



# 管理帐户

## Element Software

NetApp  
March 05, 2025

# 目录

管理帐户 .....	1
了解更多信息 .....	1
使用CHAP处理帐户 .....	1
CHAP算法 .....	1
创建帐户 .....	1
查看帐户详细信息 .....	2
编辑帐户 .....	2
删除帐户 .....	3
了解更多信息 .....	3
管理集群管理员用户帐户 .....	3
存储集群管理员帐户类型 .....	4
查看集群管理员详细信息 .....	4
创建集群管理员帐户 .....	5
编辑集群管理员权限 .....	6
更改集群管理员帐户的密码 .....	6
了解更多信息 .....	6
管理LDAP .....	6

# 管理帐户

在SolidFire 存储系统中、租户可以使用帐户使客户端能够连接到集群上的卷。创建卷时、卷会分配给特定帐户。您还可以管理 SolidFire 存储系统的集群管理员帐户。

- ["使用CHAP处理帐户"](#)
- ["管理集群管理员用户帐户"](#)

## 了解更多信息

- ["SolidFire 和 Element 软件文档"](#)
- ["适用于 vCenter Server 的 NetApp Element 插件"](#)

## 使用CHAP处理帐户

在SolidFire 存储系统中、租户可以使用帐户使客户端能够连接到集群上的卷。帐户包含访问分配给它的卷所需的质询握手身份验证协议(Challenge-Handshake Authentication Protocol、CHAP)身份验证。创建卷时、卷会分配给特定帐户。

一个帐户最多可以分配 2,000 个卷，但一个卷只能属于一个帐户。

### CHAP算法

从Element 12.7开始、支持符合FIPS的安全CHAP算法SHA1、SHA-256和SHA3-256。对于Element 12.7、当主机iSCSI启动程序创建与Element iSCSI目标的iSCSI会话时、它会请求一个要使用的CHAP算法列表。Element iSCSI目标会从主机iSCSI启动程序请求的列表中选择它支持的第一个算法。要确认Element iSCSI目标选择的是最安全的算法、您必须将主机iSCSI启动程序配置为发送从最安全位置(例如SHA3-256)到最不安全位置(例如SHA1或MD5)。如果主机iSCSI启动程序未请求SHA算法、则Element iSCSI目标会选择MD5、前提是主机中的建议算法列表包含MD5。您可能需要更新主机iSCSI启动程序配置、以支持安全算法。

在Element 12.7升级期间、如果您已更新主机iSCSI启动程序配置、以便在存储节点重新启动时发送包含SHA算法列表的会话请求、此时将激活新的安全算法、并使用最安全的协议建立新的或重新连接的iSCSI会话。在升级期间、所有现有iSCSI会话都会从MD5过渡到SHA。如果不更新主机iSCSI启动程序配置以请求SHA、则现有iSCSI会话将继续使用MD5。稍后、在更新主机iSCSI启动程序CHAP算法后、iSCSI会话应根据导致iSCSI会话重新连接的维护活动逐渐从MD5过渡到SHA。

例如、Red Hat Enterprise Linux (RHEL) 8.3中的默认主机iSCSI启动程序的设置已`node.session.auth.chap\_algs = SHA3-256,SHA256,SHA1,MD5`注释掉、从而导致iSCSI启动程序仅使用MD5。在主机上取消此设置的注释并重新启动iSCSI启动程序会触发来自该主机的iSCSI会话、以便开始使用SHA3-256。

如果需要、您可以使用 ["ListISCSISessions"](#) API方法查看每个会话所使用的CHAP算法。

### 创建帐户

您可以创建帐户以允许访问卷。

系统中的每个帐户名称都必须是唯一的。

1. 选择 \* 管理 \* > \* 帐户 \* 。
2. 单击 \* 创建帐户 \* 。
3. 输入 \* 用户名 \* 。
4. 在 \* CHAP Settings\* 部分中，输入以下信息：



将凭据字段留空可自动生成任一密码。

- 用于 CHAP 节点会话身份验证的 \* 启动程序机密 \* 。
  - 用于 CHAP 节点会话身份验证的 \* 目标机密 \* 。
5. 单击 \* 创建帐户 \* 。

## 查看帐户详细信息

您可以通过图形格式查看各个帐户的性能活动。

图形信息提供帐户的 I/O 和吞吐量信息。平均和峰值活动级别以 10 秒报告周期为增量进行显示。这些统计信息包括分配给帐户的所有卷的活动。

1. 选择 \* 管理 \* > \* 帐户 \* 。
2. 单击帐户对应的 "Actions" 图标。
3. 单击 \* 查看详细信息 \* 。

下面是一些详细信息：

- \* 状态 \*：帐户的状态。可能值：
  - Active：处于活动状态的帐户。
  - locked：已锁定的帐户。
  - removed：已删除并清除的帐户。
- \* 活动卷 \*：分配给帐户的活动卷数。
- \* 压缩 \*：分配给帐户的卷的压缩效率得分。
- \* 重复数据删除 \*：分配给帐户的卷的重复数据删除效率得分。
- \* 精简配置 \*：分配给帐户的卷的精简配置效率得分。
- \* 整体效率 \*：分配给帐户的卷的整体效率得分。

## 编辑帐户

您可以编辑帐户以更改状态，更改 CHAP 密码或修改帐户名称。

修改帐户中的 CHAP 设置或从访问组中删除启动程序或卷可能会使发生原因启动程序意外丢失对卷的访问权限。要验证卷访问不会意外丢失，请始终注销将受帐户或访问组更改影响的 iSCSI 会话，并验证启动程序是否可以在完成启动程序设置和集群设置的任何更改后重新连接到卷。



与管理服务关联的永久性卷将分配给在安装或升级期间创建的新帐户。如果您使用的是永久性卷，请勿修改或删除其关联帐户。

1. 选择 \* 管理 \* > \* 帐户 \*。
2. 单击帐户对应的 "Actions" 图标。
3. 在显示的菜单中，选择 \* 编辑 \*。
4. \* 可选：\* 编辑 \* 用户名 \*。
5. \* 可选：\* 单击 \* 状态 \* 下拉列表并选择其他状态。



将状态更改为 \* 已锁定 \* 将终止与帐户的所有 iSCSI 连接，并且无法再访问此帐户。与帐户关联的卷会保留下来，但这些卷不能通过 iSCSI 发现。

6. \* 可选：\* 在 \* CHAP Settings \* 下，编辑用于节点会话身份验证的 \* 启动程序机密 \* 和 \* 目标机密 \* 凭据。



如果不更改 \* CHAP Settings \* 凭据，它们将保持不变。如果将凭据字段留空，系统将生成新密码。

7. 单击 \* 保存更改 \*。

## 删除帐户

您可以删除不再需要的帐户。

删除帐户之前，请删除并清除与帐户关联的所有卷。



与管理服务关联的永久性卷将分配给在安装或升级期间创建的新帐户。如果您使用的是永久性卷，请勿修改或删除其关联帐户。

1. 选择 \* 管理 \* > \* 帐户 \*。
2. 单击要删除的帐户对应的 "Actions" 图标。
3. 在显示的菜单中，选择 \* 删除 \*。
4. 确认操作。

## 了解更多信息

- ["SolidFire 和 Element 软件文档"](#)
- ["适用于 vCenter Server 的 NetApp Element 插件"](#)

## 管理集群管理员用户帐户

您可以通过创建，删除和编辑集群管理员帐户，更改集群管理员密码以及配置 LDAP 设置来管理用户的系统访问来管理 SolidFire 存储系统的集群管理员帐户。

## 存储集群管理员帐户类型

运行 NetApp Element 软件的存储集群中可以存在两种类型的管理员帐户：主集群管理员帐户和集群管理员帐户。

- \* 主集群管理员帐户 \*

此管理员帐户是在创建集群时创建的。此帐户是对集群具有最高访问级别的主管理帐户。此帐户类似于 Linux 系统中的 root 用户。您可以更改此管理员帐户的密码。

- \* 集群管理员帐户 \*

您可以为集群管理员帐户授予有限的管理访问权限，以便在集群中执行特定任务。分配给每个集群管理员帐户的凭据用于对存储系统中的 API 和 Element UI 请求进行身份验证。



要通过每节点 UI 访问集群中的活动节点，需要使用本地（非 LDAP）集群管理员帐户。访问尚未加入集群的节点不需要帐户凭据。

## 查看集群管理员详细信息

1. 要创建集群范围（非 LDAP）的集群管理员帐户，请执行以下操作：

a. 单击 \* 用户 \* > \* 集群管理员 \*。

2. 在用户选项卡的集群管理员页面上，您可以查看以下信息。

- \* ID \*：分配给集群管理员帐户的序列号。
- \* 用户名 \*：创建集群管理员帐户时为其指定的名称。
- \* 访问 \*：分配给用户帐户的用户权限。可能值：

- 读取
- 报告
- 节点
- 驱动器
- 卷
- 帐户
- clusterAdmins
- 管理员
- 支持管理员



所有权限均可用于管理员访问类型。

- \* 类型 \*：集群管理员的类型。可能值：
  - 集群
  - ldap
- \* 属性 \*：如果集群管理员帐户是使用 Element API 创建的，则此列将显示使用该方法设置的任何名称 -

值对。

请参阅。 "《NetApp Element 软件 API 参考》"

## 创建集群管理员帐户

您可以创建具有允许或限制对存储系统特定区域的访问权限的新集群管理员帐户。设置集群管理员帐户权限时，系统会为您未分配给集群管理员的任何权限授予只读权限。

如果要创建 LDAP 集群管理员帐户，请确保在开始之前已在集群上配置 LDAP。

### "使用 Element 用户界面启用 LDAP 身份验证"

您可以稍后更改报告，节点，驱动器，卷，帐户的集群管理员帐户权限。和集群级别访问。启用某个权限后，系统会为此级别分配写入访问权限。系统会为管理员用户授予对您未选择的级别的只读访问权限。

您也可以稍后删除系统管理员创建的任何集群管理员用户帐户。您不能删除在创建集群时创建的主集群管理员帐户。

1. 要创建集群范围（非 LDAP）的集群管理员帐户，请执行以下操作：
  - a. 单击 \* 用户 \* > \* 集群管理员 \*。
  - b. 单击 \* 创建集群管理员 \*。
  - c. 选择 \* 集群 \* 用户类型。
  - d. 输入帐户的用户名和密码并确认密码。
  - e. 选择要应用于帐户的用户权限。
  - f. 选中此复选框以同意最终用户许可协议。
  - g. 单击 \* 创建集群管理员 \*。
2. 要在 LDAP 目录中创建集群管理员帐户，请执行以下操作：
  - a. 单击 \* 集群 \* > \* LDAP \*。
  - b. 确保已启用 LDAP 身份验证。
  - c. 单击 \* 测试用户身份验证 \*，然后复制为用户或用户所属组之一显示的可分辨名称，以便您可以稍后粘贴。
  - d. 单击 \* 用户 \* > \* 集群管理员 \*。
  - e. 单击 \* 创建集群管理员 \*。
  - f. 选择 LDAP 用户类型。
  - g. 在 Distinguished Name 字段中，按照文本框中的示例输入用户或组的完整可分辨名称。或者，也可以从先前复制的可分辨名称中粘贴该名称。

如果可分辨名称属于某个组，则 LDAP 服务器上属于该组的任何用户都将拥有此管理员帐户的权限。

要添加 LDAP 集群管理员用户或组，用户名的常规格式为 "ldap： <完整可分辨名称>"。

- a. 选择要应用于帐户的用户权限。

- b. 选中此复选框以同意最终用户许可协议。
- c. 单击 \* 创建集群管理员 \*。

## 编辑集群管理员权限

您可以更改报告，节点，驱动器，卷，帐户的集群管理员帐户权限，和集群级别访问。启用某个权限后，系统会为此级别分配写入访问权限。系统会为管理员用户授予对您未选择的级别的只读访问权限。

1. 单击 \* 用户 \* > \* 集群管理员 \*。
2. 单击要编辑的集群管理员对应的 "Actions" 图标。
3. 单击 \* 编辑 \*。
4. 选择要应用于帐户的用户权限。
5. 单击 \* 保存更改 \*。

## 更改集群管理员帐户的密码

您可以使用 Element UI 更改集群管理员密码。

1. 单击 \* 用户 \* > \* 集群管理员 \*。
2. 单击要编辑的集群管理员对应的 "Actions" 图标。
3. 单击 \* 编辑 \*。
4. 在更改密码字段中，输入新密码并进行确认。
5. 单击 \* 保存更改 \*。

## 了解更多信息

- ["使用 Element 用户界面启用 LDAP 身份验证"](#)
- ["禁用LDAP"](#)
- ["SolidFire 和 Element 软件文档"](#)
- ["适用于 vCenter Server 的 NetApp Element 插件"](#)

## 管理LDAP

您可以设置轻型目录访问协议（ Lightweight Directory Access Protocol ， LDAP ），以便为 SolidFire 存储启用基于目录的安全登录功能。您可以在集群级别配置 LDAP 并授权 LDAP 用户和组。

管理 LDAP 涉及使用现有 Microsoft Active Directory 环境为 SolidFire 集群设置 LDAP 身份验证并测试配置。



您可以同时使用 IPv4 和 IPv6 地址。

启用 LDAP 涉及以下高级步骤，详细说明如下：



1. \* 完成 LDAP 支持的预配置步骤 \*。验证您是否具有配置 LDAP 身份验证所需的所有详细信息。
2. \* 启用 LDAP 身份验证 \*。使用 Element UI 或 Element API。
3. \* 验证 LDAP 配置 \*。或者，也可以通过运行 GetLdapConfiguration API 方法或使用 Element UI 检查 LDAP 配置来检查集群是否配置了正确的值。
4. 测试LDAP身份验证(与用户一起 readonly)。通过运行 TestLdapAuthentication API 方法或使用 Element UI 测试 LDAP 配置是否正确。对于此初始测试、请使用用户的用户名`AMAccountName s `readonly。这将验证是否已为集群正确配置LDAP身份验证、同时还将验证`readonly`凭据和访问是否正确。如果此步骤失败，请重复步骤 1 到 3。
5. \* 测试 LDAP 身份验证 \*（使用要添加的用户帐户）。使用要添加为 Element 集群管理员的用户帐户重复 step 4。复制`distinguished`名称(DN)或用户(或组)。此 DN 将在步骤 6 中使用。
6. \* 添加 LDAP 集群管理 \*（复制并粘贴测试 LDAP 身份验证步骤中的 DN）。使用 Element UI 或 AddLdapClusterAdmin API 方法，创建具有适当访问级别的新集群管理员用户。对于用户名，请粘贴您在步骤 5 中复制的完整 DN。这样可以确保 DN 格式正确。
7. \* 测试集群管理员访问权限 \*。使用新创建的 LDAP 集群管理员用户登录到集群。如果添加了 LDAP 组，则可以以该组中的任何用户身份登录。

### 完成 LDAP 支持的预配置步骤

在 Element 中启用 LDAP 支持之前，您应先设置 Windows Active Directory 服务器并执行其他预配置任务。

#### 步骤

1. 设置 Windows Active Directory 服务器。
2. \* 可选： \* 启用 LDAPS 支持。
3. 创建用户和组。
4. 创建一个只读服务帐户（例如 sfreadonly），用于搜索 LDAP 目录。

### 使用 Element 用户界面启用 LDAP 身份验证

您可以配置存储系统与现有 LDAP 服务器的集成。这样，LDAP 管理员就可以集中管理用户的存储系统访问权限。

您可以使用 Element 用户界面或 Element API 配置 LDAP。此操作步骤介绍了如何使用 Element UI 配置 LDAP。

此示例显示了如何在SolidFire上配置LDAP身份验证、并使用`SearchAndBind`作为身份验证类型。此示例使用一个 Windows Server 2012 R2 Active Directory 服务器。

#### 步骤

1. 单击 \* 集群 \* > \* LDAP \*。
2. 单击 \* 是 \* 以启用 LDAP 身份验证。
3. 单击 \* 添加服务器 \*。
4. 输入 \* 主机名 /IP 地址 \*。



也可以输入可选的自定义端口号。

例如，要添加自定义端口号，请输入 < 主机名或 IP 地址 > : < 端口号 >

5. \* 可选：\* 选择 \* 使用 LDAPS 协议 \*。
6. 在 \* 常规设置 \* 中输入所需信息。

#### LDAP Servers

Host Name/IP Address	<input type="text" value="192.168.9.99"/>	<a href="#">Remove</a>
	<input type="checkbox"/> Use LDAPS Protocol	

[Add a Server](#)

#### General Settings

Auth Type	<input type="text" value="Search and Bind"/>	
Search Bind DN	<input type="text" value="msmyth@thesmyths.ca"/>	
Search Bind Password	<input type="text" value="e.g. password"/>	<input type="checkbox"/> Show password
User Search Base DN	<input type="text" value="OU=Home users,DC=thesmyths,DC=ca"/>	
User Search Filter	<input type="text" value="(&amp;(objectClass=person)((sAMAccountName=%USER"/>	
Group Search Type	<input type="text" value="Active Directory"/>	
Group Search Base DN	<input type="text" value="OU=Home users,DC=thesmyths,DC=ca"/>	

[Save Changes](#)

7. 单击\*启用LDAP\*。
8. 如果要测试用户的服务器访问权限，请单击 \* 测试用户身份验证 \*。
9. 复制显示的可分辨名称和用户组信息，以供日后创建集群管理员时使用。
10. 单击 \* 保存更改 \* 以保存任何新设置。
11. 要在此组中创建用户以便任何人都可以登录，请完成以下操作：
  - a. 单击 \* 用户 \* > \* 查看 \*。

## Create a New Cluster Admin

### Select User Type

Cluster  LDAP

### Enter User Details

Distinguished Name

CN=StorageAdmins,OU=Home  
users,DC=thesmyths,DC=ca

### Select User Permissions

- |                                    |  |
|------------------------------------|--|
| <input type="checkbox"/> Reporting | <input type="checkbox"/> Volumes       |
| <input type="checkbox"/> Nodes     | <input type="checkbox"/> Accounts      |
| <input type="checkbox"/> Drives    | <input type="checkbox"/> Cluster Admin |

### Accept the Following End User License Agreement

- 对于新用户，单击 "User Type"（用户类型）中的 "\* ldap\*"，然后将您复制的组粘贴到 "Distinguished Name"（可分辨名称）字段中。
- 选择权限，通常为所有权限。
- 向下滚动到最终用户许可协议，然后单击 \* 我接受 \*。
- 单击 \* 创建集群管理员 \*。

现在，您的用户具有 Active Directory 组的值。

要对此进行测试，请从 Element UI 中注销，然后以该组中的用户身份重新登录。

#### 使用 **Element API** 启用 **LDAP** 身份验证

您可以配置存储系统与现有 LDAP 服务器的集成。这样，LDAP 管理员就可以集中管理用户的存储系统访问权限。

您可以使用 Element 用户界面或 Element API 配置 LDAP。此操作步骤介绍了如何使用 Element API 配置

LDAP。

要在SolidFire集群上利用LDAP身份验证、请首先使用API方法在集群上启用LDAP身份验证 EnableLdapAuthentication。

步骤

1. 首先使用API方法在集群上启用LDAP身份验证 EnableLdapAuthentication。
2. 输入所需信息。

```
{
  "method": "EnableLdapAuthentication",
  "params": {
    "authType": "SearchAndBind",
    "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
    "groupSearchType": "ActiveDirectory",
    "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
    "searchBindPassword": "ReadOnlyPW",
    "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
    "userSearchFilter":
    "(&(objectClass=person)(sAMAccountName=%USERNAME%))"
    "serverURIs": [
      "ldap://172.27.1.189",
    ],
    "id": "1"
  }
}
```

3. 更改以下参数的值:

使用的参数	说明
AuthType : SearchAndBind	指示集群将使用只读服务帐户首先搜索要进行身份验证的用户，然后在发现并经过身份验证后绑定该用户。
groupSearchBaseDN : DC=prodtest , dc=solidfire , dc=net	指定 LDAP 树中开始搜索组的位置。在本示例中，我们使用了树的根。如果 LDAP 树非常大，您可能需要将其设置为更精细的子树以减少搜索时间。
userSearchBaseDN : DC=prodtest , dc=solidfire , dc=net	指定 LDAP 树中开始搜索用户的位置。在本示例中，我们使用了树的根。如果 LDAP 树非常大，您可能需要将其设置为更精细的子树以减少搜索时间。
groupSearchType : ActiveDirectory	使用 Windows Active Directory 服务器作为 LDAP 服务器。

使用的参数	说明
<pre>userSearchFilter: "(&amp;(objectClass=person)(sAMAccountName=%USERNAME%))"</pre> <p>要使用 userPrincipalName (用于登录的电子邮件地址)，您可以将 userSearchFilter 更改为：</p> <pre>"(&amp;(objectClass=person)(userPrincipalName=%USERNAME%))"</pre> <p>或者，要同时搜索 userPrincipalName 和 sAMAccountName，您可以使用以下 userSearchFilter：</p> <pre>"(&amp;(objectClass=person)(</pre>	<pre>( sAMAccountName=%USERNAME% ) ( userPrincipalName=%USERNAME% ) ) " ——</pre>
<p>利用 sAMAccountName 作为我们登录到 SolidFire 集群的用户名。这些设置会指示 LDAP 在 sAMAccountName 属性中搜索登录期间指定的用户名，并将搜索限制为在 objectClass 属性中使用 "person" 作为值的条目。</p>	searchBindDN
<p>这是将用于搜索 LDAP 目录的只读用户的可分辨名称。对于 Active Directory，通常最容易为用户使用 userPrincipalName (电子邮件地址格式)。</p>	searchBindPassword

要对此进行测试，请从 Element UI 中注销，然后以该组中的用户身份重新登录。

### 查看 LDAP 详细信息

在 "Cluster" 选项卡上的 "LDAP" 页面上查看 LDAP 信息。



要查看这些 LDAP 配置设置，必须启用 LDAP。

1. 要使用 Element UI 查看 LDAP 详细信息，请单击 \* 集群 \* > \* LDAP \*。
  - \* 主机名 /IP 地址 \*：LDAP 或 LDAPS 目录服务器的地址。
  - \* 身份验证类型 \*：用户身份验证方法。可能值：
    - 直接绑定
    - 搜索并绑定
  - \* 搜索绑定 DN\*：用于登录以对用户执行 LDAP 搜索的完全限定 DN (需要对 LDAP 目录具有绑定级别

访问权限)。

- \* 搜索绑定密码 \*：用于对 LDAP 服务器访问进行身份验证的密码。
- \* 用户搜索基础 DN\*：用于开始用户搜索的树的基础 DN。系统将从指定位置搜索子树。
- \* 用户搜索筛选器 \*：使用您的域名输入以下内容：

```
(&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERN  
AME%)))
```

- \* 组搜索类型 \*：用于控制使用的默认组搜索筛选器的搜索类型。可能值：
  - Active Directory：用户的所有 LDAP 组的嵌套成员资格。
  - 无组：无组支持。
  - Member DN：成员 DN 样式的组（单层）。
- \* 组搜索基础 DN\*：用于开始组搜索的树的基础 DN。系统将从指定位置搜索子树。
- \* 测试用户身份验证 \*：配置 LDAP 后，使用此选项测试 LDAP 服务器的用户名和密码身份验证。输入已存在的帐户以测试此问题。此时将显示可分辨名称和用户组信息，您可以复制这些信息以供日后创建集群管理员时使用。

## 测试 LDAP 配置

配置LDAP后、您应使用Element UI或Element API方法对其进行测试 TestLdapAuthentication。

### 步骤

1. 要使用 Element UI 测试 LDAP 配置，请执行以下操作：
  - a. 单击 \* 集群 \* > \* LDAP \*。
  - b. 单击 \* 测试 LDAP 身份验证 \*。
  - c. 使用下表中的信息解决任何问题：

错误消息	说明
xLDAPUserNotFound	<ul style="list-style-type: none"><li>• 在配置的子树中找不到要测试的用户 userSearchBaseDN。</li><li>• `userSearchFilter` 配置不正确。</li></ul>
xLDAPBindFailed (Error: Invalid credentials)	<ul style="list-style-type: none"><li>• 要测试的用户名是有效的 LDAP 用户，但提供的密码不正确。</li><li>• 要测试的用户名是有效的 LDAP 用户，但此帐户当前已禁用。</li></ul>
xLDAPSearchBindFailed (Error: Can't contact LDAP server)	LDAP 服务器 URI 不正确。

错误消息	说明
xLDAPSearchBindFailed (Error: Invalid credentials)	只读用户名或密码配置不正确。
xLDAPSearchFailed (Error: No such object)	`userSearchBaseDN`不是LDAP树中的有效位置。
xLDAPSearchFailed (Error: Referral)	<ul style="list-style-type: none"> <li>• `userSearchBaseDN`不是LDAP树中的有效位置。</li> <li>• `userSearchBaseDN`和`groupSearchBaseDN`位于嵌套OU中。这可能会引发发生原因权限问题。解决方法是在用户和组基础DN条目中包括OU (例如: `ou=storage, cn=company, cn=com`)</li> </ul>

2. 要使用 Element API 测试 LDAP 配置，请执行以下操作：

a. 调用 TestLdapAuthentication 方法。

```
{
  "method": "TestLdapAuthentication",
  "params": {
    "username": "admin1",
    "password": "admin1PASS"
  },
  "id": 1
}
```

b. 查看结果。如果 API 调用成功，结果将包括指定用户的可分辨名称以及用户所属的组列表。

```
{
  "id": 1
  "result": {
    "groups": [
      "CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
    ],
    "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
  }
}
```

## 禁用LDAP

您可以使用 Element UI 禁用 LDAP 集成。

开始之前，您应记下所有配置设置，因为禁用 LDAP 会擦除所有设置。

### 步骤

1. 单击 \* 集群 \* > \* LDAP \*。
2. 单击 \* 否 \*。
3. 单击 \* 禁用 LDAP\*。

### 了解更多信息

- ["SolidFire 和 Element 软件文档"](#)
- ["适用于 vCenter Server 的 NetApp Element 插件"](#)



## 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。