



使用**NetApp Console**

NetApp Console setup and administration

NetApp

January 23, 2026

This PDF was generated from <https://docs.netapp.com/zh-cn/console-setup-admin/task-logging-in.html> on January 23, 2026. Always check docs.netapp.com for the latest.

目录

使用NetApp Console	1
登录NetApp Console	1
使用多个控制台代理	2
在控制台代理之间切换	3
查看NetApp Console主页上的指标	3
所需的NetApp Console角色	4
启用指标以显示在主页上	6
查看整体存储容量	6
查看ONTAP警报	6
查看存储性能容量	7
查看您拥有的许可证和订阅	8
查看勒索软件抵御能力状态	8
查看备份和恢复状态	8
管理您的NetApp Console用户设置	9
更改您的显示名称	9
提升您在只读模式下的角色	9
配置多重身份验证	9
重新生成您的 MFA 恢复代码	10
删除您的 MFA 配置	10
联系您的组织管理员	11
配置暗黑模式（暗黑主题）	11

使用NetApp Console

登录NetApp Console

如何登录NetApp Console取决于您使用的部署模式。

24 小时后或关闭浏览器后，您将自动退出。

["了解控制台部署模式"](#)。

标准模式

注册NetApp Console后，您可以从基于 Web 的控制台登录，开始管理您的数据和存储基础架构。

关于此任务

您可以使用以下选项之一登录NetApp Console：

- 您现有的NetApp支持站点 (NSS) 凭证
- 使用您的电子邮件地址和密码的NetApp Console帐户
- 联合连接

您可以使用单点登录，使用公司目录（联合身份）中的凭据登录。["了解如何设置身份联合"](#)。

步骤

1. 打开 Web 浏览器并转到 ["NetApp Console"](#)
2. 在*登录*页面上，输入与您的登录关联的电子邮件地址。
3. 根据与您的登录相关的身份验证方法，系统将提示您输入您的凭据：
 - NetApp云凭证：输入您的密码
 - 联合用户：输入您的联合身份凭证
 - NetApp支持站点帐户：输入您的NetApp支持站点凭据

结果

您现在已登录并可以开始使用它来管理您的混合多云基础设施。

限制模式

在受限模式下使用控制台时，您需要从代理上本地运行的用户界面登录到控制台。

关于此任务

在受限模式下，控制台支持使用以下选项之一登录：

- 使用您的电子邮件地址和密码登录NetApp Console
- 联合连接

您可以使用单点登录，使用公司目录（联合身份）中的凭据登录。["了解如何使用身份联合"](#)。

步骤

1. 打开 Web 浏览器并输入安装代理的 IP 地址。
2. 输入您的用户名和密码登录。

使用多个控制台代理

如果您使用多个控制台代理，则可以直接从控制台在这些控制台代理之间切换以查看相关系统。

在控制台代理之间切换

如果您有多个控制台代理，您可以在它们之间切换以查看与特定代理关联的系统。

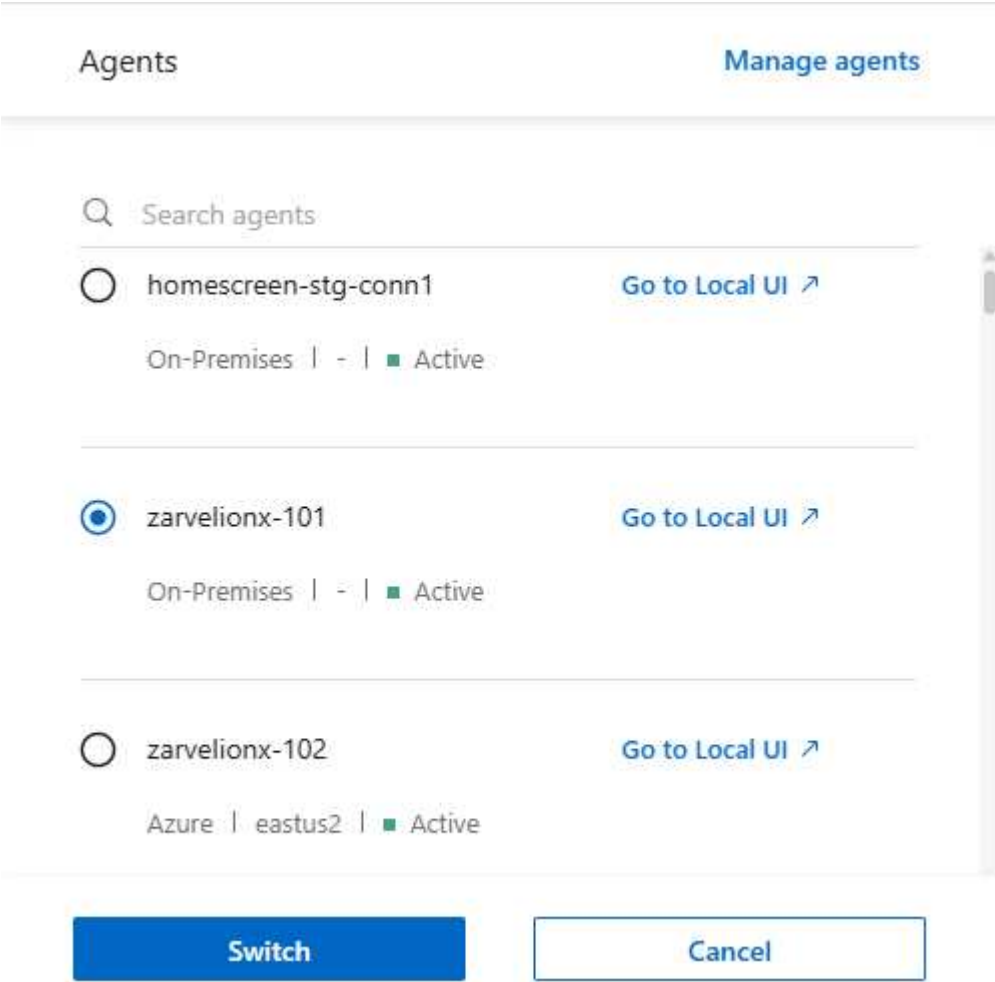
例如，在多云环境中，您可能在 AWS 中有一个代理，在 Google Cloud 中有一个代理。在这些代理之间切换以管理各自云环境中的Cloud Volumes ONTAP系统。



从代理的本地 UI 查看NetApp Console时，此选项不可用

步骤

1. 选择控制台代理图标 () 查看可用代理的列表。



结果

控制台刷新并显示与所选代理关联的系统。

查看NetApp Console主页上的指标

监控存储资产的健康状况可确保您了解存储保护问题并采取措施解决这些问题。使用NetApp Console主页，查看NetApp Backup and Recovery的备份和恢复状态，以及面临勒索软件攻击风险或受到NetApp Ransomware Resilience保护的工作负载数量。您可以

查看单个集群和Cloud Volumes ONTAP的存储容量、ONTAP警报、每个集群或Cloud Volumes ONTAP系统的存储性能容量、您拥有的不同类型的许可证等等。

主页上的所有窗格均显示组织级别的数据。存储容量和存储性能窗格显示用户可以根据 IAM 权限访问的与项目相关的系统。

系统每五分钟刷新一次主页上的数据。缓存可能会导致此页面上的数据与实际值相差长达 15 分钟。



主页上的准确指标需要适当大小和配置的控制台代理。

所需的NetApp Console角色

主页中的每个窗格都需要不同的用户角色：

- 存储容量窗格：能够查看NetApp Console系统页面
- * ONTAP警报窗格*：文件夹或项目管理员、运营支持分析师、组织管理员、组织查看者、超级管理员、超级查看者
- 存储性能容量窗格：能够查看NetApp Console系统页面
- **Licenses and subscriptions**窗格：文件夹或项目管理员、组织管理员、组织查看者、超级管理员、超级查看者
- 勒索软件恢复力窗格：文件夹或项目管理员、组织管理员、勒索软件恢复力管理员、勒索软件恢复力查看器、超级管理员、超级查看器
- 备份和恢复窗格：备份和恢复备份管理员、备份和恢复超级管理员、备份和恢复备份查看器、备份和恢复克隆管理员、文件夹或项目管理员、组织管理员、备份和恢复恢复管理员、超级管理员、超级查看器

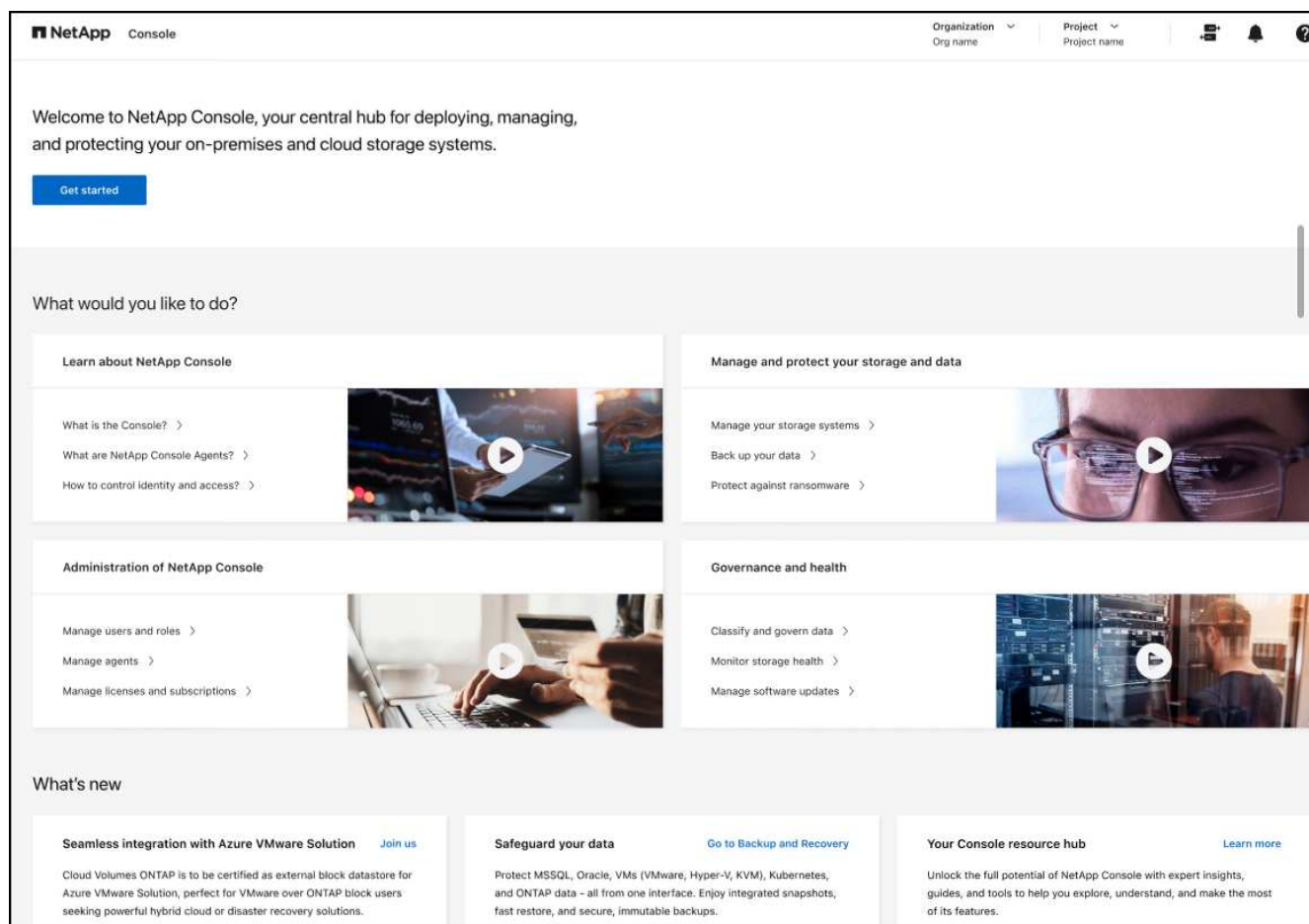
如果您没有访问窗格的权限，该窗格会显示一条消息，表明您没有使用该窗格的权限。

["了解NetApp Console访问角色。"](#)。

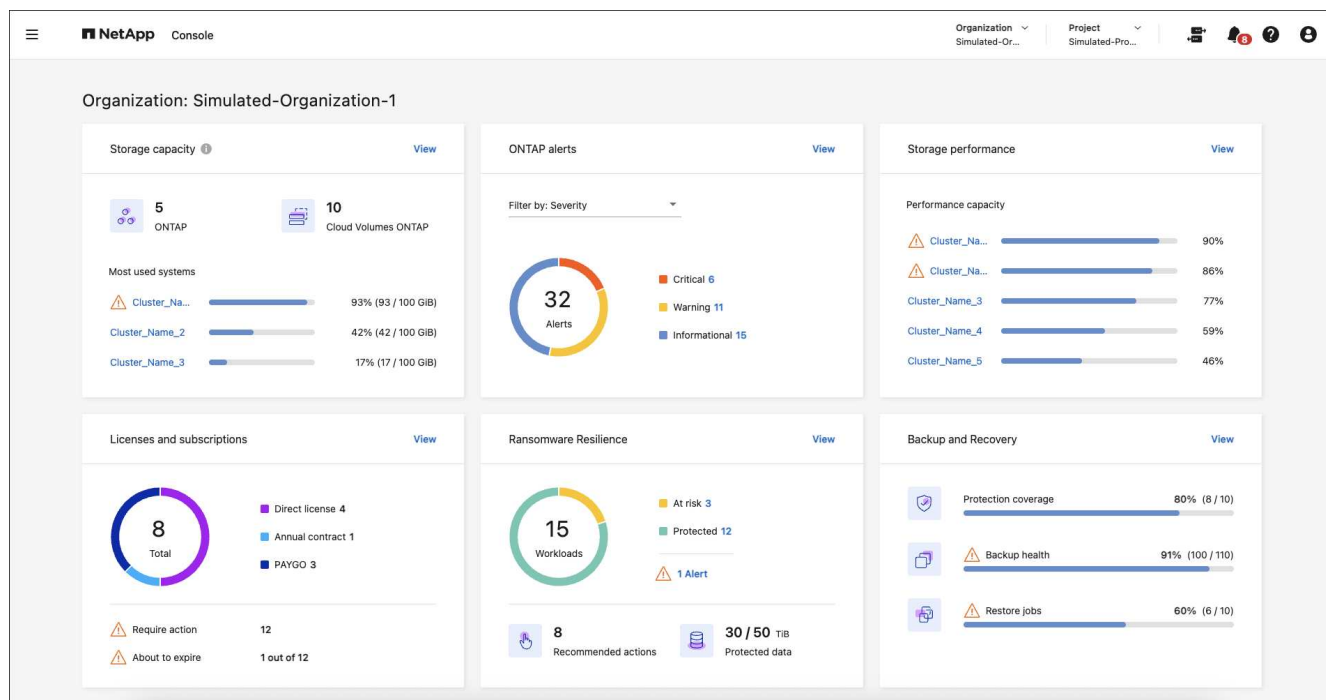
步骤

1. 从NetApp Console菜单中，选择 主页。

如果您具有组织管理员角色并且未设置代理或存储系统，则主页将显示入门信息。



如果您已设置NetApp Console，至少启用了—个控制台代理，并且在该代理上添加了至少一个集群或Cloud Volumes ONTAP系统，则主页将显示有关您的存储环境的指标。



启用指标以显示在主页上

当满足以下条件时，您可以在主页上看到指标：

- 您已登录到NetApp Console的 SaaS 实例。
- 您属于具有现有存储资源（代理和集群或Cloud Volumes ONTAP系统）的组织。
- 至少启用了—个控制台代理。
- 该代理上至少添加了一个集群或Cloud Volumes ONTAP系统。

要使指标显示在主页上，请完成以下任务：

- 启用至少一个控制台代理。
- 使用该代理添加至少一个集群或一个Cloud Volumes ONTAP 。

查看整体存储容量

存储容量窗格提供跨ONTAP集群和Cloud Volumes ONTAP系统的以下信息：

- 控制台发现的ONTAP系统数量
- 控制台发现的Cloud Volumes ONTAP系统数量
- 每个集群的容量使用情况

集群或Cloud Volumes ONTAP系统的顺序基于所使用的容量。容量最高的集群或系统会首先出现，以便于识别。

警告指示器显示集群容量为 80%，数据每五分钟更新一次。



如果您有多个项目，您可能在“存储容量”窗格中看到与“系统”页面不同的数据。这是因为“系统”页面显示基于项目级别的信息，而“存储容量”窗格显示组织级别的信息。此外，此窗格上的数据可能与实际值最多相差 15 分钟，因为数据会在此期间被缓存以优化性能。

步骤

1. 从NetApp Console菜单中，查看存储容量窗格。
2. 在存储容量窗格中，选择“查看”转到“控制台系统”页面。
3. 在系统页面上，选择包含要查看的集群的项目。
4. 在系统页面上，选择一个集群以查看有关该集群的更多详细信息。

查看ONTAP警报

查看NetApp本地ONTAP环境中的问题或潜在风险。您可以看到一些非 EMS 警报和一些 EMS 警报。

数据每 5 分钟更新一次。

您可以看到具有以下严重程度的ONTAP警报：

- 批判的

- 警告
- 信息

您可以看到针对以下影响区域的ONTAP警报：

- 容量
- 性能
- 保护
- 可用性
- 安全性



缓存可优化性能，但可能会导致此窗格上的数据与实际值相差长达 15 分钟。

支持的系统

- 支持本地ONTAP NAS 或 SAN 系统。
- 不支持Cloud Volumes ONTAP系统。

支持的数据源

查看有关ONTAP中发生的某些事件的警报。它们是 EMS 和基于指标的警报的组合。

有关ONTAP警报的详细信息，请参阅 ["关于ONTAP警报"](#)。

有关您可能会看到的警报列表，请参阅 ["查看ONTAP存储中的潜在风险"](#)。

步骤

1. 从NetApp Console菜单中，查看ONTAP警报窗格。
2. 或者，通过选择严重性级别来过滤警报，或者更改过滤器以根据影响区域显示警报。
3. 在ONTAP警报窗格中，选择“查看”以转到“控制台警报”页面。

查看存储性能容量

检查每个集群或Cloud Volumes ONTAP系统使用的存储性能容量，以确定性能容量、延迟和 IOPS 如何影响您的工作负载。例如，您可能会发现需要转移工作负载以最大限度地减少延迟并最大限度地提高关键工作负载的 IOPS 和吞吐量。

系统按性能容量排列集群和系统，首先列出最高容量，以便于识别。



缓存可优化性能，但可能会导致此窗格上的数据与实际值相差长达 15 分钟。

步骤

1. 从NetApp Console菜单中，查看存储性能窗格。
2. 在存储性能窗格中，选择“查看”转到“性能”页面，该页面列出了所有集群和Cloud Volumes ONTAP系统的性能容量、IOPS 和延迟数据。

3. 选择一个集群以在系统管理器中查看其详细信息。

查看您拥有的许可证和订阅

查看Licenses and subscriptions窗格中的以下信息：

- 您拥有的许可证和订阅的总数。
- 您拥有的每种许可证和订阅的数量（直接许可证、年度合同或 PAYGO）。
- 处于活动状态、需要操作或即将到期的许可证和订阅的数量。
- 系统会在需要采取行动或即将到期的许可证类型旁边显示指示符。

数据每 5 分钟刷新一次。



缓存可优化性能，但可能会导致此窗格上的数据与实际值相差长达 15 分钟。

步骤

1. 从NetApp Console菜单中，查看Licenses and subscriptions窗格。
2. 在Licenses and subscriptions窗格中，选择“查看”以转到控制台Licenses and subscriptions页面。

查看勒索软件抵御能力状态

了解工作负载是否面临勒索软件攻击的风险或是否受到NetApp Ransomware Resilience数据服务的保护。您可以查看受保护的数据总量、查看建议的操作数量以及查看与勒索软件防护相关的警报数量。

数据每 5 分钟刷新一次，并与NetApp Ransomware Resilience仪表板中显示的数据相匹配。

["了解NetApp Ransomware Resilience"](#)。

步骤

1. 从NetApp Console菜单中，查看“勒索软件恢复力”窗格。
2. 在“勒索软件恢复”窗格中执行以下操作之一：
 - 选择“查看”转到NetApp Ransomware Resilience仪表板。有关详细信息，请参阅 ["使用NetApp Ransomware Resilience仪表板监控工作负载健康状况"](#)。
 - 查看NetApp Ransomware Resilience仪表板中的“推荐操作”。有关详细信息，请参阅 ["查看NetApp Ransomware Resilience仪表板上的保护建议"](#)。
 - 选择警报链接以查看NetApp Ransomware Resilience警报页面中的警报。有关详细信息，请参阅 ["使用NetApp Ransomware Resilience处理检测到的勒索软件警报"](#)。

查看备份和恢复状态

查看NetApp Backup and Recovery的备份和恢复的总体状态。您可以看到受保护和不受保护的资源的数量。您还可以查看备份和恢复操作的百分比，以保护您的工作负载。百分比越高，表示数据保护越好。

数据每 5 分钟刷新一次。



缓存可优化性能，但可能会导致此窗格上的数据与实际值相差长达 15 分钟。

步骤

1. 从NetApp Console菜单中，查看“备份和恢复”窗格。
2. 选择“查看”转到NetApp Backup and Recovery仪表板。有关详细信息，请参阅 ["NetApp Backup and Recovery文档"](#)。

管理您的NetApp Console用户设置

您可以修改您的控制台配置文件，包括更改您的密码、启用多重身份验证 (MFA) 以及查看您的控制台管理员是谁。

在控制台中，每个用户都有一个配置文件，其中包含有关用户及其设置的信息。您可以查看和编辑您的个人资料设置。

更改您的显示名称

您可以更改控制台显示名称，以便其他用户识别您的身份。您无法更改用户名或电子邮件地址。

步骤

1. 选择控制台右上角的配置文件图标以查看用户设置面板。
2. 选择您姓名旁边的“编辑”图标。
3. 在“名称”字段中输入您的新显示名称。

提升您在只读模式下的角色

在某些情况下，您的组织管理员可能会将您的组织设置为只读模式。如果您拥有管理员角色，则必须提升权限才能进行更改。这样可以确保变更都是有意为之且获得授权的。

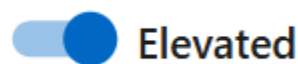
提升角色后，您可以在控制台进行更改，直到当前会话过期。

完成后，要么退出控制台，要么将滑块移回只读模式。会话过期后，系统将撤销您的高级权限。

步骤

1. 选择控制台右上角的配置文件图标以查看用户设置面板。
2. 要进入*只读模式*，请将滑块移动到*提升*位置并确认更改。

Read-Only mode status



配置多重身份验证

配置多重身份验证 (MFA)，通过要求第二种验证方法来提高安全性。

使用外部身份提供商或NetApp支持站点进行单点登录的用户无法启用 MFA。如果以上两种情况中的任何一种适

用于您，您将在个人资料设置中看不到启用 MFA 的选项。

如果您的用户帐户用于 API 访问，请不要启用 MFA。当为用户帐户启用多因素身份验证时，它会停止 API 访问。使用服务帐户进行所有 API 访问。

开始之前

- 您必须已将身份验证应用程序（例如 Google Authenticator 或 Microsoft Authenticator）下载到您的设备。
- 您需要密码来设置 MFA。



如果您无法访问身份验证应用程序或丢失恢复代码，请联系控制台管理员寻求帮助。

步骤

1. 选择控制台右上角的配置文件图标以查看用户设置面板。
2. 选择“多重身份验证”标题旁边的“配置”。
3. 按照提示为您的帐户设置 MFA。
4. 完成后，系统将提示您保存恢复代码。选择复制代码或下载包含代码的文本文件。请将此代码保存在安全的地方。如果您无法访问身份验证应用程序，则需要恢复代码。

设置 MFA 后，控制台会在您每次登录时提示您输入来自身份验证应用程序的一次性代码。

重新生成您的 MFA 恢复代码

您只能使用一次恢复代码。如果您使用或丢失了您的，请创建一个新的。

步骤

1. 选择控制台右上角的配置文件图标以查看用户设置面板。
2. 选择 ... 在“多重身份验证”标题旁边。
3. 选择*重新生成恢复代码*。
4. 复制生成的恢复代码并将其保存在安全的位置。

删除您的 MFA 配置

完成后，要么退出控制台，要么将滑块移回只读模式。会话过期后，系统将撤销您的高级权限。



如果您无法访问您的身份验证应用程序或恢复代码，您将需要联系您的组织管理员来重置您的 MFA 配置。

步骤

1. 选择控制台右上角的配置文件图标以查看用户设置面板。
2. 选择 ... 在“多重身份验证”标题旁边。
3. 选择*删除*。

联系您的组织管理员

如果您需要联系您的组织管理员，您可以直接从控制台向他们发送电子邮件。管理员管理组织内的用户帐户和权限。



您必须为浏览器配置默认电子邮件应用程序才能使用“联系管理员”功能。

步骤

1. 选择控制台右上角的配置文件图标以查看用户设置面板。
2. 选择“联系管理员”向您的组织管理员发送电子邮件。
3. 选择要使用的电子邮件应用程序。
4. 完成电子邮件并选择*发送*。

配置暗黑模式（暗黑主题）

您可以将控制台设置为以暗模式显示。

步骤

1. 选择控制台右上角的配置文件图标以查看用户设置面板。
2. 移动*黑暗主题*滑块以启用它。

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。