はじめに

NetApp Console local deployment

NetApp
August 10, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/console-local/concept-netapp-console-local.html on August 10, 2026. Always check docs.netapp.com for the latest.

目次

はじめに

NetApp Console のローカル展開について

NetApp Console のローカル展開では、お客様独自のインフラストラクチャで NetApp Console の自律コントロールプレーンをホストして実行できます。

統合ストレージ管理、ポリシー適用、フリート規模の自動化、AI支援による運用を実現します。データ、メタデータ、管理トラフィックは、お客様の環境外には一切送信されません。

独自のインフラストラクチャに **Console** をデプロイして運用する

NetApp Console ローカルデプロイメントは、お客様自身のインフラストラクチャ内で実行されるため、お客様のチームがデプロイメント、接続性、および日常的な運用を管理できます。Console エージェントをデプロイし、Console 仮想マシンを維持管理し、監視および管理トラフィックに必要なネットワークパスを管理します。これにより、企業管理者は運用境界を完全に制御しながら、管理データを環境内に保持できます。

- "vCenterでOVAを使用してNetApp Consoleのローカルデプロイをインストールします".
- "NetApp Consoleのローカルデプロイ用のvCenterまたはESXiホストのメンテナンス".
- "オンプレミス Console エージェントのポートについては、NetApp Console ローカル展開を参照してください".

APIとサービスアカウントを使用してストレージ操作を自動化する

NetApp Console のローカル展開は API ベースの統合をサポートしているため、組織は反復可能なストレージ操作を自動化できます。サービスアカウントを使用すると、アプリケーションは割り当てられたロールで認証および操作を行うことができます。インタラクティブユーザーに適用されるものと同じロールベースのアクセス制御および監査制御が、これらの操作を管理します。これにより、アクセス範囲を限定して説明責任を維持しながら、エンタープライズの自動化を支援します。

- "メンバーを NetApp Console ローカル展開組織に追加する".
- "NetApp Console IAM の API について"

RBACと**Active Directory**の統合によるアクセス制御

NetApp Console のローカル展開は、ユーザーが管理するフリートやリソース内でユーザーが参照・実行できる内容を制限する、ゼロトラストのロールベースアクセス制御（RBAC）を提供します。Active Directory と統合することで、ユーザーは既存の企業認証情報でサインインできるようになり、ローカルユーザーは多要素認証（MFA）を追加してさらなる検証レイヤーを設けることができます。アクセスガバナンスは、組織の幅広いアイデンティティおよびアクセス管理の実践と整合性を保ちます。

- "NetApp Console ローカル展開におけるアイデンティティとアクセス管理について".
- "NetApp Console ローカル展開への安全なアクセスについて".

フリートを整理してストレージ管理を委任する

NetApp Console のローカル展開では、リソースをフォルダとフリートに整理することで、管理の拡張性を高

めます。フリートを環境、事業部門、または地域にマッピングし、組織、フォルダ、またはフリートのスコープで管理を委任することで、所有権を明確に保つことができます。この構造により、大規模なストレージチームは、ポリシーの一貫性やガバナンスを損なうことなく、作業を分散させることができます。

- "NetApp Console ローカル展開におけるフォルダーとフリートについて".
- "NetApp Console ローカル展開のストレージフリートについて".

コンプライアンスのために管理活動を追跡およびエクスポートする

すべての管理操作は監査レコードを生成します。セキュリティおよびコンプライアンスチームは、これらのレコードを利用して、インシデントの調査、統制の有効性の証明、および監査要件への対応を行うことができます。集中監視、長期保存、および分析のために、Webhookを介して syslog サーバーに監査ログをエクスポートします。NetApp Console のローカルデプロイメントはお客様自身の環境で実行されるため、ログデータがお客様のインフラストラクチャの外部に送信されることはありません。

- "NetApp Consoleのローカル デプロイ アクティビティの監査".

ストレージクラスポリシーに従ってストレージを一貫してプロビジョニングする

NetApp Console のローカル展開では、ストレージクラス（パフォーマンス、容量、階層化ポリシーを再利用可能な定義にまとめたテンプレート）を通じて、一貫したストレージ動作が適用されます。管理者はストレージ基準を一度定義します。管理者と自動化されたワークフローは、承認されたクラスを使用して、環境全体におけるすべてのプロビジョニング活動を実行します。これにより、構成のずれを防ぎ、経験の浅い管理者がプロビジョニングの決定に費やす時間を短縮し、すべてのワークロードが組織の基準を即座に満たすことが保証されます。プロビジョニング後、Console のローカル展開は、各ワークロードのコンプライアンスを継続的に監視します。

- "NetApp Console ローカル展開によるストレージ管理について".

ストレージクラスのコンプライアンスを監視し、ドリフトを自動的に修復します

NetApp Console のローカルデプロイメントは、プロビジョニングに使用されたストレージクラスに対して、すべてのワークロードを監視します。ワークロードが、クラスタ構成の直接的な変更やパフォーマンスの低下によって変動する場合、NetApp Console のローカルデプロイメントは違反を即座に検出します。管理者は、ガイド付きの修復手順に従うか、自動修復を設定することで、手動による介入なしに一般的なドリフト状態を解決できます。この継続的な実施により、監査リスクが軽減され、定期監査の間も環境がコンプライアンス状態を維持できます。

ストレージの状態を監視し、複数のフリートにわたるアラートを受信する

NetApp Console のローカルデプロイメントでは、管理するすべてのクラスターの状態とパフォーマンスを単一の場所で監視できます。フリート全体のダッシュボードには、注意が必要なクラスターとボリュームが表示されます。カスタムダッシュボードを使用すると、管理者は自身の責任範囲に合った監視ビューを作成できます。ワークロードアナライザーは、レイテンシ、スループット、リソース使用率、構成変更を時系列で相関分析し、問題がワークロードに影響を与える前に根本原因を特定するのに役立ちます。

状況が変化した際に適切なチームにアラートが届くよう、メールとWebhookの配信チャネルを設定してください。組織管理者が宛先を設定し、ストレージ管理者がアラートルールにそれらを適用することで、応答パスが運用モデルに一致するようにします。これにより、企業チームは容量、パフォーマンス、および保護に関するイベントに迅速に対応できるようになります。

- "NetApp Console ローカル展開におけるストレージの健全性監視について".
- "NetApp Console ローカル展開で通知配信チャネルを設定する".
- "NetApp Console ローカル展開でアラートの通知ルールを設定する".

自然言語でストレージをプロビジョニングし、アラートを調査する

NetApp Console ローカル展開では、独自の大規模言語モデル（LLM）に接続して、AI支援によるストレージ管理を提供できます。ワークロードを平易な言葉で説明することで、プロビジョニングプランを取得したり、Console にアクティブなアラートの調査を依頼したり、ストレージ環境に関する状況に応じた回答を得たりすることができます。すべての AI アクションは、ストレージクラスのガードレールおよびお客様のアカウントに適用されるロールベースのアクセス制御の範囲内に留まり、機密性の高い操作を実行する前に確認が必要です。Console ローカル展開では、管理者が設定した LLM エンドポイントにのみリクエストが送信されます。

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

NetApp Backup and Recoveryを使用したストレージのバックアップとリストア

プロビジョニングとモニタリングにとどまらず、NetApp Console のローカル展開により NetApp Backup and Recovery へのアクセスが可能になり、同じインターフェースからデータを保護できます。データのバックアップとリストアを実行することで、保護とリカバリの要件を満たすことができます。ストレージと並行してデータ保護を管理することで、ガバナンスの一貫性が保たれ、チームが業務を遂行するために必要なツールの数を削減できます。

- "NetApp Console ローカル展開のデータサービスについて".

NetApp Console ローカル展開のIDとアクセス管理について

NetApp Consoleのローカル展開におけるIDとアクセス管理（IAM）では、サインインできるユーザー、IDの検証方法、ユーザーがアクセスできるリソース、およびユーザーが実行できるアクションを制御します。NetApp Consoleのローカル展開において、IAMには、ロールベースのアクセス制御（RBAC）、多要素認証（MFA）、ディレクトリベースの認証のほか、委任管理をサポートする階層モデルおよび監査モデルが含まれます。

このページでは、NetApp Console のローカル展開における IAM モデルの概要を説明します。詳細な階層計画の例については、"NetApp Console ローカル展開におけるフォルダーとフリートについて"。

NetApp Console で IAM を管理するには、スーパー管理者、組織管理者、または フォルダーまたはフリート管理者 のロールが必要です。

IAMがNetApp Consoleのローカル展開において意味すること

NetApp Console ローカル展開 IAM は、ID 検証、アクセス制御、委任、および監査可能性を統合します：

- 認証は、ユーザーがローカルの認証情報を使用するか、ディレクトリ構成を通じてサインインするかを決定します。
- _認可_は、事前に定義されたロールと、それらを割り当てるスコープに基づいて、メンバーがサインイン後に実行できる操作を決定します。

- 階層とスコープによって、メンバーがアクセスできるフォルダー、フリート、およびリソースが決まります。
- _メンバーと認証情報の管理_では、ユーザーやサービスアカウントを追加する方法、およびMFAとサービスアカウントのシークレットを管理する方法を決定します。
- _監査およびコンプライアンス追跡_は、IAM関連のアクティビティを記録するため、誰がいつアクセス権限を変更したかを確認できます。

認証の仕組み

NetApp Console のローカル展開は、ローカル ID と外部 ID 統合の両方をサポートしています。

NetApp Consoleのローカル展開をActive Directoryと統合することで、ユーザーは既存の企業の資格情報を使用してサインインできるようになります。これにより、Consoleのローカル展開で個別のパスワードを使用する必要がなくなり、管理者はアクセス権を割り当てる際にディレクトリユーザーを検索できるようになります。

ローカルユーザーの場合、MFA は認証情報が漏洩した場合の不正アクセスリスクを軽減するために、追加の認証手順を追加します。

認証と安全なサインインオプションの詳細については、"NetApp Consoleのローカル デプロイにおけるセキュア アクセスについて説明します"。

認可の仕組み

ユーザーがサインインした後、NetApp Console のローカル展開では、RBAC を使用して、そのユーザーが何を表示および実行できるかを決定します。

認証はActive DirectoryまたはLDAPとの連携によって処理されます。NetApp Consoleのローカル展開における認可は別個のものであり、管理者は組織、フォルダ、またはフリートレベルで事前定義されたロールを割り当てて、各メンバーがアクセスできる内容を制御します。

同じロールであっても、割り当てるスコープによって有効なアクセス権限は異なります。このモデルでは、中央管理者には広範なアクセス権限を付与しつつ、地域管理者やチームレベルの管理者にはそれぞれが管理するフリートへのアクセス権限を制限できます。

組織レベルまたはフォルダレベルで割り当てたロールは、子スコープに継承されます。この継承モデルは、NetApp Console がフォルダとフリート間でアクセス権を委任する方法の重要な部分です。

NetApp は、最小権限の原則に基づいて NetApp Console のローカル展開ロールを設計しており、各ロールにはそのタスクに必要な権限のみが含まれます。

"NetApp Console ローカル展開におけるロールベースのアクセス制御とロール継承について学ぶ".

IAM階層の仕組み

NetApp Console のローカル展開では、階層構造を使用してリソースをグループ化し、アクセス範囲を限定します。最上位に組織があり、その下にフォルダ、次にフリート、そしてそれらのフリートに関連付けられたリソース（サブフォルダを含む場合もあります）が続きます。

この階層構造こそが、権限委譲を可能にするものです。例えば、組織管理者は組織全体にわたるアクセスを管理できますが、フォルダ管理者やフリート管理者は、自身が所有する階層内のリソースとメンバーのみを管理

できます。

NetApp Console IAMは、階層構造を定義する組織コンポーネント、その階層構造内に割り当てられるリソース、そして誰が何にアクセスできるかを制御するメンバーとロールという、3種類のコンポーネントに基づいて構築されています。

役割はこの階層を通じて継承されるため、フォルダとフリートの設計は、各アクセス割り当ての適用範囲に直接影響します。

"組織にフリートを追加する方法について説明します。".

メンバーのセキュリティと認証情報

NetApp Console のローカル展開における IAM には、アカウント作成後のメンバーアクセスを保護するための運用制御機能も含まれています。

ローカルユーザーの場合、管理者はパスワードのリセットを指示したり、MFAを削除または一時的に無効化したり、ローカルユーザーのMFAの動作を確認したりすることで、ユーザーのアクセス回復を支援できます。サービスアカウントの場合、管理者はシークレットが紛失またはローテーションされた場合に認証情報を再作成できます。

これらの制御はIAMの一部です。これは、アクセス権限が最初にどのように割り当てられるかだけでなく、時間の経過とともにIDがどのように安全に維持されるかを決定するためです。

"メンバーのセキュリティを管理する方法を説明します".

IAMアクティビティの監査

NetApp Console のローカル展開における IAM には、アクセス関連のアクティビティを確認およびエクスポートする機能が含まれています。

監査ページからは、メンバーの追加、フリートの作成、リソースの関連付けなど、組織の管理に関連する操作を確認できます。また、監査記録をテナントサービスでフィルタリングしてIAM関連の変更に絞り込んだり、監査ログを外部システムにエクスポートしたりすることもできます。

監査可能性は、IAMの重要な原則です。なぜなら、誰がアクセス権限を変更したか、変更が行われた日時、そして変更が成功したかどうかを検証できるからです。

"NetApp Console のローカル展開アクティビティを監査する方法を学ぶ".

NetApp ConsoleでのIAMの次のステップ

- "NetApp Consoleでのアイデンティティとアクセス管理を開始する"
- "NetApp Consoleのローカル デプロイにおけるセキュア アクセスについて説明します"
- "NetApp Console ローカル展開における RBAC について"
- "コンソールのローカル展開アクティビティを監視または監査する"
- "NetApp Console IAM の API について"

NetApp Console ローカルデプロイにおけるフリート管理について説明します

NetApp Consoleのローカル展開におけるフリート管理とは、ストレージシステムを論理グループに整理することで、一貫したポリシーの適用、アクセス制御、および関連するクラスター全体のヘルス状態の監視を行うプラクティスです。フリート管理を使用すると、各クラスターを個別に管理する代わりに、フリートを共通のリソースプールとして扱い、データストレージの目標をサポートできます。

ストレージ環境が拡大するにつれて、個々のクラスターを管理することは非現実的になります。フリート管理は、関連するシステムを体系的にグループ化し、責任を委任し、すべてのクラスターが同じ基準で運用されるようにすることで、この問題を解決します。

フリート管理が重要な理由

フリート管理は、以下の3つの主要な課題に対処します：

- 抽象化による簡素化 - フリート管理は、個々のストレージインフラストラクチャの管理の複雑さを抽象化します。クラスターごとに設定を行う代わりに、ストレージ環境全体を統一的に管理することで、運用上の負担と意思決定の負担を軽減できます。
- 一貫性と拡張性 - 明確な組織体制がないと、異なるチームが類似のワークロードに対して異なる決定を下し、断片化された構成につながります。フリート管理機能を使用すると、数十ものシステムに同時に標準を適用できるため、新しいワークロードがチームやフリート全体で同じ基準から開始されることが保証されます。
- ガバナンスと管理 - チームが大きくなるにつれて、誰が何を管理できるかについて明確な境界線が必要になります。フリート管理は、組織構造とアクセス制御を通じてこれらの境界を設定し、ストレージに関する決定が統制され、監査可能であることを保証します。

フリートによるリソースの整理方法

組織のリソース階層は、フォルダーとフリートで構成されています。

階層構造とアクセスモデルの詳細については、"NetApp Console ローカル展開におけるフォルダーとフリートについて"を参照してください。

- 組織 - お客様の会社を表す最上位レベル。
- 「フォルダー」：関連するフリートを整理するのに役立ちます。たとえば、リージョンやビジネスユニットごとにフォルダーを作成し、各フォルダー内にフリートを作成できます。フォルダーには、他のフォルダーやフリートを含めることができます。フォルダーレベルでロールを割り当てると、メンバーはそのフォルダー内のすべてのフリートに対してそのロールを継承します。
- フリート - 管理しているストレージシステムをグループ化します。ストレージシステムをフリートに関連付け、メンバーをフリートに割り当てることでアクセス権を付与します。

> フォルダは組織管理ツールであり、組織管理者、フォルダ管理者、フリート管理者などのIAM権限を持たないメンバーには表示されません。メンバーはフォルダではなく、フリートにアクセスします。

一般的なフリート編成パターン

フリートの編成方法は、運用モデルによって異なります。

- 環境別 - 本番環境、開発環境、テスト環境のワークロード用に個別のフリートを作成します。これにより、本番環境のストレージはより厳格なポリシーの下で管理される一方、下位環境ではより高い柔軟性が確保されます。
- 事業部門別 - 財務、エンジニアリング、人事など、特定の部門にサービスを提供するクラスターを専用のフリートにまとめます。そうすることで、他のフリートを公開することなく、その事業部門内のチームメンバーにストレージ管理の責任を割り当てることができます。
- 場所またはデータセンター別 - クラスターが複数のサイトに分散している場合、場所別に整理することで、サイトレベルの健全性を監視したり、地域固有のポリシーを適用したり、サイトごとの容量消費量を追跡したりできます。
- アプリケーション層別 - データベース、ファイル共有、仮想マシンなど、特定の種類のワークロードをホストするクラスターをグループ化することで、そのワークロードタイプに合わせて調整された一貫した標準をフリート全体に適用できます。

フォルダを使用して、さらに整理のレベルを追加します。例えば、地域ごとにフォルダを作成し、各地域フォルダ内に環境ベースのフリートを作成します。

フリート管理がアクセス制御を可能にする方法

フリートとフォルダは、ユーザーアクセスと管理責任の境界として機能します。

- フォルダレベルのアクセス - フォルダレベルで役割を割り当てると、メンバーはそのフォルダ内のすべてのフリートとリソースに対してその役割を継承します。これにより、組織全体へのアクセス権を付与することなく、管理上の責任を委任できます。
- フリートレベルのアクセス - フリートレベルで役割を割り当てると、メンバーはそのフリート内のストレージシステムにのみアクセスできます。これにより、インフラストラクチャの無関係な部分を公開することなく、ストレージ管理をチームメンバーやアプリケーション所有者に委任できます。

コンソールローカル展開では、フリートレベルの健全性とパフォーマンスの監視機能が提供されるため、フリート内のすべてのクラスターの状態を単一のビューで確認し、問題を早期に特定して、ワークロードに影響が出る前に対応できます。

ストレージ管理の仕組み

ストレージ管理とは、ストレージの標準を定義し、それを一貫して適用し、ワークロードが長期にわたって整合性を保つように運用する実践のことです。Console のローカル展開では、これらの標準はストレージクラスポリシーとストレージクラスとして表現され、フリートごとにスコープが設定され、RBAC と監査ログによって管理されるプロビジョニングワークフローを通じて適用されます。

コンソールローカル展開では、4つの概念が1つのワークフローに統合されます：

- *フリート*は、ストレージを管理する範囲を定義します。フリートとは、システムをグループ化することで、アクセスを制御し、標準を一貫して適用し、リソースを単位として管理できるようにするものです。
- *ストレージクラスポリシー*は、再利用可能な構成要素（パフォーマンス、容量、セキュリティ、データ保護）として標準を定義します。
- *ストレージクラス*はワークロードの意図を表します。ストレージクラスとは、1つ以上のポリシーから構

成される、名前付きのテンプレートのことです。

- *プロビジョニングワークフロー*は、ガードレール内でストレージを作成します。ワークフローによって構成決定の方法は異なりますが、いずれの場合もストレージクラスを適用でき、RBACと監査ログによって管理されます。

プロビジョニングのアプローチ

コンソールのローカル展開では、3つのプロビジョニング方式がサポートされており、いずれもRBAC、監査ログ、およびストレージクラス標準によって管理されます。

- 手動プロビジョニング - 対象システムを選択し、構成の詳細を直接指定します。システム選択と構成を明示的に制御する必要がある場合に使用します。
- 自動プロビジョニング - ワークロードの入力値を指定し、必要に応じてストレージクラスを選択します。NetApp Console のローカル展開では、最適な配置が推奨され、クラス駆動型の設定が適用されるため、手動での決定が軽減されます。
- **AI**支援（エージェント型）プロビジョニング - 必要なものを自然言語で説明します。Console のローカル展開では、RBAC とストレージクラスによって制約されたプランが提案され、お客様が確認して承認した後にのみプロビジョニングが実行されます。

次のステップ

- ストレージ規格を理解するには、"NetApp Console ローカル展開におけるストレージクラスとポリシーについて"を参照してください。
- フリートの作成と管理については、"フォルダとフリートを管理する"を参照してください。
- "ストレージを手動でプロビジョニングする"
- "ストレージを自動的にプロビジョニングします"
- "AI支援によるストレージの提供"

NetApp Console ローカル展開におけるストレージクラスとポリシーについて

ストレージクラスとは、ストレージがどのように動作するべきかを定義する、再利用可能なテンプレートです。ストレージクラスを使用してストレージをプロビジョニングする場合、NetApp Console のローカル展開では、管理者がワークロードごとに個別の構成決定を行う必要なく、そのクラスにエンコードされた標準が自動的に適用されます。

ストレージクラスは、ストレージ動作の個々の側面を定義するストレージクラスポリシーに基づいて構築されます。これらを組み合わせることで、組織のストレージ標準を一度設定すれば、それをすべてのシステムで一貫して適用できるようになります。

ストレージクラスポリシーとは

ストレージクラスポリシーは、ストレージの動作の一側面を定義します。ポリシーは、ストレージクラスを作成するために組み合わせる、再利用可能な構成要素です。

一般的なポリシーの種類は以下のとおりです：

- パフォーマンス ポリシー - レイテンシー ターゲット、IOPS、またはスループット要件を定義します。
- 容量ポリシー - プロビジョニングモード、しきい値アラート、または拡張制限を定義します。
- セキュリティポリシー - 暗号化、コンプライアンス、またはアクセス制御の要件を定義します。
- データ保護ポリシー - スナップショットのスケジュール、レプリケーションのターゲット、または保持期間を定義します。

ポリシーは個別に定義し、ストレージクラスを構築する際にそれらを組み合わせます。これにより、複数のクラスで同じパフォーマンス ポリシーを再利用したり、容量ポリシーを 1 か所で更新して、そのポリシーを使用するすべてのクラスにその変更を適用したりすることができます。

ストレージクラスとは

ストレージクラスとは、1つ以上のポリシーから構成される、名前付きのテンプレートのことです。これは、特定の種類のワークロードに対する組織のストレージ標準を表すものです。

例えば、ハイパフォーマンス、高可用性、厳格な保護ポリシーを組み合わせた **Production Database** ストレージクラス、または適度なパフォーマンス、柔軟な容量、基本的な保護ポリシーを組み合わせた **Development File Share** ストレージクラスを作成することができます。

ストレージ管理者は、企業要件を反映させるためにストレージクラスを定義します。プロビジョニング活動は、手動で行う場合でも、ガイド付きワークフローを通じて行う場合でも、自動化によって行う場合でも、管理者が承認したクラスのライブラリからデータを取得します。

ストレージクラスが標準をどのように適用するか

ストレージをプロビジョニングする際は、個々の設定を構成するのではなく、ストレージクラスを選択します。Console のローカル展開では、そのクラスのポリシーを使用して、フリート内のどのクラスターがワークロードをサポートする容量とパフォーマンスの余裕を持っているかを特定し、最適な配置オプションを推奨し、プロビジョニング時にクラス駆動型の設定を自動的に適用します。

プロビジョニング後、NetApp Console のローカルデプロイメントは、各ワークロードをストレージクラスの標準に照らし合わせて継続的に評価します。

ストレージクラスの変更とコンプライアンス

ワークロードがストレージクラスの意図と一致しなくなった場合、Console のローカルデプロイメントは、調査と修復のためにそのワークロードにフラグを立てます。

問題は2つのカテゴリーに分類されます：

- 構成のずれ：ストレージクラスポリシーによって管理されるストレージ設定が、意図した構成と一致しなくなりました。これは、ONTAP クラスターで直接変更が行われた場合、または標準のプロビジョニングワークフロー外で変更が行われた場合に発生する可能性があります。
- パフォーマンス不適合：ワークロードの実行時動作がストレージクラスのパフォーマンス要件を満たさなくなりました（たとえば、QoS 制限付近での持続的な負荷、またはテールレイテンシの増加など）。

分析ビューでは、何が変わったのか、そしてなぜ変わったのかが説明されます。コンプライアンスを回復するために、ガイド付きの是正措置（例えば、**Fix it** など）が利用できる場合があります。一部の修復策はそのまま適用できますが、意図した動作を復元するためにワークロードを別のストレージクラスに調整する必要がある場合もあります。

調査する場所

通常、以下のいずれかの場所からドリフトやコンプライアンス違反を調査できます（利用可能かどうかは、デプロイメントと権限によって異なります）：

- ストレージクラス： ドリフト / コンプライアンス
- アラート： 分析

手順の詳細については、ストレージクラスのずれを修正するを参照してください。

エンドツーエンドのワークフロー

以下の手順では、ストレージクラスを使用して環境内のストレージを標準化および管理するプロセスについて説明します。

1. ストレージクラスポリシーの作成 - ポリシーは、ストレージ動作の個々の側面（パフォーマンス目標、容量設定、セキュリティ要件、データ保護スケジュール）を定義します。ストレージクラスを構築する前に、ポリシーを作成してください。
2. ストレージクラスの作成 - 該当する各カテゴリから1つのポリシーを組み合わせてストレージクラスを作成します。事前定義されたストレージクラスを使用するか、組織の基準に合わせてカスタムのストレージクラスを作成することができます。
3. ストレージクラスをフリートに関連付ける - ストレージクラスを作成したら、プロビジョニングとコンプライアンス監視に使用するフリートに関連付けます。
4. ストレージクラスを使用してストレージをプロビジョニングする - ボリュームまたは LUN をプロビジョニングする際に、個々の設定を構成する代わりにストレージクラスを選択します。Console のローカル展開では、クラスを使用して最適なクラスタ配置を推奨し、クラスで定義された設定でプロビジョニングを行います。
5. ワークロードのずれを監視する - Console のローカル展開では、各ワークロードをストレージクラスにエンコードされた標準と照らし合わせて継続的に評価します。設定のずれやパフォーマンスの不適合が発生した場合、その問題にフラグが付けられ、アラートが発生する可能性があります。
6. ドリフトを修復してコンプライアンスを回復する - ドリフトまたはパフォーマンスの非コンプライアンスが検出された場合、ガイド付き手順に従って問題を手動で修正したり、Console のローカル展開で一般的なドリフト状態を自動的に解決したり、設定を変更する必要がある場合はワークロードをストレージ クラスから切り離したりできます。

ストレージクラスがフリートとどのように連携するか

ストレージクラスはフリートに関連付けられています。ストレージクラスをフリートに関連付けると、そのクラスはフリート内のすべてのプロビジョニングで使用できるようになります。これにより、フリート内でプロビジョニングされるすべてのワークロードが同じ標準に従うことが保証され、フリートは関連するクラスター全体で一貫したストレージ動作を適用するための主要な手段となります。

フリートの整理方法の詳細については、"NetApp Console ローカルデプロイにおけるフリート管理について説明します"を参照してください。

次のステップ

- フリート編成を理解するには、"NetApp Console ローカルデプロイにおけるフリート管理について説明します"を参照してください。

- ポリシーとストレージ クラスを作成するには、"ストレージクラスとポリシーを管理する"を参照してください。
- "ストレージを手動でプロビジョニングする"
- "ストレージを自動的にプロビジョニングします"
- "AI支援によるストレージの提供"
- ドリフトの分析と修正については、"ストレージクラスのずれを修正する"を参照してください。

NetApp Console ローカル展開における LLM 統合について

NetApp Console のローカル展開は、AI支援によるストレージ管理のために、大規模言語モデル（LLM）に接続します。セットアップ後、ユーザーは自然言語を使用してストレージをプロビジョニングしたり、アラートを調査したり、ストレージに関するガイダンスを取得したりできます。

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。

AI支援による管理機能により、ユーザーは平易な言葉でリクエストを記述でき、Console のローカル展開でお客様のストレージポリシーが適用されます。

コンソールローカル展開では、LLMリクエストは設定したエンドポイントにのみ送信されます。

AIを活用したストレージ管理でできること

LLM統合を有効にすると、Console ローカル展開はConsole アシスタントを通じて次の3つの機能を提供します。

- ストレージプロビジョニング ワークロード要件を平易な言葉で説明してください。Console のローカル展開機能は、ストレージクラスに基づいてプロビジョニングプランを推奨し、実行します。
- アラートへの対応 Console のローカルデプロイメントにアクティブなアラートの調査を依頼します。問題を分析し、割り当てられた権限に基づいてアクションを提案または実行します。
- 検索とガイダンス ストレージ環境またはONTAP管理について質問できます。NetApp Console のローカルデプロイメントは、ドキュメントと現在のフリートの状態から状況に応じた回答を返します。

Console アシスタントの読み取り専用または読み取り / 書き込みアクセスを選択する

ユーザーは、望む結果に基づいてアシスタントのアクセスモードを選択します：

- インフラストラクチャの変更を行わずにガイダンスや調査を行うための*読み取り専用*モード。
- ガイド付き実行のための*読み取り / 書き込み*モード。コンソールのローカルデプロイメントでは、提案されたアクションが表示され、確認を求めた後、変更が実行されます。

コンソールアシスタントのアクションを制御するものを理解する

コンソールのローカル展開は、プラットフォーム全体で使用されているのと同じガバナンスモデルを通じて、

コンソールアシスタントのアクションを制御します：

- 役割ベースのアクセス制御は、各ユーザーが見たり実行したりできる内容を制限します。
- ストレージポリシーは、プロビジョニングおよび関連するアクションを制約します。
- コンソールアシスタントは、ストレージを変更する操作を実行する前に確認を求めます。

LLMプロバイダーパスを選択する

NetApp Console のローカル展開では、以下の LLM プロバイダータイプがサポートされます：

- **OpenAI**：OpenAIモデルへの直接アクセス。
- エンタープライズゲートウェイやプロキシサービスなどの互換性のあるエンドポイントに対応した **OpenAI-compatible** 。
- Anthropic の Claude モデル用。

モデルの可用性は、設定するエンドポイントによって異なります。Console のローカルデプロイメントで、リストからモデルを選択してください。

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リクエストの送信先を理解する

データの流れは、選択したエンドポイントパスによって異なります。

- OpenAIエンドポイントを設定すると、コンソールのローカルデプロイメントはプロンプトとコンテキストをOpenAIエンドポイントに送信します。
- OpenAI互換エンドポイントを設定すると、Console のローカルデプロイメントは、組織が設定した互換エンドポイントにプロンプトとコンテキストを送信します。

LLM認証情報を保護し、管理者アクセスを制御する

これらの制御機能を使用して統合を保護します：

- APIキーは特権認証情報として扱い、組織のポリシーに従って定期的に更新してください。
- プロバイダー側の使用状況とアラートを確認し、予期しないアクティビティを検出します。

LLMを接続する

これらの決定を下したら、"LLMを接続してNetApp Consoleアシスタントを有効にする"に進みます。

接続または実行時チェックが失敗した場合は、"LLM統合のトラブルシューティング"を参照してください。

NetApp Console ローカル展開における NetApp Backup and Recovery について

NetApp Backup and Recovery は、ボリューム、データベース、仮想マシ

ン、Kubernetes ワークロードなど、すべての ONTAP ワークロードに対して効率的で安全かつ対費用効果の高いデータ保護を提供するデータサービスです。

ワークロードとは、システム内のリソースを論理的にグループ化したものであり、保護、ガバナンス、検出、および復旧のために単一の単位として管理されます。Backup and Recoveryにおいて、ワークロードとは保護対象となる単位のことです。その意味はデータソースによって異なります：Kubernetesの場合、ワークロードはアプリケーションであり、VM環境の場合は仮想マシンであり、データベース環境の場合はデータベースです。

バックアップとリカバリのサポートは、すべての ONTAP システムにすでに組み込まれているため、追加のハードウェアやメディアゲートウェイは不要です。これにより、バックアップ作業がシンプルになり、コスト効率も向上します。NetApp Console を使用すると、複数のリソースマネージャや専門の担当者を必要とせずに、3-2-1 バックアップのすべてのバリエーションを含む、あらゆるバックアップ戦略の実装を簡素化できます。

NetApp Backup and Recovery は NetApp Console ローカル展開のプレビューモードです。本サービスはまだ一般提供されておらず、機能は変更される可能性があります。

"NetApp Backup and Recovery の詳細をご確認ください。".

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。