# Konsolenintegrationen und Dienste konfigurieren

## NetApp Console local deployment

NetApp
August 10, 2026

# Inhalt

# Konsolenintegrationen und Dienste konfigurieren

## Lokale Bereitstellung der NetApp Console in Active Directory integrieren

Die lokale NetApp Console-Bereitstellung kann mit Active Directory für verzeichnisgestützte Anmeldung und Benutzersuche integriert werden. Der Verzeichnisdienst authentifiziert die Benutzer, anschließend wird diesen Benutzern in der lokalen NetApp Console-Bereitstellung Zugriff zugewiesen.

**Erforderliche Zugriffsrollen**

Super Admin oder Organisationsadministrator. "Informationen zu Zugriffsrollen".

Bei der Integration mit Active Directory authentifiziert die lokale Bereitstellung von Console die Benutzer über Ihr bestehendes Verzeichnis. Nachdem ein Verzeichnisbenutzer hinzugefügt wurde, können Console Zugriffsrollen zugewiesen werden, um zu steuern, worauf dieser Benutzer zugreifen kann.

Die Active Directory Integration unterstützt zudem die Erfüllung von Compliance-Anforderungen, indem bestehende Kontrollen, Audit-Trails und Richtlinien auf den lokalen NetApp Console-Bereitstellungszugriff angewendet werden.

- Die Active Directory Integration erstellt keine föderierten Gruppen, synchronisiert keine Verzeichnisgruppen-Zuordnungen und gewährt keinen automatischen Zugriff. Administratoren fügen weiterhin Verzeichnisbenutzer zur Organisation hinzu und weisen Rollen in der lokalen Console-Bereitstellung zu.
- Es wird jeweils nur eine Active Directory Integration unterstützt. Sobald eine Integration konfiguriert ist, ist die Schaltfläche **Integration hinzufügen** deaktiviert. Um zu einem anderen Verzeichnis zu wechseln, muss zunächst die bestehende Integration deaktiviert oder gelöscht werden.
- Verzeichnisbenutzer konfigurieren oder verwenden keine Multi-Faktor Authentifizierung (MFA). Die lokale Konsolenbereitstellung unterstützt MFA nur für lokale Benutzer. "Informationen zur Verwaltung der Sicherheitseinstellungen für Mitglieder".

### Bevor Sie beginnen

Bevor Sie die Integration mit Active Directory vornehmen, vergewissern Sie sich, dass Sie Folgendes haben:

- Eine Active Directory Domain und Anmeldeinformationen, die das Verzeichnis abfragen können
- Die LDAP-Serveradresse und der Basis individueller Name (DN) für den Verzeichnisbaum
- Netzwerkzugriff von der lokalen NetApp Console-Bereitstellung auf Ihren LDAP-Server über Port 389 (LDAP) oder 636 (LDAPS)
- SSL/TLS-Zertifikate, wenn die Verwendung von LDAPS vorgesehen ist

**Schritte**

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Verzeichnisdienste** auswählen, um die Seite „Verbände“ zu öffnen.

3. **Integration hinzufügen** auswählen.
4. Geben Sie die Verbindungsdetails für Ihren Active Directory Server ein:
   - Ein beschreibender Name für die Integration.
   - Der **LDAP-Host**: Hostname oder IP-Adresse Ihres LDAP-Servers. Bei mehreren Servern den primären angeben.
   - Der Port: 389 für LDAP oder 636 für LDAPS.
   - Die **Verbindungs-Zeitüberschreitung** in Millisekunden. Der Standardwert beträgt 1000 ms.
5. **SSL/TLS verwenden** auswählen, um LDAPS zu nutzen. Es sollte bestätigt werden, dass der LDAP-Server LDAPS unterstützt und dass die Konsole auf die erforderlichen Zertifikate zugreifen kann.
6. Die Verbindung testen. Falls diese fehlschlägt, den LDAP-Host, den Port, die Netzwerkverbindung und die SSL/TLS-Zertifikate überprüfen.
7. Nach erfolgreichem Test sind das Verzeichnis und die Benutzerdaten einzugeben:
   - **Base DN-Bindung**: Geben Sie den Bind DN für das LDAP/AD-Konto ein, das diese Anwendung für die Verbindung zum Verzeichnis verwendet, und geben Sie die Bind-Anmeldeinformationen (Passwort) für dieses Konto ein. Die Console verwendet diese Angaben, um eine Verbindung zu LDAP herzustellen und die Verbindung zu validieren.
   - **Benutzer-DN**: Ein Benutzerkonto mit der Berechtigung, das Verzeichnis abzufragen. Zum Beispiel `CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`.
8. **Hinzufügen** auswählen, um die Integration zu speichern.

#### Nachdem Sie fertig sind

Nachdem die Integration gespeichert wurde, können Verzeichnisbenutzer zur Organisation hinzugefügt und Rollen zugewiesen werden. Mindestens eine Active Directory Integration muss konfiguriert und aktiviert sein, bevor Verzeichnisbenutzer hinzugefügt werden können. "Informationen zum Hinzufügen von Verzeichnisbenutzern und zum Zuweisen von Rollen".

## Eine Active Directory Integration deaktivieren oder aktivieren

Eine Integration kann deaktiviert werden, um die verzeichnisbasierte Authentifizierung vorübergehend auszusetzen, ohne die Konfiguration zu löschen. Wenn ein Verzeichnisdienst deaktiviert ist, können sich Verzeichnisbenutzer nicht über das Verzeichnis anmelden.

#### Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.
2. **Verzeichnisdienste** auswählen, um die Seite „Verbände“ zu öffnen.
3. In der Integrationsliste die Integration suchen und das Aktionsmenü für diese Zeile auswählen.
4. **Deaktivieren** setzt die Integration aus, **Aktivieren** stellt sie wieder her.

## Eine Active Directory Integration löschen

Durch das Löschen einer Integration wird die Verzeichnisdienstkonfiguration dauerhaft entfernt. Vor dem Löschen sind alle Warnungen zu den mit der Integration verknüpften Verzeichnisbenutzern zu prüfen, da deren Zugriff beeinträchtigt wird.

#### Schritte

1. **Verwaltung > Identität und Zugriff** auswählen.

2. **Verzeichnisdienste** auswählen, um die Seite „Verbände“ zu öffnen.
3. In der Integrationsliste die Integration suchen und das Aktionsmenü für diese Zeile auswählen.
4. **Löschen** auswählen und die Löschung bestätigen.

# LLM verbinden und den NetApp Console Assistenten in der NetApp Console lokalen Bereitstellung aktivieren

Verbinden Sie Ihr großes Sprachmodell (LLM) mit der lokalen NetApp Console-Bereitstellung, um den Console-Assistenten und die KI-gestützte Speicherverwaltung zu aktivieren.

Diese Dokumentation zur Verbindung eines LLM mit dem Konsolenassistenten zur Aktivierung von KI-Funktionen wird als Technologievorschau bereitgestellt. Mit diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

**Erforderliche Zugriffsrollen**

Super Admin oder Organisationsadministrator. "Informationen zu Zugriffsrollen".

Nach der Einrichtung öffnen die Benutzer den Konsolenassistenten über das Dashboard und wählen einen Zugriffsmodus aus:

- Im **Nur-Lese-Modus** beantwortet der Assistent Fragen und gibt Hilfestellungen, ohne Änderungen vorzunehmen.
- Im **Lese/Schreib**-Modus kann der Assistent auf die Speicherinfrastruktur zugreifen. Vor jeder Änderung werden Details zur Überprüfung und Bestätigung angezeigt. Für asynchrone Vorgänge, wie die Volume-Erstellung, wird ein Auftrag erstellt, den Benutzer über den Assistenten einsehen können.

Um Ihr LLM zu verbinden, einen Anbieterpfad auswählen, Endpunktdetails und API-Schlüssel eingeben und anschließend ein Modell unter **Administration > AI Tools** auswählen. Assistentenaktionen bleiben innerhalb Ihrer Speicherrichtlinien und rollenbasierten Zugriffskontrollen.

## Sammeln Sie alles Notwendige, bevor Sie eine Verbindung zu einem LLM herstellen.

Bevor Sie Ihr LLM verbinden, sollten Sie Folgendes bereithalten:

- Ihre Entscheidung für einen Anbietertyp: OpenAI oder OpenAI-kompatibel. "Informationen zu den verfügbaren Anbieteroptionen."
- Ein gültiger API-Schlüssel für den ausgewählten Anbieterpfad.
- Die Endpunkt-URL für Ihren Anbieterpfad.
- Ihre Proxy- oder Gateway-URL, falls Ihre Organisation eine benötigt.
- Ihr Benutzername oder Ihre Single Sign-On (SSO)-ID für das LLM-Anbieterkonto, falls erforderlich.
- Netzwerkzugriff von der lokalen NetApp Console-Bereitstellung zum ausgewählten Endpunkt.
- Speicherklassen und rollenbasierte Zugriffskontrollen für die Assistentenaktionen, die Sie zulassen möchten.

Details zu den unterstützten Modellen sind unter "Informationen zu unterstützten LLM-Anbietern und Modellen

in der lokalen NetApp Console-Bereitstellung" zu finden.

## Eine LLM mit einer lokalen NetApp Console-Bereitstellung verbinden

Anbietereinstellungen, API-Schlüssel und Modell eingeben, um Ihre LLM mit der lokalen NetApp Console-Bereitstellung zu verbinden.

**Schritte**

1. Anmeldung bei der lokalen NetApp Console-Bereitstellung.
2. **Administration > AI Tools** auswählen.
3. Das Menü auswählen und anschließend **Bearbeiten** wählen.
4. Unter **Anbietertyp** einen Anbietertyp auswählen.

   "Informationen zur LLM-Integration in der lokalen NetApp Console-Bereitstellung".

5. Wenn Sie nach einem Provider-Endpunkt gefragt werden, die Endpunkt-URL für den ausgewählten Provider-Pfad eingeben.
6. Geben Sie die Proxy- oder Gateway-URL und die Zugangsdaten ein.
7. Im Feld **Benutzername** ist Ihr Benutzername oder Ihre SSO-ID einzugeben, wenn Ihr Providerpfad dies erfordert.
8. Im Feld **API-Schlüssel** den API-Schlüssel aus dem Pfad des ausgewählten Anbieters einfügen.
9. Ein Modell aus der Liste auswählen.
10. Die Konfiguration kann überprüft und anschließend **Speichern** ausgewählt werden.

    Falls das Speichern oder Testen fehlschlägt, sollten der Anbietertyp, die Endpunkt-URL, der API-Schlüssel und das ausgewählte Modell überprüft und anschließend ein erneuter Versuch unternommen werden.

"Fehlerbehebung bei Ihrer LLM-Integration".

## Es wird überprüft, ob die LLM Integration funktioniert.

Nachdem die Konfiguration gespeichert wurde, lassen sich die Verfügbarkeit und das Verhalten des Assistenten überprüfen.

**Schritte**

1. Bestätigt wird, dass die Schaltfläche **Konsolenassistent** auf dem NetApp Console Dashboard für die lokale Bereitstellung angezeigt wird.
2. Den Assistenten im **Nur-Lese-Modus** öffnen und eine einfache Abfrage ausführen.
3. Den Assistenten im **Lese-/Schreibmodus** öffnen und bestätigen, dass speicherverändernde Aktionen vor der Ausführung eine Benutzerbestätigung erfordern.
4. Es sollte überprüft werden, dass die Benutzer, die Aktionsworkflows benötigen, über die erforderlichen rollenbasierten Zugriffskontrollen verfügen.

Nach Abschluss der Validierung können Benutzer den Konsolenassistenten über das Dashboard öffnen und Aufgaben in einfacher Sprache beschreiben. Beispiele für die Nutzung und Endbenutzer-Workflows finden sich unter "Den NetApp Console Assistenten verwenden".

### Zugangsdaten schützen und LLM-Nutzung überwachen

- Nach Möglichkeit sollte ein dedizierter API-Schlüssel für die lokale Bereitstellungsintegration der Konsole verwendet werden.
- API-Schlüssel werden gemäß den Richtlinien Ihrer Organisation rotiert.
- Der Zugriff auf die Einstellungen der KI-Tools ist ausschließlich auf die erforderlichen Administratorrollen beschränkt.
- Die API-Nutzung und Warnmeldungen auf Anbieterseite werden überwacht, um ungewöhnliche Aktivitäten oder Kostenspitzen nachzuverfolgen.

# Fehlerbehebung bei der LLM-Integration in der lokalen NetApp Console-Bereitstellung

Mit diesem Schnelltest lassen sich häufige LLM-Integrationsprobleme in der lokalen NetApp Console-Bereitstellung diagnostizieren und beheben.

> Diese Dokumentation zur Verbindung eines LLM mit dem Konsolenassistenten zur Aktivierung von KI-Funktionen wird als Technologievorschau bereitgestellt. Mit diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

Falls die Einrichtung noch nicht abgeschlossen ist, siehe "Verbinden Sie Ihren LLM und aktivieren Sie den NetApp Console Assistenten".

## LLM-Integrationsprobleme schnell eingrenzen

1. Die Konfiguration der KI-Tools in **Administration > KI-Tools** kann validiert werden.

   Anbietertyp, Endpunkt-URL, API-Schlüssel, ausgewähltes Modell und ausgehender Netzwerkzugriff werden bestätigt.

2. Die Verfügbarkeit des Assistenten im Dashboard wird angezeigt.

   Bestätigt wird, dass die Schaltfläche **Konsolenassistent** für die erwarteten Benutzer und Organisationen erscheint.

3. Laufzeitverhalten überprüfen.

   Eine einfache Leseanfrage ausführen und die Erreichbarkeit des Provider-Endpunkts, die Verfügbarkeit des Modells sowie den Zustand des Provider-Dienstes bestätigen.

## Fehlerbehebung anhand der Symptome

| Symptom | Wahrscheinliche Ursache | Was überprüft werden sollte | Nächster Schritt |
|---|---|---|---|
| Speichern oder Testen schlägt in AI Tools fehl | Konfigurations- oder Verbindungsinkonsistenz | Anbietertyp, Endpunkt-URL, API-Schlüsselformat, ausgewähltes Modell und ausgehender Zugriff | Der Wert, der die Validierung nicht besteht, muss korrigiert und erneut gespeichert werden. |

| Symptom | Wahrscheinliche Ursache | Was überprüft werden sollte | Nächster Schritt |
|---|---|---|---|
| Die Schaltfläche „Console assistant“ fehlt. | Unzureichender Integrationsstatus, Organisationskonflikt oder RBAC-Konflikt | Erfolgreiche Speicherung von KI-Tools, Integrationsstatus, aktuelle Organisation und erwartete Zugriffsrolle | Die Sitzung wird aktualisiert und mit einem bekannten, funktionierenden Administratorkonto überprüft. |
| Assistent öffnet sich, aber die Anfrage schlägt fehl | Problem mit dem Anbieter oder dem Laufzeitpfad | Erreichbarkeit des Endpunkts, Modellverfügbarkeit auf diesem Endpunkt, Anbieterlimits und temporärer Anbieterstatus | Nach Behebung von Endpunkt-/Modellkonflikten oder Anbieterseitigen Limitproblemen erneut versuchen |
| Die Antwort des Assistenten ist langsam oder inkonsistent. | Eingabeaufforderungsgröße, Endpunktleistung oder Netzwerk-/Proxy-Instabilität | Kurzer Schnelltest, Verfügbarkeit des Anbieterdienstes und Netzwerk-/Proxy-Stabilität | Eine kürzere Eingabeaufforderung verwenden, ein anderes unterstütztes Modell ausprobieren und das Netzwerk- oder Proxy-Routing stabilisieren |

## Auf Offenlegung oder Missbrauch von LLM-Anmeldedaten reagieren

Wenn Sie den Verdacht haben, dass der API-Schlüssel offengelegt oder unbefugt verwendet wurde:

1. Der bestehende API-Schlüssel wird im Anbietersystem widerrufen.
2. Einen neuen API-Schlüssel erstellen.
3. Der Schlüssel wird unter **Administration > AI Tools** aktualisiert.
4. Die erfolgreiche Wiederverbindung mit einem schreibgeschützten Assistententest wird überprüft.

# Benachrichtigungszustellungskanäle in der lokalen NetApp Console-Bereitstellung einrichten

In der lokalen NetApp Console-Bereitstellung können mehrere Kanäle für Benachrichtigungen eingerichtet werden, darunter E-Mail und Webhooks.

**Erforderliche Zugriffsrollen**

Super Admin oder Organisationsadministrator. "Informationen zu Zugriffsrollen".

Standardmäßig werden Benachrichtigungen bei der lokalen Bereitstellung der Console über das integrierte Benachrichtigungssystem angezeigt. Die Konfiguration zusätzlicher Zustellungskanäle ermöglicht den Empfang von Benachrichtigungen auf die Weise, die am besten zum eigenen Workflow passt.

Sie können alle Benachrichtigungen über dieselben Kanäle versenden oder für verschiedene Benachrichtigungstypen unterschiedliche Kanäle verwenden. Beispielsweise können dringende Speicherwarnungen per E-Mail versendet werden, während anderer Alarmverkehr über einen Webhook an ein externes Überwachungstool weitergeleitet wird.

Nachdem Benachrichtigungskanäle eingerichtet wurden, lassen sich Benachrichtigungsregeln konfigurieren und verschiedenen Kanälen zuweisen. "Informationen zur Konfiguration von Benachrichtigungsregeln".

## E-Mail-Server konfigurieren

Wenn ein E-Mail-Server konfiguriert ist, sendet Console local deployment Benachrichtigungen, Warnungen und Benutzereinladungen darüber. Console local deployment unterstützt SMTP-E-Mail-Server, die entweder Ihr bestehender Unternehmens-E-Mail-Server oder ein E-Mail-Dienst eines Drittanbieters sein können.

**Schritte**

1. **Administration > Konsole** auswählen.
2. **Konfiguration** öffnet die Seite „Systemkonfigurationen“.
3. Im Abschnitt **E-Mail-Server** auf **Konfigurieren** auswählen.
4. Geben Sie die Verbindungsdetails für Ihren E-Mail-Server ein:
   - Einen Absendernamen und eine Absender-E-Mail-Adresse hinzufügen.
   - Der **SMTP-Host**: Hostname oder IP-Adresse Ihres SMTP-Servers. Bei mehreren Servern ist der primäre anzugeben.
   - Wählen Sie das Verbindungsprotokoll aus der Dropdown-Liste **Verbindungssicherheit** aus. Der Port ist vorkonfiguriert und schreibgeschützt: 25 für SMTP mit STARTTLS oder 465 für SMTPS.

     SMTPS (Port 465) stellt sofort eine verschlüsselte Verbindung her und wird für sicherheitskritische Umgebungen empfohlen. STARTTLS (Port 25) wertet eine unverschlüsselte Verbindung auf und kann auf unverschlüsselte Übertragung zurückgreifen, falls die Verschlüsselungsaushandlung fehlschlägt.
5. **Test-E-Mail** auswählen, um eine Test-E-Mail an einen angegebenen Empfänger zu senden.
6. Nach erfolgreichem Test **Speichern** auswählen, um die Konfiguration zu speichern.

   Falls der Test fehlschlägt, sollten die eingegebenen Einstellungen erneut überprüft und zusätzlich sichergestellt werden, dass die lokale Console-Bereitstellung Netzwerkzugriff auf den E-Mail-Server hat.

### Aktualisierung einer E-Mail-Server-Konfiguration

Sie können eine bestehende E-Mail-Server-Konfiguration aktualisieren, wenn Sie einen anderen E-Mail-Server verwenden möchten.

**Schritte**

1. **Administration > Konsole** auswählen.
2. **Konfiguration** öffnet die Seite „Systemkonfigurationen“.
3. Im Abschnitt **E-Mail-Server** auf **Konfigurieren** auswählen.
4. **Felder löschen** auswählen, um die bestehende Konfiguration zu löschen.
5. Geben Sie die neuen Verbindungsdaten für Ihren E-Mail-Server ein.
6. **Test-E-Mail** auswählen, um eine Test-E-Mail an einen angegebenen Empfänger zu senden.
7. Nach erfolgreichem Test auf **Speichern** auswählen, um die neue Konfiguration zu speichern.

   Falls der Test fehlschlägt, sollten die eingegebenen Einstellungen erneut überprüft und zusätzlich sichergestellt werden, dass die lokale Console-Bereitstellung Netzwerkzugriff auf den E-Mail-Server hat.

### Eine E-Mail-Serverkonfiguration entfernen

Sie können die E-Mail-Server-Konfiguration entfernen, wenn Sie nicht mehr möchten, dass die lokale Console

Bereitstellung E-Mails versendet.

**Schritte**

1. **Administration > Konsole** auswählen.
2. **Konfiguration** auswählen, um die Seite Systemkonfiguration zu öffnen.
3. Im Abschnitt **E-Mail-Server** auf **Konfigurieren** auswählen.
4. **Felder löschen** auswählen, um die bestehende Konfiguration zu löschen.
5. **Speichern** auswählen, um die gelöschte Konfiguration zu speichern, wodurch die E-Mail-Server-Konfiguration aus der Console lokalen Bereitstellung entfernt wird.

## Einen Webhook konfigurieren

Webhooks können eingerichtet werden, um Benachrichtigungen von der lokalen Console Bereitstellung an andere Tools oder Dienste zu senden. Es ist möglich, mehrere Webhooks zu konfigurieren, die jeweils auf einen anderen Endpunkt verweisen. Zum Beispiel einen für ein SIEM und einen weiteren für einen On-Call-Paging-Dienst.

Nachdem ein Webhook erstellt wurde, können Benutzer mit der Rolle Storage admin diesen bestimmten Alarmregeln zuweisen. Beispielsweise ist es möglich, kritische Alarme per E-Mail zu versenden, während alle Alarme über einen Webhook an ein Drittanbieter-Überwachungstool weitergeleitet werden.

> Bei der lokalen Bereitstellung über die Konsole wird keine Zugriffskontrolle für Webhook-Endpunkte erzwungen. Jeder Benutzer oder jedes System, das die Endpunkt-URL erreichen kann, erhält die Alarmdaten. Es sollte sichergestellt sein, dass der Zugriff auf die empfangende Anwendung durch die Zugriffskontrollen dieser Anwendung auf autorisierte Benutzer beschränkt ist.

**Bevor Sie beginnen**

Es sollte bestätigt werden, dass die lokale Console-Bereitstellung die empfangende Anwendung über das Netzwerk erreichen kann, und die Endpunkt-URL, die HTTP-Methode sowie alle von dieser Anwendung benötigten Authentifizierungs- oder Zertifikatsdetails sollten erfasst werden.

**Schritte**

1. **Administration > Konsole** auswählen.
2. **Konfiguration** öffnet die Seite „Systemkonfigurationen“.
3. Im Abschnitt **Webhook-Integration** auf **Konfigurieren** auswählen.
4. Geben Sie die erforderlichen Details für den Webhook ein:
   - Ein beschreibender Name für den Webhook.
   - Die von der empfangenden Anwendung bereitgestellte Endpoint-URL.
   - HTTP-Methode
   - Optional: Ein selbstsigniertes Zertifikat im PEM-Format.
   - Alle erforderlichen Header oder Geheimnisse (Authentifizierungsdaten).
   - Das Format, das beim Senden des Webhooks verwendet werden soll. JSON und OTEL (OpenTelemetry) werden unterstützt.

     JSON wird für allgemeine Webhooks und benutzerdefinierte REST-Endpunkte verwendet. OTEL wird für Observability-Plattformen verwendet, die OpenTelemetry-Signale nativ verarbeiten, wie Grafana

oder andere OpenTelemetry-kompatible Collector.

5. **Webhook testen** auswählen, um die Webhook-Verbindung zu testen und sicherzustellen, dass die Console lokale Bereitstellung erfolgreich Nachrichten an die empfangende Anwendung senden kann.
6. Nach erfolgreichem Test **Speichern** auswählen, um den Webhook zu erstellen.

   Nach dem Speichern des Webhooks steht er Benutzern zur Auswahl zur Verfügung, wo Webhooks unterstützt werden, wie beispielsweise bei den Optionen zur Benachrichtigungszustellung. "Informationen zum Erstellen von Alarmregeln und zum Zuweisen von Webhooks für die Alarmzustellung."