



基本を学ぶ

NetApp Console setup and administration

NetApp

February 09, 2026

目次

基本を学ぶ	1
NetApp Consoleについて学ぶ	1
集中ストレージ管理	1
データの保護、セキュリティ確保、最適化のための統合データサービスとストレージ管理	2
サポートされているクラウドプロバイダー	3
料金	3
NetApp Consoleの仕組み	3
SOC 2 タイプ2認証	4
NetApp Consoleの導入モードについて学ぶ	4
概要	5
標準モード	6
制限モード	7
サービスと機能の比較	10
NetApp Consoleに関連付けられたNSS資格情報を管理する	11
概要	12
NSSアカウントを追加する	12
NSSクレデンシャルの更新	13
システムを別のNSSアカウントに接続する	13
NSSアカウントのメールアドレスを表示する	14
NSSアカウントを削除する	14
NetApp Consoleエージェントについて学ぶ	15
コンソールエージェントは常に動作している必要があります	17
サポートされている場所	17
クラウドプロバイダーとのコミュニケーション	17
制限モード	17
コンソールエージェントのインストール方法	18
クラウドプロバイダーの権限	18
エージェントのアップグレード	18
オペレーティングシステムとVMのメンテナンス	19
複数のシステムとエージェント	19
NetApp Consoleのアイデンティティとアクセス管理について学ぶ	19
アイデンティティおよびアクセス管理コンポーネント	20
IAM戦略の例	22
NetApp ConsoleでのIAMの次のステップ	24

基本を学ぶ

NetApp Consoleについて学ぶ

コンソールは、統合データ サービスを使用してハイブリッド マルチクラウド全体のストレージ管理と保護を統合し、データを保護および最適化します。

これは、サービス (SaaS) プラットフォームとして、または独自のクラウドにインストールできるセルフホスト オプションとして利用できます。ストレージ管理、データの移動、データ保護、データ分析と制御を提供します。管理機能は、Webベースのコンソールと API を通じて提供されます。

集中ストレージ管理

コンソールを使用して、クラウドおよびオンプレミスのストレージを検出、展開、管理します。

サポートされているクラウドおよびオンプレミスのストレージ

コンソールから次の種類のストレージを管理できます。

クラウドストレージソリューション

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

オンプレミスのフラッシュとオブジェクトストレージ

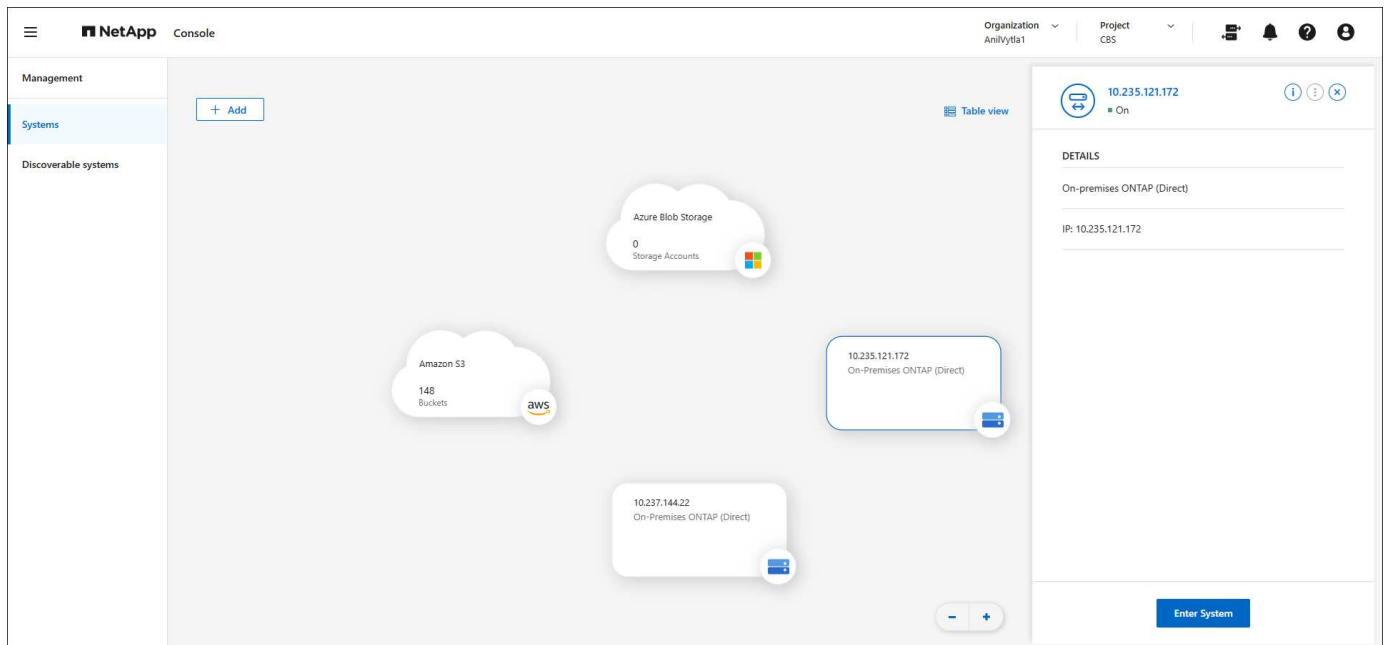
- Eシリーズシステム
- ONTAPクラスタ
- StorageGRIDシステム

クラウドオブジェクトストレージ

- Amazon S3 ストレージ
- Azure BLOB ストレージ
- Google Cloud Storage

ストレージ管理

コンソール内では、システム は検出または展開されたストレージを表します。システムを選択して、NetApp データ サービスと統合したり、ボリュームの追加などのストレージを管理したりできます。



データの保護、セキュリティ確保、最適化のための統合データサービスとストレージ管理

コンソールは、ストレージの可用性を確保し維持するためのデータ サービスを提供します。

ストレージアラート

ONTAP環境の容量、可用性、パフォーマンス、保護、セキュリティに関連する問題を表示します。

自動化ハブ

スクリプト ソリューションを使用して、NetApp製品とサービスの導入と統合を自動化します。

NetApp Backup and Recovery

クラウドとオンプレミスのデータをバックアップおよび復元します。

NetApp Data Classification

アプリケーション データとクラウド環境のプライバシーを準備します。

NetApp Copy and Sync

オンプレミスとクラウド データ ストア間でデータを同期します。

NetAppデジタルアドバイザー (Active IQ)

予測分析とプロアクティブなサポートを使用して、データ インフラストラクチャを最適化します。

Licenses and subscriptions

ライセンスとサブスクリプションを管理および監視します。

NetApp Disaster Recovery

VMware Cloud on Amazon FSx for ONTAPを災害復旧サイトとして使用して、オンプレミスの VMware ワークロードを保護します。

ライフサイクルプランニング

現在または予測される容量が低いクラスターを特定し、データ階層化または追加容量の推奨事項を実装します。

NetApp Ransomware Resilience

ランサムウェア攻撃につながる可能性のある異常を検出します。ワークロードを保護および回復します。

NetApp Replication

バックアップと災害復旧をサポートするために、ストレージ システム間でデータを複製します。

ソフトウェアアップデート

ONTAPアップグレードの評価、計画、実行を自動化します。

サステナビリティダッシュボード

ストレージ システムの持続可能性を分析します。

NetApp Cloud Tiering

オンプレミスのONTAPストレージをクラウドに拡張します。

NetApp Volume Caching

書き込み可能なキャッシュ ボリュームを作成して、データへのアクセスを高速化したり、頻繁にアクセスされるボリュームのトラフィックを軽減したりします。

NetAppワークロード

Amazon FSx for NetApp ONTAPを使用して主要なワークロードを設計、セットアップ、運用します。

["NetApp Consoleと利用可能なデータサービスの詳細"](#)

サポートされているクラウドプロバイダー

コンソールを使用すると、クラウド ストレージを管理し、Amazon Web Services、Microsoft Azure、Google Cloud のクラウド サービスを使用できます。

料金

NetApp Consoleは無料です。クラウドにコンソール エージェントを展開したり、クラウドに展開された制限モードを使用したりする場合は、コストが発生します。一部のNetAppデータ サービスにはコストがかかります。<https://bluexp.netapp.com/pricing/>["NetAppデータサービスの価格について"]

NetApp Consoleの仕組み

NetApp Consoleは、SaaS レイヤー、リソースおよびアクセス管理システム、ストレージ システムを管理してNetAppデータ サービスを有効にするコンソール エージェント、およびビジネス要件を満たすさまざまな導入モードを通じて提供される Web ベースのコンソールです。

サービスとしてのソフトウェア

コンソールにアクセスするには ["ウェブベースのインターフェース"](#)およびAPI。この SaaS エクスペリエンスにより、最新機能がリリースされると自動的にアクセスできるようになります。

アイデンティティとアクセス管理 (IAM)

コンソールは、リソースとアクセス管理のための ID およびアクセス管理 (IAM) を提供します。この IAM モデルは、リソースと権限のきめ細かな管理を提供します。

- トップレベルの組織を使用すると、さまざまなプロジェクト間のアクセスを管理できます。
- `_フォルダ_`を使用すると、関連するプロジェクトをグループ化できます
- リソース管理では、リソースを1つ以上のフォルダまたはプロジェクトに関連付けることができます。
- アクセス管理により、組織階層のさまざまなレベルのメンバーに役割を割り当てることができます。
- ["NetApp ConsoleのIAMの詳細"](#)

コンソールエージェント

いくつかの追加機能およびデータ サービスには、コンソール エージェントが必要です。オンプレミスとクラウド環境全体のリソースとプロセスを管理できます。一部のシステム (Cloud Volumes ONTAPなど) を管理し、一部のNetAppデータ サービスを使用するために必要です。

["コンソールエージェントの詳細"](#)。

SaaS とソブリンクラウドの展開

NetApp Consoleの使用を開始するには、SaaS オファリングにサインアップするか、独自のクラウドに導入します。NetApp Consoleをソブリン クラウドに導入すると、 NetApp は組織のセキュリティとコンプライアンスの要件を満たすためにアウトバウンド接続を制限します。コンソールがソブリン クラウドにデプロイされている場合、すべての機能とサービスが利用できるわけではありません。

NetApp は、アウトバウンド接続を望まないサイト向けにBlueXP を引き続き提供します。BlueXP は、アウトバウンド接続なしでネットワークにインストールできます。 ["インターネットに接続できないサイト向けのBlueXP \(プライベート モード\) について説明します。"](#)

["展開モードの詳細"](#)。

SOC 2 タイプ2認証

独立した公認会計士事務所とサービス監査人がコンソールを検査し、該当する Trust Services 基準に基づいて SOC 2 タイプ 2 レポートを達成したことを確認しました。

["NetAppのSOC 2レポートを見る"](#)

NetApp Consoleの導入モードについて学ぶ

NetApp Consoleは、ビジネス要件とセキュリティ要件を満たす複数の 導入モード を提供します。

- 標準モード では、サービスとしてのソフトウェア (SaaS) レイヤーを活用して完全な機能を提供します。ユーザーはWebベースのホストインターフェースを通じてコンソールにアクセスします。
- 制限モード は、接続制限があり、 NetApp Consoleを独自のパブリック クラウドにインストールしたい組織で利用できます。ユーザーは、クラウド環境内のコンソール エージェントでホストされている Web ベースのインターフェースを通じてコンソールにアクセスします。

NetApp Consoleは制限モードでトラフィック、通信、データを制限するため、環境 (オンプレミスおよびクラウド) が必要な規制に準拠していることを確認する必要があります。

概要

各展開モードでは、アウトバウンド接続、場所、インストール、認証、データ サービス、課金方法が異なります。

標準モード

Web ベースのコンソールから SaaS サービスを使用します。使用する予定のデータ サービスと機能に応じて、コンソール組織管理者は、ハイブリッド クラウド環境内のデータを管理するための 1 つ以上のコンソール エージェントを作成します。

このモードでは、パブリックインターネット経由で暗号化されたデータ転送が使用されます。

制限モード

コンソール エージェントをクラウド (政府、主権、または商業地域) にインストールし、NetApp ConsoleSaaS レイヤーへの送信接続が制限されます。

このモードは通常、州政府や地方自治体、規制対象企業によって使用されます。

[SaaS レイヤーへのアウトバウンド接続の詳細。](#)

BlueXPプライベート モード (従来のBlueXPインターフェイスのみ)

BlueXPプライベート モード (レガシーBlueXPインターフェイス) は通常、インターネット接続がなく、AWS Secret Cloud、AWS Top Secret Cloud、Azure IL6 などの安全なクラウド領域があるオンプレミス環境で使用されます。NetApp は、従来のBlueXPインターフェイスを使用してこれらの環境を引き続きサポートします。["BlueXPプライベートモードの PDF ドキュメント"](#)

次の表は、NetAppコンソールの比較を示しています。

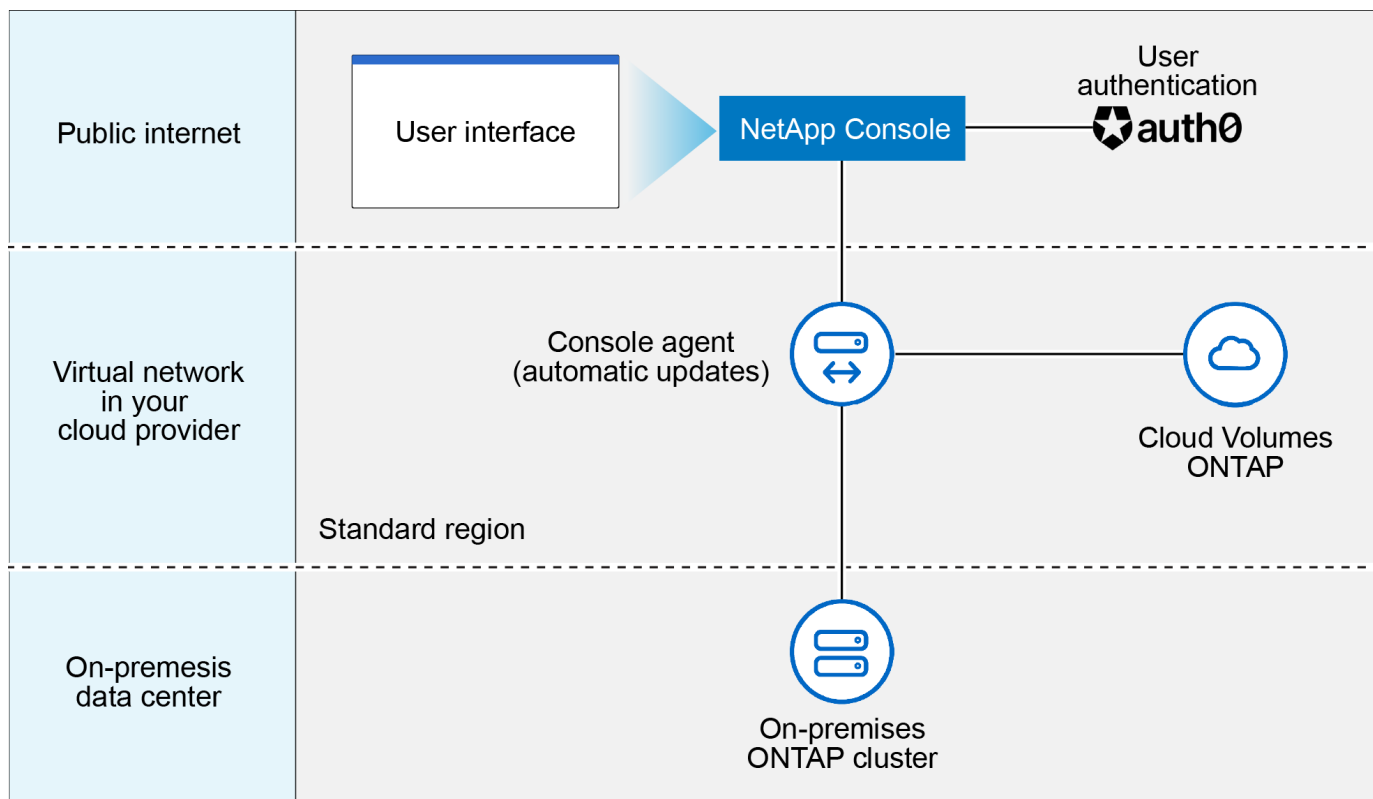
	標準モード	制限モード
NetApp ConsoleSaaS レイヤーへの接続が必要ですか?	はい	発信のみ
クラウド プロバイダー への接続が必要ですか?	はい	はい、地域内です
コンソールエージェント のインストール	コンソール、クラウドマーケットプレイス、または手動インストールから	クラウドマーケットプレイスまたは手動インストール
コンソールエージェント のアップグレード	自動アップグレード	自動アップグレード
UI アクセス	コンソールSaaSレイヤーから	エージェントVMからローカルに
API エンドポイント	コンソールSaaSレイヤー	コンソールエージェント
認証	auth0、NSSログイン、またはIDフェデレーションを使用したSaaS経由	auth0またはIDフェデレーションを使用したSaaSを通じて
多要素認証	ローカルユーザーが利用可能	使用不可

	標準モード	制限モード
ストレージおよびデータサービス	すべてサポートされています	多くが支持されている
データサービスライセンスオプション	マーケットプレースのサブスクリプションとBYOL	マーケットプレースのサブスクリプションとBYOL

サポートされているNetApp Consoleの機能とサービスなど、これらのモードの詳細については、次のセクションをお読みください。

標準モード

次の画像は標準モードの展開の例です。



コンソールは標準モードでは次のように動作します。

アウトバウンドコミュニケーション

コンソール エージェントからコンソール SaaS レイヤー、クラウド プロバイダーの公開リソース、および日常の運用に不可欠なその他のコンポーネントへの接続が必要です。

- "AWS でエージェントが接続するエンドポイント"
- "Azure でエージェントが接続するエンドポイント"
- "Google Cloud でエージェントが接続するエンドポイント"

エージェントがサポートされる場所

標準モードでは、エージェントはクラウドまたはオンプレミスでサポートされます。

コンソールエージェントのインストール

次のいずれかの方法でエージェントをインストールできます。

- コンソールから
- AWS または Azure Marketplace から
- Google Cloud SDKから
- データセンターまたはクラウド内の Linux ホストでインストーラーを手動で使用する
- 提供された OVA を VCenter 環境で使します。

コンソールエージェントのアップグレード

NetApp はエージェントを毎月自動的にアップグレードします。

ユーザーインターフェースアクセス

ユーザー インターフェイスには、SaaS レイヤーを通じて提供される Web ベースのコンソールからアクセスできます。

APIエンドポイント

API呼び出しは次のエンドポイントに対して行われます: <https://api.bluedp.netapp.com>

認証

auth0 またはNetAppサポート サイト (NSS) ログインによる認証。アイデンティティ連携が利用可能です。

サポートされているデータサービス

すべてのNetAppデータ サービスがサポートされています。"[NetAppデータサービスの詳細](#)"。

サポートされているライセンスオプション

マーケットプレースのサブスクリプションと BYOL は標準モードでサポートされていますが、サポートされるライセンス オプションは使用しているNetAppデータ サービスによって異なります。利用可能なライセンス オプションの詳細については、各サービスのドキュメントを確認してください。

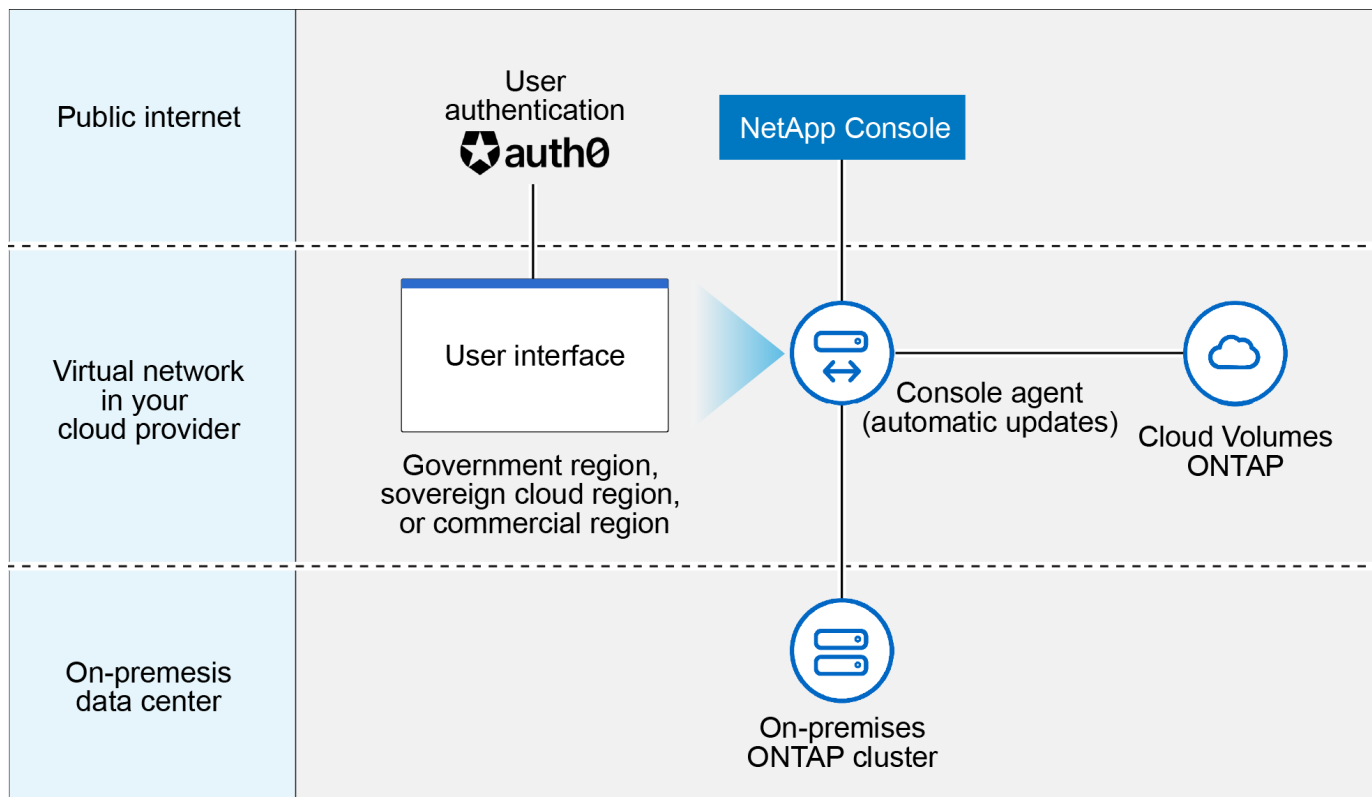
標準モードの開始方法

に行く "[NetApp Console](#)"そしてサインアップしてください。

"[標準モードの開始方法を学ぶ](#)"。

制限モード

次の画像は、制限モードの展開の例です。



制限モードではコンソールは次のように動作します。

アウトバウンドコミュニケーション

エージェントは、データ サービス、ソフトウェア アップグレード、認証、メタデータの転送のために、コンソール SaaS レイヤーへの送信接続を必要とします。

コンソール SaaS レイヤーはエージェントへの通信を開始しません。エージェントは、コンソール SaaS レイヤーとのすべての通信を開始し、必要に応じてデータをプルまたはプッシュします。

リージョン内からクラウド プロバイダー リソースへの接続も必要です。

エージェントがサポートされる場所

制限モードでは、エージェントはクラウド（政府リージョン、主権リージョン、または商用リージョン）でサポートされます。

コンソールエージェントのインストール

AWS または Azure Marketplace からインストールすることも、独自の Linux ホストに手動でインストールすることも、VCenter 環境でダウンロード可能な OVA を使用することもできます。

コンソールエージェントのアップグレード

NetApp は、毎月のアップデートでエージェント ソフトウェアを自動的にアップグレードします。

ユーザーインターフェースアクセス

ユーザー インターフェースには、クラウド リージョンにデプロイされたエージェント仮想マシンからアクセスできます。

APIエンドポイント

API 呼び出しはエージェント仮想マシンに対して行われます。

認証

認証は auth0 を通じて提供されます。アイデンティティフェデレーションも利用可能です。

サポートされているストレージ管理およびデータサービス

制限モードの次のストレージおよびデータ サービス:

サポートされているサービス	注記
Azure NetApp Files	完全サポート
バックアップとリカバリ	制限モードの政府地域および商用地域でサポートされます。制限モードの主権地域ではサポートされません。制限モードでは、NetApp Backup and Recovery はONTAPボリューム データのみのバックアップと復元をサポートします。"ONTAPデータのサポートされているバックアップ先のリストを表示します"アプリケーション データおよび仮想マシンデータのバックアップと復元はサポートされていません。
NetApp Data Classification	制限モードの政府地域でサポートされます。商用地域または制限モードのソブリン地域ではサポートされません。
Cloud Volumes ONTAP	完全サポート
Licenses and subscriptions	制限モードでサポートされている以下のライセンス オプションを使用して、ライセンスおよびサブスクリプション情報にアクセスできます。
オンプレミスのONTAPクラスター	コンソール エージェントを使用した検出とコンソール エージェントを使用しない検出 (直接検出) の両方がサポートされています。コンソール エージェントなしでオンプレミス クラスターを検出する場合、詳細ビュー (システム マネージャー) はサポートされません。
レプリケーション	制限モードの政府地域でサポートされます。商用地域または制限モードのソブリン地域ではサポートされません。

サポートされているライセンスオプション

制限モードでは、次のライセンス オプションがサポートされています。

- マーケットプレイスのサブスクリプション (時間単位および年間契約)

次の点に注意してください。

- Cloud Volumes ONTAPの場合、容量ベースのライセンスのみがサポートされます。
- Azure では、政府地域では年間契約はサポートされていません。

- BYOL

Cloud Volumes ONTAPの場合、容量ベースのライセンスとノードベースのライセンスの両方が BYOL でサポートされます。

制限モードの開始方法

NetApp Console組織を作成するときに、制限モードを有効にする必要があります。

まだ組織がない場合は、手動でインストールした、またはクラウド プロバイダーのマーケットプレイスから作成したコンソール エージェントから初めてコンソールにログインするときに、組織を作成して制限モードを有効にするように求められます。



組織を作成した後は、制限モード設定を変更することはできません。

["制限モードの開始方法を学ぶ"](#)。

サービスと機能の比較

次の表は、制限モードでサポートされているサービスと機能をすぐに識別するのに役立ちます。

一部のサービスは制限付きでサポートされる場合がありますのでご了承ください。これらのサービスが制限モードでどのようにサポートされるかの詳細については、上記のセクションを参照してください。

製品分野	NetAppデータサービスまたは機能	制限モード
ストレージ 表のこの部分には、コンソールからのストレージ システム管理のサポートがリストされています。 NetApp Backup and Recoveryでサポートされているバックアップ先は示されません。	Amazon FSx for ONTAP	いいえ
	Amazon S3	いいえ
	Azure ブロブ	いいえ
	Azure NetApp Files	はい
	Cloud Volumes ONTAP	はい
	Google Cloud NetApp Volumes	いいえ
	Google Cloud Storage	いいえ
	オンプレミスのONTAPクラスタ	はい
	Eシリーズ	いいえ
	StorageGRID	いいえ

製品分野	NetAppデータサービスまたは機能	制限モード
データサービス	NetAppバックアップとリカバリ	はい https://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-limited-internet-connectivity ["ONTAPボリュームデータのサポートされているバックアップ先のリストを表示します"]
	NetApp Data Classification	はい
	NetApp Copy and Sync	いいえ
	NetApp Disaster Recovery	いいえ
	NetApp Ransomware Resilience	いいえ
	NetApp Replication	はい
	NetApp Cloud Tiering	いいえ
	NetAppボリュームキャッシュ	いいえ
	NetAppワークロード ファクトリー	いいえ
特徴	アラート	いいえ
	Digital Advisor	いいえ
	ライセンスとサブスクリプションの管理	はい
	アイデンティティとアクセス管理	はい
	Credentials	はい
	フェデレーション	はい
	ライフサイクルプランニング	いいえ
	多要素認証	はい
	NSSアカウント	はい
	通知	はい
	検索	はい
	ソフトウェアアップデート	いいえ
	持続可能性	いいえ
	監査	はい

NetApp Consoleに関連付けられたNSS資格情報を管理する

ストレージ管理の主要なワークフローを有効にするには、NetAppサポート サイト アカウントをコンソール組織に関連付けます。これらの NSS 認証情報は組織全体に関連付けられています。

コンソールでは、ユーザー アカウントごとに 1 つの NSS アカウントに関連付けることもサポートされています。

す。"ユーザーレベルの資格情報を管理する方法を学ぶ"。

概要

次のタスクを有効にするには、NetAppサポート サイトの資格情報を特定のコンソール アカウントのシリアル番号に関連付ける必要があります。

- BYOL（個人ライセンス使用）時にCloud Volumes ONTAP を導入する

コンソールがライセンス キーをアップロードし、購入した期間のサブスクリプションを有効にするには、NSS アカウントを提供する必要があります。これには、期間更新の自動更新が含まれます。

- 従量課金制のCloud Volumes ONTAPシステムの登録

システムのサポートを有効にし、NetAppテクニカル サポート リソースにアクセスするには、NSS アカウントを提供する必要があります。

- Cloud Volumes ONTAPソフトウェアを最新リリースにアップグレードする

これらの資格情報は、特定のコンソール アカウントのシリアル番号に関連付けられています。ユーザーは、サポート > **NSS 管理** からこれらの資格情報にアクセスできます。

NSSアカウントを追加する

コンソール内のサポート ダッシュボードから、コンソールで使用するNetAppサポート サイト アカウントを追加および管理できます。

NSS アカウントを追加すると、コンソールはライセンスのダウンロード、ソフトウェア アップグレードの検証、将来のサポート登録などにこの情報を使用します。

組織に複数の NSS アカウントを関連付けることはできますが、同じ組織内に顧客アカウントとパートナー アカウントを持つことはできません。



NetApp は、サポートとライセンスに固有の認証サービスの ID プロバイダーとして Microsoft Entra ID を使用します。

手順

1. 管理 > サポート。
2. *NSS管理*を選択します。
3. *NSS アカウントの追加*を選択します。
4. *続行*を選択すると、Microsoft ログイン ページにリダイレクトされます。
5. ログイン ページで、NetAppサポート サイトに登録した電子メール アドレスとパスワードを入力します。

ログインが成功すると、NetApp はNSS ユーザー名を保存します。

これは、メールにマッピングされるシステム生成の ID です。*NSS管理*ページでは、... メニュー。

- ログイン認証トークンを更新する必要がある場合は、... メニュー。

このオプションを使用すると、再度ログインするよう求められます。これらのアカウントのトークンは 90 日後に期限切れになることに注意してください。これを知らせる通知が投稿されます。

次の手順

ユーザーは、新しいCloud Volumes ONTAPシステムを作成するとき、および既存のCloud Volumes ONTAPシステムを登録するときにアカウントを選択できるようになりました。

- ["AWS でCloud Volumes ONTAP を起動"](#)
- ["Azure でCloud Volumes ONTAP を起動する"](#)
- ["Google Cloud でCloud Volumes ONTAP を起動"](#)
- ["従量課金制システムの登録"](#)

NSSクレデンシャルの更新

セキュリティ上の理由から、NSS 認証情報は 90 日ごとに更新する必要があります。NSS 認証情報の有効期限が切れた場合は、コンソールの通知センターで通知されます。["通知センターについて学ぶ"](#)。

資格情報の有効期限が切れると、次のような問題が発生する可能性があります (ただし、これらに限定されません)。

- ライセンスが更新され、新しく購入した容量を利用できなくなります。
- サポートケースを送信および追跡する機能。

さらに、組織に関連付けられている NSS アカウントを変更する場合は、組織に関連付けられている NSS 資格情報を更新することもできます。たとえば、NSS アカウントに関連付けられている人物が退職した場合などです。

手順

1. 管理 > サポート。
2. *NSS管理*を選択します。
3. 更新したいNSSアカウントについては、...次に、[資格情報の更新]を選択します。
4. プロンプトが表示されたら、[続行] を選択して、Microsoft ログイン ページにリダイレクトします。

NetApp は、サポートおよびライセンスに関連する認証サービスの ID プロバイダーとして Microsoft Entra ID を使用します。

5. ログイン ページで、NetAppサポート サイトに登録した電子メール アドレスとパスワードを入力します。

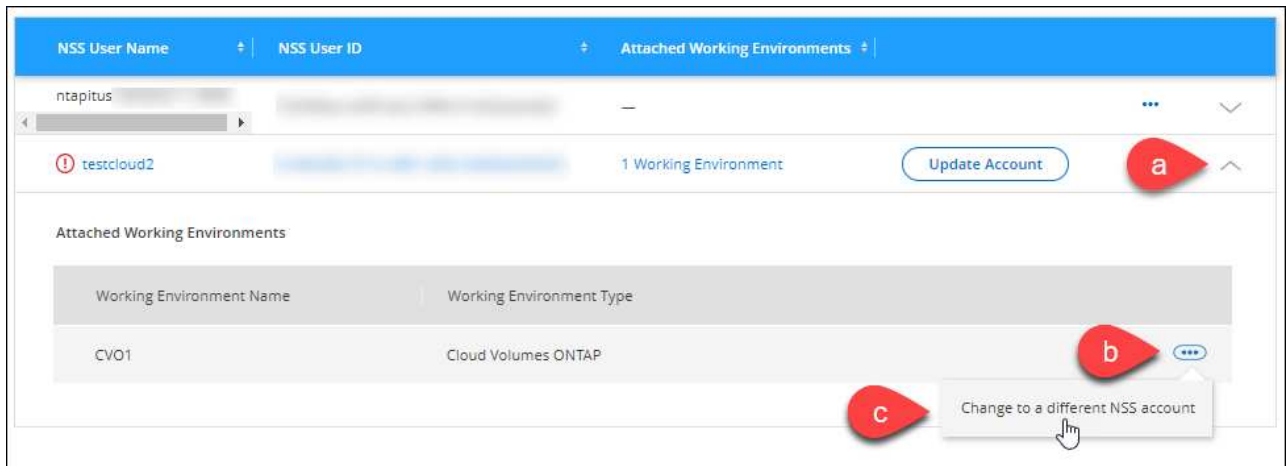
システムを別のNSSアカウントに接続する

組織に複数のNetAppサポート サイト アカウントがある場合は、Cloud Volumes ONTAPシステムに関連付けるアカウントを変更できます。

まずアカウントをコンソールに関連付ける必要があります。

手順

1. 管理 > サポート。
2. *NSS管理*を選択します。
3. NSS アカウントを変更するには、次の手順を実行します。
 - a. システムが現在関連付けられているNetAppサポート サイト アカウントの行を展開します。
 - b. 関連付けを変更するシステムについては、...
 - c. *別のNSSアカウントに変更*を選択します。



- d. アカウントを選択し、[保存]を選択します。

NSSアカウントのメールアドレスを表示する

セキュリティ上の理由から、NSS アカウントに関連付けられた電子メール アドレスはデフォルトでは表示されません。NSS アカウントの電子メール アドレスと関連付けられたユーザー名を表示できます。



NSS 管理ページに移動すると、コンソールはテーブル内の各アカウントに対してトークンを生成します。そのトークンには、関連付けられた電子メール アドレスに関する情報が含まれます。ページを離れるとトークンは削除されます。情報はキャッシュされないため、プライバシーが保護されます。

手順

1. 管理 > サポート。
2. *NSS管理*を選択します。
3. 更新したいNSSアカウントについては、...次に、[メールアドレスを表示]を選択します。コピーボタンを使用してメールアドレスをコピーできます。

NSSアカウントを削除する

コンソールで使用なくなった NSS アカウントを削除します。

現在Cloud Volumes ONTAPシステムに関連付けられているアカウントは削除できません。まず最初にこれらのシステムを別のNSSアカウントに接続する。

手順

1. 管理 > サポート。
2. *NSS管理*を選択します。
3. 削除したいNSSアカウントについては、...次に、[削除] を選択します。
4. *削除*を選択して確認します。

NetApp Consoleエージェントについて学ぶ

コンソール エージェントを使用して、 NetApp Consoleをインフラストラクチャに接続し、AWS、Azure、Google Cloud、オンプレミス環境全体でストレージ ソリューションを安全にオーケストレーションし、データ保護サービスを使用します。

コンソール エージェントを使用すると、次のことが可能になります。

- Cloud Volumes ONTAP のプロビジョニング、ストレージ ボリュームの設定、データ分類の使用など、NetApp Consoleからストレージ管理タスクを調整します。
- サブスクリプション課金統合のためにクラウドプロバイダーのIAMロールを使用して認証する
- 高度なデータ サービス (NetApp Backup and Recovery、 NetApp Disaster Recovery、 NetApp Ransomware Resilience、 NetApp Cloud Tiering) を使用する
- コンソールを制限モードで使用します。

高度なオーケストレーションやデータ保護が必要ない場合は、エージェントを導入せずに、オンプレミスのONTAPクラスターとクラウドネイティブ ストレージ サービスを一元管理できます。監視およびデータ移動ツールも利用できます。

次の表は、コンソール エージェントの有無にかかわらず使用できる機能とサービスを示しています。

	エージェントで利用可能	エージェントなしで利用可能
サポートされているストレージ システム:		
Amazon FSx for ONTAP	はい (検出および管理機能)	はい (検出のみ)
Amazon S3 ストレージ	はい	いいえ
Azure BLOB ストレージ	はい	はい
Azure NetApp Files	はい	はい
Cloud Volumes ONTAP	はい	いいえ
Eシリーズシステム	はい	いいえ
Google Cloud NetApp Volumes	はい	はい

	エージェントで利用可能	エージェントなしで利用可能
Google Cloud ストレージ バケット	はい	いいえ
StorageGRIDシステム	はい	いいえ
オンプレミスのONTAPクラスタ（高度な管理と検出）	はい（高度な管理と検出）	いいえ（基本的な検出のみ）
利用可能なストレージ管理サービス:		
アラート	はい	いいえ
自動化ハブ	はい	はい
Digital Advisor（Active IQ）	はい	いいえ
ライセンスとサブスクリプションの管理	はい	いいえ
経済効率	はい	いいえ
ホームページダッシュボードのメトリクス	はい ²	いいえ
ライフサイクルプランニング	はい	いいえ ¹
持続可能性	はい	いいえ
ソフトウェアアップデート	はい	はい
NetAppワークロード	はい	はい
利用可能なデータサービス:		
NetApp Backup and Recovery	はい	いいえ
データ分類	はい	いいえ
NetApp Cloud Tiering	はい	いいえ
NetApp Copy and Sync	はい	いいえ
NetApp Disaster Recovery	はい	いいえ
NetApp Ransomware Resilience	はい	いいえ

	エージェントで利用可能	エージェントなしで利用可能
NetApp Volume Caching	はい	いいえ

¹ コンソール エージェントがなくてもライフサイクル プランニングを表示できますが、アクションを開始するにはコンソール エージェントが必要です。

² ホーム ページで正確なメトリックを得るには、適切なサイズと構成のコンソール エージェントが必要です。

コンソールエージェントは常に動作している必要があります

コンソール エージェントは、NetApp Consoleの基本的な部分です。関連するエージェントが常に稼働し、動作し、アクセス可能であることを確認するのはお客様側の責任です。コンソールはエージェントの短時間の停止に対処できますが、インフラストラクチャの障害は迅速に修正する必要があります。

このドキュメントは EULA によって管理されます。ドキュメントの指示に従わずに製品を操作すると、製品の機能や EULA の権利に影響する可能性があります。

サポートされている場所

エージェントは次の場所にインストールできます。

- Amazon Web Services
- Microsoft Azure

管理対象のCloud Volumes ONTAPシステムと同じリージョンの Azure にコンソール エージェントをデプロイします。あるいは、["Azure リージョン ペア"](#)。これにより、Cloud Volumes ONTAPとそれに関連付けられたストレージ アカウント間で Azure Private Link 接続が使用されるようになります。["Cloud Volumes ONTAP がAzure Private Link を使用する方法を学ぶ"](#)

- Google Cloud

Google Cloud でコンソールとデータサービスを使用するには、Google Cloud にエージェントをデプロイします。

- お客様の敷地内

クラウドプロバイダーとのコミュニケーション

エージェントは、AWS、Azure、Google Cloud へのすべての通信に TLS 1.3 を使用します。

制限モード

コンソールを制限モードで使用するには、コンソール エージェントをインストールし、コンソール エージェント上でローカルに実行されているコンソール インターフェイスにアクセスします。

["NetApp Consoleの導入モードについて学ぶ"](#)。

コンソールエージェントのインストール方法

コンソール エージェントは、コンソールから直接インストールすることも、クラウド プロバイダーのマーケットプレイスからインストールすることも、独自の Linux ホストまたは VCenter 環境にソフトウェアを手動でインストールすることもできます。

- ["NetApp Consoleの導入モードについて学ぶ"](#)
- ["NetApp Consoleを標準モードで使い始める"](#)
- ["制限モードでNetApp Consoleを使い始める"](#)

クラウドプロバイダーの権限

NetApp Consoleからコンソール エージェントを直接作成するには特定の権限が必要であり、コンソール エージェント自体には別の権限セットが必要です。コンソールから直接 AWS または Azure にコンソールエージェントを作成すると、コンソールは必要な権限を持つコンソールエージェントを作成します。

コンソールを標準モードで使用する場合、権限を付与する方法は、コンソール エージェントを作成する方法によって異なります。

権限の設定方法については、以下を参照してください。

- 標準モード
 - ["AWS でのエージェントのインストールオプション"](#)
 - ["Azure のエージェントのインストール オプション"](#)
 - ["Google Cloud のエージェントのインストール オプション"](#)
 - ["オンプレミス展開用のクラウド権限を設定する"](#)
- ["制限モードの権限を設定する"](#)

コンソール エージェントが日常の操作に必要な正確な権限を確認するには、次のページを参照してください。

- ["コンソールエージェントがAWS権限を使用する方法を学ぶ"](#)
- ["コンソールエージェントがAzureの権限を使用する方法を学ぶ"](#)
- ["コンソール エージェントが Google Cloud 権限を使用する方法を説明します。"](#)

以降のリリースで新しい権限が追加された場合、コンソール エージェント ポリシーを更新するのはユーザーの責任となります。リリース ノートには新しい権限がリストされています。

エージェントのアップグレード

NetApp は、機能の追加と安定性の向上のためにエージェント ソフトウェアを毎月更新します。Cloud Volumes ONTAPやオンプレミスのONTAPクラスタ管理などの一部のコンソール機能は、コンソール エージェントのバージョンと設定に依存します。

エージェントをクラウドにインストールすると、インターネットにアクセスできる場合はコンソール エージェントが自動的に更新されます。

オペレーティングシステムとVMのメンテナンス

コンソール エージェント ホスト上のオペレーティング システムの保守はお客様の責任となります。たとえば、お客様側では、会社の標準的なオペレーティング システム配布手順に従って、コンソール エージェント ホスト上のオペレーティング システムにセキュリティ更新を適用する必要があります。

マイナーなセキュリティ更新を適用するときに、コンソール gent ホスト上のサービスを停止する必要がないことに注意してください。

顧客がコンソール エージェント VM を停止してから起動する必要がある場合は、クラウド プロバイダーのコンソールから実行するか、オンプレミス管理の標準手順を使用して実行する必要があります。

コンソールエージェントは常に動作している必要があります。

複数のシステムとエージェント

エージェントは複数のシステムを管理し、コンソールでデータ サービスをサポートできます。展開サイズと使用するデータ サービスに基づいて、単一のエージェントを使用して複数のシステムを管理できます。

大規模な導入の場合は、NetApp の担当者と協力して環境のサイズを決定してください。問題が発生した場合は、NetAppサポートにお問い合わせください。

エージェントの展開の例をいくつか示します。

- マルチクラウド環境 (AWS と Azure など) があり、AWS に 1 つのエージェントを配置し、Azure に別のエージェントを配置することを希望しています。それぞれが、それらの環境で実行されているCloud Volumes ONTAPシステムを管理します。
- サービス プロバイダーは、1 つのコンソール組織を使用して顧客にサービスを提供しながら、別の組織を使用してビジネス ユニットの 1 つに災害復旧サービスを提供する場合があります。各組織には独自のエージェントが必要です。

NetApp Consoleのアイデンティティとアクセス管理について学ぶ

NetAppコンソールの ID およびアクセス管理 (IAM) を使用して、NetAppリソースを整理し、場所、部門、プロジェクトなどのビジネス構造に応じてアクセスを制御します。

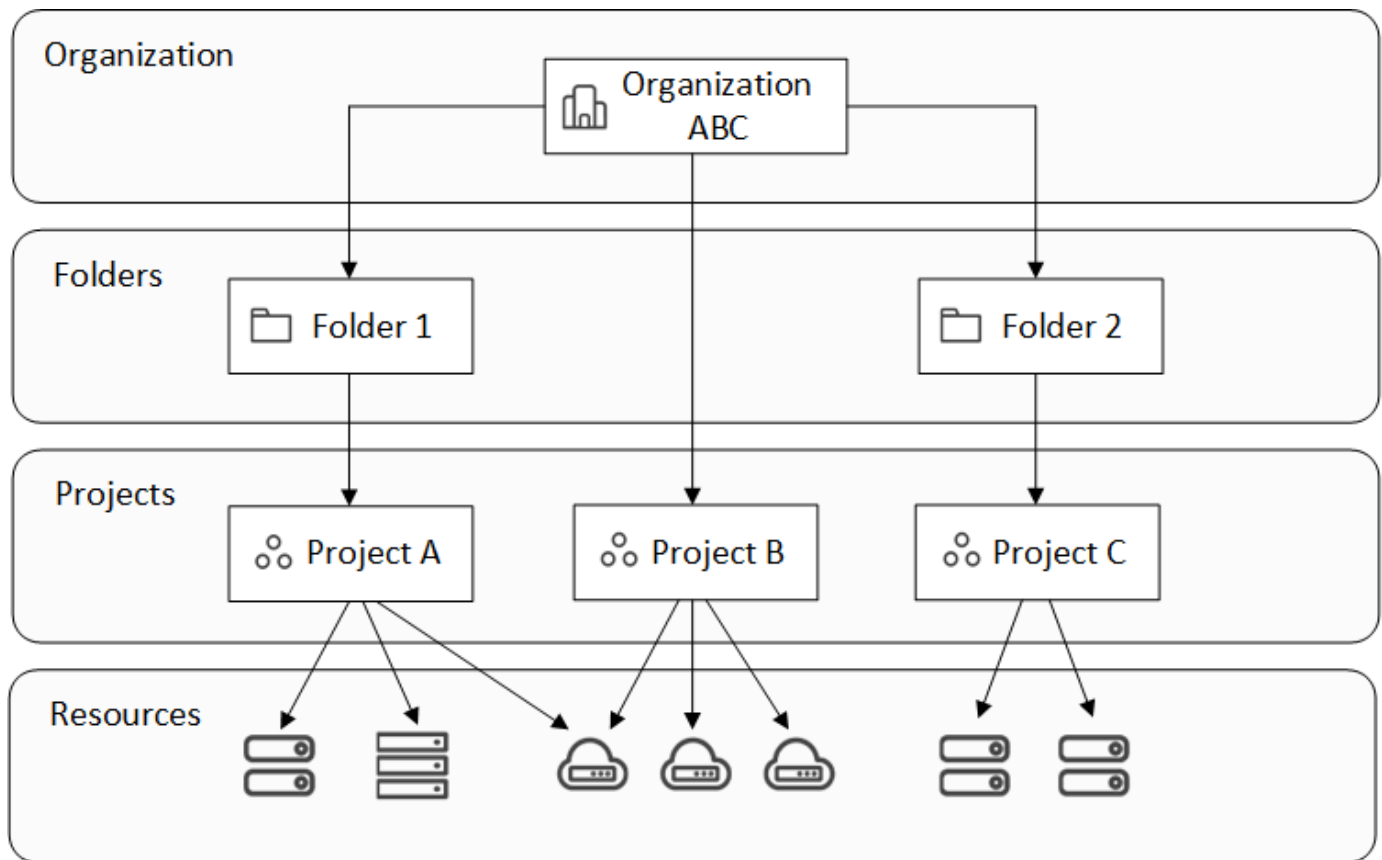
リソースは階層的に配置されます。つまり、組織が一番上にあり、次にフォルダー (他のフォルダーまたはプロジェクトを含むことができます)、そしてプロジェクト (ストレージ システム、ワークロード、エージェントを含む) が続きます。

組織、フォルダ、またはプロジェクトレベルでアクセスロールを割り当てて、ユーザーがリソースに適切にアクセスできるようにします。



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 フォルダまたはプロジェクト管理者 のロールが必要です。

次の図は、この階層を基本レベルで示しています。



]

アイデンティティおよびアクセス管理コンポーネント

NetApp Consoleでは、組織コンポーネント、リソース コンポーネント、ユーザー アクセス コンポーネントという 3 つの主要コンポーネントを使用してストレージ リソースを整理します。

組織内のプロジェクトとフォルダ

IAM 構造内では、組織、プロジェクト、フォルダという 3 つの組織コンポーネントを操作します。これらのいずれかのレベルでユーザーにロールを割り当てることで、ユーザーにアクセスを許可できます。

組織

組織は、コンソール IAM システムの最上位レベルであり、通常は会社を表します。組織は、フォルダー、プロジェクト、メンバー、ロール、リソースで構成されます。エージェントは組織内の特定のプロジェクトに関連付けられます。

プロジェクト

プロジェクトは、ストレージ リソースへのアクセスを提供するために使用されます。誰かがアクセスできるようにするには、プロジェクトにリソースを割り当てる必要があります。1 つのプロジェクトに複数のリソースを割り当てたり、複数のプロジェクトを持つこともできます。次に、ユーザーにプロジェクトへの権限を割り当てて、プロジェクト内のリソースにアクセスできるようにします。

たとえば、ニーズに応じて、オンプレミスのONTAPシステムを単一のプロジェクトまたは組織内のすべてのプロジェクトに関連付けることができます。

["組織にプロジェクトを追加する方法を学びます。"](#)

フォルダ

関連するプロジェクトを フォルダー にグループ化して、場所、サイト、またはビジネス ユニットごとに整理します。リソースをフォルダーに直接関連付けることはできませんが、フォルダー レベルでユーザーにロールを割り当てると、そのフォルダー内のすべてのプロジェクトにアクセスできるようになります。

["組織にフォルダーを追加する方法について説明します。"](#)

リソース

リソース は、コンソールが認識し、プロジェクトに割り当てることができるエンティティです。リソース には、ストレージシステム、Keystone サブスクリプション、一部のバックアップおよびリカバリのワークロード、および Console エージェントが含まれます。

+ 誰かがリソースにアクセスするには、そのリソースをプロジェクトに関連付ける必要があります。

+

たとえば、Cloud Volumes ONTAPシステムを 1 つのプロジェクトまたは組織内のすべてのプロジェクトに関連付けることができます。リソースを関連付ける方法は、組織のニーズによって異なります。

+

["リソースをプロジェクトに関連付ける方法を学習します。"](#)

ストレージシステムとKeystoneサブスクリプション

ストレージシステムは、NetApp Consoleで管理する主要なリソースです。NetApp Consoleは、オンプレミスとクラウドの両方のストレージシステムの管理をサポートしています。プロジェクトに割り当てられたユーザーがアクセスできるように、ストレージシステムをプロジェクトに追加する必要があります。

ストレージ システム

ストレージシステムは、追加されたプロジェクトに自動的に関連付けられますが、*Resources*ページから他のプロジェクトやフォルダに関連付けることもできます。FSx for NetApp ONTAPストレージシステムをプロジェクトやフォルダに関連付けることはできませんが、*Systems*ページまたはWorkloadsから表示できます。

Keystoneのサブスクリプション

Keystoneサブスクリプションは、NetApp Consoleでユーザーにサブスクリプションへのアクセスを許可するためにプロジェクトに関連付けることができるリソースでもあります。

バックアップとリカバリのワークロード (Oracle および Microsoft SQL Server)

一部の Backup and Recovery ワークロードもリソースと見なされます。ユーザーに Backup and Recovery へのアクセス権限を割り当てることができます。

コンソールエージェント

組織管理者は、ストレージ システムを管理し、NetAppデータ サービスを有効にするためにコンソール エージェントを作成します。エージェントは最初は作成されたプロジェクトに関連付けられますが、管理者はエージェント ページから他のプロジェクトやフォルダーに追加できます。

エージェントをプロジェクトに関連付けると、そのプロジェクト内のリソースを管理できるようになります。一方、エージェントをフォルダに関連付けると、フォルダ管理者またはプロジェクト管理者はどのプロジェクトでエージェントを使用するかを決定できるようになります。管理機能を提供するには、エー

エージェントを特定のプロジェクトにリンクする必要があります。

["エージェントをプロジェクトに関連付ける方法を学習します。"](#)

メンバーと役割

メンバー

組織のメンバーは、ユーザー アカウントまたはサービス アカウントです。サービス アカウントは通常、アプリケーションによって、人間の介入なしに指定されたタスクを完了するために使用されます。

NetApp Consoleにサインアップした後、メンバーを組織に追加する必要があります。追加したら、リソースへのアクセスを提供するロールを割り当てることができます。コンソール内からサービス アカウントを手動で追加することも、NetApp ConsoleIAM API を通じてサービス アカウントの作成と管理を自動化することもできます。

["組織にメンバーを追加する方法を学びます。"](#)

アクセスロール

コンソールには、組織のメンバーに割り当てることができるアクセス ロールが用意されています。

メンバーをロールに関連付けると、組織全体、特定のフォルダー、または特定のプロジェクトに対してそのロールを付与できます。選択したロールにより、階層の選択した部分にあるリソースに対する権限がメンバーに付与されます。

NetApp Consoleは、「最小権限」の原則に準拠したきめ細かなロールを提供します。つまり、アクセスロールは、ユーザーに必要なものだけへのアクセスを許可するように設計されています。

つまり、ユーザーの職務が拡大するにつれて、複数のロールが割り当てられる可能性があります。

["アクセスロールについて学ぶ"](#)。

IAM戦略の例

小規模組織戦略

ユーザー数が 50 人未満で、ストレージ管理が集中している組織の場合は、スーパー管理者とスーパー閲覧者のロールを使用した簡素化されたアプローチを検討してください。

例：**ABC株式会社（5人チーム）**

- 構造: 3 つのプロジェクト (プロダクション、開発、バックアップ) を持つ単一の組織
- 役割:
 - 上級メンバー 2 名: 完全な管理アクセス権限を持つ スーパー管理者 ロール
 - 3 人のチームメンバー: 変更権限のない監視用の スーパー ビューアー ロール
- エージェント戦略: 共有リソースアクセスのためにすべてのプロジェクトに関連付けられた単一のエージェント
- 利点: 管理が簡素化され、役割の複雑さが軽減され、幅広いアクセスを必要とするチームに適しています

多地域企業戦略

地域的な事業や専門チームを持つ大規模な組織の場合は、地理的または事業部門の境界を表すフォルダーを使用して階層的なアプローチを実装します。

例: XYZ株式会社 (多国籍企業)

- 構造: 組織 > 地域フォルダ (北米、ヨーロッパ、アジア太平洋) > 地域ごとのプロジェクトフォルダ
- プラットフォームの役割:
 - 1 組織管理者: グローバルな監視とポリシー管理
 - 3 フォルダまたはプロジェクト管理者: 地域管理 (地域ごとに 1 人)
 - 1 フェデレーション管理者: 企業IDプロバイダーの統合
- リージョン別のストレージの役割:
 - 9 ストレージ管理者: 割り当てられたリージョン内のストレージ システムを検出して管理します
 - 2 ストレージビューア: リージョン間のストレージリソースを監視する
 - 1 システムヘルススペシャリスト: システムを変更せずにストレージのヘルスを管理します
- データ サービスの役割:
 - バックアップおよびリカバリ管理者: バックアップ責任に基づいたプロジェクトごと
 - ランサムウェア耐性管理者: プロジェクト全体のセキュリティチームの監視
- エージェント戦略: 適切な地理的プロジェクトに関連付けられた地域エージェント
- 利点: 役割の分離、地域の自治、現地の規制への準拠によるセキュリティの強化

部門別専門化戦略

特定のデータ サービス アクセスを必要とする専門チームを持つ組織の場合は、機能上の責任に基づいて対象を絞ったロールの割り当てを使用します。

例: TechCorp (中規模テクノロジー企業)

- 構造: 組織 > 部門フォルダ (IT、セキュリティ、開発) > プロジェクト固有のリソース
- 専門的な役割:
 - セキュリティ チーム: ランサムウェア耐性管理者 および 分類閲覧者 の役割
 - バックアップ チーム: 包括的なバックアップ操作を担当する バックアップおよびリカバリ スーパー管理者
 - 開発チーム: テスト環境管理のための ストレージ管理者
 - コンプライアンス チーム: 監視およびサポートケース管理を行う 運用サポート アナリスト
- エージェント戦略: リソースの所有権に基づいて部門プロジェクトにリンクされたエージェント
- 利点: カスタマイズされたアクセス制御、運用効率の向上、専門的なタスクに対する明確な説明責任

NetApp ConsoleでのIAMの次のステップ

- ["NetApp ConsoleでIAMを使い始める"](#)
- ["IAMアクティビティを監視または監査する"](#)
- ["NetApp ConsoleIAMのAPIについて学ぶ"](#)

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权を有し、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权については、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。