



管理网络和安全 AFX

NetApp
February 11, 2026

目录

管理网络和安全	1
管理 AFX 存储系统集群网络	1
创建广播域	1
创建 IP 空间	1
创建子网	2
创建网络接口	2
相关信息	3
管理 AFX 存储系统以太网端口	3
创建 VLAN	3
创建 LAG	3
相关信息	4
准备 AFX 存储系统身份验证服务	4
配置 LDAP	4
配置 SAML 身份验证	4
相关信息	5
管理 AFX 存储系统集群用户和角色	5
创建帐户角色	5
创建集群帐户	5
相关信息	6
管理 AFX 存储系统上的证书	6
生成证书签名请求	6
添加受信任的证书颁发机构	6
续订或删除受信任的证书颁发机构	7
添加客户端/服务器证书或本地证书颁发机构	7
续订或删除客户端/服务器证书或本地证书颁发机构	8
相关信息	8

管理网络和安全

管理 AFX 存储系统集群网络

您需要配置 AFX 存储系统的网络。网络环境支持多种场景，包括客户端访问 SVM 上的数据和集群间通信。



创建网络资源是重要的第一步。您还需要根据需要执行其他管理操作，例如编辑或删除网络定义。

创建广播域

广播域通过对属于同一第二层网络的端口进行分组来简化集群网络的管理。然后可以为存储虚拟机 (SVM) 分配组中的端口，用于数据或管理流量。

集群设置期间会创建多个广播域，包括：

默认

该广播域包含“默认”IP空间中的端口。这些端口主要用于提供数据。还包括集群管理和节点管理端口。

集群

该广播域包含“集群”IP空间中的端口。这些端口用于集群通信，包括集群中所有节点的所有集群端口。

您可以在集群初始化后创建其他广播域。创建广播域时，将自动创建包含相同端口的故障转移组。

关于此任务

为广播域定义的端口的最大传输单元 (MTU) 值将更新为广播域中设置的 MTU 值。

步骤

1. 在系统管理器中，选择*网络*，然后选择*概览*。
2. 在“广播域”下，选择 **+ Add**。
3. 提供广播域的名称或接受默认值。

所有广播域名在 IP 空间内必须是唯一的。

4. 提供最大传输单元 (MTU) 。

MTU是广播域内可接受的最大数据包。

5. 选择所需的端口并选择*保存*。

创建 IP 空间

IP空间是IP地址和相关网络配置的管理域。这些空间可用于通过隔离管理和路由来支持您的 SVM。例如，当客户端具有来自相同 IP 地址和子网范围的重叠 IP 地址时，它们很有用。



您必须先拥有一个 IP 空间，然后才能创建子网。

步骤

1. 在系统管理器中，选择*网络*，然后选择*概览*。
2. 在“IP 空间”下，选择 **+ Add**。
3. 提供 IP 空间的名称或接受默认值。

所有 IP 空间名称在集群内必须是唯一的。

4. 选择*保存*。

下一步

您可以使用 IP 空间来创建子网。

创建子网

子网或子网强制对网络中的 IP 地址空间进行逻辑划分。它使您能够分配专用的 IP 地址块来创建网络接口 (LIF)。子网允许您使用子网名称而不是特定的 IP 地址和网络掩码组合，从而简化了 LIF 的创建。

开始之前

您必须有一个广播域和将定义子网的 IP 空间。另请注意：

- 所有子网名称在特定 IP 空间内必须是唯一的。
- 子网使用的 IP 地址范围不能与其他子网的 IP 地址重叠。

步骤

1. 在系统管理器中，选择*网络*，然后选择*概览*。
2. 在“子网”选项卡下，选择 **+ Add**。
3. 提供配置详细信息，包括子网名称、IP 地址详细信息和广播域。
4. 选择*保存*。

下一步

新的子网将简化网络接口的创建。

创建网络接口

逻辑网络接口 (LIF) 由 IP 地址和相关网络配置参数组成。它可以与物理或逻辑端口相关联，通常由客户端用来访问 SVM 提供的的数据。LIF 在发生故障时提供弹性，并且可以在节点端口之间迁移，因此通信不会中断。

步骤

1. 在系统管理器中，选择*网络*，然后选择*概览*。
2. 在“网络接口”选项卡下，选择 **+ Add**。
3. 提供配置详细信息，包括接口名称、接口类型、允许的协议和 IP 地址详细信息。
4. 选择*保存*。

相关信息

- ["管理 AFX 以太网端口"](#)
- ["了解ONTAP广播域"](#)
- ["了解ONTAP IP 空间配置"](#)
- ["了解ONTAP网络的子网"](#)
- ["网络架构概述"](#)

管理 AFX 存储系统以太网端口

AFX 系统使用的端口为网络连接和通信提供了基础。有多种选项可用于定制网络的第二层配置。

创建 VLAN

VLAN 由分组到广播域的交换机端口组成。VLAN 使您能够提高安全性、隔离潜在问题并限制 IP 网络基础设施内的可用路径。

开始之前

网络中部署的交换机必须符合 IEEE 802.1Q 标准或具有特定于供应商的 VLAN 实现。

关于此任务

请注意以下事项：

- 您无法在没有任何成员端口的接口组端口上创建 VLAN。
- 当您第一次在端口上配置 VLAN 时，端口可能会关闭，从而导致网络暂时断开。后续向同一端口添加 VLAN 不会影响端口状态。
- 您不应在网络接口上创建与交换机的本机 VLAN 具有相同标识符的 VLAN。例如，如果网络接口 e0b 位于本机 VLAN 10 上，则不应在该接口上创建 VLAN e0b-10。

步骤

1. 在系统管理器中，选择*网络*，然后选择*以太网端口*。
2. 选择 **+ VLAN**。
3. 提供配置详细信息，包括所需节点的 ID、广播域和端口。

VLAN 不能连接到托管集群 LIF 的端口或分配给集群 IP 空间的端口。

4. 选择*保存*。

结果

您已创建 VLAN 来提高安全性、隔离问题并限制 IP 网络基础设施内的可用路径。

创建 LAG

链路聚合组 (LAG) 是一种将多个物理网络连接组合成单个逻辑连接的技术。您可以使用它来增加带宽并在节点

之间提供冗余。

步骤

1. 在系统管理器中，选择*网络*，然后选择*以太网端口*。
2. 选择*链接聚合组*。
3. 提供配置详细信息，包括节点、广播域、端口、模式和负载分布。
4. 选择*保存*。

相关信息

- ["管理 AFX 群集网络"](#)
- ["了解ONTAP网络端口配置"](#)
- ["组合物理端口以创建ONTAP接口组"](#)

准备 AFX 存储系统身份验证服务

您需要准备AFX系统对用户账户和角色定义的身份验证和授权服务。

配置 LDAP

您可以配置轻量级目录访问协议 (LDAP) 服务器以在中心位置维护身份验证信息。

开始之前

您必须生成证书签名请求并添加 CA 签名的服务器数字证书。

步骤

1. 在系统管理器中，选择*集群*，然后选择*设置*。
2. 选择  在 **LDAP** 旁边。
3. 选择  **Add** 并提供 LDAP 服务器的名称或 IP 地址。
4. 提供必要的配置信息，包括架构、基本 DN、端口和绑定。
5. 选择*保存*。

配置 SAML 身份验证

安全断言标记语言 (SAML) 身份验证使用户能够通过安全身份提供商 (IdP) 而不是使用其他协议（如 LDAP）的提供商进行身份验证。

开始之前

- 必须配置您计划用于远程身份验证的身份提供者。有关配置详细信息，请参阅提供商文档。
- 您必须拥有身份提供者的 URI。

步骤

1. 在系统管理器中，选择*集群*，然后选择*设置*。

2. 选择  在 安全 下，**SAML** 身份验证 旁边。
3. 选择*启用 SAML 身份验证*。
4. 提供 **IdP URL** 和 主机系统 IP 地址并选择 保存。

确认窗口显示已自动复制到剪贴板的元数据信息。

5. 导航到您指定的 IdP 系统并从剪贴板复制元数据以更新系统元数据。
6. 返回系统管理器中的确认窗口并选择*我已使用主机 URI 或元数据配置了 IdP*。
7. 选择*注销*以启用基于 SAML 的身份验证。

IdP 系统将显示身份验证屏幕。

相关信息

- ["管理 AFX 集群用户和角色"](#)
- ["为远程ONTAP用户配置 SAML 身份验证"](#)
- ["身份验证和访问控制"](#)

管理 AFX 存储系统集群用户和角色

您可以根据 AFX 提供的身份验证和授权服务定义用户帐户和角色。

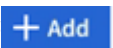


每个ONTAP用户都需要分配一个角色。角色包括权限并决定用户能够执行的操作。

创建帐户角色

当您的 AFX 集群设置并初始化时，会自动创建集群管理员和存储 VM 管理员的角色。您可以创建其他用户帐户角色来定义分配了这些角色的用户可以在您的集群上执行的特定功能。

步骤

1. 在系统管理器中，选择*集群*，然后选择*设置*。
2. 在“安全”部分中，在“用户和角色”旁边，选择 .
3. 在“角色”下，选择 .
4. 提供角色的名称和属性。
5. 选择*保存*。

创建集群帐户

您可以创建一个集群级帐户，以便在执行集群或 SVM 管理时使用。

步骤

1. 在系统管理器中，选择*集群*，然后选择*设置*。
2. 在“安全”部分中，选择  在*用户和角色*旁边。

3. 选择  **Add** . 在 用户 下。
4. 输入用户名，然后选择用户的角色。

该角色应该适合用户。例如，**admin** 角色能够在您的集群上执行所有配置任务。

5. 选择用户登录方法和身份验证方法；通常是*密码*。
6. 输入用户的密码。
7. 选择*保存*。

结果

已创建一个新帐户并可供您的 AFX 集群使用。

相关信息

- ["准备身份验证服务"](#)
- ["额外的 AFX SVM 管理"](#)

管理 AFX 存储系统上的证书

根据您的环境，您需要在管理 AFX 的过程中创建和管理数字证书。您可以执行几个相关任务。

生成证书签名请求

要开始使用数字证书，您需要生成证书签名请求 (CSR)。CSR 用于从证书颁发机构 (CA) 请求签名的证书。作为此过程的一部分，ONTAP 会创建公钥/私钥对并将公钥包含在 CSR 中。

步骤

1. 在系统管理器中，选择*集群*，然后选择*设置*。
2. 在“安全”下，在“证书”旁边，选择 
3. 选择  **Generate CSR**。
4. 提供主题的通用名称和国家/地区；可选地提供组织和组织单位。
5. 要更改定义证书的默认值，请选择  **More options** 并进行所需的更新。
6. 选择*生成*。

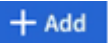
结果

您已生成可用于请求公钥证书的 CSR。

添加受信任的证书颁发机构

ONTAP 提供了一组默认的可信根证书，可用于传输层安全性 (TLS) 和其他协议。您可以根据需要添加其他受信任的证书颁发机构。

步骤

1. 在系统管理器中，选择*集群*，然后选择*设置*。
2. 在“安全”下，在“证书”旁边，选择 →。
3. 选择选项卡 受信任的证书颁发机构，然后选择 。
4. 提供配置信息，包括名称、范围、通用名称、类型和证书详细信息；您可以通过选择*导入*来导入证书。
5. 选择“添加”。

结果

您已将受信任的证书颁发机构添加到您的 AFX 系统。

续订或删除受信任的证书颁发机构

受信任的证书颁发机构必须每年更新。如果您不想更新过期的证书，您应该将其删除。

步骤

1. 选择“集群”，然后选择“设置”。
2. 在“安全”下，在“证书”旁边，选择 →。
3. 选择选项卡“受信任的证书颁发机构”。
4. 选择您想要续订或删除的信任证书颁发机构。
5. 更新或删除证书颁发机构。

要更新证书颁发机构，请执行以下操作：	要删除证书颁发机构，请执行以下操作：
a. 选择  然后选择*续订*。 b. 输入或导入证书信息并选择*更新*。	a. 选择  然后选择*删除*。 b. 确认您要删除并选择*删除*。

结果

您已更新或删除 AFX 系统上现有的受信任证书颁发机构。

添加客户端/服务器证书或本地证书颁发机构

您可以添加客户端/服务器证书或本地证书颁发机构作为启用安全 Web 服务的一部分。

步骤

1. 在系统管理器中，选择*集群*，然后选择*设置*。
2. 在“安全”下，在“证书”旁边，选择 →。
3. 根据需要选择*客户端/服务器证书*或*本地证书颁发机构*。
4. 添加证书信息并选择*保存*。

结果

您已向 AFX 系统添加了新的客户端/服务器证书或本地权限。

续订或删除客户端/服务器证书或本地证书颁发机构

客户端/服务器证书和本地证书颁发机构必须每年更新。如果您不想更新过期的证书或本地证书颁发机构，您应该删除它们。

步骤

1. 选择“集群”，然后选择“设置”。
2. 在“安全”下，在“证书”旁边，选择 .
3. 根据需要选择*客户端/服务器证书*或*本地证书颁发机构*。
4. 选择您要续订或删除的证书。
5. 更新或删除证书颁发机构。

要更新证书颁发机构，请执行以下操作：	要删除证书颁发机构，请执行以下操作：
a. 选择  然后选择*续订*。 b. 输入或导入证书信息并选择*更新*。	选择  然后选择*删除*。

结果

您已更新或删除 AFX 系统上现有的客户端/服务器证书或本地证书颁发机构。

相关信息

- ["在ONTAP中生成并安装 CA 签名的服务器证书"](#)
- ["使用 System Manager 管理ONTAP证书"](#)

版权信息

版权所有 © 2026 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。