



使用**SAML** SANtricity 11.8

NetApp
December 16, 2024

目录

使用SAML	1
配置SAML	1
更改SAML角色映射	5
导出SAML服务提供程序文件	6

使用SAML

配置SAML

要为访问管理配置身份验证、您可以使用存储阵列中嵌入的安全断言标记语言(SAML)功能。此配置将在身份提供程序和存储提供程序之间建立连接。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- 您必须知道存储阵列中控制器的IP地址或域名。
- IdP管理员已配置IdP系统。
- IdP管理员已确保IdP支持在身份验证时返回名称ID。
- 管理员已确保IdP服务器和控制器时钟同步(通过NTP服务器或通过调整控制器时钟设置)。
- Idp元数据文件将从Idp系统下载、并可在用于访问Unified Manager的本地系统上使用。

关于此任务

身份提供程序(IdP)是一种外部系统、用于向用户请求凭据并确定该用户是否已成功通过身份验证。可以将IdP配置为提供多因素身份验证并使用任何用户数据库、例如Active Directory。您的安全团队负责维护IdP。服务提供商(Service Provider、SP)是一个控制用户身份验证和访问的系统。使用SAML配置访问管理时、存储阵列充当服务提供商、向身份提供程序请求身份验证。要在IdP和存储阵列之间建立连接、您需要在这两个实体之间共享元数据文件。接下来、将IdP用户实体映射到存储阵列角色。最后、在启用SAML之前、您需要测试连接和SSO登录。



- SAML和目录服务*。如果在将目录服务配置为身份验证方法时启用SAML、则SAML将取代Unified Manager中的目录服务。如果稍后禁用SAML、则目录服务配置将返回到其先前的配置。



- *编辑和禁用。*启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。

配置SAML身份验证是一个多步骤操作步骤。

第1步：上传IdP元数据文件

要为存储阵列提供Idp连接信息、请将Idp元数据导入到Unified Manager中。IdP系统需要使用此元数据将身份验证请求重定向到正确的URL并验证收到的响应。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择*SAML*选项卡。

此页面将显示配置步骤的概述。

3. 单击*导入身份提供程序(IdP)文件*链接。

此时将打开导入身份提供程序文件对话框。

4. 单击*浏览*以选择您复制到本地系统的IdP元数据文件并将其上传。

选择文件后、将显示IdP实体ID。

5. 单击 * 导入 *。

第2步：导出服务提供商文件

要在IdP和存储阵列之间建立信任关系、请将服务提供商元数据导入到IdP中。Idp需要此元数据才能与控制器建立信任关系并处理授权请求。此文件包含控制器域名或IP地址等信息、以便IdP可以与服务提供商进行通信。

步骤

1. 单击*导出服务提供商文件*链接。

此时将打开导出服务提供商文件对话框。

2. 在*控制器A*字段中输入控制器IP地址或DNS名称、然后单击*导出*将元数据文件保存到本地系统。

单击*导出*后、服务提供商元数据将下载到本地系统。记下文件的存储位置。

3. 从本地系统中、找到您导出的XML格式的服务提供商元数据文件。
4. 从Idp服务器中、导入服务提供商元数据文件以建立信任关系。您可以直接导入文件、也可以手动输入文件中的控制器信息。

第3步：映射角色

要为用户提供对Unified Manager的授权和访问权限、您必须将Idp用户属性和组成员资格映射到存储阵列的预定义角色。

开始之前

- IdP管理员已在IdP系统中配置用户属性和组成员资格。
- Idp元数据文件将导入到Unified Manager中。
- 将控制器的服务提供商元数据文件导入到Idp系统中以建立信任关系。

步骤

1. 单击*映射Unified Manager*角色的链接。

此时将打开角色映射对话框。

2. 为预定义角色分配IdP用户属性和组。一个组可以分配多个角色。

字段详细信息

设置	说明
映射	用户属性
指定要映射的SAML组的属性(例如、"member for")。	属性值
指定要映射的组的属性值。支持正则表达式。(\ <code>\</code> 如果这些特殊正则表达式字符不属于正则表达式模式,则必须使用反斜杠转义: \ <code>\. [] { } () <> * + = ! ? ^ \$</code>)	
角色	<p>单击此字段、然后选择要映射到此属性的存储阵列角色之一。您必须单独选择要包括的每个角色。要登录到Unified Manager、需要将"监控"角色与其他角色结合使用。至少一个组还需要安全管理员角色。</p> <p>映射的角色包括以下权限:</p> <ul style="list-style-type: none">• 存储管理—对存储对象(例如卷和磁盘池)具有完全读/写访问权限、但无法访问安全配置。• 安全管理—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面(符号)的功能。• 支持管理—访问存储阵列上的所有硬件资源、故障数据、MEL事件和控制器固件升级。无法访问存储对象或安全配置。• 监控—对所有存储对象的只读访问、但无法访问安全配置。



包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则Unified Manager将无法对任何用户正常运行。

3. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。



启用SAML后、可以修改角色映射。

4. 完成映射后、单击*保存*。

第4步：测试SSO登录

为了确保IdP系统和存储阵列可以进行通信、您可以选择测试SSO登录。在启用SAML的最后一步中、也会执行此测试。

开始之前

- Idp元数据文件将导入到Unified Manager中。
- 将控制器的服务提供商元数据文件导入到Idp系统中以建立信任关系。

步骤

1. 选择*测试SSO登录*链接。

此时将打开一个对话框、用于输入SSO凭据。

2. 输入具有安全管理员权限和监控权限的用户的登录凭据。

在系统测试登录时、将打开一个对话框。

3. 查找Test Successful消息。如果测试成功完成、请转至下一步以启用SAML。

如果测试未成功完成、则会显示一条错误消息、其中包含更多信息。请确保：

- 该用户属于具有安全管理员和监控权限的组。
- 您为IdP服务器上传的元数据正确无误。
- SP元数据文件中的控制器地址正确。

第5步：启用SAML

最后一步是完成用户身份验证的SAML配置。在此过程中、系统还会提示您测试SSO登录。上一步介绍了SSO登录测试过程。

开始之前

- Idp元数据文件将导入到Unified Manager中。
- 将控制器的服务提供商元数据文件导入到Idp系统中以建立信任关系。
- 至少配置了一个监控器和一个安全管理员角色映射。



*编辑和禁用。*启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。

步骤

1. 从* SAML *选项卡中、选择*启用SAML *链接。

此时将打开确认启用SAML对话框。

2. 键入 enable, 然后单击*Enable*。
3. 输入用于SSO登录测试的用户凭据。

结果

系统启用SAML后、它将终止所有活动会话并开始通过SAML对用户进行身份验证。

更改SAML角色映射

如果先前已为访问管理配置SAML、则可以更改IdP组与存储阵列的预定义角色之间的角色映射。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- IdP管理员已在IdP系统中配置用户属性和组成员资格。
- 已配置并启用SAML。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择*SAML*选项卡。
3. 选择*角色映射*。

此时将打开角色映射对话框。

4. 为预定义角色分配IdP用户属性和组。一个组可以分配多个角色。



请注意、在启用SAML的情况下、不要删除您的权限、否则您将无法访问Unified Manager。

字段详细信息

设置	说明
映射	用户属性
指定要映射的SAML组的属性(例如、"member for")。	属性值
指定要映射的组的属性值。	角色



包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则Unified Manager将无法对任何用户正常运行。

5. 或者、也可以单击*添加另一个映射*以输入更多组到角色的映射。
6. 单击 * 保存 *。

结果

完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

导出SAML服务提供程序文件

如有必要、您可以导出存储阵列的服务提供程序元数据、然后将该文件重新导入到身份提供程序(Identity Provider、Idp)系统中。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- 已配置并启用SAML。

关于此任务

在此任务中、您将从控制器导出元数据。Idp需要此元数据才能与控制器建立信任关系并处理身份验证请求。此文件包含IdP可用于发送请求的控制器域名或IP地址等信息。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择*SAML*选项卡。
3. 选择*导出*。

此时将打开导出服务提供商文件对话框。

4. 单击*Export*将元数据文件保存到本地系统。



域名字段为只读。

记下文件的存储位置。

5. 从本地系统中、找到您导出的XML格式的服务提供商元数据文件。
6. 从Idp服务器中、导入服务提供商元数据文件。您可以直接导入文件、也可以手动输入控制器信息。
7. 单击 * 关闭 *。

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。