管理集群管理员用户帐户

Element Software

NetApp
January 15, 2024

目录

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
     - nodes
     - 驱动器
     - volumes
     - —帐户
     - clusterAdmins
     - 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。

  请参见 "《 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 LCAP 配置来检查集群是否配置了正确的值。
4. * 测试 LDAP 身份验证 * （使用 `readonly` 用户）。通过运行 TestLdapAuthentication API 方法或使用 Element UI 测试 LDAP 配置是否正确。在此初始测试中，请使用 `readonly` 用户的用户名 `sAMAccountName` 。这将验证您的集群是否已正确配置 LDAP 身份验证，并验证 `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 setp 4 。复制 `d`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

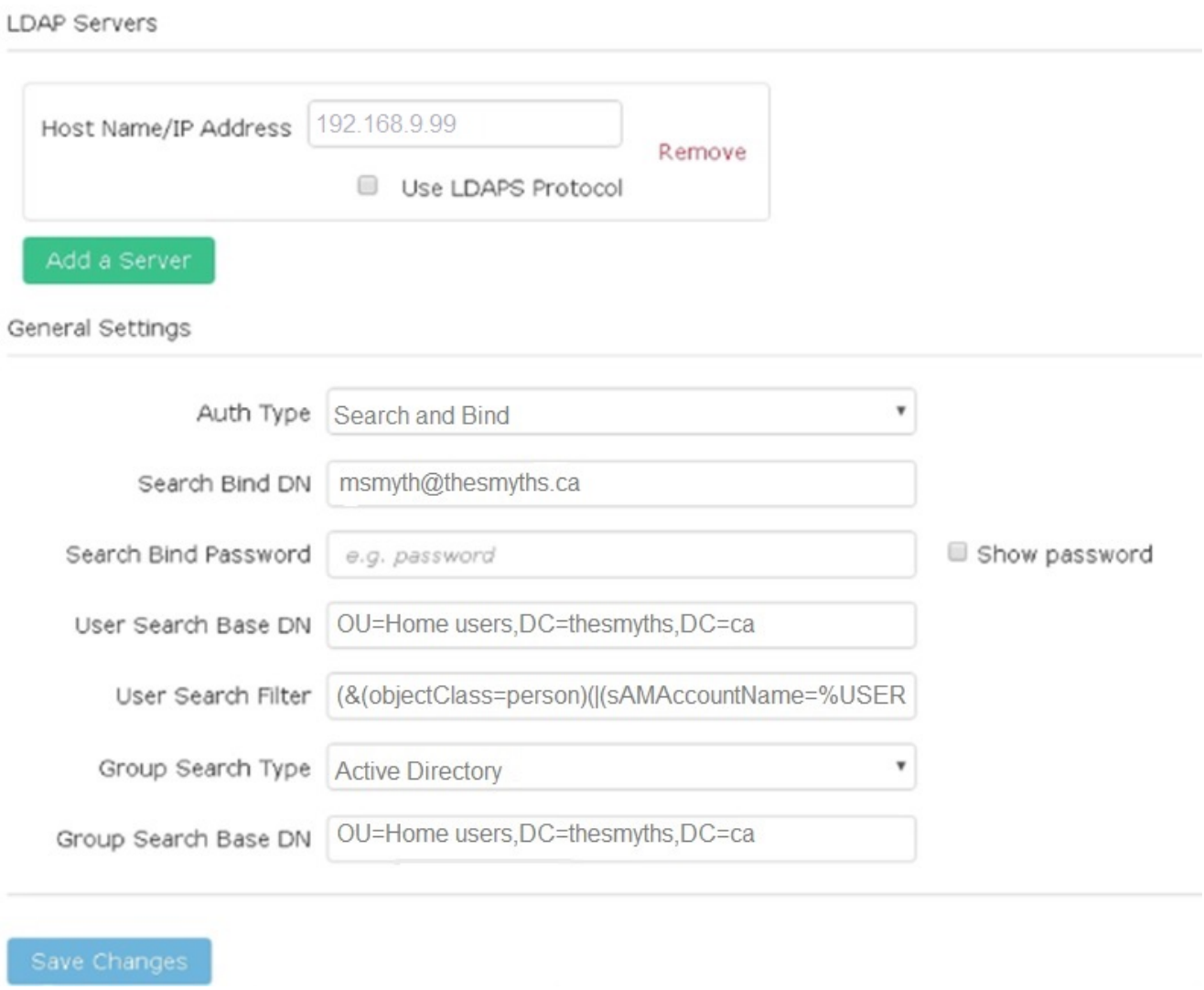
1. 单击 * 集群 * > * LDAP * 。
2. 单击 * 是 * 以启用 LDAP 身份验证。

3. 单击 * 添加服务器 * 。
4. 输入 * 主机名 /IP 地址 * 。

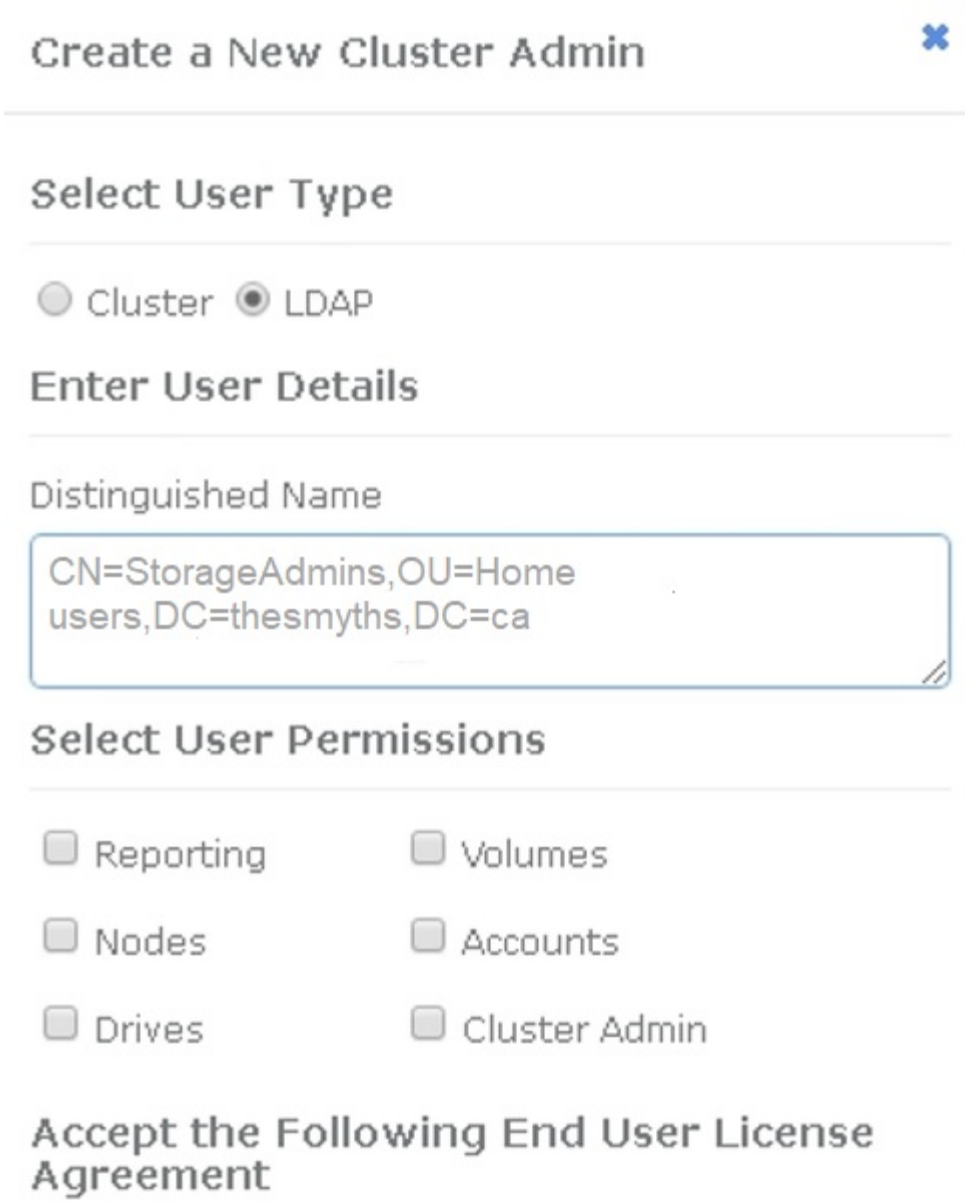
   也可以输入可选的自定义端口号。

   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。



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 * 。



b. 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。
c. 选择权限，通常为所有权限。
d. 向下滚动到最终用户许可协议，然后单击 * 我接受 * 。
e. 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 `EnableLdapAuthentication` API 方法在集群上启用 LDAP 身份验证。

步骤

1. 首先使用 `EnableLdapAuthentication` API 方法在集群上启用 LDAP 身份验证。
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	**Description**
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	Description

`userSearchFilter: “(&(objectClass=person)(sAMAccountName=%USERNAME%))”`
 	
要使用 userPrincipalName （用于登录的电子邮件地址），您可以将 userSearchFilter 更改为：
 	
`“(&(objectClass=person)(userPrincipalName=%USERNAME%))”`
 	
或者，要同时搜索 userPrincipalName 和 sAMAccountName ，您可以使用以下 userSearchFilter ：
 	
`“(&(objectClass=person)(`
	（ sAMAccountName=%USERNAME% ）（ userPrincipalName=%USERNAME% ））" ——

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。	searchBindDN
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）。	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=%USERNAME%））））`

- * 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 `TestLdapAuthentication` 方法对其进行测试。

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	Description
`xLDAPUserNotFound`	• 在已配置的 `userSearchBaseDN` 子树中未找到要测试的用户。 • `userSearchFilter` 配置不正确。
`xLDAPBindFailed (Error: Invalid credentials)`	• 要测试的用户名是有效的 LDAP 用户，但提供的密码不正确。 • 要测试的用户名是有效的 LDAP 用户，但此帐户当前已禁用。
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	LDAP 服务器 URI 不正确。

错误消息	Description
`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)`	• `userSearchBaseDN` 不是 LDAP 树中的有效位置。 • `userSearchBaseDN` 和 `groupSearchBaseDN` 位于嵌套的 OU 中。这可能会引发发生原因权限问题。临时解决策将在用户和组基本 DN 条目中包含 OU （例如：`ou=storage` ， `cn=company` ， `cn=com` ）

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"