コンソール統合とサービスの設定

NetApp Console local deployment

NetApp
August 10, 2026

目次

コンソール統合とサービスの設定

NetApp Console ローカル展開を Active Directory と統合する

NetApp Console ローカル展開を Active Directory と統合して、ディレクトリベースのサインインとユーザー検索を実現します。ディレクトリサービスを使用してユーザーを認証し、NetApp Console ローカル展開でそれらのユーザーにアクセス権を割り当てます。

必要なアクセスロール

スーパー管理者または組織管理者。"アクセスロールについて"。

Active Directoryと統合する場合、コンソールのローカル展開では、既存のディレクトリを通じてユーザー認証が行われます。ディレクトリユーザーを追加したら、コンソールアクセスロールを割り当てて、そのユーザーがアクセスできる範囲を制御します。

Active Directoryとの統合は、既存の制御、監査証跡、およびポリシーをコンソールのローカル展開アクセスに適用することで、コンプライアンス要件を満たすのにも役立ちます。

- Active Directoryとの統合では、フェデレーショングループの作成、ディレクトリグループの割り当ての同期、およびアクセス権の自動付与は行われません。管理者は引き続き、Console のローカル展開環境でディレクトリユーザーを組織に追加し、役割を割り当てます。
- 同時にサポートされるActive Directory統合は1つのみです。統合が設定されると、「統合を追加」ボタンは無効になります。別のディレクトリに切り替えるには、まず既存の統合を無効にするか削除してください。
- ディレクトリユーザーは、多要素認証（MFA）を設定したり使用したりしません。コンソールのローカル展開では、ローカルユーザーに対してのみMFAがサポートされます。"メンバーのセキュリティ設定を管理する方法を説明します"。

開始する前に

Active Directoryと統合する前に、以下の点を確認してください：

- Active Directoryドメインと、ディレクトリを照会できる資格情報
- LDAPサーバのアドレスとディレクトリツリーのベース識別名（DN）
- コンソールローカル展開からLDAPサーバへのネットワークアクセス（ポート389（LDAP）または636（LDAPS））
- LDAPSを使用する予定がある場合は、SSL/TLS証明書

手順

1. 「管理」＞「IDとアクセス」を選択してください。
2. *ディレクトリサービス*を選択して、フェデレーションページを開きます。
3. 「連携を追加」を選択します。
4. Active Directoryサーバーの接続詳細を入力してください：

- 統合内容を分かりやすく表した名称。
- **LDAP**ホスト：LDAPサーバのホスト名またはIPアドレス。複数のサーバーがある場合は、プライマリサーバーを入力してください。
- ポート番号：LDAPの場合は389、LDAPSの場合は636。
- *接続タイムアウト*時間（ミリ秒）。デフォルト値は1000ミリ秒です。

5. LDAPSを使用するには、*SSL/TLSを使用する*を選択してください。LDAPサーバがLDAPSをサポートしており、コンソールが必要な証明書にアクセスできることを確認してください。
6. 接続をテストしてください。失敗した場合は、LDAPホスト、ポート、ネットワーク接続、およびSSL/TLS証明書を確認してください。
7. テストが成功したら、ディレクトリとユーザーの詳細を入力します。
   - ベース**DN**バインディング：このアプリがディレクトリに接続するために使用するLDAP/ADアカウントのバインドDNを入力し、そのアカウントのバインド認証情報（パスワード）を入力します。Console はこれらの詳細情報を使用してLDAPにバインドし、接続を検証します。
   - ユーザー**DN**：ディレクトリを照会する権限を持つユーザーアカウント。例えば、 `CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`。
8. 統合を保存するには、*追加*を選択してください。

終了後の操作

統合設定を保存したら、ディレクトリユーザーを組織に追加し、役割を割り当ててください。ディレクトリユーザーを追加するには、少なくとも1つのActive Directory統合を設定して有効にする必要があります。"ディレクトリユーザーの追加方法とロールの割り当て方法について説明します。"。

Active Directoryとの統合を無効化または有効化する

設定を削除せずに、ディレクトリベースの認証を一時的に停止するには、統合機能を無効にします。ディレクトリサービスを無効にすると、ディレクトリユーザーはディレクトリ経由でサインインできなくなります。

手順

1. 「管理」＞「IDとアクセス」を選択してください。
2. *ディレクトリサービス*を選択して、フェデレーションページを開きます。
3. 統合リストで、該当する統合を見つけ、その行のアクションメニューを選択します。
4. 統合を一時停止するには「無効にする」を選択し、復元するには「有効にする」を選択してください。

Active Directory統合を削除する

ディレクトリサービスの設定を完全に削除するには、統合を削除します。削除する前に、統合に関連付けられているディレクトリユーザーに関する警告を確認してください。これらのユーザーのアクセス権限に影響が出る可能性があります。

手順

1. 「管理」＞「IDとアクセス」を選択してください。
2. *ディレクトリサービス*を選択して、フェデレーションページを開きます。
3. 統合リストで、該当する統合を見つけ、その行のアクションメニューを選択します。

4. 「削除」を選択し、削除を確定してください。

LLMを接続し、NetApp Consoleのローカル展開でNetApp Consoleアシスタントを有効にする

大規模言語モデル （LLM） を NetApp Console のローカル展開に接続して、Console アシスタントと AI 支援型ストレージ管理を有効にします。

LLMをコンソールアシスタントに接続してAI機能を有効にする方法に関するこのドキュメントは、技術プレビューとして提供されています。このプレビュー版では、NetApp は一般提供開始前に、提供内容、コンテンツ、およびスケジュールを変更する権利を留保します。

必要なアクセスロール

スーパー管理者または組織管理者。"アクセスロールについて"。

設定後、ユーザーはダッシュボードから Console アシスタントを開き、アクセス モードを選択します。

- *読み取り専用*モードでは、アシスタントは変更を加えることなく質問に答え、ガイダンスを提供します。
- *読み取り/書き込み*モードでは、アシスタントはストレージ インフラストラクチャに対して操作を実行できます。変更を行う前に、確認と検証のための詳細情報が表示されます。ボリューム作成などの非同期操作の場合、ユーザーがアシスタントから確認できるジョブが作成されます。

LLMを接続するには、プロバイダーパスを選択し、エンドポイントの詳細とAPIキーを入力してから、*管理 > AIツール*でモデルを選択します。アシスタントのアクションは、ストレージポリシーとロールベースのアクセス制御の範囲内に留まります。

LLMに接続する前に必要なものを確認してください

LLMを接続する前に、以下の情報を準備してください：

- プロバイダーの種類の決定：OpenAI または OpenAI 互換。"プロバイダの選択肢について説明します。"
- 選択したプロバイダ パスに対応する有効な API キー。
- プロバイダパスのエンドポイント URL。
- 組織でプロキシ サーバまたはゲートウェイが必要な場合は、そのURLを入力してください。
- LLM プロバイダ アカウントのユーザー名またはシングル サインオン（SSO）ID（必要な場合）。
- コンソールのローカル展開から選択したエンドポイントへのネットワーク アクセス。
- 許可するアシスタント アクションのストレージ クラスとロールベースのアクセス制御。

サポートされているモデルの詳細については、"NetApp Console ローカル展開でサポートされている LLM プロバイダーとモデルについて説明します"を参照してください。

LLMをNetApp Consoleのローカル展開に接続する

LLMをConsoleのローカルデプロイメントに接続するために、プロバイダ設定、APIキー、およびモデルを入力してください。

手順

1. NetApp Console のローカル展開にログインします。
2. **Administration**（管理）**> AI Tools** を選択します。
3. メニューを選択し、次に「編集」を選択します。
4. 「プロバイダタイプ」で、プロバイダタイプを選択してください。

   "NetApp Console ローカル展開における LLM 統合について".

5. プロバイダーエンドポイントの入力を求められた場合は、選択したプロバイダーパスのエンドポイントURLを入力してください。
6. プロキシまたはゲートウェイのURLと認証情報を入力してください。
7. *ユーザー名*フィールドに、プロバイダのパスで必要な場合は、ユーザー名またはSSO IDを入力してください。
8. *APIキー*フィールドに、選択したプロバイダーパスから取得したAPIキーを貼り付けてください。
9. リストからモデルを選択してください。
10. 設定内容を確認し、*保存*を選択してください。

    保存またはテストが失敗した場合は、プロバイダーの種類、エンドポイントURL、APIキー、および選択したモデルを確認してから、もう一度試してください。

"LLM統合に関するトラブルシューティング".

LLM統合が正しく機能することを確認します。

設定を保存したら、アシスタントの利用可否と動作を確認してください。

手順

1. コンソールアシスタント ボタンが NetApp Console ローカルデプロイメントダッシュボードに表示されていることを確認してください。
2. アシスタントを*読み取り専用*モードで開き、基本的なクエリを実行します。
3. アシスタントを **Read/write** モードで開き、ストレージを変更する操作を実行する前にユーザーの確認が必要であることを確認してください。
4. アクションワークフローを必要とするユーザーが、必要なロールベースのアクセス制御を持っていることを確認してください。

検証が完了すると、ユーザーはダッシュボードからコンソールアシスタントを開き、タスクを平易な言葉で説明できるようになります。使用例とエンドユーザワークフローについては、"NetApp Console アシスタントを使用する"を参照してください。

認証情報を保護し、LLMの使用状況を監視する

- 可能な限り、Console のローカル展開統合には専用の API キーを使用してください。
- 組織のポリシーに従ってAPIキーをローテーションしてください。
- AIツールの設定を編集できるユーザーを、必要な管理者ロールのみに制限します。

- プロバイダー側のAPI使用状況とアラートを監視して、異常なアクティビティやコストの急増を追跡します。

NetApp Consoleローカルデプロイにおける**LLM**統合のトラブルシューティング

NetApp Console のローカル展開における一般的な LLM 統合の問題を診断および解決するには、このクイックトリアージフローを使用してください。

LLMをコンソールアシスタントに接続してAI機能を有効にする方法に関するこのドキュメントは、技術プレビューとして提供されています。このプレビュー版では、NetApp は一般提供開始前に、提供内容、コンテンツ、およびスケジュールを変更する権利を留保します。

セットアップが完了していない場合は、"LLMを接続してNetApp Consoleアシスタントを有効にする"を参照してください。

LLM統合の問題を迅速にトリアージする

1. 管理 > **AI Tools** でAI Toolsの設定を確認してください。

   プロバイダーの種類、エンドポイント URL、API キー、選択したモデル、および送信ネットワーク アクセスを確認してください。

2. ダッシュボード上でアシスタントの可用性を確認してください。

   想定されるユーザーおよび組織に対して、**Console assistant** ボタンが表示されることを確認してください。

3. 実行時動作を検証する。

   単純な読み取り専用リクエストを実行し、プロバイダーエンドポイントへの到達可能性、モデルの可用性、およびプロバイダーサービスの健全性を確認します。

症状別にトラブルシューティングを行う

現象	考えられる原因	チェックする項目	次のアクション
AI Tools での保存またはテストの失敗	設定または接続の不一致	プロバイダーの種類、エンドポイントURL、APIキーの形式、選択されたモデル、およびアウトバウンドアクセス	検証に失敗した値を修正して、再度保存してください。
「Console assistant」ボタンがありません	統合状態が不健全、組織の不一致、またはRBACの不一致	AI ツールの保存、統合ステータス、現在の組織、および想定されるアクセスロールが正常に完了しました	セッションを更新し、既知の正常な管理者アカウントで確認してください。

現象	考えられる原因	チェックする項目	次のアクション
アシスタントは起動するが、リクエストが失敗する	プロバイダーまたはランタイムパスの問題	エンドポイントへの到達可能性、そのエンドポイントにおけるモデルの可用性、プロバイダーの制限、および一時的なプロバイダーの状態	エンドポイント/モデルの不一致またはプロバイダー側の制限の問題を修正した後、再試行してください。
アシスタントの応答が遅い、または一貫性がない	プロンプトサイズ、エンドポイントのパフォーマンス、またはネットワーク/プロキシの不安定性	短時間の簡易テスト、プロバイダーサービスの健全性、ネットワーク/プロキシの安定性	プロンプトを短くするか、別のサポートされているモデルを試すか、ネットワークまたはプロキシのルーティングを安定させる

LLM クレデンシャルの漏洩または不正使用への対応

APIキーの漏洩または不正使用が疑われる場合：

1. プロバイダーシステムに登録されている既存のAPIキーを無効にしてください。
2. 新しいAPIキーを作成します。
3. 「管理」＞「AI Tools」でキーを更新してください。
4. 読み取り専用のアシスタントテストを使用して、再接続が成功したことを確認してください。

NetApp Console ローカル展開で通知配信チャネルを設定する

NetApp Console のローカル展開では、メールや Webhook など、アラート通知用の複数のチャネルを設定できます。

必要なアクセスロール

スーパー管理者または組織管理者。"アクセスロールについて"。

デフォルトでは、コンソールのローカル展開では、組み込みの通知システムを通じて通知が表示されます。追加の配信チャネルを設定することで、ワークフローに最適な方法で通知を受け取ることができます。

すべての通知を同じチャネルで送信することも、通知の種類ごとに異なるチャネルを使用することもできます。例えば、緊急のストレージアラートはメールで送信し、その他のアラートトラフィックはWebhookを介してサードパーティの監視ツールにルーティングするといったことが可能です。

通知配信チャネルを設定した後、通知ルールを設定し、それらを異なるチャネルに割り当てることができます。"通知ルールの設定方法を確認します"。

メールサーバーの設定

メールサーバーを設定すると、コンソールのローカル展開では、通知、アラート、およびユーザー招待がそのメールサーバー経由で送信されます。コンソールのローカル展開では、SMTPメールサーバーがサポートされており、既存の社内メールサーバー、またはサードパーティのメールサービスを使用できます。

手順

1. *「管理」>「コンソール」*を選択してください。
2. 「設定」を選択して、システム設定ページを開きます。
3. 「メールサーバー」セクションで、「設定」を選択します。
4. メールサーバーの接続情報を入力してください：
   - 送信者名と送信者のメールアドレスを追加してください。
   - **SMTP** ホスト：SMTP サーバーのホスト名または IP アドレス。複数のサーバーがある場合は、プライマリサーバーを入力してください。
   - 「接続セキュリティ」ドロップダウンリストから接続プロトコルを選択してください。ポートは自動的に設定され、読み取り専用です：STARTTLS を使用する SMTP の場合は 25、SMTPS の場合は 465。

     SMTPS（ポート465）は即座に暗号化された接続を確立するため、セキュリティが重視される環境での使用が推奨されます。STARTTLS（ポート25）は暗号化されていない接続からアップグレードし、暗号化のネゴシエーションが失敗した場合は暗号化されていない送信にフォールバックする可能性があります。
5. テストメール を選択すると、指定した受信者にテストメールが送信されます。
6. テストが成功したら、*保存*を選択して設定を保存します。

   テストが失敗した場合は、入力した設定を再確認し、Console のローカル展開がメールサーバーへのネットワーク アクセスを持っていることを確認してください。

メールサーバーの設定を更新する

別のメールサーバーを使用したい場合は、既存のメールサーバー設定を更新できます。

手順

1. *「管理」>「コンソール」*を選択してください。
2. 「設定」を選択して、システム設定ページを開きます。
3. 「メールサーバー」セクションで、「設定」を選択します。
4. 既存の設定をクリアするには、*フィールドをクリア*を選択してください。
5. メールサーバーの新しい接続情報を入力してください。
6. テストメール を選択すると、指定した受信者にテストメールが送信されます。
7. テストが成功したら、*保存*を選択して新しい設定を保存します。

   テストが失敗した場合は、入力した設定を再確認し、Console のローカル展開がメールサーバーへのネットワーク アクセスを持っていることを確認してください。

メールサーバーの設定を削除する

コンソールローカル展開でメールを送信する必要がなくなった場合は、メールサーバーの設定を削除できます。

手順

1. *「管理」>「コンソール」*を選択してください。
2. 「設定」を選択して、システム設定ページを開きます。
3. 「メールサーバー」セクションで、「設定」を選択します。
4. 既存の設定をクリアするには、*フィールドをクリア*を選択してください。
5. 「保存」を選択すると、クリアした設定が保存され、Console のローカル展開からメールサーバーの設定が削除されます。

ウェブフックを設定する

コンソールのローカルデプロイメントから他のツールやサービスに通知を送信するように、Webhookを設定します。複数のWebhookを設定でき、それぞれ異なるエンドポイントを指すように設定できます。例えば、SIEMと、オンコールページングサービス用などです。

Webhookを作成すると、ストレージ管理者ロールを持つユーザーは、それを特定のアラートルールに割り当てることができます。例えば、重要なアラートはメールで送信しつつ、すべてのアラートをWebhook経由でサードパーティの監視ツールに送信するといったことが可能です。

> コンソールのローカル展開では、Webhookエンドポイントへのアクセスコントロールはされません。エンドポイントURLにアクセスできるユーザーまたはシステムは、アラートデータを受信します。受信アプリケーションへのアクセスは、そのアプリケーション独自のアクセス制御を通じて、承認されたユーザーのみに制限されるようにしてください。

開始する前に

コンソールのローカル展開がネットワーク経由で受信アプリケーションに到達できることを確認し、エンドポイントURL、HTTPメソッド、およびそのアプリケーションが必要とする認証情報や証明書の詳細情報を収集します。

手順

1. *「管理」>「コンソール」*を選択してください。
2. 「設定」を選択して、システム設定ページを開きます。
3. 「Webhook integration」セクションで、「Configure」を選択します。
4. ウェブフックに必要な詳細情報を入力してください：
   - ウェブフックを表す分かりやすい名前。
   - 受信側アプリケーションから提供されるエンドポイントURL。
   - HTTPメソッド
   - オプション：PEM形式の自己署名証明書。
   - 必要なヘッダーまたはシークレット（認証クレデンシャル）。
   - ウェブフックを送信する際に使用するフォーマット。JSONとOTEL（OpenTelemetry）がサポートされています。

     汎用的なWebhookやカスタムRESTエンドポイントにはJSONを使用してください。GrafanaなどのOpenTelemetryシグナルをネイティブに使用するオブザーバビリティプラットフォームや、その他のOpenTelemetry互換コレクターにはOTELを使用してください。

5. 「Test webhook」を選択して、Webhook 接続をテストし、Console のローカル展開が受信アプリケーションにメッセージを正常に送信できることを確認してください。
6. テストが成功したら、*保存*を選択してウェブフックを作成します。

   ウェブフックを保存すると、アラート配信オプションなど、ウェブフックがサポートされている場所をユーザーが選択できるようになります。"アラートルールを作成し、アラート配信のための Webhook を割り当てる方法について説明します。"