



配置 **Console** 集成和服务

NetApp Console local deployment

NetApp
August 10, 2026

目录

- 配置 Console 集成和服务 1
 - 将 NetApp Console 本地部署与 Active Directory 集成 1
 - 开始之前 1
 - 禁用或启用 Active Directory 集成 2
 - 删除 Active Directory 集成 2
 - 连接您的 LLM 并在 NetApp Console 本地部署中启用 NetApp Console 助手 2
 - 在连接 LLM 之前，请先收集所需信息 3
 - 将 LLM 连接到 NetApp Console 本地部署 3
 - 验证 LLM 集成是否有效 4
 - 保护凭据并监控 LLM 使用情况 4
 - 排除 NetApp Console 本地部署中的 LLM 集成故障 4
 - 快速分类 LLM 集成问题 4
 - 按症状排查故障 5
 - 应对 LLM 凭据泄露或滥用 5
 - 在 NetApp Console 本地部署中设置通知传递渠道 5
 - 配置电子邮件服务器 5
 - 配置 Webhook 7

配置 Console 集成和服务

将 NetApp Console 本地部署与 Active Directory 集成

将 NetApp Console 本地部署与 Active Directory 集成，以进行目录支持的登录和用户查找。使用目录服务对用户进行身份验证，然后在 NetApp Console 本地部署中将访问权限分配给这些用户。

必需的访问角色

超级管理员或组织管理员。["了解访问角色"](#)。

与 Active Directory 集成时，Console 本地部署将通过现有目录对用户进行身份验证。添加目录用户后，分配 Console 访问角色以控制该用户可以访问的内容。

Active Directory 集成还可以通过将现有控件、审计跟踪和策略应用于 Console 本地部署访问，帮助您满足合规性要求。



- Active Directory 集成不会创建联合组，不会同步目录组分配，也不会自动授予访问权限。管理员仍会将目录用户添加到组织并在 Console 本地部署中分配角色。
- 一次仅支持一个 Active Directory 集成。配置集成后，添加集成 按钮将被禁用。要切换到其他目录，请先禁用或删除现有集成。
- 目录用户不配置或使用多重身份验证 (MFA)。Console 本地部署仅为本地用户支持 MFA。["了解如何管理成员安全设置"](#)。

开始之前

在与 Active Directory 集成之前，请确认您已：

- 可以查询目录的Active Directory域和凭据
- LDAP 服务器地址和目录树的基本可分辨名称 (DN)
- 从 Console 本地部署到 LDAP 服务器的端口 389 (LDAP) 或 636 (LDAPS) 的网络访问
- SSL/TLS 证书（如果您计划使用 LDAPS）

步骤

1. 选择 **Administration > Identity and access**。
2. 选择*目录服务*以打开联盟页面。
3. 选择*添加集成*。
4. 输入 Active Directory 服务器的连接详细信息：
 - 集成的描述性名称。
 - **LDAP 主机**：您的 LDAP 服务器的主机名或 IP 地址。对于多台服务器，请输入主服务器。
 - 端口：LDAP 为 389，LDAPS 为 636。
 - *连接超时*以毫秒为单位。默认值为 1000 毫秒。

5. 选择 **Use SSL/TLS** 以使用 LDAPS。确认您的 LDAP 服务器支持 LDAPS，并且控制台可以访问所需的证书。
6. 测试连接。如果失败，请检查 LDAP 主机、端口、网络连接和 SSL/TLS 证书。
7. 测试成功后，输入目录和用户详细信息：
 - **Base DN binding**：输入此应用程序将用于连接到目录的 LDAP/AD 帐户的绑定 DN，并输入该帐户的绑定凭据（密码）。Console 使用这些详细信息绑定到 LDAP 并验证连接。
 - 用户 **DN**：有权查询目录的用户帐户。例如，`CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`。
8. 选择*添加*以保存此集成。

完成后

保存集成后，向组织添加目录用户并分配角色。添加目录用户之前，必须配置并启用至少一个 Active Directory 集成。[了解如何添加目录用户并分配角色](#)。

禁用或启用 Active Directory 集成

禁用集成以暂时挂起目录支持的身份验证，而不删除配置。禁用目录服务时，目录用户无法通过目录登录。

步骤

1. 选择 **Administration > Identity and access**。
2. 选择*目录服务*以打开联盟页面。
3. 在集成列表中，找到该集成，然后选择该行的操作菜单。
4. 选择*禁用*以暂停集成，或选择*启用*以恢复集成。

删除 Active Directory 集成

删除集成以永久删除目录服务配置。在删除之前，请查看有链接到集成的目录用户的任何警告，因为他们的访问权限将受到影响。

步骤

1. 选择 **Administration > Identity and access**。
2. 选择*目录服务*以打开联盟页面。
3. 在集成列表中，找到该集成，然后选择该行的操作菜单。
4. 选择 **Delete** 并确认删除。

连接您的 LLM 并在 NetApp Console 本地部署中启用 NetApp Console 助手

将您的大型语言模型 (LLM) 连接到 NetApp Console 本地部署，以启用 Console 助理和 AI 辅助存储管理。



本文档以技术预览形式提供有关将 LLM 连接到 Console 助理以启用 AI 功能的文档。通过此预览产品，NetApp 保留在正式发布之前修改产品详情、内容和时间表的权利。

必需的访问角色

超级管理员或组织管理员。["了解访问角色"](#)。

设置完成后，用户从控制面板打开 Console 助理并选择访问模式：

- 在*只读*模式下，助手回答问题并提供指导，而不进行任何更改。
- 在"读/写"模式下，助手可以对存储基础设施进行操作。它会在每次更改前显示详细信息以供审核和确认。对于异步操作（例如创建卷），它会创建一个作业，用户可以从助手检查该作业。

要连接您的 LLM，请选择提供程序路径，输入端点详细信息和 API 密钥，然后在 **Administration > AI Tools** 中选择一个模型。助手操作在您的存储策略和基于角色的访问控制范围内执行。

在连接 LLM 之前，请先收集所需信息

在连接 LLM 之前，请收集以下信息：

- 您的提供程序类型决定：OpenAI 或 OpenAI 兼容。["了解提供者的选择。"](#)
- 您选择的提供程序路径的有效 API 密钥。
- 提供程序路径的端点 URL。
- 您的代理或网关 URL（如果您的组织需要）。
- LLM 提供商帐户的用户名或单点登录 (SSO) ID（如果需要）。
- 从 Console 本地部署到选定端点的网络访问。
- 计划允许的助理操作的存储类和基于角色的访问控制。

有关支持的型号详细信息，请参见 ["了解 NetApp Console 本地部署中受支持的 LLM 提供程序和模型"](#)。

将 LLM 连接到 NetApp Console 本地部署

输入提供程序设置、API 密钥和模型，将 LLM 连接到 Console 本地部署。

步骤

1. 登录到 NetApp Console 本地部署。
2. 选择 **Administration > AI Tools**。
3. 选择菜单，然后选择 **Edit**。
4. 在*提供程序类型*中，选择一个提供程序类型。

["了解 LLM 在 NetApp Console 本地部署中的集成"](#)。

5. 如果提示输入提供程序端点，请输入所选提供程序路径的端点 URL。
6. 输入代理或网关 URL 和凭据。
7. 在*用户名*字段中，输入您的用户名或 SSO ID（如果您的提供商路径需要）。
8. 在 **API key** 字段中，粘贴您所选提供商路径中的 API 密钥。
9. 从列表中选择一个模型。

10. 查看配置，然后选择 **Save**。

如果保存或测试失败，请验证提供程序类型、端点 URL、API 密钥和所选模型，然后重试。

["排查 LLM 集成故障"](#)。

验证 LLM 集成是否有效

保存配置后，请验证助手的可用性和行为。

步骤

1. 确认 **Console assistant** 按钮出现在 NetApp Console 本地部署仪表板上。
2. 在*只读*模式下打开助手并运行基本查询。
3. 在*读/写*模式下打开助手，确认存储更改操作需要用户确认后才能执行。
4. 验证需要操作工作流的用户是否具有所需的基于角色的访问控制。

完成验证后，用户可以从仪表板打开 Console 助理，并以简单的语言描述任务。有关使用示例和最终用户工作流，请参见 ["使用 NetApp Console 助手"](#)。

保护凭据并监控 LLM 使用情况

- 尽可能使用专用 API 密钥进行 Console 本地部署集成。
- 根据您的组织策略轮换 API 密钥。
- 将可以编辑 AI Tools 设置的人员限制为仅所需的管理员角色。
- 监控提供商 API 使用情况和警报，以跟踪异常活动或成本峰值。

排除 NetApp Console 本地部署中的 LLM 集成故障

使用此快速分流流程来诊断和解决 NetApp Console 本地部署中的常见 LLM 集成问题。



本文档以技术预览形式提供有关将 LLM 连接到 Console 助理以启用 AI 功能的文档。通过此预览产品，NetApp 保留在正式发布之前修改产品详情、内容和时间表的权利。

如果您尚未完成设置，请参见 ["连接您的 LLM 并启用 NetApp Console 助理"](#)。

快速分类 LLM 集成问题

1. 在*管理 > AI Tools*中验证 AI Tools 配置。

确认提供程序类型、端点 URL、API 密钥、所选模型和出站网络访问。

2. 在控制面板上验证助手可用性。

确认预期用户和组织的 **Console assistant** 按钮是否显示。

3. 验证运行时行为。

运行一个简单的只读请求，并确认提供程序端点可访问性、模型可用性和提供程序服务运行状况。

按症状排查故障

症状	可能的原因	需要检查的内容	下一步操作
在 AI Tools 中保存或测试失败	配置或连接不匹配	提供程序类型、端点 URL、API 密钥格式、所选模型和出站访问	请更正验证失败的值，然后再次保存
Console assistant 按钮缺失	不正常的集成状态、组织不匹配或 RBAC 不匹配	成功的 AI Tools 保存、集成状态、当前组织和预期访问角色	刷新会话并使用已知良好的管理员账号进行验证
助手已打开但请求失败	提供程序或运行时路径问题	端点可达性、该端点上的模型可用性、提供程序限制和临时提供程序状态	修复端点/模型不匹配或提供方端限制问题后重试
助理响应缓慢或不一致	提示大小、端点性能或网络/代理不稳定性	短提示测试、提供商服务健康状况和网络/代理稳定性	使用较短的提示，尝试其他支持的模型，并稳定网络或代理路由

应对 LLM 凭据泄露或滥用

如果怀疑 API 密钥泄露或未经授权使用：

1. 撤销提供程序系统中的现有 API 密钥。
2. 创建新的 API 密钥。
3. 更新 **Administration > AI Tools** 中的密钥。
4. 使用只读助手测试验证重新连接是否成功。

在 NetApp Console 本地部署中设置通知传递渠道

在 NetApp Console 本地部署中，您可以为警报通知设置多个通道，包括电子邮件和 Webhook。

必需的访问角色

超级管理员或组织管理员。["了解访问角色"](#)。

默认情况下，Console 本地部署通过其内置通知系统显示通知。配置其他交付渠道可让您以最适合工作流程的方式接收通知。

您可以通过相同的渠道发送所有通知，也可以针对不同的通知类型使用不同的渠道。例如，您可以通过电子邮件发送紧急存储警报，同时通过 webhook 将其他警报流量路由到第三方监控工具。

设置通知投递通道后，您可以配置通知规则并将其分配给不同的通道。["了解如何配置通知规则"](#)。

配置电子邮件服务器

配置电子邮件服务器时，Console 本地部署会通过它发送通知、警报和用户邀请。Console 本地部署支持 SMTP 电子邮件服务器，该服务器可以是您现有的企业电子邮件服务器或第三方电子邮件服务。

步骤

1. 选择 **Administration > Console**。
2. 选择*Configuration*以打开系统配置页面。
3. 在*电子邮件服务器*部分，选择*配置*。
4. 输入电子邮件服务器的连接详细信息：
 - 添加发件人姓名和发件人电子邮件地址。
 - **SMTP 主机**：SMTP 服务器的主机名或 IP 地址。对于多台服务器，请输入主服务器。
 - 从*连接安全*下拉列表中选择连接协议。该端口已为您配置，且为只读：25 用于 SMTP with STARTTLS，或 465 用于 SMTPS。

SMTPS（端口 465）立即建立加密连接，建议用于安全敏感的环境。STARTTLS（端口 25）从未加密的连接升级，如果加密协商失败，可能会回退到未加密的传输。

5. 选择*测试电子邮件*以向您指定的收件人发送测试电子邮件。
6. 测试成功后，选择 **Save** 保存配置。

如果测试失败，请重新验证您输入的设置，并仔细检查 Console 本地部署是否具有对电子邮件服务器的网络访问权限。

更新电子邮件服务器配置

如果要使用其他电子邮件服务器，可以更新现有的电子邮件服务器配置。

步骤

1. 选择 **Administration > Console**。
2. 选择*Configuration*以打开系统配置页面。
3. 在*电子邮件服务器*部分，选择*配置*。
4. 选择*Clear fields*以清除现有配置。
5. 输入电子邮件服务器的新连接详细信息。
6. 选择*测试电子邮件*以向您指定的收件人发送测试电子邮件。
7. 测试成功后，选择 **Save** 保存新配置。

如果测试失败，请重新验证您输入的设置，并仔细检查 Console 本地部署是否具有对电子邮件服务器的网络访问权限。

删除电子邮件服务器配置

如果您不再希望 Console 本地部署发送电子邮件，则可以删除电子邮件服务器配置。

步骤

1. 选择 **Administration > Console**。
2. 选择*配置*以打开系统配置页面。

3. 在*电子邮件服务器*部分，选择*配置*。
4. 选择*Clear fields*以清除现有配置。
5. 选择 **Save** 保存已清除的配置，这将从 Console 本地部署中删除电子邮件服务器配置。

配置 Webhook

设置 Webhook，以便从 Console 本地部署向其他工具或服务发送通知。您可以配置多个 Webhook，每个 Webhook 指向不同的端点。例如，一个用于 SIEM，另一个用于值班寻呼服务。

创建 webhook 后，具有 Storage admin 角色的用户可以将其分配给特定的警报规则。例如，他们可以将关键警报发送到电子邮件，同时通过 webhook 将所有警报发送到第三方监控工具。



Console 本地部署不会在 Webhook 端点上实施访问控制。任何可以访问端点 URL 的用户或系统都会收到警报数据。确保通过应用程序自己的访问控制，将对接收应用程序的访问权限限制为授权用户。

开始之前

确认 Console 本地部署可以通过网络到达接收应用程序，并收集端点 URL、HTTP 方法以及该应用程序所需的任何身份验证或证书详细信息。

步骤

1. 选择 **Administration > Console**。
2. 选择*Configuration*以打开系统配置页面。
3. 在 **Webhook 集成** 部分，选择 **配置**。
4. 输入 Webhook 所需的详细信息：
 - Webhook 的描述性名称。
 - 接收应用程序提供的端点 URL。
 - HTTP 方法
 - 可选：PEM 格式的自签名证书。
 - 任何必需的标头或机密（身份验证凭据）。
 - 发送 Webhook 时使用的格式。支持 JSON 和 OTEL (OpenTelemetry)。

将 JSON 用于通用 Webhook 和自定义 REST 端点。将 OTEL 用于本机使用 OpenTelemetry 信号的观测性平台，例如 Grafana 或其他 OpenTelemetry 兼容的收集器。

5. 选择 **Test webhook** 以测试 webhook 连接，并确保 Console 本地部署可以成功将消息发送到接收应用程序。
6. 测试成功后，选择*保存*以创建 Webhook。

保存 Webhook 后，用户可以在支持 Webhook 的位置选择它，例如警报传递选项。 ["了解如何创建警报规则并分配用于警报传递的 Webhook。"](#)

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。