管理 SAML 身份验证设置

Active IQ Unified Manager 9.9

NetApp
January 31, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/active-iq-unified-manager-99/config/reference-identity-provider-requirements-um.html on January 31, 2025. Always check docs.netapp.com for the latest.

目录

管理 SAML 身份验证设置 1
身份提供程序要求 1
启用 SAML 身份验证 2

管理 SAML 身份验证设置

配置远程身份验证设置后，您可以启用安全断言标记语言（ Security Assertion Markup Language ， SAML ）身份验证，以便远程用户先通过安全身份提供程序（ IdP ）进行身份验证，然后才能访问 Unified Manager Web UI 。

请注意，启用 SAML 身份验证后，只有远程用户才能访问 Unified Manager 图形用户界面。本地用户和维护用户将无法访问此 UI 。此配置不会影响访问维护控制台的用户。

身份提供程序要求

在将 Unified Manager 配置为使用身份提供程序（ Identity Provider ， IdP ）对所有远程用户执行 SAML 身份验证时，您需要了解一些必需的配置设置，以便成功连接到 Unified Manager 。

您必须在 IdP 服务器中输入 Unified Manager URI 和元数据。您可以从 Unified ManagerSAML 身份验证页面复制此信息。在安全断言标记语言（ SAML ）标准中， Unified Manager 被视为服务提供商（ Service Provider ， SP ）。

支持的加密标准

- 高级加密标准（ AES ）： AES-128 和 AES-256
- 安全哈希算法（ Secure Hash Algorithm ， SHA ）： SHA-1 和 SHA-256

经过验证的身份提供程序

- Shibboleth
- Active Directory 联合身份验证服务（ ADFS ）

ADFS 配置要求

- 您必须按以下顺序定义 Unified Manager 解析此依赖方信任条目的 ADFS SAML 响应所需的三个声明规则。

声明规则	价值
sam 帐户名称	名称 ID
sam 帐户名称	urn： OID： 0.9.2342.19200300.100.1.1
令牌组—非限定名称	urn： OID： 1.3.6.1.4.1.5923.1.5.1.1

- 您必须将身份验证方法设置为 "`Forms Authentication` "，否则用户可能会在注销 Unified Manager 时收到错误。请按照以下步骤操作：
  a. 打开 ADFS 管理控制台。
  b. 单击左侧树视图中的身份验证策略文件夹。

c. 在右侧的 "Actions" 下，单击 Edit Global Primary Authentication Policy 。

d. 将 "Intranet Authentication Method" （内部网身份验证方法）设置为 "`Forms Authentication` " ，而不是默认值 "`Windows Authentication` " 。

- 在某些情况下，如果 Unified Manager 安全证书是 CA 签名的，则通过 IdP 登录将被拒绝。要解决此问题描述，可以使用两种解决方法：
  - 按照链接中的说明在 ADFS 服务器上禁用对链接的 CA 证书关联依赖方进行的撤消检查：

"禁用每个依赖方信任的撤消检查"

- 将 CA 服务器驻留在 ADFS 服务器中，以便对 Unified Manager 服务器证书请求进行签名。

其他配置要求

- Unified Manager 时钟偏差设置为 5 分钟，因此 IdP 服务器和 Unified Manager 服务器之间的时间差不能超过 5 分钟，否则身份验证将失败。

启用 SAML 身份验证

您可以启用安全断言标记语言（ SAML ）身份验证，以便远程用户在访问 Unified Manager Web UI 之前先通过安全身份提供程序（ IdP ）进行身份验证。

开始之前

- 您必须已配置远程身份验证并验证它是否成功。
- 您必须已至少创建一个具有应用程序管理员角色的远程用户或远程组。
- Unified Manager 必须支持身份提供程序（ IdP ），并且必须对其进行配置。
- 您必须具有 IdP URL 和元数据。
- 您必须有权访问 IdP 服务器。

关于此任务

从 Unified Manager 启用 SAML 身份验证后，只有在为 IdP 配置了 Unified Manager 服务器主机信息之后，用户才能访问图形用户界面。因此，在开始配置过程之前，您必须准备好完成连接的两个部分。可以在配置 Unified Manager 之前或之后配置 IdP 。

启用 SAML 身份验证后，只有远程用户才能访问 Unified Manager 图形用户界面。本地用户和维护用户将无法访问此 UI 。此配置不会影响访问维护控制台， Unified Manager 命令或 ZAPI 的用户。

在此页面上完成 SAML 配置后， Unified Manager 将自动重新启动。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * SAML 身份验证 * 。
2. 选中 * 启用 SAML 身份验证 * 复选框。

此时将显示配置 IdP 连接所需的字段。

3. 输入将 Unified Manager 服务器连接到 IdP 服务器所需的 IdP URI 和 IdP 元数据。

   如果可以直接从 Unified Manager 服务器访问 IdP 服务器，则可以在输入 IdP URI 后单击 * 提取 IdP 元数据 * 按钮以自动填充 IdP 元数据字段。

4. 复制 Unified Manager 主机元数据 URI ，或者将主机元数据保存到 XML 文本文件中。

   此时，您可以使用此信息配置 IdP 服务器。

5. 单击 * 保存 * 。

   此时将显示一个消息框，确认您要完成配置并重新启动 Unified Manager 。

6. 单击 * 确认并注销 * ， Unified Manager 将重新启动。

结果

授权远程用户下次尝试访问 Unified Manager 图形界面时，他们将在 IdP 登录页面而不是 Unified Manager 登录页面中输入凭据。

完成后

如果尚未完成，请访问 IdP 并输入 Unified Manager 服务器 URI 和元数据以完成配置。

使用 ADFS 作为身份提供程序时， Unified Manager 图形用户界面不会遵守 ADFS 超时要求，它将继续工作，直到达到 Unified Manager 会话超时为止。您可以通过单击 * 常规 * > * 功能设置 * > * 非活动超时 * 来更改 GUI 会话超时。

版权信息

版权所有 © 2025 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，本文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。