什麼是功能功能？

- 從18.3.0開始，vManage支援SSO。SSO允許使用者通過對外部身份提供程式(IP)進行身份驗證來登入到vManage。
- 僅支援SAML2.0
- 支援 — 單租戶（獨立和集群）、多租戶（在提供商級別和租戶級別），此外，多租戶部署預設情況下是集群。Provider-as-tenant不適用。
- 每個Tenant可以擁有自己的唯一身份提供者，只要IDP與SAML 2.0規範一致。
- 支援通過檔案上載以及純文字檔案複製和下載vManage後設資料來配置IDP後設資料。

- 僅支援基於瀏覽器的SSO。
- 在此版本中，無法配置用於vmanage後設資料的證書。
  它是自簽名證書，首次啟用SSO時建立，使用以下引數：

  字串CN =<TenantName>, DefaultTenant

  字串OU = <組織名稱>
  字串O = <Sp組織名稱>
  字串L ="San Jose";
  字串ST ="CA";
  字串C = "USA";
  字串有效性= 5年；
  證書簽名演算法：SHA256WithRSA
  金鑰對生成演算法：RSA

- 單一登入 — SP啟動和IDP啟動支援
- 單一註銷 — 僅SP已啟動

如何在vManage上啟用？

要為vManage NMS啟用單一登入(SSO)以允許使用者使用外部身份提供程式進行身份驗證，請執行以下操作：

1. 確保已在vManage NMS上啟用NTP。
2. 使用在IdP上配置的URL連線到vManage GUI
   (例如， vmanage-112233.example.net且不使用IP地址，因為此URL資訊包含在SAML後設資料中)
3. 按一下Identity Provider Settings欄右側的Edit按鈕。
4. 在Enable Identity Provider欄位中，按一下Enabled，
5. 複製身份提供程式後設資料並將其貼上到「上載身份提供程式後設資料」框中。或者按一下選擇檔案以上傳身份提供方後設資料檔案。
6. 按一下「儲存」。

工作流程是什麼？

1. 使用者通過上傳身份提供程式後設資料來通過「管理」 — >「設定」頁面啟用SSO。
2. 然後，使用者下載相應的vManage租戶後設資料以上載到身份提供程式（必須至少完成一次才能生成vManage後設資料）。
3. 如果需要，使用者可以隨時禁用或更新後設資料。

vManage Meta示例

vManage是否支援二元身份驗證，以及它與SSO有何不同？

雙因素身份驗證（也稱為2FA）是多因素身份驗證(MFA)的一種型別或子集。這是一種使用兩種不同因素的組合來確認使用者所聲稱的身份的方法：1)他們知道的某物，2)他們擁有的某物，或3)他們擁有的某物。

示例：Google GMail(密碼，帶一次性密碼(OTP))

2FA是SSO伺服器上提供的功能。這與我們登入內部思科網站的方式類似。

它將您重定向至Cisco SSO，在此系統將提示您輸入PingID/DUO 2FA。

解決方案中有多少個角色？

我們有3個角色：基本、操作員、網路管理員。

配置使用者訪問和身份驗證

我們支援哪些IdP?

- 奧克塔
- PingID
- ADFS
- Microsoft Azure（20.9及更高版本）

客戶可以使用其他IdP，並且可以看到其正常工作。這將屬於「盡最大努力」範疇

其它包括：Oracle Access Manager、F5網路

註：請查閱最新的思科文檔，瞭解vManage支援的最新IdP

如何在SAML斷言中指示使用者組成員身份？

問題：使用SAML IdP提前結束vManage。當使用者成功通過身份驗證後，使用者唯一可以訪問的內容是控制面板。

當使用者通過SAML進行身份驗證時，是否有方法給予使用者更多的訪問許可權（通過使用者組RBAC）？

此問題是由於IDP配置不正確造成的。這裡的關鍵是，IDP在身份驗證期間傳送的資訊必須包含「使用者名稱」和「組」作為xml中的屬性。如果使用其他字串來代替「組」，則使用者組預設為「基本」。「基本」使用者只能訪問基本的控制面板。

確保IDP將「使用者名稱/組」而不是「使用者ID/角色」傳送到vManage。

以下示例在/var/log/nms/vmanage-server.log檔案中看到：

非工作示例：

我們看到「使用者ID/角色」已由IdP傳送，並且使用者被對映到基本組。

```
01-Mar-2019 15:23:50,797 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-227) |default| A
01-Mar-2019 15:23:50,797 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-227) |default| A
01-Mar-2019 15:23:50,797 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-227) |default| I
```

工作示例：

在此例中，您將看到「使用者名稱/組」，使用者將對映到netadmin組。

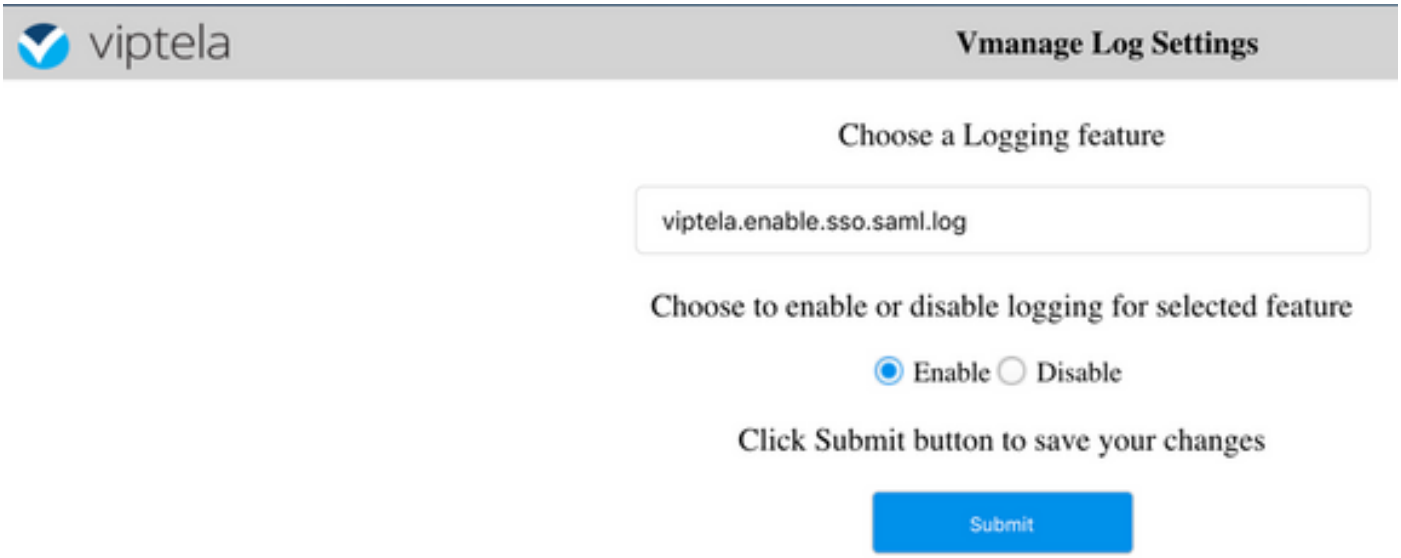
```
05-Mar-2019 21:35:55,766 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-90) |default| A
05-Mar-2019 21:35:55,766 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-90) |default| A
05-Mar-2019 21:35:55,766 UTC INFO  [vManage] [SAMLAuthenticationProvider] (default task-90) |default| R
```

如何啟用/檢查SSO是否正常工作？

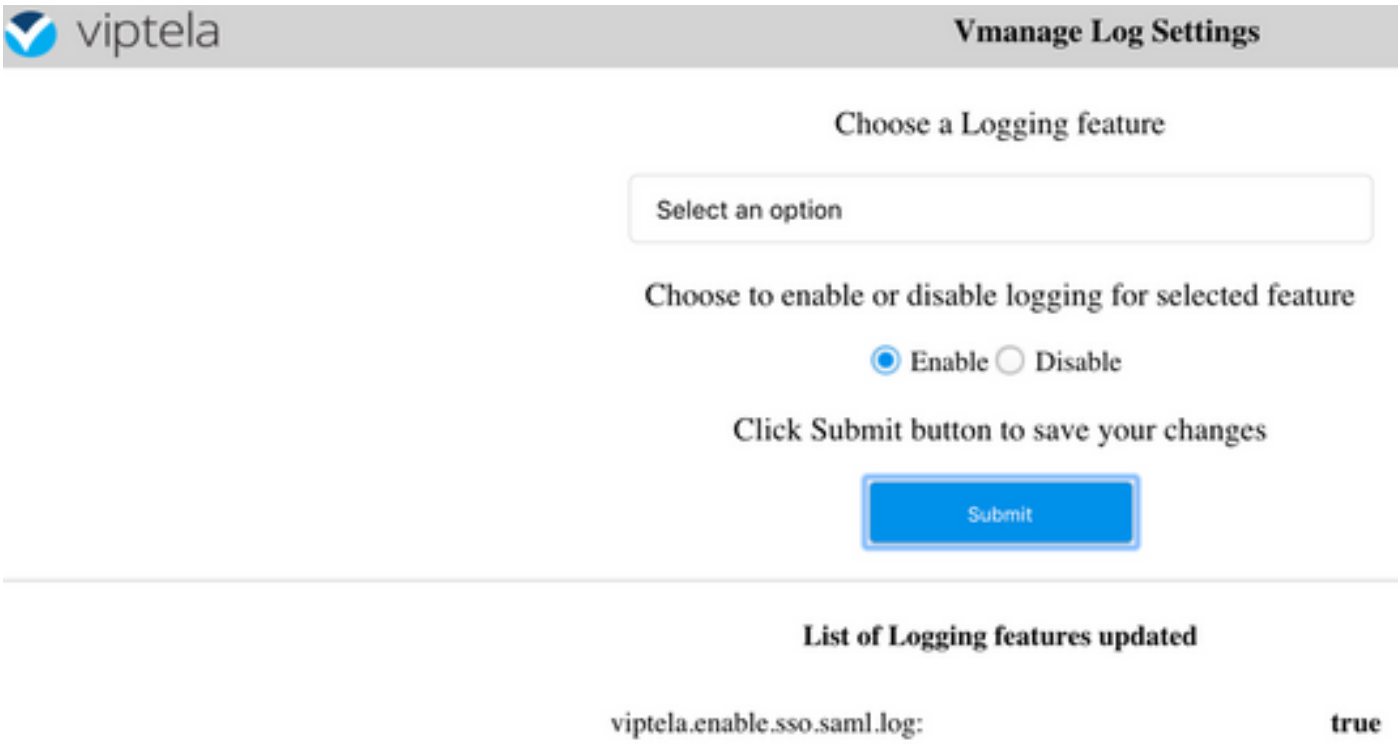
可通過以下步驟啟用SSO功能調試日誌記錄：

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

2.選擇SSO日誌記錄並啟用它，如下圖所示。



3.啟用後，按一下Submit按鈕。



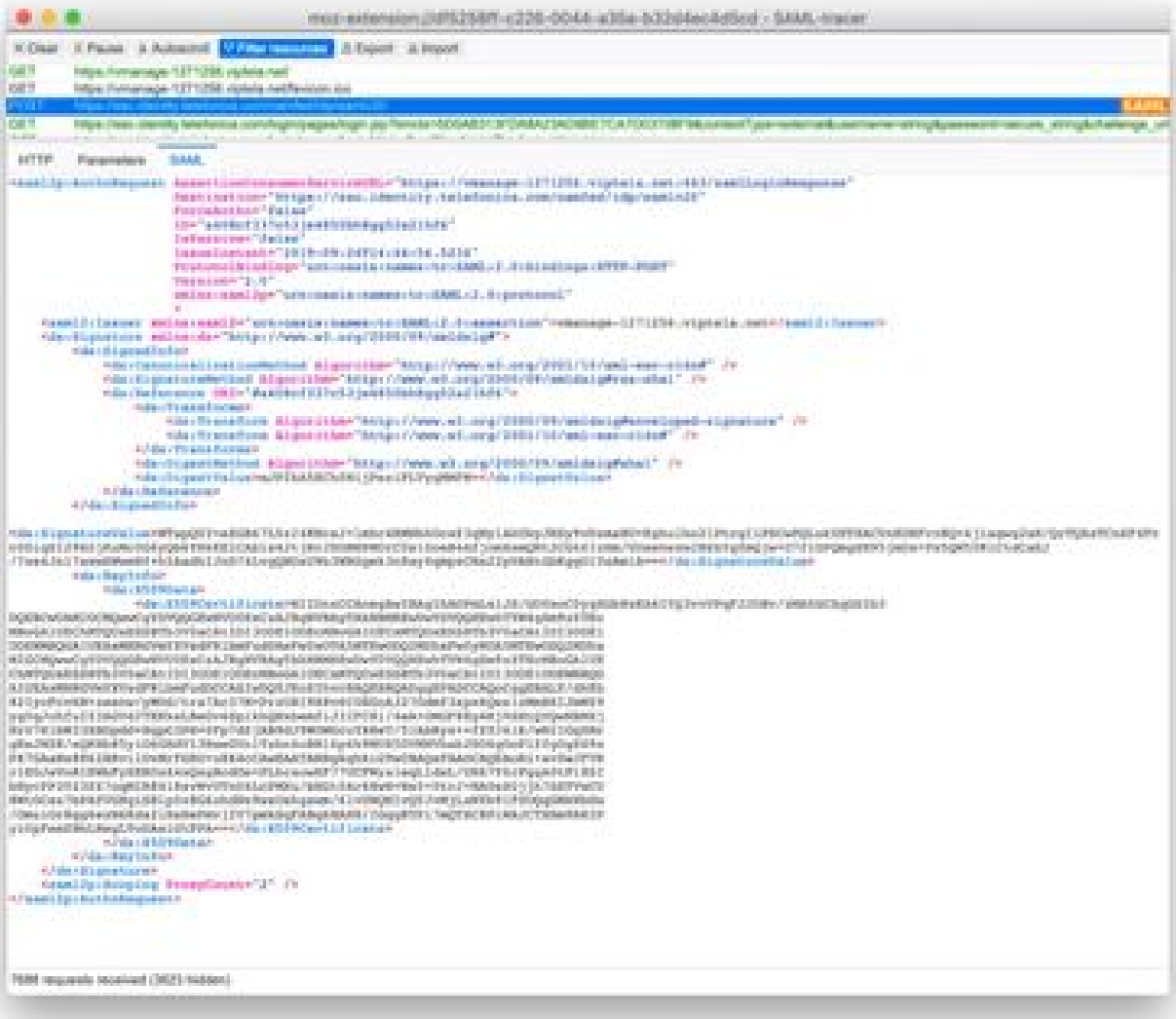
- 與SSO相關的日誌將儲存到vManage日誌檔案/var/log/nms/vmanage-server.log 中，該日誌檔案特別關注IDP授權的「組」設定。如果沒有相符專案，使用者會預設為具有唯讀存取的「Basic」群組；
- 為了調試訪問許可權問題，請檢查日誌檔案並查詢字串「SamlUserGroups」。後續輸出必須是組名字串的清單。其中一個必須與vManage上的組設定匹配。如果未找到匹配項，則使用者將預設為「基本」組。

SAML跟蹤器

用於檢視在單一登入和單一註銷期間通過瀏覽器傳送的SAML和WS-Federation消息的工具。

FireFox SAML-Tracer附加模組

Chrome SAML-Tracer擴展



saml消息示例

如何登入啟用了SSO的vManage?

SSO僅用於瀏覽器登入。您可以手動將vManage定向到傳統登入頁面，並繞過SSO，以便僅使用使用者名稱和密碼：https://<vmanage>:8443/login.html。

使用什麼加密演算法？

目前，我們支援SHA1作為加密演算法，vManage使用SHA1演算法對SAML後設資料檔案進行簽名，IdP需要接受它。　未來版本將支援SHA256，而我們目前尚不支援。

相關資訊

配置單一登入：https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-16/security-book-xe/configure-sso.html

作為參考，OKTA登入/註銷附加到案例的工作日誌。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。