管理您的帐户

Astra Control Center

NetApp
April 17, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/astra-control-center/use/manage-local-users-and-roles.html on April 17, 2024. Always check docs.netapp.com for the latest.

目录

管理您的帐户 1
管理本地用户和角色 1
管理远程身份验证 4
管理远程用户和组 6
查看和管理通知 8
添加和删除凭据 8
监控帐户活动 9
更新现有许可证 10

管理您的帐户

管理本地用户和角色

您可以使用Astra Control UI添加、删除和编辑Astra Control Center安装的用户。您可以使用 Astra Control UI 或 "Astra Control API" 以管理用户。

您还可以使用LDAP对选定用户执行身份验证。

使用 **LDAP**

LDAP是一种用于访问分布式目录信息的行业标准协议、也是企业身份验证的常见选择。您可以将Astra控制中心连接到LDAP服务器、以便对选定的Astra控制用户执行身份验证。从较高层面来看、该配置涉及将Astra与LDAP集成、并定义与LDAP定义对应的Astra Control用户和组。您可以使用Astra Control API或Web UI配置LDAP身份验证以及LDAP用户和组。有关详细信息、请参见以下文档：

- "使用Astra Control API管理远程身份验证和用户"
- "使用Astra Control UI管理远程用户和组"
- "使用Astra Control UI管理远程身份验证"

添加用户

帐户所有者和管理员可以向 Astra 控制中心安装添加更多用户。

步骤

1. 在 * 管理帐户 * 导航区域中，选择 * 帐户 * 。
2. 选择 * 用户 * 选项卡。
3. 选择 * 添加用户 * 。
4. 输入用户的名称，电子邮件地址和临时密码。

   用户需要在首次登录时更改密码。

5. 选择具有适当系统权限的用户角色。

   每个角色都提供以下权限：

   - * 查看器 * 可以查看资源。
   - " 成员 * " 具有 " 查看器 " 角色权限，可以管理应用程序和集群，取消管理应用程序以及删除快照和备份。
   - * 管理员 * 具有成员角色权限，可以添加和删除除所有者之外的任何其他用户。
   - * 所有者 * 具有管理员角色权限，可以添加和删除任何用户帐户。
6. 要为具有成员或查看器角色的用户添加约束，请启用 * 将角色限制为约束条件 * 复选框。

   有关添加约束的详细信息、请参见 "管理本地用户和角色"。

7. 选择 * 添加 * 。

管理密码

您可以在 Astra 控制中心管理用户帐户的密码。

更改密码

您可以随时更改用户帐户的密码。

步骤

1. 选择屏幕右上角的用户图标。
2. 选择 * 配置文件 * 。
3. 从选项菜单的 * 操作 * 列中选择 * 更改密码 * 。
4. 输入符合密码要求的密码。
5. 再次输入密码进行确认。
6. 选择 * 更改密码 * 。

重置其他用户的密码

如果您的帐户具有管理员或所有者角色权限，则可以重置其他用户帐户以及您自己的帐户的密码。重置密码时，您需要分配一个临时密码，用户必须在登录时更改此密码。

步骤

1. 在 * 管理帐户 * 导航区域中，选择 * 帐户 * 。
2. 选择 * 操作 * 下拉列表。
3. 选择 * 重置密码 * 。
4. 输入符合密码要求的临时密码。
5. 再次输入密码进行确认。

   用户下次登录时，系统将提示用户更改密码。

6. 选择 * 重置密码 * 。

删除用户

具有所有者或管理员角色的用户可以随时从帐户中删除其他用户。

步骤

1. 在 * 管理帐户 * 导航区域中，选择 * 帐户 * 。
2. 在 * 用户 * 选项卡中，选中要删除的每个用户所在行中的复选框。
3. 从选项菜单的 * 操作 * 列中，选择 * 删除用户 / 秒 * 。
4. 出现提示时，键入单词 "remove" 并选择 * 是，删除用户 * 以确认删除。

结果

Astra 控制中心从帐户中删除用户。

管理角色

您可以通过添加命名空间限制并将用户角色限制为这些限制来管理角色。这样，您就可以控制对组织内资源的访问。您可以使用 Astra Control UI 或 "Astra Control API" 以管理角色。

向角色添加命名空间限制

管理员或所有者用户可以向成员或查看器角色添加命名空间限制。

步骤

1. 在 * 管理帐户 * 导航区域中，选择 * 帐户 * 。
2. 选择 * 用户 * 选项卡。
3. 在 * 操作 * 列中，为具有成员或查看器角色的用户选择菜单按钮。
4. 选择 * 编辑角色 * 。
5. 启用 * 将角色限制为约束条件 * 复选框。

   此复选框仅适用于 " 成员 " 或 " 查看器 " 角色。您可以从 * 角色 * 下拉列表中选择其他角色。

6. 选择 * 添加约束 * 。

   您可以按命名空间或命名空间标签查看可用约束的列表。

7. 在 * 约束类型 * 下拉列表中，根据命名空间的配置方式选择 * Kubernetes 命名空间 * 或 * Kubernetes 命名空间标签 * 。
8. 从列表中选择一个或多个命名空间或标签，以构成一个限制，将角色限制为这些命名空间。
9. 选择 * 确认 * 。

   "* 编辑角色 * " 页面将显示您为此角色选择的约束列表。

10. 选择 * 确认 * 。

    在 * 帐户 * 页面上，您可以在 * 角色 * 列中查看任何成员或查看器角色的限制。

> 如果为某个角色启用了限制并选择了 * 确认 * 而未添加任何限制，则该角色将被视为具有完全限制（该角色将被拒绝访问分配给命名空间的任何资源）。

从角色中删除命名空间限制

管理员或所有者用户可以从角色中删除命名空间限制。

步骤

1. 在 * 管理帐户 * 导航区域中，选择 * 帐户 * 。
2. 选择 * 用户 * 选项卡。

3. 在 * 操作 * 列中，为具有成员或查看器角色且具有活动约束的用户选择菜单按钮。
4. 选择 * 编辑角色 * 。

   "* 编辑角色 " 对话框显示角色的活动约束。

5. 选择需要删除的约束右侧的 * X * 。
6. 选择 * 确认 * 。

有关详细信息 ...

- "用户角色和命名空间"

管理远程身份验证

LDAP是一种用于访问分布式目录信息的行业标准协议、也是企业身份验证的常见选择。您可以将Astra控制中心连接到LDAP服务器、以便对选定的Astra控制用户执行身份验证。

从较高层面来看、该配置涉及将Astra与LDAP集成、并定义与LDAP定义对应的Astra Control用户和组。您可以使用Astra Control API或Web UI配置LDAP身份验证以及LDAP用户和组。

> Astra Control Center使用用户登录属性(在启用远程身份验证时配置)来搜索和跟踪远程用户。对于您希望在Astra Control Center中显示的任何远程用户、此字段中必须存在电子邮件地址("mail")或用户主体名称("userPrincipalName")的属性。此属性在Astra Control Center中用作用户名以进行身份验证，并在搜索远程用户时使用。

添加用于**LDAPS**身份验证的证书

为LDAP服务器添加专用TLS证书、以便在使用LDAPS连接时、Astra控制中心可以向LDAP服务器进行身份验证。您只需要执行一次此操作、或者在安装的证书过期时执行此操作。

步骤

1. 转到*帐户*。
2. 选择*证书*选项卡。
3. 选择 * 添加 * 。
4. 上传 `.pem` 将文件内容归档或粘贴到剪贴板中。
5. 选中*可信*复选框。
6. 选择*添加证书*。

启用远程身份验证

您可以启用LDAP身份验证并配置Astra Control与远程LDAP服务器之间的连接。

开始之前

如果您计划使用LDAPS、请确保将LDAP服务器的专用TLS证书安装在Astra控制中心中、以便Astra控制中心能够向LDAP服务器进行身份验证。请参见 添加用于LDAPS身份验证的证书 有关说明，请参见。

步骤

1. 转至*帐户>连接*。
2. 在*远程身份验证*窗格中、选择配置菜单。
3. 选择 * 连接 * 。
4. 输入服务器IP地址、端口和首选连接协议(LDAP或LDAPS)。

   作为最佳实践、请在与LDAP服务器连接时使用LDAPS。在连接到LDAPS之前、您需要在Astra控制中心安装LDAP服务器的专用TLS证书。

5. 以电子邮件格式输入服务帐户凭据(administrator@example.com)。在与LDAP服务器连接时、Astra Control将使用这些凭据。
6. 在*用户匹配*部分，执行以下操作：
   a. 输入基本DN和相应的用户搜索筛选器、以便从LDAP服务器检索用户信息时使用。
   b. (可选)如果目录使用用户登录属性 `userPrincipalName` 而不是 `mail`、输入 `userPrincipalName` 在“用户登录属性”字段的正确属性中。
7. 在*组匹配*部分中、输入组搜索基础DN和相应的自定义组搜索筛选器。

   请务必对*用户匹配*和*组匹配*使用正确的基本可分辨名称(DN)和适当的搜索筛选器。基础DN用于指示Astra Control在目录树的哪个级别开始搜索、而搜索筛选器用于限制目录树Astra Control搜索的各个部分。

8. 选择 * 提交 * 。

结果

与LDAP服务器建立连接后、远程身份验证*窗格状态将移至*待定、然后移至*已连接*。

禁用远程身份验证

您可以暂时禁用与LDAP服务器的活动连接。

禁用与LDAP服务器的连接时、将保存所有设置、并保留从该LDAP服务器添加到Astra Control中的所有远程用户和组。您可以随时重新连接到此LDAP服务器。

步骤

1. 转至*帐户>连接*。
2. 在*远程身份验证*窗格中、选择配置菜单。
3. 选择 * 禁用 * 。

结果

"远程身份验证"窗格状态将移至"*已禁用"。所有远程身份验证设置、远程用户和远程组都会保留下来、您可以随时重新启用连接。

编辑远程身份验证设置

如果禁用了与LDAP服务器的连接或*远程身份验证*窗格处于"连接错误"状态、则可以编辑配置设置。

如果*远程身份验证*窗格处于"已禁用"状态、则无法编辑LDAP服务器URL或IP地址。您需要 [断开远程身份验证] 第一个。

步骤

1. 转至*帐户>连接*。
2. 在*远程身份验证*窗格中、选择配置菜单。
3. 选择 * 编辑 * 。
4. 进行必要的更改、然后选择*编辑*。

断开远程身份验证

您可以从LDAP服务器断开连接、并从Astra Control中删除配置设置。

如果您是LDAP用户并断开连接、则会话将立即结束断开与LDAP服务器的连接后、该LDAP服务器的所有配置设置以及从该LDAP服务器添加的任何远程用户和组都会从Astra Control中删除。

步骤

1. 转至*帐户>连接*。
2. 在*远程身份验证*窗格中、选择配置菜单。
3. 选择*断开连接*。

结果

"远程身份验证"窗格状态将移至"*已断开连接"。远程身份验证设置、远程用户和远程组将从Astra Control中删除。

管理远程用户和组

如果您已在Astra Control系统上启用LDAP身份验证、则可以搜索LDAP用户和组、并将其包含在系统的已批准用户中。

添加远程用户

帐户所有者和管理员可以向Astra Control添加远程用户。Astra Control Center支持多达10、000个LDAP远程用户。

Astra Control Center使用用户登录属性(在启用远程身份验证时配置)来搜索和跟踪远程用户。对于您希望在Astra Control Center中显示的任何远程用户、此字段中必须存在电子邮件地址("mail")或用户主体名称("userPrincipalName")的属性。此属性在Astra Control Center中用作用户名以进行身份验证，并在搜索远程用户时使用。

如果系统中已存在具有相同电子邮件地址(基于"mail"或"user主体名称"属性)的本地用户、则无法添加远程用户。要将此用户添加为远程用户、请先从系统中删除此本地用户。

步骤

1. 转到*帐户*区域。
2. 选择*用户和组*选项卡。
3. 在页面最右侧、选择*远程用户*。
4. 选择 * 添加 * 。
5. 或者、也可以通过在*按电子邮件筛选*字段中输入用户的电子邮件地址来搜索LDAP用户。
6. 从列表中选择一个或多个用户。
7. 为用户分配角色。

   如果您为用户和用户组分配不同的角色、则优先使用较为宽松的角色。

8. (可选)为此用户分配一个或多个命名空间约束、然后选择*将角色限制为约束条件*以强制实施这些限制。您可以通过选择*添加约束*来添加新的命名空间约束。

   如果通过LDAP组成员资格为用户分配了多个角色、则只有最宽松角色中的限制才会生效。例如、如果具有本地查看器角色的用户加入了绑定到成员角色的三个组、则成员角色的约束之和将生效、而查看器角色的任何约束将被忽略。

9. 选择 * 添加 * 。

结果

新用户将显示在远程用户列表中。在此列表中、您可以查看用户的活动约束、并从*操作*菜单管理用户。

添加远程组

要一次性添加多个远程用户、帐户所有者和管理员可以向Astra Control添加远程组。添加远程组时、该组中的所有远程用户均可登录到Astra Control、并继承与该组相同的角色。

Astra Control Center最多支持5、000个LDAP远程组。

步骤

1. 转到*帐户*区域。
2. 选择*用户和组*选项卡。
3. 在页面最右侧、选择*远程组*。
4. 选择 * 添加 * 。

   在此窗口中、您可以看到Astra Control从目录中检索到的LDAP组的公用名和可分辨名称列表。

5. 或者、也可以在*按公用名筛选*字段中输入组的公用名来搜索LDAP组。
6. 从列表中选择一个或多个组。
7. 为组分配角色。

您选择的角色将分配给此组中的所有用户。如果您为用户和用户组分配不同的角色、则优先使用较为宽松的角色。

8. (可选)为此组分配一个或多个命名空间约束、然后选择*将角色限制为约束条件*以强制实施这些限制。您可以通过选择*添加约束*来添加新的命名空间约束。

   - 如果要访问的资源属于安装了最新**Astra Connector**的集群：通过LDAP组成员资格为用户分配多个角色时，这些角色的约束条件将合并在一起。例如、如果具有本地查看器角色的用户加入绑定到成员角色的三个组、则该用户现在可以以查看器角色访问原始资源、并以成员角色访问通过组成员资格获得的资源。
   - 如果要访问的资源属于未安装**Astra Connector**的集群：通过LDAP组成员资格为用户分配多个角色时，只有最宽松角色的限制才会生效。

9. 选择 * 添加 * 。

结果

新组将显示在远程组列表中。此组中的远程用户不会显示在远程用户列表中、直到每个远程用户都登录为止。在此列表中、您可以查看有关该组的详细信息、并从*操作*菜单管理该组。

查看和管理通知

操作完成或失败时， Astra 会向您发出通知。例如，如果应用程序的备份成功完成，您将看到通知。

您可以从界面右上角管理这些通知：

步骤

1. 选择右上角的未读通知数量。
2. 查看通知，然后选择 * 标记为已读 * 或 * 显示所有通知 * 。

   如果选择 * 显示所有通知 * ，则会加载通知页面。

3. 在 * 通知 * 页面上，查看通知，选择要标记为已读的通知，选择 * 操作 * 并选择 * 标记为已读 * 。

添加和删除凭据

随时从您的帐户中添加和删除本地私有云提供商的凭据，例如 ONTAP S3 ，使用 OpenShift 管理的 Kubernetes 集群或非受管 Kubernetes 集群。Astra 控制中心使用这些凭据来发现 Kubernetes 集群和集群上的应用程序，并代表您配置资源。

请注意， Astra 控制中心中的所有用户都共享相同的凭据集。

添加凭据

您可以在管理集群时向 Astra 控制中心添加凭据。要通过添加新集群来添加凭据、请参见 "添加 Kubernetes 集群"。

> 如果创建自己的kubeconfig,则只能在其中定义*on*上下文元素。请参见 "Kubernetes 文档" 有关创建kubeconfig.文件的信息、请参见。

删除凭据

随时从帐户中删除凭据。您只能在之后删除凭据 "取消管理所有关联集群"。

> 您添加到 Astra 控制中心的第一组凭据始终在使用中，因为 Astra 控制中心使用这些凭据向备份存储分段进行身份验证。最好不要删除这些凭据。

步骤

1. 选择 * 帐户 * 。
2. 选择 * 凭据 * 选项卡。
3. 在 * 状态 * 列中选择要删除的凭据的选项菜单。
4. 选择 * 删除 * 。
5. 键入单词 "remove" 确认删除，然后选择 * 是，删除凭据 * 。

结果

Astra 控制中心将从帐户中删除凭据。

监控帐户活动

您可以在 Astra Control 帐户中查看有关活动的详细信息。例如，邀请新用户时，添加集群时或创建快照时。您还可以将帐户活动导出到 CSV 文件。

在 **Astra Control** 中查看所有帐户活动

1. 选择 * 活动 * 。
2. 使用筛选器缩小活动列表的范围，或者使用搜索框准确查找所需内容。
3. 选择 * 导出到 CSV* 将您的帐户活动下载到 CSV 文件。

查看特定应用程序的帐户活动

1. 选择 * 应用程序 * ，然后选择应用程序的名称。
2. 选择 * 活动 * 。

查看集群的帐户活动

1. 选择 * 集群 * ，然后选择集群的名称。
2. 选择 * 活动 * 。

采取措施解决需要关注的事件

1. 选择 * 活动 * 。
2. 选择需要关注的事件。
3. 选择 * 执行操作 * 下拉选项。

   从此列表中，您可以查看可能采取的更正操作，查看与问题描述 相关的文档，并获得支持以帮助解决问题描述 。

更新现有许可证

您可以将评估版许可证转换为完整许可证，也可以使用新许可证更新现有评估版许可证或完整许可证。如果您没有完整的许可证，请与 NetApp 销售联系人联系以获取完整的许可证和序列号。您可以使用Astra控制中心UI或 "Astra Control API" 更新现有许可证。

步骤

1. 登录到 "NetApp 支持站点"。
2. 访问 Astra 控制中心下载页面，输入序列号，然后下载完整的 NetApp 许可证文件（ NLF ）。
3. 登录到 Astra 控制中心 UI 。
4. 从左侧导航栏中，选择 * 帐户 * > * 许可证 * 。
5. 在 * 帐户 * > * 许可证 * 页面中，选择现有许可证的状态下拉菜单，然后选择 * 替换 * 。
6. 浏览到您下载的许可证文件。
7. 选择 * 添加 * 。
   - 帐户 * > * 许可证 * 页面显示许可证信息，到期日期，许可证序列号，帐户 ID 和使用的 CPU 单元。

有关详细信息 ...

- "Astra 控制中心许可"

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。