NetApp Consoleのセットアップと管理に関するドキュメント

NetApp Console setup and administration

NetApp
October 15, 2025

目次

NetApp Consoleのセットアップと管理に関するドキュメント

リリース ノート

新着情報

NetApp Console管理機能の新機能（アイデンティティおよびアクセス管理 (IAM)、コンソール エージェント、クラウド プロバイダーの認証情報など）について説明します。

2025年10月6日

BlueXPはNetApp Consoleになりました

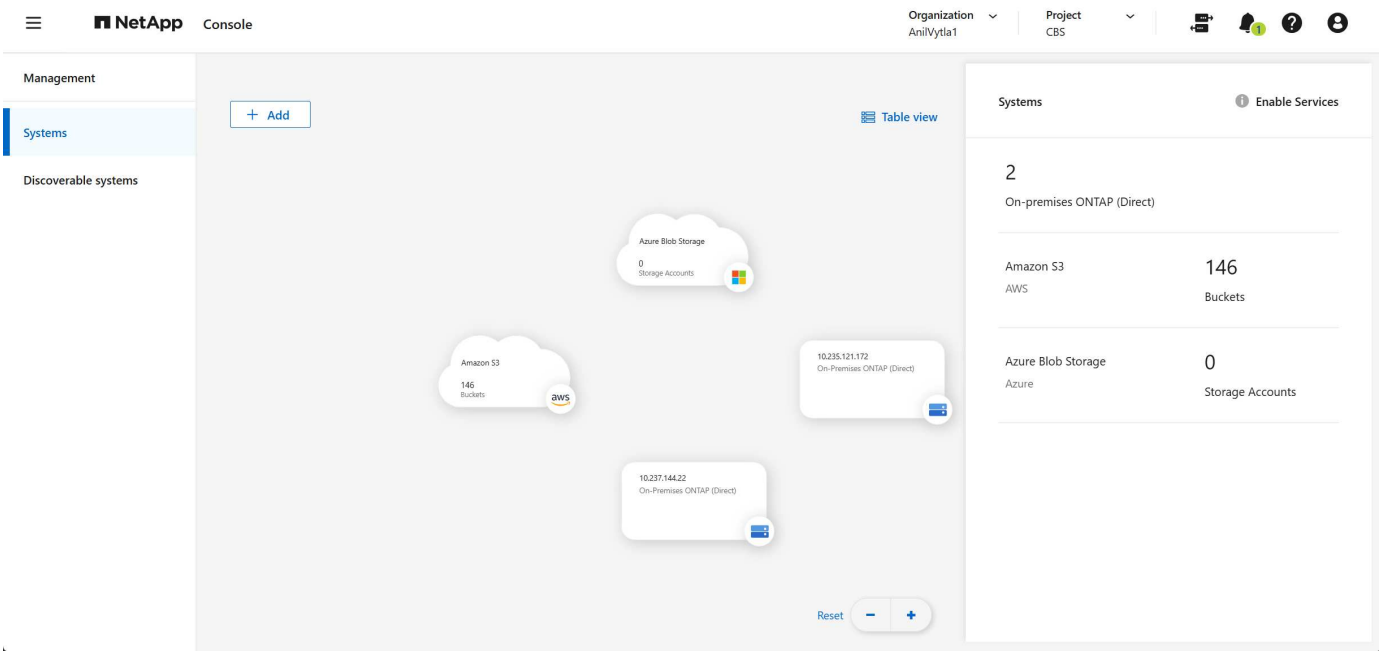
NetApp Consoleは、強化され再構築されたBlueXP基盤上に構築され、オンプレミスとクラウド環境全体にわたるエンタープライズ グレードのNetAppストレージとNetApp Data Servicesの集中管理を提供し、リアルタイムの分析情報、より高速なワークフロー、および高度に安全でコンプライアンスに準拠した簡素化された管理を実現します。

ナビゲーションメニューとページ

NetApp は、ほとんどのメニュー オプションを左側のナビゲーション ペインに移動し、メニューを再編成して、 NetApp Consoleでのナビゲーションを容易にしました。

Canvasはシステムページに置き換えられました

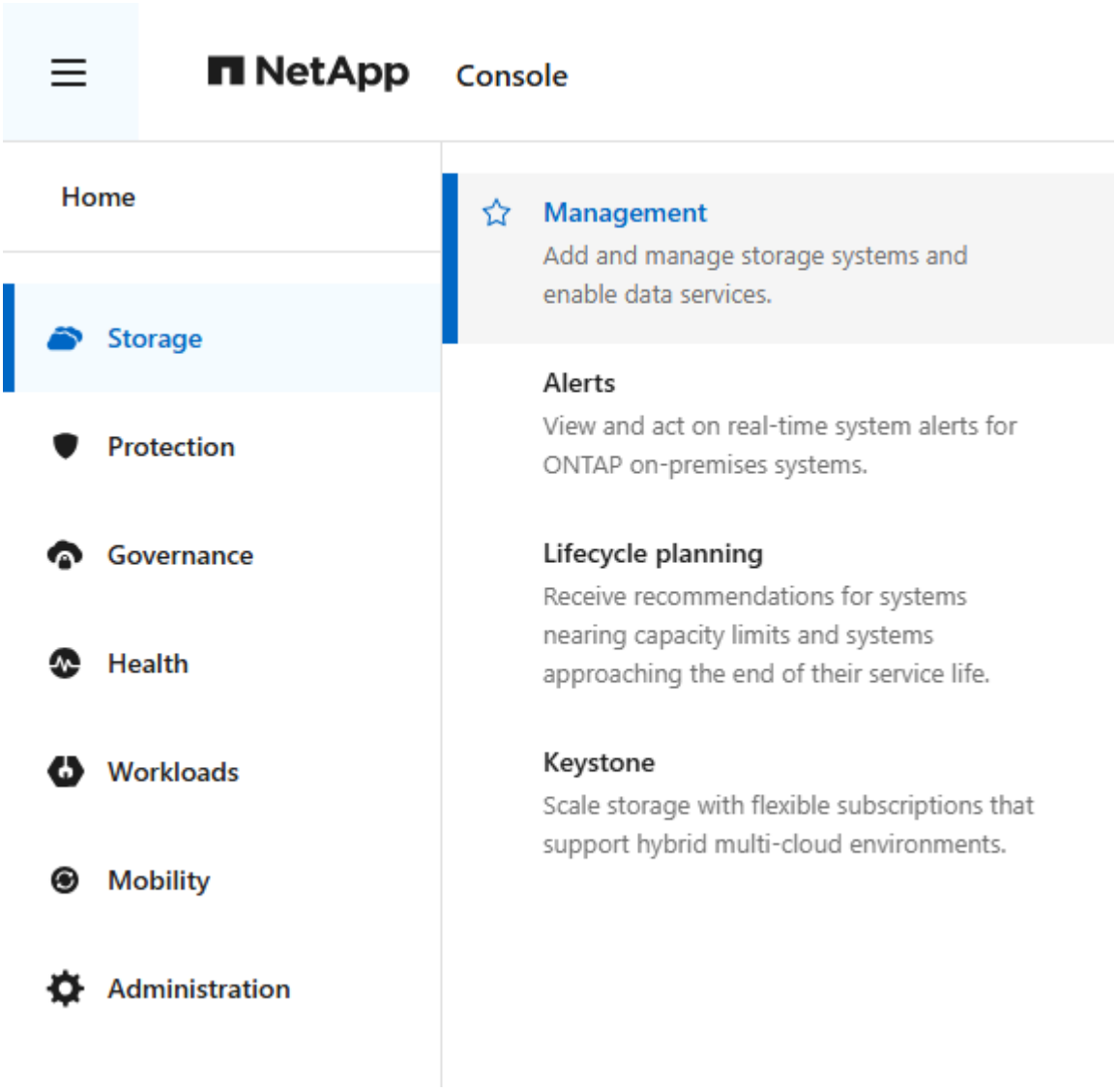
NetApp は、Canvas の名前を **Systems** ページに変更しました。 ストレージ **>** 管理 メニューから システム ページに移動します。



拡張ストレージメニュー

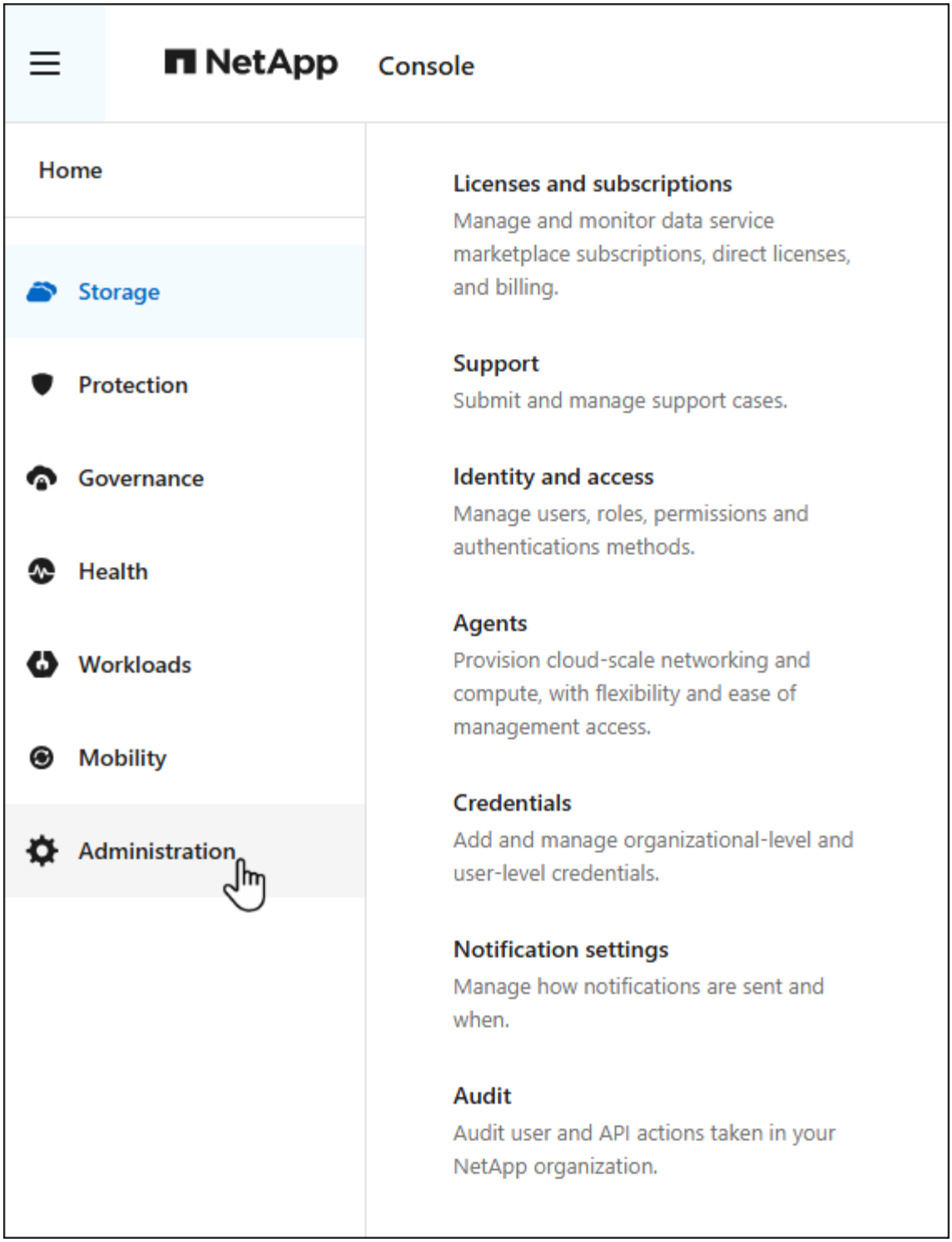
ストレージ メニューには、 ONTAPシステムのアラートを表示するための アラート と、未使用または十分に活用されていないリソースを識別するための ライフサイクル プランニング (旧 経済効率) が含まれています。

NetApp はKeystone を*ストレージ* メニューに移動しました。ここで、 NetApp Keystoneサブスクリプションを管理し、使用状況を表示できます。



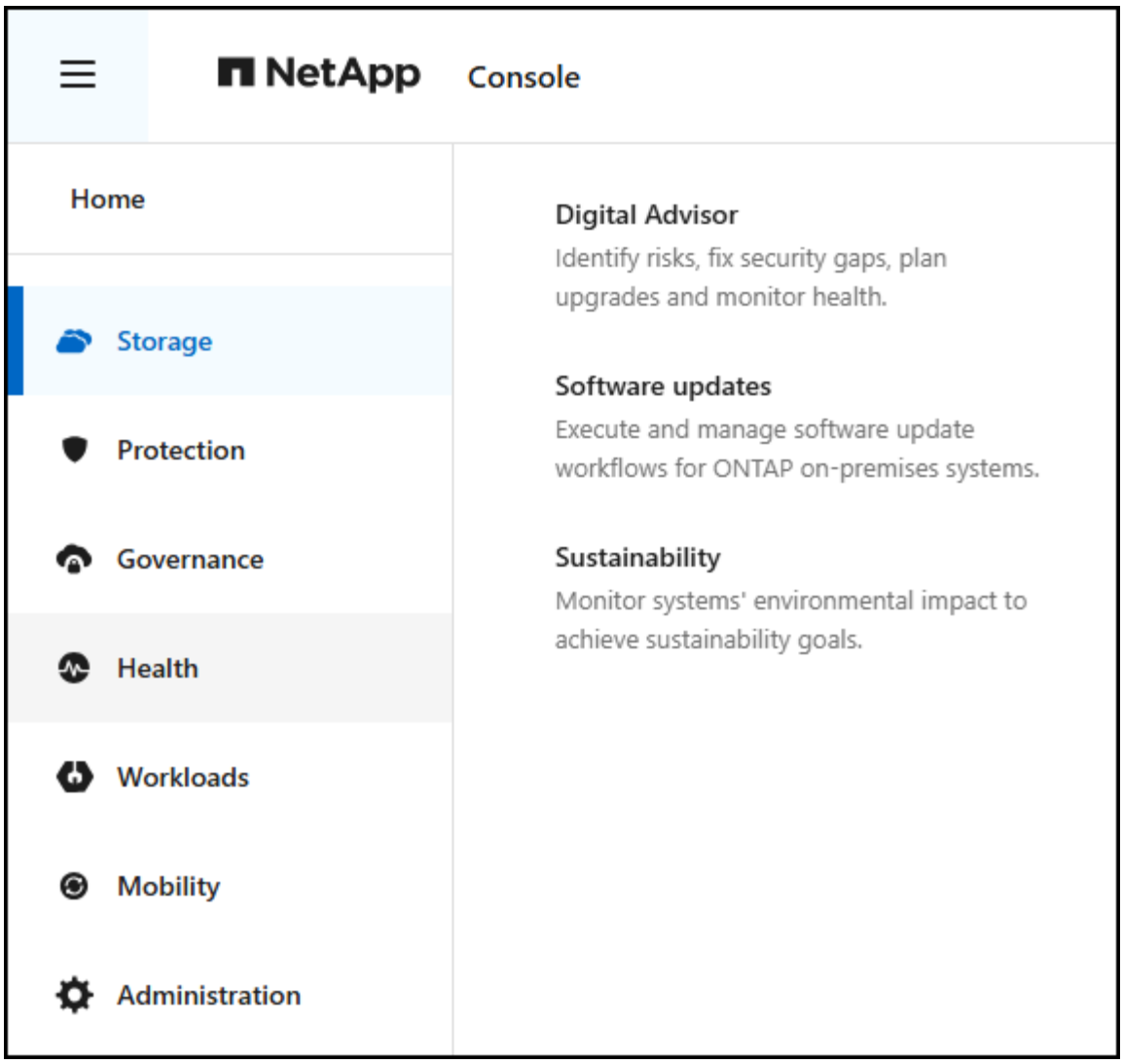
管理メニュー

一元化された 管理 メニューを使用して、 NetApp Console、サポート ケース、ライセンス、サブスクリプション (以前はデジタル ウォレットと呼ばれていました) を管理します。



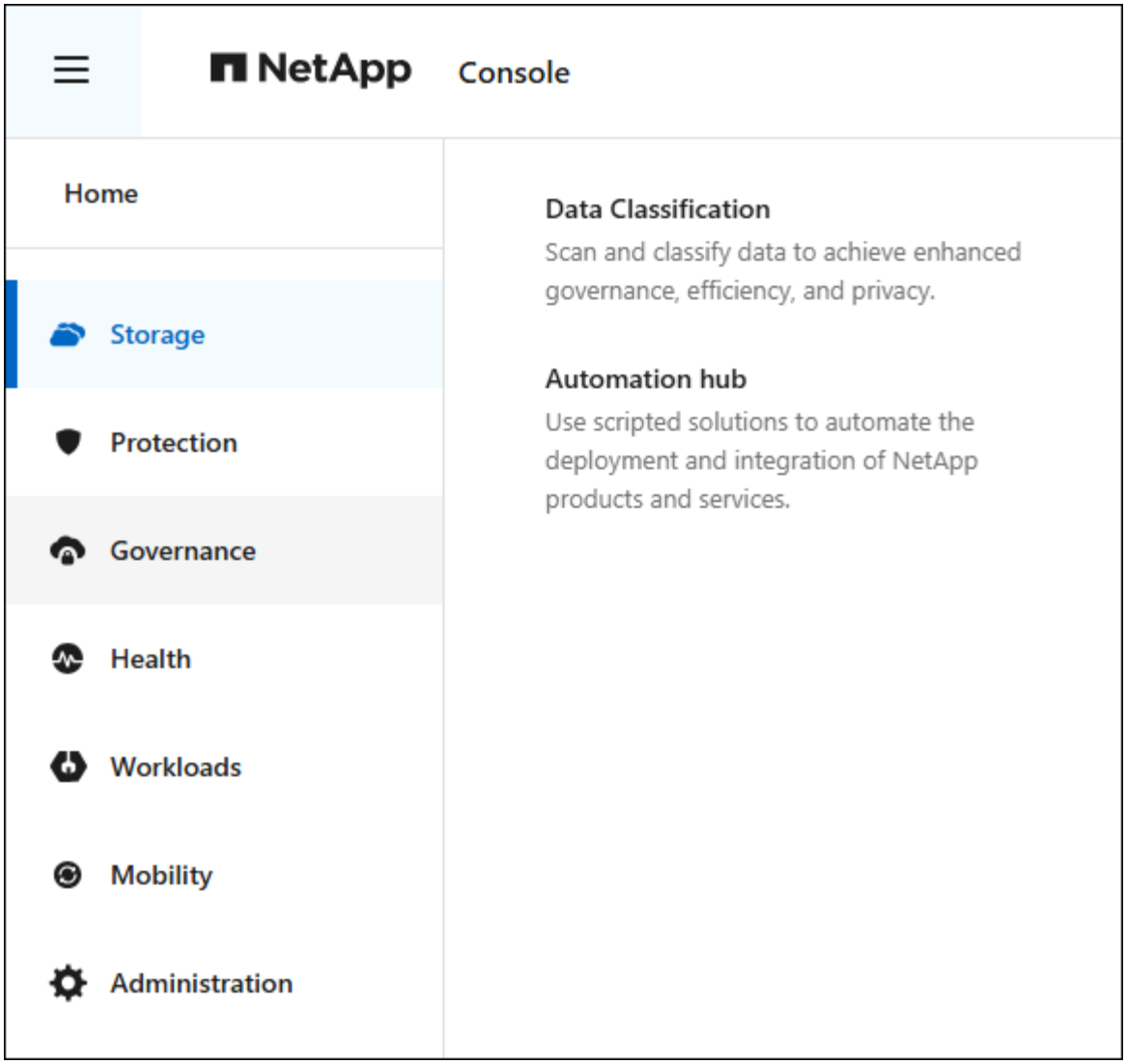
健康メニュー

効率的な **Health** メニューには、 ONTAPソフトウェアの更新を管理できる **Software updates**、環境への影響を監視できる **Sustainability**、ストレージ環境を最適化するためのプロアクティブな推奨事項を得られる * Digital Advisor* が含まれます。



ガバナンスメニュー

ガバナンス メニューには、データ分類とコンプライアンスを管理できる データ分類 と、自動化ワークフローを作成して管理できる 自動化ハブ が含まれています。



要素、データサービス、機能のより直感的な命名

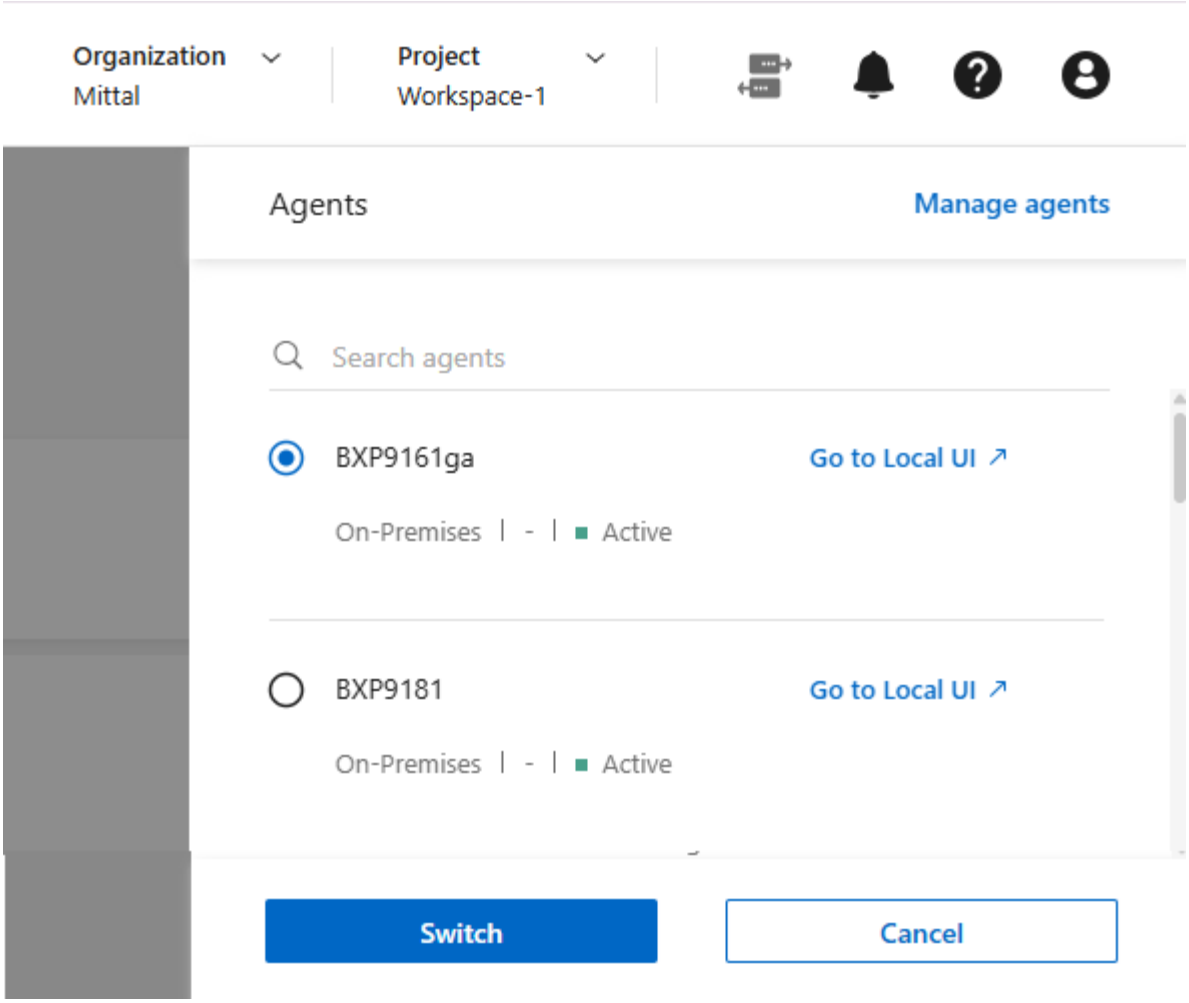
NetApp は、目的を明確にするために、いくつかの要素、データ サービス、および機能の名前を変更しました。主な変更点は次のとおりです。

以前の名前	* NetApp Console名*
コネクタ	コンソールエージェント。 管理 > エージェント メニューからエージェントを表示、追加、管理します。
タイムラインページ	監査ページ 管理 > 監査 メニューから監査コンソールのアクティビティを表示します。
労働環境	システム ストレージ > 管理 メニューからシステムを表示、追加、管理します。

以前の名前	*** NetApp Console名***
BlueXPランサムウェア対策	NetApp Ransomware Resilience。 ランサムウェア耐性は、データを保護し、ランサムウェア攻撃から迅速に回復するのに役立ちます。
BlueXPの経済効率	ライフサイクル計画。 ライフサイクル プランニングは、未使用および十分に活用されていないリソースを特定することで、ストレージ コストを最適化するのに役立ちます。 ストレージ **>** ライフサイクル プランニング メニューからライフサイクル プランニングにアクセスします。
BlueXP digital wallet	Licenses and subscriptions 管理 **>Licenses and subscriptions** メニューからライセンスとサブスクリプションにアクセスします。

コンソールエージェント

管理 **>** エージェント メニューからコンソール エージェントにアクセスして管理します。 NetApp は、**Systems** ページ (以前の Canvas) のコンソール エージェントの選択方法を変更しました。 NetAppはコネクタメニュー名をアイコンに置き換えました  、システムを表示するコンソール エージェントを選択できます。



管理 > エージェント メニューからエージェントを管理することもできます。

コンソールエージェント 4.0.0

このコンソール エージェントのリリースには、セキュリティの改善、バグ修正、および次の新機能が含まれています。

4.0.0 リリースは、標準モードと制限モードで利用できます。

必要なネットワークエンドポイントの統合と削減

NetApp は、コンソールとコンソール エージェントに必要なネットワーク エンドポイントを削減し、セキュリティを強化して導入を簡素化しました。重要なのは、バージョン 4.0.0 より前のすべてのデプロイメントが引き続き完全にサポートされていることです。以前のエンドポイントは既存のエージェントで引き続き使用できますが、 NetApp、エージェントのアップグレードが成功したことを確認した後、ファイアウォール ルールを現在のエンドポイントに更新することを強くお勧めします。

- "エンドポイントリストを更新する方法を学ぶ" 。
- "必要なエンドポイントの詳細について説明します。"

コンソールエージェントの **VCenter** 展開のサポート

OVA ファイルを使用して、VMware 環境にコンソール エージェントを展開できます。 OVA ファイルには、コンソール エージェント ソフトウェアとNetApp Consoleに接続するための設定が含まれた、事前構成された VM イメージが含まれています。ファイルのダウンロードまたは URL の展開は、 NetApp Consoleから直接行えます。"VMware 環境にコンソール エージェントを展開する方法を学習します。"

VMware 用コンソール エージェント OVA は、迅速な展開のために事前構成された VM イメージを提供します。

失敗したエージェントの展開に関する検証レポート

NetApp Consoleからコンソール エージェントを展開するときに、エージェント構成を検証するオプションが追加されました。コンソールがエージェントの展開に失敗した場合、トラブルシューティングに役立つダウンロード可能なレポートが提供されます。

コンソールエージェントのトラブルシューティングの改善

コンソール エージェントでは、問題をよりよく理解するのに役立つエラー メッセージが改善されました。"コンソール エージェントのトラブルシューティング方法を学習します。"

NetApp Console

NetApp Console管理には、次の新機能が含まれています。

ホームページダッシュボード

NetAppコンソールのホーム ページ ダッシュボードでは、ヘルス、容量、ライセンス ステータス、データ サービスのメトリックを使用して、ストレージ インフラストラクチャのリアルタイムの可視性が提供されます。"ホーム ページの詳細をご覧ください。"

NetAppアシスタント

組織管理者ロールを持つ新規ユーザーは、 NetAppアシスタントを使用して、エージェントの追加、 NetApp サポート アカウントのリンク、ストレージ システムの追加など、コンソールを構成できます。"NetAppアシスタントについて学習します。"

サービスアカウント認証

NetApp Consoleは、システム生成のクライアント ID とシークレット、または顧客管理の JWT を使用したサービス アカウント認証をサポートしているため、組織はセキュリティ要件と統合ワークフローに最適なアプローチを選択できます。秘密鍵 JWT クライアント認証では非対称暗号化が使用され、従来のクライアント ID や秘密方式よりも強力なセキュリティが提供されます。秘密鍵 JWT クライアント認証では非対称暗号化が使用され、顧客の環境で秘密鍵が安全に保たれ、資格情報の盗難リスクが軽減され、自動化スタックとクライアント アプリケーションのセキュリティが向上します。"サービス アカウントを追加する方法について説明します。"

セッション タイムアウト

システムは、24 時間後またはユーザーが Web ブラウザを閉じるとユーザーをログアウトします。

組織間のパートナーシップのサポート

NetApp Consoleでパートナーシップを作成すると、パートナーは組織の境界を越えてNetAppリソースを安全に管理できるため、コラボレーションが容易になり、セキュリティが強化されます。"パートナーシップの管理方法を学ぶ" 。

スーパー管理者とスーパー閲覧者の役割

スーパー管理者 と スーパー閲覧者 の役割を追加しました。 スーパー管理者 は、コンソールの機能、ストレージ、およびデータ サービスへの完全な管理アクセス権を付与します。 スーパー ビューアー は、監査人および関係者に読み取り専用の可視性を提供します。これらの役割は、幅広いアクセス権が一般的である上級メンバーの小規模チームに役立ちます。セキュリティと監査可能性を向上させるために、組織では スーパー管理者 アクセスを控えめに使用し、可能な場合はきめ細かな役割を割り当てることが推奨されます。"アクセス ロールの詳細について説明します。"

ランサムウェア耐性に関する追加の役割

ランサムウェア耐性ユーザー行動管理者 ロールと ランサムウェア耐性ユーザー行動閲覧者 ロールが追加されました。これらのロールにより、ユーザーはそれぞれユーザーの行動と分析データを構成および表示できます。"アクセス ロールの詳細について説明します。"

サポートチャットを削除しました

NetApp は、NetApp Consoleからサポート チャット機能を削除しました。 管理 > サポート ページを使用して、サポート ケースを作成および管理します。

2025年8月11日

コネクタ 3.9.55

BlueXPコネクタのこのリリースには、セキュリティの改善とバグ修正が含まれています。

3.9.55 リリースは、標準モードと制限モードで利用できます。

日本語サポート

BlueXP UI が日本語で利用できるようになりました。ブラウザの言語が日本語の場合、 BlueXP は日本語で表示されます。日本語のドキュメントにアクセスするには、ドキュメント Web サイトの言語メニューを使用します。

運用回復力機能

運用回復力機能はBlueXPから削除されました。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。

BlueXPアイデンティティおよびアクセス管理 (IAM)

BlueXPの ID およびアクセス管理では、次の機能が提供されるようになりました。

運用サポートのための新しいアクセスロール

BlueXP は、運用サポートアナリストの役割をサポートするようになりました。このロールは、ストレージアラートを監視し、 BlueXP監査タイムラインを表示し、 NetAppサポートケースを入力および追跡する権限をユーザーに付与します。

"アクセス ロールの使用について詳しく学習します。"

2025年7月31日

プライベートモードリリース（**3.9.54**）

新しいプライベートモードリリースがダウンロード可能になりました。 "NetAppサポート サイト"

3.9.54 リリースには、次のBlueXPコンポーネントとサービスの更新が含まれています。

コンポーネントまたはサービス	このリリースに含まれるバージョン	前回のプライベートモードリリース以降の変更点
コネクタ	3.9.54、3.9.53	に行く "BlueXPページの新着情報" バージョン 3.9.54 および 3.9.53 に含まれる変更を参照してください。
バックアップとリカバリ	2025年7月28日	に行く "BlueXP backup and recoveryページの新機能"2025 年 7 月のリリースに含まれる変更点を参照してください。
分類	2025年7月14日（バージョン1.45）	に行く "BlueXP classificationページの新機能"。

プライベート モードの詳細（アップグレード方法を含む）については、以下を参照してください。

- "プライベートモードについて学ぶ"
- "プライベートモードでBlueXPを始める方法を学ぶ"
- "プライベートモード使用時にコネクタをアップグレードする方法を学びます"

2025年7月21日

Google Cloud NetApp Volumesのサポート

BlueXPでGoogle Cloud NetApp Volumes を表示できるようになりました。"Google Cloud NetApp Volumesの詳細をご覧ください。"

BlueXPアイデンティティおよびアクセス管理 (IAM)

Google Cloud NetApp Volumesの新しいアクセスロール

BlueXPでは、次のストレージ システムへのアクセス ロールの使用がサポートされるようになりました。

- Google Cloud NetApp Volumes

"アクセス ロールの使用について詳しく学習します。"

2025年7月14日

コネクタ 3.9.54

BlueXPコネクタのこのリリースには、セキュリティの改善、バグ修正、および次の新機能が含まれています。

- Cloud Volumes ONTAPサービスのサポート専用のコネクタの透過プロキシのサポート。"透過プロキシの構成について詳しく学びます。"
- コネクタが Google Cloud 環境にデプロイされているときに、ネットワーク タグを使用してコネクタ トラフィックをルーティングする機能。
- CPU および RAM の使用状況を含む、コネクタのヘルス監視に関する追加の製品内通知。

現時点では、3.9.54 リリースは標準モードと制限モードで利用できます。

BlueXPアイデンティティおよびアクセス管理 (IAM)

BlueXPの ID およびアクセス管理では、次の機能が提供されるようになりました。

- プライベート モードでの IAM のサポートにより、 BlueXPサービスおよびアプリケーションに対するユーザー アクセスと権限を管理できます。
- より簡単なナビゲーション、フェデレーション接続を構成するためのより明確なオプション、既存のフェデレーションの可視性の向上など、ID フェデレーションの管理が合理化されます。
- BlueXP backup and recovery、 BlueXP disaster recovery、およびフェデレーション管理のアクセス ロール。

プライベートモードでのIAMのサポート

BlueXP はプライベート モードで IAM をサポートするようになり、 BlueXPサービスとアプリケーションに対するユーザー アクセスと権限を管理できるようになりました。この機能強化により、プライベート モードのお客様は、ロールベースのアクセス制御 (RBAC) を活用して、セキュリティとコンプライアンスを強化できます。

"BlueXPの IAM について詳しく学びます。"

アイデンティティ連携の合理化された管理

BlueXPでは、ID フェデレーションを管理するためのより直感的なインターフェースが提供されるようになりました。これには、より簡単なナビゲーション、フェデレーション接続を構成するためのより明確なオプション、既存のフェデレーションの可視性の向上が含まれます。

ID フェデレーションを通じてシングル サインオン (SSO) を有効にすると、ユーザーは企業の資格情報を使用してBlueXPにログインできるようになります。これにより、セキュリティが向上し、パスワードの使用が減り、オンボーディングが簡素化されます。

新しい管理機能にアクセスするには、既存のフェデレーション接続を新しいインターフェースにインポートするように求められます。これにより、フェデレーション接続を再作成することなく、最新の拡張機能を活用できるようになります。"既存のフェデレーション接続をBlueXPにインポートする方法の詳細について説明します。"

改善されたフェデレーション管理により、次のことが可能になります。

- フェデレーション接続に複数の検証済みドメインを追加すると、同じ ID プロバイダー (IdP) で複数のドメインを使用できるようになります。
- 必要に応じてフェデレーション接続を無効化または削除し、ユーザー アクセスとセキュリティを制御できます。
- IAM ロールを使用してフェデレーション管理へのアクセスを制御します。

"BlueXPの ID フェデレーションの詳細をご覧ください。"

BlueXP backup and recovery、 **BlueXP disaster recovery**、およびフェデレーション管理の新しいアクセス ロール

BlueXPでは、次の機能とデータ サービスに対する IAM ロールの使用がサポートされるようになりました。

- BlueXP backup and recovery
- BlueXP disaster recovery
- フェデレーション

"アクセス ロールの使用について詳しく学習します。"

2025年6月9日

コネクタ **3.9.53**

BlueXPコネクタのこのリリースには、セキュリティの改善とバグ修正が含まれています。

3.9.53 リリースは、標準モードと制限モードで利用できます。

ディスク容量使用状況アラート

通知センターに、コネクタのディスク領域の使用状況に関するアラートが含まれるようになりました。"詳細情報"

監査の改善

タイムラインに、ユーザーのログイン イベントとログアウト イベントが含まれるようになりました。ログインアクティビティがいつ行われたかを確認できるため、監査やセキュリティ監視に役立ちます。組織管理者のロールを持つAPIユーザーは、次の情報を含めることでログインしたユーザーのメールアドレスを表示できます。 `includeUserData=true``パラメータは次のようになります。 `/audit/<account_id>?includeUserData=true` 。

BlueXPで**Keystone**サブスクリプション管理が利用可能

BlueXPからNetApp Keystoneサブスクリプションを管理できます。

"BlueXPでのKeystoneサブスクリプション管理について学習します。"

BlueXPアイデンティティおよびアクセス管理 (IAM)

多要素認証（MFA）

非フェデレーション ユーザーは、 BlueXPアカウントに対して MFA を有効にしてセキュリティを強化できます。管理者は、必要に応じてユーザーの MFA をリセットまたは無効化するなど、MFA 設定を管理できます。これは標準モードでのみサポートされます。

"自分自身に多要素認証を設定する方法について説明します。" "ユーザーに対する多要素認証の管理について学習します。"

ワークロード

BlueXPの認証情報ページからAmazon FSx for NetApp ONTAP の認証情報を表示および削除できるようになりました。

2025年5月29日

プライベートモードリリース（**3.9.52**）

新しいプライベートモードリリースがダウンロード可能になりました。 "NetAppサポート サイト"

3.9.52 リリースには、次のBlueXPコンポーネントとサービスの更新が含まれています。

コンポーネントまたはサービス	このリリースに含まれるバージョン	前回のプライベートモードリリース以降の変更点
コネクタ	3.9.52、3.9.51	に行く "BlueXPコネクタページの新機能"バージョン 3.9.52 および 3.9.50 に含まれる変更を参照してください。
バックアップとリカバリ	2025年5月12日	に行く "BlueXP backup and recoveryページの新機能"2025 年 5 月のリリースに含まれる変更点を参照してください。
分類	2025年5月12日（バージョン1.43）	に行く "BlueXP classificationページの新機能"1.38 から 1.371.41 リリースに含まれる変更を参照してください。

プライベート モードの詳細（アップグレード方法を含む）については、以下を参照してください。

- "プライベートモードについて学ぶ"
- "プライベートモードでBlueXPを始める方法を学ぶ"
- "プライベートモード使用時にコネクタをアップグレードする方法を学びます"

2025年5月12日

コネクタ **3.9.52**

BlueXPコネクタのこのリリースには、マイナーなセキュリティの改善とバグ修正、およびいくつかの追加の更新が含まれています。

現時点では、3.9.52 リリースは標準モードと制限モードで利用できます。

Docker 27 および **Docker 28** のサポート

コネクタでは Docker 27 と Docker 28 がサポートされるようになりました。

Cloud Volumes ONTAP

コネクタがコンプライアンス違反になったり、14 日以上ダウンしたりしても、 Cloud Volumes ONTAPノードはシャットダウンしなくなりました。 Cloud Volumes ONTAP は、コネクタへのアクセスを失った場合でも、イベント管理メッセージを送信します。この変更は、コネクタが長時間ダウンした場合でも、 Cloud Volumes ONTAP が引き続き動作できるようにするためです。コネクタのコンプライアンス要件は変更されません。

BlueXPで**Keystone**管理が利用可能

BlueXPのNetApp Keystoneベータ版では、 Keystone管理へのアクセスが追加されました。 BlueXPの左側のナビゲーション バーから、 NetApp Keystoneベータ版のサインアップ ページにアクセスできます。

BlueXPアイデンティティおよびアクセス管理 **(IAM)**

新しいストレージ管理の役割

ストレージ管理者、システム正常性スペシャリスト、ストレージ閲覧者の役割が利用可能であり、ユーザーに割り当てることができます。

これらのロールを使用すると、組織内のどのユーザーがストレージ リソースを検出および管理できるかを管理できるほか、ストレージの正常性情報を表示したり、ソフトウェアの更新を実行したりすることもできます。

これらのロールは、次のストレージ リソースへのアクセスを制御するためにサポートされています。

- Eシリーズシステム
- StorageGRIDシステム
- オンプレミスのONTAPシステム

これらのロールを使用して、次のBlueXPサービスへのアクセスを制御することもできます。

- ソフトウェアアップデート
- デジタルアドバイザー
- 運用の回復力
- 経済効率
- 持続可能性

次のロールが追加されました:

- ストレージ管理者

  組織内のストレージ リソースのストレージの健全性、ガバナンス、検出を管理します。このロールは、ストレージ リソースのソフトウェア更新も実行できます。

- システムヘルススペシャリスト

  組織内のストレージ リソースのストレージの健全性とガバナンスを管理します。このロールは、ストレージ リソースのソフトウェア更新も実行できます。このロールでは、作業環境を変更または削除することはできません。

- ストレージビューア

  ストレージの健全性情報とガバナンス データを表示します。

  "アクセス ロールについて学習します。"

2025年4月14日

コネクタ 3.9.51

BlueXPコネクタのこのリリースには、マイナーなセキュリティの改善とバグ修正が含まれています。

現時点では、3.9.51 リリースは標準モードと制限モードで利用できます。

コネクタダウンロード用の安全なエンドポイントが、バックアップとリカバリ、およびランサムウェア保護でサポートされるようになりました

バックアップとリカバリまたはランサムウェア保護を使用している場合は、コネクタのダウンロードに安全なエンドポイントを使用できるようになりました。"コネクタのダウンロードのための安全なエンドポイントについて説明します。"

BlueXPアイデンティティおよびアクセス管理 (IAM)

- 組織管理者、フォルダ管理者、またはプロジェクト管理者の権限がないユーザーには、ランサムウェア保護にアクセスするために、ランサムウェア保護ロールを割り当てる必要があります。ユーザーには、ランサムウェア保護管理者またはランサムウェア保護閲覧者の 2 つのロールのいずれかを割り当てることができます。
- 組織管理者、フォルダー管理者、またはプロジェクト管理者の権限を持たないユーザーには、 Keystone にアクセスするためのKeystoneロールを割り当てる必要があります。ユーザーには、 Keystone管理者またはKeystoneビューアーのいずれかのロールを割り当てることができます。

  "アクセス ロールについて学習します。"

- 組織管理者、フォルダ管理者、またはプロジェクト管理者のロールを持っている場合は、 Keystoneサブスクリプションを IAM プロジェクトに関連付けることができるようになりました。 Keystoneサブスクリプションを IAM プロジェクトに関連付けると、 BlueXP内でKeystoneへのアクセスを制御できるようになります。

2025年3月28日

プライベートモードリリース（**3.9.50**）

新しいプライベートモードリリースがダウンロード可能になりました。 "NetAppサポート サイト"

3.9.50 リリースには、次のBlueXPコンポーネントとサービスの更新が含まれています。

コンポーネントまたはサービス	このリリースに含まれるバージョン	前回のプライベートモードリリース以降の変更点
コネクタ	3.9.50、3.9.49	に行く "BlueXPコネクタページの新機能"バージョン 3.9.50 および 3.9.49 に含まれる変更を参照してください。
バックアップとリカバリ	2025年3月17日	に行く "BlueXP backup and recoveryページの新機能"2024 年 3 月のリリースに含まれる変更点を参照してください。
分類	2025年3月10日（バージョン1.41）	に行く "BlueXP classificationページの新機能"1.38 から 1.371.41 リリースに含まれる変更を参照してください。

プライベート モードの詳細（アップグレード方法を含む）については、以下を参照してください。

- "プライベートモードについて学ぶ"
- "プライベートモードでBlueXPを始める方法を学ぶ"
- "プライベートモード使用時にコネクタをアップグレードする方法を学びます"

2025年3月10日

コネクタ **3.9.50**

BlueXPコネクタのこのリリースには、マイナーなセキュリティの改善とバグ修正が含まれています。

- Cloud Volumes ONTAPシステムの管理は、オペレーティング システムで SELinux が有効になっているコネクタによってサポートされるようになりました。

  "SELinuxについて詳しく知る"

現時点では、3.9.50 リリースは標準モードと制限モードで利用できます。

NetApp Keystoneベータ版が**BlueXP**で利用可能に

NetApp Keystone はまもなくBlueXPから入手可能になり、現在はベータ版です。 BlueXPの左側のナビゲーション バーから、 NetApp Keystoneベータ版のサインアップ ページにアクセスできます。

2025年3月6日

コネクタ 3.9.49 アップデート

BlueXPがコネクタを使用する場合のONTAP System Managerアクセス

BlueXP管理者 (組織管理者ロールを持つユーザー) は、 ONTAPシステム マネージャーにアクセスするためにユーザーにONTAP資格情報の入力を求めるようにBlueXPを設定できます。この設定を有効にすると、ONTAP認証情報はBlueXPに保存されないため、ユーザーは毎回ONTAP認証情報を入力する必要があります。

この機能は、コネクタ バージョン 3.9.49 以降で利用できます。"資格情報設定を構成する方法を学習します。" 。

コネクタ 3.9.48 アップデート

コネクタの自動アップグレード設定を無効にする機能

コネクタの自動アップグレード機能を無効にすることができます。

BlueXP を標準モードまたは制限モードで使用する場合、コネクタがソフトウェア更新を取得するためのアウトバウンド インターネット アクセスを持っている限り、 BlueXP はコネクタを最新のリリースに自動的にアップグレードします。コネクタのアップグレード時期を手動で管理する必要がある場合は、標準モードまたは制限モードの自動アップグレードを無効にできるようになりました。

> この変更は、常に自分でコネクタをアップグレードする必要があるBlueXPプライベート モードには影響しません。

この機能は、コネクタ バージョン 3.9.48 以降で利用できます。

"コネクタの自動アップグレードを無効にする方法について説明します。"

2025年2月18日

プライベートモードリリース（3.9.48）

新しいプライベートモードリリースがダウンロード可能になりました。 "NetAppサポート サイト"

3.9.48 リリースには、次のBlueXPコンポーネントとサービスの更新が含まれています。

コンポーネントまたはサービス	このリリースに含まれるバージョン	前回のプライベートモードリリース以降の変更点
コネクタ	3.9.48	に行く "BlueXPコネクタページの新機能"バージョン 3.9.48 に含まれる変更を参照してください。
バックアップとリカバリ	2025年2月21日	に行く "BlueXP backup and recoveryページの新機能"2025 年 2 月のリリースに含まれる変更点を参照してください。

コンポーネントまたはサービス	このリリースに含まれるバージョン	前回のプライベートモードリリース以降の変更点
分類	2025年1月22日（バージョン1.39）	に行く "BlueXP classificationページの新機能"1.39 リリースに含まれる変更点を参照してください。

2025年2月10日

コネクタ 3.9.49

BlueXPコネクタのこのリリースには、マイナーなセキュリティの改善とバグ修正が含まれています。

現時点では、3.9.49 リリースは標準モードと制限モードで利用できます。

BlueXPアイデンティティおよびアクセス管理 (IAM)

- BlueXPユーザーに複数のロールを割り当てるためのサポート。
- BlueXP組織 (Org/フォルダ/プロジェクト) の複数のリソースにロールを割り当てるためのサポート
- ロールは現在、プラットフォームとデータ サービスの 2 つのカテゴリのいずれかに関連付けられています。

制限モードではBlueXP IAMが使用されるようになりました

BlueXP ID およびアクセス管理 (IAM) が制限モードで使用されるようになりました。

BlueXP ID およびアクセス管理 (IAM) は、 BlueXP を標準モードおよび制限モードで使用するときにBlueXPアカウントによって提供されていた以前の機能を置き換え、強化するリソースおよびアクセス管理モデルです。

関連情報

- "BlueXP IAMについて学ぶ"
- "BlueXP IAMを使い始める"

BlueXP IAM は、リソースと権限のよりきめ細かな管理を提供します。

- 最上位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。
- _フォルダー_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。
- 強化されたリソース管理により、リソースを 1 つ以上のフォルダーまたはプロジェクトに関連付けることができます。

  たとえば、 Cloud Volumes ONTAPシステムを複数のプロジェクトに関連付けることができます。

- 強化された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ロールを割り当てることができます。

これらの機能強化により、ユーザーが実行できるアクションやアクセスできるリソースをより適切に制御できるようになります。

BlueXP IAM が制限モードの既存アカウントに与える影響

BlueXPにログインすると、次の変更に気付くでしょう。

- あなたの_アカウント_は_組織_と呼ばれるようになりました
- _ワークスペース_は_プロジェクト_と呼ばれるようになりました
- ユーザー ロールの名前が変更されました。
  - アカウント管理者 が 組織管理者 になりました
  - ワークスペース管理者 が フォルダーまたはプロジェクト管理者 になりました
  - コンプライアンス ビューア は 分類ビューア に変更されました
- 設定からBlueXPのIDとアクセス管理にアクセスして、これらの拡張機能を活用できます。

次の点に注意してください。

- 既存のユーザーや作業環境に変更はありません。
- ロールの名前は変更されていますが、権限の観点からは違いはありません。ユーザーは引き続き、以前と同じ作業環境にアクセスできます。
- BlueXPへのログイン方法に変更はありません。 BlueXP IAM は、 BlueXPアカウントと同様に、 NetApp クラウド ログイン、 NetAppサポート サイトの資格情報、およびフェデレーション接続で動作します。
- 複数のBlueXPアカウントをお持ちの場合は、複数のBlueXP組織が存在することになります。

BlueXP IAM の API

この変更により、 BlueXP IAM の新しい API が導入されますが、以前のテナンシー API との下位互換性があります。 "BlueXP IAMのAPIについて学ぶ"

サポートされている展開モード

BlueXP IAM は、 BlueXP を標準モードおよび制限モードで使用する場合にサポートされます。 BlueXP をプライベート モードで使用している場合は、引き続きBlueXP _アカウント_を使用してワークスペース、ユーザー、およびリソースを管理します。

プライベートモードリリース（**3.9.48**）

新しいプライベートモードリリースがダウンロード可能になりました。 "NetAppサポート サイト"

3.9.48 リリースには、次のBlueXPコンポーネントとサービスの更新が含まれています。

コンポーネントまたはサービス	このリリースに含まれるバージョン	前回のプライベートモードリリース以降の変更点
コネクタ	3.9.48	に行く "BlueXPコネクタページの新機能"バージョン 3.9.48 に含まれる変更を参照してください。
バックアップとリカバリ	2025年2月21日	に行く "BlueXP backup and recoveryページの新機能"2025 年 2 月のリリースに含まれる変更点を参照してください。

コンポーネントまたはサービス	このリリースに含まれるバージョン	前回のプライベートモードリリース以降の変更点
分類	2025年1月22日（バージョン1.39）	に行く "BlueXP classificationページの新機能"1.39 リリースに含まれる変更点を参照してください。

2025年1月13日

コネクタ **3.9.48**

BlueXPコネクタのこのリリースには、マイナーなセキュリティの改善とバグ修正が含まれています。

現時点では、3.9.48 リリースは標準モードと制限モードで利用できます。

BlueXPアイデンティティおよびアクセス管理

- リソース ページに、未検出のリソースが表示されるようになりました。未検出のリソースとは、 BlueXP が認識しているものの、作業環境が作成されていないストレージ リソースです。たとえば、デジタル アドバイザーに表示されるリソースのうち、まだ作業環境がないものは、未検出のリソースとしてリソース ページに表示されます。
- Amazon FSx for NetApp ONTAPリソースは、IAM ロールに関連付けることができないため、IAM リソース ページには表示されません。これらのリソースは、それぞれのキャンバスまたはワークロードから表示できます。

追加の**BlueXP**サービスのサポートケースを作成する

BlueXP をサポートに登録すると、 BlueXP のWeb ベース コンソールから直接サポート ケースを作成できます。ケースを作成するときは、問題が関連付けられているサービスを選択する必要があります。

このリリースから、サポート ケースを作成し、追加のBlueXPサービスに関連付けることができるようになりました。

- BlueXP disaster recovery
- BlueXPランサムウェア対策サービス

"サポートケースの作成について詳しくは" 。

2024年12月16日

コネクタイメージを取得するための新しい安全なエンドポイント

コネクタをインストールするとき、または自動アップグレードが発生するとき、コネクタはリポジトリに接続して、インストールまたはアップグレード用のイメージをダウンロードします。デフォルトでは、コネクタは常に次のエンドポイントに接続します。

- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

明確な場所を指定できないため、最初のエンドポイントにはワイルドカードが含まれます。リポジトリの負荷分散はサービス プロバイダーによって管理されるため、ダウンロードはさまざまなエンドポイントから発生

する可能性があります。

セキュリティ強化のため、コネクタは専用エンドポイントからインストール イメージとアップグレード イメージをダウンロードできるようになりました。

- https://bluexpinfraprod.eastus2.data.azurecr.io
- https://bluexpinfraprod.azurecr.io

ファイアウォール ルールから既存のエンドポイントを削除し、新しいエンドポイントを許可して、これらの新しいエンドポイントの使用を開始することをお勧めします。

これらの新しいエンドポイントは、コネクタの 3.9.47 リリース以降でサポートされます。コネクタの以前のリリースとの下位互換性はありません。

次の点に注意してください。

- 既存のエンドポイントは引き続きサポートされます。新しいエンドポイントを使用しない場合は、変更は必要ありません。
- コネクタはまず既存のエンドポイントに接続します。これらのエンドポイントにアクセスできない場合、コネクタは自動的に新しいエンドポイントに接続します。
- 新しいエンドポイントは、次のシナリオではサポートされません。
  - コネクタが政府地域にインストールされている場合。
  - コネクタをBlueXP backup and recoveryまたはBlueXP ransomware protectionと併用する場合。

  どちらのシナリオでも、既存のエンドポイントを引き続き使用できます。

2024年12月9日

コネクタ 3.9.47

BlueXPコネクタのこのリリースには、バグ修正と、コネクタのインストール中に接続されるエンドポイントの変更が含まれています。

現時点では、3.9.47 リリースは標準モードと制限モードで利用できます。

インストール中に**NetApp**サポートに連絡するエンドポイント

コネクタを手動でインストールすると、インストーラは\https://support.netapp.com.に接続しなくなります。

インストーラーは依然として\https://mysupport.netapp.com.に接続します

BlueXPアイデンティティおよびアクセス管理

コネクタ ページには、現在利用可能なコネクタのみがリストされます。削除したコネクタは表示されなくなります。

2024年11月26日

プライベートモードリリース（**3.9.46**）

新しいプライベートモードリリースがダウンロード可能になりました。 "NetAppサポート サイト"

3.9.46 リリースには、次のBlueXPコンポーネントとサービスの更新が含まれています。

コンポーネントまたはサービス	このリリースに含まれるバージョン	前回のプライベートモードリリース以降の変更点
コネクタ	3.9.46	マイナーなセキュリティの改善とバグ修正
バックアップとリカバリ	2024年11月22日	に行く "BlueXP backup and recoveryページの新機能"2024年11月のリリースに含まれる変更点を参照してください
分類	2024年11月4日（バージョン1.37）	に行く "BlueXP classificationページの新機能"1.32から1.37リリースに含まれる変更点を参照してください
Cloud Volumes ONTAP管理	2024年11月11日	に行く "Cloud Volumes ONTAP管理ページの新機能"2024年10月と2024年11月のリリースに含まれる変更点を参照してください。
オンプレミスのONTAPクラスタ管理	2024年11月26日	に行く "オンプレミスのONTAPクラスタ管理ページの新機能"2024年11月のリリースに含まれる変更点を参照してください

BlueXP digital walletとBlueXP replicationもプライベート モードに含まれていますが、以前のプライベート モード リリースから変更はありません。

プライベート モードの詳細（アップグレード方法を含む）については、以下を参照してください。

- "プライベートモードについて学ぶ"
- "プライベートモードでBlueXPを始める方法を学ぶ"
- "プライベートモード使用時にコネクタをアップグレードする方法を学びます"

2024年11月11日

コネクタ **3.9.46**

BlueXPコネクタのこのリリースには、マイナーなセキュリティの改善とバグ修正が含まれています。

現時点では、3.9.46 リリースは標準モードと制限モードで利用できます。

IAM プロジェクトの **ID**

BlueXP ID およびアクセス管理からプロジェクトの ID を表示できるようになりました。 API 呼び出しを行うときに ID を使用する必要がある場合があります。

"プロジェクトのIDを取得する方法を学ぶ" 。

2024年10月10日

コネクタ **3.9.45** パッチ

このパッチにはバグ修正が含まれています。

2024年10月7日

BlueXPアイデンティティおよびアクセス管理

BlueXP ID およびアクセス管理 (IAM) は、 BlueXP を標準モードで使用するときにBlueXPアカウントによって提供されていた以前の機能を置き換え、強化する新しいリソースおよびアクセス管理モデルです。

BlueXP IAM は、リソースと権限のよりきめ細かな管理を提供します。

- 最上位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。
- _フォルダー_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。
- 強化されたリソース管理により、リソースを 1 つ以上のフォルダーまたはプロジェクトに関連付けることができます。

  たとえば、 Cloud Volumes ONTAPシステムを複数のプロジェクトに関連付けることができます。

- 強化された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ロールを割り当てることができます。

これらの機能強化により、ユーザーが実行できるアクションやアクセスできるリソースをより適切に制御できるようになります。

BlueXP IAMが既存のアカウントに与える影響

BlueXPにログインすると、次の変更に気付くでしょう。

- あなたの_アカウント_は_組織_と呼ばれるようになりました
- _ワークスペース_は_プロジェクト_と呼ばれるようになりました
- ユーザー ロールの名前が変更されました。
  - アカウント管理者 が 組織管理者 になりました
  - ワークスペース管理者 が フォルダーまたはプロジェクト管理者 になりました
  - コンプライアンス ビューア は 分類ビューア に変更されました
- 設定からBlueXPのIDとアクセス管理にアクセスして、これらの拡張機能を活用できます。

次の点に注意してください。

- 既存のユーザーや作業環境に変更はありません。
- ロールの名前は変更されていますが、権限の観点からは違いはありません。ユーザーは引き続き、以前と同じ作業環境にアクセスできます。

- BlueXPへのログイン方法に変更はありません。 BlueXP IAM は、 BlueXPアカウントと同様に、 NetApp クラウド ログイン、 NetAppサポート サイトの資格情報、およびフェデレーション接続で動作します。
- 複数のBlueXPアカウントをお持ちの場合は、複数のBlueXP組織が存在することになります。

BlueXP IAM の API

この変更により、 BlueXP IAM の新しい API が導入されますが、以前のテナンシー API との下位互換性があります。 "BlueXP IAMのAPIについて学ぶ"

サポートされている展開モード

BlueXP を標準モードで使用する場合、 BlueXP IAM がサポートされます。 BlueXP を制限モードまたはプライベート モードで使用している場合は、引き続きBlueXP _アカウント_を使用してワークスペース、ユーザー、およびリソースを管理します。

次はどこへ行くか

- "BlueXP IAMについて学ぶ"
- "BlueXP IAMを使い始める"

コネクタ **3.9.45**

このリリースには、拡張されたオペレーティング システムのサポートとバグ修正が含まれています。

3.9.45 リリースは、標準モードと制限モードで利用できます。

Ubuntu 24.04 LTSのサポート

3.9.45 リリース以降、 BlueXP は、標準モードまたは制限モードでBlueXP を使用する場合、Ubuntu 24.04 LTS ホスト上のコネクタの新規インストールをサポートするようになりました。

"コネクタホストの要件を表示する" 。

RHELホストでの**SELinux**のサポート

BlueXP は、強制モードまたは許可モードのいずれかで SELinux が有効になっている Red Hat Enterprise Linux ホストでコネクタをサポートするようになりました。

SELinux のサポートは、標準モードと制限モードでは 3.9.40 リリースから、プライベート モードでは 3.9.42 リリースから開始されます。

次の制限に注意してください。

- BlueXP は、Ubuntu ホストでの SELinux をサポートしていません。
- Cloud Volumes ONTAPシステムの管理は、オペレーティング システムで SELinux が有効になっているコネクタではサポートされません。

"SELinuxについて詳しく知る"

2024年9月30日

プライベートモードリリース（**3.9.44**）

新しいプライベート モード リリースをNetAppサポート サイトからダウンロードできるようになりました。

このリリースには、プライベート モードでサポートされているBlueXPコンポーネントとサービスの次のバージョンが含まれています。

サービス	含まれるバージョン
コネクタ	3.9.44
バックアップとリカバリ	2024年9月27日
分類	2024年5月15日（バージョン1.31）
Cloud Volumes ONTAP管理	2024年9月9日
デジタルウォレット	2023年7月30日
オンプレミスのONTAPクラスタ管理	2024年4月22日
レプリケーション	2022年9月18日

コネクタの場合、3.9.44 プライベート モード リリースには、2024 年 8 月と 2024 年 9 月のリリースで導入された更新が含まれています。特に注目すべきは、Red Hat Enterprise Linux 9.4 のサポートです。

これらのBlueXPコンポーネントおよびサービスのバージョンに含まれる内容の詳細については、各BlueXPサービスのリリース ノートを参照してください。

- "コネクタの2024年9月リリースの新機能"
- "コネクタの2024年8月リリースの新機能"
- "BlueXP backup and recoveryの新機能"
- "BlueXP classificationの新機能"
- "BlueXPのCloud Volumes ONTAP管理の新機能"

プライベート モードの詳細（アップグレード方法を含む）については、以下を参照してください。

- "プライベートモードについて学ぶ"
- "プライベートモードでBlueXPを始める方法を学ぶ"
- "プライベートモード使用時にコネクタをアップグレードする方法を学びます"

2024年9月9日

コネクタ **3.9.44**

このリリースには、Docker Engine 26 のサポート、SSL 証明書の機能強化、およびバグ修正が含まれています。

3.9.44 リリースは、標準モードと制限モードで利用できます。

新規インストールでの **Docker Engine 26** のサポート

コネクタの 3.9.44 リリース以降、Ubuntu ホスト上の新しいコネクタ インストールで Docker Engine 26 がサ

ポートされるようになりました。

3.9.44 リリースより前に作成された既存のコネクタがある場合、Ubuntu ホストでサポートされる最大バージョンは Docker Engine 25.0.5 のままです。

"Docker Engineの要件について詳しく見る" 。

ローカル **UI** アクセス用の **SSL** 証明書を更新しました

BlueXP を制限モードまたはプライベート モードで使用する場合、クラウド リージョンまたはオンプレミスにデプロイされているコネクタ仮想マシンからユーザー インターフェイスにアクセスできます。デフォルトでは、 BlueXP は自己署名 SSL 証明書を使用して、コネクタ上で実行されている Web ベースのコンソールへの安全な HTTPS アクセスを提供します。

このリリースでは、新規および既存のコネクタの SSL 証明書に変更を加えました。

- 証明書の共通名が短縮ホスト名と一致するようになりました
- 証明書サブジェクト代替名は、ホストマシンの完全修飾ドメイン名（FQDN）です。

RHEL 9.4 のサポート

BlueXP は、 BlueXP を標準モードまたは制限モードで使用する場合に、Red Hat Enterprise Linux 9.4 ホストへのコネクタのインストールをサポートするようになりました。

RHEL 9.4 のサポートは、コネクタの 3.9.40 リリースから開始されます。

標準モードと制限モードでサポートされている RHEL バージョンの更新されたリストには、次のものが含まれるようになりました。

- 8.6～8.10
- 9.1～9.4

"コネクタによる RHEL 8 および 9 のサポートについて学ぶ" 。

すべての **RHEL** バージョンで **Podman 4.9.4** をサポート

Podman 4.9.4 は、サポートされているすべてのバージョンの Red Hat Enterprise Linux でサポートされるようになりました。バージョン 4.9.4 は以前は RHEL 8.10 でのみサポートされていました。

サポートされている Podman バージョンの更新されたリストには、Red Hat Enterprise Linux ホストの 4.6.1 および 4.9.4 が含まれています。

コネクタの 3.9.40 リリース以降の RHEL ホストには Podman が必要です。

"コネクタによる RHEL 8 および 9 のサポートについて学ぶ" 。

AWSと**Azure**の権限の更新

コネクタの AWS および Azure ポリシーを更新し、不要になった権限を削除しました。これらの権限はBlueXPエッジ キャッシングと Kubernetes クラスターの検出および管理に関連するものでしたが、2024 年 8 月をもってサポートされなくなりました。

- "AWSポリシーの変更点を確認する" 。
- "Azureポリシーの変更点を確認する" 。

2024年8月22日

コネクタ **3.9.43** パッチ

Cloud Volumes ONTAP 9.15.1 リリースをサポートするためにコネクタを更新しました。

このリリースのサポートには、Azure のコネクタ ポリシーの更新が含まれます。ポリシーには次の権限が含まれるようになりました。

```
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Compute/virtualMachineScaleSets/read",
"Microsoft.Compute/virtualMachineScaleSets/delete"
```

これらの権限は、仮想マシン スケール セットのCloud Volumes ONTAPサポートに必要です。既存のコネクタがあり、この新しい機能を使用する場合は、Azure 資格情報に関連付けられているカスタム ロールにこれらのアクセス許可を追加する必要があります。

- "Cloud Volumes ONTAP 9.15.1リリースについて"
- "コネクタの Azure 権限を表示する" 。

2024年8月8日

コネクタ **3.9.43**

このリリースには、マイナーな改善とバグ修正が含まれています。

3.9.43 リリースは、標準モードと制限モードで利用できます。

更新された**CPU**および**RAM**要件

より高い信頼性を提供し、 BlueXPとコネクタのパフォーマンスを向上させるために、コネクタ仮想マシンに追加の CPU と RAM が必要になりました。

- CPU: 8 コアまたは 8 vCPU (以前の要件は 4)
- RAM: 32 GB (以前の要件は 14 GB)

この変更の結果、 BlueXP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コネクタをデプロイする場合のデフォルトの VM インスタンス タイプは次のようになります。

- AWS: t3.2xlarge
- Azure: Standard_D8s_v3
- Google Cloud: n2-standard-8

更新された CPU および RAM の要件は、すべての新しいコネクタに適用されます。既存のコネクタの場合、

パフォーマンスと信頼性を向上させるために、CPU と RAM を増やすことをお勧めします。

RHEL 8.10 での **Podman 4.9.4** のサポート

Red Hat Enterprise Linux 8.10 ホストにコネクタをインストールするときに、Podman バージョン 4.9.4 がサポートされるようになりました。

アイデンティティ連携のためのユーザー検証

BlueXPで ID フェデレーションを使用する場合、 BlueXPに初めてログインする各ユーザーは、自分の ID を検証するための簡単なフォームに入力する必要があります。

2024年7月31日

プライベートモードリリース（**3.9.42**）

新しいプライベート モード リリースをNetAppサポート サイトからダウンロードできるようになりました。

RHEL 8および**9**のサポート

このリリースには、 BlueXP をプライベート モードで使用する場合に、Red Hat Enterprise Linux 8 または 9 ホストにコネクタをインストールするためのサポートが含まれています。次のバージョンの RHEL がサポートされています。

- 8.6～8.10
- 9.1～9.3

これらのオペレーティング システムでは、コンテナー オーケストレーション ツールとして Podman が必要です。

Podman の要件、既知の制限、オペレーティング システムのサポートの概要、RHEL 7 ホストがある場合の対処方法、開始方法などについて知っておく必要があります。

"コネクタによる RHEL 8 および 9 のサポートについて学ぶ" 。

このリリースに含まれるバージョン

このリリースには、プライベート モードでサポートされているBlueXPサービスの次のバージョンが含まれています。

サービス	含まれるバージョン
コネクタ	3.9.42
バックアップとリカバリ	2024年7月18日
分類	2024年7月1日（バージョン1.33）
Cloud Volumes ONTAP管理	2024年6月10日
デジタルウォレット	2023年7月30日
オンプレミスのONTAPクラスタ管理	2023年7月30日
レプリケーション	2022年9月18日

これらのBlueXPサービスのバージョンに含まれる内容の詳細については、各BlueXPサービスのリリース ノートを参照してください。

- "プライベートモードについて学ぶ"
- "プライベートモードでBlueXPを始める方法を学ぶ"
- "プライベートモード使用時にコネクタをアップグレードする方法を学びます"
- "BlueXP backup and recoveryの新機能について"
- "BlueXP classificationの新機能について学ぶ"
- "BlueXPのCloud Volumes ONTAP管理の新機能について学ぶ"

2024年7月15日

RHEL 8.10 のサポート

BlueXP は、標準モードまたは制限モードを使用しているときに、Red Hat Enterprise Linux 8.10 ホストにコネクタをインストールすることをサポートするようになりました。

RHEL 8.10 のサポートは、コネクタの 3.9.40 リリースから開始されます。

"コネクタによる RHEL 8 および 9 のサポートについて学ぶ" 。

2024年7月8日

コネクタ **3.9.42**

このリリースには、AWS カナダ西部 (カルガリー) リージョンのコネクタに対するマイナーな改善、バグ修正、およびサポートが含まれています。

3.9.42 リリースは、標準モードと制限モードで利用できます。

更新された**Docker**エンジン要件

コネクタが Ubuntu ホストにインストールされている場合、サポートされる Docker エンジンの最小バージョンは 23.0.6 になりました。以前は19.3.1でした。

サポートされる最大バージョンは 25.0.5 のままです。

"コネクタホストの要件を表示する" 。

メール認証が必要になりました

BlueXPにサインアップする新規ユーザーは、ログインする前に電子メール アドレスを確認することが必要になりました。

2024年6月12日

コネクタ **3.9.41**

BlueXPコネクタのこのリリースには、マイナーなセキュリティの改善とバグ修正が含まれています。

3.9.41 リリースは、標準モードと制限モードで利用できます。

2024年6月4日

プライベートモードリリース（**3.9.40**）

新しいプライベート モード リリースをNetAppサポート サイトからダウンロードできるようになりました。このリリースには、プライベート モードでサポートされているBlueXPサービスの次のバージョンが含まれています。

このプライベート モード リリースには、Red Hat Enterprise Linux 8 および 9 のコネクタのサポートは含まれていないことに注意してください。

サービス	含まれるバージョン
コネクタ	3.9.40
バックアップとリカバリ	2024年5月17日
分類	2024年5月15日（バージョン1.31）
Cloud Volumes ONTAP管理	2024年5月17日
デジタルウォレット	2023年7月30日
オンプレミスのONTAPクラスタ管理	2023年7月30日
レプリケーション	2022年9月18日

これらのBlueXPサービスのバージョンに含まれる内容の詳細については、各BlueXPサービスのリリース ノートを参照してください。

- "プライベートモードについて学ぶ"
- "プライベートモードでBlueXPを始める方法を学ぶ"
- "プライベートモード使用時にコネクタをアップグレードする方法を学びます"
- "BlueXP backup and recoveryの新機能について"
- "BlueXP classificationの新機能について学ぶ"
- "BlueXPのCloud Volumes ONTAP管理の新機能について学ぶ"

2024年5月17日

コネクタ **3.9.40**

BlueXPコネクタのこのリリースには、追加のオペレーティング システムのサポート、マイナーなセキュリティの改善、およびバグ修正が含まれています。

現時点では、3.9.40 リリースは標準モードと制限モードで利用できます。

RHEL 8および**9**のサポート

コネクタは、 BlueXP を標準モードまたは制限モードで使用する場合、_新しい_コネクタ インストールを備えた次のバージョンの Red Hat Enterprise Linux を実行しているホストでサポートされるようになりました。

- 8.6～8.9
- 9.1～9.3

これらのオペレーティング システムでは、コンテナー オーケストレーション ツールとして Podman が必要です。

Podman の要件、既知の制限、オペレーティング システムのサポートの概要、RHEL 7 ホストがある場合の対処方法、開始方法などについて知っておく必要があります。

"コネクタによる RHEL 8 および 9 のサポートについて学ぶ" 。

RHEL 7および**CentOS 7**のサポート終了

2024 年 6 月 30 日に、RHEL 7 はメンテナンス終了 (EOM) を迎え、CentOS 7 はサポート終了 (EOL) を迎えます。NetApp は、2024 年 6 月 30 日までこれらの Linux ディストリビューション上のコネクタのサポートを継続します。

"RHEL 7 または CentOS 7 で既存のコネクタを実行している場合の対処方法を学びます" 。

AWS 権限の更新

3.9.38 リリースでは、AWS のコネクタ ポリシーを更新し、「ec2:DescribeAvailabilityZones」権限を追加しました。Cloud Volumes ONTAPで AWS Local Zones をサポートするには、この権限が必要になりました。

- "コネクタの AWS 権限を表示する" 。
- "AWS Local Zonesのサポートについて詳しくはこちら"

NetApp Consoleの既知の制限

今回のリリースでサポートされていない、または今回のリリースでは正常に機能しないプラットフォーム、デバイス、機能が記載されています。これらの制限事項をよく確認してください。

これらの制限は、NEtApp コンソールと管理（エージェント、サービスとしてのソフトウェア (SaaS) プラットフォームなど）のセットアップに固有のものです。

コンソールエージェントの制限

172番台の**IP**アドレスとの競合の可能性

NetApp Consoleは、172.17.0.0/16 および 172.18.0.0/16 の範囲の IP アドレスを持つ 2 つのインターフェースを持つエージェントを展開します。

ネットワークにこれらのいずれかの範囲で構成されたサブネットがある場合、コンソールからの接続エラーが発生する可能性があります。たとえば、コンソールでオンプレミスのONTAPクラスターを検出できない場合があります。

ナレッジベースの記事を参照"エージェントIPが既存のネットワークと競合する"エージェントのインターフェースの IP アドレスを変更する方法については、こちらをご覧ください。

SSL復号化はサポートされていません

コンソールは、SSL 復号化が有効になっているファイアウォール構成をサポートしていません。 SSL 復号化が有効になっている場合、コンソールにエラー メッセージが表示され、エージェント インスタンスは非アクティブとして表示されます。

セキュリティを強化するために、"証明機関（CA）によって署名されたHTTPS証明書をインストールする" 。

ローカル**UI**を読み込むときに空白ページが表示される

エージェント上で実行されている Web ベースのコンソールをロードすると、インターフェイスが表示されず、空白のページが表示される場合があります。

この問題はキャッシュの問題に関連しています。回避策としては、シークレット モードまたはプライベート Web ブラウザ セッションを使用します。

共有**Linux**ホストはサポートされていません

エージェントは、他のアプリケーションと共有されている VM ではサポートされません。 VM はエージェント ソフトウェア専用にする必要があります。

サードパーティのエージェントと拡張機能

エージェント VM では、サードパーティ エージェントまたは VM 拡張機能はサポートされません。

サポートされている Linux オペレーティング システムの変更

NetApp は、特定の Linux オペレーティング システム上のコンソール エージェントのサポートを追加または削除することがあります。このサポートが既存のコンソール エージェントにどのように影響するかを確認してください。

サポートされているオペレーティングシステム

NetApp は、次の Linux オペレーティング システムでエージェントをサポートしています。

標準モード

手動インストール

- Ubuntu 24.04 LTS
- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8.6～8.10
  - 9.1～9.4

NetApp Consoleからの導入

Ubuntu 22.04 LTS

AWS Marketplaceからのデプロイメント

Ubuntu 22.04 LTS

Azure Marketplace からのデプロイ

Ubuntu 22.04 LTS

制限モード

手動インストール

- Ubuntu 24.04 LTS
- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8.6～8.10
  - 9.1～9.4

AWS Marketplaceからのデプロイメント

Ubuntu 22.04 LTS

Azure Marketplace からのデプロイ

Ubuntu 22.04 LTS

プライベートモード

手動インストール

- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8.6～8.10
  - 9.1～9.4

RHEL 8および9のサポート

RHEL 8 および 9 のサポートについては、次の点に注意してください。

制限事項

NetApp Data Classification は、オンプレミスにある RHEL 8 または 9 ホストにエージェントをインストールする場合にサポートされます。 RHEL 8 または 9 ホストが AWS、Azure、または Google Cloud に存在する場合はサポートされません。

コンテナオーケストレーションツール

RHEL 8 または 9 ホストにコンソール エージェントをインストールする場合は、コンテナ オーケストレーション ツールとして Podman ツールを使用する必要があります。 Docker Engine は RHEL 8 および 9 ではサポートされていません。

展開モード

コンソールを標準モードおよび制限モードで使用する場合、RHEL 8 および 9 がサポートされます。

サポートされているコンソールエージェントのバージョン

NetApp は、コンソール エージェントの次のバージョンから RHEL 8 および 9 をサポートしています。

- 3.9.40 コンソールを標準モードまたは制限モードで使用する場合

新規手動インストールのみ

RHEL 8 および 9 は、オンプレミスまたはクラウドで実行されているホストにエージェントを手動でインストールする場合、_新しい_エージェントのインストールでサポートされます。

RHELアップグレード

RHEL 7 ホストで既存のエージェントが実行されている場合、 NetApp はRHEL 7 オペレーティング システムを RHEL 8 または 9 にアップグレードすることをサポートしません。RHEL 7 または CentOS 7 の既存のコンソールエージェントの詳細 。

RHEL 7およびCentOS 7のサポート終了

2024 年 6 月 30 日に、RHEL 7 はメンテナンス終了 (EOM) に達し、CentOS 7 はサポート終了 (EOL) に達しました。 NetApp は、2024 年 6 月 30 日にこれらの Linux ディストリビューション上のエージェントのサポートを終了しました。

"Red Hat: Red Hat Enterprise Linux 7 のメンテナンス終了について知っておくべきこと"

RHEL 7 または **CentOS 7** 上の既存のコンソールエージェント

RHEL 7 または CentOS 7 で既存のエージェントが実行されている場合、 NetApp はオペレーティング システムを RHEL 8 または 9 にアップグレードまたは変換することをサポートしていません。サポートされているオペレーティング システムで新しいエージェントを作成する必要があります。

1. RHEL 8 または 9 ホストをセットアップします。
2. Podman をインストールします。
3. 新しいエージェントをインストールします。
4. 以前のエージェントが管理していたシステムを検出するようにエージェントを構成します。

関連情報

RHEL 8と**9**を使い始める方法

ホスト要件、Podman 要件、および Podman と Cagent をインストールする手順の詳細については、次のページを参照してください。

標準モード

- "オンプレミスでコンソールエージェントをインストールしてセットアップする"
- "AWSにコンソールエージェントを手動でインストールする"
- "Azure にコンソール エージェントを手動でインストールする"
- "Google Cloud にコンソール エージェントを手動でインストールする"

制限モード

"制限モードでの展開の準備"

システムを再発見する方法

新しいコンソール エージェントを展開した後、システムを再検出するには、次のページを参照してください。

- "既存のCloud Volumes ONTAPシステムを追加する"
- "オンプレミスのONTAPクラスタの検出"
- "FSx for ONTAPシステムを作成または検出する"
- "Azure NetApp Filesシステムを作成する"
- "Eシリーズシステムの詳細"
- "StorageGRIDシステムの詳細"

始めましょう

基本を学ぶ

NetApp Consoleについて学ぶ

NetApp Consoleは、オンプレミスとクラウド環境全体にわたるNetAppストレージとNetApp Data Servicesをエンタープライズ グレードで集中管理し、リアルタイムの分析情報、ワークフローの高速化、管理の簡素化を実現し、安全性とコンプライアンスを高く維持します。

ストレージ管理、データ モビリティ、データ保護、データ分析と制御を提供するサービス (SaaS) プラットフォームとして利用できます。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。

機能

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。

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

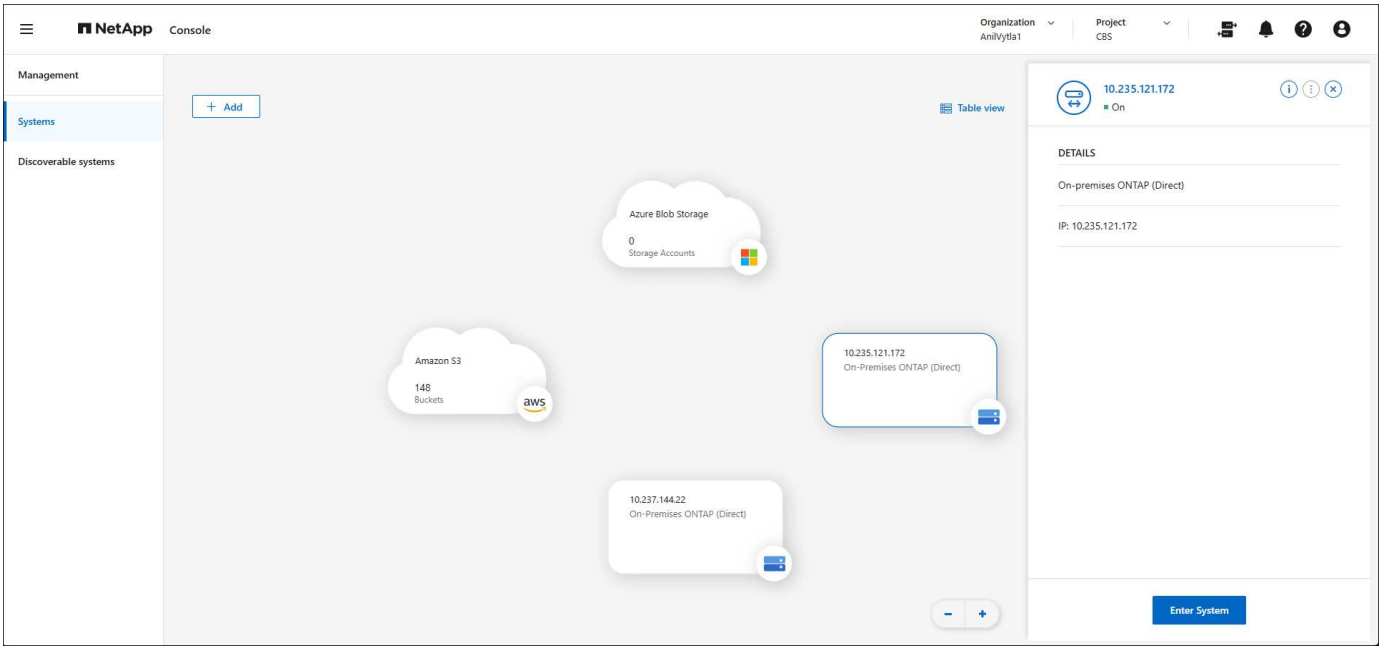
- Eシリーズシステム
- ONTAPクラスタ
- StorageGRIDシステム

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" 。

展開モード

NetApp は、NetApp Consoleに 2 つの導入モードを提供しています。標準モード では、完全な機能のためにソフトウェア アズ ア サービス (SaaS) レイヤーを使用し、制限モード では、アウトバウンド接続が制限されます。

NetApp は、アウトバウンド接続を必要としないサイト向けにBlueXP を引き続き提供します。 BlueXP はプライベート モードでのみ利用できます。"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エージェントについて学ぶ

コンソール エージェント は、クラウド ネットワークまたはオンプレミス ネットワークで実行されます。コンソール エージェントを使用して、 NetApp Consoleサービスをストレージ環境に接続します。

コンソールエージェントなしでできること

コンソール エージェントを展開しない場合でも、一部のコンソール機能とサービスが利用できます。

- Amazon FSx for NetApp ONTAP

  一部のアクションには、コンソール エージェントまたはNetAppワークロード リンクが必要です。 "コンソールエージェントまたはリンクが必要なアクションを確認する"

- 自動化ハブ
- Azure NetApp Files

  Azure NetApp Files を管理するためにコンソール エージェントは必要ありませんが、 NetApp Data Classificationを使用してAzure NetApp Files をスキャンするにはコンソール エージェントが必要です。

- Google Cloud NetApp Volumes
- NetApp Copy and Sync
- デジタルアドバイザー
- ライセンスの使用状況を監視します。サブスクリプションの監視にはコンソールエージェントが必要です。

  通常、コンソール エージェントなしでNetApp Consoleにライセンスを追加できます。

  データは Cloud Cloud Volumes ONTAP Cloud Volumes ONTAP のノードベースのライセンスを追加するにはエージェントが必要です。

- オンプレミスのONTAPクラスタの直接検出

  オンプレミスのONTAPクラスターをコンソールに追加するためにコンソール エージェントは必要ありませんが、追加のコンソール機能とデータ サービスにはコンソール エージェントが必要です。

  "オンプレミスのONTAPクラスタの検出および管理オプションの詳細"

- ソフトウェアアップデート
- 持続可能性
- NetAppワークロード

コンソールエージェントが必要な場合

標準モードでは、コンソールには次のコンソール エージェントが必要です。

- アラート
- Amazon FSx for ONTAP の管理機能
- Amazon S3 ストレージ
- Azure BLOB ストレージ
- NetApp Backup and Recovery
- データ分類

- Cloud Volumes ONTAP
- NetApp Disaster Recovery
- Eシリーズシステム
- 経済効率[1]
- Google Cloud Storage バケット
- オンプレミスのONTAPクラスタとNetAppデータ サービスの統合
- NetApp Ransomware Resilience
- StorageGRIDシステム
- NetApp Cloud Tiering
- NetApp Volume Caching

[1] コンソール エージェントがなくてもこれらのサービスにアクセスできますが、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。

コンソールを制限モードで使用するには、常にコンソール 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。開始方法は、コンソールを標準モードで使用するか、制限モードで使用するかによって異なります。

- "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 インスタンス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。

標準モードまたは制限モードでは、インターネットにアクセスできる場合、コンソール エージェントは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インターフェー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。

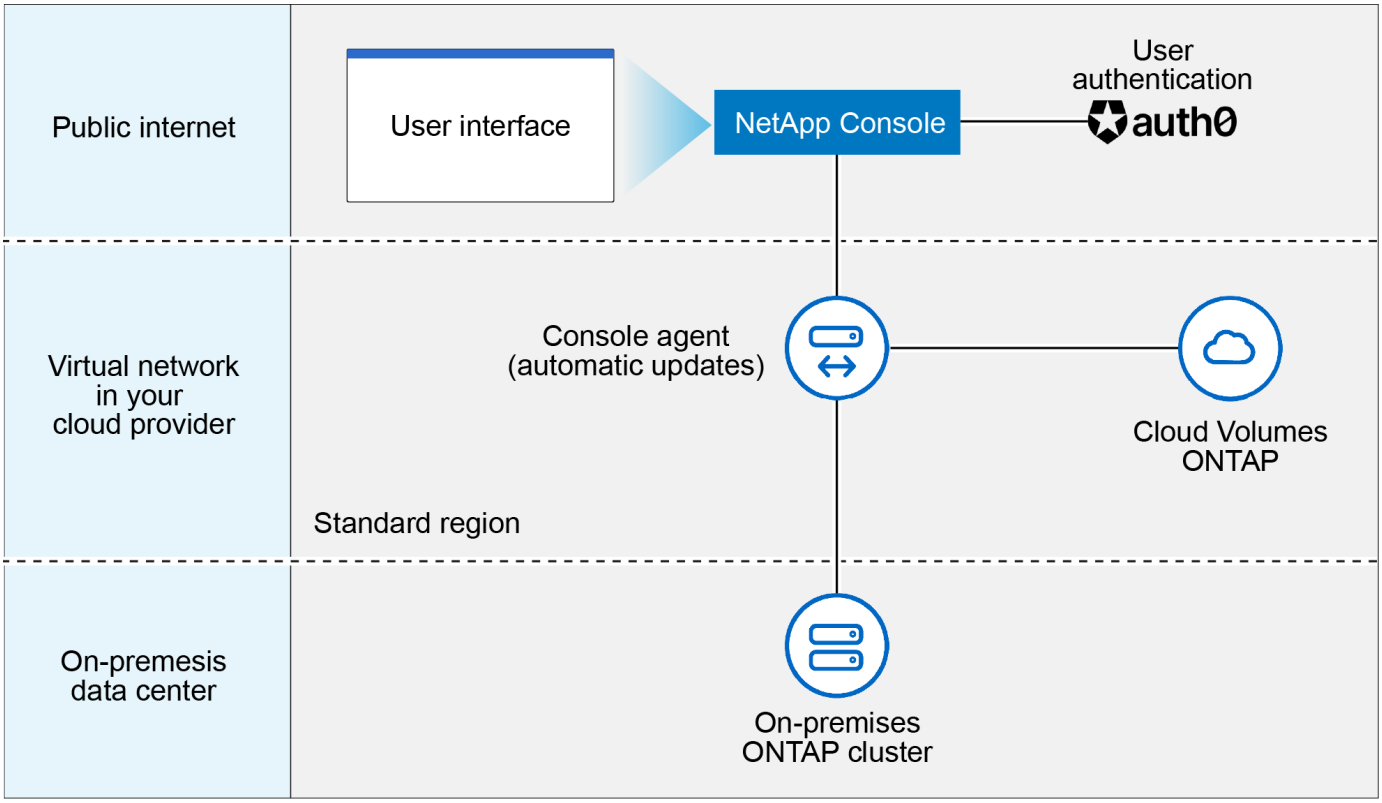
	標準モード	制限モード
NetApp ConsoleSaaS レイヤーへの接続が必要ですか**?**	はい	発信のみ
クラウド プロバイダーへの接続が必要ですか**?**	はい	はい、地域内です
コンソールエージェントのインストール	コンソール、クラウドマーケットプレイス、または手動インストールから	クラウドマーケットプレイスまたは手動インストール
コンソールエージェントのアップグレード	自動アップグレード	自動アップグレード
UIアクセス	コンソールSaaSレイヤーから	エージェントVMからローカルに
APIエンドポイント	コンソールSaaSレイヤー	コンソールエージェント
認証	auth0、NSS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	マーケットプレイスのサブスクリプションとBYOL	マーケットプレイ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 環境で使用します。

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.bluexp.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

マーケットプレイ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。

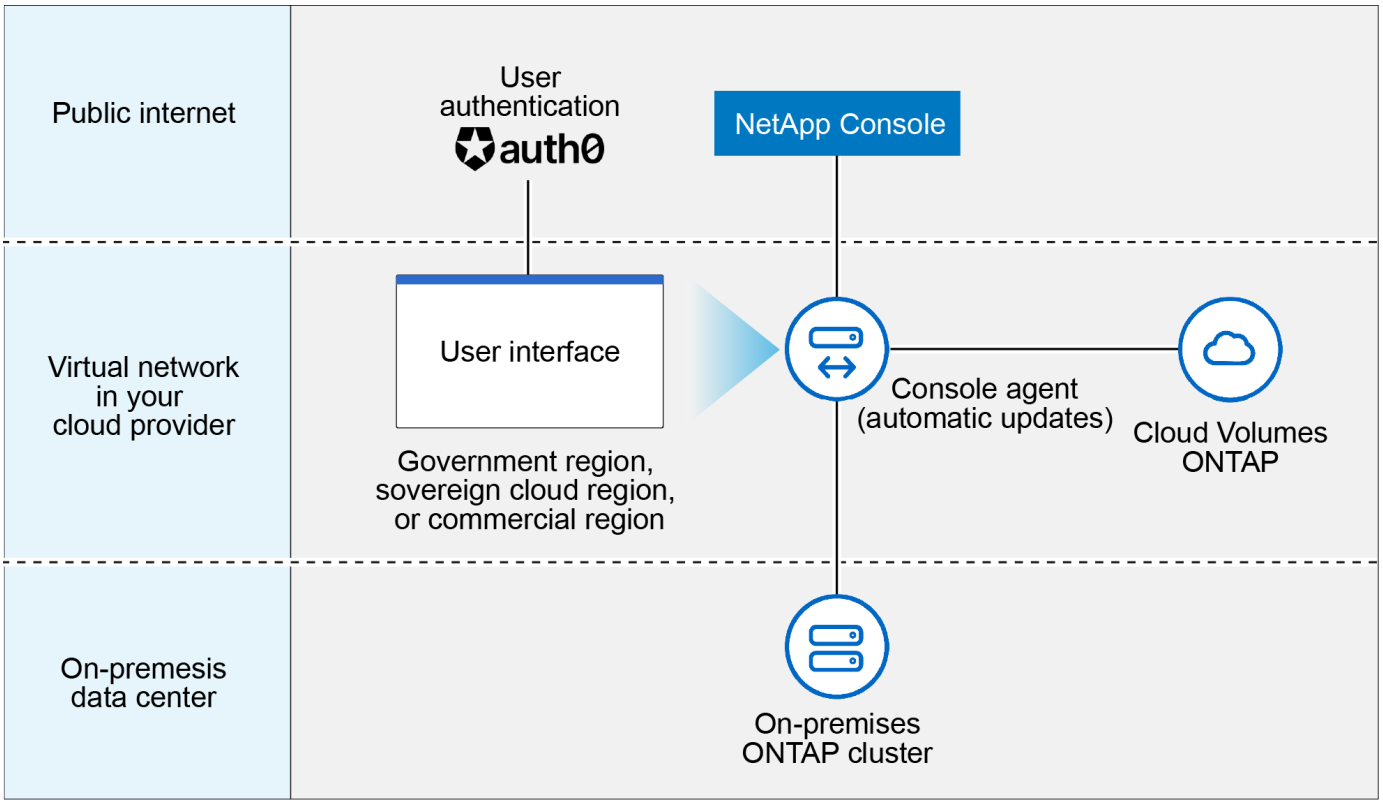
標準モードの開始方法

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	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アシスタントを使い始める

NetApp Consoleアシスタントの使用を開始する

組織管理者ロールを持つNetApp Consoleを初めて使用する場合は、コンソール アシスタントを使用して初期セットアップ プロセスをガイドできます。アシスタントを使用する

と、 NetAppサポート サイト (NSS) アカウントの追加、コンソール エージェントの追加、クラスターの追加、ライセンスまたはサブスクリプションの追加が可能になり、データの管理を簡単に開始できるようになります。

コンソールアシスタントにアクセスするために必要な役割

コンソール アシスタントは、組織管理者の役割を持つユーザーのみが利用できます。

コンソール アシスタントはいつ表示されますか?

必須のセットアップ タスクが完了するまで、コンソール アシスタントはNetApp Consoleホーム ページで利用できます。

アシスタントを使用して、次のタスクを完了します。一部のタスクは必須です。

- NetAppサポート サイト (NSS) アカウントを追加します。
- コンソール エージェントを展開してストレージ エステートに接続します (必須の手順)。
- クラスターを追加または検出してシステムを管理します (必須の手順)。
- マーケットプレイスのサブスクリプションまたは PAYGO ライセンスを追加します。
- オープンデータサービスリンク。

コンソールアシスタントを有効にする

デフォルトでは、 NetApp Consoleは、組織管理者ロールを持つ初めてのユーザーのホームページにコンソール アシスタントを表示します。

自分または他の誰かが必須項目を完了した後にのみ、アシスタントを解任することができます。必須項目を完了すると、アシスタントは組織内のすべてのユーザーに対して終了し、再び表示されなくなります。

コンソールアシスタントを使用して開始します

コンソール アシスタントは、次のタスクを実行してNetApp Console環境のセットアップをガイドします。

- NetAppサポート サイト (NSS) アカウントを追加します。
- オンプレミスまたはクラウドにコンソール エージェントを展開して、ストレージ資産に接続します。手動で展開するか、OVA をダウンロードして展開できます。この手順は必須です。
- クラスターを追加または検出してシステムを管理します。この手順は必須です。
- マーケットプレイスのサブスクリプションまたは PAYGO ライセンスを追加します。
- NetAppデータ サービスの詳細をご覧ください。

標準モードを始める

開始ワークフロー（標準モード）

コンソールのネットワークを準備し、サインアップしてアカウントを作成し、オプションでコンソール エージェントを作成して、標準モードでNetApp Consoleの使用を開始します。

標準モードでは、 NetAppの Software-as-a-service (SaaS) 製品としてホストされている Web ベースのコンソールにアクセスします。始める前に、以下の点を理解しておいてください"展開モード"そして"コンソールエージェント"。

1 "NetAppコンソールを使用するためのネットワークの準備"

NetAppコンソールにアクセスするコンピューターは、特定のエンドポイントに接続する必要があります。ネットワークで送信アクセスが制限されている場合は、これらのエンドポイントが許可されていることを確認する必要があります。

2 "サインアップして組織を作成する"

に行く "NetAppコンソール"そしてサインアップしてください。組織を作成するオプションが提供されますが、会社に既に組織が存在する場合は、その手順をスキップする必要があります。

この時点で、ログインしてストレージの管理や、 Digital Advisor、 Amazon FSx for ONTAP、 Azure NetApp Filesなどのサービスの使用を開始できます。"コンソールエージェントなしで何ができるかを学ぶ" 。

3 コンソールエージェントを作成する

高度なストレージ管理機能と一部のNetAppデータ サービスを使用するには、コンソール エージェントをインストールする必要があります。コンソール エージェントにより、コンソールはハイブリッド クラウド環境内のリソースとプロセスを管理できるようになります。

クラウドまたはオンプレミス ネットワークにコンソール エージェントを作成できます。

- "コンソールエージェントが必要な状況とその動作について詳しくは、"
- "AWS でコンソールエージェントを作成する方法を学ぶ"
- "Azure でコンソール エージェントを作成する方法を学びます"
- "Google Cloud でコンソール エージェントを作成する方法を学びます"
- "オンプレミスでコンソールエージェントを作成する方法を学ぶ"

Google Cloud でストレージとデータを管理するためNetApp Intelligent Data Services を使用するには、コンソール エージェントが Google Cloud で実行されていることを確認します。

4 "NetApp Intelligent Servicesに加入する（オプション）"

クラウド プロバイダーを通じてNetApp Intelligent Servicesにサインアップし、時間単位 (PAYGO) または年間契約で支払います。 NetApp Intelligent Servicesには、 NetApp Backup and Recovery、 Cloud Volumes ONTAP、 NetApp Cloud Tiering、 NetApp Ransomware Resilience 、 NetApp Disaster Recovery が含まれます。 NetApp Data Classification は追加料金なしでサブスクリプションに含まれています。

NetApp Consoleのネットワークアクセスを準備する

NetApp Console、 NetApp Consoleエージェント、およびNetAppデータ サービスには、アウトバウンド インターネット アクセスと、必要なエンドポイントに接続する機能が必要です。

次のネットワーク アクセスを設定する必要があります。

- NetApp Consoleに SaaS (Software as a Service) としてアクセスするコンピュータ
- オンプレミスまたはクラウドにインストールしたコンソール エージェントを展開するネットワークの場所。
- Cloud Volumes ONTAPを含む特定のNetAppデータ サービスの追加エンドポイント。

NetApp は、コンソールとコンソール エージェントに必要なネットワーク エンドポイントを削減し、セキュリティを強化して導入を簡素化しました。重要なのは、バージョン 4.0.0 より前のすべてのデプロイメントが引き続き完全にサポートされることです。以前のエンドポイントは既存のエージェントで引き続き使用できますが、 NetApp、エージェントのアップグレードが成功したことを確認した後、ファイアウォール ルールを現在のエンドポイントに更新することを強くお勧めします。"エンドポイント リストを更新する方法について説明します。"

NetApp Consoleが接続するエンドポイント

NetApp Consoleにアクセスする各コンピューターは、以下にリストされているエンドポイントに接続されている必要があります。

システムは、次の 2 つのシナリオでこれらのエンドポイントに接続します。

- アクセスしているコンピュータから "NetApp Console"サービスとしてのソフトウェア (SaaS) として。
- コンソール エージェント ホストに直接アクセスするコンピュータから、ログインして設定するか、エージェント ホストからコンソールにアクセスします。

エンドポイント	目的
https://mysupport.netapp.com	ライセンス情報を取得し、 AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、 AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェア アップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、 NetApp、ファイアウォール ルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

コンソールエージェントのネットワークを準備する

コンソール エージェントをオンプレミスまたはクラウドにインストールし、エンドポイントに接続してコンソールによって開始されたアクションを完了します。

コンソール エージェントは、 NetApp Consoleと同じエンドポイントにアクセスできる必要があります。また、エージェントのインストール場所に応じて追加のエンドポイントにもアクセスできる必要があります。

コンソール エージェントをインストールする前に、ネットワーク エンドポイント アクセスを設定します。

- "コンソールエージェントの AWS ネットワークアクセスを設定する"
- "コンソール エージェントの Azure ネットワーク アクセスを設定する"
- "コンソール エージェントの Google Cloud ネットワーク アクセスを設定する"
- "コンソール エージェントのオンプレミス ネットワーク アクセスを設定する"

Cloud Volumes ONTAPのネットワークを準備する

一部のNetAppデータ サービスとCloud Volumes ONTAP、エージェントに追加のアウトバウンド インターネット アクセスが必要です。

Cloud Volumes ONTAPのエンドポイント

- "AWS のCloud Volumes ONTAPのエンドポイント"
- "Azure のCloud Volumes ONTAPのエンドポイント"
- "Google Cloud のCloud Volumes ONTAPのエンドポイント"

"それぞれのNetAppデータ サービスのドキュメントを参照してください。"

NetApp Consoleにサインアップまたはログイン

NetApp Consoleは、Web ベースのコンソールからアクセスできます。コンソールを使い始めるには、まず、 NetAppサポート サイトの認証情報を使用してサインアップまたはログインするか、 NetApp Consoleログインを作成します。

タスク概要

コンソールに初めてアクセスする場合は、次のいずれかのオプションを使用してサインアップまたはログインできます。

NetApp Consoleログイン

ログインを作成してサインアップできます。この認証方法では、電子メール アドレスとパスワードを指定する必要があります。メールアドレスを確認したら、ログインして、まだ所属していない場合は組織を作成できます。

NetAppサポート サイト **(NSS)** の認証情報

既存のNetAppサポート サイトの認証情報をお持ちの場合は、コンソールにサインアップする必要はありません。 NSS 認証情報を使用してログインすると、まだ組織に属していない場合は、コンソールで組織を作成するように求められます。

登録したメールアドレスにワンタイムパスコード（OTP）が送信されます。サインインを試行するたびに新しい OTP が生成されます。

フェデレーション接続

会社にすでにNetApp Consoleインスタンスがある場合は、コンソール管理者が、企業ディレクトリの資格情報 (フェデレーション ID) を使用してログインするためのシングル サインオンを設定している可能性があります。

"NetApp Consoleでアイデンティティフェデレーションを使用する方法を学びます" 。

手順

1. ウェブブラウザを開いて、 "NetApp Console"
2. NetAppサポート サイトのアカウントをお持ちの場合、またはすでに ID フェデレーションを設定している場合は、ログイン ページでアカウントに関連付けられている電子メール アドレスを直接入力します。

   どちらの場合も、最初のログインの一環としてコンソールにサインアップされます。
3. コンソール ログインを作成してサインアップする場合は、[サインアップ] を選択します。
   a. *サインアップ*ページで必要な情報を入力し、*次へ*を選択します。

      サインアップフォームでは英語の文字のみが許可されていることに注意してください。

   b. 受信トレイで、電子メール アドレスを確認するための手順が記載されたNetAppからの電子メールを確認してください。

      コンソールにログインする前にこの手順を実行する必要があります。
4. ログイン後、エンドユーザー使用許諾契約書を確認し、条件に同意します。

   ユーザー アカウントがまだコンソール組織に属していない場合は、組織を作成するように求められます。

5. *ようこそ*ページで、コンソール組織の名前を入力します。

   コンソールは、コンソールの ID およびアクセス管理 (IAM) の最上位要素である組織を定義します。"IAM の詳細" 。

   会社にすでに組織があり、その組織に参加したい場合は、コンソールを閉じて、組織管理者に組織への関連付けを依頼してください。追加されたら、ログインしてコンソール組織にアクセスできるようになります。"既存の組織にメンバーを追加する方法を学ぶ" 。

6. *始めましょう*を選択します。

コンソールエージェントを作成する

AWS

AWS のコンソールエージェントのインストールオプション

AWS でコンソールエージェントを作成する方法はいくつかあります。 NetApp Console から直接行うのが最も一般的な方法です。

次のインストール オプションが利用可能です。

- "コンソールから直接コンソールエージェントを作成する"（これが標準オプションです）

  このアクションにより、選択した VPC で Linux とコンソール エージェント ソフトウェアを実行する EC2 インスタンスが起動されます。

- "AWS Marketplaceからコンソールエージェントを作成する"

  このアクションでは、Linux とコンソールエージェントソフトウェアを実行する EC2 インスタンスも起動しますが、デプロイメントはコンソールからではなく AWS Marketplace から直接開始されます。

- "自分のLinuxホストにソフトウェアをダウンロードして手動でインストールする"

選択したインストール オプションは、インストールの準備方法に影響します。これには、AWS でリソースを認証および管理するために必要な権限をコンソールに付与する方法が含まれます。

NetApp ConsoleからAWSにコンソールエージェントを作成する

NetApp Consoleから直接 AWS にコンソール エージェントを作成できます。コンソールから AWS にコンソールエージェントを作成する前に、ネットワークを設定し、AWS 権限を準備する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1: AWS**にコンソールエージェントを展開するためのネットワークを設定する

コンソール エージェントをインストールする予定のネットワークの場所が次の要件をサポートしていること

を確認します。これらの要件により、コンソール エージェントはハイブリッド クラウド内のリソースとプロセスを管理できるようになります。

VPCとサブネット

コンソール エージェントを作成するときは、そのエージェントが存在する VPC とサブネットを指定する必要があります。

ターゲットネットワークへの接続

コンソール エージェントには、システムを作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムまたはストレージ システムを作成する予定のネットワークなどです。

アウトバウンドインターネットアクセス

コンソール エージェントを展開するネットワークの場所には、特定のエンドポイントに接続するための送信インターネット接続が必要です。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

エンドポイント	目的
AWS サービス (amazonaws.com): • クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理（IAM） • キー管理サービス (KMS) • セキュリティトークンサービス（STS） • シンプルストレージサービス（S3）	AWS リソースを管理します。エンドポイントは AWS リージョンによって異なります。 "詳細についてはAWSドキュメントを参照してください"
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。

エンドポイント	目的
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォールルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

NetAppコンソールから接続されたエンドポイント

SaaS レイヤーを通じて提供される Web ベースのNetApp Consoleを使用すると、複数のエンドポイントに接続してデータ管理タスクが完了します。これには、コンソールからコンソール エージェントを展開するために接続されるエンドポイントが含まれます。

"NetAppコンソールから接続されたエンドポイントのリストを表示します" 。

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用している場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インターネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

コンソール エージェントを作成した後、このネットワーク要件を実装する必要があります。

ステップ**2:** コンソールエージェントの**AWS**権限を設定する

コンソールは、VPC にコンソールエージェントインスタンスをデプロイする前に、AWS で認証する必要があります。次のいずれかの認証方法を選択できます。

- コンソールに必要な権限を持つIAMロールを割り当てます
- 必要な権限を持つIAMユーザーにAWSアクセスキーとシークレットキーを提供します

どちらのオプションを使用する場合でも、最初のステップは IAM ポリシーを作成することです。このポリシーには、コンソールから AWS のコンソールエージェントインスタンスを起動するために必要な権限のみが含まれています。

必要に応じて、IAMを使用してIAMポリシーを制限することができます。 `Condition`要素。 "AWS ドキュメント: 条件要素"

手順

1. AWS IAM コンソールに移動します。
2. *ポリシー > ポリシーの作成*を選択します。
3. 「JSON」を選択します。
4. 次のポリシーをコピーして貼り付けます。

   このポリシーには、コンソールから AWS のコンソールエージェントインスタンスを起動するために必要な権限のみが含まれています。コンソールは、コンソールエージェントを作成すると、コンソールエージェントインスタンスに新しい権限セットを適用し、コンソールエージェントが AWS リソースを管理できるようにします。"コンソールエージェントインスタンス自体に必要な権限を表示する" 。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
```

```
            "cloudformation:ValidateTemplate",
            "ec2:AssociateIamInstanceProfile",
            "ec2:DescribeIamInstanceProfileAssociations",
            "ec2:DisassociateIamInstanceProfile",
            "iam:GetRole",
            "iam:TagRole",
            "kms:ListAliases",
            "cloudformation:ListStacks"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:TerminateInstances"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/OCCMInstance": "*"
            }
        },
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ]
    }
  ]
}
```

5. 必要に応じて、[次へ] を選択し、タグを追加します。
6. *次へ*を選択し、名前と説明を入力します。
7. *ポリシーの作成*を選択します。
8. コンソールが引き受けることができる IAM ロールまたは IAM ユーザーにポリシーをアタッチして、コンソールにアクセスキーを提供できるようにします。
   - (オプション 1) コンソールが引き受けることができる IAM ロールを設定します。
     i. ターゲットアカウントの AWS IAM コンソールに移動します。
     ii. [アクセス管理] で、**[ロール] > [ロールの作成]** を選択し、手順に従ってロールを作成します。
     iii. *信頼されたエンティティタイプ*で、*AWS アカウント*を選択します。
     iv. *別のAWSアカウント*を選択し、コンソールSaaSアカウントのIDを入力します: 952013314444
     v. 前のセクションで作成したポリシーを選択します。
     vi. ロールを作成したら、コンソール エージェントを作成するときにコンソールに貼り付けることができるように、ロール ARN をコピーします。
   - (オプション 2) コンソールにアクセスキーを提供できるように、IAM ユーザーの権限を設定します。

i. AWS IAM コンソールから [ユーザー] を選択し、ユーザー名を選択します。

ii. *権限の追加 > 既存のポリシーを直接添付*を選択します。

iii. 作成したポリシーを選択します。

iv. *次へ*を選択し、*権限の追加*を選択します。

v. IAM ユーザーのアクセスキーとシークレットキーがあることを確認します。

結果

これで、必要な権限を持つ IAM ロールまたは必要な権限を持つ IAM ユーザーが作成されているはずです。コンソールからコンソール エージェントを作成するときに、ロールまたはアクセス キーに関する情報を提供できます。

ステップ**3:** コンソールエージェントを作成する

コンソールの Web ベースのコンソールから直接コンソール エージェントを作成します。

タスク概要

- コンソールからコンソール エージェントを作成すると、デフォルト設定を使用して AWS に EC2 インスタンスがデプロイされます。コンソールエージェントを作成した後、CPU や RAM が少ない小さな EC2 インスタンスに切り替えないでください。"コンソールエージェントのデフォルト構成について学習します" 。
- コンソールがコンソール エージェントを作成すると、インスタンスの IAM ロールとインスタンス プロファイルが作成されます。このロールには、コンソールエージェントが AWS リソースを管理できるようにする権限が含まれています。将来のリリースで新しい権限が追加されたら、ロールが更新されるようにしてください。"コンソールエージェントのIAMポリシーの詳細" 。

開始する前に

次のものが必要です:

- AWS 認証方法: 必要な権限を持つ IAM ユーザーの IAM ロールまたはアクセスキーのいずれか。
- ネットワーク要件を満たす VPC とサブネット。
- EC2 インスタンスのキーペア。
- コンソール エージェントからのインターネット アクセスにプロキシが必要な場合のプロキシ サーバーの詳細。
- 設定"ネットワーク要件"。
- 設定"AWS 権限"。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、*エージェントのデプロイ > AWS*を選択します。
3. ウィザードの手順に従ってコンソール エージェントを作成します。
4. *はじめに*ページではプロセスの概要を説明します
5. **AWS** 認証情報 ページで、AWS リージョンを指定し、認証方法 (コンソールが引き受けることができる IAM ロール、または AWS アクセスキーとシークレットキーのいずれか) を選択します。

役割を引き受ける を選択した場合は、コンソール エージェント展開ウィザードから最初の資格情報セットを作成できます。追加の資格情報セットは、「資格情報」ページから作成する必要があります。これらはウィザードのドロップダウン リストで利用できるようになります。"追加の資格情報を追加する方法を学ぶ" 。

6. *詳細*ページで、コンソール エージェントに関する詳細を入力します。
   - インスタンスの名前を入力します。
   - インスタンスにカスタム タグ (メタデータ) を追加します。
   - コンソールで必要な権限を持つ新しいロールを作成するか、または既存のロールを選択するかを選択します。"必要な権限" 。
   - コンソール エージェントの EBS ディスクを暗号化するかどうかを選択します。デフォルトの暗号化キーを使用するか、カスタム キーを使用するかを選択できます。
7. ネットワーク ページで、インスタンスの VPC、サブネット、キーペアを指定し、パブリック IP アドレスを有効にするかどうかを選択し、オプションでプロキシ設定を指定します。

   コンソール エージェント仮想マシンにアクセスするための正しいキー ペアがあることを確認します。キーペアがないとアクセスできません。

8. セキュリティ グループ ページで、新しいセキュリティ グループを作成するか、必要な受信ルールと送信ルールを許可する既存のセキュリティ グループを選択するかを選択します。

   "AWS のセキュリティグループルールを表示する" 。

9. 選択内容を確認して、セットアップが正しいことを確認します。
   a. エージェント構成の検証 チェック ボックスはデフォルトでオンになっており、展開時にコンソールによってネットワーク接続要件が検証されます。コンソールがエージェントの展開に失敗した場合、トラブルシューティングに役立つレポートが提供されます。デプロイメントが成功した場合、レポートは提供されません。

   まだ使用している場合は"以前のエンドポイント"エージェントのアップグレードに使用すると、検証が失敗し、エラーが発生します。これを回避するには、チェックボックスをオフにして検証チェックをスキップします。

10. *追加*を選択します。

    コンソールは約 10 分でインスタンスを準備します。プロセスが完了するまでこのページに留まります。

結果

プロセスが完了すると、コンソール エージェントはコンソールから使用できるようになります。

デプロイメントが失敗した場合は、コンソールからレポートとログをダウンロードして、問題の解決に役立てることができます。"インストールの問題をトラブルシューティングする方法を学びます。"

コンソールエージェントを作成したのと同じ AWS アカウントに Amazon S3 バケットがある場合は、システム ページに Amazon S3 作業環境が自動的に表示されます。 "NetApp Consoleから S3 バケットを管理する方

法を学びます"

AWS Marketplaceからコンソールエージェントを作成する

AWS Marketplace から直接 AWS にコンソールエージェントを作成します。 AWS Marketplace からコンソールエージェントを作成するには、ネットワークを設定し、AWS のアクセス許可を準備し、インスタンスの要件を確認してから、コンソールエージェントを作成する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ネットワークを設定する

ハイブリッド クラウド リソースを管理するには、コンソール エージェントのネットワークの場所が次の要件を満たしていることを確認します。

VPCとサブネット

コンソール エージェントを作成するときは、そのエージェントが存在する VPC とサブネットを指定する必要があります。

ターゲットネットワークへの接続

コンソール エージェントには、システムを作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムまたはストレージ システムを作成する予定のネットワークなどです。

アウトバウンドインターネットアクセス

コンソール エージェントを展開するネットワークの場所には、特定のエンドポイントに接続するための送信インターネット接続が必要です。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

エンドポイント	目的
AWS サービス (amazonaws.com): • クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理（IAM） • キー管理サービス (KMS) • セキュリティトークンサービス（STS） • シンプルストレージサービス（S3）	AWS リソースを管理します。エンドポイントは AWS リージョンによって異なります。 "詳細についてはAWSドキュメントを参照してください"
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォール ルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用している場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インター

ネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

コンソール エージェントを作成した後、このネットワーク アクセスを実装します。

ステップ**2: AWS**権限を設定する

マーケットプレイスの展開を準備するには、AWS で IAM ポリシーを作成し、それを IAM ロールにアタッチします。 AWS Marketplace からコンソールエージェントを作成すると、その IAM ロールを選択するように求められます。

手順

1. AWS コンソールにログインし、IAM サービスに移動します。
2. ポリシーを作成します。
   a. *ポリシー > ポリシーの作成*を選択します。
   b. *JSON*を選択し、その内容をコピーして貼り付けます。"コンソールエージェントのIAMポリシー" 。
   c. 残りの手順を完了してポリシーを作成します。

      使用する予定のNetAppデータ サービスに基づいて、2 番目のポリシーを作成する必要がある場合があります。標準リージョンの場合、権限は 2 つのポリシーに分散されます。 AWS の管理ポリシーの最大文字サイズ制限により、2 つのポリシーが必要になります。"コンソールエージェントのIAMポリシーの詳細" 。
3. IAM ロールを作成します。
   a. *[ロール] > [ロールの作成]*を選択します。
   b. **AWS** サービス **> EC2** を選択します。
   c. 作成したポリシーを添付して権限を追加します。
   d. 残りの手順を完了してロールを作成します。

結果

これで、AWS Marketplace からのデプロイ時に EC2 インスタンスに関連付けることができる IAM ロールが作成されました。

ステップ**3:** インスタンス要件を確認する

コンソールエージェントを作成するときは、次の要件を満たす EC2 インスタンスタイプを選択する必要があります。

CPU

8コアまたは8vCPU

RAM

32 GB

AWS EC2インスタンスタイプ

上記の CPU および RAM の要件を満たすインスタンス タイプ。 t3.2xlarge をお勧めします。

ステップ**4:** コンソールエージェントを作成する

AWS Marketplace から直接コンソールエージェントを作成します。

タスク概要

AWS Marketplace からコンソールエージェントを作成すると、デフォルト設定を使用して AWS に EC2 インスタンスがデプロイされます。"コンソールエージェントのデフォルト構成について学習します" 。

開始する前に

次のものが必要です:

- ネットワーク要件を満たす VPC とサブネット。
- コンソール エージェントに必要な権限を含むポリシーがアタッチされた IAM ロール。
- IAM ユーザーが AWS Marketplace にサブスクライブしたり、サブスクライブ解除したりするための権限。
- インスタンスの CPU および RAM 要件を理解すること。
- EC2 インスタンスのキーペア。

手順

1. に行く "AWS Marketplace でのNetApp Consoleエージェントのリスト"
2. マーケットプレイス ページで、[サブスクリプションを続行] を選択します。
3. ソフトウェアをサブスクライブするには、「利用規約に同意」を選択します。

   サブスクリプションのプロセスには数分かかる場合があります。

4. サブスクリプションプロセスが完了したら、[構成に進む] を選択します。
5. *このソフトウェアを構成する*ページで、正しいリージョンが選択されていることを確認し、*起動を続行*を選択します。
6. このソフトウェアの起動 ページの アクションの選択 で、**EC2** 経由で起動 を選択し、起動 を選択します。

   EC2 コンソールを使用してインスタンスを起動し、IAM ロールをアタッチします。これは、**Web** サイトから起動 アクションでは不可能です。

7. プロンプトに従ってインスタンスを構成してデプロイします。

   ◦ 名前とタグ: インスタンスの名前とタグを入力します。

- アプリケーションと **OS** イメージ: このセクションはスキップします。コンソール エージェント AMI はすでに選択されています。
- インスタンス タイプ: リージョンの可用性に応じて、RAM と CPU の要件を満たすインスタンス タイプを選択します (t3.2xlarge が事前に選択されており、推奨されています)。
- キーペア **(**ログイン**)**: インスタンスに安全に接続するために使用するキーペアを選択します。
- ネットワーク設定: 必要に応じてネットワーク設定を編集します。
  - 必要な VPC とサブネットを選択します。
  - インスタンスにパブリック IP アドレスを割り当てるかどうかを指定します。
  - コンソール エージェント インスタンスに必要な接続方法 (SSH、HTTP、HTTPS) を有効にするセキュリティ グループ設定を指定します。

    "AWS のセキュリティグループルールを表示する" 。
- ストレージの構成: ルート ボリュームのデフォルトのサイズとディスク タイプを維持します。

  ルートボリュームで Amazon EBS 暗号化を有効にする場合は、[詳細] を選択し、[ボリューム **1**] を展開して、[暗号化] を選択し、KMS キーを選択します。
- 詳細: **IAM** インスタンス プロファイル で、コンソール エージェントに必要な権限を含む IAM ロールを選択します。
- 概要: 概要を確認し、*インスタンスの起動*を選択します。

  AWS は指定された設定でコンソールエージェントを起動し、コンソールエージェントは約 10 分で実行されます。

> インストールが失敗した場合は、トラブルシューティングに役立つログとレポートを表示できます。"インストールの問題をトラブルシューティングする方法を学びます。"

8. コンソール エージェント仮想マシンに接続しているホストとコンソール エージェントの URL から Web ブラウザーを開きます。
9. ログイン後、コンソール エージェントを設定します。
   a. コンソール エージェントに関連付けるコンソール組織を指定します。
   b. システムの名前を入力します。
   c. 安全な環境で実行していますか**?** の下で、制限モードを無効のままにします。

      コンソールを標準モードで使用するには、制限モードを無効にしておきます。安全な環境があり、このアカウントをコンソールのバックエンド サービスから切断する場合にのみ、制限モードを有効にする必要があります。もしそうなら、"NetApp Consoleを制限モードで使い始めるための手順" 。
   d. *始めましょう*を選択します。

結果

コンソール エージェントがインストールされ、コンソール組織に設定されました。

ウェブブラウザを開いて、 "NetApp Console"コンソールでコンソール エージェントの使用を開始します。

コンソールエージェントを作成したのと同じ AWS アカウントに Amazon S3 バケットがある場合は、システム ページに Amazon S3 作業環境が自動的に表示されます。 "NetApp Consoleから S3 バケットを管理する方法を学びます"

AWSにコンソールエージェントを手動でインストールする

AWS で実行されている Linux ホストにコンソールエージェントを手動でインストールできます。独自の Linux ホストにコンソールエージェントを手動でインストールするには、ホスト要件を確認し、ネットワークを設定し、AWS 権限を準備し、コンソールエージェントをインストールして、準備した権限を付与する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ホストの要件を確認する

コンソール エージェント ソフトウェアは、特定のオペレーティング システム要件、RAM 要件、ポート要件などを満たすホスト上で実行する必要があります。

> コンソール エージェントは、19000 ～ 19200 の UID と GID の範囲を予約します。この範囲は固定されており、変更することはできません。ホスト上のサードパーティ ソフトウェアがこの範囲内の UID または GID を使用している場合、エージェントのインストールは失敗します。NetApp、競合を回避するためにサードパーティ ソフトウェアがインストールされていないホストの使用を推奨しています。

専用ホスト

コンソール エージェントは、他のアプリケーションと共有されているホストではサポートされません。ホストは専用ホストである必要があります。ホストは、次のサイズ要件を満たす任意のアーキテクチャにすることができます。

- CPU: 8コアまたは8vCPU
- メモリ: 32 GB
- ディスク容量: ホストには 165 GB が推奨され、パーティション要件は次のとおりです。
  - `/opt`: 120 GiBの空き容量が必要です

    エージェントは `/opt`インストールするには `/opt/application/netapp`ディレクトリとその内容。
  - `/var`: 40 GiBの空き容量が必要です

    コンソールエージェントにはこのスペースが必要です `/var`Docker または Podman は、このディレクトリ内にコンテナを作成するように設計されているためです。具体的には、`/var/lib/containers/storage`ディレクトリ。このスペースでは外部マウントまたはシンボリックリンクは機能しません。

ハイパーバイザー

サポートされているオペレーティング システムを実行することが認定されているベア メタルまたはホスト型ハイパーバイザーが必要です。

オペレーティングシステムとコンテナの要件

コンソールを標準モードまたは制限モードで使用する場合、コンソール エージェントは次のオペレーティング システムでサポートされます。エージェントをインストールする前に、コンテナ オーケストレーション ツールが必要です。

オペレーティング システム	サポートされるOS バージョン	サポートされているエージェントのバージョン	必要なコンテナツール	SELinux は
Red Hat Enterprise Linux	9.1～9.4 8.6～8.10 • 英語版のみ。 • ホストは Red Hat Subscription Management に登録されている必要があります。登録されていない場合、ホストはエージェントのインストール中に必要なサードパーティ製ソフトウェアを更新するためにリポジトリにアクセスできません。	3.9.50 以降、コンソールが標準モードまたは制限モード	Podman バージョン 4.6.1 または 4.9.4 Podman の構成要件を表示する 。	強制モードまたは許可モードでサポートされます • Cloud Volumes ONTAPシステムの管理は、オペレーティングシステムで SELinux が有効になっているエージェントではサポートされません。
Ubuntu	24.04 LTS	3.9.45 以降、NetApp Consoleが標準モードまたは制限モード	Docker エンジン 23.06 から 28.0.0。	サポート対象外

AWS EC2インスタンスタイプ

上記の CPU および RAM の要件を満たすインスタンス タイプ。 t3.2xlarge をお勧めします。

鍵ペア

コンソールエージェントを作成するときは、インスタンスで使用する EC2 キーペアを選択する必要があります。

IMDSv2 使用時の PUT 応答ホップ制限

EC2 インスタンスで IMDSv2 が有効になっている場合 (これは新しい EC2 インスタンスのデフォルト設定です)、インスタンスの PUT 応答ホップ制限を 3 に変更する必要があります。 EC2 インスタンスの制限を変更しないと、エージェントを設定しようとすると UI 初期化エラーが発生します。

- "Amazon EC2 インスタンスで IMDSv2 の使用を必須にする"

- "AWSドキュメント: PUTレスポンスのホップ制限を変更する"

/optのディスク容量

100 GiBの空き容量が必要です

エージェントは `/opt`インストールするには `/opt/application/netapp`ディレクトリとその内容。

/varのディスク容量

20 GiBの空き容量が必要です

コンソールエージェントにはこのスペースが必要です `/var`Docker または Podman は、このディレクトリ内にコンテナを作成するように設計されているためです。具体的には、 `/var/lib/containers/storage`ディレクトリ。このスペースでは外部マウントまたはシンボリックリンクは機能しません。

ステップ**2: Podman**または**Docker Engine**をインストールする

オペレーティング システムに応じて、エージェントをインストールする前に Podman または Docker Engine のいずれかが必要になります。

- Red Hat Enterprise Linux 8 および 9 には Podman が必要です。

  サポートされているPodmanのバージョンを表示する 。

- Ubuntu には Docker Engine が必要です。

  サポートされている Docker エンジンのバージョンを表示する 。

例 **1.** 手順

ポッドマン

Podman をインストールして設定するには、次の手順に従います。

- podman.socket サービスを有効にして起動します
- Python3をインストールする
- podman-compose パッケージ バージョン 1.0.6 をインストールします。
- podman-composeをPATH環境変数に追加する
- Red Hat Enterprise Linux を使用している場合は、Podman バージョンが CNI ではなく Netavark Aardvark DNS を使用していることを確認してください。

DNS ポートの競合を避けるために、エージェントをインストールした後、aardvark-dns ポート (デフォルト: 53) を調整します。指示に従ってポートを構成します。

手順

1. ホストに podman-docker パッケージがインストールされている場合は削除します。

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Podman をインストールします。

   Podman は、公式の Red Hat Enterprise Linux リポジトリから入手できます。

   Red Hat Enterprise Linux 9 の場合:

```
sudo dnf install podman-2:<version>
```

   <version> は、インストールする Podman のサポートされているバージョンです。サポートされているPodmanのバージョンを表示する 。

   Red Hat Enterprise Linux 8 の場合:

```
sudo dnf install podman-3:<version>
```

   <version> は、インストールする Podman のサポートされているバージョンです。サポートされているPodmanのバージョンを表示する 。

3. podman.socket サービスを有効にして起動します。

```
sudo systemctl enable --now podman.socket
```

4. python3 をインストールします。

```
sudo dnf install python3
```

5. システムにまだインストールされていない場合は、EPEL リポジトリ パッケージをインストールします。
6. Red Hat Enterprise を使用している場合:

   podman-compose は、Extra Packages for Enterprise Linux (EPEL) リポジトリから入手できるため、この手順は必須です。

   Red Hat Enterprise Linux 9 の場合:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   Red Hat Enterprise Linux 8 の場合:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

7. podman-compose パッケージ 1.0.6 をインストールします。

```
sudo dnf install podman-compose-1.0.6
```

   使用して `dnf install`コマンドは、PATH 環境変数に podman-compose を追加するための要件を満たしています。インストールコマンドは、すでにインストールされているpodman-composeを/usr/binに追加します。 `secure_path`ホスト上のオプション。

8. Red Hat Enterprise Linux 8 を使用している場合は、Podman バージョンが CNI ではなく Aardvark DNS を備えた NetAvark を使用していることを確認します。

   a. 次のコマンドを実行して、networkBackend が CNI に設定されているかどうかを確認します。

```
podman info | grep networkBackend
```

   b. networkBackendが `CNI`、それを変更する必要があります `netavark`。

   c. インストール `netavark`そして `aardvark-dns`次のコマンドを使用します。

```
dnf install aardvark-dns netavark
```

d. 開く `/etc/containers/containers.conf`ファイルを編集し、network_backend オプションを変更して、「cni」の代わりに「netavark」を使用します。

もし `/etc/containers/containers.conf`存在しない場合は、設定を変更してください `/usr/share/containers/containers.conf`。

9. podman を再起動します。

```
systemctl restart podman
```

10. 次のコマンドを使用して、networkBackend が「netavark」に変更されていることを確認します。

```
podman info | grep networkBackend
```

Dockerエンジン

Docker のドキュメントに従って Docker Engine をインストールします。

手順

1. "Dockerからのインストール手順を見る"

   サポートされている Docker エンジン バージョンをインストールするには、手順に従ってください。最新バージョンはコンソールでサポートされていないため、インストールしないでください。

2. Docker が有効になっていて実行されていることを確認します。

```
sudo systemctl enable docker && sudo systemctl start docker
```

ステップ**3:** ネットワークを設定する

コンソール エージェントをインストールする予定のネットワークの場所が次の要件をサポートしていることを確認します。これらの要件を満たすことで、コンソール エージェントはハイブリッド クラウド環境内のリソースとプロセスを管理できるようになります。

ターゲットネットワークへの接続

コンソール エージェントには、システムを作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムまたはストレージ システムを作成する予定のネットワークなどです。

アウトバウンドインターネットアクセス

コンソール エージェントを展開するネットワークの場所には、特定のエンドポイントに接続するための送信インターネット接続が必要です。

Webベースの**NetApp Console**を使用する際にコンピュータから接続されるエンドポイント

Web ブラウザからコンソールにアクセスするコンピュータは、複数のエンドポイントに接続できる必要があります。コンソール エージェントを設定し、コンソールを日常的に使用するには、コンソールを使用す

る必要があります。

"NetAppコンソールのネットワークを準備する" 。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

エンドポイント	目的
AWS サービス (amazonaws.com): • クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理（IAM） • キー管理サービス (KMS) • セキュリティトークンサービス（STS） • シンプルストレージサービス（S3）	AWS リソースを管理します。エンドポイントは AWS リージョンによって異なります。 "詳細についてはAWSドキュメントを参照してください"
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォール ルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用している場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インター

ネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

ステップ**4:** コンソールの**AWS**権限を設定する

次のいずれかのオプションを使用して、 NetApp Consoleに AWS 権限を付与する必要があります。

- オプション 1: IAM ポリシーを作成し、EC2 インスタンスに関連付けることができる IAM ロールにポリシーをアタッチします。
- オプション 2: 必要な権限を持つ IAM ユーザーの AWS アクセスキーをコンソールに提供します。

コンソールの権限を準備するには、手順に従ってください。

IAMのロール

手順

1. AWS コンソールにログインし、IAM サービスに移動します。
2. ポリシーを作成します。
   a. *ポリシー > ポリシーの作成*を選択します。
   b. *JSON*を選択し、その内容をコピーして貼り付けます。"コンソールエージェントのIAMポリシー" 。
   c. 残りの手順を完了してポリシーを作成します。

      使用する予定のNetAppデータ サービスによっては、2 番目のポリシーを作成する必要がある場合があります。標準リージョンの場合、権限は 2 つのポリシーに分散されます。 AWS の管理ポリシーの最大文字サイズ制限により、2 つのポリシーが必要になります。"コンソールエージェントのIAMポリシーの詳細" 。
3. IAM ロールを作成します。
   a. *[ロール] > [ロールの作成]*を選択します。
   b. **AWS** サービス **> EC2** を選択します。
   c. 作成したポリシーを添付して権限を追加します。
   d. 残りの手順を完了してロールを作成します。

結果

コンソールエージェントをインストールした後、EC2 インスタンスに関連付けることができる IAM ロールが作成されます。

AWS アクセスキー

手順

1. AWS コンソールにログインし、IAM サービスに移動します。
2. ポリシーを作成します。
   a. *ポリシー > ポリシーの作成*を選択します。
   b. *JSON*を選択し、その内容をコピーして貼り付けます。"コンソールエージェントのIAMポリシー" 。
   c. 残りの手順を完了してポリシーを作成します。

      使用する予定のNetAppデータ サービスによっては、2 番目のポリシーを作成する必要がある場合があります。

   標準リージョンの場合、権限は 2 つのポリシーに分散されます。 AWS の管理ポリシーの最大文字サイズ制限により、2 つのポリシーが必要になります。"コンソールエージェントのIAMポリシーの詳細" 。
3. IAM ユーザーにポリシーをアタッチします。
   - "AWSドキュメント: IAMロールの作成"

- "AWSドキュメント: IAMポリシーの追加と削除"

4. コンソール エージェントをインストールした後、 NetApp Consoleに追加できるアクセス キーがユーザーにあることを確認します。

結果

これで、必要な権限を持つ IAM ユーザーと、コンソールに提供できるアクセス キーが作成されました。

ステップ**5:** コンソールエージェントをインストールする

前提条件が完了したら、独自の Linux ホストにソフトウェアを手動でインストールできます。

開始する前に

次のものが必要です:

- コンソール エージェントをインストールするためのルート権限。
- コンソール エージェントからのインターネット アクセスにプロキシが必要な場合のプロキシ サーバーの詳細。

  インストール後にプロキシ サーバーを構成するオプションがありますが、これを行うにはコンソール エージェントを再起動する必要があります。

- プロキシ サーバーが HTTPS を使用する場合、またはプロキシがインターセプト プロキシである場合は、CA 署名証明書。

> コンソール エージェントを手動でインストールする場合、透過プロキシ サーバーの証明書を設定することはできません。透過プロキシ サーバーの証明書を設定する必要がある場合は、インストール後にメンテナンス コンソールを使用する必要があります。詳細はこちら"エージェントメンテナンスコンソール"。

タスク概要

NetAppサポート サイトで入手できるインストーラーは、以前のバージョンである可能性があります。インストール後、新しいバージョンが利用可能な場合、コンソール エージェントは自動的に更新されます。

手順

1. ホストに *http_proxy* または *https_proxy* システム変数が設定されている場合は、それらを削除します。

```
unset http_proxy
unset https_proxy
```

   これらのシステム変数を削除しないと、インストールは失敗します。

2. コンソールエージェントソフトウェアを以下からダウンロードします。 "NetAppサポート サイト"それを Linux ホストにコピーします。

   ネットワークまたはクラウドで使用するための「オンライン」エージェント インストーラーをダウンロードする必要があります。

3. スクリプトを実行するための権限を割り当てます。

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

<version> は、ダウンロードしたコンソール エージェントのバージョンです。

4. Government Cloud 環境にインストールする場合は、構成チェックを無効にします。"手動インストールの構成チェックを無効にする方法を説明します。"
5. インストール スクリプトを実行します。

```
 ./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

ネットワークでインターネット アクセスにプロキシが必要な場合は、プロキシ情報を追加する必要があります。透過プロキシまたは明示プロキシのいずれかを追加できます。 --proxy および --cacert パラメータはオプションであり、追加するように要求されることはありません。プロキシ サーバーがある場合は、示されているようにパラメータを入力する必要があります。

CA 署名証明書を使用して明示的なプロキシ サーバーを構成する例を次に示します。

```
 ./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

`--proxy`次のいずれかの形式を使用して、コンソール エージェントが HTTP または HTTPS プロキシ サーバーを使用するように構成します。

- http://アドレス:ポート
- http://ユーザー名:パスワード@アドレス:ポート
- http://ドメイン名%92ユーザー名:パスワード@アドレス:ポート
- https://アドレス:ポート
- https://ユーザー名:パスワード@アドレス:ポート
- https://ドメイン名%92ユーザー名:パスワード@アドレス:ポート

  次の点に注意してください。

  - ユーザーはローカル ユーザーまたはドメイン ユーザーになります。
  - ドメイン ユーザーの場合は、上記のように \ の ASCII コードを使用する必要があります。
  - コンソール エージェントは、@ 文字を含むユーザー名またはパスワードをサポートしていません。
  - パスワードに以下の特殊文字が含まれている場合は、その特殊文字の前にバックスラッシュ (& または !) を付けてエスケープする必要があります。

例えば：

http://bxpproxyuser:netapp1\!@アドレス:3128

`--cacert`コンソール エージェントとプロキシ サーバー間の HTTPS アクセスに使用する CA 署名付き証明書を指定します。このパラメータは、HTTPS プロキシ サーバー、インターセプト プロキシ サーバー、および透過プロキシ サーバーに必須です。

+ 透過プロキシ サーバーを構成する例を次に示します。透過プロキシを構成する場合、プロキシ サーバーを定義する必要はありません。コンソール エージェント ホストには、CA 署名付き証明書のみを追加します。

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

1. Podman を使用した場合は、aardvark-dns ポートを調整する必要があります。
   a. コンソール エージェント仮想マシンに SSH で接続します。
   b. podman */usr/share/containers/containers.conf* ファイルを開き、Aardvark DNS サービス用に選択したポートを変更します。たとえば、54 に変更します。

      ```
      vi /usr/share/containers/containers.conf
      ...
      # Port to use for dns forwarding daemon with netavark in rootful
      bridge
      # mode and dns enabled.
      # Using an alternate port might be useful if other DNS services
      should
      # run on the machine.
      #
      dns_bind_port = 54
      ...
      Esc:wq
      ```

   c. コンソール エージェント仮想マシンを再起動します。
2. インストールが完了するまでお待ちください。

   プロキシ サーバーを指定した場合、インストールの最後に、コンソール エージェント サービス (occm) が 2 回再起動します。

インストールが失敗した場合は、インストール レポートとログを表示して問題の解決に役立てることができます。"インストールの問題をトラブルシューティングする方法を学びます。"

1. コンソール エージェント仮想マシンに接続しているホストから Web ブラウザを開き、次の URL を入力します。

https://ipaddress

2. ログイン後、コンソール エージェントを設定します。
   a. コンソール エージェントに関連付ける組織を指定します。
   b. システムの名前を入力します。
   c. 安全な環境で実行していますか**?** の下で、制限モードを無効のままにします。

      以下の手順ではコンソールを標準モードで使用する方法について説明しているため、制限モードは無効にしておく必要があります。安全な環境があり、このアカウントをバックエンド サービスから切断する場合にのみ、制限モードを有効にする必要があります。もしそうなら、"NetApp Consoleを制限モードで使い始めるための手順に従います" 。

   d. *始めましょう*を選択します。

コンソールエージェントを作成したのと同じ AWS アカウントに Amazon S3 バケットがある場合は、[システム] ページに Amazon S3 ストレージ システムが自動的に表示されます。 "NetApp ConsolePからS3バケットを管理する方法を学ぶ"

ステップ**6: NetApp Console**に権限を付与する

コンソールエージェントをインストールしたので、以前に設定した AWS 権限をコンソールに提供する必要があります。権限を付与すると、コンソールエージェントは AWS 内のデータとストレージインフラストラクチャを管理できるようになります。

IAMのロール

以前に作成した IAM ロールをコンソールエージェント EC2 インスタンスにアタッチします。

手順

1. Amazon EC2 コンソールに移動します。
2. *インスタンス*を選択します。
3. コンソール エージェント インスタンスを選択します。
4. *アクション > セキュリティ > IAM ロールの変更*を選択します。
5. IAM ロールを選択し、*IAM ロールの更新*を選択します。

に行く "NetApp Console"コンソール エージェントの使用を開始します。

AWS アクセスキー

必要な権限を持つ IAM ユーザーの AWS アクセスキーをコンソールに提供します。

手順

1. コンソールで正しいコンソール エージェントが現在選択されていることを確認します。
2. *管理 > 資格情報*を選択します。
3. *組織の資格情報*を選択します。
4. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: *Amazon Web Services > エージェントを選択します。
   b. 資格情報の定義: AWS アクセスキーとシークレットキーを入力します。
   c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。
   d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

に行く "NetApp Console"コンソール エージェントの使用を開始します。

Azure

Azure のコンソール エージェントのインストール オプション

Azure でコンソール エージェントを作成するには、いくつかの方法があります。NetApp Consoleから直接行うのが最も一般的な方法です。

次のインストール オプションが利用可能です。

- "NetApp Consoleから直接コンソールエージェントを作成する"（これが標準オプションです）

  このアクションにより、選択した VNet で Linux とコンソール エージェント ソフトウェアを実行する VM が起動します。

- "Azure Marketplace からコンソール エージェントを作成する"

このアクションでは、Linux とコンソール エージェント ソフトウェアを実行する VM も起動しますが、展開はコンソールからではなく、Azure Marketplace から直接開始されます。

- "自分のLinuxホストにソフトウェアをダウンロードして手動でインストールする"

選択したインストール オプションは、インストールの準備方法に影響します。これには、Azure でリソースを認証および管理するために必要なアクセス許可をコンソール エージェントに付与する方法が含まれます。

NetApp Consoleから Azure にコンソール エージェントを作成する

NetApp Consoleから Azure にコンソール エージェントを作成するには、ネットワークを設定し、Azure 権限を準備してから、コンソール エージェントを作成する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ネットワークを設定する

コンソール エージェントをインストールする予定のネットワークの場所が次の要件をサポートしていることを確認します。これらの要件により、コンソール エージェントはハイブリッド クラウド リソースを管理できるようになります。

Azureリージョン

Cloud Volumes ONTAPを使用する場合、コンソールエージェントは、管理するCloud Volumes ONTAPシステムと同じAzureリージョン、または "Azure リージョン ペア"Cloud Volumes ONTAPシステム用。この要件により、 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"

VNetとサブネット

コンソール エージェントを作成するときは、そのエージェントが存在する VNet とサブネットを指定する必要があります。

ターゲットネットワークへの接続

コンソール エージェントには、システムを作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムまたはストレージ システムを作成する予定のネットワークなどです。

アウトバウンドインターネットアクセス

コンソール エージェントを展開するネットワークの場所には、特定のエンドポイントに接続するための送信インターネット接続が必要です。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

エンドポイント	目的
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure パブリック リージョン内のリソースを管理します。
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure China リージョンのリソースを管理します。
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォール ルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

NetAppコンソールから接続されたエンドポイント

SaaS レイヤーを通じて提供される Web ベースのNetApp Consoleを使用すると、複数のエンドポイントに接続してデータ管理タスクが完了します。これには、コンソールからコンソール エージェントを展開するために接続されるエンドポイントが含まれます。

"NetAppコンソールから接続されたエンドポイントのリストを表示します" 。

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用している場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インターネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

コンソール エージェントを作成した後、このネットワーク要件を実装する必要があります。

ステップ **2:** コンソール エージェント展開ポリシー **(**カスタム ロール**)** を作成する

Azure にコンソール エージェントをデプロイする権限を持つカスタム ロールを作成する必要があります。

Azure アカウントまたは Microsoft Entra サービス プリンシパルに割り当てることができる Azure カスタム ロールを作成します。コンソールは Azure で認証し、これらのアクセス許可を使用してユーザーに代わってコンソール エージェント インスタンスを作成します。

コンソールはAzureにコンソールエージェントVMを展開し、 "システム割り当てマネージドID"必要なロールを作成し、それを VM に割り当てます。"コンソールが権限をどのように使用するかを確認します" 。

Azure ポータル、Azure PowerShell、Azure CLI、または REST API を使用して、Azure カスタム ロールを作成できます。次の手順は、Azure CLI を使用してロールを作成する方法を示しています。別の方法をご希望の場合は、 "Azureドキュメント"

手順

1. Azure の新しいカスタム ロールに必要なアクセス許可をコピーし、JSON ファイルに保存します。

   このカスタム ロールには、コンソールから Azure のコンソール エージェント VM を起動するために必要なアクセス許可のみが含まれています。このポリシーを他の状況では使用しないでください。コンソールは、コンソール エージェントを作成するときに、コンソール エージェントが Azure リソースを管理できるようにする新しいアクセス許可セットをコンソール エージェント VM に適用します。

```
{
    "Name": "Azure SetupAsService",
    "Actions": [
        "Microsoft.Compute/disks/delete",
        "Microsoft.Compute/disks/read",
        "Microsoft.Compute/disks/write",
        "Microsoft.Compute/locations/operations/read",
```

```
        "Microsoft.Compute/operations/read",
        "Microsoft.Compute/virtualMachines/instanceView/read",
        "Microsoft.Compute/virtualMachines/read",
        "Microsoft.Compute/virtualMachines/write",
        "Microsoft.Compute/virtualMachines/delete",
        "Microsoft.Compute/virtualMachines/extensions/write",
        "Microsoft.Compute/virtualMachines/extensions/read",
        "Microsoft.Compute/availabilitySets/read",
        "Microsoft.Network/locations/operationResults/read",
        "Microsoft.Network/locations/operations/read",
        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Network/networkInterfaces/read",
        "Microsoft.Network/networkInterfaces/write",
        "Microsoft.Network/networkInterfaces/delete",
        "Microsoft.Network/networkSecurityGroups/join/action",
        "Microsoft.Network/networkSecurityGroups/read",
        "Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
        "Microsoft.Network/virtualNetworks/virtualMachines/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/networkSecurityGroups/securityRules/read",
        "Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/networkSecurityGroups/securityRules/delete",
        "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
        "Microsoft.Network/networkInterfaces/ipConfigurations/read",
        "Microsoft.Resources/deployments/operations/read",
        "Microsoft.Resources/deployments/read",
        "Microsoft.Resources/deployments/delete",
        "Microsoft.Resources/deployments/cancel/action",
        "Microsoft.Resources/deployments/validate/action",
        "Microsoft.Resources/resources/read",
        "Microsoft.Resources/subscriptions/operationresults/read",
        "Microsoft.Resources/subscriptions/resourceGroups/delete",
        "Microsoft.Resources/subscriptions/resourceGroups/read",
```

```
"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
        "Microsoft.Resources/subscriptions/resourceGroups/write",
        "Microsoft.Authorization/roleDefinitions/write",
        "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Authorization/roleAssignments/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}
```

2. 割り当て可能なスコープに Azure サブスクリプション ID を追加して JSON を変更します。

   例

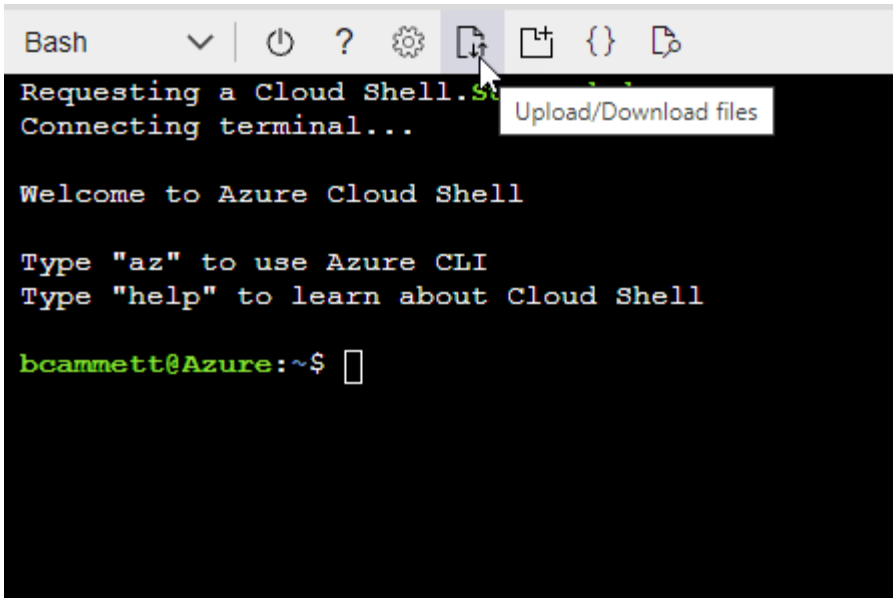
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],
```

3. JSON ファイルを使用して、Azure でカスタム ロールを作成します。

   次の手順では、Azure Cloud Shell で Bash を使用してロールを作成する方法について説明します。

   a. 始める "Azure クラウド シェル"Bash 環境を選択します。

   b. JSON ファイルをアップロードします。



c. 次の Azure CLI コマンドを入力します。

```
az role definition create --role-definition
Policy_for_Setup_As_Service_Azure.json
```

これで、*Azure SetupAsService* というカスタム ロールが作成されました。このカスタム ロールは、ユーザー アカウントまたはサービス プリンシパルに適用できます。

ステップ**3:** 認証を設定する

コンソールからコンソール エージェントを作成するときは、コンソールが Azure で認証して VM をデプロイできるようにするためのログインを提供する必要があります。次の 2 つのオプションがあります。

1. プロンプトが表示されたら、Azure アカウントでSign in。このアカウントには特定の Azure 権限が必要です。これがデフォルトのオプションです。
2. Microsoft Entra サービス プリンシパルに関する詳細を提供します。このサービス プリンシパルには特定のアクセス許可も必要です。

コンソールで使用するために、これらの認証方法のいずれかを準備するには、手順に従ってください。

Azureアカウント

コンソールからコンソール エージェントを展開するユーザーにカスタム ロールを割り当てます。

手順

1. Azure ポータルで、サブスクリプション サービスを開き、ユーザーのサブスクリプションを選択します。
2. アクセス制御 **(IAM)** をクリックします。
3. 追加 > ロール割り当ての追加 をクリックし、権限を追加します。
   a. **Azure SetupAsService** ロールを選択し、次へ をクリックします。

   Azure SetupAsService は、Azure のコンソール エージェント展開ポリシーで提供される既定の名前です。ロールに別の名前を選択した場合は、代わりにその名前を選択します。

   b. *ユーザー、グループ、またはサービス プリンシパル*を選択したままにします。
   c. *メンバーを選択*をクリックし、ユーザーアカウントを選択して*選択*をクリックします。
   d. *次へ*をクリックします。
   e. *レビュー+割り当て*をクリックします。

サービスプリンシパル

Azure アカウントでログインするのではなく、必要な権限を持つ Azure サービス プリンシパルの資格情報をコンソールに提供できます。

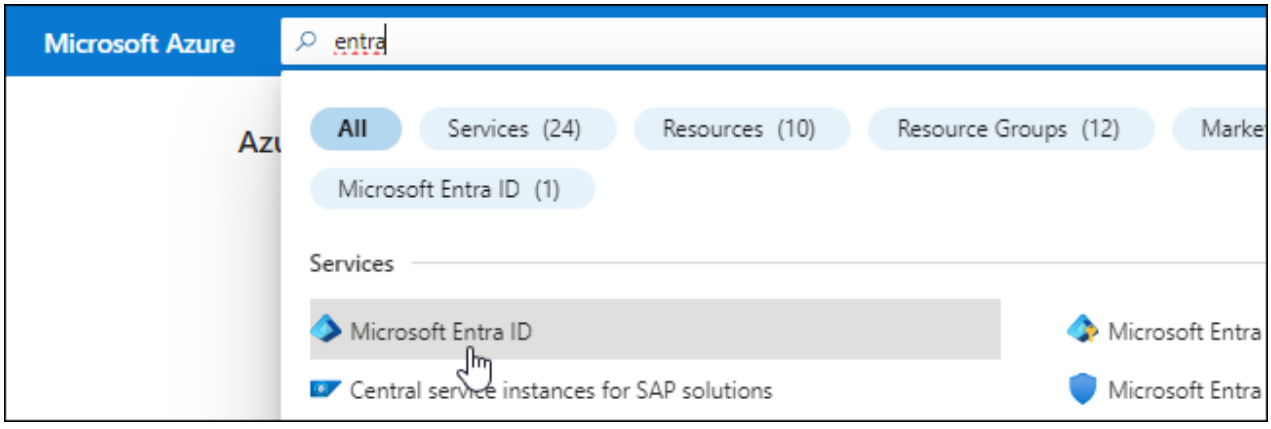
Microsoft Entra ID でサービス プリンシパルを作成して設定し、コンソールに必要な Azure 資格情報を取得します。

ロールベースのアクセス制御用の **Microsoft Entra** アプリケーションを作成する

1. Azure で Active Directory アプリケーションを作成し、そのアプリケーションをロールに割り当てるためのアクセス許可があることを確認します。

   詳細については、 "Microsoft Azure ドキュメント: 必要な権限"

2. Azure ポータルから、**Microsoft Entra ID** サービスを開きます。

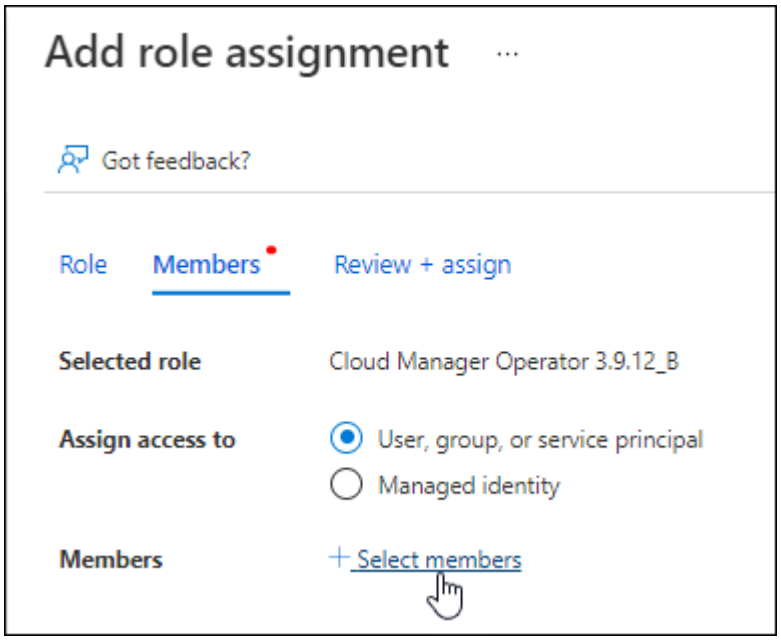


3. メニューで*アプリ登録*を選択します。
4. *新規登録*を選択します。
5. アプリケーションの詳細を指定します。
   - 名前: アプリケーションの名前を入力します。
   - アカウント タイプ: アカウント タイプを選択します (いずれのタイプもNetApp Consoleで使用できます)。
   - リダイレクト **URI**: このフィールドは空白のままにすることができます。
6. *登録*を選択します。

   AD アプリケーションとサービス プリンシパルを作成しました。

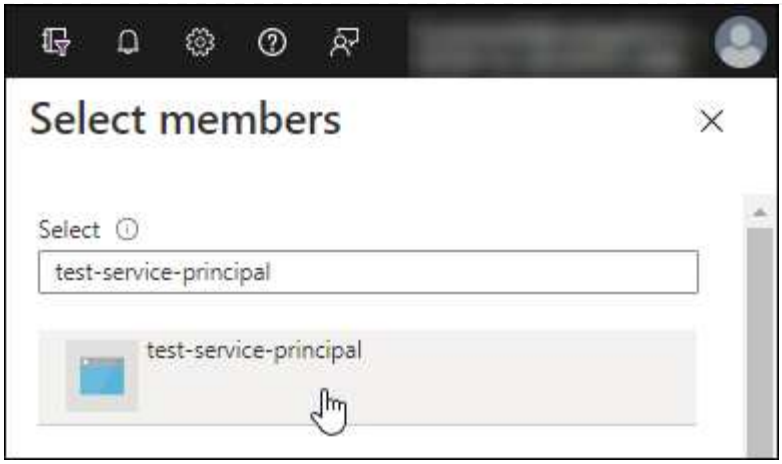
アプリケーションにカスタムロールを割り当てる

1. Azure ポータルから、サブスクリプション サービスを開きます。
2. サブスクリプションを選択します。
3. アクセス制御 **(IAM) >** 追加 **>** ロール割り当ての追加 をクリックします。
4. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*をクリックします。
5. *メンバー*タブで、次の手順を実行します。
   a. *ユーザー、グループ、またはサービス プリンシパル*を選択したままにします。
   b. *メンバーを選択*をクリックします。



   c. アプリケーションの名前を検索します。

      次に例を示します。



a. アプリケーションを選択し、「選択」をクリックします。

b. *次へ*をクリックします。

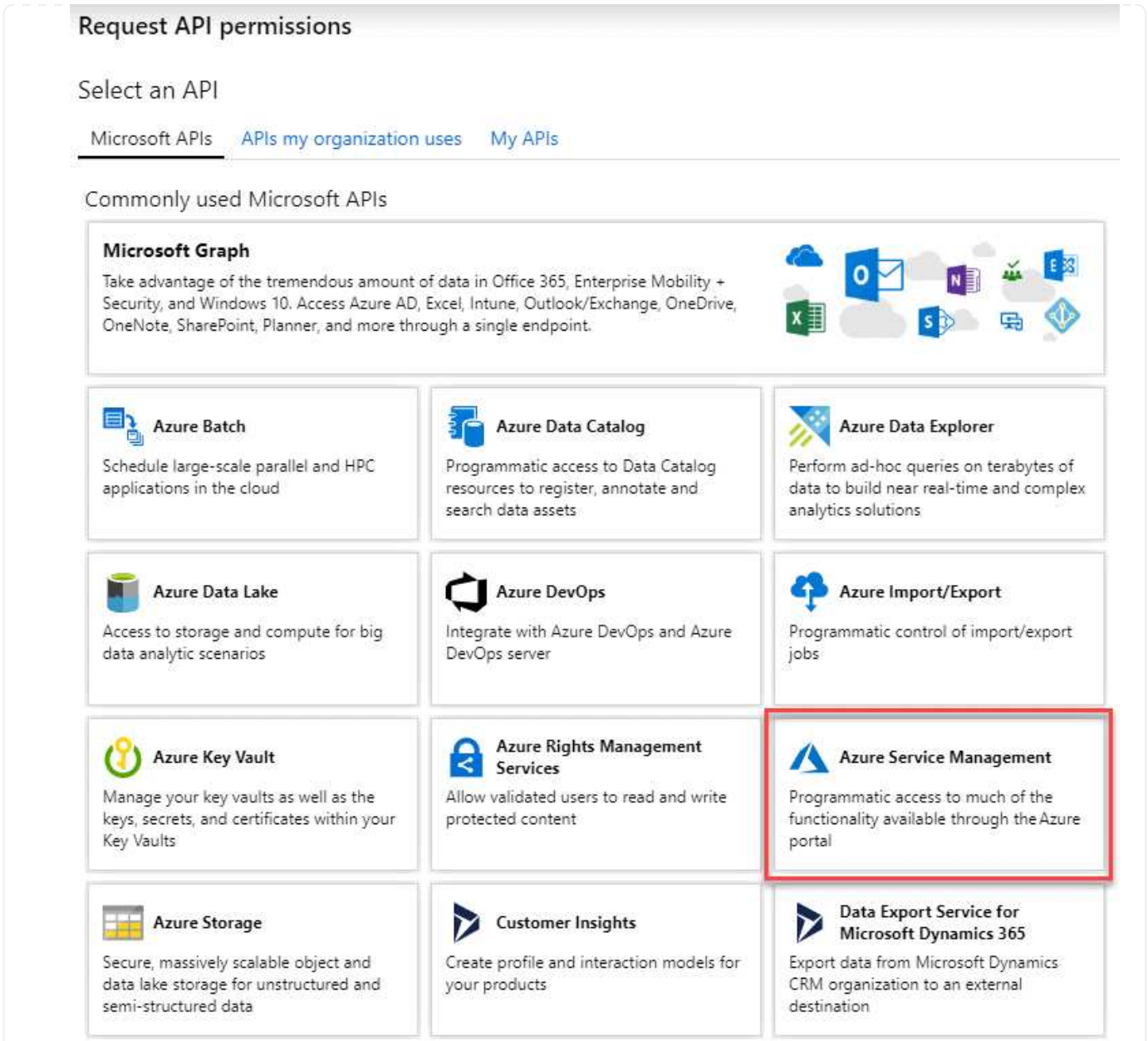
6. *レビュー+割り当て*をクリックします。

これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

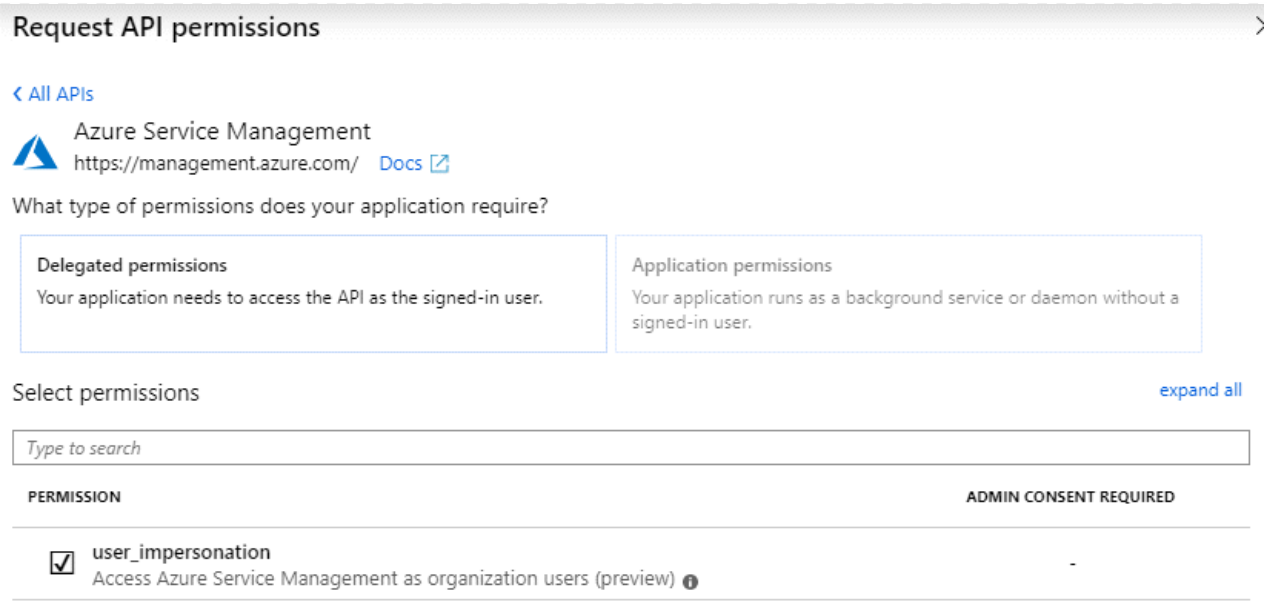
複数の Azure サブスクリプションのリソースを管理する場合は、サービス プリンシパルを各サブスクリプションにバインドする必要があります。たとえば、コンソールを使用すると、 Cloud Volumes ONTAPをデプロイするときに使用するサブスクリプションを選択できます。

Windows Azure サービス管理 **API** 権限を追加する

1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. **API** 権限 **>** 権限の追加 を選択します。
3. **Microsoft API** の下で、**Azure Service Management** を選択します。

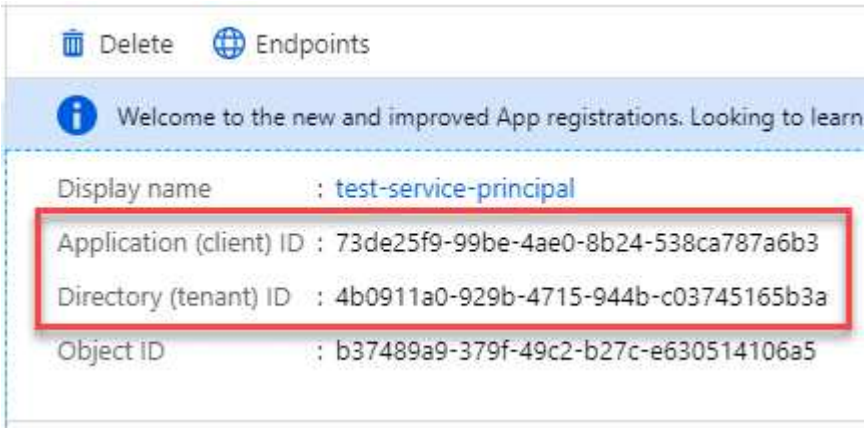


4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。



アプリケーションのアプリケーション**ID**とディレクトリ**ID**を取得します

1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. アプリケーション **(**クライアント**) ID** と ディレクトリ **(**テナント**) ID** をコピーします。



Azure アカウントをコンソールに追加するときは、アプリケーションのアプリケーション (クライアント) ID とディレクトリ (テナント) ID を指定する必要があります。コンソールは ID を使用してプログラムでサインインします。

クライアントシークレットを作成する

1. **Microsoft Entra ID** サービスを開きます。
2. *アプリ登録*を選択し、アプリケーションを選択します。
3. *証明書とシークレット > 新しいクライアント シークレット*を選択します。
4. シークレットの説明と期間を指定します。
5. *追加*を選択します。
6. クライアント シークレットの値をコピーします。

結果

これでサービス プリンシパルが設定され、アプリケーション (クライアント) ID、ディレクトリ (テナント) ID、およびクライアント シークレットの値がコピーされているはずです。コンソール エージェントを作成するときに、この情報をコンソールに入力する必要があります。

ステップ**4:** コンソールエージェントを作成する

NetApp Consoleから直接コンソール エージェントを作成します。

タスク概要

- コンソールからコンソール エージェントを作成すると、既定の構成を使用して Azure に仮想マシンがデプロイされます。コンソール エージェントを作成した後、CPU や RAM が少ない小さな VM インスタンスに切り替えないでください。"コンソールエージェントのデフォルト構成について学習します" 。
- コンソールはコンソール エージェントを展開するときに、カスタム ロールを作成し、それをコンソール エージェント VM に割り当てます。このロールには、コンソール エージェントが Azure リソースを管理できるようにする権限が含まれています。後続のリリースで新しい権限が追加されるので、ロールが最新の状態に保たれていることを確認する必要があります。"コンソールエージェントのカスタムロールの詳細" 。

開始する前に

次のものが必要です:

- Azure サブスクリプション。
- 選択した Azure リージョン内の VNet とサブネット。
- 組織ですべての送信インターネット トラフィックにプロキシが必要な場合のプロキシ サーバーの詳細:
  - IPアドレス
  - Credentials
  - HTTPS証明書
- コンソール エージェント仮想マシンにその認証方法を使用する場合は、SSH 公開キー。認証方法のもう 1 つのオプションは、パスワードを使用することです。

  "Azure の Linux VM への接続について学習します"

- コンソールエージェント用のAzureロールをコンソールが自動的に作成しないようにするには、独自のロールを作成する必要があります。"このページのポリシーを使用する" 。

  これらの権限は、コンソール エージェント インスタンス自体に適用されます。これは、コンソール エージェント VM を展開するために以前に設定した権限セットとは異なります。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、*エージェントのデプロイ > Azure*を選択します。
3. レビュー ページで、エージェントを展開するための要件を確認します。これらの要件についてはこのページの上部にも詳しく記載されています。
4. *仮想マシン認証*ページで、Azure のアクセス許可の設定方法に一致する認証オプションを選択します。
   - ログイン を選択して、必要な権限を持つ Microsoft アカウントにログインします。

     このフォームは Microsoft によって所有およびホストされています。資格情報がNetAppに提供されていません。

     すでに Azure アカウントにログインしている場合は、コンソールは自動的にそのアカウントを使用します。複数のアカウントをお持ちの場合は、正しいアカウントを使用していることを確認するために、最初にログアウトする必要がある場合があります。

   - 必要な権限を付与する Microsoft Entra サービス プリンシパルに関する情報を入力するには、**Active Directory** サービス プリンシパル を選択します。
     - アプリケーション（クライアント）ID
     - ディレクトリ（テナント）ID
     - クライアントシークレット

   サービスプリンシパルのこれらの値を取得する方法を学びます 。
5. 仮想マシン認証 ページで、Azure サブスクリプション、場所、新しいリソース グループまたは既存のリソース グループを選択し、作成するコンソール エージェント仮想マシンの認証方法を選択します。

   仮想マシンの認証方法は、パスワードまたは SSH 公開キーです。

   "Azure の Linux VM への接続について学習します"
6. *詳細*ページで、インスタンスの名前を入力し、タグを指定して、コンソールで必要な権限を持つ新しいロールを作成するか、または既存のロールを選択するかを選択します。"必要な権限" 。

   このロールに関連付けられた Azure サブスクリプションを選択できることに注意してください。選択した各サブスクリプションは、そのサブスクリプション内のリソースを管理するためのコンソール エージェント権限を付与します (たとえば、 Cloud Volumes ONTAP)。
7. ネットワーク ページで、VNet とサブネットを選択し、パブリック IP アドレスを有効にするかどうかを選択し、必要に応じてプロキシ構成を指定します。
   - セキュリティ グループ ページで、新しいセキュリティ グループを作成するか、必要な受信ルールと送信ルールを許可する既存のセキュリティ グループを選択するかを選択します。

     "Azure のセキュリティ グループ ルールを表示する" 。
8. 選択内容を確認して、セットアップが正しいことを確認します。
   a. エージェント構成の検証 チェック ボックスはデフォルトでオンになっており、展開時にコンソールによってネットワーク接続要件が検証されます。コンソールがエージェントの展開に失敗した場合、ト

ラブルシューティングに役立つレポートが提供されます。デプロイメントが成功した場合、レポートは提供されません。

まだ使用している場合は"以前のエンドポイント"エージェントのアップグレードに使用すると、検証が失敗し、エラーが発生します。これを回避するには、チェックボックスをオフにして検証チェックをスキップします。

9. *追加*を選択します。

コンソールは約 10 分でインスタンスを準備します。プロセスが完了するまでこのページに留まります。

結果

プロセスが完了すると、コンソール エージェントはコンソールから使用できるようになります。

デプロイメントが失敗した場合は、コンソールからレポートとログをダウンロードして、問題の解決に役立てることができます。"インストールの問題をトラブルシューティングする方法を学びます。"

コンソール エージェントを作成したのと同じ Azure サブスクリプションに Azure Blob ストレージがある場合は、システム ページに Azure Blob ストレージ システムが自動的に表示されます。 "NetApp ConsoleからAzure Blob ストレージを管理する方法を学びます"

Azure Marketplace からコンソール エージェントを作成する

Azure Marketplace から直接、Azure にコンソール エージェントを作成できます。Azure Marketplace からコンソール エージェントを作成するには、ネットワークを設定し、Azure のアクセス許可を準備し、インスタンスの要件を確認してから、コンソール エージェントを作成する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- レビュー"コンソールエージェントの制限"。

ステップ**1:** ネットワークを設定する

コンソール エージェントをインストールする予定のネットワークの場所が次の要件をサポートしていることを確認します。これらの要件により、コンソール エージェントはハイブリッド クラウド内のリソースを管理できるようになります。

Azureリージョン

Cloud Volumes ONTAPを使用する場合、コンソールエージェントは、管理するCloud Volumes ONTAPシステムと同じAzureリージョン、または "Azure リージョン ペア"Cloud Volumes ONTAPシステム用。この要件により、 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"

VNetとサブネット

コンソール エージェントを作成するときは、そのエージェントが存在する VNet とサブネットを指定する必要があります。

ターゲットネットワークへの接続

コンソール エージェントには、システムを作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムまたはストレージ システムを作成する予定のネットワークなどです。

アウトバウンドインターネットアクセス

コンソール エージェントを展開するネットワークの場所には、特定のエンドポイントに接続するための送信インターネット接続が必要です。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

エンドポイント	目的
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure パブリック リージョン内のリソースを管理します。
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure China リージョンのリソースを管理します。
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェア アップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォール ルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用している場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インター

ネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

コンソール エージェントを作成した後、ネットワーク要件を実装します。

ステップ**2: VM**の要件を確認する

コンソール エージェントを作成するときは、次の要件を満たす仮想マシンの種類を選択します。

CPU

8コアまたは8vCPU

RAM

32 GB

Azure VM サイズ

上記の CPU および RAM の要件を満たすインスタンス タイプ。 Standard_D8s_v3 をお勧めします。

ステップ**3:** 権限を設定する

権限は次の方法で付与できます。

- オプション 1: システム割り当てマネージド ID を使用して、Azure VM にカスタム ロールを割り当てます。
- オプション 2: 必要な権限を持つ Azure サービス プリンシパルの資格情報をコンソールに提供します。

コンソールの権限を設定するには、次の手順に従います。

カスタムロール

Azure ポータル、Azure PowerShell、Azure CLI、または REST API を使用して、Azure カスタム ロールを作成できます。次の手順は、Azure CLI を使用してロールを作成する方法を示しています。別の方法をご希望の場合は、 "Azureドキュメント"

手順

1. 独自のホストにソフトウェアを手動でインストールする予定の場合は、カスタム ロールを通じて必要な Azure アクセス許可を提供できるように、VM でシステム割り当てマネージド ID を有効にします。

   "Microsoft Azure ドキュメント: Azure ポータルを使用して VM 上の Azure リソースのマネージド ID を構成する"

2. の内容をコピーします"コネクタのカスタムロール権限"JSON ファイルに保存します。
3. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、JSON ファイルを変更します。

   NetApp Consoleで使用する各 Azure サブスクリプションの ID を追加する必要があります。

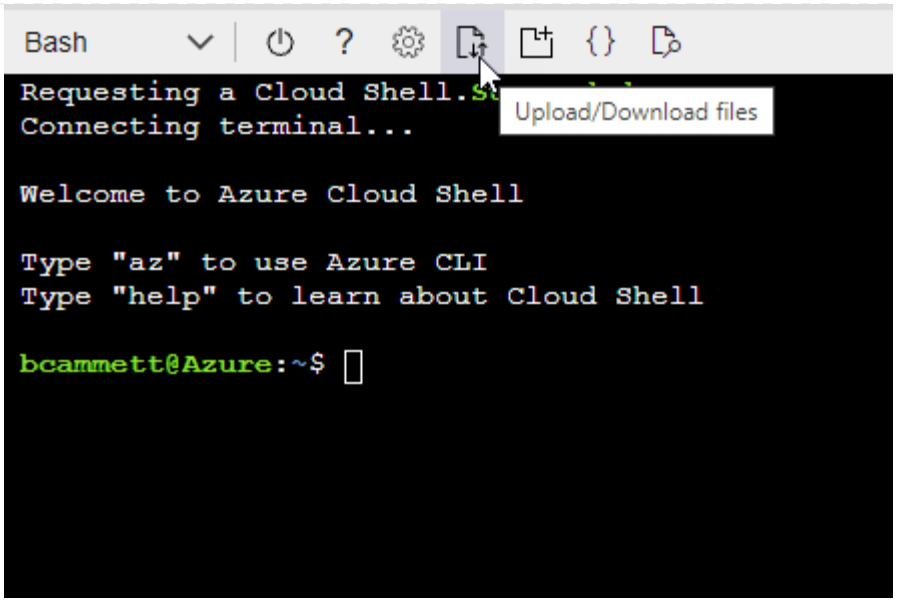
   例

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

4. JSON ファイルを使用して、Azure でカスタム ロールを作成します。

   次の手順では、Azure Cloud Shell で Bash を使用してロールを作成する方法について説明します。

   a. 始める "Azure クラウド シェル"Bash 環境を選択します。
   b. JSON ファイルをアップロードします。



c. Azure CLI を使用してカスタム ロールを作成します。

```
az role definition create --role-definition Connector_Policy.json
```

サービスプリンシパル

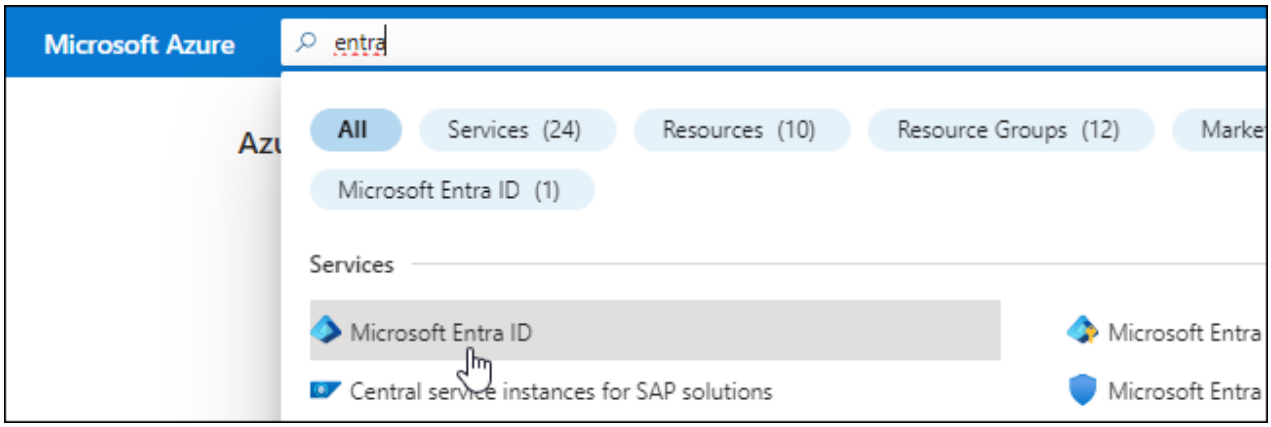
Microsoft Entra ID でサービス プリンシパルを作成して設定し、コンソールに必要な Azure 資格情報を取得します。

ロールベースのアクセス制御用の **Microsoft Entra** アプリケーションを作成する

1. Azure で Active Directory アプリケーションを作成し、そのアプリケーションをロールに割り当てるためのアクセス許可があることを確認します。

   詳細については、 "Microsoft Azure ドキュメント: 必要な権限"

2. Azure ポータルから、**Microsoft Entra ID** サービスを開きます。



3. メニューで*アプリ登録*を選択します。
4. *新規登録*を選択します。

5. アプリケーションの詳細を指定します。
   - 名前: アプリケーションの名前を入力します。
   - アカウント タイプ: アカウント タイプを選択します (いずれのタイプもNetApp Consoleで使用できます)。
   - リダイレクト **URI**: このフィールドは空白のままにすることができます。
6. *登録*を選択します。

   AD アプリケーションとサービス プリンシパルを作成しました。

アプリケーションをロールに割り当てる

1. カスタム ロールを作成します。

   Azure ポータル、Azure PowerShell、Azure CLI、または REST API を使用して、Azure カスタム ロールを作成できます。次の手順は、Azure CLI を使用してロールを作成する方法を示しています。別の方法をご希望の場合は、 "Azureドキュメント"

   a. の内容をコピーします"コンソールエージェントのカスタムロール権限"JSON ファイルに保存します。
   b. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、JSON ファイルを変更します。

      ユーザーがCloud Volumes ONTAPシステムを作成する各 Azure サブスクリプションの ID を追加する必要があります。

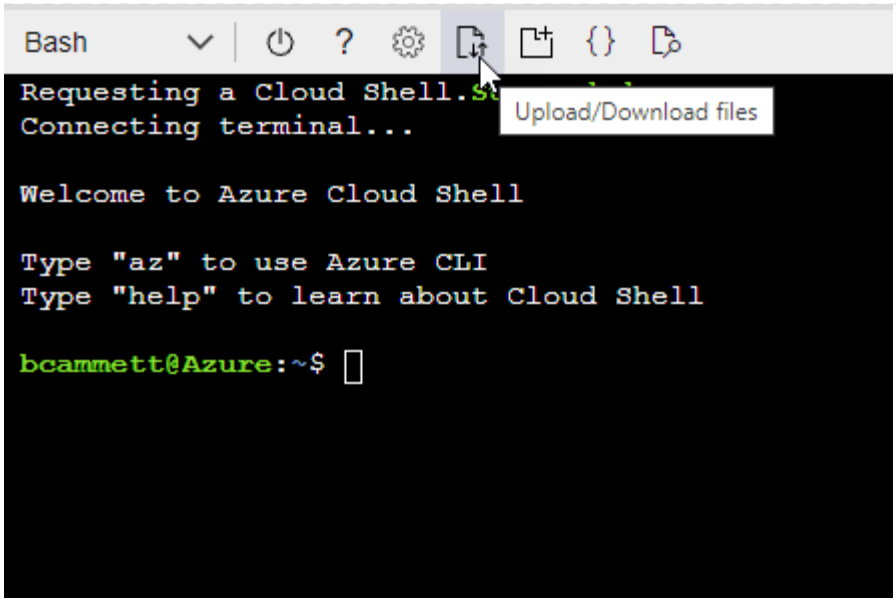
      例

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

   c. JSON ファイルを使用して、Azure でカスタム ロールを作成します。

      次の手順では、Azure Cloud Shell で Bash を使用してロールを作成する方法について説明します。

      - 始める "Azure クラウド シェル"Bash 環境を選択します。
      - JSON ファイルをアップロードします。



- Azure CLI を使用してカスタム ロールを作成します。

```
az role definition create --role-definition
Connector_Policy.json
```

これで、コンソール エージェント仮想マシンに割り当てることができる、コンソール オペレーターと呼ばれるカスタム ロールが作成されます。

2. アプリケーションをロールに割り当てます。

a. Azure ポータルから、サブスクリプション サービスを開きます。

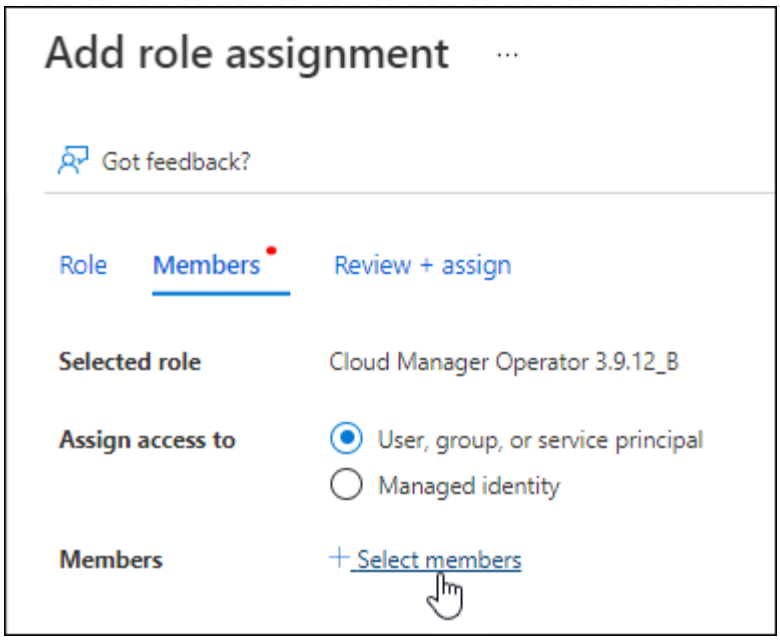
b. サブスクリプションを選択します。

c. アクセス制御 **(IAM) >** 追加 **>** ロール割り当ての追加 を選択します。

d. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。

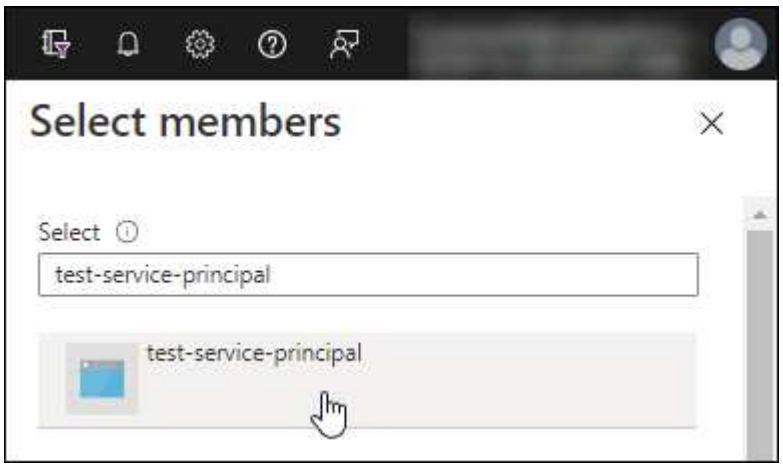
e. *メンバー*タブで、次の手順を実行します。

- *ユーザー、グループ、またはサービス プリンシパル*を選択したままにします。
- *メンバーを選択*を選択します。



- アプリケーションの名前を検索します。

  次に例を示します。



- アプリケーションを選択し、[選択] を選択します。
- *次へ*を選択します。

f. *レビュー + 割り当て*を選択します。

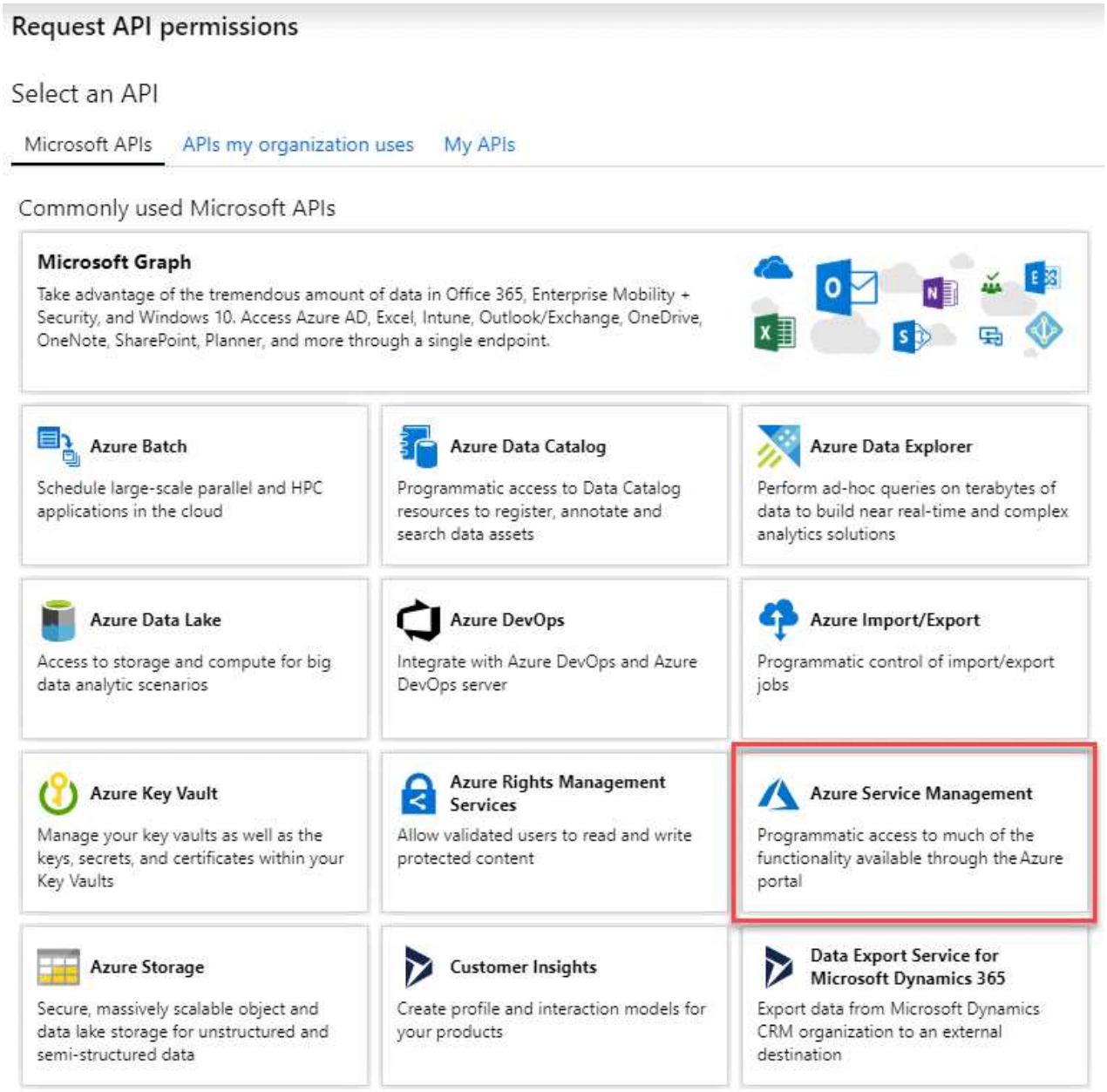
これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

複数の Azure サブスクリプションからCloud Volumes ONTAPをデプロイする場合は、サービス プリンシパルを各サブスクリプションにバインドする必要があります。 NetApp Consoleでは、 Cloud Volumes ONTAP をデプロイするときに使用するサブスクリプションを選択できます。

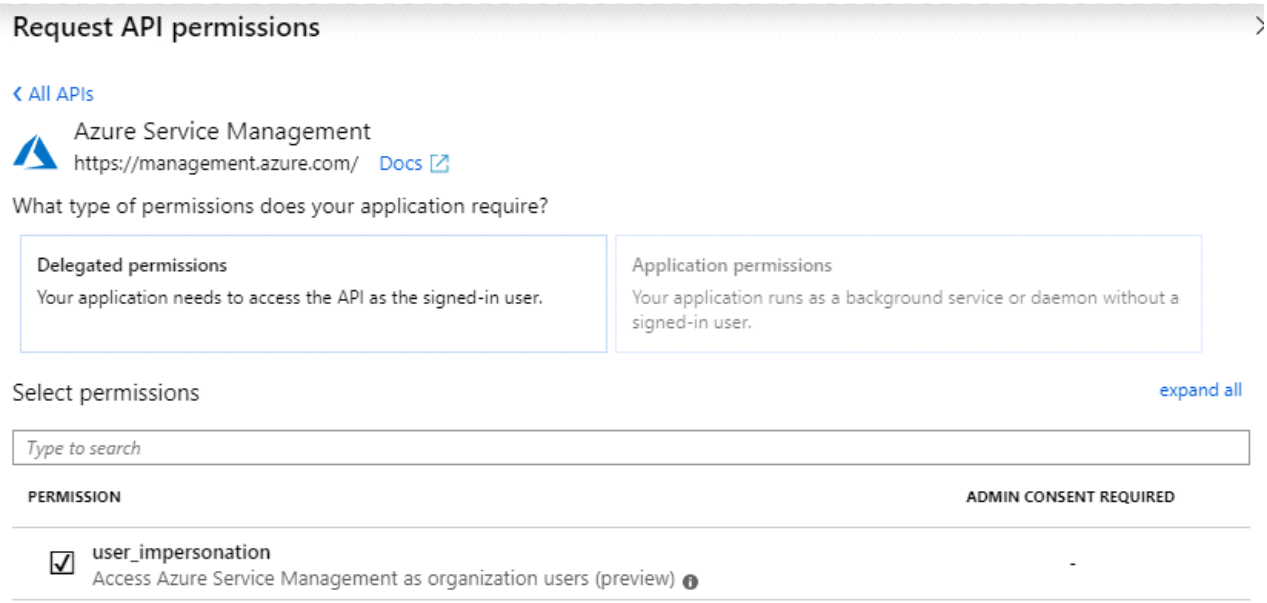
Windows Azure サービス管理 **API** 権限を追加する

1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. **API** 権限 **>** 権限の追加 を選択します。

3. **Microsoft API** の下で、**Azure Service Management** を選択します。

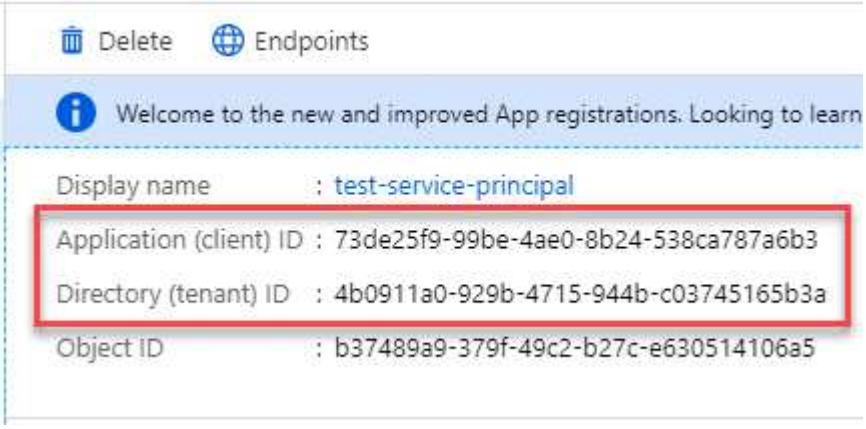


4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。



アプリケーションのアプリケーション**ID**とディレクトリ**ID**を取得します

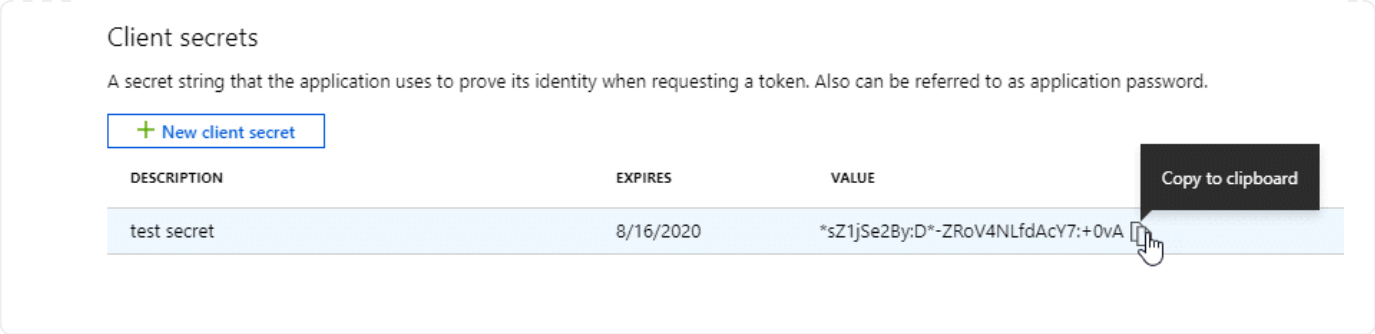
1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. アプリケーション **(**クライアント**) ID** と ディレクトリ **(**テナント**) ID** をコピーします。



Azure アカウントをコンソールに追加するときは、アプリケーションのアプリケーション (クライアント) ID とディレクトリ (テナント) ID を指定する必要があります。コンソールは ID を使用してプログラムでサインインします。

クライアントシークレットを作成する

1. **Microsoft Entra ID** サービスを開きます。
2. *アプリ登録*を選択し、アプリケーションを選択します。
3. *証明書とシークレット > 新しいクライアント シークレット*を選択します。
4. シークレットの説明と期間を指定します。
5. *追加*を選択します。
6. クライアント シークレットの値をコピーします。



ステップ**4:** コンソールエージェントを作成する

Azure Marketplace からコンソール エージェントを直接起動します。

タスク概要

Azure Marketplace からコンソール エージェントを作成すると、既定の構成で仮想マシンが設定されます。"コンソールエージェントのデフォルト構成について学習します" 。

開始する前に

次のものが必要です:

- Azure サブスクリプション。
- 選択した Azure リージョン内の VNet とサブネット。
- 組織ですべての送信インターネット トラフィックにプロキシが必要な場合のプロキシ サーバーの詳細:
  - IPアドレス
  - Credentials
  - HTTPS証明書
- コンソール エージェント仮想マシンにその認証方法を使用する場合は、SSH 公開キー。認証方法のもう 1 つのオプションは、パスワードを使用することです。

  "Azure の Linux VM への接続について学習します"

- コンソールエージェント用のAzureロールをコンソールが自動的に作成しないようにするには、独自のロールを作成する必要があります。"このページのポリシーを使用する" 。

  これらの権限は、コンソール エージェント インスタンス自体に適用されます。これは、コンソール エージェント VM を展開するために以前に設定した権限セットとは異なります。

手順

1. Azure Marketplace のNetApp Consoleエージェント VM ページに移動します。

   "商用リージョン向けの Azure Marketplace ページ"

2. *今すぐ入手*を選択し、*続行*を選択します。
3. Azure ポータルから [作成] を選択し、手順に従って仮想マシンを構成します。

   VM を構成する際には、次の点に注意してください。

- **VM** サイズ: CPU と RAM の要件を満たす VM サイズを選択します。 Standard_D8s_v3 をお勧めします。
- ディスク: コンソール エージェントは、HDD ディスクまたは SSD ディスクのいずれでも最適に動作します。
- ネットワーク セキュリティ グループ: コンソール エージェントには、SSH、HTTP、および HTTPS を使用した受信接続が必要です。

  "Azure のセキュリティ グループ ルールを表示する" 。

- ID*: 管理 の下で、システム割り当てマネージド **ID** を有効にする を選択します。

  この設定は重要です。マネージド ID を使用すると、コンソール エージェント仮想マシンは資格情報を提供せずに Microsoft Entra ID に対して自身を識別できるためです。 "Azure リソースのマネージド ID の詳細" 。

4. 確認 **+** 作成 ページで選択内容を確認し、作成 を選択してデプロイを開始します。

   Azure は指定された設定で仮想マシンをデプロイします。約 10 分以内に仮想マシンとコンソール エージェント ソフトウェアが実行されるはずです。

   インストールが失敗した場合は、トラブルシューティングに役立つログとレポートを表示できます。"インストールの問題をトラブルシューティングする方法を学びます。"

5. コンソール エージェント仮想マシンに接続しているホストから Web ブラウザを開き、次の URL を入力します。

   https://ipaddress

6. ログイン後、コンソール エージェントを設定します。
   a. コンソール エージェントに関連付けるコンソール組織を指定します。
   b. システムの名前を入力します。
   c. 安全な環境で実行していますか**?** の下で、制限モードを無効のままにします。

      コンソールを標準モードで使用するには、制限モードを無効にしておきます。安全な環境があり、このアカウントをコンソールのバックエンド サービスから切断する場合にのみ、制限モードを有効にする必要があります。もしそうなら、"制限モードでコンソールを開始するには、以下の手順に従ってください。" 。

   d. *始めましょう*を選択します。

結果

これで、コンソール エージェントがインストールされ、コンソール組織で設定されました。

コンソール エージェントを作成したのと同じ Azure サブスクリプションに Azure Blob ストレージがある場合は、システム ページに Azure Blob ストレージ システムが自動的に表示されます。 "コンソールから Azure Blob ストレージを管理する方法を学びます"

ステップ**5:** コンソールエージェントに権限を付与する

コンソール エージェントを作成したので、以前に設定した権限をエージェントに付与する必要があります。権限を付与すると、コンソール エージェントは Azure 内のデータとストレージ インフラストラクチャを管理できるようになります。

カスタムロール

Azure ポータルに移動し、1 つ以上のサブスクリプションのコンソール エージェント仮想マシンに Azure カスタム ロールを割り当てます。

手順

1. Azure ポータルから サブスクリプション サービスを開き、サブスクリプションを選択します。

   サブスクリプション サービスからロールを割り当てることが重要です。これは、サブスクリプション レベルでのロール割り当ての範囲を指定するためです。 *scope* は、アクセスが適用されるリソースのセットを定義します。別のレベル (たとえば、仮想マシン レベル) でスコープを指定すると、NetApp Console内からアクションを完了する機能に影響します。

   "Microsoft Azure ドキュメント: Azure RBAC のスコープを理解する"

2. アクセス制御 **(IAM)** > 追加 > ロール割り当ての追加 を選択します。
3. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。

   コンソール オペレーターは、ポリシーで提供されるデフォルト名です。ロールに別の名前を選択した場合は、代わりにその名前を選択します。

4. *メンバー*タブで、次の手順を実行します。
   a. マネージド **ID** へのアクセスを割り当てます。
   b. *メンバーの選択*を選択し、コンソール エージェント仮想マシンが作成されたサブスクリプションを選択し、*マネージド ID*の下で*仮想マシン*を選択して、コンソール エージェント仮想マシンを選択します。
   c. *選択*を選択します。
   d. *次へ*を選択します。
   e. *レビュー + 割り当て*を選択します。
   f. 追加の Azure サブスクリプションのリソースを管理する場合は、そのサブスクリプションに切り替えて、これらの手順を繰り返します。

次の手順

に行く "NetApp Console"コンソール エージェントの使用を開始します。

サービスプリンシパル

手順

1. *管理 > 資格情報*を選択します。
2. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: **Microsoft Azure >** エージェント を選択します。
   b. 資格情報の定義: 必要な権限を付与する Microsoft Entra サービス プリンシパルに関する情報を入力します。
      - アプリケーション（クライアント）ID
      - ディレクトリ（テナント）ID

- クライアントシークレット

c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。

d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

結果

これで、コンソールに、ユーザーに代わって Azure でアクションを実行するために必要なアクセス許可が付与されました。

Azure にコンソール エージェントを手動でインストールする

独自の Linux ホストにコンソール エージェントを手動でインストールするには、ホストの要件を確認し、ネットワークを設定し、Azure のアクセス許可を準備し、コンソール エージェントをインストールして、準備したアクセス許可を付与する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ホストの要件を確認する

コンソール エージェント ソフトウェアは、特定のオペレーティング システム要件、RAM 要件、ポート要件などを満たすホスト上で実行する必要があります。

コンソール エージェントは、19000 ～ 19200 の UID と GID の範囲を予約します。この範囲は固定されており、変更することはできません。ホスト上のサードパーティ ソフトウェアがこの範囲内の UID または GID を使用している場合、エージェントのインストールは失敗します。NetApp、競合を回避するためにサードパーティ ソフトウェアがインストールされていないホストの使用を推奨しています。

専用ホスト

コンソール エージェントは、他のアプリケーションと共有されているホストではサポートされません。ホストは専用ホストである必要があります。ホストは、次のサイズ要件を満たす任意のアーキテクチャにすることができます。

- CPU: 8コアまたは8vCPU
- メモリ: 32 GB
- ディスク容量: ホストには 165 GB が推奨され、パーティション要件は次のとおりです。
  - `/opt`: 120 GiBの空き容量が必要です

    エージェントは `/opt`インストールするには `/opt/application/netapp`ディレクトリとその内容。

  - `/var`: 40 GiBの空き容量が必要です

    コンソールエージェントにはこのスペースが必要です `/var`Docker または Podman は、このディレクトリ内にコンテナを作成するように設計されているためです。具体的には、

`/var/lib/containers/storage`ディレクトリ。このスペースでは外部マウントまたはシンボリックリンクは機能しません。

ハイパーバイザー

サポートされているオペレーティング システムを実行することが認定されているベア メタルまたはホスト型ハイパーバイザーが必要です。

オペレーティングシステムとコンテナの要件

コンソールを標準モードまたは制限モードで使用する場合、コンソール エージェントは次のオペレーティング システムでサポートされます。エージェントをインストールする前に、コンテナ オーケストレーション ツールが必要です。

オペレーティング システム	サポートされる**OS** バージョン	サポートされているエージェントのバージョン	必要なコンテナツール	**SELinux** は
Red Hat Enterprise Linux	9.1～9.4 8.6～8.10 • 英語版のみ。 • ホストは Red Hat Subscription Management に登録されている必要があります。登録されていない場合、ホストはエージェントのインストール中に必要なサードパーティ製ソフトウェアを更新するためにリポジトリにアクセスできません。	3.9.50 以降、コンソールが標準モードまたは制限モード	Podman バージョン 4.6.1 または 4.9.4 Podman の構成要件を表示する 。	強制モードまたは許可モードでサポートされます • Cloud Volumes ONTAPシステムの管理は、オペレーティングシステムで SELinux が有効になっているエージェントではサポートされません。
Ubuntu	24.04 LTS	3.9.45 以降、NetApp Consoleが標準モードまたは制限モード	Docker エンジン 23.06 から 28.0.0。	サポート対象外

Azure VM サイズ

上記の CPU および RAM の要件を満たすインスタンス タイプ。 Standard_D8s_v3 をお勧めします。

/optのディスク容量

100 GiBの空き容量が必要です

エージェントは `/opt`インストールするには `/opt/application/netapp`ディレクトリとその内容。

/varのディスク容量

20 GiBの空き容量が必要です

コンソールエージェントにはこのスペースが必要です `/var`Docker または Podman は、このディレクトリ内にコンテナを作成するように設計されているためです。具体的には、 `/var/lib/containers/storage`ディレクトリ。このスペースでは外部マウントまたはシンボリックリンクは機能しません。

ステップ**2: Podman**または**Docker Engine**をインストールする

オペレーティング システムに応じて、エージェントをインストールする前に Podman または Docker Engine のいずれかが必要になります。

- Red Hat Enterprise Linux 8 および 9 には Podman が必要です。

  サポートされているPodmanのバージョンを表示する 。

- Ubuntu には Docker Engine が必要です。

  サポートされている Docker エンジンのバージョンを表示する 。

例 **2.** 手順

ポッドマン

Podman をインストールして設定するには、次の手順に従います。

- podman.socket サービスを有効にして起動します
- Python3をインストールする
- podman-compose パッケージ バージョン 1.0.6 をインストールします。
- podman-composeをPATH環境変数に追加する
- Red Hat Enterprise Linux を使用している場合は、Podman バージョンが CNI ではなく Netavark Aardvark DNS を使用していることを確認してください。

DNS ポートの競合を避けるために、エージェントをインストールした後、aardvark-dns ポート (デフォルト: 53) を調整します。指示に従ってポートを構成します。

手順

1. ホストに podman-docker パッケージがインストールされている場合は削除します。

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Podman をインストールします。

   Podman は、公式の Red Hat Enterprise Linux リポジトリから入手できます。

   Red Hat Enterprise Linux 9 の場合:

```
sudo dnf install podman-2:<version>
```

   <version> は、インストールする Podman のサポートされているバージョンです。サポートされているPodmanのバージョンを表示する 。

   Red Hat Enterprise Linux 8 の場合:

```
sudo dnf install podman-3:<version>
```

   <version> は、インストールする Podman のサポートされているバージョンです。サポートされているPodmanのバージョンを表示する 。

3. podman.socket サービスを有効にして起動します。

```
sudo systemctl enable --now podman.socket
```

4. python3 をインストールします。

```
sudo dnf install python3
```

5. システムにまだインストールされていない場合は、EPEL リポジトリ パッケージをインストールします。
6. Red Hat Enterprise を使用している場合:

   podman-compose は、Extra Packages for Enterprise Linux (EPEL) リポジトリから入手できるため、この手順は必須です。

   Red Hat Enterprise Linux 9 の場合:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   Red Hat Enterprise Linux 8 の場合:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

7. podman-compose パッケージ 1.0.6 をインストールします。

```
sudo dnf install podman-compose-1.0.6
```

   使用して `dnf install`コマンドは、PATH 環境変数に podman-compose を追加するための要件を満たしています。インストールコマンドは、すでにインストールされているpodman-composeを/usr/binに追加します。 `secure_path`ホスト上のオプション。

8. Red Hat Enterprise Linux 8 を使用している場合は、Podman バージョンが CNI ではなく Aardvark DNS を備えた NetAvark を使用していることを確認します。

   a. 次のコマンドを実行して、networkBackend が CNI に設定されているかどうかを確認します。

```
podman info | grep networkBackend
```

   b. networkBackendが `CNI`、それを変更する必要があります `netavark`。

   c. インストール `netavark`そして `aardvark-dns`次のコマンドを使用します。

```
dnf install aardvark-dns netavark
```

d. 開く `/etc/containers/containers.conf`ファイルを編集し、network_backend オプションを変更して、「cni」の代わりに「netavark」を使用します。

もし `/etc/containers/containers.conf`存在しない場合は、設定を変更してください `/usr/share/containers/containers.conf`。

9. podman を再起動します。

```
systemctl restart podman
```

10. 次のコマンドを使用して、networkBackend が「netavark」に変更されていることを確認します。

```
podman info | grep networkBackend
```

Dockerエンジン

Docker のドキュメントに従って Docker Engine をインストールします。

手順

1. "Dockerからのインストール手順を見る"

   サポートされている Docker エンジン バージョンをインストールするには、手順に従ってください。最新バージョンはコンソールでサポートされていないため、インストールしないでください。

2. Docker が有効になっていて実行されていることを確認します。

```
sudo systemctl enable docker && sudo systemctl start docker
```

ステップ**3:** ネットワークを設定する

コンソール エージェントをインストールする予定のネットワークの場所が次の要件をサポートしていることを確認します。これらの要件を満たすことで、コンソール エージェントはハイブリッド クラウド環境内のリソースとプロセスを管理できるようになります。

Azureリージョン

Cloud Volumes ONTAPを使用する場合、コンソールエージェントは、管理するCloud Volumes ONTAPシステムと同じAzureリージョン、または "Azure リージョン ペア"Cloud Volumes ONTAPシステム用。この要件により、 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"

ターゲットネットワークへの接続

コンソール エージェントには、システムを作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムまたはストレージ システムを作成する予定のネットワークなどです。

アウトバウンドインターネットアクセス

コンソール エージェントを展開するネットワークの場所には、特定のエンドポイントに接続するための送信インターネット接続が必要です。

Webベースの**NetApp Console**を使用する際にコンピュータから接続されるエンドポイント

Web ブラウザからコンソールにアクセスするコンピュータは、複数のエンドポイントに接続できる必要があります。コンソール エージェントを設定し、コンソールを日常的に使用するには、コンソールを使用する必要があります。

"NetAppコンソールのネットワークを準備する" 。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

エンドポイント	目的
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure パブリック リージョン内のリソースを管理します。
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure China リージョンのリソースを管理します。
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェア アップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォール ルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用している場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インター

ネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

ステップ**4:** コンソールエージェントの展開権限を設定する

次のいずれかのオプションを使用して、コンソール エージェントに Azure 権限を付与する必要があります。

- オプション 1: システム割り当てマネージド ID を使用して、Azure VM にカスタム ロールを割り当てます。
- オプション 2: 必要なアクセス許可を持つ Azure サービス プリンシパルの資格情報をコンソール エージェントに提供します。

手順に従って、コンソール エージェントの権限を準備します。

コンソールエージェントの展開用のカスタムロールを作成する

Azure ポータル、Azure PowerShell、Azure CLI、または REST API を使用して、Azure カスタム ロールを作成できます。次の手順は、Azure CLI を使用してロールを作成する方法を示しています。別の方法をご希望の場合は、 "Azureドキュメント"

手順

1. 独自のホストにソフトウェアを手動でインストールする予定の場合は、カスタム ロールを通じて必要な Azure アクセス許可を提供できるように、VM でシステム割り当てマネージド ID を有効にします。

   "Microsoft Azure ドキュメント: Azure ポータルを使用して VM 上の Azure リソースのマネージド ID を構成する"

2. の内容をコピーします"コネクタのカスタムロール権限"JSON ファイルに保存します。
3. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、JSON ファイルを変更します。

   NetApp Consoleで使用する各 Azure サブスクリプションの ID を追加する必要があります。

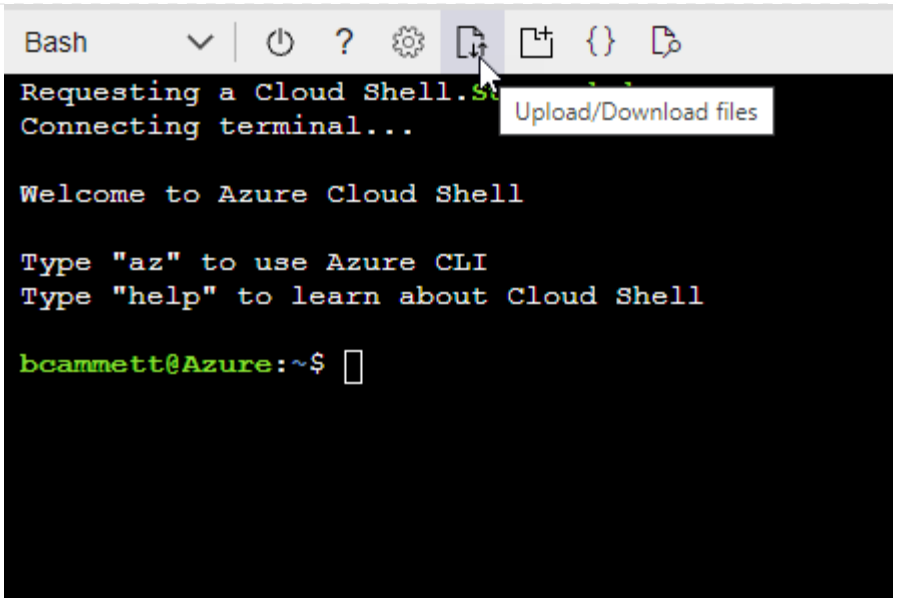
   例

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

4. JSON ファイルを使用して、Azure でカスタム ロールを作成します。

   次の手順では、Azure Cloud Shell で Bash を使用してロールを作成する方法について説明します。

   a. 始める "Azure クラウド シェル"Bash 環境を選択します。
   b. JSON ファイルをアップロードします。



c. Azure CLI を使用してカスタム ロールを作成します。

```
az role definition create --role-definition Connector_Policy.json
```

サービスプリンシパル

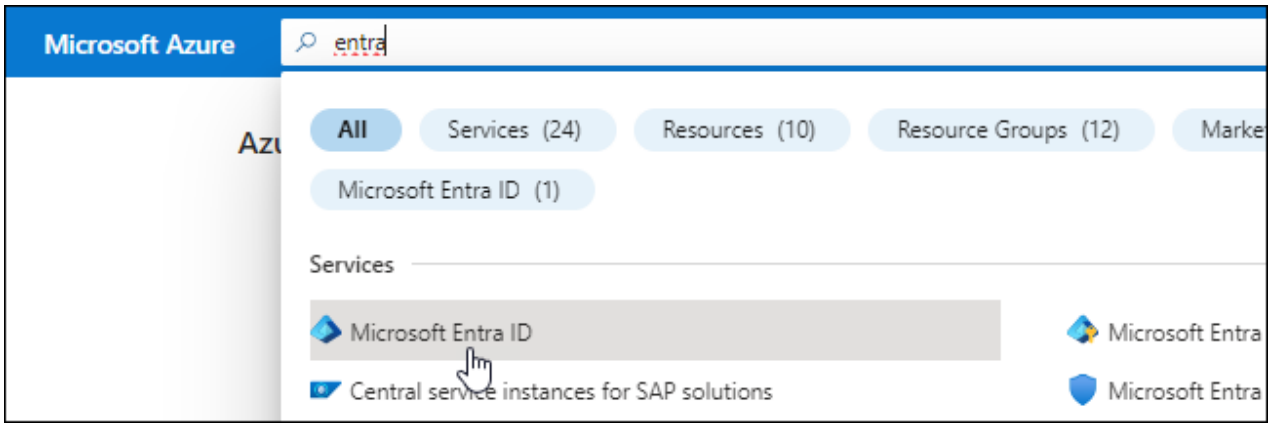
Microsoft Entra ID でサービス プリンシパルを作成して設定し、コンソール エージェントに必要な Azure 資格情報を取得します。

ロールベースのアクセス制御用の **Microsoft Entra** アプリケーションを作成する

1. Azure で Active Directory アプリケーションを作成し、そのアプリケーションをロールに割り当てるためのアクセス許可があることを確認します。

   詳細については、 "Microsoft Azure ドキュメント: 必要な権限"

2. Azure ポータルから、**Microsoft Entra ID** サービスを開きます。



3. メニューで*アプリ登録*を選択します。
4. *新規登録*を選択します。

5. アプリケーションの詳細を指定します。
   - 名前: アプリケーションの名前を入力します。
   - アカウント タイプ: アカウント タイプを選択します (いずれのタイプもNetApp Consoleで使用できます)。
   - リダイレクト **URI**: このフィールドは空白のままにすることができます。
6. *登録*を選択します。

   AD アプリケーションとサービス プリンシパルを作成しました。

アプリケーションをロールに割り当てる

1. カスタム ロールを作成します。

   Azure ポータル、Azure PowerShell、Azure CLI、または REST API を使用して、Azure カスタム ロールを作成できます。次の手順は、Azure CLI を使用してロールを作成する方法を示しています。別の方法をご希望の場合は、 "Azureドキュメント"

   a. の内容をコピーします"コンソールエージェントのカスタムロール権限"JSON ファイルに保存します。
   b. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、JSON ファイルを変更します。

      ユーザーがCloud Volumes ONTAPシステムを作成する各 Azure サブスクリプションの ID を追加する必要があります。

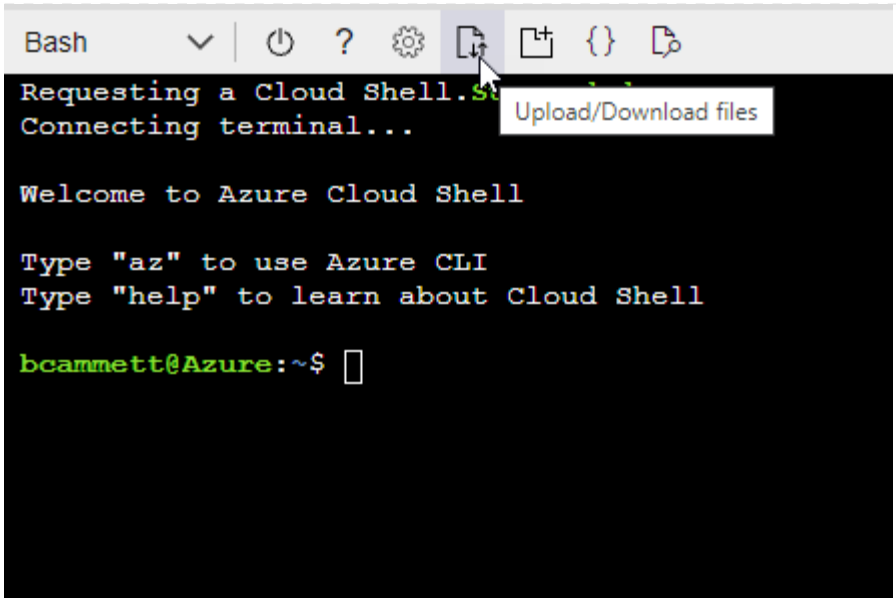
      例

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

   c. JSON ファイルを使用して、Azure でカスタム ロールを作成します。

      次の手順では、Azure Cloud Shell で Bash を使用してロールを作成する方法について説明します。

      - 始める "Azure クラウド シェル"Bash 環境を選択します。
      - JSON ファイルをアップロードします。



- Azure CLI を使用してカスタム ロールを作成します。

```
az role definition create --role-definition
Connector_Policy.json
```

これで、コンソール エージェント仮想マシンに割り当てることができる、コンソール オペレーターと呼ばれるカスタム ロールが作成されます。

2. アプリケーションをロールに割り当てます。

a. Azure ポータルから、サブスクリプション サービスを開きます。

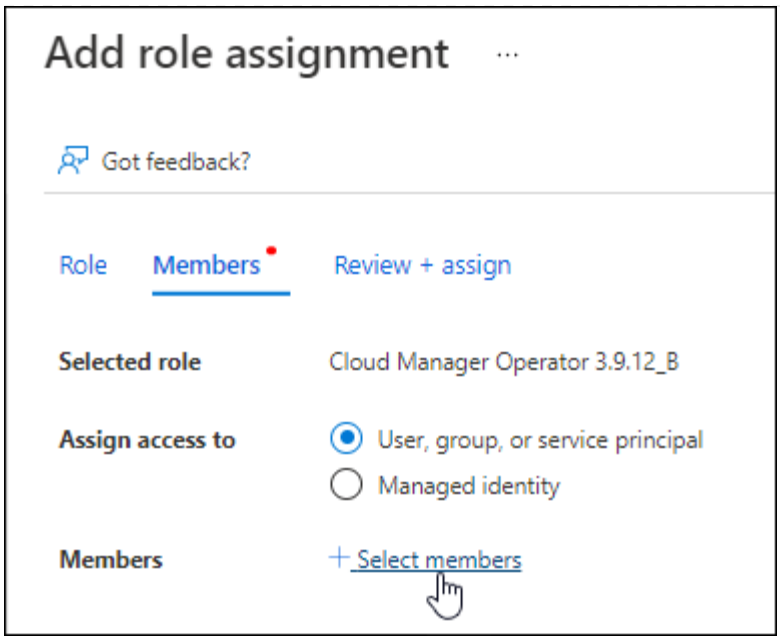
b. サブスクリプションを選択します。

c. アクセス制御 **(IAM) >** 追加 **>** ロール割り当ての追加 を選択します。

d. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。

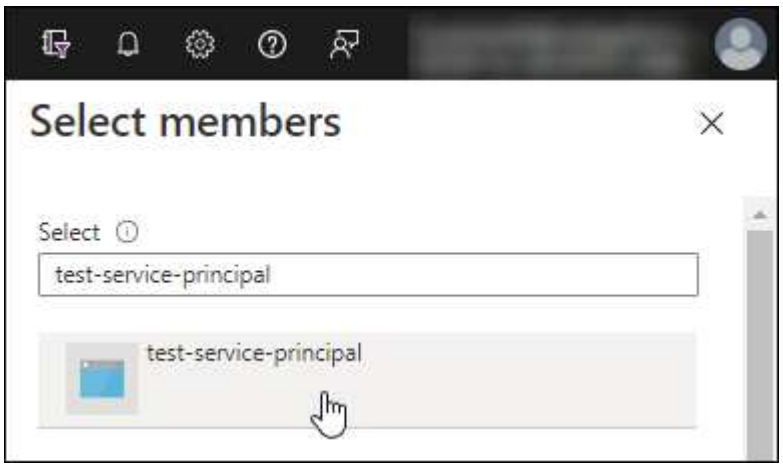
e. *メンバー*タブで、次の手順を実行します。

- *ユーザー、グループ、またはサービス プリンシパル*を選択したままにします。
- *メンバーを選択*を選択します。



- アプリケーションの名前を検索します。

  次に例を示します。



- アプリケーションを選択し、[選択] を選択します。
- *次へ*を選択します。

f. *レビュー + 割り当て*を選択します。

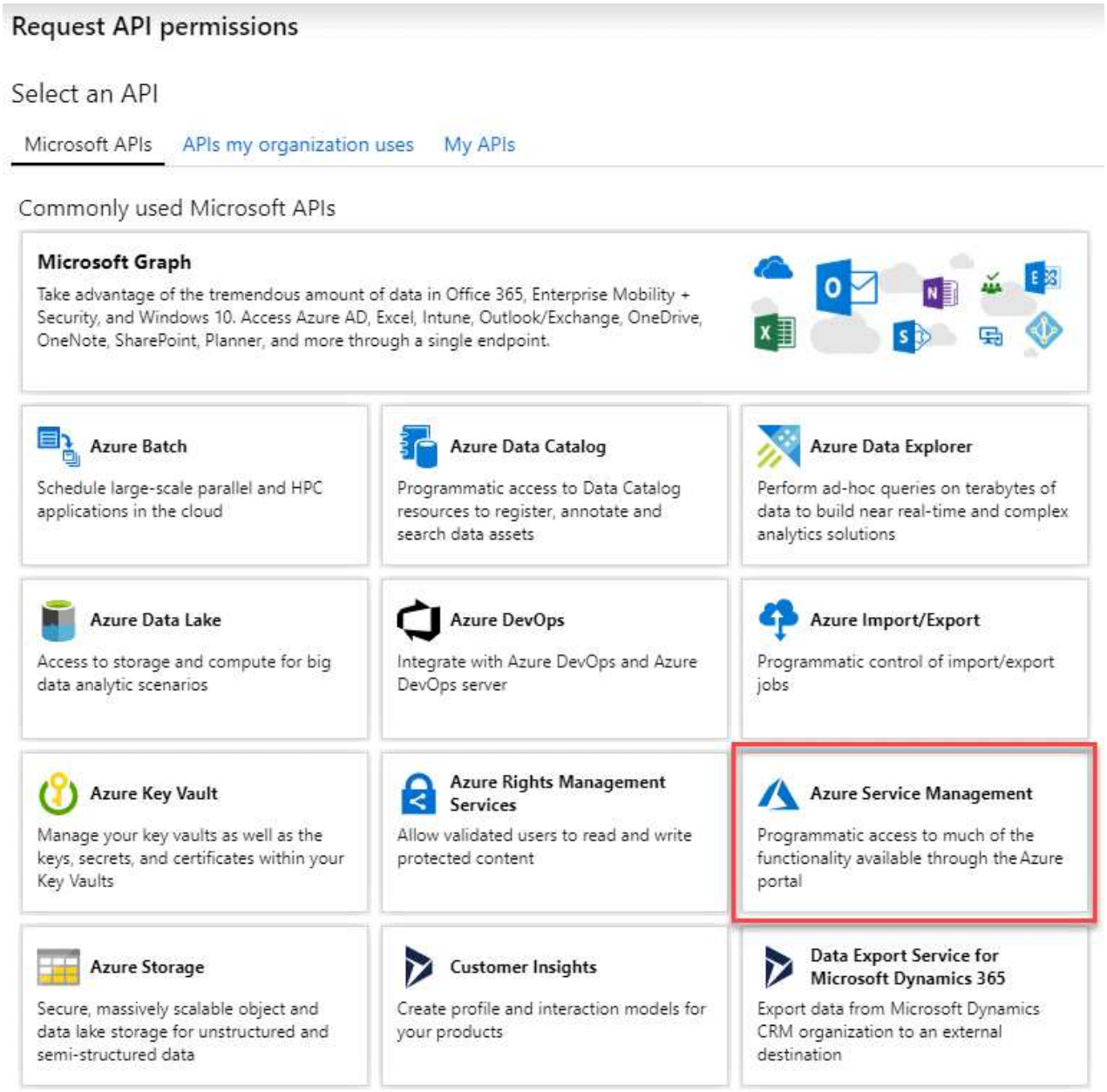
これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

複数の Azure サブスクリプションからCloud Volumes ONTAPをデプロイする場合は、サービス プリンシパルを各サブスクリプションにバインドする必要があります。 NetApp Consoleでは、 Cloud Volumes ONTAP をデプロイするときに使用するサブスクリプションを選択できます。

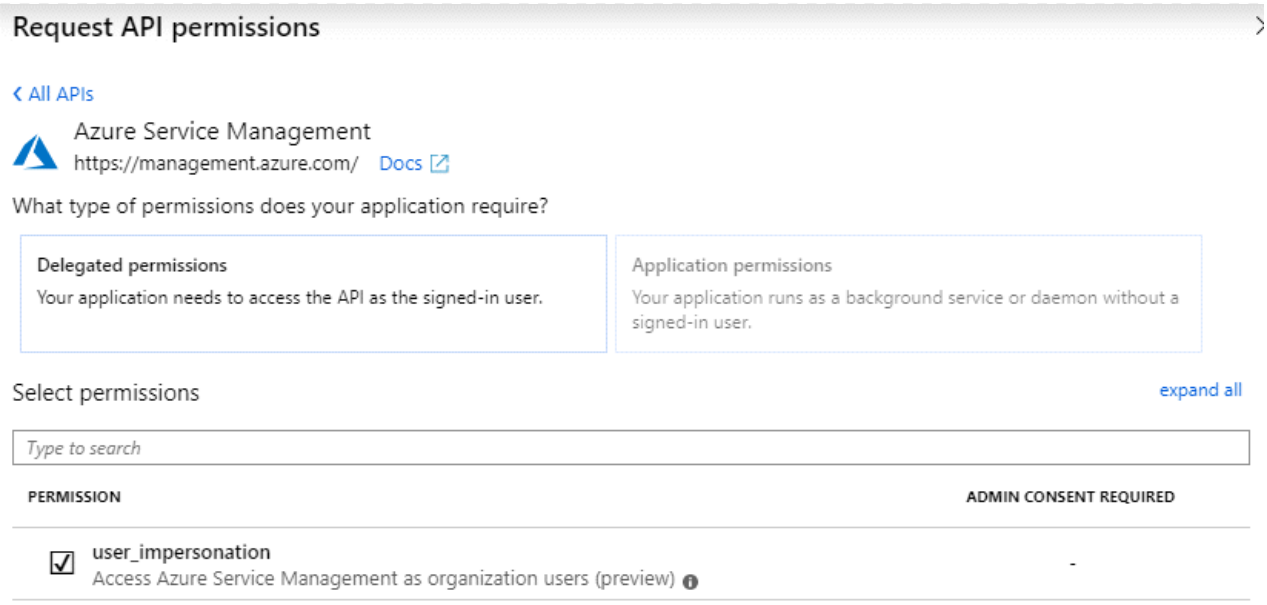
Windows Azure サービス管理 **API** 権限を追加する

1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. **API** 権限 **>** 権限の追加 を選択します。

3. **Microsoft API** の下で、**Azure Service Management** を選択します。

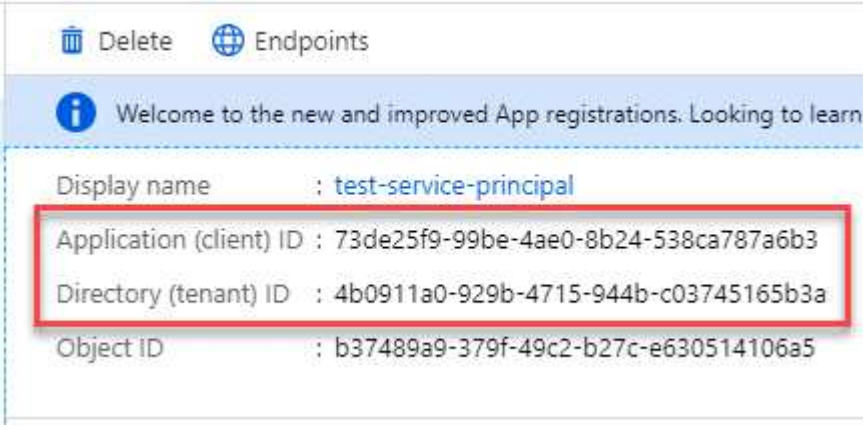


4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。



アプリケーションのアプリケーション**ID**とディレクトリ**ID**を取得します

1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. アプリケーション **(**クライアント**) ID** と ディレクトリ **(**テナント**) ID** をコピーします。



Azure アカウントをコンソールに追加するときは、アプリケーションのアプリケーション (クライアント) ID とディレクトリ (テナント) ID を指定する必要があります。コンソールは ID を使用してプログラムでサインインします。

クライアントシークレットを作成する

1. **Microsoft Entra ID** サービスを開きます。
2. *アプリ登録*を選択し、アプリケーションを選択します。
3. *証明書とシークレット > 新しいクライアント シークレット*を選択します。
4. シークレットの説明と期間を指定します。
5. *追加*を選択します。
6. クライアント シークレットの値をコピーします。

結果

これでサービス プリンシパルが設定され、アプリケーション (クライアント) ID、ディレクトリ (テナント) ID、およびクライアント シークレットの値がコピーされているはずです。 Azure アカウントを追加するときに、コンソールにこの情報を入力する必要があります。

ステップ**5:** コンソールエージェントをインストールする

前提条件が完了したら、独自の Linux ホストにソフトウェアを手動でインストールできます。

開始する前に

次のものが必要です:

- コンソール エージェントをインストールするためのルート権限。
- コンソール エージェントからのインターネット アクセスにプロキシが必要な場合のプロキシ サーバーの詳細。

  インストール後にプロキシ サーバーを構成するオプションがありますが、これを行うにはコンソール エージェントを再起動する必要があります。

- プロキシ サーバーが HTTPS を使用する場合、またはプロキシがインターセプト プロキシである場合は、CA 署名証明書。

> コンソール エージェントを手動でインストールする場合、透過プロキシ サーバーの証明書を設定することはできません。透過プロキシ サーバーの証明書を設定する必要がある場合は、インストール後にメンテナンス コンソールを使用する必要があります。詳細はこちら"エージェントメンテナンスコンソール"。

- カスタム ロールを通じて必要な Azure アクセス許可を提供できるように、Azure の VM で有効になっているマネージド ID。

  "Microsoft Azure ドキュメント: Azure ポータルを使用して VM 上の Azure リソースのマネージド ID を構成する"

タスク概要

NetAppサポート サイトで入手できるインストーラーは、以前のバージョンである可能性があります。インストール後、新しいバージョンが利用可能な場合、コンソール エージェントは自動的に更新されます。

手順

1. ホストに *http_proxy* または *https_proxy* システム変数が設定されている場合は、それらを削除します。

```
unset http_proxy
unset https_proxy
```

これらのシステム変数を削除しないと、インストールは失敗します。

2. コンソールエージェントソフトウェアを以下からダウンロードします。 "NetAppサポート サイト"それを Linux ホストにコピーします。

   ネットワークまたはクラウドで使用するための「オンライン」エージェント インストーラーをダウンロードする必要があります。

3. スクリプトを実行するための権限を割り当てます。

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

<version> は、ダウンロードしたコンソール エージェントのバージョンです。

4. Government Cloud 環境にインストールする場合は、構成チェックを無効にします。"手動インストールの構成チェックを無効にする方法を説明します。"
5. インストール スクリプトを実行します。

```
 ./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

ネットワークでインターネット アクセスにプロキシが必要な場合は、プロキシ情報を追加する必要があります。透過プロキシまたは明示プロキシのいずれかを追加できます。 --proxy および --cacert パラメータはオプションであり、追加するように要求されることはありません。プロキシ サーバーがある場合は、示されているようにパラメータを入力する必要があります。

CA 署名証明書を使用して明示的なプロキシ サーバーを構成する例を次に示します。

```
 ./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

`--proxy`次のいずれかの形式を使用して、コンソール エージェントが HTTP または HTTPS プロキシ サーバーを使用するように構成します。

- http://アドレス:ポート
- http://ユーザー名:パスワード@アドレス:ポート
- http://ドメイン名%92ユーザー名:パスワード@アドレス:ポート
- https://アドレス:ポート
- https://ユーザー名:パスワード@アドレス:ポート

◦ https://ドメイン名%92ユーザー名:パスワード@アドレス:ポート

次の点に注意してください。

- ユーザーはローカル ユーザーまたはドメイン ユーザーになります。
- ドメイン ユーザーの場合は、上記のように \ の ASCII コードを使用する必要があります。
- コンソール エージェントは、@ 文字を含むユーザー名またはパスワードをサポートしていません。
- パスワードに以下の特殊文字が含まれている場合は、その特殊文字の前にバックスラッシュ (& または !) を付けてエスケープする必要があります。

例えば：

http://bxpproxyuser:netapp1\!@アドレス:3128

`--cacert`コンソール エージェントとプロキシ サーバー間の HTTPS アクセスに使用する CA 署名付き証明書を指定します。このパラメータは、HTTPS プロキシ サーバー、インターセプト プロキシ サーバー、および透過プロキシ サーバーに必須です。

+ 透過プロキシ サーバーを構成する例を次に示します。透過プロキシを構成する場合、プロキシ サーバーを定義する必要はありません。コンソール エージェント ホストには、CA 署名付き証明書のみを追加します。

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

1. Podman を使用した場合は、aardvark-dns ポートを調整する必要があります。
   a. コンソール エージェント仮想マシンに SSH で接続します。
   b. podman */usr/share/containers/containers.conf* ファイルを開き、Aardvark DNS サービス用に選択したポートを変更します。たとえば、54 に変更します。

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

   c. コンソール エージェント仮想マシンを再起動します。

2. インストールが完了するまでお待ちください。

   プロキシ サーバーを指定した場合、インストールの最後に、コンソール エージェント サービス (occm) が 2 回再起動します。

   インストールが失敗した場合は、インストール レポートとログを表示して問題の解決に役立てることができます。"インストールの問題をトラブルシューティングする方法を学びます。"

1. コンソール エージェント仮想マシンに接続しているホストから Web ブラウザを開き、次の URL を入力します。

   https://ipaddress

2. ログイン後、コンソール エージェントを設定します。
   a. コンソール エージェントに関連付ける組織を指定します。
   b. システムの名前を入力します。
   c. 安全な環境で実行していますか**?** の下で、制限モードを無効のままにします。

      以下の手順ではコンソールを標準モードで使用する方法について説明しているため、制限モードは無効にしておく必要があります。安全な環境があり、このアカウントをバックエンド サービスから切断する場合にのみ、制限モードを有効にする必要があります。もしそうなら、"NetApp Consoleを制限モードで使い始めるための手順に従います" 。

   d. *始めましょう*を選択します。

コンソール エージェントを作成したのと同じ Azure サブスクリプションに Azure Blob ストレージがある場合は、システム ページに Azure Blob ストレージ システムが自動的に表示されます。 "NetApp ConsoleからAzure Blob ストレージを管理する方法を学びます"

ステップ**6: NetApp Console**に権限を付与する

コンソール エージェントをインストールしたので、以前に設定した Azure アクセス許可をコンソール エージェントに付与する必要があります。権限を付与すると、コンソールで Azure のデータとストレージ インフラストラクチャを管理できるようになります。

カスタムロール

Azure ポータルに移動し、1 つ以上のサブスクリプションのコンソール エージェント仮想マシンに Azure カスタム ロールを割り当てます。

手順

1. Azure ポータルから サブスクリプション サービスを開き、サブスクリプションを選択します。

   サブスクリプション サービスからロールを割り当てることが重要です。これは、サブスクリプション レベルでのロール割り当ての範囲を指定するためです。 *scope* は、アクセスが適用されるリソースのセットを定義します。別のレベル (たとえば、仮想マシン レベル) でスコープを指定すると、NetApp Console内からアクションを完了する機能に影響します。

   "Microsoft Azure ドキュメント: Azure RBAC のスコープを理解する"

2. アクセス制御 **(IAM)** > 追加 > ロール割り当ての追加 を選択します。
3. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。

   コンソール オペレーターは、ポリシーで提供されるデフォルト名です。ロールに別の名前を選択した場合は、代わりにその名前を選択します。

4. *メンバー*タブで、次の手順を実行します。
   a. マネージド **ID** へのアクセスを割り当てます。
   b. *メンバーの選択*を選択し、コンソール エージェント仮想マシンが作成されたサブスクリプションを選択し、*マネージド ID*の下で*仮想マシン*を選択して、コンソール エージェント仮想マシンを選択します。
   c. *選択*を選択します。
   d. *次へ*を選択します。
   e. *レビュー + 割り当て*を選択します。
   f. 追加の Azure サブスクリプションのリソースを管理する場合は、そのサブスクリプションに切り替えて、これらの手順を繰り返します。

次の手順

に行く "NetApp Console"コンソール エージェントの使用を開始します。

サービスプリンシパル

手順

1. *管理 > 資格情報*を選択します。
2. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: **Microsoft Azure >** エージェント を選択します。
   b. 資格情報の定義: 必要な権限を付与する Microsoft Entra サービス プリンシパルに関する情報を入力します。
      - アプリケーション（クライアント）ID
      - ディレクトリ（テナント）ID

- クライアントシークレット

c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。

d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

結果

これで、コンソール エージェントには、ユーザーに代わって Azure でアクションを実行するために必要なアクセス許可が付与されました。

Google Cloud

Google Cloud のコンソール エージェントのインストール オプション

Google Cloud でコンソール エージェントを作成するには、いくつかの方法があります。 NetApp Consoleから直接行うのが最も一般的な方法です。---

次のインストール オプションが利用可能です。

- "コンソールから直接コンソールエージェントを作成する"（これが標準オプションです）

  このアクションにより、選択した VPC で Linux とコンソール エージェント ソフトウェアを実行する VM インスタンスが起動します。

- "Google プラットフォームを使用してコンソール エージェントを作成する"

  このアクションでは、Linux とコンソール エージェント ソフトウェアを実行する VM インスタンスも起動しますが、デプロイはコンソールからではなく Google Cloud から直接開始されます。

- "自分のLinuxホストにソフトウェアをダウンロードして手動でインストールする"

選択したインストール オプションは、インストールの準備方法に影響します。これには、Google Cloud でリソースを認証および管理するために必要な権限をコンソールに付与する方法が含まれます。

NetApp Consoleから Google Cloud にコンソール エージェントを作成する

コンソールから Google Cloud にコンソール エージェントを作成できます。ネットワークを設定し、Google Cloud の権限を準備し、Google Cloud API を有効にして、コンソール エージェントを作成する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ネットワークを設定する

コンソール エージェントがターゲット ネットワークへの接続とアウトバウンド インターネット アクセスを使用してリソースを管理できるように、ネットワークを設定します。

VPCとサブネット

コンソール エージェントを作成するときは、そのエージェントが存在する VPC とサブネットを指定する必要があります。

ターゲットネットワークへの接続

コンソール エージェントには、システムを作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムまたはストレージ システムを作成する予定のネットワークなどです。

アウトバウンドインターネットアクセス

コンソール エージェントを展開するネットワークの場所には、特定のエンドポイントに接続するための送信インターネット接続が必要です。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

エンドポイント	目的
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Google Cloud 内のリソースを管理します。
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェア アップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォール ルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

NetAppコンソールから接続されたエンドポイント

SaaS レイヤーを通じて提供される Web ベースのNetApp Consoleを使用すると、複数のエンドポイントに接続してデータ管理タスクが完了します。これには、コンソールからコンソール エージェントを展開するために接続されるエンドポイントが含まれます。

"NetAppコンソールから接続されたエンドポイントのリストを表示します" 。

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用している場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インターネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

コンソール エージェントを作成した後、このネットワーク要件を実装します。

ステップ**2:** コンソールエージェントを作成するための権限を設定する

コンソールからコンソール エージェントをデプロイする前に、コンソール エージェント VM をデプロイする Google プラットフォーム ユーザーの権限を設定する必要があります。

手順

1. Google プラットフォームでカスタムロールを作成します。

   a. 次の権限を含む YAML ファイルを作成します。

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
```

```
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

b. Google Cloud から Cloud Shell を有効にします。

c. 必要な権限を含む YAML ファイルをアップロードします。

d. カスタムロールを作成するには、 `gcloud iam roles create`指示。

次の例では、プロジェクト レベルで「connectorDeployment」という名前のロールを作成します。

gcloud iam ロール コネクタデプロイメントを作成 --project=myproject --file=connector
-deployment.yaml

"Google Cloud ドキュメント: カスタムロールの作成と管理"

2. このカスタムロールは、コンソールから、または gcloud を使用してコンソール エージェントをデプロイするユーザーに割り当てます。

"Google Cloud ドキュメント: 単一のロールを付与する"

ステップ**3:** コンソールエージェント操作の権限を設定する

Google Cloud 内のリソースを管理するためにコンソールが必要とする権限をコンソール エージェントに付与するには、Google Cloud サービス アカウントが必要です。コンソール エージェントを作成するときは、このサービス アカウントをコンソール エージェント VM に関連付ける必要があります。

以降のリリースで新しい権限が追加された場合、カスタム ロールを更新するのはお客様の責任となります。新しい権限が必要な場合は、リリース ノートに記載されます。

手順

1. Google Cloud でカスタムロールを作成します。

   a. 以下の内容を含むYAMLファイルを作成します。"コンソールエージェントのサービスアカウント権限"。

   b. Google Cloud から Cloud Shell を有効にします。

   c. 必要な権限を含む YAML ファイルをアップロードします。

   d. カスタムロールを作成するには、 `gcloud iam roles create`指示。

      次の例では、プロジェクト レベルで「connector」という名前のロールを作成します。

      ```
      gcloud iam roles create connector --project=myproject --file=connector.yaml
      ```

   "Google Cloud ドキュメント: カスタムロールの作成と管理"

2. Google Cloud でサービス アカウントを作成し、そのサービス アカウントにロールを割り当てます。

   a. IAM & Admin サービスから、サービス アカウント > サービス アカウントの作成 を選択します。

   b. サービス アカウントの詳細を入力し、[作成して続行] を選択します。

   c. 作成したロールを選択します。

   d. 残りの手順を完了してロールを作成します。

      "Google Cloud ドキュメント: サービス アカウントの作成"

3. コンソール エージェントが存在するプロジェクトとは異なるプロジェクトにCloud Volumes ONTAPシステムを展開する予定の場合は、コンソール エージェントのサービス アカウントにそれらのプロジェクトへのアクセス権を付与する必要があります。

たとえば、コンソール エージェントがプロジェクト 1 にあり、プロジェクト 2 にCloud Volumes ONTAPシステムを作成するとします。プロジェクト 2 のサービス アカウントにアクセス権を付与する必要があります。

a. IAM & Admin サービスから、 Cloud Volumes ONTAPシステムを作成する Google Cloud プロジェクトを選択します。
b. **IAM** ページで、アクセスを許可 を選択し、必要な詳細を入力します。
   - コンソール エージェントのサービス アカウントの電子メールを入力します。
   - コンソール エージェントのカスタム ロールを選択します。
   - *保存*を選択します。

詳細については、 "Google Cloud ドキュメント"

ステップ**4:** 共有**VPC**権限を設定する

共有 VPC を使用してリソースをサービス プロジェクトにデプロイする場合は、権限を準備する必要があります。

この表は参考用であり、IAM 構成が完了すると、環境に権限表が反映されるはずです。

共有 **VPC** 権限を表示する

身元	クリエイター	開催地	サービスプロジェクトの権限	ホストプロジェクトの権限	目的
エージェントを展開するためのGoogleアカウント	カスタム	奉仕プロジェクト	"エージェント展開ポリシー"	compute.networkUser	サービスプロジェクトにエージェントをデプロイする
エージェントサービスアカウント	カスタム	奉仕プロジェクト	"エージェント サービス アカウント ポリシー"	compute.networkUser デプロイメントマネージャー.エディター	サービス プロジェクトでCloud Volumes ONTAPとサービスをデプロイおよび保守する
Cloud Volumes ONTAP サービスアカウント	カスタム	奉仕プロジェクト	storage.admin メンバー: serviceAccount.user としてのNetApp Consoleサービスアカウント	該当なし	（オプション） NetApp Cloud TieringおよびNetApp Backup and Recoveryの場合
Google API サービス エージェント	Google Cloud	奉仕プロジェクト	(デフォルト) エディター	compute.networkUser	デプロイメントに代わってGoogle Cloud API と対話します。コンソールが共有ネットワークを使用できるようにします。
Google Compute Engine のデフォルトのサービスアカウント	Google Cloud	奉仕プロジェクト	(デフォルト) エディター	compute.networkUser	デプロイメントに代わって、Google Cloud インスタンスとコンピューティング インフラストラクチャをデプロイします。コンソールが共有ネットワークを使用できるようにします。

注：

1. ファイアウォール ルールをデプロイメントに渡さず、コンソールで自動的に作成するように選択した場合にのみ、ホスト プロジェクトで deploymentmanager.editor が必要になります。ルールが指定されていない場合、 NetApp Consoleは、VPC0 ファイアウォール ルールを含むデプロイメントをホスト プロジェクトに作成します。
2. firewall.create と firewall.delete は、デプロイメントにファイアウォール ルールを渡さず、コンソールで自動的に作成するように選択した場合にのみ必要です。これらの権限は、コンソール アカウントの .yaml ファイルにあります。共有 VPC を使用して HA ペアを展開する場合、これらの権限は VPC1、2、3 のファイアウォール ルールを作成するために使用されます。他のすべてのデプロイメントでは、これらの権限は VPC0 のルールの作成にも使用されます。
3. クラウド階層化の場合、階層化サービス アカウントには、プロジェクト レベルだけでなく、サービス アカウントに対する serviceAccount.user ロールが必要です。現在、プロジェクト レベルで serviceAccount.user を割り当てると、getIAMPolicy を使用してサービス アカウントをクエリしても

権限が表示されません。

ステップ**5: Google Cloud API**を有効にする

Console エージェントとCloud Volumes ONTAPをデプロイする前に、いくつかの Google Cloud API を有効にする必要があります。

手順

1. プロジェクトで次の Google Cloud API を有効にします。
   - クラウド デプロイメント マネージャー V2 API
   - クラウドロギングAPI
   - クラウド リソース マネージャー API
   - コンピューティングエンジン API
   - アイデンティティとアクセス管理 (IAM) API
   - クラウド キー管理サービス (KMS) API

     （顧客管理暗号化キー（CMEK）を使用したNetApp Backup and Recoveryを使用する予定の場合のみ必要）

"Google Cloud ドキュメント: API の有効化"

ステップ**6:** コンソールエージェントを作成する

コンソールから直接コンソール エージェントを作成します。

タスク概要

コンソール エージェントを作成すると、デフォルト構成を使用して Google Cloud に仮想マシン インスタンスがデプロイされます。コンソール エージェントを作成した後、CPU や RAM が少ない小さな VM インスタンスに切り替えないでください。"コンソールエージェントのデフォルト構成について学習します" 。

開始する前に

次のものが必要です:

- コンソール エージェントとコンソール エージェント VM のサービス アカウントを作成するために必要な Google Cloud 権限。
- ネットワーク要件を満たす VPC とサブネット。
- コンソール エージェントからのインターネット アクセスにプロキシが必要な場合のプロキシ サーバーの詳細。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、*エージェントのデプロイ > Google Cloud*を選択します。
3. *エージェントのデプロイ*ページで、必要なものの詳細を確認します。次の 2 つのオプションがあります。

a. 製品内ガイドを使用して展開の準備をするには、[続行] を選択します。製品内ガイドの各ステップには、ドキュメントのこのページに記載されている情報が含まれています。

b. このページの手順に従ってすでに準備している場合は、[展開にスキップ] を選択します。

4. ウィザードの手順に従ってコンソール エージェントを作成します。

   - プロンプトが表示されたら、仮想マシン インスタンスを作成するために必要な権限を持つ Google アカウントにログインします。

     このフォームは Google が所有し、ホストしています。資格情報がNetAppに提供されていません。

   - 詳細: 仮想マシン インスタンスの名前を入力し、タグを指定して、プロジェクトを選択し、必要な権限を持つサービス アカウントを選択します (詳細については上記のセクションを参照してください)。
   - 場所: インスタンスのリージョン、ゾーン、VPC、サブネットを指定します。
   - ネットワーク: パブリック IP アドレスを有効にするかどうかを選択し、オプションでプロキシ構成を指定します。
   - ネットワーク タグ: 透過プロキシを使用している場合は、コンソール エージェント インスタンスにネットワーク タグを追加します。ネットワーク タグは小文字で始まる必要があり、小文字、数字、ハイフンを含めることができます。タグは小文字または数字で終わる必要があります。たとえば、「console-agent-proxy」というタグを使用できます。
   - ファイアウォール ポリシー: 新しいファイアウォール ポリシーを作成するか、必要な受信ルールと送信ルールを許可する既存のファイアウォール ポリシーを選択するかを選択します。

     "Google Cloud のファイアウォール ルール"

5. 選択内容を確認して、セットアップが正しいことを確認します。

   a. エージェント構成の検証 チェック ボックスはデフォルトでオンになっており、展開時にコンソールによってネットワーク接続要件が検証されます。コンソールがエージェントの展開に失敗した場合、トラブルシューティングに役立つレポートが提供されます。デプロイメントが成功した場合、レポートは提供されません。

   まだ使用している場合は"以前のエンドポイント"エージェントのアップグレードに使用すると、検証が失敗し、エラーが発生します。これを回避するには、チェックボックスをオフにして検証チェックをスキップします。

6. *追加*を選択します。

   インスタンスは約 10 分で準備完了します。プロセスが完了するまで、このページに留まってください。

結果

プロセスが完了すると、コンソール エージェントが使用できるようになります。

デプロイメントが失敗した場合は、コンソールからレポートとログをダウンロードして、問題の解決に役立てることができます。"インストールの問題をトラブルシューティングする方法を学びます。"

コンソール エージェントを作成したのと同じ Google Cloud アカウントに Google Cloud Storage バケットがある場合は、[システム] ページに Google Cloud Storage システムが自動的に表示されます。 "コンソールから

Google Cloud Storage を管理する方法を学びます"

Google Cloud からコンソール エージェントを作成する

Google Cloud を使用して Google Cloud にコンソール エージェントを作成するには、ネットワークを設定し、Google Cloud の権限を準備し、Google Cloud API を有効にして、コンソール エージェントを作成する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ネットワークを設定する

コンソール エージェントがリソースを管理し、ターゲット ネットワークおよびインターネットに接続できるようにネットワークを設定します。

VPCとサブネット

コンソール エージェントを作成するときは、そのエージェントが存在する VPC とサブネットを指定する必要があります。

ターゲットネットワークへの接続

コンソール エージェントには、システムを作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムまたはストレージ システムを作成する予定のネットワークなどです。

アウトバウンドインターネットアクセス

コンソール エージェントを展開するネットワークの場所には、特定のエンドポイントに接続するための送信インターネット接続が必要です。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

エンドポイント	目的
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Google Cloud 内のリソースを管理します。

エンドポイント	目的
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォールルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

NetAppコンソールから接続されたエンドポイント

SaaS レイヤーを通じて提供される Web ベースのNetApp Consoleを使用すると、複数のエンドポイントに接続してデータ管理タスクが完了します。これには、コンソールからコンソール エージェントを展開するために接続されるエンドポイントが含まれます。

"NetAppコンソールから接続されたエンドポイントのリストを表示します" 。

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用している場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インターネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

コンソール エージェントを作成した後、このネットワーク要件を実装します。

ステップ**2:** コンソールエージェントを作成するための権限を設定する

Google Cloud ユーザーが Google Cloud からコンソール エージェント VM をデプロイするための権限を設定します。

手順

1. Google プラットフォームでカスタムロールを作成します。

   a. 次の権限を含む YAML ファイルを作成します。

```
title: Console agent deployment policy
description: Permissions for the user who deploys the NetApp Console
agent
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
```

```
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

b. Google Cloud から Cloud Shell を有効にします。

c. 必要な権限を含む YAML ファイルをアップロードします。

d. カスタムロールを作成するには、 `gcloud iam roles create`指示。

次の例では、プロジェクト レベルで「connectorDeployment」という名前のロールを作成します。

gcloud iam ロール コネクタデプロイメントを作成 --project=myproject --file=connector -deployment.yaml

"Google Cloud ドキュメント: カスタムロールの作成と管理"

2. このカスタムロールを、Google Cloud からコンソール エージェントをデプロイするユーザーに割り当てます。

"Google Cloud ドキュメント: 単一のロールを付与する"

ステップ**3:** コンソールエージェント操作の権限を設定する

Google Cloud 内のリソースを管理するためにコンソールが必要とする権限をコンソール エージェントに付与するには、Google Cloud サービス アカウントが必要です。コンソール エージェントを作成するときは、このサービス アカウントをコンソール エージェント VM に関連付ける必要があります。

以降のリリースで新しい権限が追加された場合、カスタム ロールを更新するのはお客様の責任となります。新しい権限が必要な場合は、リリース ノートに記載されます。

手順

1. Google Cloud でカスタムロールを作成します。

a. 以下の内容を含むYAMLファイルを作成します。"コンソールエージェントのサービスアカウント権限"。

b. Google Cloud から Cloud Shell を有効にします。

c. 必要な権限を含む YAML ファイルをアップロードします。

d. カスタムロールを作成するには、 `gcloud iam roles create`指示。

次の例では、プロジェクト レベルで「connector」という名前のロールを作成します。

```
gcloud iam roles create connector --project=myproject --file=connector.yaml
```

"Google Cloud ドキュメント: カスタムロールの作成と管理"

2. Google Cloud でサービス アカウントを作成し、そのサービス アカウントにロールを割り当てます。

a. IAM & Admin サービスから、サービス アカウント **>** サービス アカウントの作成 を選択します。

b. サービス アカウントの詳細を入力し、[作成して続行] を選択します。

c. 作成したロールを選択します。

d. 残りの手順を完了してロールを作成します。

"Google Cloud ドキュメント: サービス アカウントの作成"

3. コンソール エージェントが存在するプロジェクトとは異なるプロジェクトにCloud Volumes ONTAPシステムを展開する予定の場合は、コンソール エージェントのサービス アカウントにそれらのプロジェクトへのアクセス権を付与する必要があります。

たとえば、コンソール エージェントがプロジェクト 1 にあり、プロジェクト 2 にCloud Volumes ONTAPシステムを作成するとします。プロジェクト 2 のサービス アカウントにアクセス権を付与する必要があります。

a. IAM & Admin サービスから、 Cloud Volumes ONTAPシステムを作成する Google Cloud プロジェクトを選択します。

b. **IAM** ページで、アクセスを許可 を選択し、必要な詳細を入力します。

- コンソール エージェントのサービス アカウントの電子メールを入力します。
- コンソール エージェントのカスタム ロールを選択します。
- *保存*を選択します。

詳細については、 "Google Cloud ドキュメント"

ステップ**4:** 共有**VPC**権限を設定する

共有 VPC を使用してリソースをサービス プロジェクトにデプロイする場合は、権限を準備する必要があります。

この表は参考用であり、IAM 構成が完了すると、環境に権限表が反映されるはずです。

共有 **VPC** 権限を表示する

身元	クリエイター	開催地	サービスプロジェクトの権限	ホストプロジェクトの権限	目的
エージェントを展開するためのGoogleアカウント	カスタム	奉仕プロジェクト	"エージェント展開ポリシー"	compute.networkUser	サービスプロジェクトにエージェントをデプロイする
エージェントサービスアカウント	カスタム	奉仕プロジェクト	"エージェント サービス アカウント ポリシー"	compute.networkUser デプロイメントマネージャー.エディター	サービス プロジェクトでCloud Volumes ONTAPとサービスをデプロイおよび保守する
Cloud Volumes ONTAP サービスアカウント	カスタム	奉仕プロジェクト	storage.admin メンバー: serviceAccount.user としてのNetApp Consoleサービスアカウント	該当なし	（オプション） NetApp Cloud TieringおよびNetApp Backup and Recoveryの場合
Google API サービス エージェント	Google Cloud	奉仕プロジェクト	(デフォルト) エディター	compute.networkUser	デプロイメントに代わってGoogle Cloud API と対話します。コンソールが共有ネットワークを使用できるようにします。
Google Compute Engine のデフォルトのサービスアカウント	Google Cloud	奉仕プロジェクト	(デフォルト) エディター	compute.networkUser	デプロイメントに代わって、Google Cloud インスタンスとコンピューティング インフラストラクチャをデプロイします。コンソールが共有ネットワークを使用できるようにします。

注：

1. ファイアウォール ルールをデプロイメントに渡さず、コンソールで自動的に作成するように選択した場合にのみ、ホスト プロジェクトで deploymentmanager.editor が必要になります。ルールが指定されていない場合、 NetApp Consoleは、VPC0 ファイアウォール ルールを含むデプロイメントをホスト プロジェクトに作成します。
2. firewall.create と firewall.delete は、デプロイメントにファイアウォール ルールを渡さず、コンソールで自動的に作成するように選択した場合にのみ必要です。これらの権限は、コンソール アカウントの .yaml ファイルにあります。共有 VPC を使用して HA ペアを展開する場合、これらの権限は VPC1、2、3 のファイアウォール ルールを作成するために使用されます。他のすべてのデプロイメントでは、これらの権限は VPC0 のルールの作成にも使用されます。
3. クラウド階層化の場合、階層化サービス アカウントには、プロジェクト レベルだけでなく、サービス アカウントに対する serviceAccount.user ロールが必要です。現在、プロジェクト レベルで serviceAccount.user を割り当てると、getIAMPolicy を使用してサービス アカウントをクエリしても

権限が表示されません。

ステップ**5: Google Cloud API**を有効にする

Console エージェントとCloud Volumes ONTAP をデプロイする前に、いくつかの Google Cloud API を有効にします。

手順

1. プロジェクトで次の Google Cloud API を有効にします。
   - クラウド デプロイメント マネージャー V2 API
   - クラウドロギングAPI
   - クラウド リソース マネージャー API
   - コンピューティングエンジン API
   - アイデンティティとアクセス管理 (IAM) API
   - クラウド キー管理サービス (KMS) API

     （顧客管理暗号化キー（CMEK）を使用したNetApp Backup and Recoveryを使用する予定の場合のみ必要）

"Google Cloud ドキュメント: API の有効化"

ステップ**6:** コンソールエージェントを作成する

Google Cloud を使用してコンソール エージェントを作成します。

コンソール エージェントを作成すると、デフォルト構成で Google Cloud に VM インスタンスがデプロイされます。コンソール エージェントを作成した後、CPU や RAM が少ない小さな VM インスタンスに切り替えないでください。"コンソールエージェントのデフォルト構成について学習します" 。

開始する前に

次のものが必要です:

- コンソール エージェントとコンソール エージェント VM のサービス アカウントを作成するために必要な Google Cloud 権限。
- ネットワーク要件を満たす VPC とサブネット。
- VM インスタンスの要件を理解していること。
  - **CPU**: 8 コアまたは 8 vCPU
  - **RAM**: 32 GB
  - マシンタイプ: n2-standard-8 を推奨します。

    Console エージェントは、Shielded VM 機能をサポートする OS を搭載した VM インスタンス上の Google Cloud でサポートされます。

手順

1. お好みの方法で Google Cloud SDK にログインします。

   この例では、gcloud SDK がインストールされたローカル シェルを使用していますが、Google Cloud Shell を使用することもできます。

   Google Cloud SDKの詳細については、"Google Cloud SDK ドキュメント ページ" 。

2. 上記のセクションで定義されている必要な権限を持つユーザーとしてログインしていることを確認します。

   ```
   gcloud auth list
   ```

   出力には次のように表示されます。* ユーザー アカウントは、ログインに使用するユーザー アカウントです。

   ```
   Credentialed Accounts
   ACTIVE  ACCOUNT
        some_user_account@domain.com
   *    desired_user_account@domain.com
   To set the active account, run:
    $ gcloud config set account `ACCOUNT`
   Updates are available for some Cloud SDK components. To install them,
   please run:
   $ gcloud components update
   ```

3. 実行 `gcloud compute instances create`指示：

   ```
   gcloud compute instances create <instance-name>
     --machine-type=n2-standard-8
     --image-project=netapp-cloudmanager
     --image-family=cloudmanager
     --scopes=cloud-platform
     --project=<project>
     --service-account=<service-account>
     --zone=<zone>
     --no-address
     --tags <network-tag>
     --network <network-path>
     --subnet <subnet-path>
     --boot-disk-kms-key <kms-key-path>
   ```

   インスタンス名
   : VM インスタンスの希望するインスタンス名。

プロジェクト
(オプション) VM をデプロイするプロジェクト。

サービスアカウント
手順 2 の出力で指定されたサービス アカウント。

ゾーン
VMを展開するゾーン

住所なし
(オプション) 外部 IP アドレスは使用されません (トラフィックをパブリック インターネットにルーティングするには、クラウド NAT またはプロキシが必要です)

ネットワークタグ
(オプション) ネットワーク タグ付けを追加して、タグを使用してファイアウォール ルールをコンソール エージェント インスタンスにリンクします。

ネットワークパス
(オプション) コンソールエージェントをデプロイするネットワークの名前を追加します (共有 VPC の場合はフルパスが必要です)

サブネットパス
(オプション) コンソールエージェントをデプロイするサブネットの名前を追加します (共有 VPC の場合はフルパスが必要です)

kmsキーパス
(オプション) コンソール エージェントのディスクを暗号化するための KMS キーを追加します (IAM 権限も適用する必要があります)

これらの旗の詳細については、"Google Cloud Compute SDK ドキュメント" 。

コマンドを実行すると、コンソール エージェントがデプロイされます。コンソール エージェント インスタンスとソフトウェアは、約 5 分以内に実行されるはずです。

4. Web ブラウザを開き、コンソール エージェント ホストの URL を入力します。

   コンソール ホスト URL は、ホストの構成に応じて、ローカルホスト、プライベート IP アドレス、またはパブリック IP アドレスになります。たとえば、コンソール エージェントがパブリック IP アドレスのないパブリック クラウドにある場合は、コンソール エージェント ホストに接続しているホストのプライベート IP アドレスを入力する必要があります。

5. ログイン後、コンソール エージェントを設定します。

   a. コンソール エージェントに関連付けるコンソール組織を指定します。

      "アイデンティティとアクセス管理について学ぶ" 。

   b. システムの名前を入力します。

結果

コンソール エージェントがインストールされ、コンソール組織に設定されました。

ウェブブラウザを開いて、 "NetApp Console"コンソール エージェントの使用を開始します。

Google Cloud にコンソール エージェントを手動でインストールする

独自の Linux ホストに Console エージェントを手動でインストールするには、ホストの要件を確認し、ネットワークを設定し、Google Cloud の権限を準備し、Google Cloud API を有効にし、Console をインストールして、準備した権限を付与する必要があります。

開始する前に

- あなたは"コンソールエージェントの理解"。
- 確認すべき"コンソールエージェントの制限"。

ステップ**1:** ホストの要件を確認する

コンソール エージェント ソフトウェアは、特定のオペレーティング システム要件、RAM 要件、ポート要件などを満たすホスト上で実行する必要があります。

> コンソール エージェントは、19000 ～ 19200 の UID と GID の範囲を予約します。この範囲は固定されており、変更することはできません。ホスト上のサードパーティ ソフトウェアがこの範囲内の UID または GID を使用している場合、エージェントのインストールは失敗します。NetApp、競合を回避するためにサードパーティ ソフトウェアがインストールされていないホストの使用を推奨しています。

専用ホスト

コンソール エージェントは、他のアプリケーションと共有されているホストではサポートされません。ホストは専用ホストである必要があります。ホストは、次のサイズ要件を満たす任意のアーキテクチャにすることができます。

- CPU: 8コアまたは8vCPU
- メモリ: 32 GB
- ディスク容量: ホストには 165 GB が推奨され、パーティション要件は次のとおりです。
  - `/opt`: 120 GiBの空き容量が必要です

    エージェントは `/opt`インストールするには `/opt/application/netapp`ディレクトリとその内容。
  - `/var`: 40 GiBの空き容量が必要です

    コンソールエージェントにはこのスペースが必要です `/var`Docker または Podman は、このディレクトリ内にコンテナを作成するように設計されているためです。具体的には、`/var/lib/containers/storage`ディレクトリ。このスペースでは外部マウントまたはシンボリックリンクは機能しません。

ハイパーバイザー

サポートされているオペレーティング システムを実行することが認定されているベア メタルまたはホスト型ハイパーバイザーが必要です。

オペレーティングシステムとコンテナの要件

コンソールを標準モードまたは制限モードで使用する場合、コンソール エージェントは次のオペレーティング システムでサポートされます。エージェントをインストールする前に、コンテナ オーケストレーション ツールが必要です。

オペレーティング システム	サポートされるOS バージョン	サポートされているエージェントのバージョン	必要なコンテナツール	SELinux は
Red Hat Enterprise Linux	9.1～9.4 8.6～8.10 • 英語版のみ。 • ホストは Red Hat Subscription Management に登録されている必要があります。登録されていない場合、ホストはエージェントのインストール中に必要なサードパーティ製ソフトウェアを更新するためにリポジトリにアクセスできません。	3.9.50 以降、コンソールが標準モードまたは制限モード	Podman バージョン 4.6.1 または 4.9.4 Podman の構成要件を表示する 。	強制モードまたは許可モードでサポートされます • Cloud Volumes ONTAPシステムの管理は、オペレーティングシステムで SELinux が有効になっているエージェントではサポートされません。
Ubuntu	24.04 LTS	3.9.45 以降、NetApp Consoleが標準モードまたは制限モード	Docker エンジン 23.06 から 28.0.0。	サポート対象外

Google Cloud マシンタイプ

上記の CPU および RAM の要件を満たすインスタンス タイプ。 n2-standard-8 をお勧めします。

コンソールエージェントは、Google Cloud の VM インスタンスで、以下の OS がサポートする環境でサポートされます。 "シールドされたVMの機能"

/optのディスク容量

100 GiBの空き容量が必要です

エージェントは `/opt`インストールするには `/opt/application/netapp`ディレクトリとその内容。

/varのディスク容量

20 GiBの空き容量が必要です

コンソールエージェントにはこのスペースが必要です `/var`Docker または Podman は、このディレクトリ内にコンテナを作成するように設計されているためです。具体的には、 `/var/lib/containers/storage`ディレクトリ。このスペースでは外部マウントまたはシンボリックリンクは機能しません。

ステップ**2: Podman**または**Docker Engine**をインストールする

オペレーティング システムに応じて、エージェントをインストールする前に Podman または Docker Engine のいずれかが必要になります。

- Red Hat Enterprise Linux 8 および 9 には Podman が必要です。

  サポートされているPodmanのバージョンを表示する 。

- Ubuntu には Docker Engine が必要です。

  サポートされている Docker エンジンのバージョンを表示する 。

例 3. 手順

ポッドマン

Podman をインストールして設定するには、次の手順に従います。

- podman.socket サービスを有効にして起動します
- Python3をインストールする
- podman-compose パッケージ バージョン 1.0.6 をインストールします。
- podman-composeをPATH環境変数に追加する
- Red Hat Enterprise Linux を使用している場合は、Podman バージョンが CNI ではなく Netavark Aardvark DNS を使用していることを確認してください。

DNS ポートの競合を避けるために、エージェントをインストールした後、aardvark-dns ポート (デフォルト: 53) を調整します。指示に従ってポートを構成します。

手順

1. ホストに podman-docker パッケージがインストールされている場合は削除します。

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Podman をインストールします。

   Podman は、公式の Red Hat Enterprise Linux リポジトリから入手できます。

   Red Hat Enterprise Linux 9 の場合:

```
sudo dnf install podman-2:<version>
```

   <version> は、インストールする Podman のサポートされているバージョンです。サポートされているPodmanのバージョンを表示する 。

   Red Hat Enterprise Linux 8 の場合:

```
sudo dnf install podman-3:<version>
```

   <version> は、インストールする Podman のサポートされているバージョンです。サポートされているPodmanのバージョンを表示する 。

3. podman.socket サービスを有効にして起動します。

```
sudo systemctl enable --now podman.socket
```

4. python3 をインストールします。

```
sudo dnf install python3
```

5. システムにまだインストールされていない場合は、EPEL リポジトリ パッケージをインストールします。
6. Red Hat Enterprise を使用している場合:

   podman-compose は、Extra Packages for Enterprise Linux (EPEL) リポジトリから入手できるため、この手順は必須です。

   Red Hat Enterprise Linux 9 の場合:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   Red Hat Enterprise Linux 8 の場合:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

7. podman-compose パッケージ 1.0.6 をインストールします。

```
sudo dnf install podman-compose-1.0.6
```

   使用して `dnf install`コマンドは、PATH 環境変数に podman-compose を追加するための要件を満たしています。インストールコマンドは、すでにインストールされているpodman-composeを/usr/binに追加します。 `secure_path`ホスト上のオプション。

8. Red Hat Enterprise Linux 8 を使用している場合は、Podman バージョンが CNI ではなく Aardvark DNS を備えた NetAvark を使用していることを確認します。

   a. 次のコマンドを実行して、networkBackend が CNI に設定されているかどうかを確認します。

```
podman info | grep networkBackend
```

   b. networkBackendが `CNI`、それを変更する必要があります `netavark`。

   c. インストール `netavark`そして `aardvark-dns`次のコマンドを使用します。

```
dnf install aardvark-dns netavark
```

d. 開く `/etc/containers/containers.conf`ファイルを編集し、network_backend オプションを変更して、「cni」の代わりに「netavark」を使用します。

もし `/etc/containers/containers.conf`存在しない場合は、設定を変更してください `/usr/share/containers/containers.conf`。

9. podman を再起動します。

```
systemctl restart podman
```

10. 次のコマンドを使用して、networkBackend が「netavark」に変更されていることを確認します。

```
podman info | grep networkBackend
```

Dockerエンジン

Docker のドキュメントに従って Docker Engine をインストールします。

手順

1. "Dockerからのインストール手順を見る"

   サポートされている Docker エンジン バージョンをインストールするには、手順に従ってください。最新バージョンはコンソールでサポートされていないため、インストールしないでください。

2. Docker が有効になっていて実行されていることを確認します。

```
sudo systemctl enable docker && sudo systemctl start docker
```

ステップ**3:** ネットワークを設定する

コンソール エージェントがハイブリッド クラウド環境内のリソースとプロセスを管理できるようにネットワークを設定します。たとえば、ターゲット ネットワークへの接続が利用可能であること、および発信インターネット アクセスが利用可能であることを確認する必要があります。

ターゲットネットワークへの接続

コンソール エージェントには、システムを作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムまたはストレージ システムを作成する予定のネットワークなどです。

アウトバウンドインターネットアクセス

コンソール エージェントを展開するネットワークの場所には、特定のエンドポイントに接続するための送信インターネット接続が必要です。

Webベースの**NetApp Console**を使用する際にコンピュータから接続されるエンドポイント

Web ブラウザからコンソールにアクセスするコンピュータは、複数のエンドポイントに接続できる必要があります。コンソール エージェントを設定し、コンソールを日常的に使用するには、コンソールを使用す

る必要があります。

"NetAppコンソールのネットワークを準備する" 。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

エンドポイント	目的
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Google Cloud 内のリソースを管理します。
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォール ルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用している場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インター

ネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

ステップ**4:** コンソールエージェントの権限を設定する

Google Cloud 内のリソースを管理するためにコンソールが必要とする権限をコンソール エージェントに付与するには、Google Cloud サービス アカウントが必要です。コンソール エージェントを作成するときは、このサービス アカウントをコンソール エージェント VM に関連付ける必要があります。

以降のリリースで新しい権限が追加された場合、カスタム ロールを更新するのはお客様の責任となります。新しい権限が必要な場合は、リリース ノートに記載されます。

手順

1. Google Cloud でカスタムロールを作成します。

   a. 以下の内容を含むYAMLファイルを作成します。"コンソールエージェントのサービスアカウント権限"。

   b. Google Cloud から Cloud Shell を有効にします。

   c. 必要な権限を含む YAML ファイルをアップロードします。

   d. カスタムロールを作成するには、 `gcloud iam roles create`指示。

      次の例では、プロジェクト レベルで「connector」という名前のロールを作成します。

      ```
      gcloud iam roles create connector --project=myproject --file=connector.yaml
      ```

   "Google Cloud ドキュメント: カスタムロールの作成と管理"

2. Google Cloud でサービス アカウントを作成し、そのサービス アカウントにロールを割り当てます。

   a. IAM & Admin サービスから、サービス アカウント **>** サービス アカウントの作成 を選択します。

   b. サービス アカウントの詳細を入力し、[作成して続行] を選択します。

   c. 作成したロールを選択します。

   d. 残りの手順を完了してロールを作成します。

      "Google Cloud ドキュメント: サービス アカウントの作成"

3. コンソール エージェントが存在するプロジェクトとは異なるプロジェクトにCloud Volumes ONTAPシステムを展開する予定の場合は、コンソール エージェントのサービス アカウントにそれらのプロジェクトへのアクセス権を付与する必要があります。

   たとえば、コンソール エージェントがプロジェクト 1 にあり、プロジェクト 2 にCloud Volumes ONTAPシステムを作成するとします。プロジェクト 2 のサービス アカウントにアクセス権を付与する必要があ

ります。

a. IAM & Admin サービスから、 Cloud Volumes ONTAPシステムを作成する Google Cloud プロジェクトを選択します。

b. **IAM** ページで、アクセスを許可 を選択し、必要な詳細を入力します。

   - コンソール エージェントのサービス アカウントの電子メールを入力します。
   - コンソール エージェントのカスタム ロールを選択します。
   - *保存*を選択します。

詳細については、 "Google Cloud ドキュメント"

ステップ**5:** 共有**VPC**権限を設定する

共有 VPC を使用してリソースをサービス プロジェクトにデプロイする場合は、権限を準備する必要があります。

この表は参考用であり、IAM 構成が完了すると、環境に権限表が反映されるはずです。

共有 **VPC** 権限を表示する

身元	クリエイター	開催地	サービスプロジェクトの権限	ホストプロジェクトの権限	目的
エージェントを展開するためのGoogleアカウント	カスタム	奉仕プロジェクト	"エージェント展開ポリシー"	compute.networkUser	サービスプロジェクトにエージェントをデプロイする
エージェントサービスアカウント	カスタム	奉仕プロジェクト	"エージェント サービス アカウント ポリシー"	compute.networkUser デプロイメントマネージャー.エディター	サービス プロジェクトでCloud Volumes ONTAPとサービスをデプロイおよび保守する
Cloud Volumes ONTAP サービスアカウント	カスタム	奉仕プロジェクト	storage.admin メンバー: serviceAccount.user としてのNetApp Consoleサービスアカウント	該当なし	（オプション） NetApp Cloud TieringおよびNetApp Backup and Recoveryの場合
Google API サービス エージェント	Google Cloud	奉仕プロジェクト	(デフォルト) エディター	compute.networkUser	デプロイメントに代わって Google Cloud API と対話します。コンソールが共有ネットワークを使用できるようにします。
Google Compute Engine のデフォルトのサービスアカウント	Google Cloud	奉仕プロジェクト	(デフォルト) エディター	compute.networkUser	デプロイメントに代わって、Google Cloud インスタンスとコンピューティング インフラストラクチャをデプロイします。コンソールが共有ネットワークを使用できるようにします。

注：

1. ファイアウォール ルールをデプロイメントに渡さず、コンソールで自動的に作成するように選択した場合にのみ、ホスト プロジェクトで deploymentmanager.editor が必要になります。ルールが指定されていない場合、 NetApp Consoleは、VPC0 ファイアウォール ルールを含むデプロイメントをホスト プロジェクトに作成します。
2. firewall.create と firewall.delete は、デプロイメントにファイアウォール ルールを渡さず、コンソールで自動的に作成するように選択した場合にのみ必要です。これらの権限は、コンソール アカウントの .yaml ファイルにあります。共有 VPC を使用して HA ペアを展開する場合、これらの権限は VPC1、2、3 のファイアウォール ルールを作成するために使用されます。他のすべてのデプロイメントでは、これらの権限は VPC0 のルールの作成にも使用されます。
3. クラウド階層化の場合、階層化サービス アカウントには、プロジェクト レベルだけでなく、サービス アカウントに対する serviceAccount.user ロールが必要です。現在、プロジェクト レベルで serviceAccount.user を割り当てると、getIAMPolicy を使用してサービス アカウントをクエリしても

権限が表示されません。

ステップ6: Google Cloud APIを有効にする

Google Cloud にCloud Volumes ONTAPシステムをデプロイする前に、いくつかの Google Cloud API を有効にする必要があります。

手順

1. プロジェクトで次の Google Cloud API を有効にします。
   - クラウド デプロイメント マネージャー V2 API
   - クラウドロギングAPI
   - クラウド リソース マネージャー API
   - コンピューティングエンジン API
   - アイデンティティとアクセス管理 (IAM) API
   - クラウド キー管理サービス (KMS) API

     （顧客管理暗号化キー（CMEK）を使用したNetApp Backup and Recoveryを使用する予定の場合のみ必要）

"Google Cloud ドキュメント: API の有効化"

ステップ7: コンソールエージェントをインストールする

前提条件が完了したら、独自の Linux ホストにソフトウェアを手動でインストールできます。

開始する前に

次のものが必要です:

- コンソール エージェントをインストールするためのルート権限。
- コンソール エージェントからのインターネット アクセスにプロキシが必要な場合のプロキシ サーバーの詳細。

  インストール後にプロキシ サーバーを構成するオプションがありますが、これを行うにはコンソール エージェントを再起動する必要があります。

- プロキシ サーバーが HTTPS を使用する場合、またはプロキシがインターセプト プロキシである場合は、CA 署名証明書。

コンソール エージェントを手動でインストールする場合、透過プロキシ サーバーの証明書を設定することはできません。透過プロキシ サーバーの証明書を設定する必要がある場合は、インストール後にメンテナンス コンソールを使用する必要があります。詳細はこちら"エージェントメンテナンスコンソール"。

タスク概要

NetAppサポート サイトで入手できるインストーラーは、以前のバージョンである可能性があります。インストール後、新しいバージョンが利用可能な場合、コンソール エージェントは自動的に更新されます。

手順

1. ホストに *http_proxy* または *https_proxy* システム変数が設定されている場合は、それらを削除します。

```
unset http_proxy
unset https_proxy
```

これらのシステム変数を削除しないと、インストールは失敗します。

2. コンソールエージェントソフトウェアを以下からダウンロードします。 "NetAppサポート サイト"それを Linux ホストにコピーします。

ネットワークまたはクラウドで使用するための「オンライン」エージェント インストーラーをダウンロードする必要があります。

3. スクリプトを実行するための権限を割り当てます。

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

<version> は、ダウンロードしたコンソール エージェントのバージョンです。

4. Government Cloud 環境にインストールする場合は、構成チェックを無効にします。"手動インストールの構成チェックを無効にする方法を説明します。"

5. インストール スクリプトを実行します。

```
 ./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

ネットワークでインターネット アクセスにプロキシが必要な場合は、プロキシ情報を追加する必要があります。透過プロキシまたは明示プロキシのいずれかを追加できます。 --proxy および --cacert パラメータはオプションであり、追加するように要求されることはありません。プロキシ サーバーがある場合は、示されているようにパラメータを入力する必要があります。

CA 署名証明書を使用して明示的なプロキシ サーバーを構成する例を次に示します。

```
 ./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

`--proxy`次のいずれかの形式を使用して、コンソール エージェントが HTTP または HTTPS プロキシ サーバーを使用するように構成します。

- http://アドレス:ポート
- http://ユーザー名:パスワード@アドレス:ポート

- http://ドメイン名%92ユーザー名:パスワード@アドレス:ポート
- https://アドレス:ポート
- https://ユーザー名:パスワード@アドレス:ポート
- https://ドメイン名%92ユーザー名:パスワード@アドレス:ポート

  次の点に注意してください。

  - ユーザーはローカル ユーザーまたはドメイン ユーザーになります。
  - ドメイン ユーザーの場合は、上記のように \ の ASCII コードを使用する必要があります。
  - コンソール エージェントは、@ 文字を含むユーザー名またはパスワードをサポートしていません。
  - パスワードに以下の特殊文字が含まれている場合は、その特殊文字の前にバックスラッシュ (& または !) を付けてエスケープする必要があります。

    例えば：

http://bxpproxyuser:netapp1\!@アドレス:3128

`--cacert`コンソール エージェントとプロキシ サーバー間の HTTPS アクセスに使用する CA 署名付き証明書を指定します。このパラメータは、HTTPS プロキシ サーバー、インターセプト プロキシ サーバー、および透過プロキシ サーバーに必須です。

+ 透過プロキシ サーバーを構成する例を次に示します。透過プロキシを構成する場合、プロキシ サーバーを定義する必要はありません。コンソール エージェント ホストには、CA 署名付き証明書のみを追加します。

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

1. Podman を使用した場合は、aardvark-dns ポートを調整する必要があります。
   a. コンソール エージェント仮想マシンに SSH で接続します。
   b. podman */usr/share/containers/containers.conf* ファイルを開き、Aardvark DNS サービス用に選択したポートを変更します。たとえば、54 に変更します。

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

c. コンソール エージェント仮想マシンを再起動します。

2. インストールが完了するまでお待ちください。

プロキシ サーバーを指定した場合、インストールの最後に、コンソール エージェント サービス (occm) が 2 回再起動します。

インストールが失敗した場合は、インストール レポートとログを表示して問題の解決に役立てることができます。"インストールの問題をトラブルシューティングする方法を学びます。"

1. コンソール エージェント仮想マシンに接続しているホストから Web ブラウザを開き、次の URL を入力します。

https://ipaddress

2. ログイン後、コンソール エージェントを設定します。

a. コンソール エージェントに関連付ける組織を指定します。

b. システムの名前を入力します。

c. 安全な環境で実行していますか**?** の下で、制限モードを無効のままにします。

以下の手順ではコンソールを標準モードで使用する方法について説明しているため、制限モードは無効にしておく必要があります。安全な環境があり、このアカウントをバックエンド サービスから切断する場合にのみ、制限モードを有効にする必要があります。もしそうなら、"NetApp Consoleを制限モードで使い始めるための手順に従います" 。

d. *始めましょう*を選択します。

インストールが失敗した場合は、トラブルシューティングに役立つログとレポートを表示できます。"インストールの問題をトラブルシューティングする方法を学びます。"

コンソール エージェントを作成したのと同じ Google Cloud アカウントに Google Cloud Storage バケットがある場合は、[システム] ページに Google Cloud Storage システムが自動的に表示されます。 "NetApp Consoleから Google Cloud Storage を管理する方法を学びます"

ステップ**8:** コンソールエージェントに権限を付与する

以前に設定した Google Cloud 権限をコンソール エージェントに提供する必要があります。権限を付与すると、コンソール エージェントが Google Cloud 内のデータとストレージ インフラストラクチャを管理できるようになります。

手順

1. Google Cloud ポータルに移動し、サービス アカウントをコンソール エージェント VM インスタンスに割り当てます。

   "Google Cloud ドキュメント: インスタンスのサービス アカウントとアクセス スコープの変更"

2. 他の Google Cloud プロジェクトのリソースを管理する場合は、コンソール エージェントのロールを持つサービス アカウントをそのプロジェクトに追加してアクセス権を付与します。プロジェクトごとにこの手順を繰り返す必要があります。

オンプレミスにエージェントをインストールする

オンプレミスにコンソールエージェントを手動でインストールする

オンプレミスにコンソール エージェントをインストールし、ログインして、コンソール組織で動作するように設定します。

VMWare ユーザーの場合は、OVA を使用して VCenter にコンソール エージェントをインストールできます。"VCenter にエージェントをインストールする方法の詳細について説明します。"

インストールする前に、ホスト (VM または Linux ホスト) が要件を満たしていること、およびコンソール エージェントがインターネットと対象ネットワークへの送信アクセスできることを確認する必要があります。NetAppデータ サービス、またはCloud Volumes ONTAPなどのクラウド ストレージ オプションを使用する予定の場合は、コンソール エージェントがユーザーに代わってクラウド内でアクションを実行できるように、クラウド プロバイダーで資格情報を作成してコンソールに追加する必要があります。

コンソールエージェントのインストールの準備

コンソール エージェントをインストールする前に、インストール要件を満たすホスト マシンがあることを確認する必要があります。また、ネットワーク管理者と協力して、コンソール エージェントが必要なエンドポイントへの送信アクセスと対象ネットワークへの接続を持っていることを確認する必要があります。

コンソールエージェントホストの要件を確認する

オペレーティング システム、RAM、およびポートの要件を満たす x86 ホストでコンソール エージェントを実行します。コンソール エージェントをインストールする前に、ホストがこれらの要件を満たしていることを確認してください。

コンソール エージェントは、19000 ～ 19200 の UID と GID の範囲を予約します。この範囲は固定されており、変更することはできません。ホスト上のサードパーティ ソフトウェアがこの範囲内の UID または GID を使用している場合、エージェントのインストールは失敗します。NetApp、競合を回避するためにサードパーティ ソフトウェアがインストールされていないホストの使用を推奨しています。

専用ホスト

コンソール エージェントは、他のアプリケーションと共有されているホストではサポートされません。ホストは専用ホストである必要があります。ホストは、次のサイズ要件を満たす任意のアーキテクチャにすることができます。

- CPU: 8コアまたは8vCPU
- メモリ: 32 GB
- ディスク容量: ホストには 165 GB が推奨され、パーティション要件は次のとおりです。
  - `/opt`: 120 GiBの空き容量が必要です

    エージェントは `/opt`インストールするには `/opt/application/netapp`ディレクトリとその内容。

  - `/var`: 40 GiBの空き容量が必要です

    コンソールエージェントにはこのスペースが必要です `/var`Docker または Podman は、このディレクトリ内にコンテナを作成するように設計されているためです。具体的には、`/var/lib/containers/storage`ディレクトリ。このスペースでは外部マウントまたはシンボリックリンクは機能しません。

ハイパーバイザー

サポートされているオペレーティング システムを実行することが認定されているベア メタルまたはホスト型ハイパーバイザーが必要です。

オペレーティングシステムとコンテナの要件

コンソールを標準モードまたは制限モードで使用する場合、コンソール エージェントは次のオペレーティング システムでサポートされます。エージェントをインストールする前に、コンテナ オーケストレーション ツールが必要です。

オペレーティングシステム	サポートされるOSバージョン	サポートされているエージェントのバージョン	必要なコンテナツール	SELinux は
Red Hat Enterprise Linux	9.1～9.4 8.6～8.10 • 英語版のみ。 • ホストは Red Hat Subscription Management に登録されている必要があります。登録されていない場合、ホストはエージェントのインストール中に必要なサードパーティ製ソフトウェアを更新するためにリポジトリにアクセスできません。	3.9.50 以降、コンソールが標準モードまたは制限モード	Podman バージョン 4.6.1 または 4.9.4 Podman の構成要件を表示する 。	強制モードまたは許可モードでサポートされます • Cloud Volumes ONTAPシステムの管理は、オペレーティングシステムで SELinux が有効になっているエージェントではサポートされません。
Ubuntu	24.04 LTS	3.9.45 以降、NetApp Consoleが標準モードまたは制限モード	Docker エンジン 23.06 から 28.0.0。	サポート対象外

コンソールエージェントのネットワークアクセスを設定する

コンソール エージェントがリソースを管理できるようにネットワーク アクセスを設定します。ターゲット ネットワークへの接続と特定のエンドポイントへのアウトバウンド インターネット アクセスが必要です。

ターゲットネットワークへの接続

コンソール エージェントには、システムを作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムまたはストレージ システムを作成する予定のネットワークなどです。

アウトバウンドインターネットアクセス

コンソール エージェントを展開するネットワークの場所には、特定のエンドポイントに接続するための送信インターネット接続が必要です。

Webベースの**NetApp Console**を使用する際にコンピュータから接続されるエンドポイント

Web ブラウザからコンソールにアクセスするコンピュータは、複数のエンドポイントに接続できる必要があります。コンソール エージェントを設定し、コンソールを日常的に使用するには、コンソールを使用する必要があります。

"NetAppコンソールのネットワークを準備する" 。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

オンプレミスにインストールされたコンソール エージェントは、Google Cloud 内のリソースを管理できません。 Google Cloud リソースを管理するには、Google Cloud にエージェントをインストールする必要があります。

AWS

コンソール エージェントをオンプレミスでインストールする場合、AWS に導入されたNetAppシステム (Cloud Volumes ONTAPなど) を管理するために、次の AWS エンドポイントへのネットワーク アクセスが必要です。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

エンドポイント	目的
AWS サービス (amazonaws.com): • クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理（IAM） • キー管理サービス (KMS) • セキュリティトークンサービス（STS） • シンプルストレージサービス（S3）	AWS リソースを管理します。エンドポイントは AWS リージョンによって異なります。 "詳細についてはAWSドキュメントを参照してください"
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォール ルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

Azure

コンソール エージェントがオンプレミスにインストールされている場合、Azure にデプロイされたNetAppシステム (Cloud Volumes ONTAPなど) を管理するために、次の Azure エンドポイントへのネットワーク アクセスが必要です。

エンドポイント	目的
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure パブリック リージョン内のリソースを管理します。
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure China リージョンのリソースを管理します。
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。

エンドポイント	目的
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォールルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用して

いる場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インターネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

AWS または **Azure** のコンソール エージェント クラウド権限を作成する

オンプレミスのコンソールエージェントを使用して AWS または Azure のNetAppデータ サービスを使用する場合は、クラウド プロバイダーで権限を設定し、インストール後にコンソールエージェントに資格情報を追加する必要があります。

Google Cloud に存在するリソースを管理するには、Google Cloud に Console エージェントをインストールする必要があります。

AWS

コンソール エージェントがオンプレミスにインストールされている場合は、必要な権限を持つ IAM ユーザーのアクセス キーを追加して、コンソールに AWS 権限を付与する必要があります。

コンソール エージェントがオンプレミスにインストールされている場合は、この認証方法を使用する必要があります。 IAM ロールは使用できません。

手順

1. AWS コンソールにログインし、IAM サービスに移動します。
2. ポリシーを作成します。

   a. *ポリシー > ポリシーの作成*を選択します。

   b. *JSON*を選択し、その内容をコピーして貼り付けます。"コンソールエージェントのIAMポリシー" 。

   c. 残りの手順を完了してポリシーを作成します。

      使用する予定のNetAppデータ サービスによっては、2 番目のポリシーを作成する必要がある場合があります。

   標準リージョンの場合、権限は 2 つのポリシーに分散されます。 AWS の管理ポリシーの最大文字サイズ制限により、2 つのポリシーが必要になります。"コンソールエージェントのIAMポリシーの詳細" 。

3. IAM ユーザーにポリシーをアタッチします。
   - "AWSドキュメント: IAMロールの作成"
   - "AWSドキュメント: IAMポリシーの追加と削除"
4. コンソール エージェントをインストールした後、 NetApp Consoleに追加できるアクセス キーがユーザーにあることを確認します。

結果

これで、必要な権限を持つ IAM ユーザーのアクセス キーを取得できるはずです。コンソール エージェントをインストールした後、コンソールからこれらの資格情報をコンソール エージェントに関連付けます。

Azure

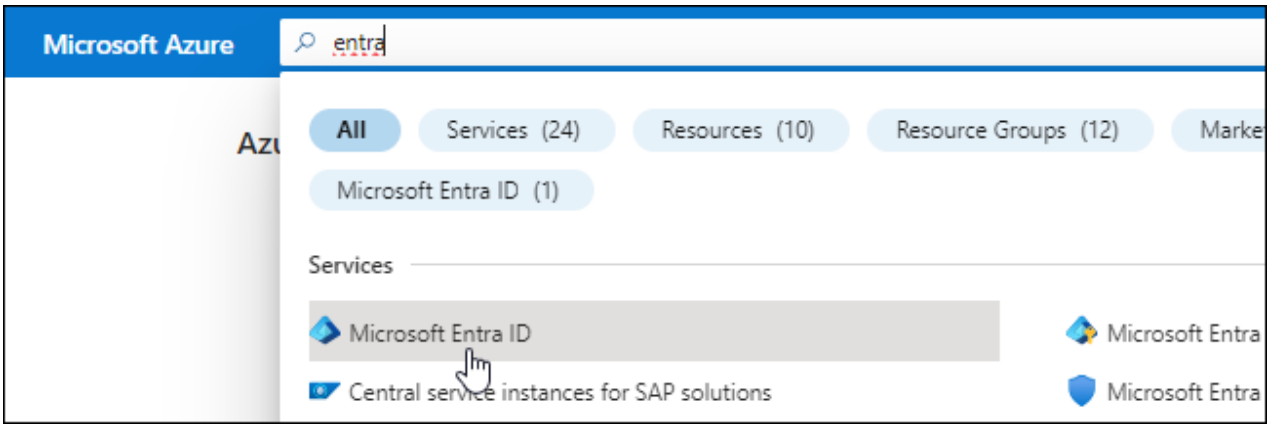
コンソール エージェントがオンプレミスでインストールされている場合は、Microsoft Entra ID でサービス プリンシパルを設定し、コンソール エージェントに必要な Azure 資格情報を取得して、コンソール エージェントに Azure 権限を付与する必要があります。

ロールベースのアクセス制御用の **Microsoft Entra** アプリケーションを作成する

1. Azure で Active Directory アプリケーションを作成し、そのアプリケーションをロールに割り当てるためのアクセス許可があることを確認します。

   詳細については、 "Microsoft Azure ドキュメント: 必要な権限"

2. Azure ポータルから、**Microsoft Entra ID** サービスを開きます。



3. メニューで*アプリ登録*を選択します。
4. *新規登録*を選択します。
5. アプリケーションの詳細を指定します。
   - 名前: アプリケーションの名前を入力します。
   - アカウント タイプ: アカウント タイプを選択します (いずれのタイプもNetApp Consoleで使用できます)。
   - リダイレクト **URI**: このフィールドは空白のままにすることができます。
6. *登録*を選択します。

   AD アプリケーションとサービス プリンシパルを作成しました。

アプリケーションをロールに割り当てる

1. カスタム ロールを作成します。

   Azure ポータル、Azure PowerShell、Azure CLI、または REST API を使用して、Azure カスタム ロールを作成できます。次の手順は、Azure CLI を使用してロールを作成する方法を示しています。別の方法をご希望の場合は、 "Azureドキュメント"

   a. の内容をコピーします"コンソールエージェントのカスタムロール権限"JSON ファイルに保存します。
   b. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、JSON ファイルを変更します。

      ユーザーがCloud Volumes ONTAPシステムを作成する各 Azure サブスクリプションの ID を追加する必要があります。

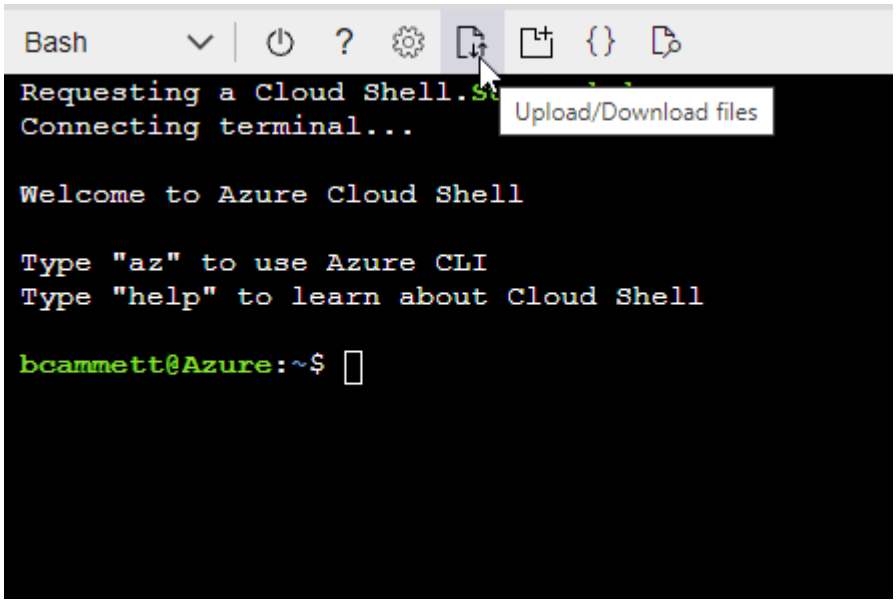
      例

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

c. JSON ファイルを使用して、Azure でカスタム ロールを作成します。

次の手順では、Azure Cloud Shell で Bash を使用してロールを作成する方法について説明します。

- 始める "Azure クラウド シェル"Bash 環境を選択します。
- JSON ファイルをアップロードします。



- Azure CLI を使用してカスタム ロールを作成します。

```
az role definition create --role-definition
Connector_Policy.json
```

これで、コンソール エージェント仮想マシンに割り当てることができる、コンソール オペレーターと呼ばれるカスタム ロールが作成されます。

2. アプリケーションをロールに割り当てます。

a. Azure ポータルから、サブスクリプション サービスを開きます。

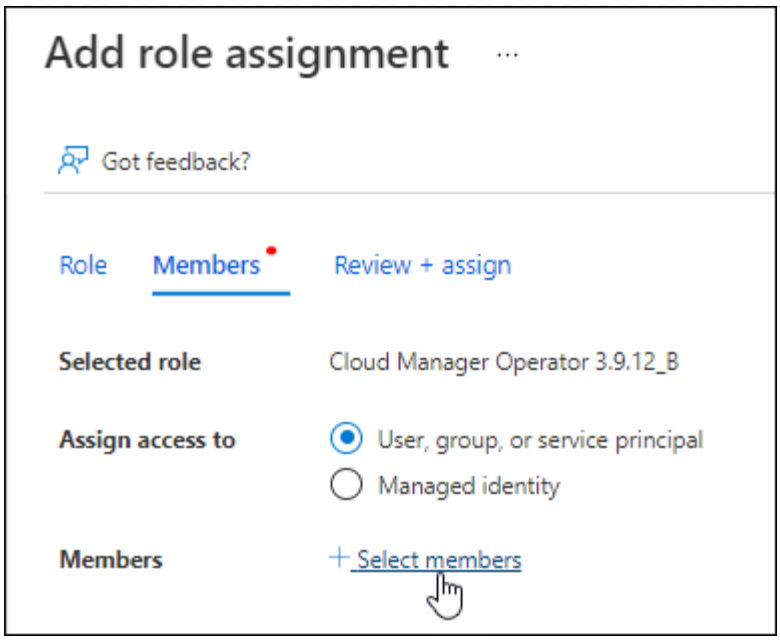
b. サブスクリプションを選択します。

c. アクセス制御 **(IAM) >** 追加 **>** ロール割り当ての追加 を選択します。

d. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。

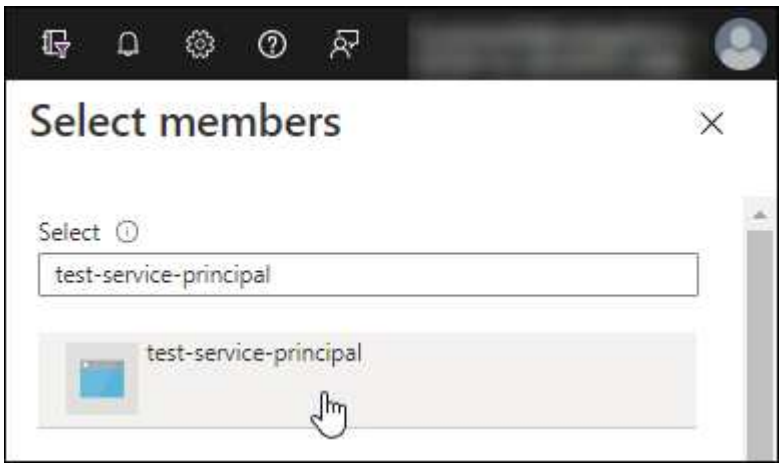
e. *メンバー*タブで、次の手順を実行します。

- *ユーザー、グループ、またはサービス プリンシパル*を選択したままにします。
- *メンバーを選択*を選択します。



- アプリケーションの名前を検索します。

  次に例を示します。



- アプリケーションを選択し、[選択] を選択します。
- *次へ*を選択します。

f. *レビュー + 割り当て*を選択します。

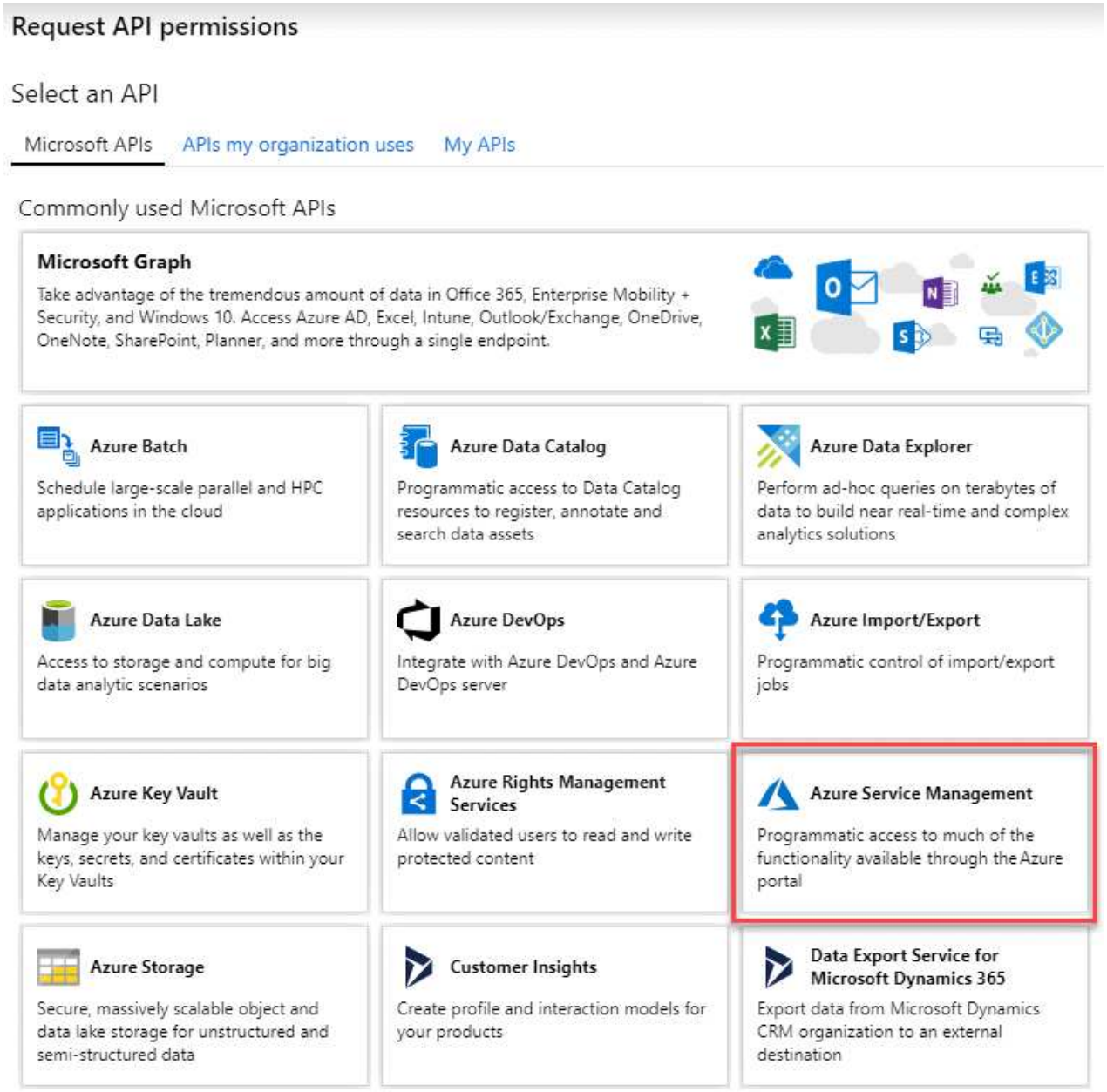
これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

複数の Azure サブスクリプションからCloud Volumes ONTAPをデプロイする場合は、サービス プリンシパルを各サブスクリプションにバインドする必要があります。 NetApp Consoleでは、 Cloud Volumes ONTAP をデプロイするときに使用するサブスクリプションを選択できます。

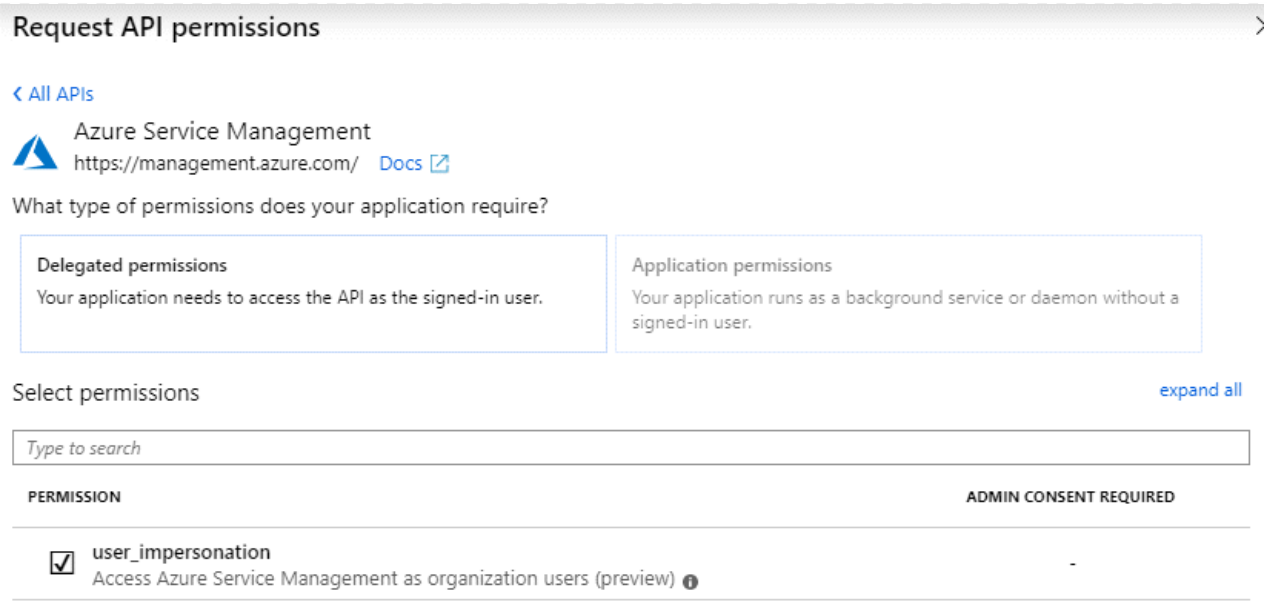
Windows Azure サービス管理 **API** 権限を追加する

1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. **API** 権限 **>** 権限の追加 を選択します。

3. **Microsoft API** の下で、**Azure Service Management** を選択します。

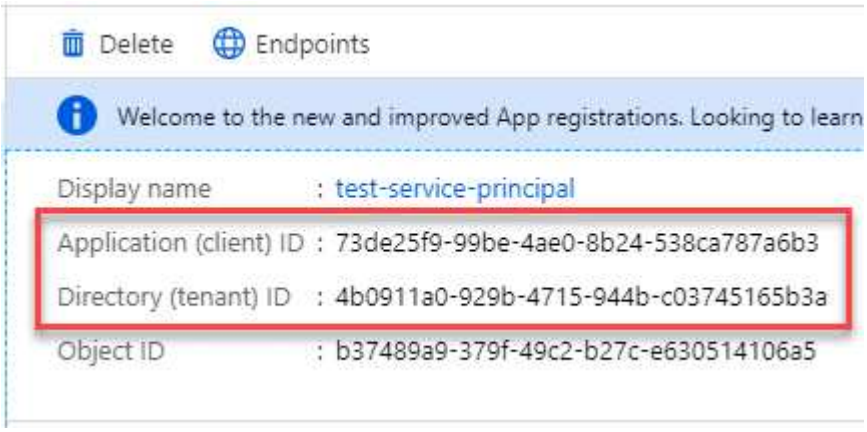


4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。



アプリケーションのアプリケーション**ID**とディレクトリ**ID**を取得します

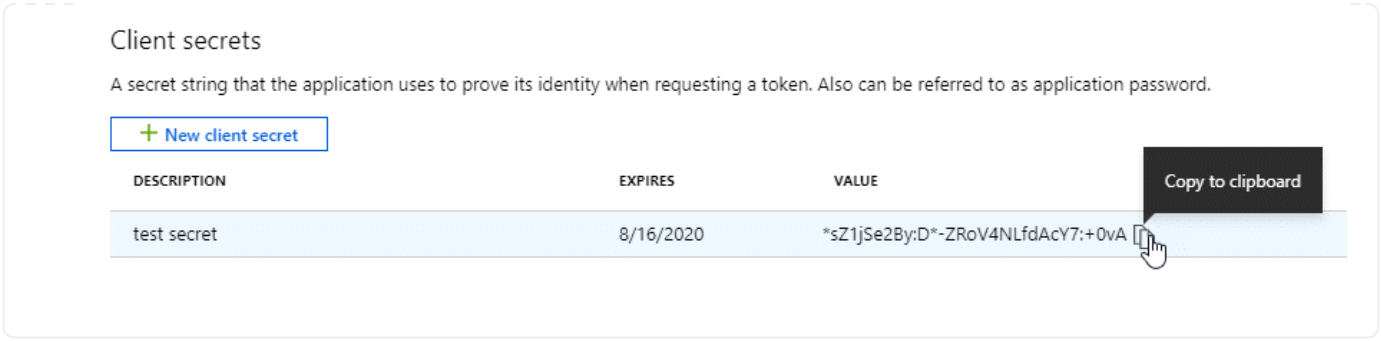
1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. アプリケーション **(**クライアント**) ID** と ディレクトリ **(**テナント**) ID** をコピーします。



Azure アカウントをコンソールに追加するときは、アプリケーションのアプリケーション (クライアント) ID とディレクトリ (テナント) ID を指定する必要があります。コンソールは ID を使用してプログラムでサインインします。

クライアントシークレットを作成する

1. **Microsoft Entra ID** サービスを開きます。
2. *アプリ登録*を選択し、アプリケーションを選択します。
3. *証明書とシークレット > 新しいクライアント シークレット*を選択します。
4. シークレットの説明と期間を指定します。
5. *追加*を選択します。
6. クライアント シークレットの値をコピーします。



コンソールエージェントを手動でインストールする

コンソール エージェントを手動でインストールする場合は、要件を満たすようにマシン環境を準備する必要があります。 Linux マシンが必要であり、Linux オペレーティング システムに応じて Podman または Docker をインストールする必要があります。

Podmanまたは**Docker Engine**をインストールする

オペレーティング システムに応じて、エージェントをインストールする前に Podman または Docker Engine のいずれかが必要になります。

- Red Hat Enterprise Linux 8 および 9 には Podman が必要です。

  サポートされているPodmanのバージョンを表示する 。

- Ubuntu には Docker Engine が必要です。

  サポートされている Docker エンジンのバージョンを表示する 。

例 **4.** 手順

ポッドマン

Podman をインストールして設定するには、次の手順に従います。

- podman.socket サービスを有効にして起動します
- Python3をインストールする
- podman-compose パッケージ バージョン 1.0.6 をインストールします。
- podman-composeをPATH環境変数に追加する
- Red Hat Enterprise Linux を使用している場合は、Podman バージョンが CNI ではなく Netavark Aardvark DNS を使用していることを確認してください。

DNS ポートの競合を避けるために、エージェントをインストールした後、aardvark-dns ポート (デフォルト: 53) を調整します。指示に従ってポートを構成します。

手順

1. ホストに podman-docker パッケージがインストールされている場合は削除します。

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Podman をインストールします。

   Podman は、公式の Red Hat Enterprise Linux リポジトリから入手できます。

   Red Hat Enterprise Linux 9 の場合:

```
sudo dnf install podman-2:<version>
```

   <version> は、インストールする Podman のサポートされているバージョンです。サポートされているPodmanのバージョンを表示する 。

   Red Hat Enterprise Linux 8 の場合:

```
sudo dnf install podman-3:<version>
```

   <version> は、インストールする Podman のサポートされているバージョンです。サポートされているPodmanのバージョンを表示する 。

3. podman.socket サービスを有効にして起動します。

```
sudo systemctl enable --now podman.socket
```

4. python3 をインストールします。

```
sudo dnf install python3
```

5. システムにまだインストールされていない場合は、EPEL リポジトリ パッケージをインストールします。
6. Red Hat Enterprise を使用している場合:

   podman-compose は、Extra Packages for Enterprise Linux (EPEL) リポジトリから入手できるため、この手順は必須です。

   Red Hat Enterprise Linux 9 の場合:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   Red Hat Enterprise Linux 8 の場合:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

7. podman-compose パッケージ 1.0.6 をインストールします。

```
sudo dnf install podman-compose-1.0.6
```

   使用して `dnf install`コマンドは、PATH 環境変数に podman-compose を追加するための要件を満たしています。インストールコマンドは、すでにインストールされているpodman-composeを/usr/binに追加します。 `secure_path`ホスト上のオプション。

8. Red Hat Enterprise Linux 8 を使用している場合は、Podman バージョンが CNI ではなく Aardvark DNS を備えた NetAvark を使用していることを確認します。

   a. 次のコマンドを実行して、networkBackend が CNI に設定されているかどうかを確認します。

```
podman info | grep networkBackend
```

   b. networkBackendが `CNI`、それを変更する必要があります `netavark`。

   c. インストール `netavark`そして `aardvark-dns`次のコマンドを使用します。

```
dnf install aardvark-dns netavark
```

d. 開く `/etc/containers/containers.conf`ファイルを編集し、network_backend オプションを変更して、「cni」の代わりに「netavark」を使用します。

もし `/etc/containers/containers.conf`存在しない場合は、設定を変更してください `/usr/share/containers/containers.conf`。

9. podman を再起動します。

```
systemctl restart podman
```

10. 次のコマンドを使用して、networkBackend が「netavark」に変更されていることを確認します。

```
podman info | grep networkBackend
```

Dockerエンジン

Docker のドキュメントに従って Docker Engine をインストールします。

手順

1. "Dockerからのインストール手順を見る"

   サポートされている Docker エンジン バージョンをインストールするには、手順に従ってください。最新バージョンはコンソールでサポートされていないため、インストールしないでください。

2. Docker が有効になっていて実行されていることを確認します。

```
sudo systemctl enable docker && sudo systemctl start docker
```

コンソールエージェントを手動でインストールする

オンプレミスの既存の Linux ホストにコンソール エージェント ソフトウェアをダウンロードしてインストールします。

開始する前に

次のものが必要です:

- コンソール エージェントをインストールするためのルート権限。
- コンソール エージェントからのインターネット アクセスにプロキシが必要な場合のプロキシ サーバーの詳細。

  インストール後にプロキシ サーバーを構成するオプションがありますが、これを行うにはコンソール エージェントを再起動する必要があります。

- プロキシ サーバーが HTTPS を使用する場合、またはプロキシがインターセプト プロキシである場合は、CA 署名証明書。

コンソール エージェントを手動でインストールする場合、透過プロキシ サーバーの証明書を設定することはできません。透過プロキシ サーバーの証明書を設定する必要がある場合は、インストール後にメンテナンス コンソールを使用する必要があります。詳細はこちら"エージェントメンテナンスコンソール"。

タスク概要

NetAppサポート サイトで入手できるインストーラーは、以前のバージョンである可能性があります。インストール後、新しいバージョンが利用可能な場合、コンソール エージェントは自動的に更新されます。

手順

1. ホストに *http_proxy* または *https_proxy* システム変数が設定されている場合は、それらを削除します。

```
unset http_proxy
unset https_proxy
```

これらのシステム変数を削除しないと、インストールは失敗します。

2. コンソールエージェントソフトウェアを以下からダウンロードします。 "NetAppサポート サイト"それを Linux ホストにコピーします。

ネットワークまたはクラウドで使用するための「オンライン」エージェント インストーラーをダウンロードする必要があります。

3. スクリプトを実行するための権限を割り当てます。

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

<version> は、ダウンロードしたコンソール エージェントのバージョンです。

4. Government Cloud 環境にインストールする場合は、構成チェックを無効にします。"手動インストールの構成チェックを無効にする方法を説明します。"
5. インストール スクリプトを実行します。

```
 ./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

ネットワークでインターネット アクセスにプロキシが必要な場合は、プロキシ情報を追加する必要があります。透過プロキシまたは明示プロキシのいずれかを追加できます。 --proxy および --cacert パラメータはオプションであり、追加するように要求されることはありません。プロキシ サーバーがある場合は、示されているようにパラメータを入力する必要があります。

CA 署名証明書を使用して明示的なプロキシ サーバーを構成する例を次に示します。

```
 ./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

`--proxy`次のいずれかの形式を使用して、コンソール エージェントが HTTP または HTTPS プロキシ サーバーを使用するように構成します。

- http://アドレス:ポート
- http://ユーザー名:パスワード@アドレス:ポート
- http://ドメイン名%92ユーザー名:パスワード@アドレス:ポート
- https://アドレス:ポート
- https://ユーザー名:パスワード@アドレス:ポート
- https://ドメイン名%92ユーザー名:パスワード@アドレス:ポート

  次の点に注意してください。

  - ユーザーはローカル ユーザーまたはドメイン ユーザーになります。
  - ドメイン ユーザーの場合は、上記のように \ の ASCII コードを使用する必要があります。
  - コンソール エージェントは、@ 文字を含むユーザー名またはパスワードをサポートしていません。
  - パスワードに以下の特殊文字が含まれている場合は、その特殊文字の前にバックスラッシュ (& または !) を付けてエスケープする必要があります。

    例えば：

http://bxpproxyuser:netapp1\!@アドレス:3128

`--cacert`コンソール エージェントとプロキシ サーバー間の HTTPS アクセスに使用する CA 署名付き証明書を指定します。このパラメータは、HTTPS プロキシ サーバー、インターセプト プロキシ サーバー、および透過プロキシ サーバーに必須です。

+ 透過プロキシ サーバーを構成する例を次に示します。透過プロキシを構成する場合、プロキシ サーバーを定義する必要はありません。コンソール エージェント ホストには、CA 署名付き証明書のみを追加します。

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

1. Podman を使用した場合は、aardvark-dns ポートを調整する必要があります。
   a. コンソール エージェント仮想マシンに SSH で接続します。
   b. podman */usr/share/containers/containers.conf* ファイルを開き、Aardvark DNS サービス用に選択したポートを変更します。たとえば、54 に変更します。

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

c. コンソール エージェント仮想マシンを再起動します。

次は何？

NetApp Console内でコンソール エージェントを登録する必要があります。

NetApp Consoleにコンソールエージェントを登録する

コンソールにログインし、コンソール エージェントを組織に関連付けます。ログイン方法は、コンソールを使用しているモードによって異なります。コンソールを標準モードで使用している場合は、SaaS Web サイトからログインします。コンソールを制限モードで使用している場合は、コンソール エージェント ホストからローカルにログインします。

手順

1. Web ブラウザを開き、コンソール エージェント ホストの URL を入力します。

   コンソール ホスト URL は、ホストの構成に応じて、ローカルホスト、プライベート IP アドレス、またはパブリック IP アドレスになります。たとえば、コンソール エージェントがパブリック IP アドレスのないパブリック クラウドにある場合は、コンソール エージェント ホストに接続しているホストのプライベート IP アドレスを入力する必要があります。

2. サインアップまたはログインしてください。
3. ログイン後、コンソールを設定します。
   a. コンソール エージェントに関連付けるコンソール組織を指定します。
   b. システムの名前を入力します。
   c. 安全な環境で実行していますか**?** の下で、制限モードを無効のままにします。

      コンソール エージェントがオンプレミスにインストールされている場合、制限モードはサポートされません。

   d. *始めましょう*を選択します。

NetApp Consoleにクラウドプロバイダーの資格情報を提供する

コンソール エージェントをインストールしてセットアップしたら、コンソール エージェントが AWS または Azure でアクションを実行するために必要な権限を持つように、クラウド資格情報を追加します。

AWS

開始する前に

これらの AWS 認証情報を作成したばかりの場合は、使用可能になるまでに数分かかることがあります。資格情報をコンソールに追加する前に、数分待ってください。

手順

1. *管理 > 資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: *Amazon Web Services > エージェントを選択します。
   b. 資格情報の定義: AWS アクセスキーとシークレットキーを入力します。
   c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。
   d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

これで、 "NetApp Console"コンソール エージェントの使用を開始します。

Azure

開始する前に

これらの Azure 資格情報を作成したばかりの場合は、使用可能になるまでに数分かかることがあります。コンソール エージェントに資格情報を追加する前に、数分間お待ちください。

手順

1. *管理 > 資格情報*を選択します。
2. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: **Microsoft Azure >** エージェント を選択します。
   b. 資格情報の定義: 必要な権限を付与する Microsoft Entra サービス プリンシパルに関する情報を入力します。
      - アプリケーション（クライアント）ID
      - ディレクトリ（テナント）ID
      - クライアントシークレット
   c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。
   d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

結果

これで、コンソール エージェントには、ユーザーに代わって Azure でアクションを実行するために必要なアクセス許可が付与されました。これで、 "NetApp Console"コンソール エージェントの使用を開始します。

VMWare ユーザーの場合は、OVA を使用して VCenter にコンソール エージェントをインストールできます。 OVA のダウンロードまたは URL は、NetApp Consoleから入手できます。

VCenter ツールと共にコンソール エージェントをインストールすると、VM Web コンソールを使用してメンテナンス タスクを実行できます。"エージェントの VM コンソールの詳細について説明します。"

コンソールエージェントのインストールの準備

インストールする前に、VM ホストが要件を満たしており、コンソール エージェントがインターネットおよび対象のネットワークにアクセスできることを確認してください。 NetAppデータ サービスまたはCloud Volumes ONTAP を使用するには、コンソール エージェントがユーザーに代わってアクションを実行できるように、クラウド プロバイダの資格情報を作成します。

コンソールエージェントホストの要件を確認する

コンソール エージェントをインストールする前に、ホスト マシンがインストール要件を満たしていることを確認してください。

- CPU: 8コアまたは8vCPU
- メモリ: 32 GB
- ディスク容量: 165 GB (シックプロビジョニング)
- vSphere 7.0以降
- ESXi ホスト 7.03 以上

エージェントを ESXi ホストに直接インストールするのではなく、vCenter 環境にインストールします。

コンソールエージェントのネットワークアクセスを設定する

ネットワーク管理者と協力して、コンソール エージェントが必要なエンドポイントへの送信アクセスと対象ネットワークへの接続を持っていることを確認します。

ターゲットネットワークへの接続

コンソール エージェントには、システムを作成および管理する予定の場所へのネットワーク接続が必要です。たとえば、オンプレミス環境にCloud Volumes ONTAPシステムまたはストレージ システムを作成する予定のネットワークなどです。

アウトバウンドインターネットアクセス

コンソール エージェントを展開するネットワークの場所には、特定のエンドポイントに接続するための送信インターネット接続が必要です。

Webベースの**NetApp Console**を使用する際にコンピュータから接続されるエンドポイント

Web ブラウザからコンソールにアクセスするコンピュータは、複数のエンドポイントに接続できる必要があります。コンソール エージェントを設定し、コンソールを日常的に使用するには、コンソールを使用す

る必要があります。

"NetAppコンソールのネットワークを準備する" 。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

オンプレミスにコンソール エージェントがインストールされている場合、Google Cloud のリソースを管理することはできません。 Google Cloud リソースを管理するには、Google Cloud にエージェントをインストールします。

AWS

コンソール エージェントをオンプレミスでインストールする場合、AWS に導入されたNetAppシステム (Cloud Volumes ONTAPなど) を管理するために、次の AWS エンドポイントへのネットワーク アクセスが必要です。

コンソールエージェントから接続されたエンドポイント

コンソール エージェントは、日常業務でパブリック クラウド環境内のリソースとプロセスを管理するために、次のエンドポイントに接続するために、送信インターネット アクセスを必要とします。

以下にリストされているエンドポイントはすべて CNAME エントリです。

エンドポイント	目的
AWS サービス (amazonaws.com): • クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理（IAM） • キー管理サービス (KMS) • セキュリティトークンサービス（STS） • シンプルストレージサービス（S3）	AWS リソースを管理します。エンドポイントは AWS リージョンによって異なります。 "詳細についてはAWSドキュメントを参照してください"
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォール ルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

Azure

コンソール エージェントがオンプレミスにインストールされている場合、Azure にデプロイされたNetAppシステム (Cloud Volumes ONTAPなど) を管理するために、次の Azure エンドポイントへのネットワーク アクセスが必要です。

エンドポイント	目的
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure パブリック リージョン内のリソースを管理します。
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure China リージョンのリソースを管理します。
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。

エンドポイント	目的
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォールルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用して

いる場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インターネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

AWS または **Azure** のコンソール エージェント クラウド権限を作成する

オンプレミスのコンソールエージェントを使用して AWS または Azure のNetAppデータ サービスを使用する場合は、インストール後にコンソールエージェントに資格情報を追加できるように、クラウド プロバイダーで権限を設定する必要があります。

オンプレミスにコンソール エージェントがインストールされている場合、Google Cloud のリソースを管理することはできません。 Google Cloud リソースを管理するには、Google Cloud にエージェントをインストールする必要があります。

AWS

オンプレミスのコンソールエージェントの場合は、IAM ユーザーアクセスキーを追加して AWS 権限を付与します。

オンプレミスのコンソール エージェントには IAM ユーザー アクセス キーを使用します。オンプレミスのコンソール エージェントでは IAM ロールはサポートされていません。

手順

1. AWS コンソールにログインし、IAM サービスに移動します。
2. ポリシーを作成します。

   a. *ポリシー > ポリシーの作成*を選択します。

   b. *JSON*を選択し、その内容をコピーして貼り付けます。"コンソールエージェントのIAMポリシー" 。

   c. 残りの手順を完了してポリシーを作成します。

      使用する予定のNetAppデータ サービスによっては、2 番目のポリシーを作成する必要がある場合があります。

   標準リージョンの場合、権限は 2 つのポリシーに分散されます。 AWS の管理ポリシーの最大文字サイズ制限により、2 つのポリシーが必要になります。"コンソールエージェントのIAMポリシーの詳細" 。

3. IAM ユーザーにポリシーをアタッチします。
   - "AWSドキュメント: IAMロールの作成"
   - "AWSドキュメント: IAMポリシーの追加と削除"
4. コンソール エージェントをインストールした後、 NetApp Consoleに追加できるアクセス キーがユーザーにあることを確認します。

結果

これで、必要な権限を持つ IAM ユーザー アクセス キーを取得できるはずです。コンソール エージェントをインストールした後、コンソールからこれらの認証情報をコンソール エージェントに関連付けます。

Azure

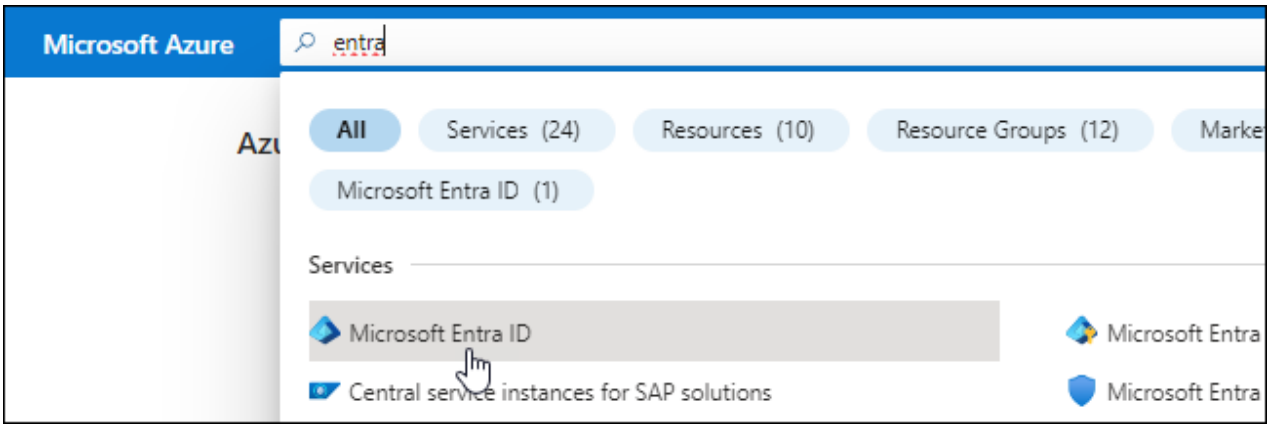
コンソール エージェントがオンプレミスでインストールされている場合は、Microsoft Entra ID でサービス プリンシパルを設定し、コンソール エージェントに必要な Azure 資格情報を取得して、コンソール エージェントに Azure 権限を付与する必要があります。

ロールベースのアクセス制御用の **Microsoft Entra** アプリケーションを作成する

1. Azure で Active Directory アプリケーションを作成し、そのアプリケーションをロールに割り当てるためのアクセス許可があることを確認します。

   詳細については、 "Microsoft Azure ドキュメント: 必要な権限"

2. Azure ポータルから、**Microsoft Entra ID** サービスを開きます。



3. メニューで*アプリ登録*を選択します。
4. *新規登録*を選択します。
5. アプリケーションの詳細を指定します。
   - 名前: アプリケーションの名前を入力します。
   - アカウント タイプ: アカウント タイプを選択します (いずれのタイプもNetApp Consoleで使用できます)。
   - リダイレクト **URI**: このフィールドは空白のままにすることができます。
6. *登録*を選択します。

AD アプリケーションとサービス プリンシパルを作成しました。

アプリケーションをロールに割り当てる

1. カスタム ロールを作成します。

   Azure ポータル、Azure PowerShell、Azure CLI、または REST API を使用して、Azure カスタム ロールを作成できます。次の手順は、Azure CLI を使用してロールを作成する方法を示しています。別の方法をご希望の場合は、 "Azureドキュメント"

   a. の内容をコピーします"コンソールエージェントのカスタムロール権限"JSON ファイルに保存します。
   b. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、JSON ファイルを変更します。

      ユーザーがCloud Volumes ONTAPシステムを作成する各 Azure サブスクリプションの ID を追加する必要があります。

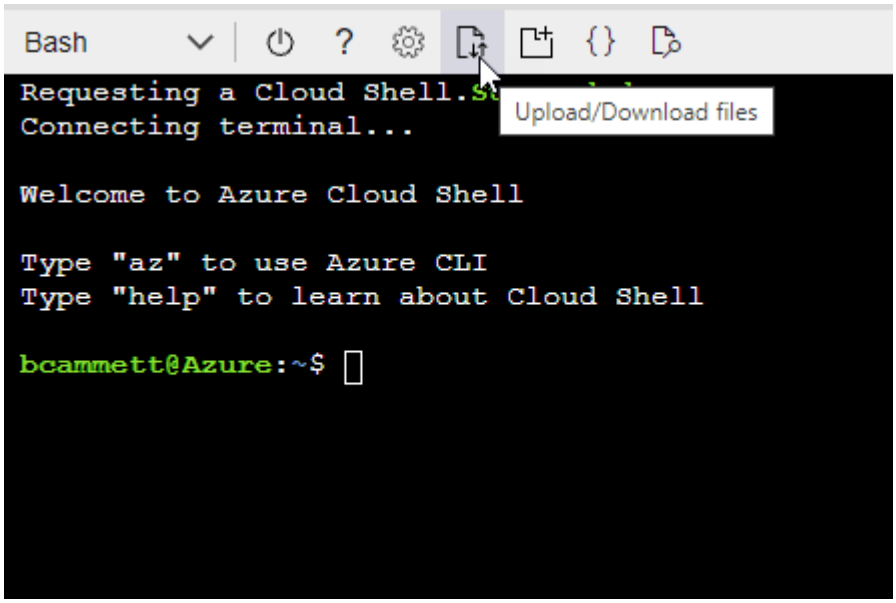
      例

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

c. JSON ファイルを使用して、Azure でカスタム ロールを作成します。

次の手順では、Azure Cloud Shell で Bash を使用してロールを作成する方法について説明します。

- 始める "Azure クラウド シェル"Bash 環境を選択します。
- JSON ファイルをアップロードします。



- Azure CLI を使用してカスタム ロールを作成します。

```
az role definition create --role-definition
Connector_Policy.json
```

これで、コンソール エージェント仮想マシンに割り当てることができる、コンソール オペレーターと呼ばれるカスタム ロールが作成されます。

2. アプリケーションをロールに割り当てます。

a. Azure ポータルから、サブスクリプション サービスを開きます。

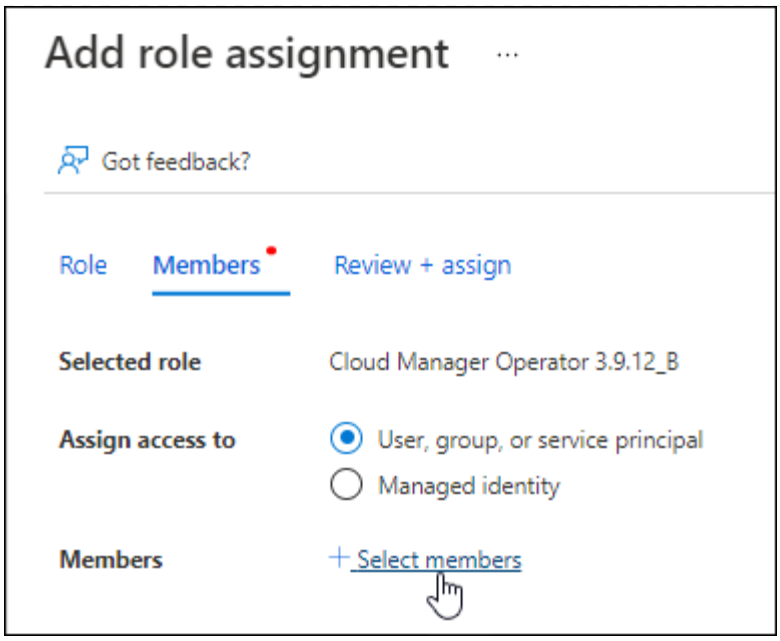
b. サブスクリプションを選択します。

c. アクセス制御 **(IAM) >** 追加 **>** ロール割り当ての追加 を選択します。

d. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。

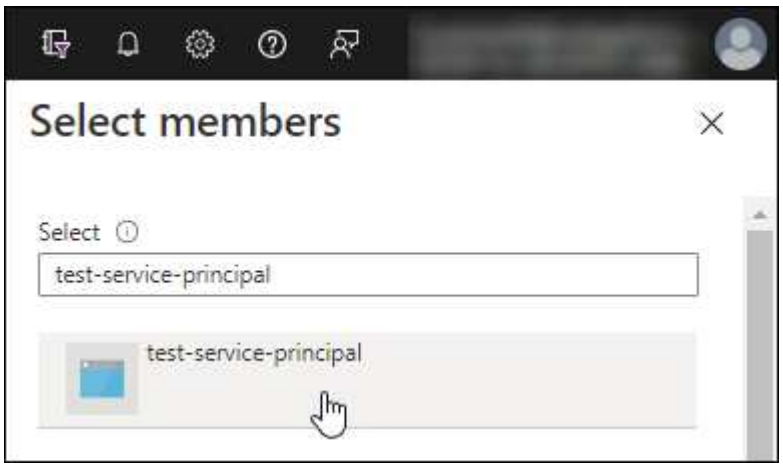
e. *メンバー*タブで、次の手順を実行します。

- *ユーザー、グループ、またはサービス プリンシパル*を選択したままにします。
- *メンバーを選択*を選択します。



- アプリケーションの名前を検索します。

  次に例を示します。



- アプリケーションを選択し、[選択] を選択します。
- *次へ*を選択します。

f. *レビュー + 割り当て*を選択します。

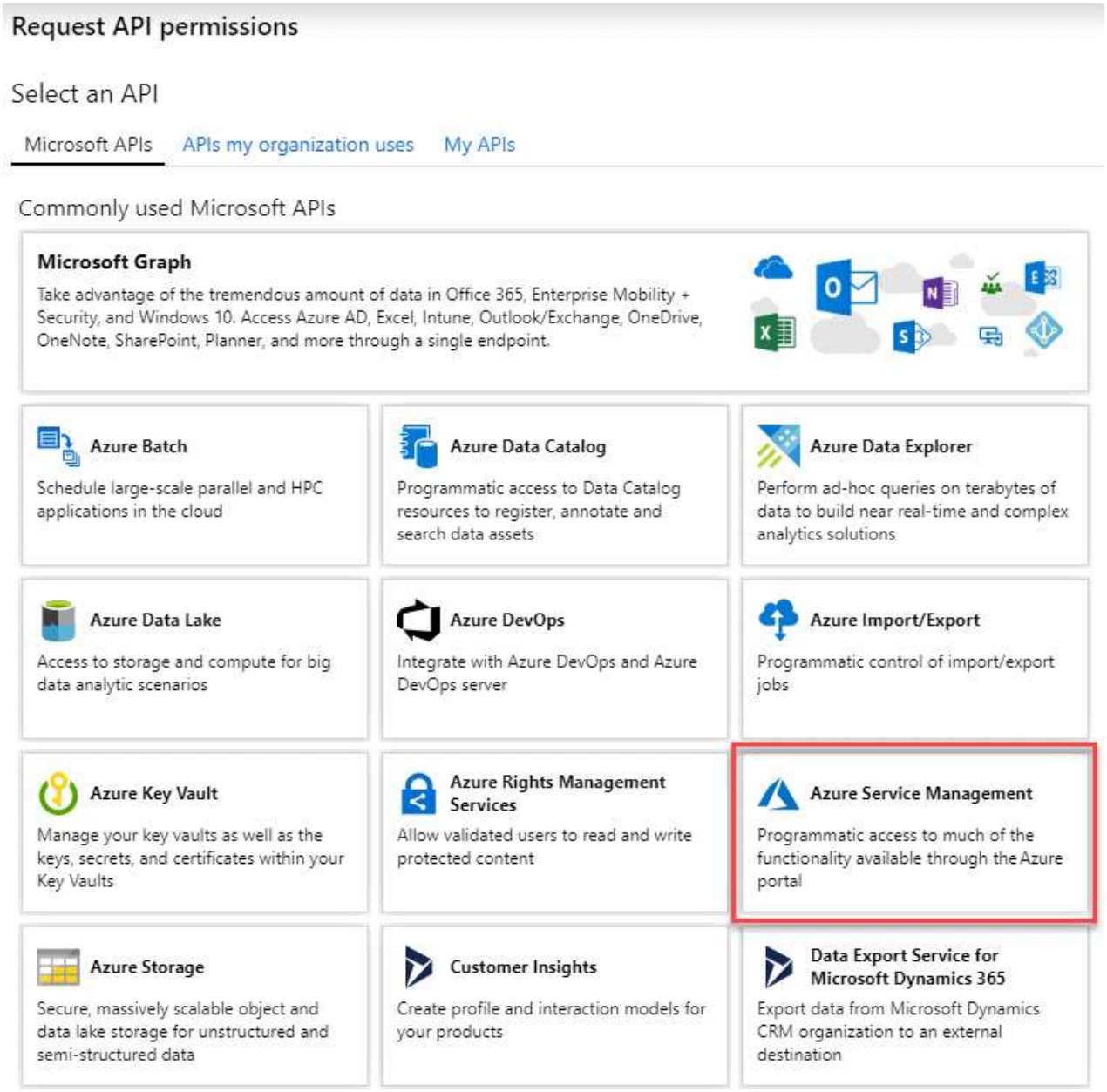
これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

複数の Azure サブスクリプションからCloud Volumes ONTAPをデプロイする場合は、サービス プリンシパルを各サブスクリプションにバインドする必要があります。 NetApp Consoleでは、 Cloud Volumes ONTAP をデプロイするときに使用するサブスクリプションを選択できます。

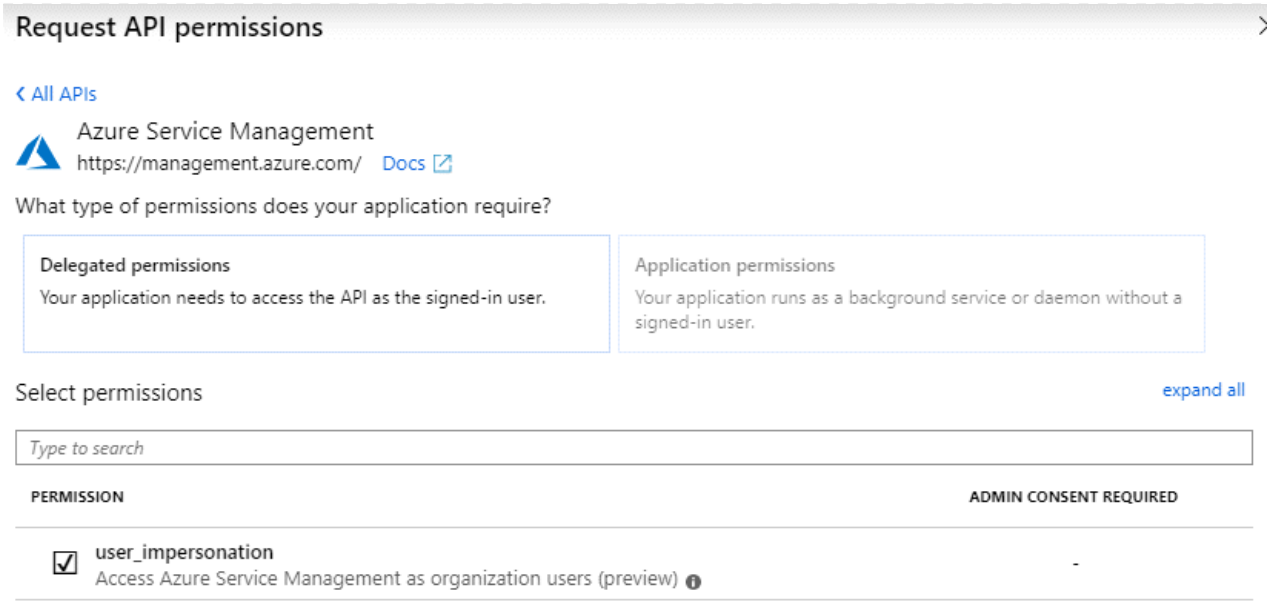
Windows Azure サービス管理 **API** 権限を追加する

1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. **API** 権限 **>** 権限の追加 を選択します。

3. **Microsoft API** の下で、**Azure Service Management** を選択します。

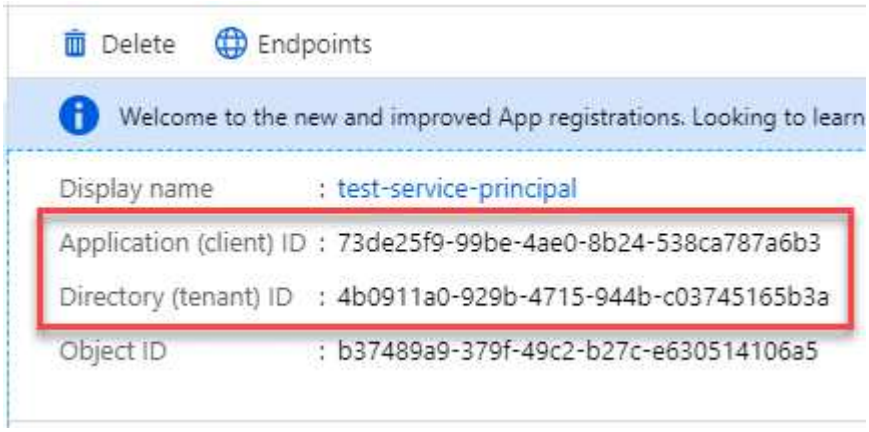


4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。



アプリケーションのアプリケーション**ID**とディレクトリ**ID**を取得します

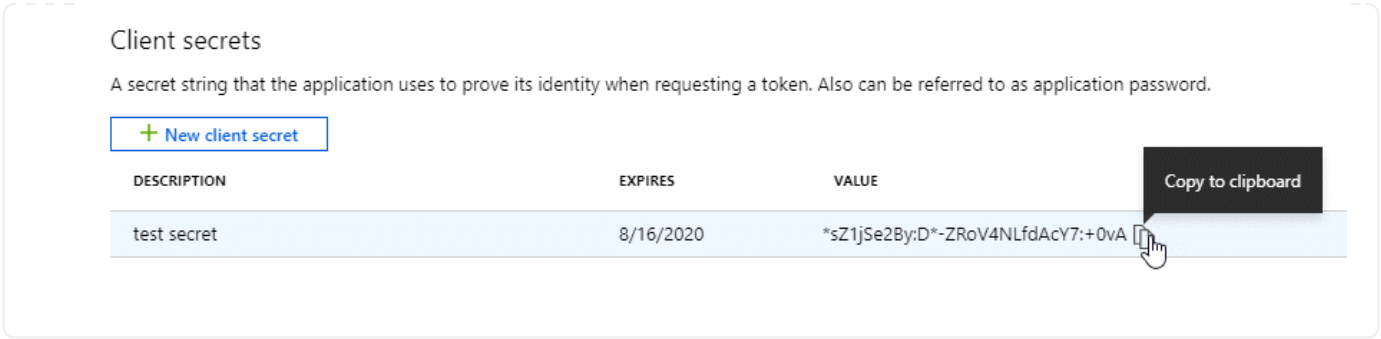
1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. アプリケーション **(**クライアント**) ID** と ディレクトリ **(**テナント**) ID** をコピーします。



Azure アカウントをコンソールに追加するときは、アプリケーションのアプリケーション (クライアント) ID とディレクトリ (テナント) ID を指定する必要があります。コンソールは ID を使用してプログラムでサインインします。

クライアントシークレットを作成する

1. **Microsoft Entra ID** サービスを開きます。
2. *アプリ登録*を選択し、アプリケーションを選択します。
3. *証明書とシークレット > 新しいクライアント シークレット*を選択します。
4. シークレットの説明と期間を指定します。
5. *追加*を選択します。
6. クライアント シークレットの値をコピーします。



VCenter環境にコンソールエージェントをインストールする

NetApp は、VCenter 環境へのコンソール エージェントのインストールをサポートしています。 OVA ファイルには、VMware 環境に展開できる事前構成済みの VM イメージが含まれています。ファイルのダウンロードまたは URL の展開は、 NetApp Consoleから直接行えます。コンソール エージェント ソフトウェアと自己署名証明書が含まれています。

OVAをダウンロードするか**URL**をコピーしてください

OVA をダウンロードするか、 NetApp Consoleから OVA URL を直接コピーします。

1. *管理 > エージェント*を選択します。
2. *概要*ページで、*エージェントのデプロイ > オンプレミス*を選択します。
3. *OVA付き*を選択してください。
4. OVA をダウンロードするか、VCenter で使用する URL をコピーするかを選択します。

VCenterにエージェントを展開する

エージェントを展開するには、VCenter 環境にログインします。

手順

1. 環境で必要な場合は、自己署名証明書を信頼できる証明書にアップロードします。インストール後にこの証明書を置き換えます。"自己署名証明書を置き換える方法を学びます。"
2. コンテンツ ライブラリまたはローカル システムから OVA を展開します。

ローカルシステムから	コンテンツライブラリから
a. 右クリックして、[OVF テンプレートのデプロイ…] を選択します。b. URL から OVA ファイルを選択するか、その場所を参照して、[次へ] を選択します。	a. コンテンツライブラリに移動し、コンソールエージェントOVAを選択します。b. アクション > *このテンプレートから新しいVM*を選択します。

3. OVF テンプレートのデプロイ ウィザードを完了して、コンソール エージェントをデプロイします。
4. VM の名前とフォルダーを選択し、[次へ] を選択します。
5. コンピューティング リソースを選択し、[次へ] を選択します。
6. テンプレートの詳細を確認し、[次へ] を選択します。
7. ライセンス契約に同意し、[次へ] を選択します。

8. 使用するプロキシ構成のタイプ（明示的プロキシ、透過プロキシ、またはプロキシなし）を選択します。
9. VM を展開するデータストアを選択し、[次へ] を選択します。ホストの要件を満たしていることを確認してください。
10. VM を接続するネットワークを選択し、[次へ] を選択します。ネットワークが IPv4 であり、必要なエンドポイントへのアウトバウンド インターネット アクセスできることを確認します。
11. *テンプレートのカスタマイズ*ウィンドウで、次のフィールドに入力します。
    - プロキシ情報
      - 明示的なプロキシを選択した場合は、プロキシ サーバーのホスト名または IP アドレスとポート番号、およびユーザー名とパスワードを入力します。
      - 透過プロキシを選択した場合は、それぞれの証明書をアップロードします。
    - 仮想マシンの構成
      - 構成チェックをスキップ: このチェックボックスはデフォルトでオフになっており、エージェントはネットワーク アクセスを検証するために構成チェックを実行します。
        - NetApp、インストールにエージェントの構成チェックが含まれるように、このボックスをオフのままにしておくことを推奨しています。構成チェックでは、エージェントが必要なエンドポイントへのネットワーク アクセス権を持っているかどうかを検証します。接続の問題によりデプロイメントが失敗した場合は、エージェント ホストから検証レポートとログにアクセスできます。場合によっては、エージェントがネットワークにアクセスできることが確実な場合は、チェックをスキップすることもできます。例えば、まだ"以前のエンドポイント"エージェントのアップグレードに使用すると、検証が失敗し、エラーが発生します。これを回避するには、検証チェックなしでインストールするためのチェックボックスをオンにします。"エンドポイントリストを更新する方法を学ぶ" 。
      - メンテナンスパスワード: `maint`エージェントメンテナンスコンソールへのアクセスを許可するユーザー。
      - **NTP** サーバー: 時刻同期用の 1 つ以上の NTP サーバーを指定します。
      - ホスト名: この VM のホスト名を設定します。検索ドメインを含めることはできません。たとえば、console10.searchdomain.company.com の FQDN は console10 と入力する必要があります。
      - プライマリ **DNS**: 名前解決に使用するプライマリ DNS サーバーを指定します。
      - セカンダリ **DNS**: 名前解決に使用するセカンダリ DNS サーバーを指定します。
      - 検索ドメイン: ホスト名を解決するときに使用する検索ドメイン名を指定します。たとえば、FQDN が console10.searchdomain.company.com の場合は、searchdomain.company.com と入力します。
      - **IPv4** アドレス: ホスト名にマッピングされる IP アドレス。
      - **IPv4** サブネット マスク: IPv4 アドレスのサブネット マスク。
      - **IPv4** ゲートウェイ アドレス: IPv4 アドレスのゲートウェイ アドレス。
12. *次へ*を選択します。
13. *完了準備完了*ウィンドウで詳細を確認し、*完了*を選択します。

    vSphere タスク バーには、コンソール エージェントの展開の進行状況が表示されます。
14. VMの電源をオンにします。

デプロイメントが失敗した場合は、エージェント ホストから検証レポートとログにアクセスできます。"インストールの問題をトラブルシューティングする方法を学びます。"

NetApp Consoleにコンソールエージェントを登録する

コンソールにログインし、コンソール エージェントを組織に関連付けます。ログイン方法は、コンソールを使用しているモードによって異なります。コンソールを標準モードで使用している場合は、SaaS Web サイトからログインします。コンソールを制限モードまたはプライベート モードで使用している場合は、コンソール エージェント ホストからローカルにログインします。

手順

1. Web ブラウザを開き、コンソール エージェント ホストの URL を入力します。

   コンソール ホスト URL は、ホストの構成に応じて、ローカルホスト、プライベート IP アドレス、またはパブリック IP アドレスになります。たとえば、コンソール エージェントがパブリック IP アドレスのないパブリック クラウドにある場合は、コンソール エージェント ホストに接続しているホストのプライベート IP アドレスを入力する必要があります。

2. サインアップまたはログインしてください。
3. ログイン後、コンソールを設定します。
   a. コンソール エージェントに関連付けるコンソール組織を指定します。
   b. システムの名前を入力します。
   c. 安全な環境で実行していますか**?** の下で、制限モードを無効のままにします。

      コンソール エージェントがオンプレミスにインストールされている場合、制限モードはサポートされません。

   d. *始めましょう*を選択します。

コンソールにクラウドプロバイダーの資格情報を追加する

コンソール エージェントをインストールしてセットアップしたら、コンソール エージェントが AWS または Azure でアクションを実行するために必要な権限を持つように、クラウド資格情報を追加します。

AWS

開始する前に

これらの AWS 認証情報を作成したばかりの場合は、使用可能になるまでに数分かかることがあります。資格情報をコンソールに追加する前に、数分待ってください。

手順

1. *管理 > 資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: *Amazon Web Services > エージェントを選択します。
   b. 資格情報の定義: AWS アクセスキーとシークレットキーを入力します。
   c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。
   d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

これで、 "NetApp Console"コンソール エージェントの使用を開始します。

Azure

開始する前に

これらの Azure 資格情報を作成したばかりの場合は、使用可能になるまでに数分かかることがあります。コンソール エージェントに資格情報を追加する前に、数分間お待ちください。

手順

1. *管理 > 資格情報*を選択します。
2. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: **Microsoft Azure >** エージェント を選択します。
   b. 資格情報の定義: 必要な権限を付与する Microsoft Entra サービス プリンシパルに関する情報を入力します。
      - アプリケーション（クライアント）ID
      - ディレクトリ（テナント）ID
      - クライアントシークレット
   c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。
   d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

結果

これで、コンソール エージェントに、ユーザーに代わって Azure でアクションを実行するために必要なアクセス許可が付与されました。これで、 "NetApp Console"コンソール エージェントの使用を開始します。

NetApp Intelligent Services （標準モード）にサブスクライブする

クラウド プロバイダーのマーケットプレイスからNetApp Intelligent Servicesにサブスクライブして、時間単位の料金 (PAYGO) または年間契約でデータ サービスの料金を支払います。 NetAppからライセンスを購入した場合 (BYOL)、マーケットプレイス オファリングにもサブスクライブする必要があります。最初にライセンスに対して課金が行われますが、ライセンス容量を超えた場合、またはライセンスの有効期限が切れた場合は、時間単位で課金されます。

マーケットプレイス サブスクリプションにより、次のNetAppデータ サービスに対する課金が可能になります。

- NetApp Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

NetApp Data Classification はサブスクリプションを通じて有効になりますが、分類の使用には料金はかかりません。

開始する前に

データ サービスをサブスクライブするには、コンソール エージェントをすでに展開しておく必要があります。コンソール エージェントに接続されたクラウド資格情報にマーケットプレイス サブスクリプションを関連付ける必要があります。

AWS

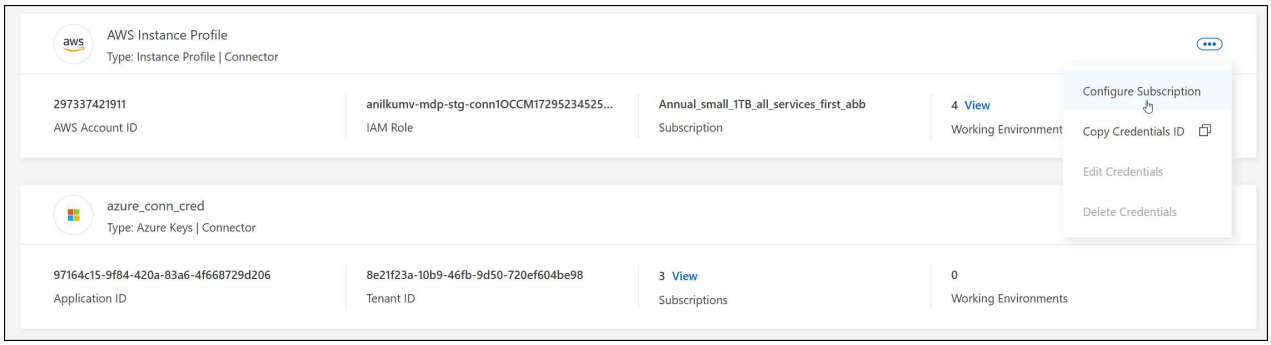
次のビデオは、AWS Marketplace からNetApp Intelligent Servicesをサブスクライブする手順を示しています。

AWS MarketplaceからNetApp Intelligent Servicesをサブスクライブする

手順

1. *管理 > 資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. コンソール エージェントに関連付けられている資格情報のセットのアクション メニューを選択し、[サブスクリプションの構成] を選択します。

   コンソール エージェントに関連付けられている資格情報を選択する必要があります。マーケットプレイス サブスクリプションを、 NetApp Consoleに関連付けられている資格情報に関連付けることはできません。



4. 資格情報を既存のサブスクリプションに関連付けるには、ドロップダウン リストからサブスクリプションを選択し、[構成] を選択します。
5. 認証情報を新しいサブスクリプションに関連付けるには、[サブスクリプションの追加] > [続行] を選択し、AWS Marketplace の手順に従います。

   a. *購入オプションを表示*を選択します。
   b. *購読*を選択します。
   c. *アカウントを設定*を選択します。

      NetApp Consoleにリダイレクトされます。

   d. *サブスクリプションの割り当て*ページから:

      - このサブスクリプションを関連付けるコンソール組織またはアカウントを選択します。
      - 既存のサブスクリプションを置き換える フィールドで、1 つの組織またはアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        コンソールは、組織またはアカウント内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。

- *保存*を選択します。

Azure

手順

1. *管理 > 資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. コンソール エージェントに関連付けられている資格情報のセットのアクション メニューを選択し、[サブスクリプションの構成] を選択します。

   コンソール エージェントに関連付けられている資格情報を選択する必要があります。マーケットプレイス サブスクリプションを、 NetApp Consoleに関連付けられている資格情報に関連付けることはできません。

4. 資格情報を既存のサブスクリプションに関連付けるには、ドロップダウン リストからサブスクリプションを選択し、[構成] を選択します。
5. 資格情報を新しいサブスクリプションに関連付けるには、[サブスクリプションの追加] > [続行] を選択し、Azure Marketplace の手順に従います。

   a. プロンプトが表示されたら、Azure アカウントにログインします。
   b. *購読*を選択します。
   c. フォームに記入し、「購読」を選択します。
   d. サブスクリプションプロセスが完了したら、「今すぐアカウントを構成」を選択します。

      NetApp Consoleにリダイレクトされます。

   e. *サブスクリプションの割り当て*ページから:

      - このサブスクリプションを関連付けるコンソール組織またはアカウントを選択します。
      - 既存のサブスクリプションを置き換える フィールドで、1 つの組織またはアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        コンソールは、組織またはアカウント内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

   他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。

      - *保存*を選択します。

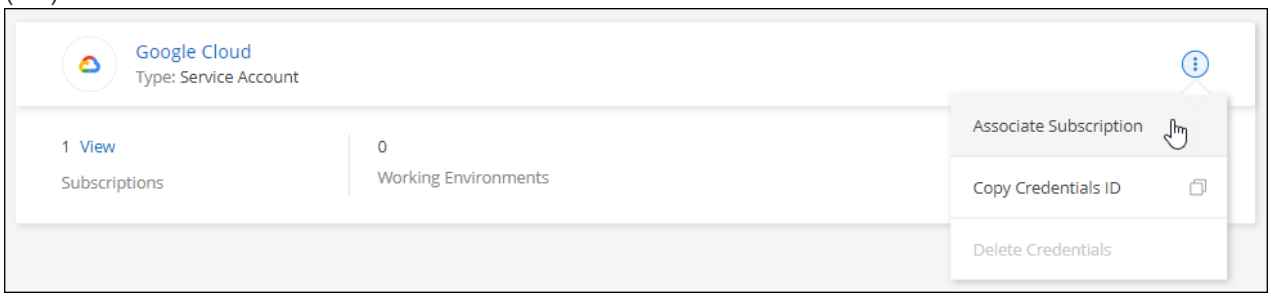
        次のビデオでは、Azure Marketplace からサブスクライブする手順を示します。

Azure Marketplace からNetApp Intelligent Servicesをサブスクライブする

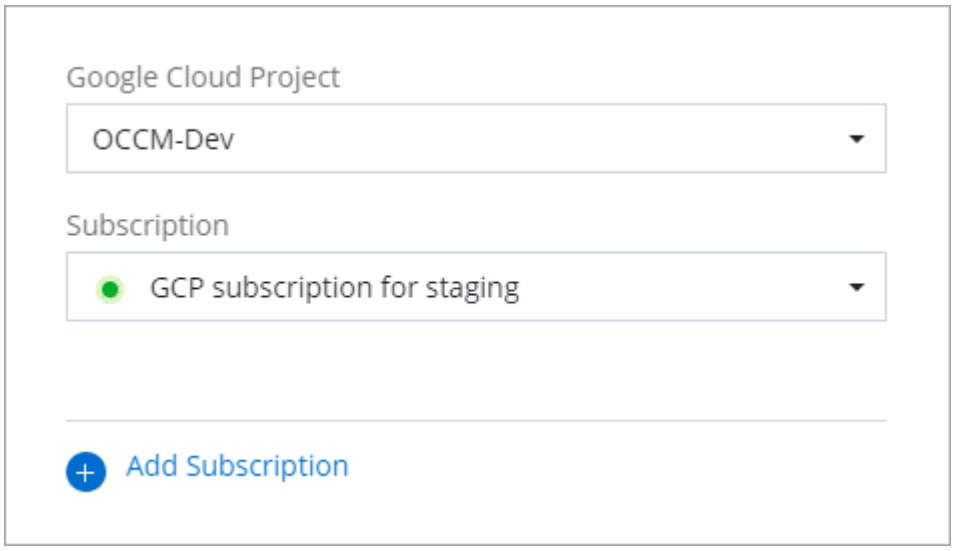
Google Cloud

手順

1. *管理 > *資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. コンソール エージェントに関連付けられている資格情報のセットのアクション メニューを選択し、[サブスクリプションの構成] を選択します。 +新しいスクリーンショットが必要です (TS)



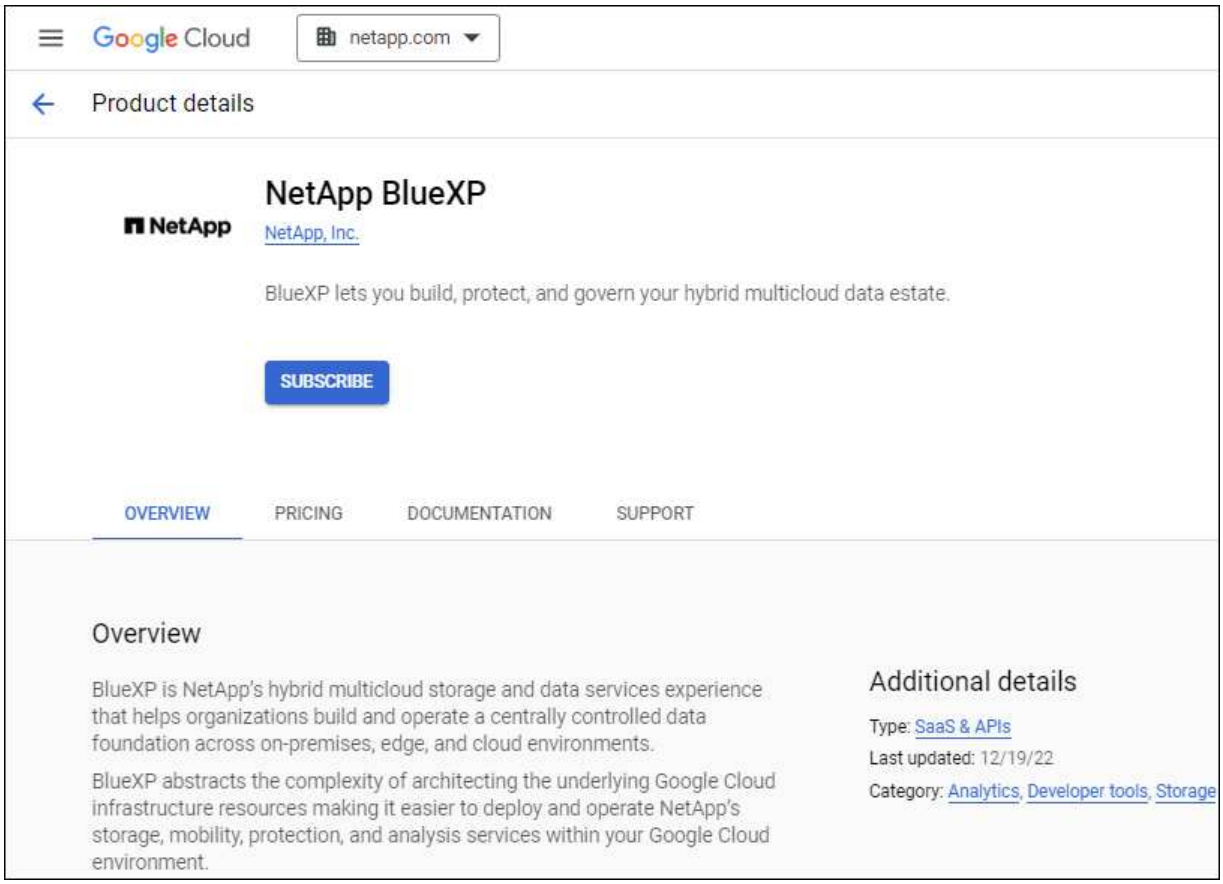
4. 選択した認証情報を使用して既存のサブスクリプションを構成するには、ドロップダウン リストから Google Cloud プロジェクトとサブスクリプションを選択し、[構成] を選択します。



5. まだサブスクリプションをお持ちでない場合は、[サブスクリプションを追加] > [続行] を選択し、Google Cloud Marketplace の手順に従います。

次の手順を完了する前に、Google Cloud アカウントの課金管理者権限とNetApp Consoleのログイン権限の両方があることを確認してください。

a. リダイレクトされたら "Google Cloud Marketplace のNetApp Intelligent Servicesページ"上部のナビゲーション メニューで正しいプロジェクトが選択されていることを確認します。



b. *購読*を選択します。

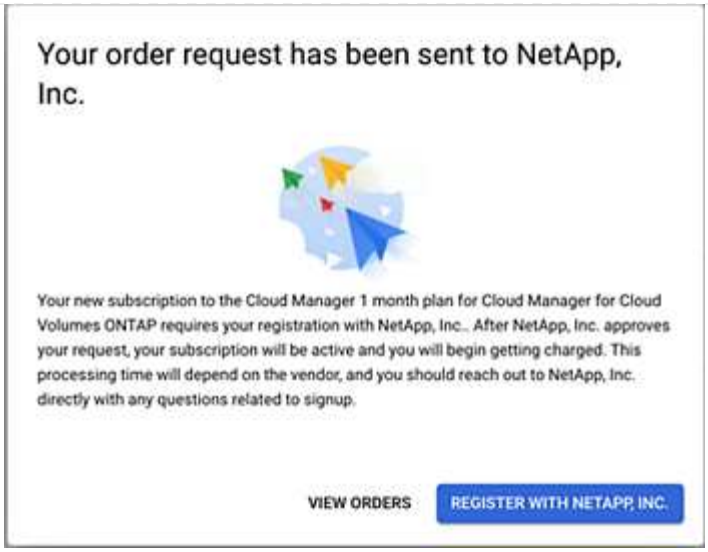
c. 適切な請求先アカウントを選択し、利用規約に同意します。

d. *購読*を選択します。

この手順により、転送リクエストがNetAppに送信されます。

e. ポップアップダイアログボックスで、* NetApp, Inc.に登録*を選択します。

Google Cloud サブスクリプションをコンソールの組織またはアカウントにリンクするには、この手順を完了する必要があります。このページからリダイレクトされ、コンソールにサインインするまで、サブスクリプションをリンクするプロセスは完了しません。



f. サブスクリプションの割り当て ページの手順を完了します。

> 組織内の誰かが既に請求先アカウントからマーケットプレイスサブスクリプションを利用している場合は、次のページにリダイレクトされます。 "NetApp Console内のCloud Volumes ONTAPページ"その代わり。予期しない事態が発生した場合は、 NetAppの営業チームにお問い合わせください。 Google では、Google 請求先アカウントごとに 1 つのサブスクリプションのみ有効になります。

- このサブスクリプションを関連付けるコンソール組織またはアカウントを選択します。
- 既存のサブスクリプションを置き換える フィールドで、1 つの組織またはアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

  コンソールは、組織またはアカウント内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

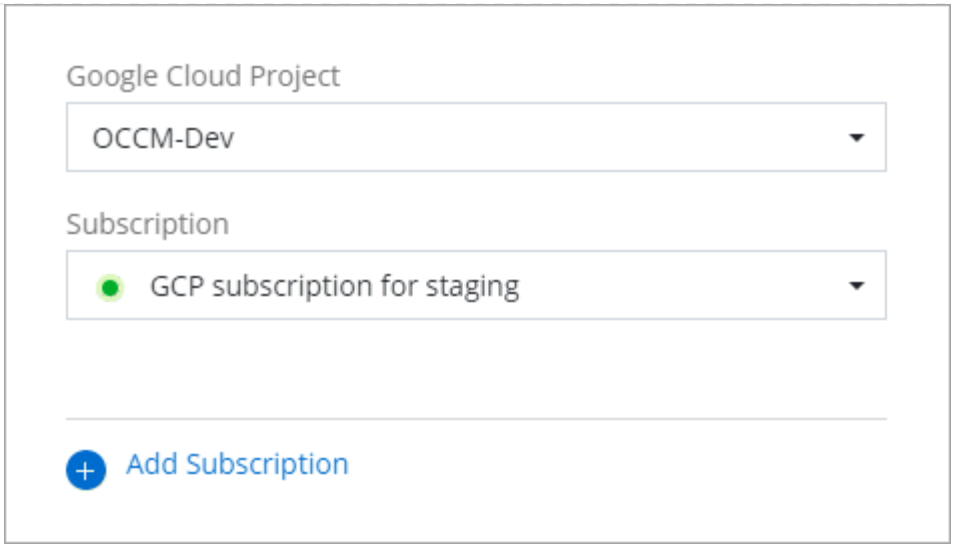
他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。

- *保存*を選択します。

  次のビデオでは、Google Cloud Marketplace からサブスクライブする手順を示します。

Google Cloud Marketplace から登録する

a. このプロセスが完了したら、コンソールの [資格情報] ページに戻り、この新しいサブスクリプションを選択します。



関連情報

- "Cloud Volumes ONTAPのBYOL容量ベースライセンスを管理する"
- "データサービスのBYOLライセンスを管理する"
- "AWS の認証情報とサブスクリプションを管理する"
- "Azure の資格情報とサブスクリプションを管理する"
- "Google Cloud の認証情報とサブスクリプションを管理する"

次にできること（標準モード）

NetApp Consoleを標準モードでログインしてセットアップしたので、ユーザーはストレージ システムを作成および検出し、 NetAppデータ サービスを使用できるようになります。

AWS、Microsoft Azure、または Google Cloud にコンソール エージェントをインストールした場合、コンソールは、エージェントがインストールされている場所にある Amazon S3 バケット、Azure Blob ストレージ、または Google Cloud Storage バケットに関する情報を自動的に検出します。これらのシステムは自動的に システム ページに追加されます。

ヘルプが必要な場合は、 "NetApp Consoleドキュメントのホームページ" NetApp Consoleのドキュメントを表示します。

関連情報

"NetApp Consoleの展開モード"

制限モードを始める

開始ワークフロー（制限モード）

環境を準備し、コンソール エージェントを展開して、制限モードでNetApp Consoleの使

用を開始します。

制限モードは通常、AWS GovCloud および Azure Government リージョンでの展開を含む、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。始める前に、以下の点を理解しておいてください。"コンソールエージェント"そして"展開モード"。

1 "展開の準備"

1. CPU、RAM、ディスク容量、コンテナ オーケストレーション ツールなどの要件を満たす専用の Linux ホストを準備します。
2. ターゲット ネットワークへのアクセス、手動インストール用のアウトバウンド インターネット アクセス、および日常的なアクセス用のアウトバウンド インターネットを提供するネットワークをセットアップします。
3. クラウド プロバイダーで権限を設定し、展開後にそれらの権限をコンソール エージェント インスタンスに関連付けることができるようにします。

2 "コンソールエージェントを展開する"

1. クラウド プロバイダーのマーケットプレイスからコンソール エージェントをインストールするか、独自の Linux ホストにソフトウェアを手動でインストールします。
2. Web ブラウザを開き、Linux ホストの IP アドレスを入力して、 NetApp Consoleを設定します。
3. 以前に設定した権限をコンソール エージェントに提供します。

3 "NetApp Intelligent Servicesに加入する（オプション）"

オプション: クラウド プロバイダーのマーケットプレイスからNetApp Intelligent Servicesにサブスクライブして、時間単位の料金 (PAYGO) または年間契約でデータ サービスの料金を支払います。 NetApp Intelligent Servicesには、 NetApp Backup and Recovery、 Cloud Volumes ONTAP、 NetApp Cloud Tiering、 NetApp Ransomware Resilience 、 NetApp Disaster Recovery が含まれます。 NetApp Data Classification は追加料金なしでサブスクリプションに含まれています。

制限モードでの展開の準備

NetApp Consoleを制限モードで展開する前に、環境を準備します。ホストの要件を確認し、ネットワークを準備し、権限を設定するなどする必要があります。

ステップ**1:** 制限モードの仕組みを理解する

開始する前に、 NetApp Consoleが制限モードでどのように動作するかを理解してください。

インストールされたNetApp Consoleエージェントからローカルで利用できるブラウザベースのインターフェイスを使用します。 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NetApp Consoleにアクセスすることはできません。

また、すべてのコンソール機能とNetAppデータ サービスが利用できるわけではありません。

"制限モードの仕組みを学ぶ" 。

ステップ**2:** インストールオプションを確認する

制限モードでは、コンソール エージェントをクラウドにのみインストールできます。次のインストール オプションが利用可能です。

- AWSマーケットプレイスから
- Azure Marketplaceから
- AWS、Azure、または Google Cloud で実行されている独自の Linux ホストにコンソール エージェントを手動でインストールする

ステップ**3:** ホストの要件を確認する

コンソール エージェントを実行するには、ホストが特定の OS、RAM、およびポートの要件を満たしている必要があります。

AWS または Azure Marketplace からコンソールエージェントをデプロイする場合、イメージには必要な OS およびソフトウェア コンポーネントが含まれます。 CPU と RAM の要件を満たすインスタンス タイプを選択するだけです。

専用ホスト

コンソール エージェントは、他のアプリケーションと共有されているホストではサポートされません。ホストは専用ホストである必要があります。ホストは、次のサイズ要件を満たす任意のアーキテクチャにすることができます。

- CPU: 8コアまたは8vCPU
- メモリ: 32 GB
- ディスク容量: ホストには 165 GB が推奨され、パーティション要件は次のとおりです。
  - `/opt`: 120 GiBの空き容量が必要です

    エージェントは `/opt`インストールするには `/opt/application/netapp`ディレクトリとその内容。
  - `/var`: 40 GiBの空き容量が必要です

    コンソールエージェントにはこのスペースが必要です `/var`Docker または Podman は、このディレクトリ内にコンテナを作成するように設計されているためです。具体的には、`/var/lib/containers/storage`ディレクトリ。このスペースでは外部マウントまたはシンボリックリンクは機能しません。

ハイパーバイザー

サポートされているオペレーティング システムを実行することが認定されているベア メタルまたはホスト型ハイパーバイザーが必要です。

オペレーティングシステムとコンテナの要件

コンソールを標準モードまたは制限モードで使用する場合、コンソール エージェントは次のオペレーティング システムでサポートされます。エージェントをインストールする前に、コンテナ オーケストレーション ツールが必要です。

オペレーティングシステム	サポートされるOSバージョン	サポートされているエージェントのバージョン	必要なコンテナツール	SELinux は
Red Hat Enterprise Linux	9.1～9.4 8.6～8.10 • 英語版のみ。 • ホストは Red Hat Subscription Management に登録されている必要があります。登録されていない場合、ホストはエージェントのインストール中に必要なサードパーティ製ソフトウェアを更新するためにリポジトリにアクセスできません。	3.9.50 以降、コンソールが標準モードまたは制限モード	Podman バージョン 4.6.1 または 4.9.4 Podman の構成要件を表示する 。	強制モードまたは許可モードでサポートされます • Cloud Volumes ONTAPシステムの管理は、オペレーティングシステムで SELinux が有効になっているエージェントではサポートされません。
Ubuntu	24.04 LTS	3.9.45 以降、NetApp Consoleが標準モードまたは制限モード	Docker エンジン 23.06 から 28.0.0。	サポート対象外

AWS EC2インスタンスタイプ

上記の CPU および RAM の要件を満たすインスタンス タイプ。 t3.2xlarge をお勧めします。

Azure VM サイズ

上記の CPU および RAM の要件を満たすインスタンス タイプ。 Standard_D8s_v3 をお勧めします。

Google Cloud マシンタイプ

上記の CPU および RAM の要件を満たすインスタンス タイプ。 n2-standard-8 をお勧めします。

コンソールエージェントは、Google Cloud の VM インスタンスで、以下の OS がサポートする環境でサポートされます。 "シールドされたVMの機能"

/optのディスク容量

100 GiBの空き容量が必要です

エージェントは `/opt`インストールするには `/opt/application/netapp`ディレクトリとその内容。

/varのディスク容量

20 GiBの空き容量が必要です

コンソールエージェントにはこのスペースが必要です `/var`Docker または Podman は、このディレクトリ内にコンテナを作成するように設計されているためです。具体的には、 `/var/lib/containers/storage`ディレクトリ。このスペースでは外部マウントまたはシンボリックリンクは機能しません。

ステップ**4: Podman**または**Docker Engine**をインストールする

コンソール エージェントを手動でインストールするには、Podman または Docker Engine をインストールしてホストを準備します。

オペレーティング システムに応じて、エージェントをインストールする前に Podman または Docker Engine のいずれかが必要になります。

- Red Hat Enterprise Linux 8 および 9 には Podman が必要です。

  サポートされているPodmanのバージョンを表示する 。

- Ubuntu には Docker Engine が必要です。

  サポートされている Docker エンジンのバージョンを表示する 。

例 **5.** 手順

ポッドマン

Podman をインストールして設定するには、次の手順に従います。

- podman.socket サービスを有効にして起動します
- Python3をインストールする
- podman-compose パッケージ バージョン 1.0.6 をインストールします。
- podman-composeをPATH環境変数に追加する
- Red Hat Enterprise Linux を使用している場合は、Podman バージョンが CNI ではなく Netavark Aardvark DNS を使用していることを確認してください。

DNS ポートの競合を避けるために、エージェントをインストールした後、aardvark-dns ポート (デフォルト: 53) を調整します。指示に従ってポートを構成します。

手順

1. ホストに podman-docker パッケージがインストールされている場合は削除します。

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Podman をインストールします。

   Podman は、公式の Red Hat Enterprise Linux リポジトリから入手できます。

   Red Hat Enterprise Linux 9 の場合:

```
sudo dnf install podman-2:<version>
```

   <version> は、インストールする Podman のサポートされているバージョンです。サポートされているPodmanのバージョンを表示する 。

   Red Hat Enterprise Linux 8 の場合:

```
sudo dnf install podman-3:<version>
```

   <version> は、インストールする Podman のサポートされているバージョンです。サポートされているPodmanのバージョンを表示する 。

3. podman.socket サービスを有効にして起動します。

```
sudo systemctl enable --now podman.socket
```

4. python3 をインストールします。

```
sudo dnf install python3
```

5. システムにまだインストールされていない場合は、EPEL リポジトリ パッケージをインストールします。
6. Red Hat Enterprise を使用している場合:

   podman-compose は、Extra Packages for Enterprise Linux (EPEL) リポジトリから入手できるため、この手順は必須です。

   Red Hat Enterprise Linux 9 の場合:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   Red Hat Enterprise Linux 8 の場合:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

7. podman-compose パッケージ 1.0.6 をインストールします。

```
sudo dnf install podman-compose-1.0.6
```

   使用して `dnf install`コマンドは、PATH 環境変数に podman-compose を追加するための要件を満たしています。インストールコマンドは、すでにインストールされているpodman-composeを/usr/binに追加します。 `secure_path`ホスト上のオプション。

8. Red Hat Enterprise Linux 8 を使用している場合は、Podman バージョンが CNI ではなく Aardvark DNS を備えた NetAvark を使用していることを確認します。

   a. 次のコマンドを実行して、networkBackend が CNI に設定されているかどうかを確認します。

```
podman info | grep networkBackend
```

   b. networkBackendが `CNI`、それを変更する必要があります `netavark`。

   c. インストール `netavark`そして `aardvark-dns`次のコマンドを使用します。

```
dnf install aardvark-dns netavark
```

d. 開く `/etc/containers/containers.conf`ファイルを編集し、network_backend オプションを変更して、「cni」の代わりに「netavark」を使用します。

もし `/etc/containers/containers.conf`存在しない場合は、設定を変更してください `/usr/share/containers/containers.conf`。

9. podman を再起動します。

```
systemctl restart podman
```

10. 次のコマンドを使用して、networkBackend が「netavark」に変更されていることを確認します。

```
podman info | grep networkBackend
```

Dockerエンジン

Docker のドキュメントに従って Docker Engine をインストールします。

手順

1. "Dockerからのインストール手順を見る"

   サポートされている Docker エンジン バージョンをインストールするには、手順に従ってください。最新バージョンはコンソールでサポートされていないため、インストールしないでください。

2. Docker が有効になっていて実行されていることを確認します。

```
sudo systemctl enable docker && sudo systemctl start docker
```

ステップ**5:** ネットワークアクセスを準備する

コンソール エージェントがパブリック クラウド内のリソースを管理できるように、ネットワーク アクセスを設定します。コンソール エージェント用の仮想ネットワークとサブネットがあることに加えて、次の要件が満たされていることを確認する必要があります。

ターゲットネットワークへの接続

コンソール エージェントがストレージの場所へのネットワーク接続を持っていることを確認します。たとえば、 Cloud Volumes ONTAPをデプロイする予定の VPC または VNet、またはオンプレミスのONTAPクラスターが存在するデータセンターなどです。

NetApp Consoleへのユーザーアクセスのためのネットワークを準備する

制限モードでは、ユーザーはコンソール エージェント VM からコンソールにアクセスします。コンソール エージェントは、データ管理タスクを完了するためにいくつかのエンドポイントに接続します。これらのエンドポイントは、コンソールから特定のアクションを完了するときに、ユーザーのコンピューターから接続されます。

バージョン 4.0.0 より前のコンソール エージェントには追加のエンドポイントが必要です。4.0.0 以降にアップグレードした場合は、許可リストから古いエンドポイントを削除できます。"4.0.0 より前のバージョンに必要なネットワーク アクセスの詳細について説明します。"

+

エンドポイント	目的
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。
https://cdn.auth0.com https://services.cloud.netapp.com	Web ブラウザはこれらのエンドポイントに接続し、NetApp Consoleを通じて集中的なユーザー認証を行います。

日常業務のためのアウトバウンドインターネットアクセス

コンソール エージェントのネットワークの場所には、送信インターネット アクセスが必要です。 NetApp Consoleの SaaS サービスと、それぞれのパブリック クラウド環境内のエンドポイントにアクセスできる必要があります。

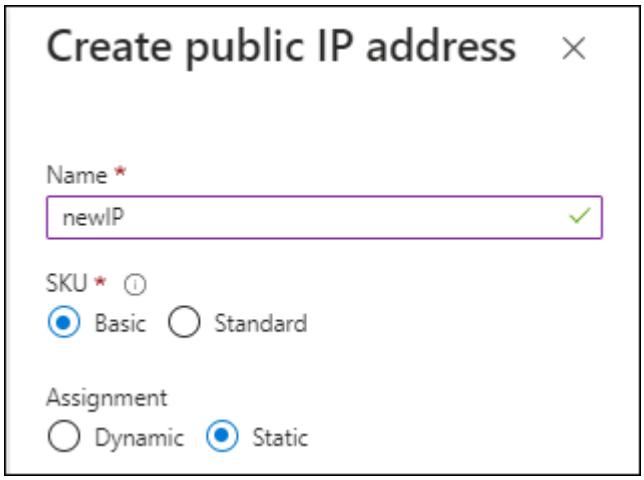
エンドポイント	目的
AWS 環境	AWS サービス (amazonaws.com): • クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理（IAM） • キー管理サービス (KMS) • セキュリティトークンサービス（STS） • シンプルストレージサービス（S3）
AWS リソースを管理します。エンドポイントは AWS リージョンによって異なります。 "詳細についてはAWSドキュメントを参照してください"	**Azure** 環境
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure パブリック リージョン内のリソースを管理します。
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Azure Government リージョン内のリソースを管理します。

エンドポイント	目的
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure China リージョンのリソースを管理します。
Google Cloud 環境	https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects
Google Cloud 内のリソースを管理します。	• NetApp Consoleエンドポイント*
https://mysupport.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信します。
https://signin.b2c.netapp.com	NetAppサポート サイト (NSS) の資格情報を更新したり、 NetApp Consoleに新しい NSS 資格情報を追加したりします。
https://support.netapp.com	ライセンス情報を取得し、AutoSupportメッセージをNetAppサポートに送信し、 Cloud Volumes ONTAPのソフトウェアアップデートを受信します。
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 • 新しいエージェントを展開すると、検証チェックによって現在のエンドポイントへの接続がテストされます。使用する場合"以前のエンドポイント"、検証チェックは失敗します。この失敗を回避するには、検証チェックをスキップします。 以前のエンドポイントも引き続きサポートされますが、NetApp、ファイアウォール ルールをできるだけ早く現在のエンドポイントに更新することをお勧めします。"エンドポイントリストを更新する方法を学ぶ" 。 • ファイアウォールの現在のエンドポイントに更新すると、既存のエージェントは引き続き動作します。

Azureのパブリック**IP**アドレス

Azure のコンソール エージェント VM でパブリック IP アドレスを使用する場合は、コンソールがこのパブリック IP アドレスを使用するように、IP アドレスで Basic SKU を使用する必要があります。



代わりに標準 SKU IP アドレスを使用する場合、コンソールはパブリック IP ではなく、コンソール エージェントのプライベート IP アドレスを使用します。コンソールにアクセスするために使用しているマシンがそのプライベート IP アドレスにアクセスできない場合、コンソールからのアクションは失敗します。

"Azure ドキュメント: パブリック IP SKU"

プロキシ サーバ

NetApp は明示的プロキシ構成と透過的プロキシ構成の両方をサポートしています。透過プロキシを使用している場合は、プロキシ サーバーの証明書のみを提供する必要があります。明示的なプロキシを使用している場合は、IP アドレスと資格情報も必要になります。

- IPアドレス
- Credentials
- HTTPS証明書

ポート

ユーザーが開始した場合、またはCloud Volumes ONTAPからNetAppサポートにAutoSupportメッセージを送信するためのプロキシとして使用された場合を除いて、コンソール エージェントへの着信トラフィックはありません。

- HTTP (80) と HTTPS (443) は、まれにしか使用されないローカル UI へのアクセスを提供します。
- SSH（22）は、トラブルシューティングのためにホストに接続する必要がある場合にのみ必要です。
- アウトバウンド インターネット接続が利用できないサブネットにCloud Volumes ONTAPシステムを展開する場合は、ポート 3128 経由のインバウンド接続が必要です。

  Cloud Volumes ONTAPシステムにAutoSupportメッセージを送信するためのアウトバウンド インターネット接続がない場合、コンソールは、コンソール エージェントに含まれているプロキシ サーバーを使用するようにそれらのシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

NTP を有効にする

NetApp Data Classificationを使用して企業のデータ ソースをスキャンする予定の場合は、システム間で時刻が同期されるように、コンソール エージェントとNetApp Data Classificationシステムの両方で Network Time Protocol (NTP) サービスを有効にする必要があります。 "NetAppデータ分類の詳細"

クラウド プロバイダーのマーケットプレイスからコンソール エージェントを作成する予定の場合は、コンソール エージェントを作成した後にこのネットワーク要件を実装します。

ステップ**6:** クラウド権限を準備する

コンソール エージェントには、仮想ネットワークにCloud Volumes ONTAPを展開し、 NetAppデータ サービスを使用するために、クラウド プロバイダーからの権限が必要です。クラウド プロバイダーで権限を設定し、それらの権限をコンソール エージェントに関連付ける必要があります。

必要な手順を表示するには、クラウド プロバイダーで使用する認証オプションを選択します。

AWS IAM ロール

IAM ロールを使用して、コンソール エージェントに権限を付与します。

AWS Marketplace からコンソールエージェントを作成している場合は、EC2 インスタンスを起動するときにその IAM ロールを選択するように求められます。

独自の Linux ホストにコンソールエージェントを手動でインストールする場合は、ロールを EC2 インスタンスにアタッチします。

手順

1. AWS コンソールにログインし、IAM サービスに移動します。
2. ポリシーを作成します。
   a. *ポリシー > ポリシーの作成*を選択します。
   b. *JSON*を選択し、その内容をコピーして貼り付けます。"コンソールエージェントのIAMポリシー" 。
   c. 残りの手順を完了してポリシーを作成します。
3. IAM ロールを作成します。
   a. *[ロール] > [ロールの作成]*を選択します。
   b. **AWS** サービス **> EC2** を選択します。
   c. 作成したポリシーを添付して権限を追加します。
   d. 残りの手順を完了してロールを作成します。

結果

これで、コンソール エージェント EC2 インスタンスの IAM ロールが作成されました。

AWS アクセスキー

IAM ユーザーの権限とアクセスキーを設定します。コンソールエージェントをインストールしてコンソールを設定した後、コンソールに AWS アクセスキーを提供する必要があります。

手順

1. AWS コンソールにログインし、IAM サービスに移動します。
2. ポリシーを作成します。
   a. *ポリシー > ポリシーの作成*を選択します。
   b. *JSON*を選択し、その内容をコピーして貼り付けます。"コンソールエージェントのIAMポリシー" 。
   c. 残りの手順を完了してポリシーを作成します。

      使用する予定のNetAppデータ サービスによっては、2 番目のポリシーを作成する必要がある場合があります。

   標準リージョンの場合、権限は 2 つのポリシーに分散されます。 AWS の管理ポリシーの最大文字サイズ制限により、2 つのポリシーが必要になります。"コンソールエージェントのIAMポリシーの詳細" 。

3. IAM ユーザーにポリシーをアタッチします。
   - "AWSドキュメント: IAMロールの作成"
   - "AWSドキュメント: IAMポリシーの追加と削除"
4. コンソール エージェントをインストールした後、 NetApp Consoleに追加できるアクセス キーがユーザーにあることを確認します。

Azure ロール

必要な権限を持つ Azure カスタム ロールを作成します。このロールをコンソール エージェント VM に割り当てます。

Azure ポータル、Azure PowerShell、Azure CLI、または REST API を使用して、Azure カスタム ロールを作成できます。次の手順は、Azure CLI を使用してロールを作成する方法を示しています。別の方法をご希望の場合は、 "Azureドキュメント"

手順

1. 独自のホストにソフトウェアを手動でインストールする予定の場合は、カスタム ロールを通じて必要な Azure アクセス許可を提供できるように、VM でシステム割り当てマネージド ID を有効にします。

   "Microsoft Azure ドキュメント: Azure ポータルを使用して VM 上の Azure リソースのマネージド ID を構成する"

2. の内容をコピーします"コネクタのカスタムロール権限"JSON ファイルに保存します。
3. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、JSON ファイルを変更します。

   NetApp Consoleで使用する各 Azure サブスクリプションの ID を追加する必要があります。

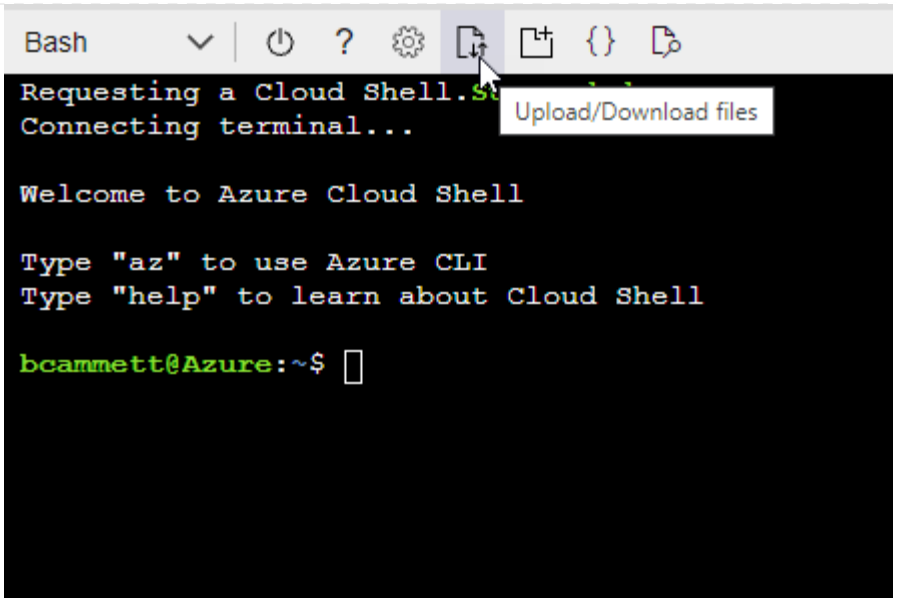
   例

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

4. JSON ファイルを使用して、Azure でカスタム ロールを作成します。

   次の手順では、Azure Cloud Shell で Bash を使用してロールを作成する方法について説明します。

   a. 始める "Azure クラウド シェル"Bash 環境を選択します。
   b. JSON ファイルをアップロードします。



c. Azure CLI を使用してカスタム ロールを作成します。

```
az role definition create --role-definition Connector_Policy.json
```

Azure サービスプリンシパル

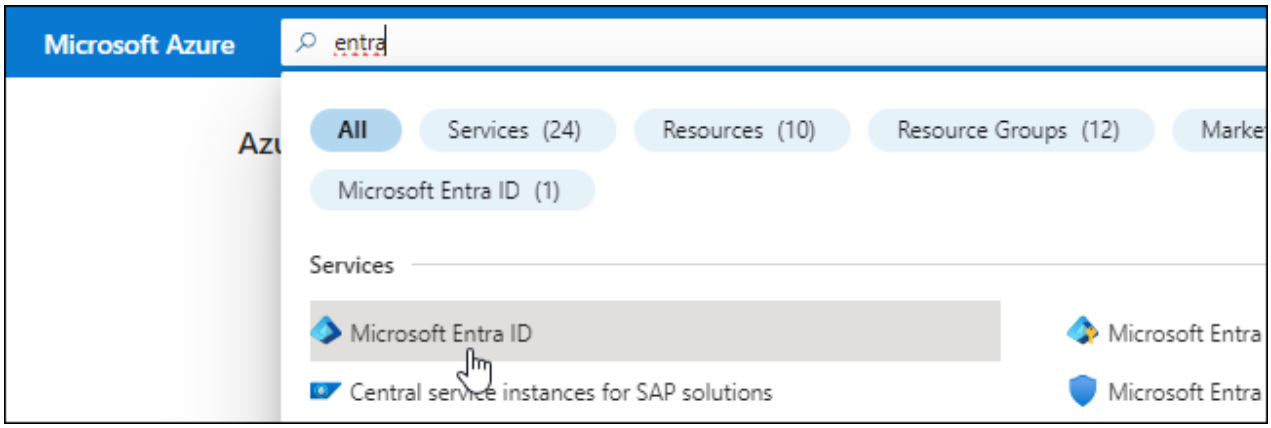
Microsoft Entra ID でサービス プリンシパルを作成して設定し、コンソールに必要な Azure 資格情報を取得します。コンソール エージェントをインストールした後、コンソールにこれらの資格情報を提供する必要があります。

ロールベースのアクセス制御用の **Microsoft Entra** アプリケーションを作成する

1. Azure で Active Directory アプリケーションを作成し、そのアプリケーションをロールに割り当てるためのアクセス許可があることを確認します。

   詳細については、 "Microsoft Azure ドキュメント: 必要な権限"

2. Azure ポータルから、**Microsoft Entra ID** サービスを開きます。



3. メニューで*アプリ登録*を選択します。
4. *新規登録*を選択します。

5. アプリケーションの詳細を指定します。
   - 名前: アプリケーションの名前を入力します。
   - アカウント タイプ: アカウント タイプを選択します (いずれのタイプもNetApp Consoleで使用できます)。
   - リダイレクト **URI**: このフィールドは空白のままにすることができます。
6. *登録*を選択します。

   AD アプリケーションとサービス プリンシパルを作成しました。

アプリケーションをロールに割り当てる

1. カスタム ロールを作成します。

   Azure ポータル、Azure PowerShell、Azure CLI、または REST API を使用して、Azure カスタム ロールを作成できます。次の手順は、Azure CLI を使用してロールを作成する方法を示しています。別の方法をご希望の場合は、 "Azureドキュメント"

   a. の内容をコピーします"コンソールエージェントのカスタムロール権限"JSON ファイルに保存します。
   b. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、JSON ファイルを変更します。

      ユーザーがCloud Volumes ONTAPシステムを作成する各 Azure サブスクリプションの ID を追加する必要があります。

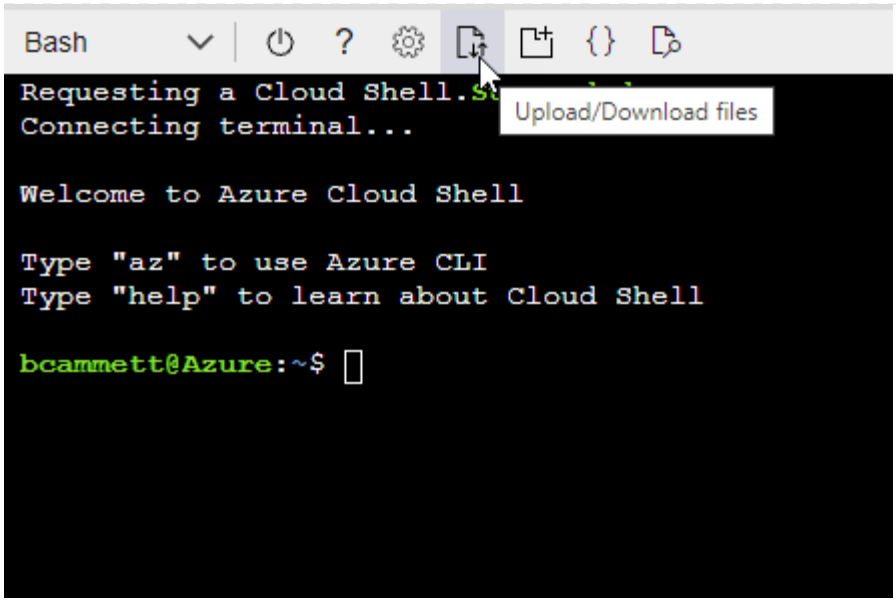
      例

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

   c. JSON ファイルを使用して、Azure でカスタム ロールを作成します。

      次の手順では、Azure Cloud Shell で Bash を使用してロールを作成する方法について説明します。

      - 始める "Azure クラウド シェル"Bash 環境を選択します。
      - JSON ファイルをアップロードします。



- Azure CLI を使用してカスタム ロールを作成します。

```
az role definition create --role-definition
Connector_Policy.json
```

これで、コンソール エージェント仮想マシンに割り当てることができる、コンソール オペレーターと呼ばれるカスタム ロールが作成されます。

2. アプリケーションをロールに割り当てます。

a. Azure ポータルから、サブスクリプション サービスを開きます。

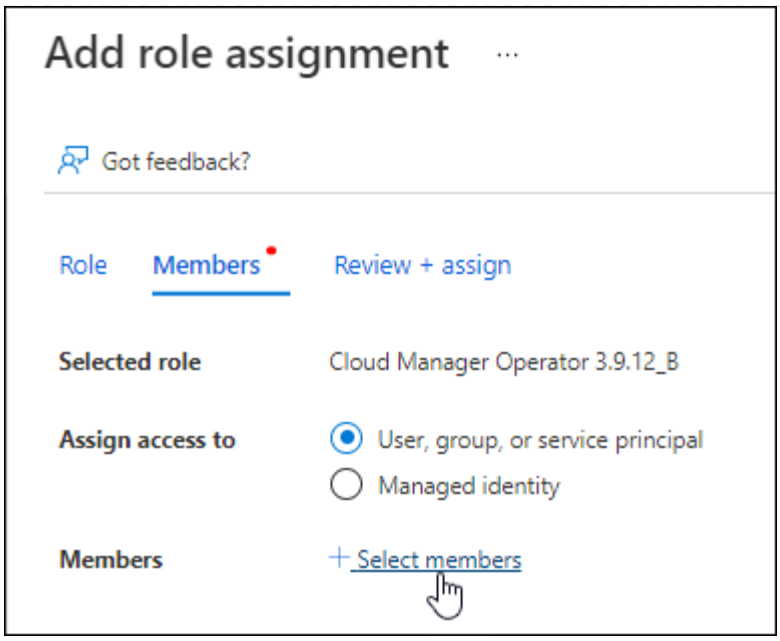
b. サブスクリプションを選択します。

c. アクセス制御 **(IAM) >** 追加 **>** ロール割り当ての追加 を選択します。

d. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。

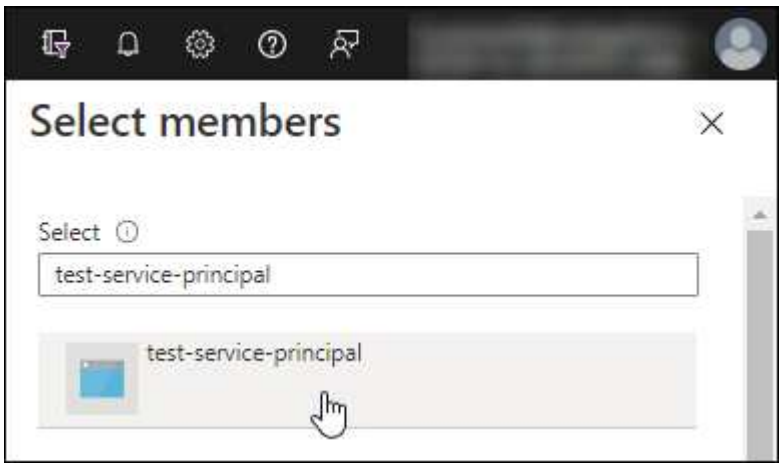
e. *メンバー*タブで、次の手順を実行します。

- *ユーザー、グループ、またはサービス プリンシパル*を選択したままにします。
- *メンバーを選択*を選択します。



- アプリケーションの名前を検索します。

  次に例を示します。



- アプリケーションを選択し、[選択] を選択します。
- *次へ*を選択します。

f. *レビュー + 割り当て*を選択します。

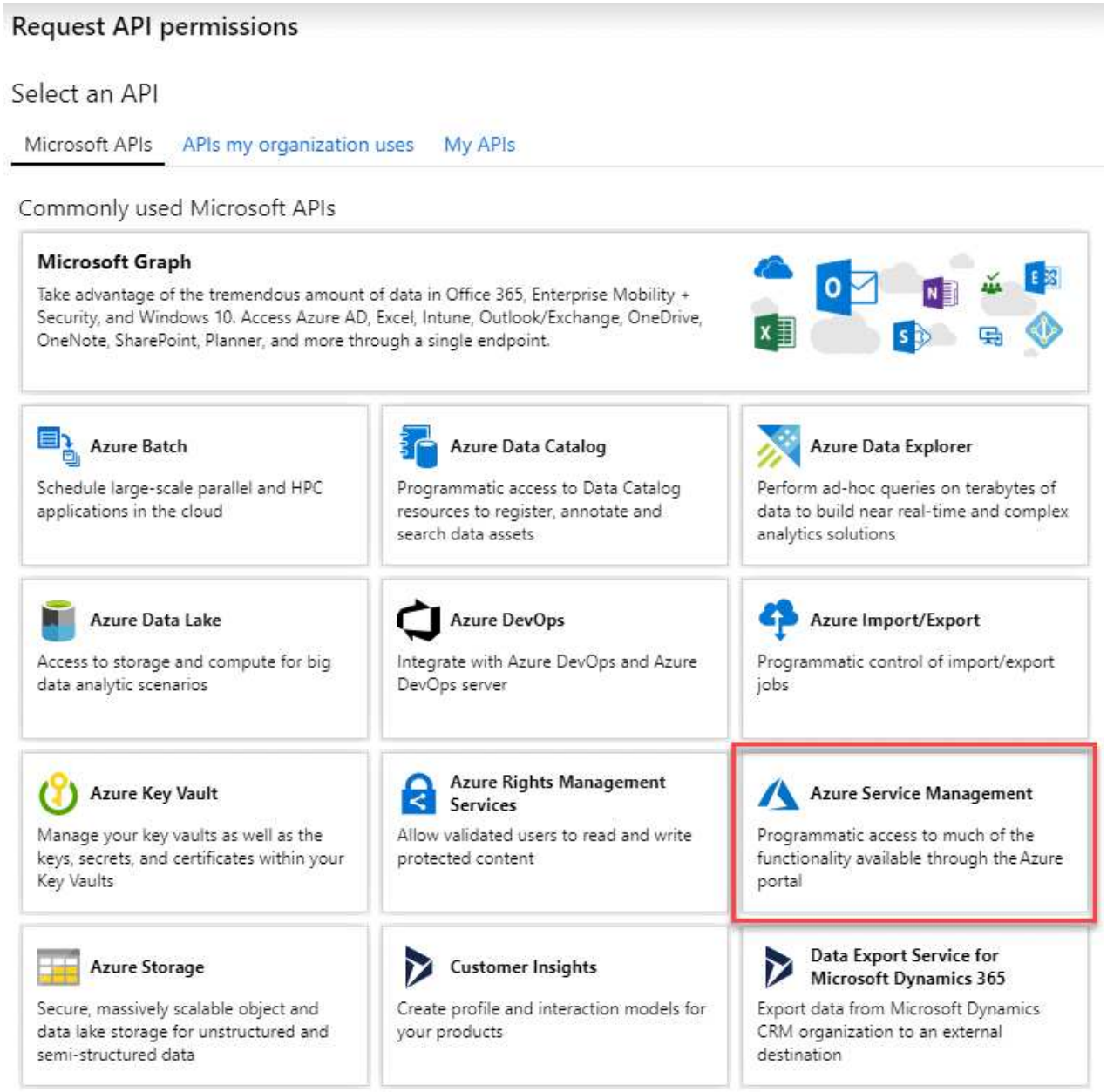
これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

複数の Azure サブスクリプションからCloud Volumes ONTAPをデプロイする場合は、サービス プリンシパルを各サブスクリプションにバインドする必要があります。 NetApp Consoleでは、 Cloud Volumes ONTAP をデプロイするときに使用するサブスクリプションを選択できます。

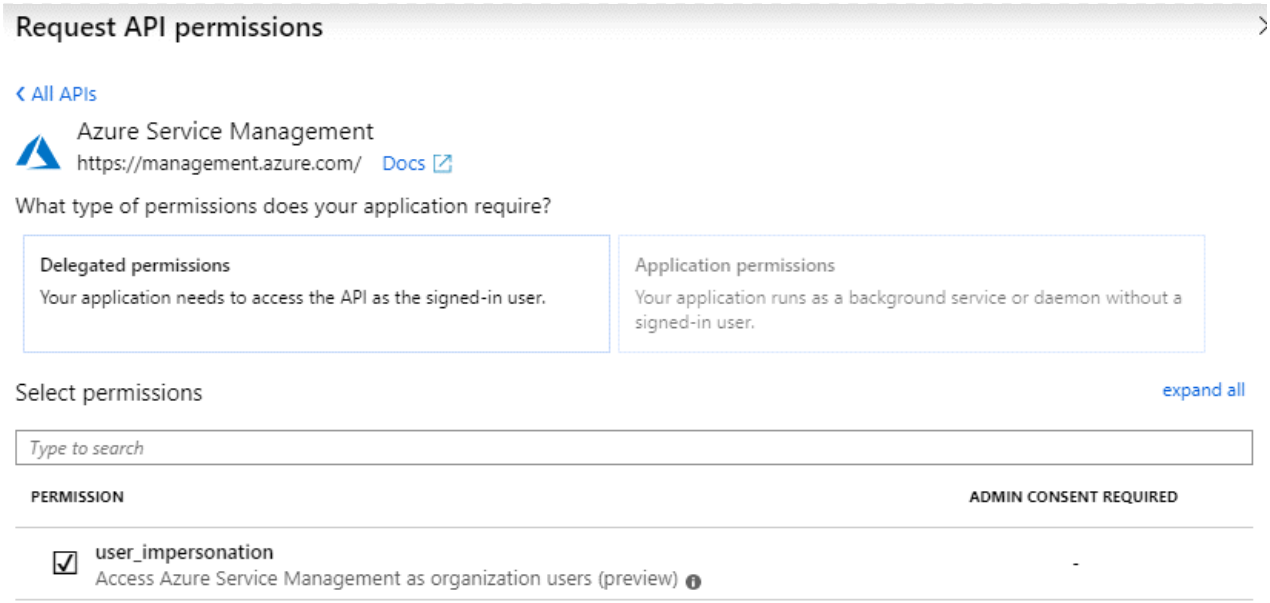
Windows Azure サービス管理 **API** 権限を追加する

1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. **API** 権限 **>** 権限の追加 を選択します。

3. **Microsoft API** の下で、**Azure Service Management** を選択します。

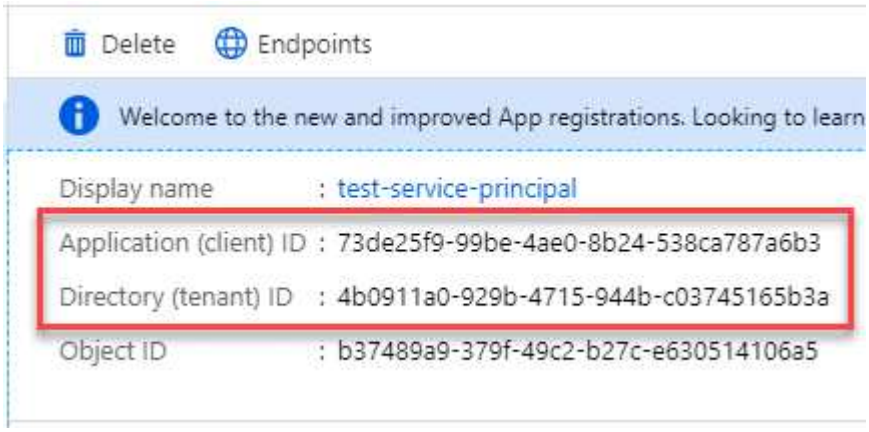


4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。



アプリケーションのアプリケーション**ID**とディレクトリ**ID**を取得します

1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. アプリケーション **(**クライアント**) ID** と ディレクトリ **(**テナント**) ID** をコピーします。



Azure アカウントをコンソールに追加するときは、アプリケーションのアプリケーション (クライアント) ID とディレクトリ (テナント) ID を指定する必要があります。コンソールは ID を使用してプログラムでサインインします。

クライアントシークレットを作成する

1. **Microsoft Entra ID** サービスを開きます。
2. *アプリ登録*を選択し、アプリケーションを選択します。
3. *証明書とシークレット > 新しいクライアント シークレット*を選択します。
4. シークレットの説明と期間を指定します。
5. *追加*を選択します。
6. クライアント シークレットの値をコピーします。

結果

これでサービス プリンシパルが設定され、アプリケーション (クライアント) ID、ディレクトリ (テナント) ID、およびクライアント シークレットの値がコピーされているはずです。 Azure アカウントを追加するときに、コンソールにこの情報を入力する必要があります。

Google Cloud サービス アカウント

ロールを作成し、コンソール エージェント VM インスタンスに使用するサービス アカウントに適用します。

手順

1. Google Cloud でカスタムロールを作成します。

   a. 定義された権限を含むYAMLファイルを作成します。"Google Cloud のコンソール エージェント ポリシー" 。

   b. Google Cloud から Cloud Shell を有効にします。

   c. コンソール エージェントに必要な権限を含む YAML ファイルをアップロードします。

   d. カスタムロールを作成するには、 `gcloud iam roles create`指示。

      次の例では、プロジェクト レベルで「connector」という名前のロールを作成します。

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

   +
   "Google Cloud ドキュメント: カスタムロールの作成と管理"

2. Google Cloud でサービス アカウントを作成します。

   a. IAM & Admin サービスから、サービス アカウント > サービス アカウントの作成 を選択します。

   b. サービス アカウントの詳細を入力し、[作成して続行] を選択します。

   c. 作成したロールを選択します。

   d. 残りの手順を完了してロールを作成します。

      "Google Cloud ドキュメント: サービス アカウントの作成"

結果

これで、コンソール エージェント VM インスタンスに割り当てることができるサービス アカウントが作

成されました。

ステップ**7: Google Cloud API**を有効にする

Google Cloud にCloud Volumes ONTAPをデプロイするには、いくつかの API が必要です。

手順

1. "プロジェクトで次の Google Cloud API を有効にします"
    - クラウド デプロイメント マネージャー V2 API
    - クラウドロギングAPI
    - クラウド リソース マネージャー API
    - コンピューティングエンジン API
    - アイデンティティとアクセス管理 (IAM) API
    - クラウド キー管理サービス (KMS) API

      （顧客管理暗号化キー（CMEK）を使用したNetApp Backup and Recoveryを使用する予定の場合のみ必要）

制限モードでコンソールエージェントを展開する

制限されたアウトバウンド接続でNetApp Consoleを使用できるように、コンソール エージェントを制限モードで展開します。開始するには、コンソール エージェントをインストールし、コンソール エージェントで実行されているユーザー インターフェイスにアクセスしてコンソールをセットアップし、以前に設定したクラウド権限を提供します。

ステップ**1:** コンソールエージェントをインストールする

コンソール エージェントをクラウド 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か、Linux ホストに手動でインストールします。

AWS コマーシャルマーケットプレイス

開始する前に

次のものが必要です:

- ネットワーク要件を満たす VPC とサブネット。

  "ネットワーク要件について学ぶ"

- コンソール エージェントに必要な権限を含むポリシーがアタッチされた IAM ロール。

  "AWS権限の設定方法を学ぶ"

- IAM ユーザーが AWS Marketplace にサブスクライブしたり、サブスクライブ解除したりするための権限。
- インスタンスの CPU および RAM 要件を理解すること。

  "インスタンス要件を確認する" 。

- EC2 インスタンスのキーペア。

手順

1. に行く "AWS Marketplace でのNetApp Consoleエージェントのリスト"
2. マーケットプレイス ページで、[サブスクリプションを続行] を選択します。
3. ソフトウェアをサブスクライブするには、「利用規約に同意」を選択します。

   サブスクリプションのプロセスには数分かかる場合があります。

4. サブスクリプションプロセスが完了したら、[構成に進む] を選択します。
5. *このソフトウェアを構成する*ページで、正しいリージョンが選択されていることを確認し、*起動を続行*を選択します。
6. このソフトウェアの起動 ページの アクションの選択 で、**EC2** 経由で起動 を選択し、起動 を選択します。

   EC2 コンソールを使用してインスタンスを起動し、IAM ロールをアタッチします。これは、**Web** サイトから起動 アクションでは不可能です。

7. プロンプトに従ってインスタンスを構成してデプロイします。
   - 名前とタグ: インスタンスの名前とタグを入力します。
   - アプリケーションと **OS** イメージ: このセクションはスキップします。コンソール エージェント AMI はすでに選択されています。
   - インスタンス タイプ: リージョンの可用性に応じて、RAM と CPU の要件を満たすインスタンス タイプを選択します (t3.2xlarge が事前に選択されており、推奨されています)。
   - キーペア (ログイン): インスタンスに安全に接続するために使用するキーペアを選択します。
   - ネットワーク設定: 必要に応じてネットワーク設定を編集します。
     - 必要な VPC とサブネットを選択します。

- インスタンスにパブリック IP アドレスを割り当てるかどうかを指定します。
- コンソール エージェント インスタンスに必要な接続方法 (SSH、HTTP、HTTPS) を有効にするセキュリティ グループ設定を指定します。

  "AWS のセキュリティグループルールを表示する" 。

◦ ストレージの構成: ルート ボリュームのデフォルトのサイズとディスク タイプを維持します。

ルートボリュームで Amazon EBS 暗号化を有効にする場合は、[詳細] を選択し、[ボリューム **1**] を展開して、[暗号化] を選択し、KMS キーを選択します。

◦ 詳細: **IAM** インスタンス プロファイル で、コンソール エージェントに必要な権限を含む IAM ロールを選択します。

◦ 概要: 概要を確認し、*インスタンスの起動*を選択します。

結果

AWS は指定された設定でソフトウェアを起動します。コンソール エージェント インスタンスとソフトウェアは約 5 分で実行されます。

次の手順

NetApp Consoleをセットアップします。

AWS Gov マーケットプレイス

開始する前に

次のものが必要です:

- ネットワーク要件を満たす VPC とサブネット。

  "ネットワーク要件について学ぶ"

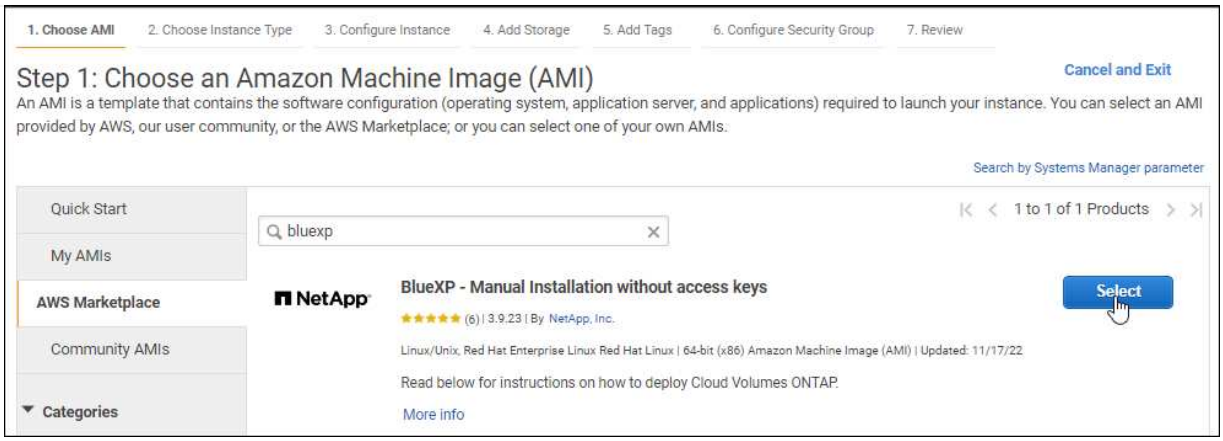
- コンソール エージェントに必要な権限を含むポリシーがアタッチされた IAM ロール。

  "AWS権限の設定方法を学ぶ"

- IAM ユーザーが AWS Marketplace にサブスクライブしたり、サブスクライブ解除したりするための権限。
- EC2 インスタンスのキーペア。

手順

1. AWS Marketplace で提供されているNetApp Consoleエージェントにアクセスします。
   a. EC2 サービスを開き、*インスタンスの起動*を選択します。
   b. *AWS Marketplace*を選択します。
   c. NetApp Consoleを検索し、オファリングを選択します。



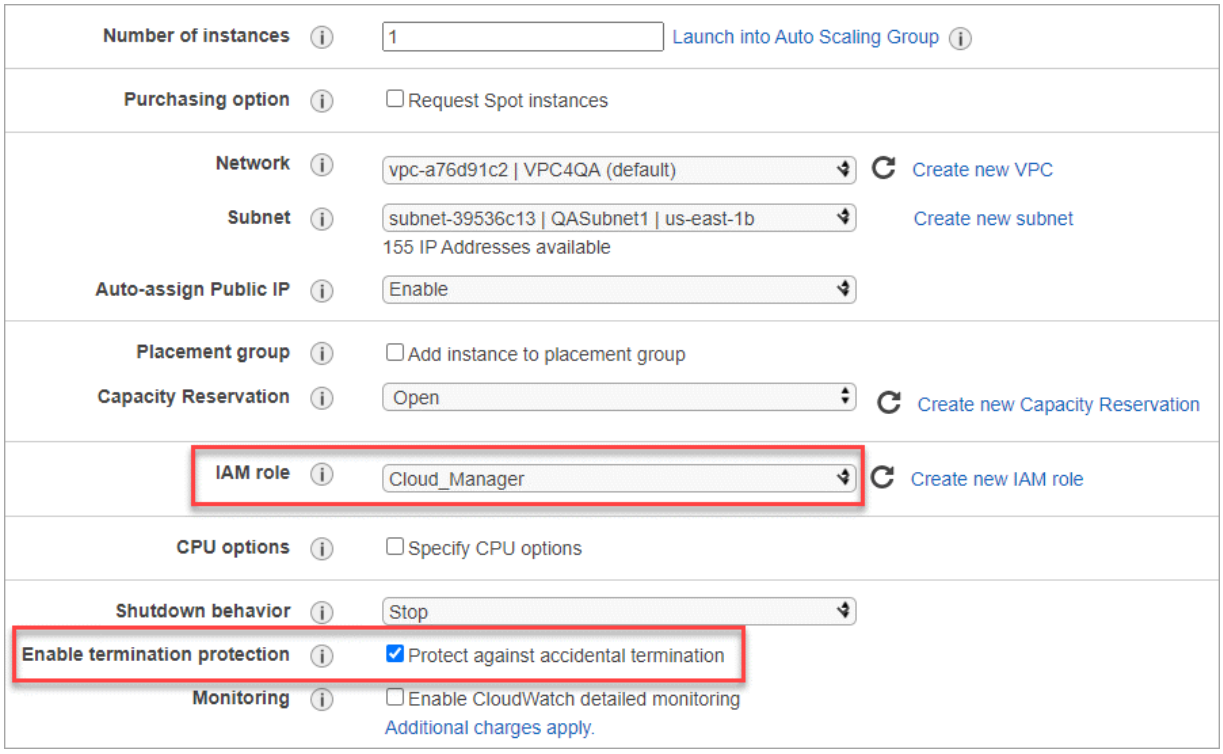
d. *続行*を選択します。

2. プロンプトに従ってインスタンスを構成してデプロイします。

   - インスタンス タイプを選択: リージョンの可用性に応じて、サポートされているインスタンス タイプのいずれかを選択します (t3.2xlarge が推奨されます)。

     "インスタンス要件を確認する" 。

   - インスタンスの詳細の設定: VPC とサブネットを選択し、手順 1 で作成した IAM ロールを選択し、終了保護を有効にして (推奨)、要件を満たすその他の設定オプションを選択します。



   - ストレージの追加: デフォルトのストレージ オプションをそのままにします。
   - タグの追加: 必要に応じて、インスタンスのタグを入力します。
   - セキュリティ グループの構成: コンソール エージェント インスタンスに必要な接続方法 (SSH 、HTTP、HTTPS) を指定します。
   - 確認: 選択内容を確認し、*起動*を選択します。

結果

AWS は指定された設定でソフトウェアを起動します。コンソール エージェント インスタンスとソフトウェアは約 5 分で実行されます。

次の手順

コンソールをセットアップします。

Azure Gov マーケットプレイス

開始する前に

次のものが必要です:

- ネットワーク要件を満たす VNet とサブネット。

  "ネットワーク要件について学ぶ"

- コンソール エージェントに必要なアクセス許可を含む Azure カスタム ロール。

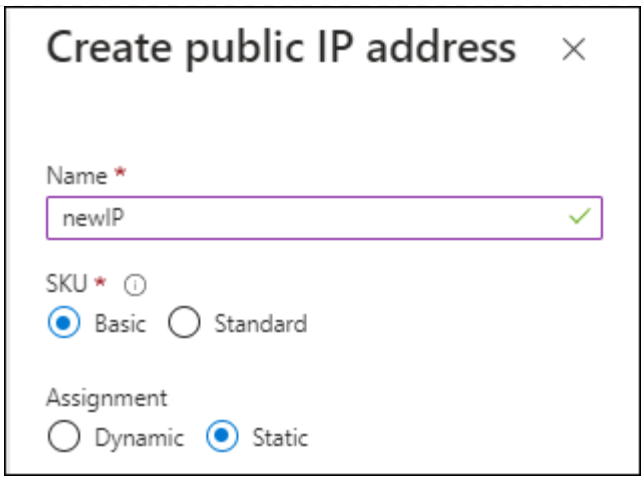
  "Azure の権限を設定する方法を学ぶ"

手順

1. Azure Marketplace のNetApp Consoleエージェント VM ページに移動します。
   - "商用リージョン向けの Azure Marketplace ページ"
   - "Azure Government リージョンの Azure Marketplace ページ"
2. *今すぐ入手*を選択し、*続行*を選択します。
3. Azure ポータルから [作成] を選択し、手順に従って仮想マシンを構成します。

   VM を構成する際には、次の点に注意してください。

   - **VM** サイズ: CPU と RAM の要件を満たす VM サイズを選択します。 Standard_D8s_v3 をお勧めします。
   - ディスク: コンソール エージェントは、HDD ディスクまたは SSD ディスクのいずれでも最適に動作します。
   - パブリック **IP**: コンソール エージェント VM でパブリック IP アドレスを使用する場合は、コンソールがこのパブリック IP アドレスを使用するように、IP アドレスで Basic SKU を使用する必要があります。



代わりに標準 SKU IP アドレスを使用する場合、コンソールはパブリック IP ではなく、コンソール エージェントのプライベート IP アドレスを使用します。コンソールにアクセスするために使用しているマシンがそのプライベート IP アドレスにアクセスできない場合、コンソールからのアクションは失敗します。

"Azure ドキュメント: パブリック IP SKU"

- ネットワーク セキュリティ グループ: コンソール エージェントには、SSH、HTTP、および HTTPS を使用した受信接続が必要です。

  "Azure のセキュリティ グループ ルールを表示する" 。

- **ID**: 管理 の下で、システム割り当てマネージド **ID** を有効にする を選択します。

  この設定は重要です。マネージド ID を使用すると、コンソール エージェント仮想マシンは資格情報を提供せずに Microsoft Entra ID に対して自身を識別できるためです。 "Azure リソースのマネージド ID の詳細" 。

4. 確認 + 作成 ページで選択内容を確認し、作成 を選択してデプロイを開始します。

結果

Azure は指定された設定で仮想マシンをデプロイします。仮想マシンとコンソール エージェント ソフトウェアは約 5 分以内に実行されるはずです。

次の手順

NetApp Consoleをセットアップします。

手動インストール

開始する前に

次のものが必要です:

- コンソール エージェントをインストールするためのルート権限。
- コンソール エージェントからのインターネット アクセスにプロキシが必要な場合のプロキシ サーバーの詳細。

  インストール後にプロキシ サーバーを構成するオプションがありますが、これを行うにはコンソール エージェントを再起動する必要があります。

- プロキシ サーバーが HTTPS を使用する場合、またはプロキシがインターセプト プロキシである場合は、CA 署名証明書。

> コンソール エージェントを手動でインストールする場合、透過プロキシ サーバーの証明書を設定することはできません。透過プロキシ サーバーの証明書を設定する必要がある場合は、インストール後にメンテナンス コンソールを使用する必要があります。詳細はこちら"エージェントメンテナンスコンソール"。

- インストール中に送信接続を検証する構成チェックを無効にする必要があります。このチェックが無効になっていない場合、手動インストールは失敗します。"手動インストールの構成チェックを無効にする方法を説明します。"
- オペレーティング システムに応じて、コンソール エージェントをインストールする前に Podman または Docker Engine のいずれかが必要です。

タスク概要

NetAppサポート サイトで入手できるインストーラーは、以前のバージョンである可能性があります。インストール後、新しいバージョンが利用可能な場合、コンソール エージェントは自動的に更新されます。

手順

1. ホストに *http_proxy* または *https_proxy* システム変数が設定されている場合は、それらを削除します。

```
unset http_proxy
unset https_proxy
```

   これらのシステム変数を削除しないと、インストールは失敗します。

2. コンソールエージェントソフトウェアを以下からダウンロードします。 "NetAppサポート サイト"それを Linux ホストにコピーします。

   ネットワークまたはクラウドで使用するための「オンライン」エージェント インストーラーをダウンロードする必要があります。

3. スクリプトを実行するための権限を割り当てます。

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

   <version> は、ダウンロードしたコンソール エージェントのバージョンです。

4. Government Cloud 環境にインストールする場合は、構成チェックを無効にします。"手動インストールの構成チェックを無効にする方法を説明します。"
5. インストール スクリプトを実行します。

```
 ./NetApp_Console_Agent_Cloud_<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

ネットワークでインターネット アクセスにプロキシが必要な場合は、プロキシ情報を追加する必要があります。透過プロキシまたは明示プロキシのいずれかを追加できます。 --proxy および --cacert パラメータはオプションであり、追加するように要求されることはありません。プロキシ サーバーがある場合は、示されているようにパラメータを入力する必要があります。

CA 署名証明書を使用して明示的なプロキシ サーバーを構成する例を次に示します。

```
 ./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

`--proxy`次のいずれかの形式を使用して、コンソール エージェントが HTTP または HTTPS プロキシ サーバーを使用するように構成します。

- http://アドレス:ポート
- http://ユーザー名:パスワード@アドレス:ポート
- http://ドメイン名%92ユーザー名:パスワード@アドレス:ポート
- https://アドレス:ポート
- https://ユーザー名:パスワード@アドレス:ポート
- https://ドメイン名%92ユーザー名:パスワード@アドレス:ポート

  次の点に注意してください。

  - ユーザーはローカル ユーザーまたはドメイン ユーザーになります。
  - ドメイン ユーザーの場合は、上記のように \ の ASCII コードを使用する必要があります。
  - コンソール エージェントは、@ 文字を含むユーザー名またはパスワードをサポートしていません。
  - パスワードに以下の特殊文字が含まれている場合は、その特殊文字の前にバックスラッシュ (& または !) を付けてエスケープする必要があります。

    例えば：

http://bxpproxyuser:netapp1\!@アドレス:3128

`--cacert`コンソール エージェントとプロキシ サーバー間の HTTPS アクセスに使用する CA 署名付き証明書を指定します。このパラメータは、HTTPS プロキシ サーバー、インターセプト プロキシ サーバー、および透過プロキシ サーバーに必須です。

+ 透過プロキシ サーバーを構成する例を次に示します。透過プロキシを構成する場合、プロキシ サーバーを定義する必要はありません。コンソール エージェント ホストには、CA 署名付き証明書のみを追加します。

+

```
 ./NetApp_Console_Agent_Cloud_v4.0.0 --cacert
/tmp/cacert/certificate.cer
```

1. Podman を使用した場合は、aardvark-dns ポートを調整する必要があります。
   a. コンソール エージェント仮想マシンに SSH で接続します。
   b. podman */usr/share/containers/containers.conf* ファイルを開き、Aardvark DNS サービス用に選択したポートを変更します。たとえば、54 に変更します。

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

   c. コンソール エージェント仮想マシンを再起動します。

結果

コンソール エージェントがインストールされました。プロキシ サーバーを指定した場合、インストールの最後に、コンソール エージェント サービス (occm) が 2 回再起動します。

次の手順

NetApp Consoleをセットアップします。

ステップ**2: NetApp Console**をセットアップする

コンソールに初めてアクセスすると、コンソール エージェントの組織を選択するように求められ、制限モードを有効にする必要があります。

開始する前に

コンソール エージェントを設定するユーザーは、コンソール組織に属していないログインを使用してコンソールにログインする必要があります。

ログインが別の組織に関連付けられている場合は、新しいログインでサインアップする必要があります。そうしないと、セットアップ画面に制限モードを有効にするオプションが表示されません。

手順

1. コンソール エージェント インスタンスに接続しているホストから Web ブラウザを開き、インストールし

たコンソール エージェントの次の URL を入力します。

2. NetApp Consoleにサインアップまたはログインします。
3. ログインしたら、コンソールを設定します。

    a. コンソール エージェントの名前を入力します。

    b. 新しいコンソール組織の名前を入力します。

    c. 安全な環境で実行していますか**?** を選択します。

    d. *このアカウントで制限モードを有効にする*を選択します。

        アカウントの作成後はこの設定を変更できないことに注意してください。制限モードを後から有効にしたり無効にしたりすることはできません。

    コンソール エージェントを政府リージョンに展開した場合、チェック ボックスは既に有効になっており、変更できません。これは、制限モードが政府地域でサポートされている唯一のモードであるためです。

    a. *始めましょう*を選択します。

結果

コンソール エージェントがインストールされ、コンソール組織に設定されました。すべてのユーザーは、コンソール エージェント インスタンスの IP アドレスを使用してコンソールにアクセスする必要があります。

次の手順

以前に設定した権限をコンソールに提供します。

ステップ**3: NetApp Console**に権限を付与する

Azure Marketplace からコンソール エージェントを展開した場合、またはコンソール エージェント ソフトウェアを手動でインストールした場合は、以前に設定したアクセス許可を提供する必要があります。

デプロイ中に必要な IAM ロールを選択したため、AWS Marketplace からコンソールエージェントをデプロイした場合は、これらの手順は適用されません。

"クラウド権限の準備方法を学ぶ" 。

AWS IAM ロール

以前に作成した IAM ロールを、コンソールエージェントをインストールした EC2 インスタンスにアタッチします。

これらの手順は、AWS にコンソールエージェントを手動でインストールした場合にのみ適用されます。AWS Marketplace のデプロイメントでは、コンソールエージェントインスタンスは、必要な権限を含む IAM ロールにすでに関連付けられています。

手順

1. Amazon EC2 コンソールに移動します。
2. *インスタンス*を選択します。
3. コンソール エージェント インスタンスを選択します。
4. *アクション > セキュリティ > IAM ロールの変更*を選択します。
5. IAM ロールを選択し、*IAM ロールの更新*を選択します。

AWS アクセスキー

必要な権限を持つ IAM ユーザーの AWS アクセス キーをNetApp Consoleに提供します。

手順

1. *管理 > 資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: *Amazon Web Services > エージェントを選択します。
   b. 資格情報の定義: AWS アクセスキーとシークレットキーを入力します。
   c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。
   d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

Azure ロール

Azure ポータルに移動し、1 つ以上のサブスクリプションのコンソール エージェント仮想マシンに Azure カスタム ロールを割り当てます。

手順

1. Azure ポータルから サブスクリプション サービスを開き、サブスクリプションを選択します。

   サブスクリプション サービスからロールを割り当てることが重要です。これは、サブスクリプション レベルでのロール割り当ての範囲を指定するためです。 *scope* は、アクセスが適用されるリソースのセットを定義します。別のレベル (たとえば、仮想マシン レベル) でスコープを指定すると、NetApp Console内からアクションを完了する機能に影響します。

   "Microsoft Azure ドキュメント: Azure RBAC のスコープを理解する"

2. アクセス制御 **(IAM)** > 追加 > ロール割り当ての追加 を選択します。
3. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。

コンソール オペレーターは、ポリシーで提供されるデフォルト名です。ロールに別の名前を選択した場合は、代わりにその名前を選択します。

4. *メンバー*タブで、次の手順を実行します。
   a. マネージド **ID** へのアクセスを割り当てます。
   b. *メンバーの選択*を選択し、コンソール エージェント仮想マシンが作成されたサブスクリプションを選択し、*マネージド ID*の下で*仮想マシン*を選択して、コンソール エージェント仮想マシンを選択します。
   c. *選択*を選択します。
   d. *次へ*を選択します。
   e. *レビュー + 割り当て*を選択します。
   f. 追加の Azure サブスクリプションのリソースを管理する場合は、そのサブスクリプションに切り替えて、これらの手順を繰り返します。

Azure サービスプリンシパル

以前に設定した Azure サービス プリンシパルの資格情報をNetApp Consoleに提供します。

手順

1. *管理 > 資格情報*を選択します。
2. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: **Microsoft Azure >** エージェント を選択します。
   b. 資格情報の定義: 必要な権限を付与する Microsoft Entra サービス プリンシパルに関する情報を入力します。
      - アプリケーション（クライアント）ID
      - ディレクトリ（テナント）ID
      - クライアントシークレット
   c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。
   d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

結果

NetApp Consoleに、ユーザーに代わって Azure でアクションを実行するために必要な権限が付与されました。

Google Cloud サービス アカウント

サービス アカウントをコンソール エージェント VM に関連付けます。

手順

1. Google Cloud ポータルに移動し、サービス アカウントをコンソール エージェント VM インスタンスに割り当てます。

   "Google Cloud ドキュメント: インスタンスのサービス アカウントとアクセス スコープの変更"

2. 他のプロジェクトのリソースを管理する場合は、コンソール エージェント ロールを持つサービス アカウントをそのプロジェクトに追加してアクセスを許可します。プロジェクトごとにこの手順を繰り返す必要があります。

NetApp Intelligent Servicesにサブスクライブする（制限モード）

クラウド プロバイダーのマーケットプレイスからNetApp Intelligent Servicesにサブスクライブして、時間単位の料金 (PAYGO) または年間契約でデータ サービスの料金を支払います。 NetAppからライセンスを購入した場合 (BYOL)、マーケットプレイス オファリングにもサブスクライブする必要があります。最初にライセンスに対して課金が行われますが、ライセンス容量を超えた場合、またはライセンスの有効期限が切れた場合は、時間単位で課金されます。

マーケットプレイス サブスクリプションでは、制限モードで次のデータ サービスに対して課金できます。

- NetApp Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

NetApp Data Classification はサブスクリプションを通じて有効になりますが、分類の使用には料金はかかりません。

開始する前に

データ サービスをサブスクライブするには、コンソール エージェントをすでに展開しておく必要があります。コンソール エージェントに接続されたクラウド資格情報にマーケットプレイス サブスクリプションを関連付ける必要があります。

AWS

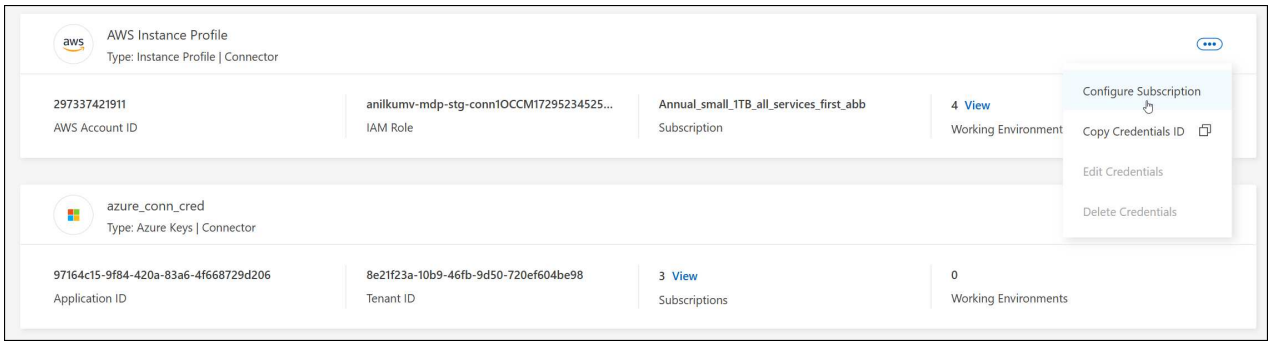
次のビデオは、AWS Marketplace からNetApp Intelligent Servicesをサブスクライブする手順を示しています。

AWS MarketplaceからNetApp Intelligent Servicesをサブスクライブする

手順

1. *管理 > 資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. コンソール エージェントに関連付けられている資格情報のセットのアクション メニューを選択し、[サブスクリプションの構成] を選択します。

   コンソール エージェントに関連付けられている資格情報を選択する必要があります。マーケットプレイス サブスクリプションを、 NetApp Consoleに関連付けられている資格情報に関連付けることはできません。



4. 資格情報を既存のサブスクリプションに関連付けるには、ドロップダウン リストからサブスクリプションを選択し、[構成] を選択します。
5. 認証情報を新しいサブスクリプションに関連付けるには、[サブスクリプションの追加] > [続行] を選択し、AWS Marketplace の手順に従います。

   a. *購入オプションを表示*を選択します。

   b. *購読*を選択します。

   c. *アカウントを設定*を選択します。

      NetApp Consoleにリダイレクトされます。

   d. *サブスクリプションの割り当て*ページから:

      - このサブスクリプションを関連付けるコンソール組織またはアカウントを選択します。
      - 既存のサブスクリプションを置き換える フィールドで、1 つの組織またはアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        コンソールは、組織またはアカウント内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。

- *保存*を選択します。

Azure

手順

1. *管理 > 資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. コンソール エージェントに関連付けられている資格情報のセットのアクション メニューを選択し、[サブスクリプションの構成] を選択します。

   コンソール エージェントに関連付けられている資格情報を選択する必要があります。マーケットプレイス サブスクリプションを、 NetApp Consoleに関連付けられている資格情報に関連付けることはできません。

4. 資格情報を既存のサブスクリプションに関連付けるには、ドロップダウン リストからサブスクリプションを選択し、[構成] を選択します。
5. 資格情報を新しいサブスクリプションに関連付けるには、[サブスクリプションの追加] > [続行] を選択し、Azure Marketplace の手順に従います。

   a. プロンプトが表示されたら、Azure アカウントにログインします。
   b. *購読*を選択します。
   c. フォームに記入し、「購読」を選択します。
   d. サブスクリプションプロセスが完了したら、「今すぐアカウントを構成」を選択します。

      NetApp Consoleにリダイレクトされます。

   e. *サブスクリプションの割り当て*ページから:

      - このサブスクリプションを関連付けるコンソール組織またはアカウントを選択します。
      - 既存のサブスクリプションを置き換える フィールドで、1 つの組織またはアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        コンソールは、組織またはアカウント内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

   他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。

      - *保存*を選択します。

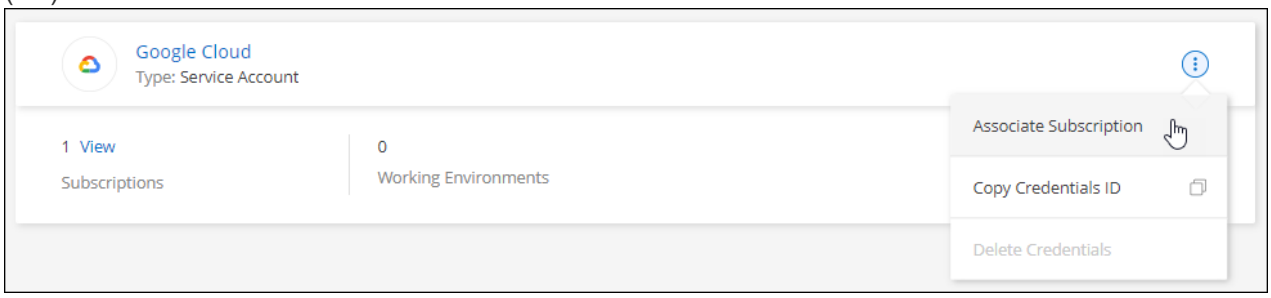
        次のビデオでは、Azure Marketplace からサブスクライブする手順を示します。

Azure Marketplace からNetApp Intelligent Servicesをサブスクライブする

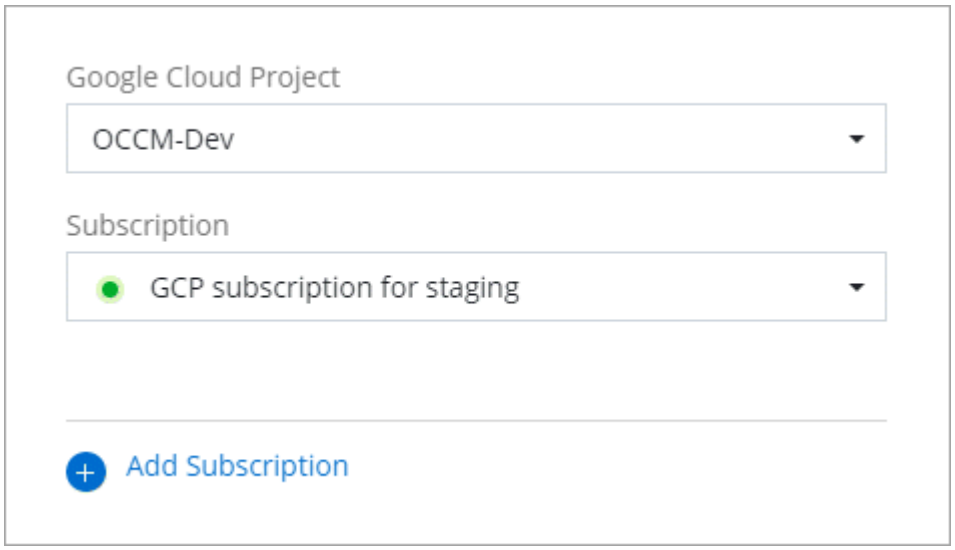
Google Cloud

手順

1. *管理 > *資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. コンソール エージェントに関連付けられている資格情報のセットのアクション メニューを選択し、[サブスクリプションの構成] を選択します。 +新しいスクリーンショットが必要です (TS)



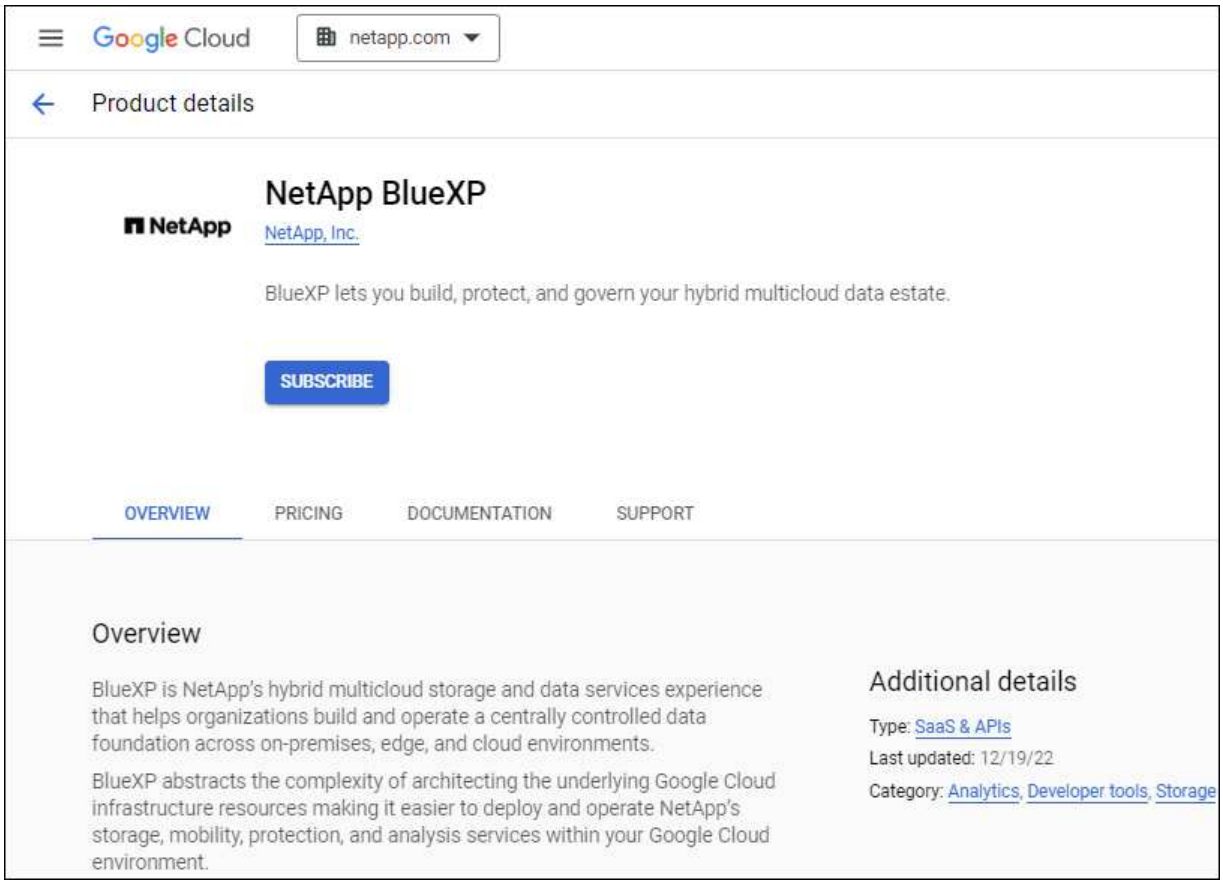
4. 選択した認証情報を使用して既存のサブスクリプションを構成するには、ドロップダウン リストから Google Cloud プロジェクトとサブスクリプションを選択し、[構成] を選択します。



5. まだサブスクリプションをお持ちでない場合は、[サブスクリプションを追加] > [続行] を選択し、Google Cloud Marketplace の手順に従います。

次の手順を完了する前に、Google Cloud アカウントの課金管理者権限とNetApp Consoleのログイン権限の両方があることを確認してください。

a. リダイレクトされたら "Google Cloud Marketplace のNetApp Intelligent Servicesページ"上部のナビゲーション メニューで正しいプロジェクトが選択されていることを確認します。

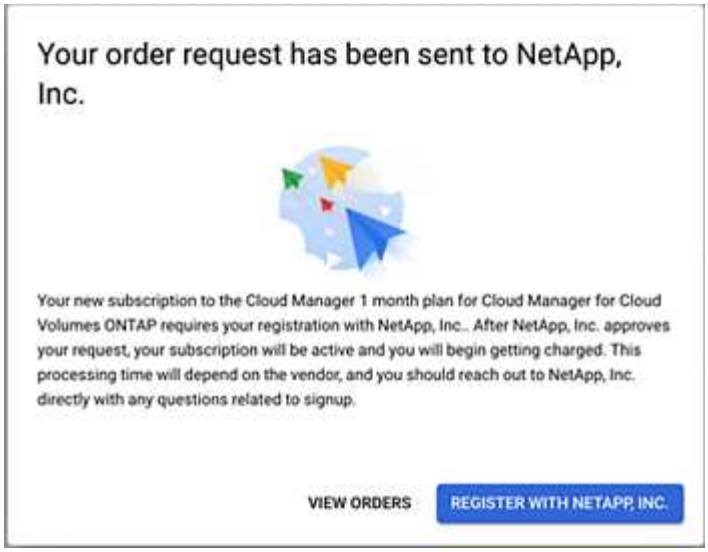


b. *購読*を選択します。
c. 適切な請求先アカウントを選択し、利用規約に同意します。
d. *購読*を選択します。

   この手順により、転送リクエストがNetAppに送信されます。

e. ポップアップダイアログボックスで、* NetApp, Inc.に登録*を選択します。

   Google Cloud サブスクリプションをコンソールの組織またはアカウントにリンクするには、この手順を完了する必要があります。このページからリダイレクトされ、コンソールにサインインするまで、サブスクリプションをリンクするプロセスは完了しません。



f. サブスクリプションの割り当て ページの手順を完了します。

> 組織内の誰かが既に請求先アカウントからマーケットプレイスサブスクリプションを利用している場合は、次のページにリダイレクトされます。 "NetApp Console内のCloud Volumes ONTAPページ"その代わり。予期しない事態が発生した場合は、 NetAppの営業チームにお問い合わせください。 Google では、Google 請求先アカウントごとに 1 つのサブスクリプションのみ有効になります。

- このサブスクリプションを関連付けるコンソール組織またはアカウントを選択します。
- 既存のサブスクリプションを置き換える フィールドで、1 つの組織またはアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

  コンソールは、組織またはアカウント内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

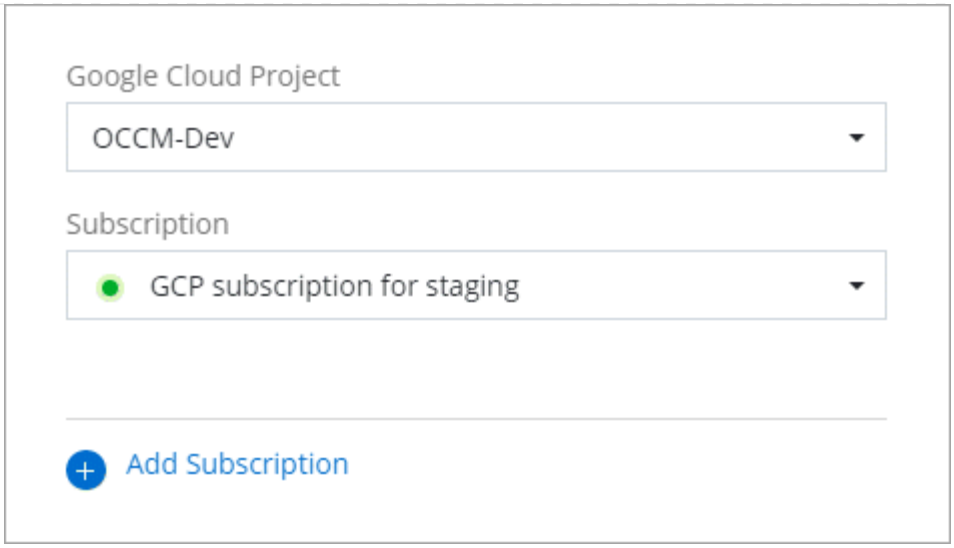
他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。

- *保存*を選択します。

  次のビデオでは、Google Cloud Marketplace からサブスクライブする手順を示します。

Google Cloud Marketplace から登録する

a. このプロセスが完了したら、コンソールの [資格情報] ページに戻り、この新しいサブスクリプションを選択します。



関連情報

- "Cloud Volumes ONTAPのBYOL容量ベースライセンスを管理する"
- "データサービスのBYOLライセンスを管理する"
- "AWS の認証情報とサブスクリプションを管理する"
- "Azure の資格情報とサブスクリプションを管理する"
- "Google Cloud の認証情報とサブスクリプションを管理する"

次にできること（制限モード）

NetApp Consoleを制限モードで起動して実行すると、制限モードでサポートされているサービスの使用を開始できます。

ヘルプについては、次のサービスのドキュメントを参照してください。

- "Azure NetApp Filesドキュメント"
- "バックアップとリカバリのドキュメント"
- "分類ドキュメント"
- "Cloud Volumes ONTAPドキュメント"
- "デジタルウォレットのドキュメント"
- "オンプレミスのONTAPクラスタのドキュメント"
- "レプリケーションドキュメント"

関連情報

"NetApp Consoleの展開モード"

BlueXPレガシーインターフェース（プライベートモード）の使用を開始する

開始ワークフロー（BlueXPプライベートモード）

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インターフェー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"

プライベートモードでサポートされる機能とデータサービス

次の表は、どのBlueXPサービスと機能がプライベート モードでサポートされているか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。

製品分野	BlueXPのサービスまたは機能	プライベートモード
作業環境 表のこの部分には、 BlueXPキャンバスからの作業環境管理のサポートがリストされています。 BlueXP 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	いいえ
	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	**BlueXP**のサービスまたは機能	プライベートモード
サービス	アラート	いいえ
	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-no-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"^]
	分類	はい
	コピーと同期	いいえ
	デジタルアドバイザー	いいえ
	デジタルウォレット	はい
	ディザスタ リカバリ	いいえ
	経済効率	いいえ
	ランサムウェア耐性	いいえ
	レプリケーション	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
	階層化	いいえ
	ボリュームキャッシュ	いいえ
	ワークロードファクトリー	いいえ
特徴	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	いいえ
	多要素認証	いいえ
	NSSアカウント	いいえ
	通知	いいえ
	検索	いいえ
	スケジュール	はい

NetApp Consoleを使用する

NetApp Consoleにログインする

NetApp Consoleにログインする方法は、使用している展開モードによって異なります。

24 時間経過またはブラウザを閉じると、自動的にログアウトされます。

"コンソールの展開モードについて学ぶ" 。

標準モード

NetApp Consoleにサインアップすると、Web ベースのコンソールからログインして、データとストレージ インフラストラクチャの管理を開始できます。

タスク概要

次のいずれかのオプションを使用してNetApp Consoleにログインできます。

- 既存のNetAppサポートサイト（NSS）の認証情報
- メールアドレスとパスワードを使用したNetApp Consoleアカウント
- フェデレーション接続

  シングル サインオンを使用すると、企業ディレクトリ (フェデレーション ID) の資格情報を使用してログインできます。"ID連携の設定方法を学ぶ" 。

手順

1. ウェブブラウザを開いて、 "NetApp Console"
2. *ログイン*ページで、ログインに関連付けられているメールアドレスを入力します。
3. ログインに関連付けられた認証方法に応じて、資格情報を入力するよう求められます。
   - NetAppクラウド認証情報: パスワードを入力してください
   - フェデレーションユーザー: フェデレーションIDの資格情報を入力してください
   - NetAppサポートサイトアカウント: NetAppサポートサイトの認証情報を入力します

結果

これでログインが完了し、ハイブリッド マルチクラウド インフラストラクチャの管理を開始できるようになりました。

制限モード

コンソールを制限モードで使用する場合は、エージェント上でローカルに実行されるユーザー インターフェイスからコンソールにログインする必要があります。

タスク概要

コンソールは、制限モードの場合、次のいずれかのオプションを使用してログインすることをサポートします。

- メールアドレスとパスワードを使用したNetApp Consoleログイン
- フェデレーション接続

  シングル サインオンを使用すると、企業ディレクトリ (フェデレーション ID) の資格情報を使用してログインできます。"アイデンティティフェデレーションの使い方を学ぶ" 。

手順

1. Web ブラウザを開き、エージェントがインストールされている IP アドレスを入力します。
2. ユーザー名とパスワードを入力してログインしてください。

NetApp Consoleのホームページでメトリックを表示する

ストレージ資産の健全性を監視することで、ストレージ保護に関する問題を認識し、解決するための手順を実行できるようになります。 NetApp Consoleのホーム ページを使用して、 NetApp Backup and Recoveryからのバックアップとリストアのステータスと、 NetApp Ransomware Resilienceによって示されるようにランサムウェア攻撃のリスクがあるワークロードや保護されているワークロードの数を表示します。個々のクラスターとCloud Volumes ONTAPのストレージ容量、 ONTAPアラート、クラスターまたはCloud Volumes ONTAPシステムごとのストレージ パフォーマンス容量、保有しているさまざまな種類のライセンスなどを確認できます。

ホーム ページのすべてのペインには、組織レベルのデータが表示されます。ストレージ容量とストレージ パフォーマンス ペインには、IAM 権限に基づいてユーザーがアクセスできるプロジェクトに関連付けられたシステムが表示されます。

システムは、ホームページのデータを 5 分ごとに更新します。キャッシュにより、このページのデータが実際の値と最大 15 分間異なる可能性があります。

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。

必要なNetApp Consoleのロール

ホーム ページの各ペインには、異なるユーザー ロールが必要です。

- ストレージ容量ペイン: NetApp Consoleシステムページを表示する機能
- * ONTAPアラート ペイン*: フォルダまたはプロジェクト管理者、運用サポート アナリスト、組織管理者、組織閲覧者、スーパー管理者、スーパー閲覧者
- ストレージパフォーマンス容量ペイン: NetApp Consoleシステムページを表示する機能
- **Licenses and subscriptions**ペイン: フォルダーまたはプロジェクト管理者、組織管理者、組織閲覧者、スーパー管理者、スーパー閲覧者
- ランサムウェア耐性ペイン: フォルダまたはプロジェクト管理者、組織管理者、ランサムウェア耐性管理者、ランサムウェア耐性閲覧者、スーパー管理者、スーパー閲覧者
- バックアップとリカバリ ペイン: バックアップとリカバリ バックアップ管理者、バックアップとリカバリ スーパー管理者、バックアップとリカバリ バックアップ ビューアー、バックアップとリカバリ クローン管理者、フォルダーまたはプロジェクト管理者、組織管理者、バックアップとリカバリ リストア管理者、スーパー管理者、スーパー ビューアー

ペインにアクセスする権限がない場合は、そのペインを使用する権限がないことを示すメッセージが表示されます。

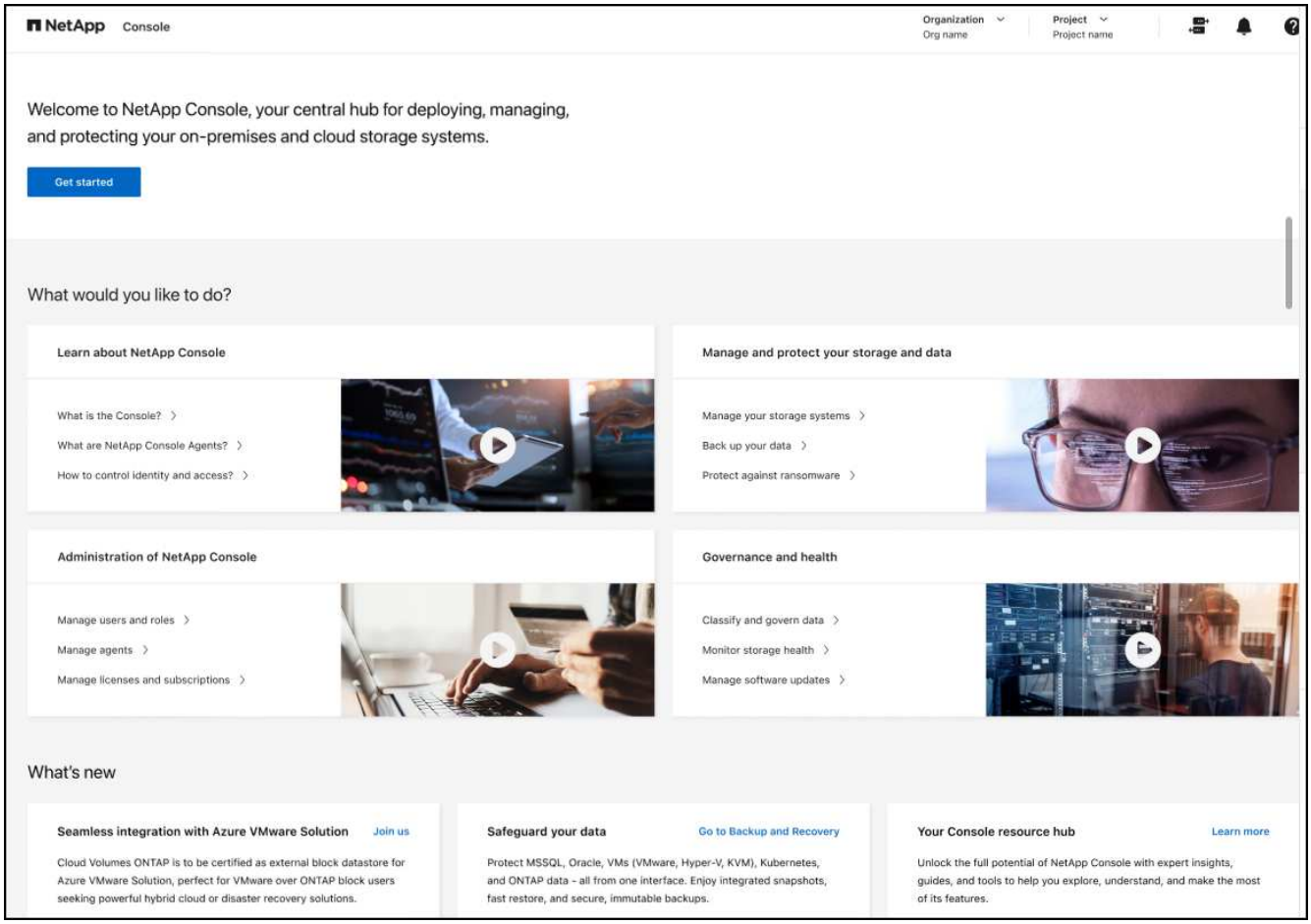
"NetApp Consoleのアクセス ロールについて学習します。" 。

手順

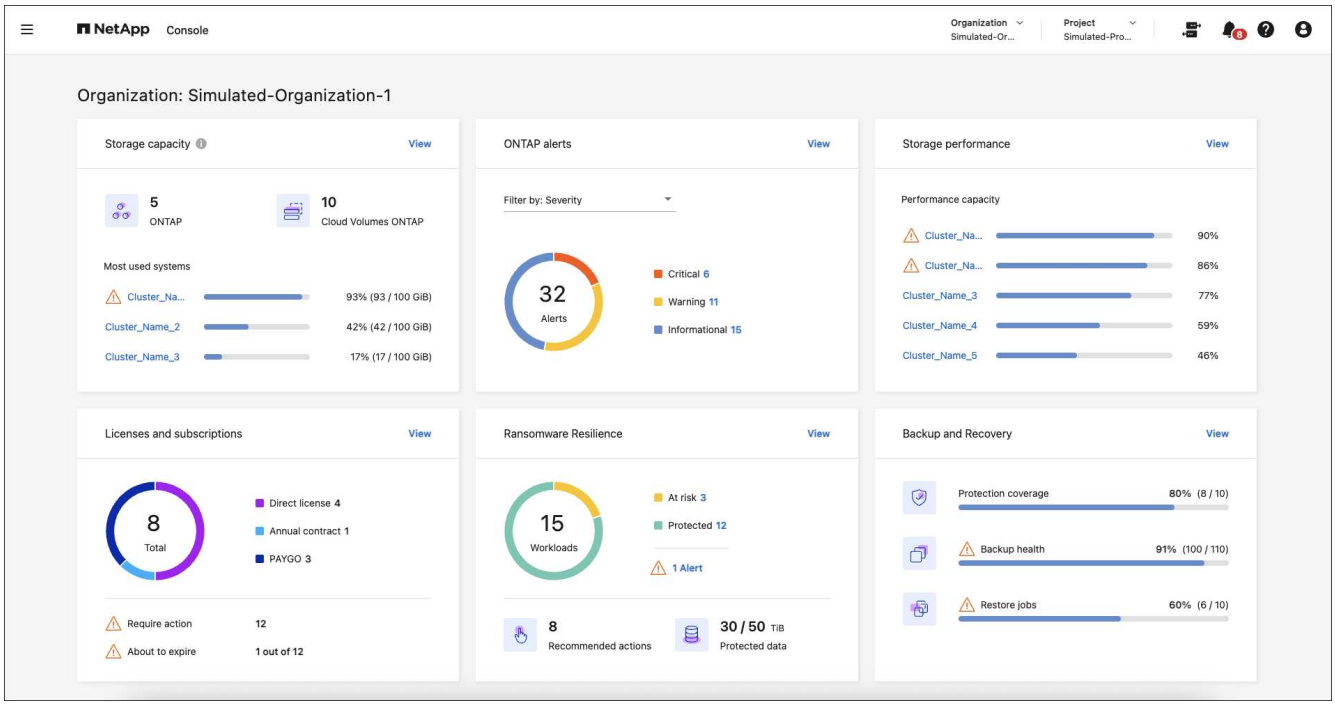
1. NetApp Consoleメニューから、[ホーム] を選択します。

   組織管理者のロールがあり、エージェントまたはストレージ システムが設定されていない場合は、ホーム

ページに開始方法の情報が表示されます。



NetApp Consoleがすでに設定されていて、少なくとも 1 つのコンソール エージェントが有効になっていて、そのエージェントに少なくとも 1 つのクラスタまたはCloud Volumes ONTAPシステムが追加されている場合は、ホーム ページにストレージ環境に関するメトリックが表示されます。



ホーム ページに指標が表示されるようにする

次の条件が満たされると、ホーム ページでメトリックを表示できます。

- NetApp Consoleの SaaS インスタンスにログインしています。
- 既存のストレージ リソース (エージェントとクラスター、またはCloud Volumes ONTAPシステム) を持つ組織に属している。
- 少なくとも 1 つのコンソール エージェントが有効になっています。
- そのエージェントに少なくとも 1 つのクラスターまたはCloud Volumes ONTAPシステムが追加されています。

ホーム ページにメトリックが表示されるようにするには、次のタスクを実行します。

- 少なくとも 1 つのコンソール エージェントを有効にします。
- そのエージェントを使用して、少なくとも 1 つのクラスターまたは 1 つのCloud Volumes ONTAP を追加します。

全体のストレージ容量を表示する

ストレージ容量ペインには、 ONTAPクラスターとCloud Volumes ONTAPシステム全体の次の情報が表示されます。

- コンソールで検出されたONTAPシステムの数
- コンソールで検出されたCloud Volumes ONTAPシステムの数
- クラスターあたりの容量使用量

クラスターまたはCloud Volumes ONTAPシステムの順序は、使用される容量の量に基づいています。簡単に識別できるように、容量が最も大きいクラスターまたはシステムが最初に表示されます。

クラスターの容量が 80% になると警告インジケーターが表示され、データは 5 分ごとに更新されます。

> 複数のプロジェクトがある場合、システム ページと比較して、ストレージ容量ペインに異なるデータが表示されることがあります。これは、システム ページにはプロジェクト レベルに基づいて情報が表示されるのに対し、ストレージ容量ペインには組織レベルの情報が表示されるためです。また、パフォーマンスを最適化するためにデータがその期間キャッシュされるため、このペインのデータは最大 15 分間、実際の値と異なる場合があります。

手順

1. NetApp Consoleメニューから、ストレージ容量ペインを確認します。
2. ストレージ容量ペインで、表示 を選択して、コンソール システム ページに移動します。
3. 「システム」ページで、表示するクラスターを含むプロジェクトを選択します。
4. 「システム」ページでクラスターを選択すると、そのクラスターの詳細が表示されます。

ONTAPアラートを表示する

NetAppオンプレミスONTAP環境における問題または潜在的なリスクを表示します。 EMS 以外のアラートと

EMS アラートがいくつか表示されます。

データは5分ごとに更新されます。

次の重大度のONTAPアラートが表示されます。

- 致命的
- 警告
- 情報

次の影響領域に関するONTAPアラートを確認できます。

- 容量
- パフォーマンス
- 保護
- 可用性
- セキュリティ

キャッシュによりパフォーマンスが最適化されますが、このペインのデータが実際の値と最大 15 分間異なる可能性があります。

サポートされているシステム

- オンプレミスのONTAP NAS または SAN システムがサポートされています。
- Cloud Volumes ONTAPシステムはサポートされていません。

サポートされているデータソース

ONTAPで発生する特定のイベントに関するアラートを表示します。これらは、EMS とメトリックベースのアラートの組み合わせです。

ONTAPアラートの詳細については、 "ONTAPアラートについて" 。

表示される可能性のあるアラートのリストについては、以下を参照してください。 "ONTAPストレージの潜在的なリスクを表示する" 。

手順

1. NetApp Consoleメニューから、 ONTAPアラート ペインを確認します。
2. 必要に応じて、重大度レベルを選択してアラートをフィルタリングするか、影響領域に基づいてアラートを表示するようにフィルターを変更します。
3. ONTAPアラート ペインで [表示] を選択して、コンソール アラート ページに移動します。

ストレージパフォーマンス容量を表示

クラスターまたはCloud Volumes ONTAPシステムごとに使用されているストレージ パフォーマンス容量を確認し、パフォーマンス容量、レイテンシ、および IOPS がワークロードにどのような影響を与えているかを判断します。たとえば、重要なワークロードのレイテンシを最小限に抑え、IOPS とスループットを最大化する

ために、ワークロードをシフトする必要があることがわかる場合があります。

システムは、クラスターとシステムをパフォーマンス容量別に整理し、簡単に識別できるように、最も容量が大きいものを最初にリストします。

キャッシュによりパフォーマンスが最適化されますが、このペインのデータが実際の値と最大15 分間異なる可能性があります。

手順

1. NetApp Consoleメニューから、ストレージ パフォーマンス ペインを確認します。
2. ストレージ パフォーマンス ペインで [表示] を選択すると、パフォーマンス容量、IOPS、レイテンシに関するすべてのクラスターとCloud Volumes ONTAPシステム データが一覧表示される [パフォーマンス] ページに移動します。
3. クラスターを選択すると、System Manager でその詳細が表示されます。

所有しているライセンスとサブスクリプションを表示する

[Licenses and subscriptions]ペインで次の情報を確認します。

- 保有しているライセンスとサブスクリプションの合計数。
- 保有しているライセンスおよびサブスクリプションの種類ごとの数 (直接ライセンス、年間契約、またはPAYGO)。
- アクティブ、アクションが必要、または有効期限が近づいているライセンスとサブスクリプションの数。
- システムは、アクションが必要なライセンス タイプまたは有効期限が近づいているライセンス タイプの横にインジケーターを表示します。

データは5分ごとに更新されます。

キャッシュによりパフォーマンスが最適化されますが、このペインのデータが実際の値と最大15 分間異なる可能性があります。

手順

1. NetApp Consoleメニューから、 [Licenses and subscriptions]ペインを確認します。
2. [Licenses and subscriptions]ペインで [表示] を選択して、コンソールの[Licenses and subscriptions]ページに移動します。

ランサムウェア耐性ステータスの表示

NetApp Ransomware Resilienceデータ サービスを使用して、ワークロードがランサムウェア攻撃のリスクにさらされているかどうか、または保護されているかどうかを確認します。保護されているデータの合計量を確認したり、推奨されるアクションの数を表示したり、ランサムウェア保護に関連するアラートの数を表示したりできます。

データは 5 分ごとに更新され、 NetApp Ransomware Resilience Dashboard に表示されるデータと一致します。

"NetApp Ransomware Resilienceについて学ぶ" 。

手順

1. NetApp Consoleメニューから、ランサムウェア耐性ペインを確認します。
2. ランサムウェア耐性ペインで次のいずれかを実行します。
   - 表示 を選択して、 NetApp Ransomware Resilienceダッシュボードに移動します。詳細については、"NetApp Ransomware Resilienceダッシュボードを使用してワークロードの健全性を監視する" 。
   - NetApp Ransomware Resilienceダッシュボードの「推奨アクション」を確認します。詳細については、 "NetApp Ransomware Resilienceダッシュボードで保護推奨事項を確認する" 。
   - アラート リンクを選択して、 NetApp Ransomware Resilience Alerts ページでアラートを確認します。詳細については、 "NetApp Ransomware Resilienceで検出されたランサムウェアアラートを処理する" 。

バックアップとリカバリのステータスを表示する

NetApp Backup and Recoveryからのバックアップと復元の全体的なステータスを確認します。保護されているリソースと保護されていないリソースの数を確認できます。ワークロードの保護のためのバックアップと復元操作の割合を確認することもできます。パーセンテージが高いほど、データ保護が強化されていることを示します。

データは5分ごとに更新されます。

キャッシュによりパフォーマンスが最適化されますが、このペインのデータが実際の値と最大15 分間異なる可能性があります。

手順

1. NetApp Consoleメニューから、[バックアップとリカバリ] ペインを確認します。
2. 表示 を選択して、 NetApp Backup and Recoveryダッシュボードに移動します。詳細については、"NetApp Backup and Recoveryのドキュメント" 。

NetApp Consoleのユーザー設定を管理する

パスワードの変更、多要素認証 (MFA) の有効化、コンソール管理者の確認など、コンソール プロファイルを変更できます。

コンソール内では、各ユーザーにはユーザーとその設定に関する情報が含まれるプロファイルがあります。プロフィール設定を表示および編集できます。

表示名を変更する

自分を識別するために使用され、他のユーザーに表示されるコンソールの表示名を変更できます。表示名はユーザー名やメール アドレスとは異なります。ユーザー名やメール アドレスは変更できません。

手順

1. コンソールの右上隅にあるプロフィール アイコンを選択して、ユーザー設定パネルを表示します。
2. 名前の横にある*編集*アイコンを選択します。
3. 名前 フィールドに新しい表示名を入力します。

多要素認証を設定する

2 番目の検証方法を必須にしてセキュリティを強化するには、多要素認証 (MFA) を構成します。

外部 ID プロバイダーまたはNetAppサポート サイトでシングル サインオンを使用するユーザーは、MFA を有効にできません。これらのいずれかに該当する場合、プロフィール設定で MFA を有効にするオプションは表示されません。

ユーザー アカウントが API アクセスに使用されている場合は、MFA を有効にしないでください。ユーザー アカウントに対して多要素認証を有効にすると、API アクセスが停止されます。すべての API アクセスにサービス アカウントを使用します。

開始する前に

- Google Authenticator や Microsoft Authenticator などの認証アプリをデバイスにダウンロードしておく必要があります。
- MFA を設定するにはパスワードが必要です。

認証アプリにアクセスできない場合、または回復コードを紛失した場合は、コンソール管理者に問い合わせてください。

手順

1. コンソールの右上隅にあるプロフィール アイコンを選択して、ユーザー設定パネルを表示します。
2. *多要素認証*ヘッダーの横にある*構成*を選択します。
3. 指示に従ってアカウントの MFA を設定します。
4. 完了すると、リカバリコードを保存するように求められます。コードをコピーするか、コードを含むテキスト ファイルをダウンロードするかを選択します。このコードを安全な場所に保管してください。認証アプリにアクセスできなくなった場合は、回復コードが必要になります。

   MFA を設定すると、コンソールにログインするたびに、認証アプリからのワンタイム コードを入力するように求められます。

MFA回復コードを再生成する

リカバリコードは 1 回のみ使用できます。使用済みまたは紛失した場合は、新しいものを作成してください。

手順

1. コンソールの右上隅にあるプロフィール アイコンを選択して、ユーザー設定パネルを表示します。
2. 選択 ••• *多要素認証*ヘッダーの横。
3. *リカバリコードの再生成*を選択します。
4. 生成されたリカバリコードをコピーし、安全な場所に保存します。

MFA設定を削除する

ログインに多要素認証 (MFA) の使用を停止するには、MFA 構成を削除します。これにより、ログイン時に認証アプリからワンタイムコードを入力する必要がなくなります。

認証アプリまたは回復コードにアクセスできない場合は、組織の管理者に連絡して MFA 構成をリセットする必要があります。

手順

1. コンソールの右上隅にあるプロフィール アイコンを選択して、ユーザー設定パネルを表示します。
2. 選択 ... *多要素認証*ヘッダーの横。
3. *削除*を選択します。

組織管理者にお問い合わせください

組織の管理者に連絡する必要がある場合は、コンソールから直接メールを送信できます。管理者は、組織内のユーザー アカウントと権限を管理します。

*管理者に連絡*機能を使用するには、ブラウザにデフォルトの電子メール アプリケーションが設定されている必要があります。

手順

1. コンソールの右上隅にあるプロフィール アイコンを選択して、ユーザー設定パネルを表示します。
2. 組織の管理者にメールを送信するには、[管理者に連絡] を選択します。
3. 使用する電子メール アプリケーションを選択します。
4. メールを終了し、[送信] を選択します。

ダークモード（ダークテーマ）を設定する

コンソールをダークモードで表示するように設定できます。

手順

1. コンソールの右上隅にあるプロフィール アイコンを選択して、ユーザー設定パネルを表示します。
2. ダーク テーマ スライダーを動かして有効にします。

NetApp Consoleの管理

アイデンティティとアクセス管理

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 Console内の ID およびアクセス管理 (IAM) を使用すると、 NetAppリソースへのアクセスを整理および制御できます。組織の階層に従ってリソースを整理できます。たとえば、地理的な場所、サイト、またはビジネス ユニット別にリソースを整理できます。その後、階層の特定の部分のメンバーに IAM ロールを割り当てて、階層の他の部分にあるリソースへのアクセスを防ぐことができます。

- "コンソールの展開モードについて学ぶ"

IAMの動作

IAM を使用すると、階層の特定の部分へのアクセス ロールをユーザーに割り当てることで、リソースへのアクセスを許可できます。たとえば、5 つのリソースを持つプロジェクトのフォルダー管理者またはプロジェクト管理者の役割をメンバーに割り当てることができます。

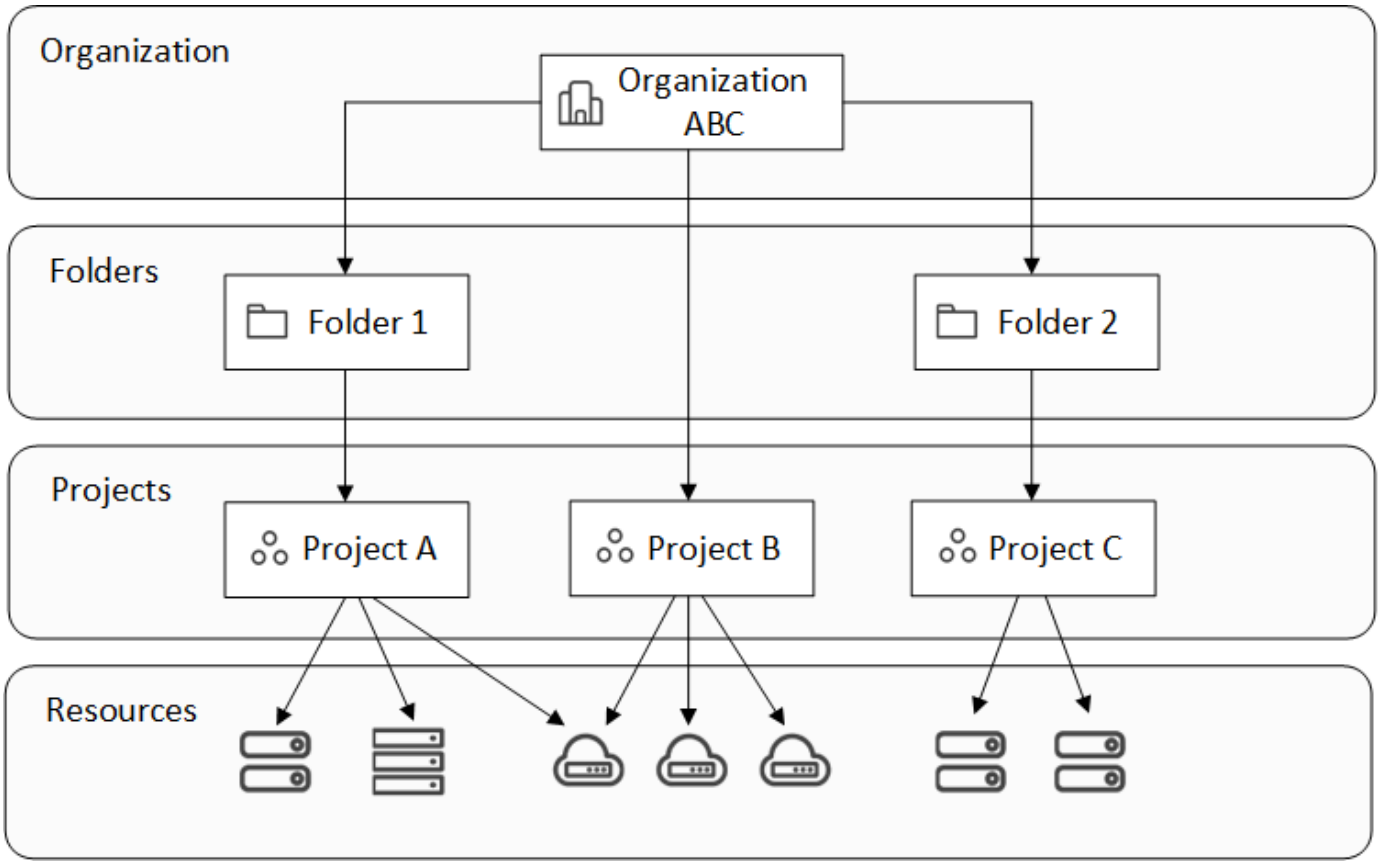
IAM を使用する場合、次のコンポーネントを管理します。

- 組織
- フォルダ
- プロジェクト
- リソース
- メンバー
- ロールと権限
- コンソールエージェント

リソースは階層的に編成されます。

- 組織は階層の最上位にあります。
- フォルダーは、組織または別のフォルダーの子です。
- プロジェクトは組織またはフォルダーの子です。
- リソースは 1 つ以上のフォルダーまたはプロジェクトに関連付けられます。

次の図は、この階層を基本レベルで示しています。



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。

フォルダ

_フォルダー_を使用すると、関連するプロジェクトをグループ化し、組織内の他のプロジェクトから分離することができます。たとえば、フォルダーは地理的な場所 (EU または米国東部)、サイト (ロンドンまたはトロント)、またはビジネス ユニット (エンジニアリングまたはマーケティング) を表す場合があります。

フォルダーを整理して、プロジェクト、他のフォルダー、またはその両方を含めることができます。これらはオプションです。

プロジェクト

プロジェクト は、組織のメンバーがリソースを管理するために システム ページからアクセスするコンソールのワークスペースを表します。たとえば、プロジェクトには、 Cloud Volumes ONTAPシステム、オンプレミスのONTAPクラスター、または FSx for ONTAPファイル システムを含めることができます。

組織は 1 つまたは複数のプロジェクトを持つことができます。プロジェクトは、組織の直下またはフォルダー内に配置できます。

リソース

リソース は、コンソールで作成または検出されたシステムです。

リソースを作成または検出すると、そのリソースは現在選択されているプロジェクトに関連付けられます。このリソースを関連付ける唯一のプロジェクトである可能性があります。ただし、リソースを組織内の追加のプロジェクトに関連付けることもできます。

たとえば、 Cloud Volumes ONTAPシステムを 1 つの追加プロジェクトに関連付けることも、組織内のすべてのプロジェクトに関連付けることもできます。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。

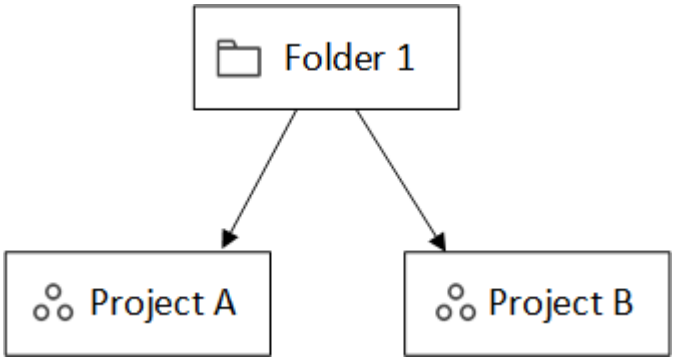
エージェントを複数のプロジェクトに関連付けることもできます。IAM でエージェントを使用する方法の詳細 。

リソースをフォルダに関連付けるタイミング

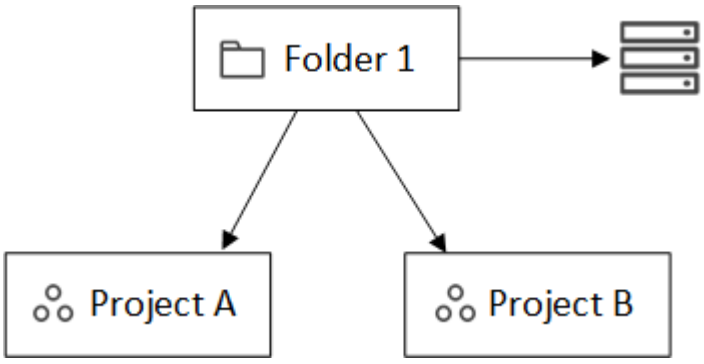
リソースをフォルダーに関連付けるオプションもありますが、これはオプションであり、特定のユースケースのニーズを満たすものです。

組織管理者 はリソースをフォルダーに関連付けることができるため、フォルダーまたはプロジェクト管理者 はリソースをフォルダー内の適切なプロジェクトにリンクできます。

たとえば、次の 2 つのプロジェクトを含むフォルダーがあるとします。

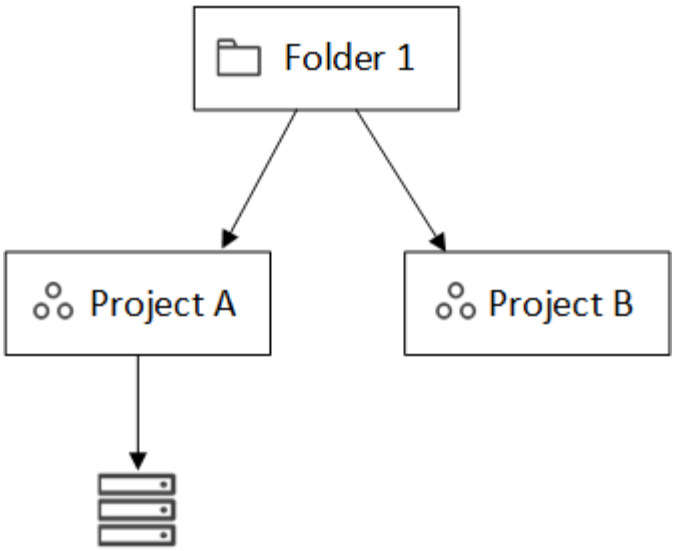


組織管理者は、リソースをフォルダに関連付けることができます。



リソースをフォルダーに関連付けても、すべてのプロジェクトがそのリソースにアクセスできるようになるわけではありません。フォルダーまたはプロジェクトの管理者 のみがそれを表示できます。 フォルダーまたはプロジェクト管理者 は、どのプロジェクトがアクセスできるかを決定し、リソースを適切なプロジェクトに関連付けます。

この例では、管理者はリソースをプロジェクト A に関連付けます。



プロジェクト A の権限を持つメンバーは、リソースにアクセスできるようになりました。

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。

各組織には、組織管理者 ロールを持つユーザーが少なくとも 1 人含まれます (コンソールは、組織を作成したユーザーにこのロールを自動的に割り当てます)。組織に他のメンバーを追加し、リソース階層のさまざまなレベルにわたって異なる権限を割り当てることができます。

ロールと権限

組織のメンバーに直接権限を付与することはありません。代わりに、各メンバーにロールを付与します。ロールには、メンバーがリソース階層の特定のレベルで特定のアクションを実行できるようにする一連の権限が含まれています。

階層レベルでロールを付与すると、メンバーが必要とするリソースとサービスへのアクセスが制限されます。

階層内で役割を割り当てることができる場所

メンバーをロールに関連付ける場合は、組織全体、特定のフォルダー、または特定のプロジェクトを選択する必要があります。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。

役割の継承

ロールを割り当てると、そのロールは組織階層の下位に継承されます。

組織

組織レベルでメンバーにアクセス ロールを付与すると、すべてのフォルダ、プロジェクト、リソースへの権限が付与されます。

フォルダ

フォルダー レベルでアクセス ロールを付与すると、フォルダー内のすべてのフォルダー、プロジェクト、リソースがそのロールを継承します。

たとえば、フォルダー レベルでロールを割り当て、そのフォルダーに 3 つのプロジェクトがある場合、メンバーにはそれらの 3 つのプロジェクトと関連するリソースに対する権限が付与されます。

プロジェクト

プロジェクト レベルでアクセス ロールを付与すると、そのプロジェクトに関連付けられているすべてのリソースがそのロールを継承します。

複数の役割

組織階層のさまざまなレベルで各組織メンバーにロールを割り当てることができます。同じ役割でも異なる役割でも構いません。たとえば、プロジェクト 1 とプロジェクト 2 にメンバー ロール A を割り当てることができます。または、プロジェクト 1 にメンバー ロール A を割り当て、プロジェクト 2 にロール B を割り当てることもできます。

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。

"アクセスロールについて学ぶ" 。

コンソールエージェント

組織管理者がコンソール エージェントを作成すると、コンソールはそのエージェントを組織および現在選択されているプロジェクトに自動的に関連付けます。 組織管理者 は、組織内のどこからでもそのエージェントに自動的にアクセスできます。ただし、組織内に異なる役割を持つ他のメンバーがいる場合、そのエージェントを他のプロジェクトに関連付けない限り、それらのメンバーは、そのエージェントが作成されたプロジェクトからのみそのエージェントにアクセスできます。

次の場合には、コンソール エージェントを別のプロジェクトで使用できるようにします。

- 組織内のメンバーが既存のエージェントを使用して、別のプロジェクトで追加のシステムを作成または検出できるようにしたい
- 既存のリソースを別のプロジェクトに関連付け、そのリソースはコンソール エージェントによって管理されています

  追加のプロジェクトに関連付けたリソースがコンソール エージェントを使用して検出された場合は、そのリソースが現在関連付けられているプロジェクトにエージェントを関連付ける必要もあります。そうしないと、組織管理者 ロールを持たないメンバーは、システム ページからエージェントとその関連リソースにアクセスできなくなります。

コンソール IAM 内の エージェント ページから関連付けを作成できます。

- コンソールエージェントをプロジェクトに関連付ける

  コンソール エージェントをプロジェクトに関連付けると、プロジェクトを表示するときに、システム ページからそのエージェントにアクセスできるようになります。

- コンソールエージェントをフォルダに関連付ける

  コンソール エージェントをフォルダーに関連付けても、そのエージェントがフォルダー内のすべてのプロジェクトから自動的にアクセス可能になるわけではありません。エージェントを特定のプロジェクトに関連付けるまで、組織のメンバーはプロジェクトからコンソール エージェントにアクセスできません。

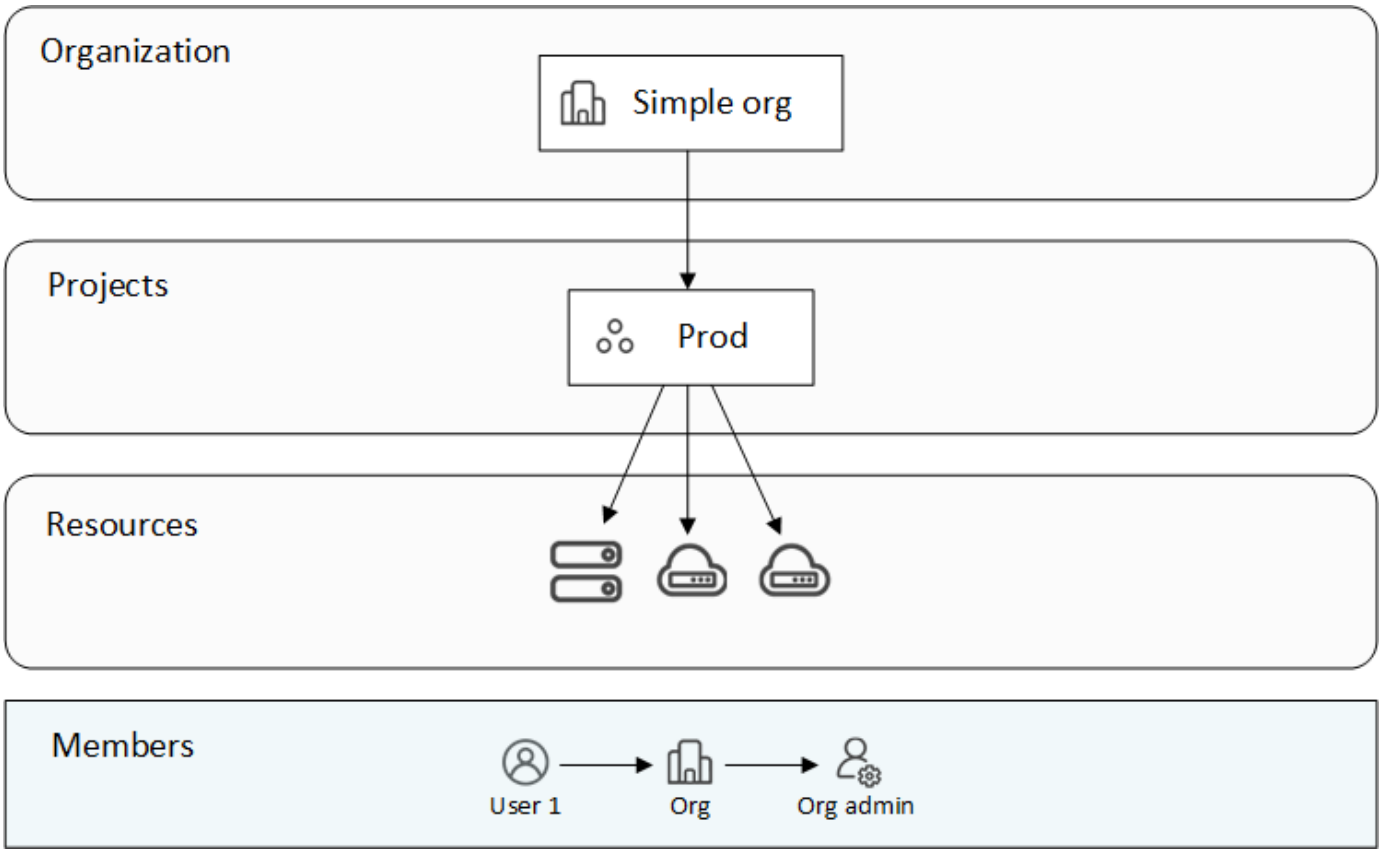
組織管理者 はコンソール エージェントをフォルダーに関連付けて、フォルダーまたはプロジェクト管理者 がそのエージェントをフォルダー内にある適切なプロジェクトに関連付ける決定を下せるようにすることができます。

IAMの例

これらの例は、組織をどのように設定するかを示しています。

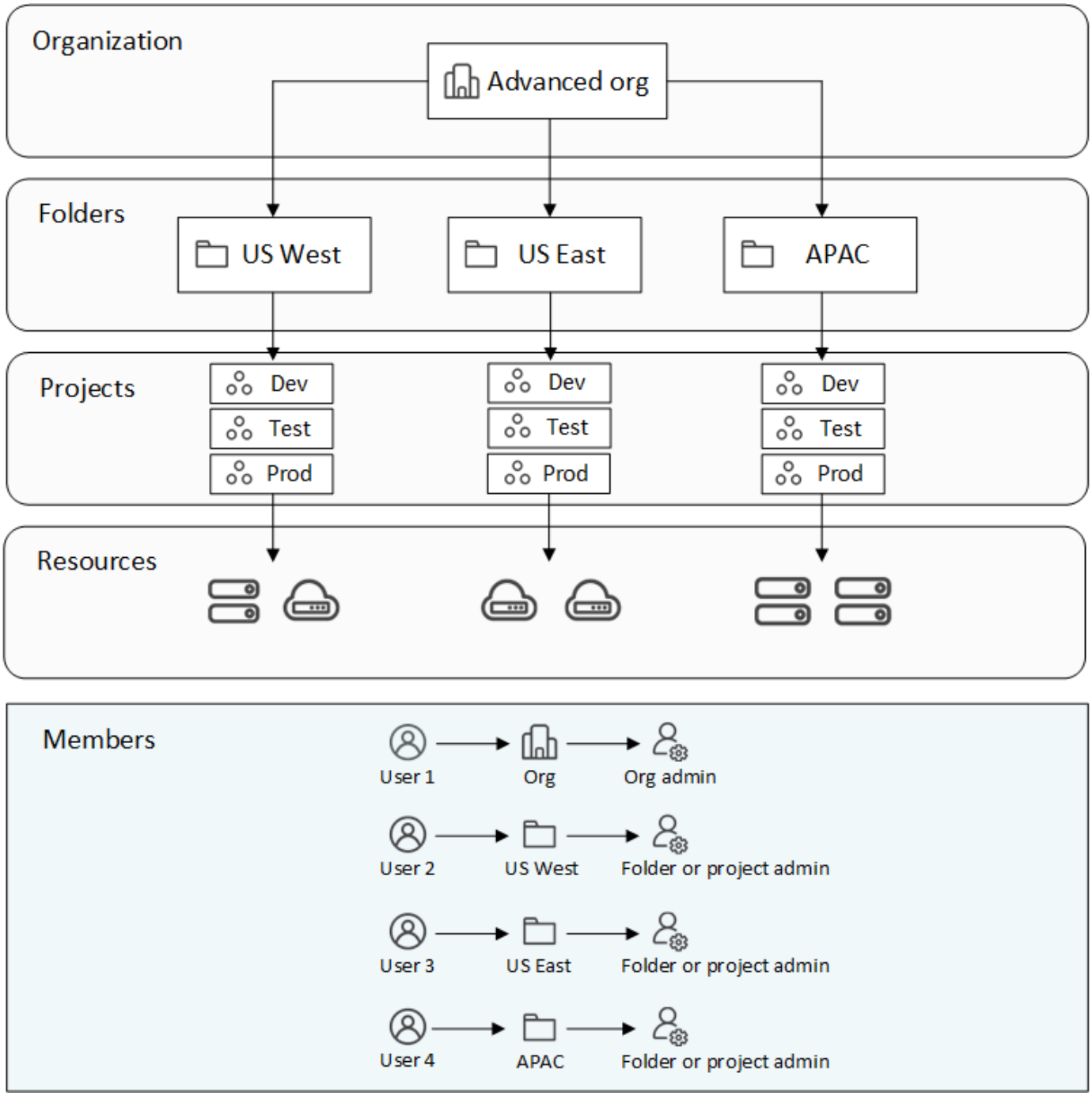
シンプルな構成

次の図は、デフォルトのプロジェクトを使用し、フォルダーを使用しない組織の簡単な例を示しています。 1人のメンバーが組織全体を管理します。



高度な組織

次の図は、フォルダーを使用してビジネス内の各地理的な場所のプロジェクトを整理する組織を示しています。各プロジェクトには、関連するリソースのセットが独自に存在します。メンバーには、組織管理者と組織内の各フォルダの管理者が含まれます。



IAMでできること

次の例では、IAM を使用してコンソール組織を管理する方法について説明します。

- 特定のメンバーに特定のロールを与えて、必要なタスクのみを完了できるようにします。
- 部署が異動になった場合や、追加の責任がある場合などに、メンバーの権限を変更します。
- 退職したユーザーを削除します。
- 新しいビジネス ユニットがNetAppストレージを追加したため、階層にフォルダーまたはプロジェクトを追加します。
- リソースには別のチームが利用できる容量があるため、そのリソースを別のプロジェクトに関連付けます。

- メンバーがアクセスできるリソースを表示します。
- 特定のプロジェクトに関連付けられているメンバーとリソースを表示します。

次はどこへ行くか

- "NetApp ConsoleでIAMを使い始める"
- "NetApp Consoleでフォルダとプロジェクトを使用してリソースを整理します"
- "NetApp Consoleのメンバーとその権限を管理する"
- "NetApp Console組織内のリソース階層を管理する"
- "エージェントをフォルダとプロジェクトに関連付ける"
- "NetApp Consoleのプロジェクトと組織を切り替える"
- "NetApp Console組織の名前を変更する"
- "IAMアクティビティを監視または監査する"
- "NetApp Consoleアクセスロール"
- "NetApp ConsoleIAMのAPIについて学ぶ"

NetApp ConsoleでIDとアクセスを開始する

NetApp Consoleにサインアップすると、新しい組織を作成するように求められます。組織には、メンバー 1 人 (組織管理者) とデフォルト プロジェクト 1 つが含まれます。ビジネス ニーズを満たすように ID およびアクセス管理 (IAM) を設定するには、組織の階層をカスタマイズし、メンバーを追加し、リソースを追加または検出し、それらのリソースを階層全体に関連付ける必要があります。

組織全体の ID とアクセスを管理するには、組織管理者 権限が必要です。 *フォルダーまたはプロジェクトの管理者*権限を持っている場合は、権限を持つフォルダーとプロジェクトのみを管理できます。

新しい組織を設定するには、次の手順に従ってください。順序は組織のニーズに応じて異なる場合があります。

1 デフォルトのプロジェクトを編集するか、組織の階層に追加します

デフォルトのプロジェクトを使用するか、ビジネス階層に一致する追加のプロジェクトとフォルダーを作成します。

"フォルダとプロジェクトを使ってリソースを整理する方法を学びます" 。

2 メンバーを組織に関連付ける

ユーザー アカウントを組織にリンクし、権限を割り当てます。組織にサービス アカウントを追加することもできます。

"メンバーとその権限を管理する方法を学ぶ" 。

3 リソースを追加または発見する

コンソールにリソース (システム) を追加または検出します。組織のメンバーはプロジェクト内からシステムを管理します。

リソースを作成または検出する方法を学びます。

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "Eシリーズシステム"
- "オンプレミスのONTAPクラスタ"
- "StorageGRID"

4 リソースを追加プロジェクトに関連付ける

コンソールでシステムを追加または検出すると、リソースが現在選択されているプロジェクトに自動的に関連付けられます。そのリソースを組織内の別のプロジェクトで使用できるようにするには、それぞれのプロジェクトに関連付けます。リソースの管理にコンソール エージェントを使用する場合は、コンソール エージェントをそれぞれのプロジェクトに関連付けます。

- "組織のリソース階層を管理する方法を学ぶ" 。
- "コンソールエージェントをフォルダまたはプロジェクトに関連付ける方法を学びます" 。

関連情報

- "NetApp Consoleのアイデンティティとアクセス管理について学ぶ"
- "IDとアクセスのためのAPIについて学ぶ"

NetApp Consoleのリソースをフォルダとプロジェクトで整理する

NetApp Console内で、プロジェクトとフォルダを使用してNetAppリソースを整理します。 プロジェクト は、組織のメンバーが リソース (たとえば、 Cloud Volumes ONTAP システム) を管理するためにアクセスするコンソールのワークスペースを表します。 フォルダー は関連するプロジェクトをグループ化します。リソースをフォルダーとプロジェクトに整理したら、組織のメンバーに特定のフォルダーとプロジェクトへの権限を付与することで、リソースへのきめ細かなアクセスを許可できます。

フォルダまたはプロジェクトを追加する

組織を作成すると、1 つのプロジェクトが含まれます。リソースを管理するためのプロジェクトと、関連するプロジェクトをグループ化するためのフォルダーを追加します。

組織のリソース階層は最大 7 レベルまで設定でき、フォルダーは 6 レベルまでネストされ、プロジェクトは 7 レベル目になります。

手順

1. *管理 > IDとアクセス*を選択します。
2. *組織*を選択します。
3. *組織*ページから、*フォルダーまたはプロジェクトの追加*を選択します。
4. *フォルダー*または*プロジェクト*を選択します。
5. フォルダーまたはプロジェクトの詳細を入力します。

    - 名前と場所: 名前を入力し、フォルダーまたはプロジェクトの階層内の場所を選択します。フォルダーまたはプロジェクトは、組織の直下またはフォルダー内に配置できます。
    - リソース: このフォルダーまたはプロジェクトに関連付けるリソースを選択します。

      親フォルダーまたはプロジェクトに関連付けられているリソースを選択できます。

      "リソースをフォルダに関連付けるタイミングを学ぶ" 。
    - アクセス: リソース階層で既に定義されている既存の権限に基づいて、フォルダーまたはプロジェクトにアクセスできるメンバーを表示します。

      追加のメンバーにアクセス権とロールを割り当てるには、「メンバーを追加」を選択します。ロールは、メンバーがフォルダーまたはプロジェクトに対して持つ権限を定義します。

    "アクセスロールについて学ぶ" 。
6. *追加*を選択します。

フォルダまたはプロジェクトの名前を変更する

必要に応じて、フォルダーとプロジェクトの名前を変更できます。

手順

1. *組織*ページで、テーブル内のプロジェクトまたはフォルダに移動し、•••次に、*フォルダーの編集*または*プロジェクトの編集*を選択します。
2. *編集*ページで新しい名前を入力し、*適用*を選択します。

フォルダまたはプロジェクトを削除する

不要になったフォルダーとプロジェクトを削除します。

開始する前に

- フォルダーまたはプロジェクトに関連付けられたリソースがないことを確認します。リソースの関連付けを解除する方法を学ぶ 。
- フォルダーまたはプロジェクトに関連付けられたリソースがないことを確認してください。

手順

1. *組織*ページで、テーブル内のプロジェクトまたはフォルダに移動し、•••次に、[削除] を選択します。
2. フォルダーまたはプロジェクトを削除することを確認します。

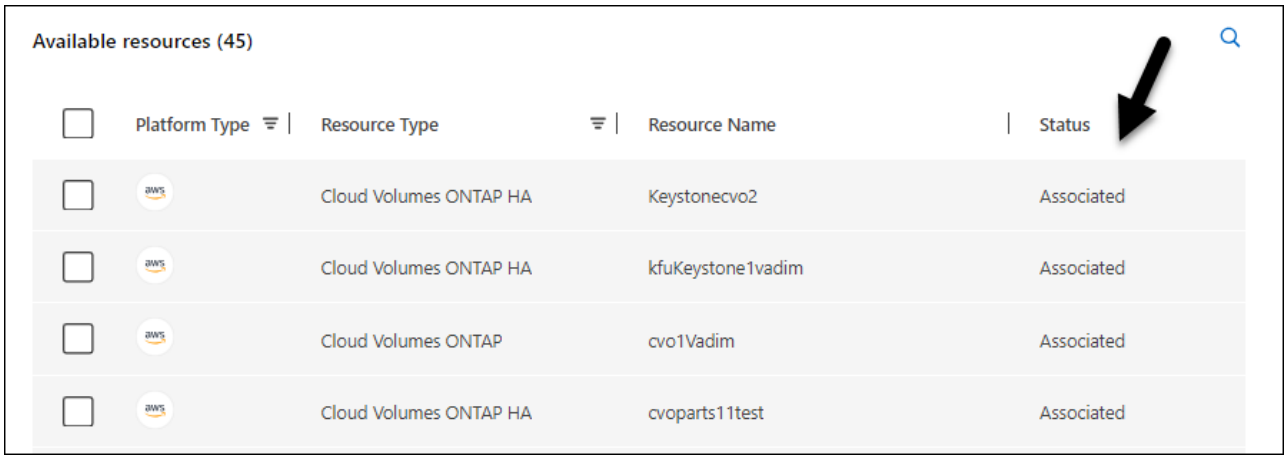
フォルダまたはプロジェクトに関連付けられたリソースを表示する

フォルダーまたはプロジェクトに関連付けられているリソースとメンバーを表示します。

手順

1. *組織*ページで、テーブル内のプロジェクトまたはフォルダに移動し、次に、*フォルダーの編集*または*プロジェクトの編集*を選択します。

2. *編集*ページでは、*リソース*または*アクセス*セクションを展開して、選択したフォルダーまたはプロジェクトの詳細を表示できます。
   - 関連するリソースを表示するには、[リソース] を選択します。表の ステータス 列には、フォルダーまたはプロジェクトに関連付けられているリソースが識別されます。



フォルダまたはプロジェクトに関連付けられたリソースを変更する

フォルダーまたはプロジェクトに対する権限を持つメンバーは、それに関連付けられたリソースにアクセスできます。

開始する前に

"リソースをフォルダに関連付けるタイミングを学ぶ" 。

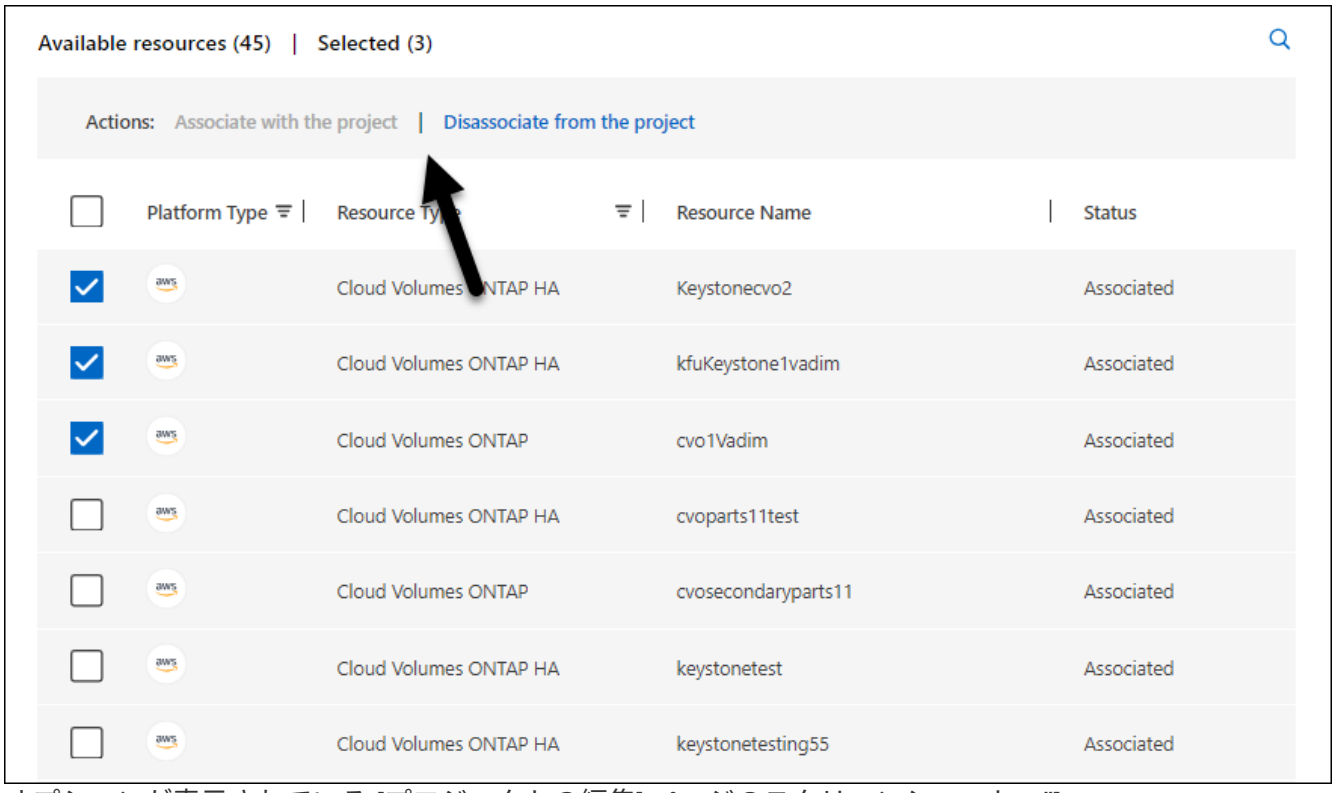
手順

1. *組織*ページで、テーブル内のプロジェクトまたはフォルダに移動し、次に、*フォルダーの編集*または*プロジェクトの編集*を選択します。
2. *編集*ページで*リソース*を選択します。

   表の ステータス 列には、フォルダーまたはプロジェクトに関連付けられているリソースが識別されま

す。

3. 関連付けまたは関連付けを解除するリソースを選択します。
4. 選択したリソースに応じて、*プロジェクトに関連付ける*または*プロジェクトとの関連付けを解除する*のいずれかを選択します。

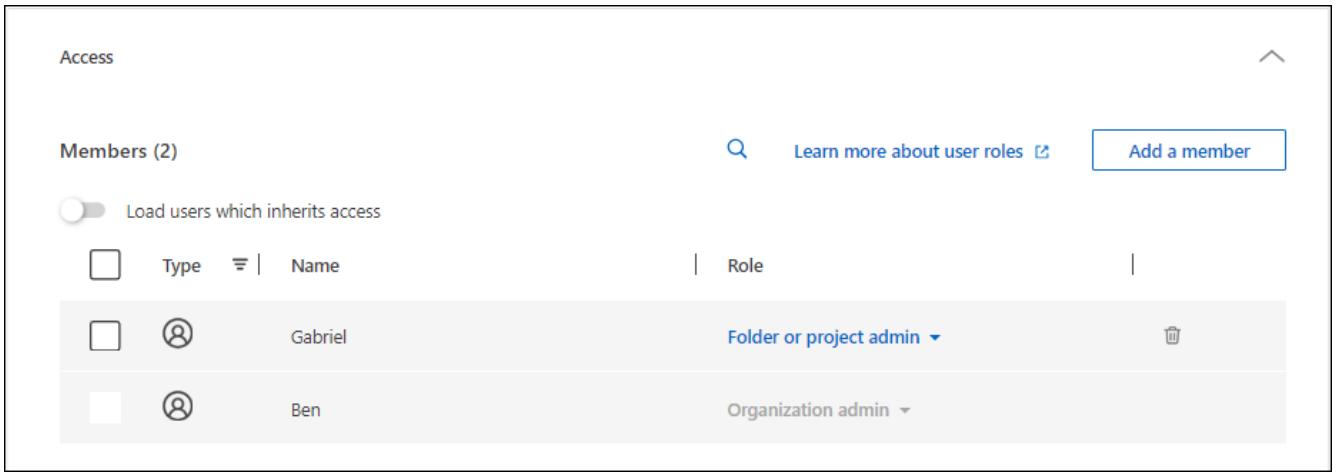


オプションが表示されている [プロジェクトの編集] ページのスクリーンショット。"]

5. *適用*を選択

フォルダまたはプロジェクトに関連付けられたメンバーを表示する

- フォルダーまたはプロジェクトにアクセスできるメンバーを表示するには、「アクセス」を選択します。



フォルダまたはプロジェクトへのメンバーアクセスを変更する

適切なメンバーが関連付けられたリソースにアクセスできるように、メンバー アクセスを変更します。

上位階層レベルで提供されるメンバー アクセスは、下位レベルでは変更できません。アクセスを変更するには、上位階層レベルでメンバーの権限を更新します。あるいは、"メンバーページから権限を管理する" 。

"ロール継承の詳細" 。

手順

1. *組織*ページで、テーブル内のプロジェクトまたはフォルダに移動し、•••次に、*フォルダーの編集*または*プロジェクトの編集*を選択します。
2. *編集*ページで*アクセス*を選択すると、選択したフォルダーまたはプロジェクトにアクセスできるメンバーのリストが表示されます。
3. メンバーアクセスの変更:
   - メンバーを追加: フォルダーまたはプロジェクトに追加するメンバーを選択し、役割を割り当てます。
   - メンバーの役割を変更する: 組織管理者以外の役割を持つメンバーの場合は、既存の役割を選択してから、新しい役割を選択します。
   - メンバーのアクセスを削除: 表示しているフォルダーまたはプロジェクトで定義されたロールを持つメンバーのアクセスを削除できます。
4. *適用*を選択します。

関連情報

- "NetApp ConsoleのIDとアクセスについて学ぶ"
- "アイデンティティとアクセスを始める"
- "アイデンティティとアクセスAPIについて学ぶ"

NetApp Consoleにメンバーとサービスアカウントを追加する

コンソール内で、ユーザーとサービス アカウントを組織に追加し、リソース階層全体で 1 つ以上のロールを割り当てることができます。 ロール には、メンバー (ユーザーまたはサービス アカウント) がリソース階層の特定のレベルで特定のアクションを実行できるようにする一連の権限が含まれています。

ユーザーと権限を管理するには、次のいずれかのロールが必要です。

- 組織管理者

  この役割を持つユーザーはすべてのメンバーを管理できます

- フォルダまたはプロジェクトの管理者

  この役割を持つユーザーは、指定されたフォルダまたはプロジェクトのメンバーのみを管理できます。

  フォルダーまたはプロジェクト管理者 は、メンバー ページですべてのメンバーを表示できますが、アクセス権を持つフォルダーとプロジェクトの権限のみを管理できます。"フォルダまたはプロジェクト管理者

が実行できるアクションの詳細" 。

組織にメンバーを追加する

組織には、ユーザー アカウントとサービス アカウントの 2 種類のメンバーを追加できます。アプリケーションはサービス アカウントを使用して、人間の介入なしに API タスクを実行します。通常、ユーザーはユーザー アカウントを使用してログインし、リソースを管理します。

ユーザーを組織に追加したり、ロールを割り当てたりする前に、そのユーザーがNetApp Consoleにサインアップする必要があります。サービス アカウントはコンソールから直接作成します。

ユーザーとその権限を管理するには、組織管理者 ロールまたは フォルダーまたはプロジェクト管理者 ロールが必要です。 フォルダーまたはプロジェクト管理者 ロールを持つユーザーは、管理者権限を持つフォルダーまたはプロジェクトのメンバーのみを管理できることに注意してください。

ユーザーアカウントを追加する

ユーザーはNetApp Consoleに自分でサインアップしますが、コンソールのリソースにアクセスするには、組織または特定のフォルダやプロジェクトに明示的に追加する必要があります。

手順

1. ユーザーを訪問するように誘導する "NetApp Console"サインアップしてください。

   ユーザーはサインアップすると、サインアップ ページを完了し、メールを確認してログインします。コンソールで組織の作成を要求された場合は、コンソールを閉じてアカウント作成を通知します。その後、ユーザーを既存の組織に追加できます。

   "NetApp Consoleへのサインアップ方法を学ぶ" 。

2. *管理 > IDとアクセス*を選択します。
3. *メンバー*を選択します。
4. *メンバーを追加*を選択します。
5. *メンバータイプ*では*ユーザー*を選択したままにします。
6. *ユーザーのメール*には、ユーザーが作成したログインに関連付けられているメール アドレスを入力します。
7. *組織、フォルダ、またはプロジェクトを選択*セクションを使用して、メンバーに権限を与えるリソース階層のレベルを選択します。

   次の点に注意してください。

   - 権限を持つフォルダーとプロジェクトからのみ選択できます。
   - 組織またはフォルダを選択すると、そのすべてのコンテンツに対する権限がメンバーに付与されます。
   - 組織管理者 ロールは組織レベルでのみ割り当てることができます。
8. *カテゴリを選択*し、選択した組織、フォルダ、またはプロジェクトに関連付けられているリソースに対する権限をメンバーに付与する*ロール*を選択します。

   "アクセスロールについて学ぶ" 。

9. オプション: 追加の役割またはプロジェクトを選択します。組織内の追加のフォルダーまたはプロジェクトへのアクセスを提供したり、選択した領域でユーザーに追加のロールを与えたりする場合は、「ロールの追加」を選択し、別のフォルダーまたはプロジェクト、あるいは別のロール カテゴリを指定してから、ロールを選択します。
10. *追加*を選択します。

    コンソールはユーザーに手順を記載した電子メールを送信します。

サービスアカウントを追加する

サービス アカウントを使用すると、タスクを自動化し、コンソール API と安全に統合できます。サービス アカウントを作成するときは、クライアント ID とシークレットを使用するか、JWT (JSON Web Token) 認証を使用するかの 2 つの認証方法から選択します。クライアント ID とシークレット方式はシンプルなセットアップに適しており、JWT 認証は自動化された環境やクラウドネイティブ環境に対してより強力なセキュリティを提供します。セキュリティ ニーズとコンソールの使用方法に最適なオプションを選択します。

JWT 認証を使用する場合は、公開キーまたは証明書を用意しておいてください。

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。
3. *メンバーを追加*を選択します。
4. *メンバータイプ*では*サービスアカウント*を選択します。
5. サービス アカウントの名前を入力します。
6. JWT 認証を使用する場合は、「秘密鍵 **JWT** 認証を使用する」を選択し、公開 RSA キーまたは証明書をアップロードします。代わりにクライアント ID とシークレットを使用する場合は、この手順をスキップしてください。

    X.509 証明書。 PEM、CRT、または CER 形式である必要があります。

7. *組織、フォルダ、またはプロジェクトを選択*セクションを使用して、メンバーに権限を与えるリソース階層のレベルを選択します。

    次の点に注意してください。

    - 権限を持つフォルダーとプロジェクトからのみ選択できます。
    - 組織またはフォルダを選択すると、そのすべてのコンテンツに対する権限がメンバーに付与されます。
    - 組織管理者 ロールは組織レベルでのみ割り当てることができます。
8. *カテゴリー*を選択し、選択した組織、フォルダ、またはプロジェクトに関連付けられているリソースに対する権限をメンバーに付与する*ロール*を選択します。

    "アクセスロールについて学ぶ" 。

9. オプション: 追加の役割またはプロジェクトを選択します。組織内の追加のフォルダーまたはプロジェクトへのアクセスを提供したり、選択した領域でユーザーに追加のロールを与えたりする場合は、「ロールの追加」を選択し、別のフォルダーまたはプロジェクト、あるいは別のロール カテゴリを指定してから、ロールを選択します。

10. JWT 認証を使用しない場合は、クライアント ID とクライアント シークレットをダウンロードまたはコピーします。 + コンソールにはクライアント シークレットが 1 回だけ表示されます。安全にコピーしておけば、必要に応じて後で再作成できます。
11. JWT 認証を選択した場合は、クライアント ID と JWT オーディエンスをダウンロードまたはコピーします。この情報は一度だけ表示され、後で取得することはできません。
12. *閉じる*を選択します。

組織メンバーを表示

メンバーが利用できるリソースと権限を理解するには、組織のリソース階層のさまざまなレベルでメンバーに割り当てられているロールを表示できます。"ロールを使用してコンソール リソースへのアクセスを制御する方法を学習します。"

メンバー ページからユーザー アカウントとサービス アカウントの両方を表示できます。

特定のフォルダーまたはプロジェクトに関連付けられているすべてのメンバーを表示することもできます。"詳細情報" 。

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。

   メンバー テーブルには組織のメンバーがリストされます。

3. *メンバー*ページで、テーブル内のメンバーに移動し、 次に、[詳細を表示] を選択します。

組織からメンバーを削除する

たとえば、メンバーが会社を辞めた場合など、組織からメンバーを削除する必要がある場合があります。

システムはメンバーの権限を削除しますが、コンソールとNetAppサポート サイトのアカウントは保持されます。

手順

1. メンバー*ページで、テーブル内のメンバーに移動し、 次に、[*ユーザーの削除]を選択します。
2. 組織からメンバーを削除することを確認します。

サービス アカウントの認証情報を再作成する

資格情報を紛失した場合や更新する必要がある場合は、新しい資格情報を作成してください。

資格情報を再作成する場合は、サービス アカウントの既存の資格情報を削除し、新しい資格情報を作成します。以前の資格情報は使用できません。

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。
3. メンバー*テーブルでサービスアカウントに移動し、 次に、[*シークレットの再作成]を選択します。

4. *再作成*を選択します。
5. クライアント ID とクライアント シークレットをダウンロードまたはコピーします。 + クライアントシークレットは 1 回だけ表示されます。コピーまたはダウンロードして安全に保管してください。

ユーザーの多要素認証（**MFA**）を管理する

ユーザーが MFA デバイスにアクセスできなくなった場合は、MFA 構成を削除するか無効にすることができます。

削除後、ユーザーはログイン時に MFA を再設定する必要があります。ユーザーが MFA デバイスへのアクセスを一時的に失っただけの場合は、MFA を設定したときに保存した回復コードを使用してログインできます。

回復コードがない場合は、一時的に MFA を無効にしてログインを許可します。ユーザーの MFA を無効にすると、8 時間だけ無効になり、その後自動的に再度有効になります。その間、ユーザーは MFA なしで 1 回のログインが許可されます。8 時間経過後、ユーザーは MFA を使用してログインする必要があります。

ユーザーの多要素認証を管理するには、影響を受けるユーザーと同じドメインのメール アドレスが必要です。

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*を選択します。

   メンバー テーブルには組織のメンバーがリストされます。
3. メンバー*ページで、テーブル内のメンバーに移動し、 次に、[*多要素認証の管理]を選択します。
4. ユーザーの MFA 構成を削除するか無効にするかを選択します。

ロールを使用して、 **NetApp Console**リソースへのユーザー アクセスを管理します。

コンソール内では、ユーザーの実行内容と場所に基づいて、ユーザーにロールを割り当てることができます。

組織管理者 または フォルダーまたはプロジェクト管理者 の役割を持つユーザーには、他のユーザーに役割を割り当てる責任があります。プロジェクトまたはフォルダーごとにアクセス ロールを割り当てることができます。たとえば、あるプロジェクトでは Ransomware Resilience 管理者ロールをユーザーに割り当てることができ、別のプロジェクトではSnapCenter管理者ロールを割り当てることができます。あるいは、ユーザーが特定のフォルダー内のすべてのプロジェクトに対して分類管理者ロールを必要とする場合は、フォルダー レベルでこのロールを付与できます。

アクセス ロールを使用して、ユーザーが実行する必要がある特定のタスクに基づいてストレージ リソースへのアクセスを割り当てます。たとえば、ユーザーが Ransomware Resilience と対話する必要がある場合、アクセス ロールが付与されているプロジェクトの Ransomware Resilience の表示権限または管理権限のいずれかを含むアクセス ロールをユーザーに付与する必要があります。

セキュリティを強化するために、IAM 戦略に基づいてユーザーにロールを割り当てます。 IAM ロールにより、ユーザーは必要なアクセス権のみを持つことができます。

リソースへのアクセスを直接許可することはできないことに注意してください。まずプロジェクトにリソースを割り当てます。ユーザーにアクセスを割り当てる前に、リソース階層を設定することを検討してください。"フォルダーとプロジェクトを使用してリソースを整理する方法を学びます。"

メンバーに割り当てられた役割を表示する

組織にメンバーを追加すると、そのメンバーにロールを割り当てるように求められます。メンバーに現在割り当てられているロールを確認できます。

フォルダーまたはプロジェクト管理者 ロールを持っている場合、ページには組織内のすべてのメンバーが表示されます。ただし、メンバー権限を表示および管理できるのは、権限を持つフォルダーとプロジェクトのみです。"フォルダまたはプロジェクト管理者が実行できるアクションの詳細" 。

1. *メンバー*ページで、テーブル内のメンバーに移動し、次に、[詳細を表示] を選択します。
2. 表で、メンバーに割り当てられたロールを表示する組織、フォルダ、またはプロジェクトのそれぞれの行を展開し、「ロール」列で「表示」を選択します。

メンバーにアクセスロールを追加する

通常、組織にメンバーを追加するときにロールを割り当てますが、ロールを削除または追加することでいつでも更新できます。

組織、フォルダ、またはプロジェクトへのアクセス ロールをユーザーに割り当てることができます。

メンバーは、同じプロジェクト内および異なるプロジェクト内で複数の役割を持つことができます。たとえば、小規模な組織では、利用可能なすべてのアクセス ロールを同じユーザーに割り当てる場合がありますが、大規模な組織では、ユーザーにさらに専門的なタスクを実行させる場合があります。あるいは、組織の Ransomware Resilience 管理者ロールを 1 人のユーザーに割り当てることもできます。この例では、ユーザーは組織内のすべてのプロジェクトでランサムウェア耐性タスクを実行できるようになります。

アクセス ロール戦略は、 NetAppリソースの編成方法と一致する必要があります。

組織管理者の役割が割り当てられているメンバーには、追加の役割を割り当てることはできません。組織全体にわたる権限がすでに付与されています。フォルダーまたはプロジェクトのロールを持つメンバーには、そのロールがすでに割り当てられているフォルダーまたはプロジェクト内の他のロールを割り当てることはできません。これら両方のロールは、割り当てられた範囲内のすべてのサービスへのアクセスを提供します。

手順

1. *管理 > IDとアクセス*を選択します。
2. アクションメニューを選択役割を割り当てるメンバーの横にある をクリックし、[役割の追加] を選択します。
3. ロールを追加するには、ダイアログ ボックスの手順を完了します。
   - 組織、フォルダ、またはプロジェクトを選択: メンバーに権限を与えるリソース階層のレベルを選択します。

     組織またはフォルダを選択した場合、メンバーにはその組織またはフォルダ内に存在するすべてのものに対する権限が付与されます。

- カテゴリを選択: 役割のカテゴリを選択します。"アクセスロールについて学ぶ" 。
- *ロール*を選択: 選択した組織、フォルダ、またはプロジェクトに関連付けられているリソースに対する権限をメンバーに付与するロールを選択します。
- ロールの追加: 組織内の追加のフォルダーまたはプロジェクトへのアクセス権を付与する場合は、*ロールの追加*を選択し、別のフォルダーまたはプロジェクトまたはロールのカテゴリを指定してから、ロールのカテゴリと対応するロールを選択します。

4. *新しいロールを追加*を選択します。

メンバーに割り当てられた役割を変更する

ユーザーのアクセスを調整する必要がある場合は、メンバーに割り当てられたロールを変更できます。

ユーザーには少なくとも 1 つのロールが割り当てられている必要があります。ユーザーからすべてのロールを削除することはできません。すべてのロールを削除する必要がある場合は、組織からユーザーを削除する必要があります。

手順

1. *管理 > IDとアクセス*を選択します。
2. *メンバー*ページで、テーブル内のメンバーに移動し、次に、[詳細を表示] を選択します。
3. 表で、メンバーに割り当てられたロールを変更する組織、フォルダ、またはプロジェクトのそれぞれの行を展開し、「ロール」列で「表示」を選択して、このメンバーに割り当てられているロールを表示します。
4. メンバーの既存の役割を変更したり、役割を削除したりできます。
   a. メンバーの役割を変更するには、変更したい役割の横にある「変更」を選択します。ロールを変更できるのは、同じロール カテゴリ内のロールのみです。たとえば、あるデータ サービス ロールから別のデータ サービス ロールに変更できます。変更を確認します。
   b. メンバーの役割の割り当てを解除するには、をクリックして、メンバーから該当のロールの割り当てを解除します。削除の確認を求められます。

NetApp Console組織内のリソース階層を管理する

メンバーを組織に関連付ける場合は、組織、フォルダ、またはプロジェクト レベルで権限を付与します。これらのメンバーが適切なリソースにアクセスする権限を持っていることを確認するには、リソースを特定のプロジェクトやフォルダに関連付けることで、組織のリソース階層を管理する必要があります。 リソース とは、コンソールが既に管理しているか認識しているストレージ システムまたはコンソール エージェントです。

組織内のリソースを表示する

組織に関連付けられている検出されたリソースと未検出のリソースの両方を表示できます。未検出のリソースは、識別されているがコンソールにまだ追加されていないストレージ リソースです。

注意: ユーザーがロールに関連付けることができないため、[リソース] ページではAmazon FSx for NetApp ONTAPリソースは除外されます。システム ページまたはワークロードから表示します。

手順

1. *管理 > IDとアクセス*を選択します。
2. *リソース*を選択します。
3. *高度な検索とフィルタリング*を選択します。
4. 利用可能なオプションのいずれかを使用して、探しているリソースを見つけます。
   - リソース名で検索: テキスト文字列を入力し、*追加*を選択します。
   - プラットフォーム: Amazon Web Services など、1 つ以上のプラットフォームを選択します。
   - リソース: Cloud Volumes ONTAPなどの 1 つ以上のリソースを選択します。
   - 組織、フォルダー、またはプロジェクト: 組織全体、特定のフォルダー、または特定のプロジェクトを選択します。
5. *検索*を選択します。

リソースをフォルダやプロジェクトに関連付ける

リソースをフォルダーまたはプロジェクトに関連付けて、利用できるようにします。

開始する前に

リソースの関連付けがどのように機能するかを理解する必要があります。"リソースについて、リソースをフォルダに関連付けるタイミングなどについて学習します。" 。

手順

1. リソース*ページで、テーブル内のリソースに移動し、 ••• 次に、[*フォルダーまたはプロジェクトに関連付ける]を選択します。
2. フォルダーまたはプロジェクトを選択し、[承認] を選択します。
3. 追加のフォルダーまたはプロジェクトを関連付けるには、[フォルダーまたはプロジェクトの追加] を選択し、フォルダーまたはプロジェクトを選択します。

   管理者権限を持つフォルダーとプロジェクトからのみ選択できることに注意してください。

4. *リソースの関連付け*を選択します。
   - リソースをプロジェクトに関連付けると、それらのプロジェクトに対する権限を持つメンバーは、コンソールからリソースにアクセスできるようになります。
   - リソースをフォルダーに関連付けると、フォルダーまたはプロジェクトの管理者がリソースにアクセスし、フォルダー内のプロジェクトに関連付けることができるようになります。"リソースをフォルダに関連付ける方法について学習します" 。

終了後の操作

コンソール エージェントを使用してリソースを検出する場合は、コンソール エージェントをプロジェクトに関連付けてアクセスを許可します。そうでない場合、組織管理者 ロールを持たないメンバーはコンソール エージェントとその関連リソースにアクセスできません。

"コンソールエージェントをフォルダまたはプロジェクトに関連付ける方法を学びます" 。

リソースに関連付けられたフォルダとプロジェクトを表示する

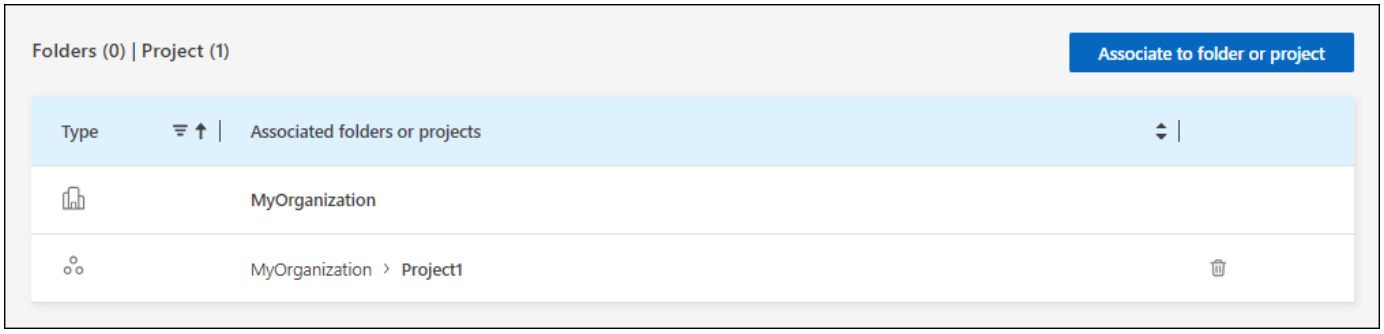
特定のリソースに関連付けられているフォルダーとプロジェクトを表示できます。

どの組織メンバーがリソースにアクセスできるのかを確認する必要がある場合は、"リソースに関連付けられているフォルダとプロジェクトにアクセスできるメンバーを表示します" 。

手順

1. *リソース*ページで、テーブル内のリソースに移動し、次に、[詳細を表示] を選択します。

次の例は、1 つのプロジェクトに関連付けられているリソースを示しています。



どの組織メンバーがリソースにアクセスできるのかを判断する必要がある場合は、"リソースに関連付けられているフォルダとプロジェクトにアクセスできるメンバーを表示します" 。

フォルダまたはプロジェクトからリソースを削除する

フォルダーまたはプロジェクトからリソースを削除するには、フォルダーまたはプロジェクトとリソース間の関連付けを削除する必要があります。関連付けを削除すると、メンバーはフォルダーまたはプロジェクト内のリソースを管理できなくなります。

検出されたリソースを組織全体から削除するには、システム ページからシステムを削除します。

手順

1. *リソース*ページで、テーブル内のリソースに移動し、次に、[詳細を表示] を選択します。
2. リソースを削除するフォルダまたはプロジェクトで、
3. 削除 を選択して、関連付けを削除することを確認します。

関連情報

- "NetApp ConsoleのIDとアクセスについて学ぶ"
- "NetApp ConsoleでIDとアクセスを開始する"
- "IDとアクセスのためのAPIについて学ぶ"

コンソールエージェントを他のフォルダやプロジェクトに関連付ける

組織管理者がコンソール エージェントを作成すると、そのコンソール エージェントは組織内で現在選択されているプロジェクトに自動的に関連付けられます。ただし、組織管理者 ロールを持つユーザーは、組織内のどこからでもそのコンソール エージェントにアクセスできます。組織内の他のメンバーは、そのコンソール エージェントを他のプロジェクトに関連付けない限り、そのコンソール エージェントが作成されたプロジェクトからのみそのコンソール エージェントにアクセスできます。

開始する前に

コンソール エージェントの関連付けの仕組みを確認します。"Identity and Access でコンソール エージェントを使用する方法について学習します" 。

タスク概要

フォルダーまたはプロジェクト管理者 は、エージェント ページですべてのコンソール エージェントを表示できますが、コンソール エージェントを関連付けることができるのは、権限を持つフォルダーおよびプロジェクトのみです。"フォルダまたはプロジェクト管理者が実行できるアクションの詳細" 。

手順

1. 管理 **> ID**とアクセス > *エージェント*を選択します。
2. 表から、関連付けるコンソール エージェントを見つけます。

   特定のコンソール エージェントを検索するには、表の上にある検索機能を使用するか、リソース階層で表をフィルター処理します。

3. コンソールエージェントにリンクされたフォルダとプロジェクトを表示するには、 ••• 次に、[詳細を表示] を選択します。

   このページには、コンソール エージェントに関連付けられているフォルダーとプロジェクトの詳細が表示されます。

4. *フォルダーまたはプロジェクトに関連付ける*を選択します。
5. フォルダーまたはプロジェクトを選択し、[承認] を選択します。
6. コンソール エージェントを追加のフォルダーまたはプロジェクトに関連付けるには、[フォルダーまたはプロジェクトの追加] を選択し、フォルダーまたはプロジェクトを選択します。
7. *Associate Agent*を選択します。

終了後の操作

コンソール エージェントのリソースを、リソース ページの同じフォルダーおよびプロジェクトに関連付けます。

"リソースをフォルダやプロジェクトに関連付ける方法を学びます" 。

関連情報

- "NetApp Consoleエージェントについて学ぶ"
- "NetApp Consoleのアイデンティティとアクセス管理について学ぶ"
- "アイデンティティとアクセスを始める"

- "IDとアクセス管理のためのAPIについて学ぶ"

コンソールの組織、プロジェクト、エージェントを切り替える

複数のコンソール組織に属している場合や、組織内の複数のプロジェクトまたはエージェントにアクセスする権限を持っている場合があります。必要に応じて、組織、プロジェクト、コンソール エージェント間を簡単に切り替えて、その組織、プロジェクト、またはエージェントに関連付けられているリソースにアクセスできます。

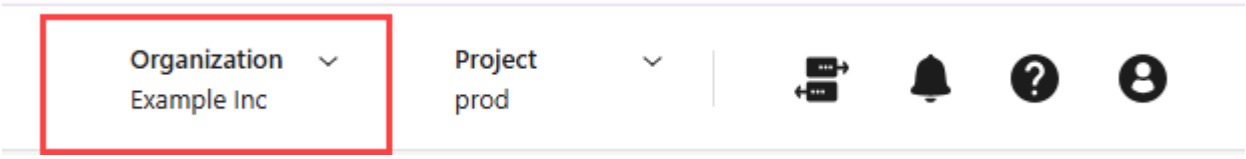
別の組織から参加を招待された場合、または自分で組織を作成した場合は、複数の組織に所属する可能性があります。 API を使用して追加の組織を作成できます。 "新しい組織を作成する方法を学ぶ"

組織間の切り替え

複数の組織のメンバーである場合は、いつでも組織を切り替えることができます。

手順

1. コンソールの上部のヘッダーで、*組織*を選択します。



2. パートナーシップ組織がある場合は、「パートナーシップ」タブを選択して、利用可能なパートナー組織を表示します。

+ パートナー組織がない場合、「パートナーシップ」タブは表示されません。

1. 別の組織を選択し、[切り替え] を選択します。

+ パートナーシップ組織がある場合は、[パートナーシップ] タブを選択して、利用可能なパートナー組織を表示します。

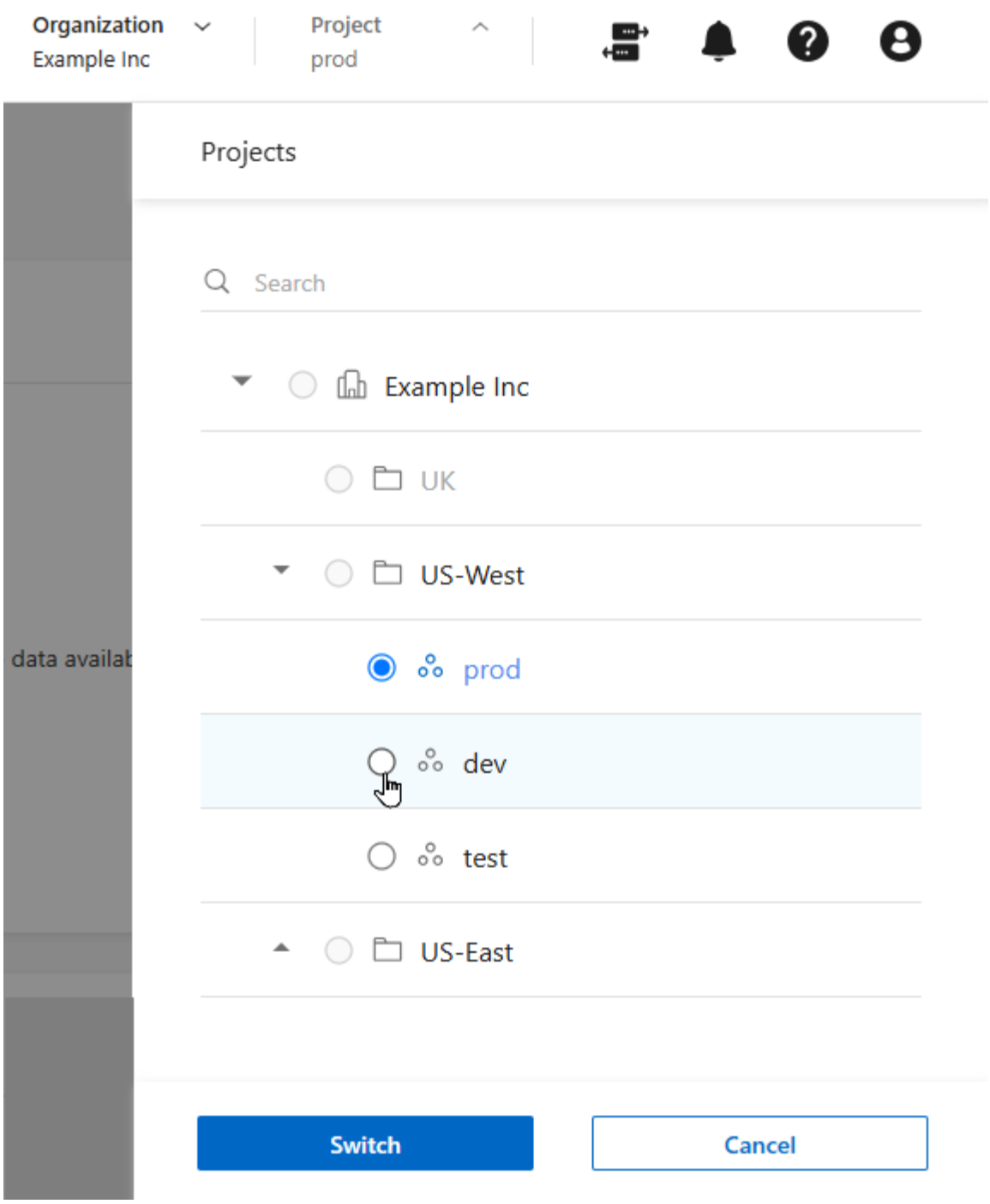
プロジェクト間の切り替え

組織に複数のプロジェクトが含まれており、それらのプロジェクトにアクセスできる場合は、いつでもプロジェクトを切り替えることができます。

ID とアクセス ページのいずれかを表示している間は、別のプロジェクトに切り替えることはできません。

手順

1. コンソールの上部のヘッダーで、*プロジェクト*を選択します。
2. 組織内のフォルダーとプロジェクトを参照し、必要なプロジェクトを選択して、[切り替え] を選択します。



コンソールエージェントを切り替える

複数のコンソール エージェントがある場合は、それらを切り替えて、特定のエージェントに関連付けられているシステムを表示できます。

手順

1. コンソールの上部ヘッダーで、エージェント アイコンを選択します。
2. 別のエージェントを選択し、[切り替え] を選択します。

関連情報

"エージェントをフォルダとプロジェクトに関連付ける" 。

関連情報

- "NetApp ConsoleのIDとアクセスについて学ぶ"
- "アイデンティティとアクセスを始める"
- "IDとアクセスのためのAPIについて学ぶ"

組織IDとプロジェクトID

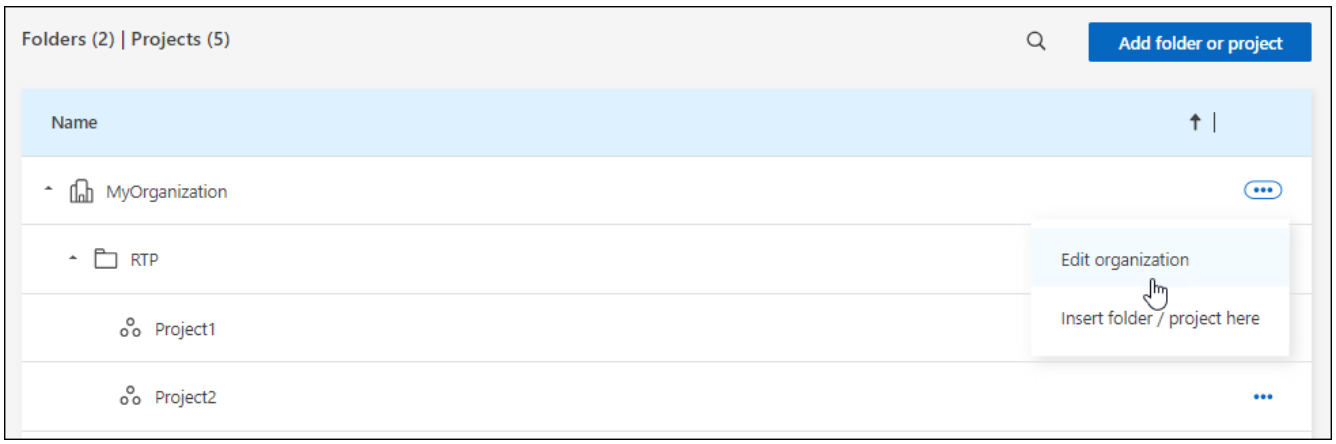
NetApp Console組織には名前と ID があります。組織を識別しやすいように、組織の名前を選択できます。特定の統合では組織 ID を取得する必要がある場合もあります。

組織名を変更する

組織の名前を変更できます。複数の組織をサポートする場合に役立ちます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *組織*を選択します。
3. *組織*ページで、表の最初の行に移動し、 次に、[組織の編集] を選択します。



4. 新しい組織名を入力し、「適用」を選択します。

組織IDを取得する

組織 ID は、コンソールとの特定の統合に使用されます。

組織ページから組織 ID を表示し、必要に応じてクリップボードにコピーすることができます。

手順

1. 管理 **> ID** とアクセス > 組織 を選択します。
2. 組織 ページの概要バーで組織 ID を探し、クリップボードにコピーします。これを後で使用するために保存することも、必要な場所に直接コピーすることもできます。

プロジェクトのIDを取得する

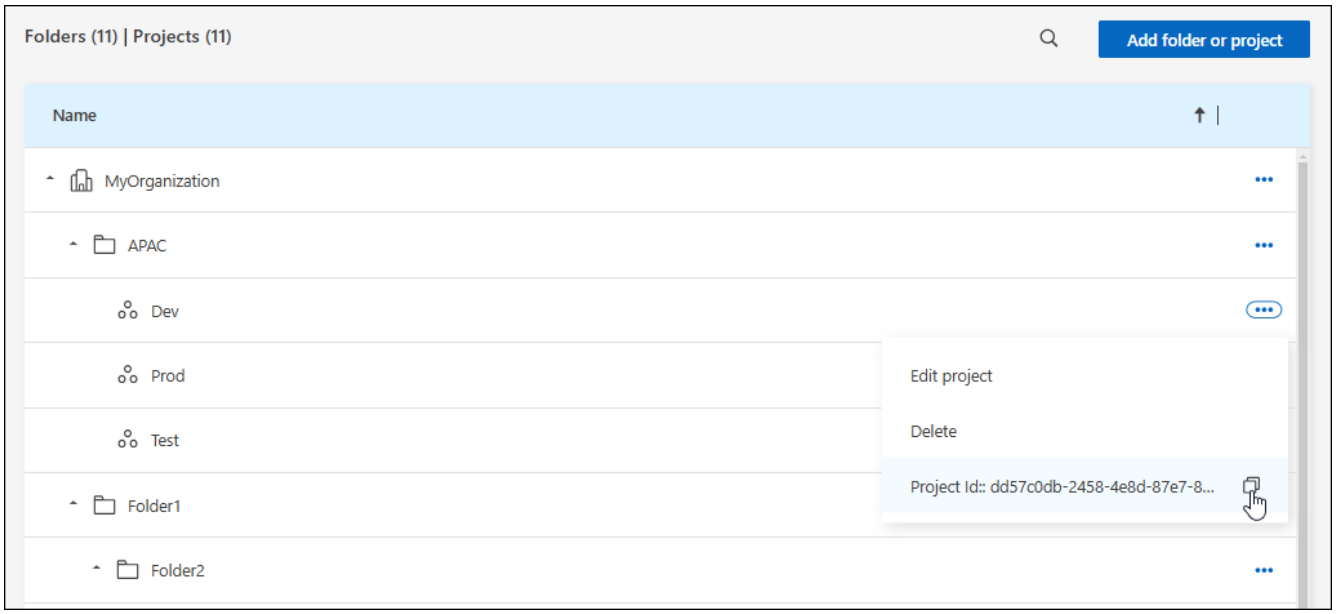
API を使用している場合は、プロジェクトの ID を取得する必要があります。たとえば、 Cloud Volumes ONTAPシステムを作成する場合などです。

手順

1. *組織*ページで、表内のプロジェクトに移動し、 •••

   プロジェクト ID が表示されます。

2. ID をコピーするには、コピー ボタンを選択します。



関連情報

- "アイデンティティとアクセス管理について学ぶ"
- "アイデンティティとアクセスを始める"
- "IDとアクセスのためのAPIについて学ぶ"

IAMアクティビティを監視または監査する

ID とアクセスに関連して完了したアクションを監視または監査する必要がある場合は、[監査] ページから詳細を表示できます。たとえば、誰が組織にメンバーを追加したか、またはプロジェクトが正常に削除されたかを確認したい場合があります。

手順

1. *管理 > 監査*を選択します。
2. *監査*ページで、フィルターを使用して結果を絞り込みます。 *サービス*を選択し、次に*テナンシー*を選択します。
3. 他のフィルターを使用して、テーブルに表示されるアクションを変更します。

   たとえば、ユーザー フィルターを使用して、特定のユーザー アカウントに関連するアクションを表示で

きます。

NetApp Consoleアクセスロール

NetApp Consoleのアクセスロールについて学ぶ

NetApp Consoleの ID およびアクセス管理 (IAM) では、リソース階層のさまざまなレベルにわたって組織のメンバーに割り当てることができる定義済みのロールが提供されます。これらのロールを割り当てる前に、各ロールに含まれる権限を理解しておく必要があります。ロールは、プラットフォーム、アプリケーション、データ サービスというカテゴリに分類されます。

プラットフォームの役割

プラットフォーム ロールは、ロールの割り当てやユーザー管理などのNetApp Console管理権限を付与します。コンソールにはいくつかのプラットフォーム ロールがあります。

プラットフォームの役割	責任
"組織管理者"	ユーザーは、組織内のすべてのプロジェクトとフォルダに無制限にアクセスでき、任意のプロジェクトまたはフォルダにメンバーを追加できるほか、任意のタスクを実行したり、明示的にロールが関連付けられていない任意のデータ サービスを使用したりできます。このロールを持つユーザーは、適切な資格情報を持っている場合、フォルダーとプロジェクトの作成、ロールの割り当て、ユーザーの追加、システムの管理を行うことで組織を管理します。これは、コンソール エージェントを作成できる唯一のアクセス ロールです。
"フォルダまたはプロジェクトの管理者"	割り当てられたプロジェクトとフォルダーへのユーザーの無制限アクセスを許可します。管理するフォルダーまたはプロジェクトにメンバーを追加できるほか、割り当てられたフォルダーまたはプロジェクト内のリソースに対して任意のタスクを実行したり、任意のデータ サービスやアプリケーションを使用したりすることもできます。フォルダーまたはプロジェクト管理者はコンソール エージェントを作成できません。
"連盟管理者"	ユーザーがコンソールを使用してフェデレーションを作成および管理し、シングル サインオン (SSO) を有効にすることを許可します。
"連盟ビューア"	ユーザーがコンソールを使用して既存のフェデレーションを表示できるようにします。フェデレーションを作成または管理できません。
"パートナーシップ管理者"	ユーザーがパートナーシップを作成および管理できるようにします。
"パートナーシップビューアー"	ユーザーが既存のパートナーシップを表示できるようにします。パートナーシップを作成または管理することはできません。
"スーパー管理者"	ユーザーに管理者ロールのサブセットを付与します。この役割は、コンソールの責任を複数のユーザーに分散する必要がない小規模な組織向けに設計されています。
"スーパービューアー"	ユーザーにサブセット閲覧者ロールを付与します。この役割は、コンソールの責任を複数のユーザーに分散する必要がない小規模な組織向けに設計されています。

アプリケーションロール

以下は、アプリケーション カテゴリ内のロールの一覧です。各ロールは、指定された範囲内で特定の権限を付与します。必要なアプリケーションまたはプラットフォームのロールを持たないユーザーは、それぞれのアプリケーションにアクセスできません。

アプリケーションロール	責任
"Google Cloud NetApp Volumes管理者"	Google Cloud NetApp Volumesロールを持つユーザーは、Google Cloud NetApp Volumes を検出して管理できます。
"Keystone管理者"	Keystone管理者ロールを持つユーザーは、サービス リクエストを作成できます。ユーザーがアクセスしているKeystoneテナント内の使用状況、リソース、および管理の詳細を監視および表示できるようにします。
"Keystoneビューア"	Keystoneビューア ロールを持つユーザーは、サービス リクエストを作成できません。ユーザーがアクセスしているKeystoneテナント内の消費量、資産、管理情報を監視および表示できるようにします。
ONTAPメディエーターのセットアップロール	ONTAP Mediator セットアップ ロールを持つサービス アカウントは、サービス リクエストを作成できます。このロールは、サービスアカウントでインスタンスを構成するために必要です。"ONTAPクラウドメディエーター" 。
"オペレーションサポートアナリスト"	アラートおよび監視ツールへのアクセスと、サポートケースの入力および管理機能を提供します。
"Storage Admin"	ストレージの健全性とガバナンス機能を管理し、ストレージ リソースを検出し、既存のシステムを変更および削除します。
"ストレージビューア"	ストレージの健全性とガバナンス機能を表示し、以前に検出されたストレージ リソースも表示します。既存のストレージ システムを検出、変更、または削除することはできません。
"システムヘルススペシャリスト"	ストレージとヘルスおよびガバナンス機能を管理します。ストレージ管理者のすべての権限がありますが、既存のシステムを変更または削除することはできません。

データサービスの役割

以下は、データ サービス カテゴリのロールの一覧です。各ロールは、指定された範囲内で特定の権限を付与します。必要なデータ サービス ロールまたはプラットフォーム ロールを持たないユーザーは、データ サービスにアクセスできません。

データサービスの役割	責任
"バックアップとリカバリのスーパー管理者"	NetApp Backup and Recoveryで任意のアクションを実行します。
"バックアップとリカバリの管理者"	ローカル スナップショットへのバックアップ、セカンダリ ストレージへの複製、オブジェクト ストレージへのバックアップを実行します。
"バックアップとリカバリの復元管理者"	バックアップとリカバリでワークロードを復元します。
"バックアップとリカバリのクローン管理者"	バックアップとリカバリでアプリケーションとデータを複製します。

データサービスの役割	責任
"バックアップとリカバリビューア"	バックアップとリカバリの情報を表示します。
"災害復旧管理者"	NetApp Disaster Recoveryサービスで任意のアクションを実行します。
"災害復旧フェイルオーバー管理者"	フェイルオーバーと移行を実行します。
"災害復旧アプリケーション管理者"	レプリケーション プランを作成し、レプリケーション プランを変更し、テスト フェイルオーバーを開始します。
"災害復旧ビューア"	情報の表示のみ。
分類ビューア	ユーザーがNetApp Data Classificationスキャン結果を表示できるようにします。このロールを持つユーザーは、コンプライアンス情報を表示し、アクセス権限を持つリソースのレポートを生成できます。これらのユーザーは、ボリューム、バケット、またはデータベース スキーマのスキャンを有効または無効にすることはできません。分類には閲覧者の役割はありません。
"ランサムウェア耐性管理者"	NetApp Ransomware Resilienceの「保護」、「アラート」、「回復」、「設定」、「レポート」タブでアクションを管理します。
"ランサムウェア耐性ビューア"	ランサムウェア耐性で、ワークロード データを表示し、アラート データを表示し、回復データをダウンロードし、レポートをダウンロードします。
"ランサムウェア耐性ユーザー行動管理者"	Ransomware Resilience で、疑わしいユーザー行動の検出、アラート、監視を構成、管理、表示します。
"ランサムウェア耐性ユーザー行動ビューア"	ランサムウェア耐性で疑わしいユーザー行動のアラートと分析情報を表示します。
SnapCenter管理者	NetApp Backup and Recovery for Applications を使用してオンプレミスのONTAPクラスターからスナップショットをバックアップする機能を提供します。このロールを持つメンバーは、次のアクションを実行できます。 * [バックアップとリカバリ] > [アプリケーション] から任意のアクションを実行する * 権限を持つプロジェクトおよびフォルダ内のすべてのシステムを管理する * すべてのNetApp Consoleサービスを使用するSnapCenterには、閲覧者ロールはありません。

関連リンク

- "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 ConsoleIAMを使い始める"
- "NetApp Consoleのメンバーとその権限を管理する"
- "NetApp ConsoleIAMのAPIについて学ぶ"

NetApp Consoleプラットフォームアクセスロール

ユーザーにプラットフォーム ロールを割り当てて、 NetApp Consoleの管理、ロールの割り当て、ユーザーの追加、コンソール エージェントの作成、フェデレーションの管理を行う権限を付与します。

大規模な多国籍組織の組織役割の例

XYZ 社は、北米、ヨーロッパ、アジア太平洋の地域別にデータ ストレージ アクセスを整理し、集中管理による地域制御を実現しています。

XYZ 社のコンソールの 組織管理者 は、初期組織と各リージョンの個別のフォルダーを作成します。各リージョンの*フォルダーまたはプロジェクト管理者*は、リージョンのフォルダー内のプロジェクト (および関連するリソース) を整理します。

フォルダーまたはプロジェクト管理者 の役割を持つ地域管理者は、リソースとユーザーを追加することでフォルダーを積極的に管理します。これらの地域管理者は、管理するフォルダやプロジェクトを追加、削除、または名前変更することもできます。組織管理者 は新しいリソースの権限を継承し、組織全体のストレージ使用状況の可視性を維持します。

同じ組織内で、1 人のユーザーに フェデレーション管理者 ロールが割り当てられ、組織の企業 IdP とのフェデレーションを管理します。このユーザーはフェデレーション組織を追加または削除できますが、組織内のユーザーまたはリソースを管理することはできません。組織管理者 は、フェデレーション ステータスを確認し、フェデレーション組織を表示するための フェデレーション ビューアー ロールをユーザーに割り当てます。

次の表は、各コンソール プラットフォーム ロールが実行できるアクションを示しています。

組織管理の役割

Task	組織管理者	フォルダまたはプロジェクトの管理者
エージェントを作成する	はい	いいえ
コンソールからシステムを作成、変更、または削除する（システムの追加または検出）	はい	はい
フォルダとプロジェクトの作成（削除を含む）	はい	いいえ
既存のフォルダとプロジェクトの名前を変更する	はい	はい
役割を割り当ててユーザーを追加する	はい	はい
リソースをフォルダとプロジェクトに関連付ける	はい	はい
エージェントをフォルダとプロジェクトに関連付ける	はい	いいえ
フォルダとプロジェクトからエージェントを削除する	はい	いいえ
エージェントの管理（証明書、設定などの編集）	はい	いいえ
管理 > 資格情報から資格情報を管理する	はい	はい
フェデレーションの作成、管理、表示	はい	いいえ
コンソールからサポートに登録し、ケースを送信します	はい	はい
明示的なアクセス ロールに関連付けられていないデータ サービスを使用する	はい	はい
監査ページと通知を表示する	はい	はい

連盟の役割

Task	連盟管理者	連盟ビューア
連盟を作成する	はい	いいえ
ドメインを確認する	はい	いいえ
フェデレーションにドメインを追加する	はい	いいえ
フェデレーションを無効化および削除する	はい	いいえ
テスト連盟	はい	いいえ
連盟とその詳細を表示する	はい	はい

パートナーシップの役割

Task	パートナーシップ管理者	パートナーシップビューアー
パートナーシップを構築できる	はい	いいえ
パートナーメンバーに役割を割り当てる	はい	いいえ
パートナーシップにメンバーを追加できます	はい	いいえ
組織のパートナーシップの詳細を表示できます	はい	はい

スーパー管理者と閲覧者の役割

スーパー管理者 ロールには、コンソールの機能、ストレージ、およびデータ サービスを管理するための完全なアクセス権が付与されます。この役割は、管理とガバナンスを監督する人に適しています。対照的に、スーパー ビューアー ロールは読み取り専用アクセスを提供するため、変更を加えずに可視性を必要とする監査人や関係者に最適です。

組織は、セキュリティ リスクを最小限に抑え、最小権限の原則に従うために、スーパー管理者 アクセスを控えめに使用する必要があります。ほとんどの組織では、リスクを軽減し、監査可能性を向上させるために、必要な権限のみを持つきめ細かいロールを割り当てる必要があります。

スーパーロールの例

ABC コーポレーションには、データ サービスとストレージ管理にNetApp Consoleを活用する 5 人の小規模なチームがあります。複数の役割を配分する代わりに、ユーザー管理やリソース構成などのすべての管理タスクを担当する 2 人の上級チーム メンバーに スーパー管理者 の役割を割り当てます。残りの 3 人のチーム メンバーには スーパー ビューアー ロールが割り当てられており、設定を変更する権限なしで、ストレージの健全性とデータ サービスの状態を監視できます。

ロール	継承された役割
スーパー管理者	• 組織管理者 • フォルダまたはプロジェクトの管理者 • 連盟管理者 • パートナーシップ管理者 • ランサムウェア耐性管理者 • 災害復旧管理者 • バックアップスーパー管理者 • Storage Admin • Keystone管理者 • Google Cloud NetApp Volumes管理者
スーパービューアー	• 組織閲覧者 • 連盟ビューア • パートナーシップビューアー • ランサムウェア耐性ビューア • 災害復旧ビューア • バックアップビューア • ストレージビューア • Keystoneビューア • Google Cloud NetApp Volumes閲覧者

アプリケーションロール

NetApp ConsoleのGoogle Cloud NetApp Volumesロール

ユーザーに次のロールを割り当てて、 NetApp ConsoleでGoogle Cloud NetApp Volumesにアクセスできるようにすることができます。

Google Cloud NetApp Volumes は次のロールを使用します。

- * Google Cloud NetApp Volumes管理者*: コンソールでGoogle Cloud NetApp Volumes を検出し、管理します。

NetApp ConsoleのKeystoneアクセス ロール

Keystoneロールは、 Keystoneダッシュボードへのアクセスを提供し、ユーザーがKeystoneサブスクリプションを表示および管理できるようにします。 Keystone の役

割には、 Keystone管理者とKeystoneビューアーの 2 つがあります。 2 つのロールの主な違いは、 Keystoneで実行できるアクションです。 Keystone管理者ロールは、サービス リクエストの作成やサブスクリプションの変更が許可される唯一のロールです。

NetApp Consoleの**Keystone**ロールの例

XYZ 社には、 Keystoneサブスクリプション情報を閲覧できる、さまざまな部門のストレージ エンジニアが 4 人います。これらのユーザー全員がKeystoneサブスクリプションを監視する必要がありますが、サービス リクエストを作成できるのはチーム リーダーのみです。チーム メンバーのうち 3 名に * Keystoneビューア* ロールが付与され、チーム リーダーには * Keystone管理者* ロールが付与されるため、会社のサービス リクエストを制御できるようになります。

次の表は、各Keystoneロールが実行できるアクションを示しています。

特徴とアクション	**Keystone**管理者	**Keystone**ビューア
次のタブを表示します: サブスクリプション、資産、モニター、管理	はい	はい
* Keystoneサブスクリプションページ*:		
サブスクリプションを表示	はい	はい
サブスクリプションの修正または更新	はい	いいえ
* Keystoneアセット ページ*:		
アセットを表示	はい	はい
資産管理	はい	いいえ
* Keystoneアラートページ*:		
アラートを表示	はい	はい
アラートを管理する	はい	いいえ
自分用のアラートを作成する	はい	はい
Licenses and subscriptions:		
ライセンスとサブスクリプションを表示できます	はい	はい
* Keystoneレポートページ*:		
レポートをダウンロード	はい	はい
レポートを管理する	はい	はい
自分用のレポートを作成する	はい	はい

特徴とアクション	**Keystone**管理者	**Keystone**ビューア
サービスリクエスト:		
サービスリクエストを作成する	はい	いいえ
組織内の任意のユーザーが作成したサービスリクエストを表示する	はい	はい

NetApp Consoleの運用サポートアナリスト アクセス ロール

アラートと監視へのアクセスを提供するために、ユーザーに次のロールを割り当てることができます。この役割を持つユーザーはサポートケースを開くこともできます。

運用サポートアナリスト

Task	実行できる
設定 > 資格情報から自分のユーザー資格情報を管理します	はい
発見されたリソースを表示する	はい
コンソールからサポートに登録し、ケースを送信します	はい
はい	監査ページと通知を表示する
はい	アラートの表示、ダウンロード、設定

NetApp Consoleのストレージアクセスロール

ユーザーに次のロールを割り当てて、 NetApp Consoleのストレージ管理機能へのアクセスを許可できます。ユーザーに、ストレージを管理するための管理者ロールまたは監視するための閲覧者ロールを割り当てることができます。

これらのロールは、NetApp Consoleパートナーシップ API からは使用できません。

管理者は、次のストレージ リソースと機能についてユーザーにストレージ ロールを割り当てることができます。

ストレージ リソース:

- オンプレミスのONTAPクラスタ
- StorageGRID
- Eシリーズ

コンソールのサービスと機能:

- デジタルアドバイザー
- ソフトウェアアップデート

- ライフサイクルプランニング
- 持続可能性

NetApp Consoleのストレージロールの例

多国籍企業である XYZ 社には、大規模なストレージ エンジニアとストレージ管理者のチームが存在します。これにより、このチームは、ユーザー管理、エージェントの作成、ライセンス管理などのコアコンソールタスクへのアクセスを制限しながら、担当リージョンのストレージ資産を管理できるようになります。

12 人のチーム内で、2 人のユーザーに ストレージ閲覧者 ロールが付与され、割り当てられたコンソール プロジェクトに関連付けられたストレージ リソースを監視できるようになります。残りの 9 人には、ソフトウェア更新の管理、コンソール経由のONTAP System Manager へのアクセス、ストレージ リソースの検出 (システムの追加) などの機能を含む **Storage admin** ロールが付与されます。チームの 1 人に システム ヘルス スペシャリスト の役割が付与され、担当リージョン内のストレージ リソースのヘルスを管理できるようになりますが、システムを変更または削除することはできません。このユーザーは、割り当てられたプロジェクトのストレージ リソースに対してソフトウェア更新を実行することもできます。

組織には、ユーザー管理、エージェント作成、ライセンス管理など、コンソールのあらゆる側面を管理できる組織管理者 ロールを持つ 2 人の追加ユーザーと、割り当てられているフォルダーとプロジェクトのコンソール管理タスクを実行できる フォルダーまたはプロジェクト管理者 ロールを持つ複数のユーザーがいます。

次の表は、各ストレージ ロールが実行するアクションを示しています。

特徴とアクション	**Storage Admin**	システムヘルススペシャリスト	ストレージビューア
ストレージ管理:			
新しいリソースを発見する（システムを作成する）	はい	はい	いいえ
検出されたシステムを表示	はい	はい	いいえ
コンソールからシステムを削除する	はい	いいえ	いいえ
システムを変更する	はい	いいえ	いいえ
エージェントを作成する	いいえ	いいえ	いいえ
デジタルアドバイザー			
すべてのページと機能を表示	はい	はい	はい
Licenses and subscriptions			
すべてのページと機能を表示	いいえ	いいえ	いいえ
ソフトウェアアップデート			
ランディングページと推奨事項を表示	はい	はい	はい

特徴とアクション	**Storage Admin**	システムヘルススペシャリスト	ストレージビューア
潜在的なバージョンの推奨事項と主な利点を確認する	はい	はい	はい
クラスターの更新の詳細を表示する	はい	はい	はい
更新前のチェックを実行し、アップグレードプランをダウンロードする	はい	はい	はい
ソフトウェアアップデートをインストールする	はい	はい	いいえ
ライフサイクルプランニング			
キャパシティプランニングの状況を確認する	はい	はい	はい
次のアクションを選択する（ベストプラクティス、階層）	はい	いいえ	いいえ
コールドデータをクラウドストレージに階層化してストレージを解放する	はい	はい	いいえ
リマインダーを設定する	はい	はい	はい
持続可能性			
ダッシュボードと推奨事項を表示する	はい	はい	はい
レポートデータをダウンロード	はい	はい	はい
炭素削減率を編集	はい	はい	いいえ
修正の推奨事項	はい	はい	いいえ
推奨を延期する	はい	はい	いいえ
システム管理者アクセス			
資格情報を入力できます	はい	はい	いいえ
資格			
ユーザ クレデンシャル	はい	はい	いいえ

データサービスの役割

NetApp ConsoleのNetApp Backup and Recoveryの役割

コンソール内でNetApp Backup and Recoveryにアクセスできるように、ユーザーに次のロールを割り当てることができます。バックアップとリカバリのロールにより、組織内

でユーザーが実行する必要があるタスクに固有のロールを柔軟に割り当てることができます。ロールの割り当て方法は、独自のビジネスおよびストレージ管理の実践によって異なります。

このサービスは、NetApp Backup and Recoveryに固有の次のロールを使用します。

- バックアップおよびリカバリ スーパー管理者: NetApp Backup and Recoveryであらゆるアクションを実行します。
- バックアップとリカバリ バックアップ管理者: NetApp Backup and Recoveryで、ローカル スナップショットへのバックアップ、セカンダリ ストレージへの複製、オブジェクト ストレージへのバックアップ アクションを実行します。
- バックアップおよびリカバリの復元管理者: NetApp Backup and Recoveryを使用してワークロードを復元します。
- バックアップおよびリカバリ クローン管理者: NetApp Backup and Recoveryを使用してアプリケーションとデータをクローンします。
- バックアップおよびリカバリ ビューア: NetApp Backup and Recoveryの情報を表示しますが、アクションは実行しません。

NetApp Consoleのアクセスロールの詳細については、 "コンソールのセットアップと管理に関するドキュメント" 。

一般的なアクションに使用されるロール

次の表は、すべてのワークロードに対して各NetApp Backup and Recoveryロールが実行できるアクションを示しています。

特徴とアクション	バックアップとリカバリのスーパー管理者	バックアップとリカバリのバックアップ管理者	バックアップとリカバリの復元管理者	バックアップとリカバリのクローン管理者	バックアップとリカバリビューア
ホストを追加、編集、または削除する	はい	いいえ	いいえ	いいえ	いいえ
プラグインをインストールする	はい	いいえ	いいえ	いいえ	いいえ
資格情報を追加する（ホスト、インスタンス、vCenter）	はい	いいえ	いいえ	いいえ	いいえ
ダッシュボードとすべてのタブを表示	はい	はい	はい	はい	はい
無料トライアルを始める	はい	いいえ	いいえ	いいえ	いいえ
ワークロードの検出を開始する	いいえ	はい	はい	はい	いいえ
ライセンス情報を表示	はい	はい	はい	はい	はい

特徴とアクション	バックアップとリカバリのスーパー管理者	バックアップとリカバリのバックアップ管理者	バックアップとリカバリの復元管理者	バックアップとリカバリのクローン管理者	バックアップとリカバリビューア
ライセンスを有効化	はい	いいえ	いいえ	いいえ	いいえ
ホストを表示	はい	はい	はい	はい	はい
スケジュール:					
スケジュールをアクティブ化	はい	はい	はい	はい	いいえ
スケジュールを中断	はい	はい	はい	はい	いいえ
ポリシーと保護:					
保護プランを見る	はい	はい	はい	はい	はい
保護プランを作成、変更、または削除する	はい	はい	いいえ	いいえ	いいえ
ワークロードを復元する	はい	いいえ	はい	いいえ	いいえ
クローンを作成、分割、または削除する	はい	いいえ	いいえ	はい	いいえ
ポリシーの作成、変更、または削除	はい	はい	いいえ	いいえ	いいえ
レポート:					
レポートを表示	はい	はい	はい	はい	はい
レポートを作成する	はい	はい	はい	はい	いいえ
レポートを削除する	はい	いいえ	いいえ	いいえ	いいえ
* SnapCenterからインポートしてホストを管理する*:					
インポートされたSnapCenterデータを表示する	はい	はい	はい	はい	はい
SnapCenterからデータをインポートする	はい	はい	いいえ	いいえ	いいえ
ホストの管理（移行）	はい	はい	いいえ	いいえ	いいえ
設定を構成する:					

特徴とアクション	バックアップとリカバリのスーパー管理者	バックアップとリカバリのバックアップ管理者	バックアップとリカバリの復元管理者	バックアップとリカバリのクローン管理者	バックアップとリカバリビューア
ログ ディレクトリを設定	はい	はい	はい	いいえ	いいえ
インスタンス資格情報の関連付けまたは削除	はい	はい	はい	いいえ	いいえ
バケツ:					
バケットを表示	はい	はい	はい	はい	はい
バケットを作成、編集、または削除する	はい	はい	いいえ	いいえ	いいえ

ワークロード固有のアクションに使用されるロール

次の表は、各NetApp Backup and Recoveryロールが特定のワークロードに対して実行できるアクションを示しています。

Kubernetes ワークロード

この表は、Kubernetes ワークロードに固有のアクションに対して各NetApp Backup and Recoveryロールが実行できるアクションを示しています。

特徴とアクション	バックアップとリカバリのスーパー管理者	バックアップとリカバリのバックアップ管理者	バックアップとリカバリの復元管理者	バックアップとリカバリビューア
クラスター、名前空間、ストレージ クラス、API リソースを表示する	はい	はい	はい	はい
新しいKubernetesクラスターを追加する	はい	はい	いいえ	いいえ
クラスタ構成を更新する	はい	いいえ	いいえ	いいえ
管理からクラスタを削除する	はい	いいえ	いいえ	いいえ
アプリケーションを表示する	はい	はい	はい	はい
新しいアプリケーションの作成と定義	はい	はい	いいえ	いいえ
アプリケーション構成を更新する	はい	はい	いいえ	いいえ
管理からアプリケーションを削除する	はい	はい	いいえ	いいえ

特徴とアクション	バックアップとリカバリのスーパー管理者	バックアップとリカバリのバックアップ管理者	バックアップとリカバリの復元管理者	バックアップとリカバリビューア
保護されたリソースとバックアップステータスを表示する	はい	はい	はい	はい
バックアップを作成し、ポリシーでアプリケーションを保護する	はい	はい	いいえ	いいえ
アプリの保護を解除し、バックアップを削除する	はい	はい	いいえ	いいえ
リカバリポイントとリソースビューアの結果を表示する	はい	はい	はい	はい
リカバリポイントからアプリケーションを復元する	はい	いいえ	はい	いいえ
Kubernetes バックアップ ポリシーを表示する	はい	はい	はい	はい
Kubernetes バックアップ ポリシーを作成する	はい	はい	はい	いいえ
バックアップポリシーを更新する	はい	はい	はい	いいえ
バックアップポリシーを削除する	はい	はい	はい	いいえ
実行フックとフックソースを表示する	はい	はい	はい	はい
実行フックとフックソースを作成する	はい	はい	はい	いいえ
実行フックとフックソースを更新する	はい	はい	はい	いいえ
実行フックとフックソースを削除する	はい	はい	はい	いいえ
実行フックテンプレートを表示する	はい	はい	はい	はい
実行フックテンプレートを作成する	はい	はい	はい	いいえ
実行フックテンプレートを更新する	はい	はい	はい	いいえ
実行フックテンプレートを削除する	はい	はい	はい	いいえ
ワークロードの概要と分析ダッシュボードを表示する	はい	はい	はい	はい

特徴とアクション	バックアップとリカバリのスーパー管理者	バックアップとリカバリのバックアップ管理者	バックアップとリカバリの復元管理者	バックアップとリカバリビューア
StorageGRIDバケットとストレージターゲットを表示する	はい	はい	はい	はい

NetApp ConsoleのNetApp Disaster Recoveryロール

コンソール内でNetApp Disaster Recoveryにアクセスできるように、ユーザーに次のロールを割り当てることができます。災害復旧ロールを使用すると、組織内でユーザーが実行する必要があるタスクに固有のロールを柔軟に割り当てることができます。ロールの割り当て方法は、独自のビジネスおよびストレージ管理の実践によって異なります。

災害復旧では次のロールが使用されます。

- 災害復旧管理者: あらゆるアクションを実行します。
- 災害復旧フェールオーバー管理者: フェールオーバーと移行を実行します。
- 災害復旧アプリケーション管理者: レプリケーション プランを作成します。レプリケーション プランを変更します。テストフェイルオーバーを開始します。
- 災害復旧ビューアー: 情報の表示のみ。

次の表は、各ロールが実行できるアクションを示しています。

特徴とアクション	災害復旧管理者	災害復旧フェイルオーバー管理者	災害復旧アプリケーション管理者	災害復旧ビューア
ダッシュボードとすべてのタブを表示	はい	はい	はい	はい
無料トライアルを始める	はい	いいえ	いいえ	いいえ
ワークロードの検出を開始する	はい	いいえ	いいえ	いいえ
ライセンス情報を表示	はい	はい	はい	はい
ライセンスを有効化	はい	いいえ	はい	いいえ
サイトタブ:				
サイトを表示	はい	はい	はい	はい
サイトの追加、変更、削除	はい	いいえ	いいえ	いいえ
レプリケーション プラン タブで:				
レプリケーションプランの表示	はい	はい	はい	はい

特徴とアクション	災害復旧管理者	災害復旧フェイルオーバー管理者	災害復旧アプリケーション管理者	災害復旧ビューア
レプリケーションプランの詳細を表示する	はい	はい	はい	はい
レプリケーションプランを作成または変更する	はい	はい	はい	いいえ
レポートを作成する	はい	いいえ	いいえ	いいえ
スナップショットを表示	はい	はい	はい	はい
フェイルオーバーテストを実行する	はい	はい	はい	いいえ
フェイルオーバーを実行する	はい	はい	いいえ	いいえ
フェイルバックを実行する	はい	はい	いいえ	いいえ
移行を実行する	はい	はい	いいえ	いいえ
リソース グループ タブで:				
リソース グループを表示する	はい	はい	はい	はい
リソース グループの作成、変更、または削除	はい	いいえ	はい	いいえ
ジョブ監視タブで:				
ジョブの表示	はい	いいえ	はい	はい
ジョブをキャンセルする	はい	はい	はい	いいえ

NetApp Consoleのランサムウェア耐性アクセス ロール

ランサムウェア レジリエンス ロールは、ユーザーにNetApp Ransomware Resilienceへのアクセスを提供します。ランサムウェア耐性は次の役割をサポートします。

- ランサムウェア耐性管理者
- ランサムウェア耐性ビューア
- ランサムウェア耐性ユーザー行動管理者
- ランサムウェア耐性ユーザー行動ビューア

ロールによって、設定とアクションへの異なるレベルのアクセス権が付与されます。

ランサムウェア耐性ユーザー行動管理者とユーザー行動閲覧者の役割で利用できるアクションは、 "不審なユーザーアクティビティ"。これらのロールは、ランサムウェア耐性管理者または閲覧者ロールに追加されるように設計されています。疑わしいユーザーの行動設定を構成し、アラートに応答するには、ユーザーは

Ransomware Resilience ユーザー行動管理者ロールを持っている必要があります。疑わしいユーザー行動アラートのみを表示するには、ユーザーは Ransomware Resilience ユーザー行動閲覧者ロールを持っている必要があります。

次の表は、ランサムウェア レジリエンス管理者ロールとランサムウェア レジリエンス閲覧者ロールで使用できるアクションを区別しています。

特徴とアクション	ランサムウェア耐性管理者	ランサムウェア耐性ビューア
ダッシュボードとすべてのタブを表示	はい	はい
ダッシュボードで推奨事項のステータスを更新する	はい	いいえ
無料トライアルを始める	はい	いいえ
ワークロードの検出を開始する	はい	いいえ
ワークロードの再検出を開始する	はい	いいえ
[保護]タブで:		
保護プランの追加、変更、削除	はい	いいえ
ワークロードを保護する	はい	いいえ
機密データへの露出を特定する	はい	いいえ
保護プランと詳細を一覧表示する	はい	はい
保護グループの一覧	はい	はい
保護グループの詳細を表示する	はい	はい
保護グループの作成、編集、または削除	はい	いいえ
データをダウンロード	はい	はい
アラートタブ:		
アラートとアラートの詳細を表示する	はい	はい
インシデントステータスの編集	はい	いいえ
回復の警告をマーク	はい	いいえ

特徴とアクション	ランサムウェア耐性管理者	ランサムウェア耐性ビューア
インシデントの詳細を表示	はい	はい
インシデントを却下または解決する	はい	いいえ
ユーザーをブロック	はい	いいえ
影響を受けるファイルの完全なリストを取得する	はい	いいえ
アラートデータをダウンロード	はい	はい
不審なユーザーアクティビティを表示する	いいえ	いいえ
[回復]タブで:		
影響を受けるファイルをダウンロードする	はい	いいえ
ワークロードの復元	はい	いいえ
回復データをダウンロードする	はい	はい
レポートをダウンロード	はい	はい
設定タブで:		
バックアップ先を追加または変更する	はい	いいえ
バックアップ先の一覧	はい	はい
接続されたSIEMターゲットを表示する	はい	はい
SIEMターゲットの追加または変更	はい	いいえ
準備訓練を構成する	はい	いいえ
準備訓練を開始する	はい	いいえ
リセット準備訓練	はい	いいえ
編集準備訓練	はい	いいえ
準備訓練の状況を確認する	はい	はい

特徴とアクション	ランサムウェア耐性管理者	ランサムウェア耐性ビューア
検出構成の更新	はい	いいえ
検出構成の表示	はい	はい
疑わしいユーザーの行動設定を構成する	いいえ	いいえ
レポートタブ:		
レポートをダウンロード	はい	はい

パートナー組織

NetApp Consoleのパートナーシップ

NetApp Consoleを使用すると、組織間のパートナーシップを構築し、パートナーが組織の境界を越えてNetAppリソースを安全に管理し、コラボレーションを合理化し、セキュリティを強化できます。

必要な役割

パートナーシップ管理者"アクセス ロールの詳細について説明します。"

パートナーシップにより、コンソールでロール主導の関係を使用して、組織全体のNetAppリソースを安全に管理できます。開始組織はリソースへのアクセスを許可し、受け入れ組織はアクセスを許可するユーザーまたはサービス アカウントを提供します。パートナーシップはセルフサービス ワークフローを通じて確立され、開始組織は共有されるリソース、割り当てられるロール、必要に応じてパートナー アクセスをオンボード、管理、または取り消す機能などを完全に制御できます。

顧客は、複雑な設定を必要とせずに、MSP または再販業者にNetApp環境の管理を許可できます。お客様は、パートナーがアクセスできるクラスターとその役割を制御でき、セキュリティとコンプライアンスを維持するためにいつでもアクセスを取り消すことができます。

パートナーとして、顧客環境全体の一元的な可視性と制御を実現できます。顧客の組織に簡単に切り替えて、定義された境界内でリソースを管理し、データ サービスを実行し、正常性を監視できるため、カスタム ツールが削減され、各顧客のポリシーとの整合性が確保されます。

1 **1**人以上のユーザーにパートナーシップ管理者の役割を割り当てる

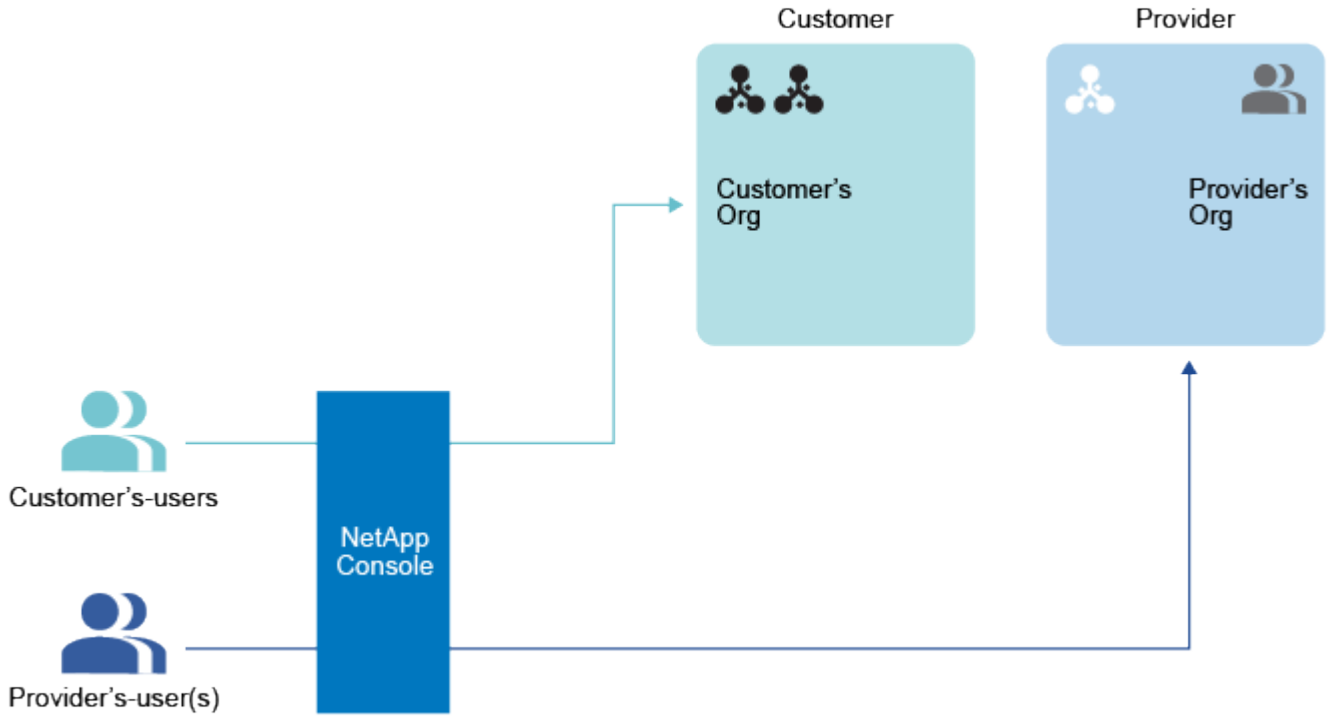
パートナーシップを作成および管理するには、開始組織と受信組織の両方で 1 人以上のユーザーにパートナーシップ管理者ロールを割り当てます。パートナーシップの表示のみが必要で、管理は必要ないユーザーには、パートナーシップ閲覧者ロールを割り当てることができます。

2 組織**ID**を開始組織と共有する

パートナーシップを開始するには、イニシエーターがターゲット組織の組織 ID を知っている必要がありま

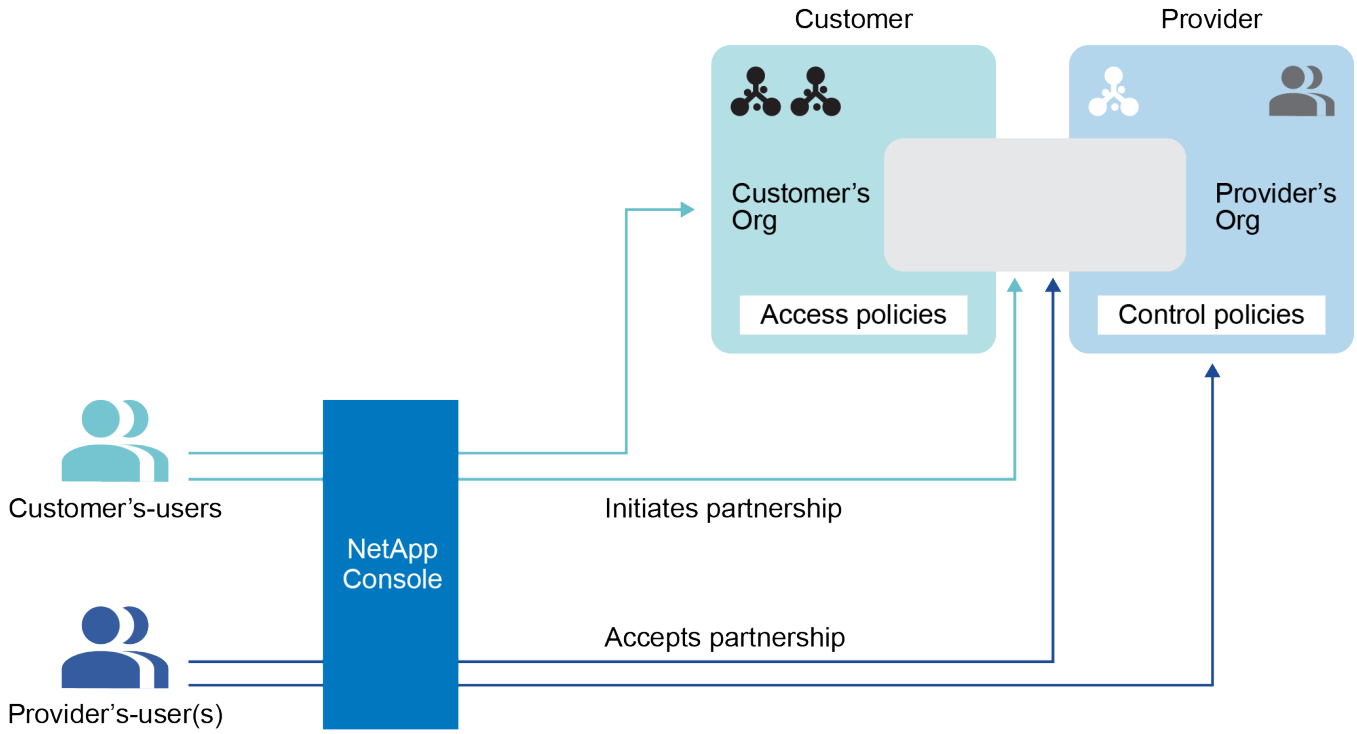
す。この組織 ID にアクセスできるのは、それぞれの組織のみです。電子メールまたは別の方法で、 NetApp Consoleの外部にある開始組織と直接共有します。

開始組織とは、そのリソースへのアクセスを許可する組織です。



3 **NetApp Console**内でパートナーシップを開始する

パートナーシップを開始する組織は、NetApp Console内からパートナーシップ要求を送信してパートナーシップを開始します。



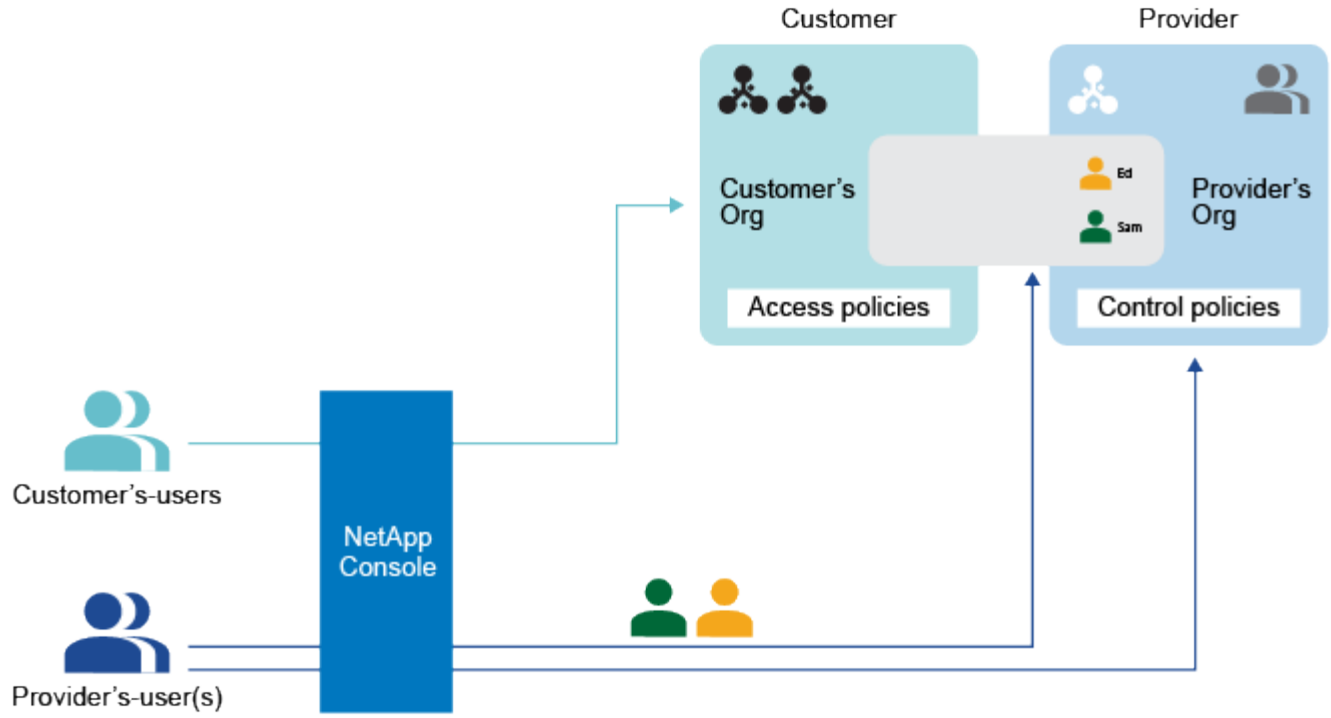
4 パートナーシップを承認する

受信組織はリクエストを承認する必要があります。

受信組織は、リソースへのアクセスを許可される組織です。

5 パートナーシップにユーザーを割り当てる

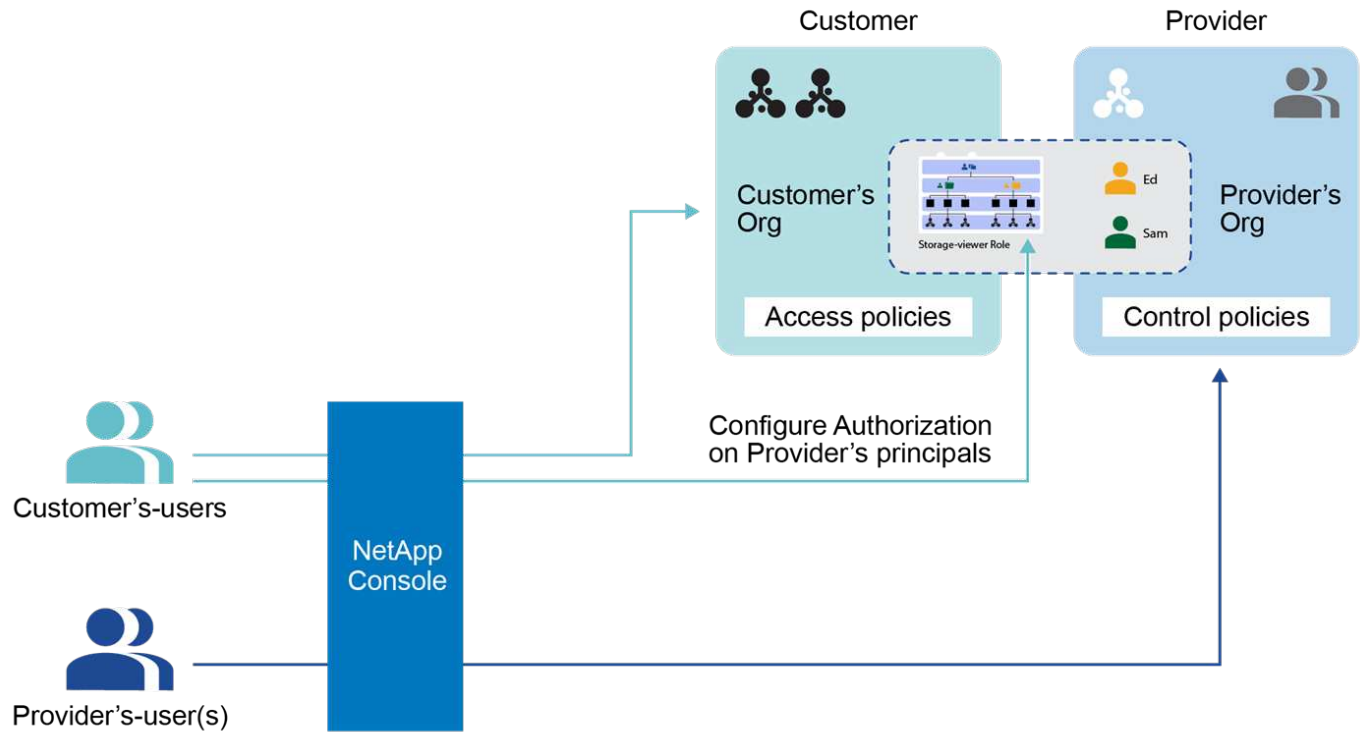
受信側組織は、組織の特定のユーザーまたはサービス アカウントをパートナーシップに割り当てます。開始組織はこれらのユーザーにロールを割り当てます。



6 割り当てられたユーザーにリソースへのアクセスを許可する

開始組織の場合は、パートナーシップに割り当てられたユーザーに特定のリソースへのアクセス権を付与できます。いつでもアクセスを取り消すことができます。

これは、組織内の特定のプロジェクトまたはフォルダーにロールを割り当てることによって行います。



NetApp Consoleでパートナーシップを管理する

パートナーシップを構築し、組織と信頼できるパートナーとの間で安全で管理された接続を確立して、共同でNetAppリソースを管理します。

パートナーシップにより、コンソールでロール主導の関係を使用して、境界を越えてNetAppリソースを安全に管理できます。開始組織はリソースへのアクセスを許可し、受け入れ組織はアクセスを許可するユーザーまたはサービス アカウントを提供します。パートナーシップはセルフサービス ワークフローを通じて確立され、開始組織は共有されるリソース、割り当てられるロール、必要に応じてパートナー アクセスをオンボード、管理、または取り消す機能などを完全に制御できます。

必要な役割

パートナーシップを作成および管理するには、パートナーシップ管理者 ロールが必要です。 *パートナーシップ閲覧者*はパートナーシップ ページを閲覧できます。"アクセス ロールの詳細について説明します。"

組織パートナーシップを開始する

他の組織の組織 ID がわかっている場合は、その組織とのパートナーシップをリクエストできます。パートナーシップを進める前に、受信側の組織がリクエストを承認する必要があります。

始める前に、パートナー組織の組織 ID があることと、パートナーシップ管理者 ロールが割り当てられていることを確認してください。

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*タブを選択します。
3. *パートナーシップを追加*を選択します。
4. パートナーシップの作成 ダイアログボックスで、要求されたパートナーのパートナー組織 ID を入力し、追加 を選択します。

   パートナーシップ リクエストは、承認のためにパートナー組織に送信されます。 *パートナーシップ*ページでパートナーシップリクエストのステータスを確認できます。

組織パートナーシップを承認する

パートナーシップを進めるには、組織パートナーシップのリクエストが受信側組織によって承認される必要があります。パートナーシップを承認および管理するには、パートナーシップ管理者 の役割が必要です。

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *パートナーシップ受信*タブを選択します。
4. 承認したい受信したパートナーシップに移動して選択します ••• 次に、[承認] を選択します。
5. パートナーシップを要求した組織の名前と組織 ID を含むパートナーシップの詳細を確認し、[次へ] を選択します。
6. オプションとして、組織のメンバーをパートナーシップに追加し、「適用」を選択します。

パートナーシップ ページからいつでもメンバーを追加できます。

追加したメンバーはパートナーの組織に表示されるようになり、パートナーはメンバーをリソースに割り当てることができます。

結果

承認したパートナーシップのステータスが「確立済み」と表示されます。どちらかの組織で パートナーシップ管理者 または パートナーシップ閲覧者 の役割を持つユーザーは、パートナーシップを表示できます。

パートナーシップのステータスを表示

パートナーシップのステータスを表示します。

必要な役割

パートナーシップ管理者、パートナーシップ閲覧者。"アクセス ロールの詳細について説明します。"

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *開始したパートナーシップ*または*受信したパートナーシップ*タブを選択します。
4. パートナーシップとそのステータスを表示するそれぞれの表を確認します。

組織のパートナーシップを無効にする

パートナーシップを無効にするには、開始組織のメンバーである必要があります。パートナーシップを無効にすると、パートナー組織と共有されていた組織内のすべてのリソースへのアクセスが直ちに取り消されます。

必要な役割

パートナーシップ管理者。"アクセス ロールの詳細について説明します。"

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *開始されたパートナーシップ*タブのいずれかを選択します。
4. パートナーシップとそのステータスを表示するそれぞれの表を確認します。
5. 無効にしたい開始済みのパートナーシップに移動し、 次に、[無効にする] を選択します。

パートナーシップ組織のメンバーを管理する

パートナー組織にユーザーを追加することで、パートナーシップにユーザーを追加できます。ユーザーを追加したら、パートナー組織は組織内の特定のリソースに対するロールをユーザーに割り当てる責任を負います。

必要な役割

パートナーシップを作成および管理するには、パートナーシップ管理者 ロールが必要です。 *パートナーシッ

プ閲覧者*はパートナーシップ ページを閲覧できます。"アクセス ロールの詳細について説明します。"

いつでもパートナーシップからユーザーを削除できます。パートナーシップからユーザーを削除すると、パートナー組織内のすべてのリソースへのアクセス権が直ちに取り消されます。

パートナーシップにメンバーを追加する

パートナーシップにメンバーを追加する場合、パートナー組織の パートナーシップ管理者 は、メンバーがリソースにアクセスできるようにする前に、組織内の特定のリソースに対するロールをメンバーに割り当てる必要があります。

パートナーシップにメンバーを追加すると、そのメンバーはパートナー組織のメンバーとして表示され、パートナーはメンバーをリソースに割り当てることができます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *パートナーシップ受信*タブを選択します。
4. アクションメニューを選択 メンバーに追加したい確立されたパートナーシップの横にある をクリックし、[メンバーを追加] を選択します。
5. パートナーシップに追加するメンバーを 1 人以上選択し、[追加] を選択します。

パートナーシップからメンバーを削除する

パートナーシップからメンバーをいつでも削除できます。パートナーシップからユーザーを削除すると、パートナー組織内のすべてのリソースへのアクセス権が直ちに取り消されます。

メンバーの役割やアクセスできるリソースを調整する場合は、パートナー組織のパートナーシップ管理者がその変更を行う必要があります。

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *パートナーシップ受信*タブを選択します。
4. アクションメニューを選択 削除するメンバーの横にある をクリックし、[関連付けを削除] を選択します。
5. ダイアログボックスで*削除*を選択してアクションを確認します。

ユーザーの役割情報を表示する

ユーザーに割り当てられているロールと関連付けられているリソースを表示できます。

ユーザーに関連付けられたロールを変更することはできません。提供されるリソースまたはロールについて質問がある場合は、パートナー組織の管理者にお問い合わせください。

手順

1. *管理 > IDとアクセス*を選択します。

2. *パートナーシップ*を選択します。
3. *パートナーシップ受信*タブを選択します。
4. *メンバー*ページで、テーブル内のメンバーに移動し、 次に、[詳細を表示] を選択します。
5. 表で、メンバーに割り当てられたロールを表示する組織、フォルダ、またはプロジェクトのそれぞれの行を展開し、「ロール」列の番号を選択します。

パートナーシップユーザーにリソースへのアクセスを提供する

組織内のフォルダやプロジェクトに対する特定のロールをパートナーシップ ユーザーに割り当てることで、パートナーシップ ユーザーにアクセス権を付与できます。

必要な役割

パートナーシップ管理者。"アクセス ロールの詳細について説明します。"

パートナー組織では、まずパートナーシップにメンバーを追加してから、組織内のリソースのロールをメンバーに割り当てる必要があります。"パートナーシップにメンバーを追加する方法を学びます。"

パートナーシップユーザーの役割を理解する

自分の組織の場合と同じ方法で、パートナー組織のメンバーの役割を管理できます。ただし、パートナーシップ ユーザーはすべてのロールを利用できるわけではありません。特に、パートナー ユーザーにソフトウェアの更新を許可するロールを付与することはできません。通常、 ONTAPソフトウェアを更新するには、直接ネットワーク アクセスが必要です。

パートナー ユーザーには次のロールを割り当てることができます。

- "組織管理者"
- "フォルダまたはプロジェクトの管理者"
- "連盟管理者"
- "連盟ビューア"
- "バックアップとリカバリの管理者"
- "バックアップビューア"
- "管理者を復元"
- "クローン管理者"
- "災害復旧管理者"
- "災害復旧フェイルオーバー管理者"
- "災害復旧アプリケーション管理者"
- "災害復旧ビューア"
- "オペレーションサポートアナリスト"
- "分類ビューア"

"定義済みロールの詳細"

パートナーユーザーに役割を追加する

メンバーにロールを追加することで、組織のリソースへのアクセス権を付与します。ロールを割り当てるときは、リソースとロールを 1 つずつ指定します。ユーザーに複数のロールを割り当てることができます。

たとえば、2 つのプロジェクトがあり、同じユーザーに両方のバックアップおよびリカバリ管理者のロールを付与したい場合は、各プロジェクトのユーザーにロールを提供する必要があります。同様に、同じプロジェクトに対してユーザーに 2 つの異なるロールを提供する場合は、各ロールを個別に割り当てる必要があります。

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *パートナーシップ開始*タブを選択します。
4. アクションメニューを選択 ••• 表示する確立されたパートナーシップの横にある をクリックし、[詳細を表示] を選択します。

   メンバー リストには、パートナー組織がパートナーシップに追加したメンバーが表示されます。

5. アクションメニューを選択 ••• 役割を割り当てるメンバーの横にある をクリックし、[役割の追加] を選択します。
6. ロールを追加するには、ダイアログ ボックスの手順を完了します。
   - 組織、フォルダ、またはプロジェクトを選択: メンバーに権限を与えるリソース階層のレベルを選択します。

     組織またはフォルダを選択した場合、メンバーにはその組織またはフォルダ内に存在するすべてのものに対する権限が付与されます。

   - カテゴリを選択: 役割のカテゴリを選択します。"アクセスロールについて学ぶ" 。
   - *ロール*を選択: 選択した組織、フォルダ、またはプロジェクトに関連付けられているリソースに対する権限をメンバーに付与するロールを選択します。
   - ロールの追加: 組織内の追加のフォルダーまたはプロジェクトへのアクセス権を付与する場合は、*ロールの追加*を選択し、別のフォルダーまたはプロジェクトまたはロールのカテゴリを指定してから、ロールのカテゴリと対応するロールを選択します。
7. *新しいロールを追加*を選択します。

パートナーユーザーの役割を変更または削除する

パートナー組織のメンバーに割り当てたロールを変更または削除できます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *パートナーシップ*を選択します。
3. *パートナーシップ開始*タブを選択します。
4. アクションメニューを選択 ••• 表示する確立されたパートナーシップの横にある をクリックし、[詳細を表示] を選択します。

メンバー リストには、パートナー組織がパートナーシップに追加したメンバーが表示されます。

5. *メンバー*ページで、テーブル内のメンバーに移動し、次に、[詳細を表示] を選択します。
6. 表で、メンバーに割り当てられたロールを変更する組織、フォルダ、またはプロジェクトのそれぞれの行を展開し、「ロール」列で「表示」を選択して、このメンバーに割り当てられているロールを表示します。
7. メンバーの既存の役割を変更したり、役割を削除したりできます。
   a. メンバーの役割を変更するには、変更したい役割の横にある「変更」を選択します。ロールを変更できるのは、同じロール カテゴリ内のロールのみです。たとえば、あるデータ サービス ロールから別のデータ サービス ロールに変更できます。変更を確認します。
   b. メンバーの役割の割り当てを解除するには、をクリックして、メンバーから該当のロールの割り当てを解除します。削除の確認を求められます。

パートナー組織で働く

パートナー組織でロールが付与されると、その組織に切り替えて、実行権限があるアクションを実行できるようになります。

組織メニューを使用して、自分の組織とアクセス権を持つパートナー組織を切り替えることができます。"組織とプロジェクトの切り替えについて詳しく学びます。"

パートナー組織内で共有されているリソースを確認し、割り当てられたロールに基づいてアクションを実行できるようになります。パートナーシップ管理者と協力して、アクセスする必要があるリソースに対して適切なロールがあることを確認してください。

アイデンティティ連携

NetApp ConsoleでIDフェデレーションを使用してシングルサインオンを有効にする

シングル サインオン (フェデレーション) により、ユーザーは企業の認証情報を使用してNetApp Consoleにログインできるため、ログイン プロセスが簡素化され、セキュリティが強化されます。アイデンティティ プロバイダー (IdP) またはNetAppサポート サイトを使用してシングル サインオン (SSO) を有効にできます。

必要な役割

組織管理者、フェデレーション管理者、フェデレーション閲覧者。"アクセス ロールの詳細について説明します。"

NetAppサポート サイトとの ID 連携

NetAppサポート サイトと連携すると、ユーザーは同じ資格情報を使用してコンソール、 Active IQ Digital Advisor、およびその他の関連アプリケーションにログインできるようになります。

NetAppサポート サイトと連携する場合、企業の ID 管理プロバイダーとも連携することはできません。組織に最適なものを選択してください。

手順

1. ダウンロードして完了 "NetAppフェデレーション リクエスト フォーム"。
2. フォームに指定されたメールアドレスにフォームを送信します。

   NetAppサポート チームがお客様のリクエストを確認し、処理します。

IDプロバイダとのフェデレーション接続を設定する

コンソールのシングル サインオン (SSO) を有効にするには、ID プロバイダーとのフェデレーション接続を設定できます。このプロセスでは、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成し、コンソールで接続を作成します。

> 以前にNetApp Cloud Central (コンソールの外部アプリケーション) を使用してフェデレーションを構成した場合は、コンソール内でフェデレーションを管理するために、フェデレーション ページを使用してフェデレーションをインポートする必要があります。"フェデレーションをインポートする方法を学びます。"

サポートされているIDプロバイダー

NetApp は、フェデレーション用に次のプロトコルと ID プロバイダーをサポートしています。

プロトコル

- セキュリティアサーションマークアップ言語（SAML）IDプロバイダー
- アクティブ ディレクトリ フェデレーション サービス (AD FS)

アイデンティティプロバイダー

- Microsoft Entra ID
- PingFederate

NetApp Consoleワークフローとの連携

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

自分のメールドメインまたは自分が所有する別のドメインと連携できます。メール ドメインとは異なるドメインとフェデレーションするには、まずそのドメインを所有していることを確認します。


ドメインを確認する（メールドメインを使用していないとき）

メール ドメインとは異なるドメインとフェデレーションするには、そのドメインを所有していることを確認します。追加の手順なしで電子メールドメインを統合できます。


IdP を設定して、 **NetApp** をサービス プロバイダーとして信頼します。

新しいアプリケーションを作成し、ACS URL、エンティティ ID、その他の資格情報などの詳細を指定して、NetAppを信頼するように ID プロバイダーを構成します。サービス プロバイダー情報は ID プロバイダーによって異なるため、詳細については特定の ID プロバイダーのドキュメントを参照してください。この手順を完了するには、IdP 管理者と協力する必要があります。

3 コンソールでフェデレーション接続を作成する

接続を作成するには、ID プロバイダーからの SAML メタデータ URL またはファイルを指定します。この情報は、コンソールと ID プロバイダー間の信頼関係を確立するために使用されます。提供する情報は、使用している IdP によって異なります。たとえば、Microsoft Entra ID を使用している場合は、クライアント ID、シークレット、ドメインを指定する必要があります。

4 コンソールでフェデレーションをテストする

フェデレーション接続を有効にする前にテストしてください。コンソールのフェデレーション ページのテスト オプションを使用して、テスト ユーザーが正常に認証できることを確認します。テストが成功した場合は、接続を有効にできます。

5 コンソールで接続を有効にする

接続を有効にすると、ユーザーは企業の資格情報を使用してコンソールにログインできるようになります。

開始するには、それぞれのプロトコルまたは IdP のトピックを確認してください。

- "AD FSとのフェデレーション接続を設定する"
- "Microsoft Entra ID とのフェデレーション接続を設定する"
- "PingFederateでフェデレーション接続を設定する"
- "SAML ID プロバイダとのフェデレーション接続を設定する"

ドメイン検証

フェデレーション接続のメールドメインを確認する

電子メール ドメインとは異なるドメインとフェデレーションを行う場合は、まずそのドメインを所有していることを確認する必要があります。フェデレーションには検証済みのドメインのみを使用できます。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

ドメインを確認するには、ドメインの DNS 設定に TXT レコードを追加する必要があります。このレコードは、ドメインを所有していることを証明するために使用され、 NetApp Consoleがフェデレーションのためにドメインを信頼できるようにします。この手順を完了するには、IT またはネットワーク管理者との調整が必要になる場合があります。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。

4. *ドメインの所有権を確認*を選択します。
5. 検証するドメインを入力し、「続行」を選択します。
6. 提供された TXT レコードをコピーします。
7. ドメインの DNS 設定に移動し、ドメインの TXT レコードとして提供された TXT 値を設定します。必要に応じて、IT 管理者またはネットワーク管理者と協力してください。
8. TXT レコードが追加されたら、コンソールに戻り、[検証] を選択します。

フェデレーションを構成する

NetApp ConsoleをActive Directory フェデレーション サービス (AD FS) と連携する

Active Directory フェデレーション サービス (AD FS) をNetApp Consoleと連携させて、NetApp Consoleのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してコンソールにログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。 NetApp、両方ではなく、どちらか一方を選択することを推奨しています。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp Consoleをサービス プロバイダーとして信頼するように ID プロバイダーを構成します。次に、ID プロバイダーの構成を使用してコンソールで接続を作成します。

AD FS サーバーとのフェデレーションを設定して、 NetApp Consoleのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、コンソールをサービス プロバイダーとして信頼するように AD FS を構成し、 NetApp Consoleで接続を作成します。

開始する前に

- 管理者権限を持つ IdP アカウントが必要です。 IdP 管理者と調整して手順を完了してください。
- フェデレーションに使用するドメインを特定します。自分のメールドメインまたは自分が所有する別のドメインを使用できます。電子メール ドメイン以外のドメインを使用する場合は、まずコンソールでドメインを確認する必要があります。以下の手順に従ってこれを行うことができます。"NetApp Consoleでドメインを確認する"トピック。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。
4. ドメインの詳細を入力してください:
    a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
    b. 構成するフェデレーションの名前を入力します。

c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。

5. *次へ*を選択します。
6. 接続方法として、[プロトコル] を選択し、[**Active Directory** フェデレーション サービス **(AD FS)**] を選択します。
7. *次へ*を選択します。
8. AD FS サーバーに証明書利用者信頼を作成します。 PowerShell を使用することも、AD FS サーバー上で手動で構成することもできます。証明書利用者信頼を作成する方法の詳細については、AD FS のドキュメントを参照してください。

   a. 次のスクリプトを使用して PowerShell を使用して信頼を作成します。

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

   b. または、AD FS 管理コンソールで信頼を手動で作成することもできます。信頼を作成するときは、次のNetApp Consoleの値を使用します。

      - 信頼信頼識別子を作成するときは、**YOUR_TENANT** 値を使用します。 `netapp-cloud-account`
      - **WS-Federation** のサポートを有効にする を選択した場合は、**YOUR_AUTH0_DOMAIN** 値を使用します。 `netapp-cloud-account.auth0.com`

   c. 信頼を作成した後、AD FS サーバーからメタデータ URL をコピーするか、フェデレーション メタデータ ファイルをダウンロードします。コンソールで接続を完了するには、この URL またはファイルが必要になります。

   NetApp、メタデータ URL を使用してNetApp Consoleが最新の AD FS 構成を自動的に取得できるようにすることをお勧めします。フェデレーション メタデータ ファイルをダウンロードした場合は、AD FS 構成に変更があるたびに、 NetApp Consoleで手動で更新する必要があります。

9. コンソールに戻り、[次へ] を選択して接続を作成します。
10. AD FS との接続を作成します。

    a. 前の手順で AD FS サーバーからコピーした **AD FS URL** を入力するか、AD FS サーバーからダウンロードしたフェデレーション メタデータ ファイルをアップロードします。

11. *接続を作成*を選択します。接続の作成には数秒かかる場合があります。
12. *次へ*を選択します。
13. 接続をテストするには、[接続テスト] を選択します。 IdP サーバーのログイン ページに移動します。 IdP 資格情報を使用してログインし、テストを完了してコンソールに戻り、接続を有効にします。
14. *次へ*を選択します。
15. *フェデレーションの有効化*ページでフェデレーションの詳細を確認し、*フェデレーションの有効化*を選択します。
16. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインできるようになります。

NetApp Consoleを**Microsoft Entra ID** と連携する

Microsoft Entra ID IdP プロバイダーと連携して、 NetApp Consoleのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。 NetApp、両方ではなく、どちらか一方を選択することを推奨しています。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

Microsoft Entra ID とのフェデレーション接続を設定して、コンソールのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、コンソールをサービス プロバイダーとして信頼するように Microsoft Entra ID を構成し、コンソールで接続を作成します。

開始する前に

- 管理者権限を持つ IdP アカウントが必要です。 IdP 管理者と調整して手順を完了してください。
- フェデレーションに使用するドメインを特定します。自分のメールドメインまたは自分が所有する別のドメインを使用できます。電子メール ドメイン以外のドメインを使用する場合は、まずコンソールでドメインを確認する必要があります。以下の手順に従ってこれを行うことができます。"NetApp Consoleでドメインを確認する"トピック。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。

ドメインの詳細

1. ドメインの詳細を入力してください:
   a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
   b. 構成するフェデレーションの名前を入力します。
   c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。
2. *次へ*を選択します。

接続方法

1. 接続方法として、*プロバイダー*を選択し、*Microsoft Entra ID*を選択します。
2. *次へ*を選択します。

設定手順

1. NetApp をサービス プロバイダーとして信頼するように Microsoft Entra ID を構成します。この手順は Microsoft Entra ID サーバーで実行する必要があります。
   a. コンソールを信頼するには、Microsoft Entra ID アプリを登録するときに次の値を使用します。
      - *リダイレクトURL*には、 `https://services.cloud.netapp.com`
      - *返信URL*には、 `https://netapp-cloud-account.auth0.com/login/callback`
   b. Microsoft Entra ID アプリのクライアント シークレットを作成します。フェデレーションを完了するには、クライアント ID、クライアント シークレット、Entra ID ドメイン名を提供する必要があります。
2. コンソールに戻り、[次へ] を選択して接続を作成します。

接続を作成

1. Microsoft Entra IDで接続を作成する
   a. 前の手順で作成したクライアント ID とクライアント シークレットを入力します。
   b. Microsoft Entra ID ドメイン名を入力します。
2. *接続を作成*を選択します。システムは数秒で接続を作成します。

接続をテストして有効にする

1. *次へ*を選択します。
2. 接続をテストするには、[接続テスト] を選択します。 IdP サーバーのログイン ページに移動します。 IdP 資格情報を使用してログインし、テストを完了してコンソールに戻り、接続を有効にします。
3. *次へ*を選択します。
4. *フェデレーションの有効化*ページでフェデレーションの詳細を確認し、*フェデレーションの有効化*を選択します。
5. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインできるようになります。

PingFederateで**NetApp Console**を連携

PingFederate IdP プロバイダーと連携して、 NetApp Consoleのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。 NetApp、両方ではなく、どちらか一方を選択することを推奨しています。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

PingFederate とのフェデレーション接続を設定して、コンソールのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、コンソールをサービス プロバイダーとして信頼するように PingFederate サーバーを構成し、コンソールで接続を作成します。

開始する前に

- 管理者権限を持つ IdP アカウントが必要です。 IdP 管理者と調整して手順を完了してください。
- フェデレーションに使用するドメインを特定します。自分のメールドメインまたは自分が所有する別のドメインを使用できます。電子メール ドメイン以外のドメインを使用する場合は、まずコンソールでドメインを確認する必要があります。以下の手順に従ってこれを行うことができます。"NetApp Consoleでドメインを確認する"トピック。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。
4. ドメインの詳細を入力してください:
   a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
   b. 構成するフェデレーションの名前を入力します。
   c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。
5. *次へ*を選択します。
6. 接続方法として、*プロバイダー*を選択し、次に*PingFederate*を選択します。
7. *次へ*を選択します。
8. PingFederate サーバーを、サービス プロバイダーとしてNetApp を信頼するように構成します。この手順は PingFederate サーバーで実行する必要があります。
   a. PingFederate を構成してNetApp Consoleを信頼する場合は、次の値を使用します。
      - *返信URL*または*アサーションコンシューマーサービス（ACS）URL*の場合は、`https://netapp-cloud-account.auth0.com/login/callback`
      - *ログアウトURL*には、`https://netapp-cloud-account.auth0.com/logout`
      - *オーディエンス/エンティティID*には、`urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`ここで、`<fed-domain-name-pingfederate>` はフェデレーションのドメイン名です。たとえば、ドメインが `example.com`オーディエンス/エンティティIDは次のようになります。 `urn:auth0:netappcloud-account:fed-example-com-pingfederate` 。
   b. PingFederate サーバーの URL をコピーします。コンソールで接続を作成するときに、この URL が必要になります。

c. PingFederate サーバーから X.509 証明書をダウンロードします。 Base64 でエンコードされた PEM 形式 (.pem、.crt、.cer) である必要があります。

9. コンソールに戻り、[次へ] を選択して接続を作成します。
10. PingFederateで接続を作成する
    a. 前の手順でコピーした PingFederate サーバーの URL を入力します。
    b. X.509 署名証明書をアップロードします。証明書は PEM、CER、または CRT 形式である必要があります。
11. *接続を作成*を選択します。システムは数秒で接続を作成します。
12. *次へ*を選択します。
13. 接続をテストするには、[接続テスト] を選択します。 IdP サーバーのログイン ページに移動します。 IdP 資格情報を使用してログインし、テストを完了してコンソールに戻り、接続を有効にします。
14. *次へ*を選択します。
15. *フェデレーションの有効化*ページでフェデレーションの詳細を確認し、*フェデレーションの有効化*を選択します。
16. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインできるようになります。

SAML ID プロバイダとの連携

SAML 2.0 IdP プロバイダーと連携して、NEtApp コンソールのシングル サインオン (SSO) を有効にします。これにより、ユーザーは企業の資格情報を使用してログインできるようになります。

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

企業の IdP またはNetAppサポート サイトと連携できます。両方と連携することはできません。

NetApp は、サービス プロバイダー開始 (SP開始) SSO のみをサポートします。まず、 NetApp をサービス プロバイダーとして信頼するように ID プロバイダーを構成する必要があります。次に、コンソールで ID プロバイダーの構成を使用する接続を作成できます。

SAML 2.0 プロバイダーとのフェデレーション接続を設定して、コンソールのシングル サインオン (SSO) を有効にすることができます。このプロセスでは、プロバイダーがNetApp をサービス プロバイダーとして信頼するように構成し、コンソールで接続を作成します。

開始する前に

- 管理者権限を持つ IdP アカウントが必要です。 IdP 管理者と調整して手順を完了してください。
- フェデレーションに使用するドメインを特定します。自分のメールドメインまたは自分が所有する別のドメインを使用できます。電子メール ドメイン以外のドメインを使用する場合は、まずコンソールでドメインを確認する必要があります。以下の手順に従ってこれを行うことができます。"NetApp Consoleでドメ

インを確認する"トピック。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federation** ページを表示するには、**Federation** を選択します。
3. *新しいフェデレーションの構成*を選択します。
4. ドメインの詳細を入力してください:
   a. 検証済みドメインを使用するか、メールドメインを使用するかを選択します。電子メール ドメインは、ログインしているアカウントに関連付けられているドメインです。
   b. 構成するフェデレーションの名前を入力します。
   c. 検証済みのドメインを選択する場合は、リストからドメインを選択します。
5. *次へ*を選択します。
6. 接続方法として、*プロトコル*を選択し、*SAML ID プロバイダー*を選択します。
7. *次へ*を選択します。
8. SAML ID プロバイダーを構成して、 NetApp をサービス プロバイダーとして信頼します。この手順は SAML プロバイダー サーバーで実行する必要があります。
   a. IdPに属性があることを確認する `email`ユーザーのメールアドレスに設定されます。これは、コンソールがユーザーを正しく識別するために必要です。

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">
        <saml:AttributeValue xsi:type="xs:string">
email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

   b. SAML アプリケーションをコンソールに登録するときは、次の値を使用します。
      - *返信URL*または*アサーションコンシューマーサービス（ACS）URL*の場合は、 https://netapp-cloud-account.auth0.com/login/callback
      - *ログアウトURL*には、 https://netapp-cloud-account.auth0.com/logout
      - *オーディエンス/エンティティID*には、 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`ここで、<fed-domain-name-saml> はフェデレーションに使用するドメイン名です。たとえば、ドメインが `example.com`オーディエンス/エンティティIDは次のようになります。 `urn:auth0:netapp-cloud-account:fed-example-com-samlp` 。
   c. 信頼を作成したら、SAML プロバイダー サーバーから次の値をコピーします。

- サインインURL
- サインアウトURL（オプション）

d. SAML プロバイダー サーバーから X.509 証明書をダウンロードします。 PEM、CER、または CRT 形式である必要があります。

9. コンソールに戻り、[次へ] を選択して接続を作成します。
10. SAML を使用して接続を作成します。
    a. SAML サーバーの サインイン **URL** を入力します。
    b. SAML プロバイダー サーバーからダウンロードした X.509 証明書をアップロードします。
    c. 必要に応じて、SAML サーバーの サインアウト **URL** を入力します。
11. *接続を作成*を選択します。システムは数秒で接続を作成します。
12. *次へ*を選択します。
13. 接続をテストするには、[接続テスト] を選択します。 IdP サーバーのログイン ページに移動します。 IdP 資格情報を使用してログインし、テストを完了してコンソールに戻り、接続を有効にします。
14. *次へ*を選択します。
15. *フェデレーションの有効化*ページでフェデレーションの詳細を確認し、*フェデレーションの有効化*を選択します。
16. プロセスを完了するには、[完了] を選択します。

フェデレーションを有効にすると、ユーザーは企業の資格情報を使用してNetApp Consoleにログインできるようになります。

NetApp Consoleでフェデレーションを管理する

NetApp Consoleでフェデレーションを管理できます。無効にしたり、期限切れの資格情報を更新したり、不要になった場合に無効にしたりすることができます。

NetApp Cloud Central を使用してフェデレーションを構成した場合は、フェデレーション ページからインポートして、コンソールで管理します。"フェデレーションをインポートする方法を学ぶ"

検証済みのドメインを既存のフェデレーションに追加することもできます。これにより、フェデレーション接続に複数のドメインを使用できるようになります。

フェデレーションの有効化、無効化、更新などのフェデレーション管理イベントがタイムラインに表示されます。"NetApp Consoleでの操作の監視について詳しく学習します。"

必要な役割

フェデレーションを作成および管理するには、フェデレーション管理者ロールが必要です。フェデレーション ビューアーはフェデレーション ページを表示できます。"アクセス ロールの詳細について説明します。"

フェデレーションを有効にする

フェデレーションを作成したが有効になっていない場合は、フェデレーション ページから有効にすることが

できます。フェデレーションを有効にすると、フェデレーションに関連付けられたユーザーは、企業の資格情報を使用してコンソールにログインできるようになります。フェデレーションを有効にする前に、フェデレーションを作成してテストしてください。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. アクションメニューを選択 有効にするフェデレーションの横にある をクリックし、[有効] を選択します。

検証済みのドメインを既存のフェデレーションに追加する

コンソールで既存のフェデレーションに検証済みのドメインを追加して、同じ ID プロバイダー (IdP) で複数のドメインを使用できます。

ドメインをフェデレーションに追加する前に、コンソールでドメインを検証しておく必要があります。ドメインをまだ確認していない場合は、以下の手順に従って確認することができます。"コンソールでドメインを確認する" 。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. アクションメニューを選択 検証済みドメインを追加するフェデレーションの横にある をクリックし、[ドメインの更新] を選択します。 ドメインの更新 ダイアログ ボックスには、このフェデレーションにすでに関連付けられているドメインが表示されます。
4. 利用可能なドメインのリストから検証済みのドメインを選択します。
5. *更新*を選択します。新しいドメイン ユーザーは、30 秒以内にフェデレーション コンソール アクセスを取得できます。

期限切れのフェデレーション接続の更新

コンソールでフェデレーションの詳細を更新できます。たとえば、証明書やクライアント シークレットなどの資格情報の有効期限が切れた場合は、フェデレーションを更新する必要があります。必要に応じて通知日を更新し、接続が期限切れになる前に更新するよう通知します。

ログインの問題を回避するには、IdP を更新する前にまずコンソールを更新してください。プロセス中はコンソールにログインしたままにしてください。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. 更新するフェデレーションの横にあるアクション メニュー (縦に並んだ 3 つのドット) を選択し、フェデレーションの更新 を選択します。
4. 必要に応じてフェデレーションの詳細を更新します。
5. *更新*を選択します。

既存のフェデレーションをテストする

既存のフェデレーションの接続をテストして、それが機能することを確認します。これにより、フェデレーションに関する問題を特定し、トラブルシューティングすることができます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. アクションメニューを選択:検証済みドメインを追加するフェデレーションの横にある をクリックし、[テスト接続] を選択します。
4. *テスト*を選択します。システムは、企業の資格情報を使用してログインするように要求します。接続が成功すると、 NetApp Consoleにリダイレクトされます。接続に失敗した場合は、フェデレーションの問題を示すエラー メッセージが表示されます。
5. *完了*を選択して*連合*タブに戻ります。

フェデレーションを無効にする

フェデレーションが不要になった場合は、無効にすることができます。これにより、フェデレーションに関連付けられたユーザーが企業の資格情報を使用してコンソールにログインできなくなります。必要に応じて、後でフェデレーションを再度有効にすることができます。

IdP を廃止する場合やフェデレーションを中止する場合など、フェデレーションを削除する前に無効にします。これにより、必要に応じて後で再度有効にすることができます。

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. アクションメニューを選択:検証済みドメインを追加するフェデレーションの横にある をクリックし、[無効にする] を選択します。

フェデレーションを削除する

フェデレーションが不要になった場合は、削除できます。これにより、フェデレーションが削除され、フェデレーションに関連付けられたすべてのユーザーが企業の資格情報を使用してコンソールにログインできなくなります。たとえば、IdP が廃止される場合や、フェデレーションが不要になった場合などです。

フェデレーションを削除した後は、回復することはできません。新しいフェデレーションを作成する必要があります。

フェデレーションを削除する前に無効にする必要があります。フェデレーションを削除した後で、元に戻すことはできません。

手順

1. *管理 > IDとアクセス*を選択します。
2. **Federations** ページを表示するには、**Federations** を選択します。
3. アクションメニューを選択:検証済みドメインを追加するフェデレーションの横にある をクリックし、[削除] を選択します。

NetApp Consoleにフェデレーションをインポートする

以前にNetApp Cloud Central (NetApp Consoleの外部アプリケーション) を通じてフェデレーションを設定したことがある場合は、フェデレーション ページで、既存のフェデレーション接続をコンソールにインポートして、新しいインターフェイスで管理できるようにするように求められます。そうすれば、フェデレーション接続を再作成しなくても、最新の拡張機能を活用できるようになります。

既存のフェデレーションをインポートした後、フェデレーション ページからフェデレーションを管理できます。"フェデレーションの管理について詳しく学びます。"

必要な役割

組織管理者またはフェデレーション管理者。"アクセス ロールの詳細について説明します。"

手順

1. *管理 > IDとアクセス*を選択します。
2. *Federation*タブを選択します。
3. *インポートフェデレーション*を選択します。

コンソールエージェント

コンソールエージェントVMとオペレーティングシステムを保守する

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、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。

既存のエージェントがいる場合は、次の点に注意してください。"サポートされている Linux オペレーティングシステムの変更" 。

オペレーティングシステムのパッチとエージェント

エージェント ホスト サービスを停止せずに OS セキュリティ パッチを適用します。

VMまたはインスタンスタイプ

コンソールからコンソール エージェントを作成すると、デフォルトの構成でクラウド プロバイダーに VM インスタンスがデプロイされます。エージェントを作成した後は、CPU や RAM が少ない小さな VM インスタンスに切り替えないでください。

次の表に、CPU と RAM の要件を示します。

CPU

8コアまたは8vCPU

RAM

32 GB

"エージェントのデフォルト設定について学ぶ" 。

エージェントを監視する

コンソールは、ディスク容量、RAM、CPU の問題など、エージェント VM に異常がある場合に通知します。コンソール内の通知センターでこれらの通知を監視するか、電子メール通知を構成します。ディスク容量、メモリ、CPU 使用率が時々増加するのは正常ですが、頻繁に発生する場合は、解決するための手順を実行する必要があります。

たとえば、エージェント リソース (CPU、RAM、またはディスク領域) が 30 分間連続して合計容量の 90% を超えると、コンソールから通知が届きます。その後、リソース使用量がそのしきい値を下回ると、通知センターに通知が解決済み (緑) として表示されます。

エージェント VM の変更について質問がある場合は、 NetAppサポートにお問い合わせください。

"詳細情報"

通知	必要な行動
ディスク容量が多すぎる	"NetAppナレッジベースの記事を確認する" 。
CPU使用率が高すぎる	インストールした場所に応じて、クラウド プロバイダーまたはオンプレミスのエージェント VM の CPU サイズを増やします。または、追加のエージェントを作成し、ワークロードを複数のエージェントに分散します。 RAM の使用率は、環境、 ONTAPワークロード、 Cloud Volumes ONTAPシステムの数、および使用しているデータ サービスによって異なります。
RAM使用量が高すぎる	インストールした場所に応じて、クラウド プロバイダーまたはオンプレミスのエージェント VM の RAM を増やします。または、追加のエージェントを作成し、ワークロードを複数のエージェントに分散します。 RAM の使用率は、環境、 ONTAPワークロード、 Cloud Volumes ONTAPシステムの数、および使用しているデータ サービスによって異なります。

エージェント**VM**の停止と起動

必要に応じて、クラウド プロバイダーのコンソールまたは標準のオンプレミス手順を使用して、エージェント VM を停止および起動します。

"コンソールエージェントは常に動作している必要があることに注意してください" 。

Linux VMに接続する

エージェントが実行される Linux VM に接続する必要がある場合は、クラウド プロバイダーの接続オプションを使用します。

AWS

AWS でエージェントインスタンスを作成するときは、AWS アクセスキーとシークレットキーを指定します。このキー ペアを使用してインスタンスに SSH 接続できます。 EC2 Linux インスタンスにはユーザー名「ubuntu」を使用します。 2023 年 5 月より前に作成されたエージェントの場合は、ユーザー名「ec2-user」を使用します。

"AWS ドキュメント: Linux インスタンスに接続する"

Azure

Azure でエージェント VM を作成するときは、ユーザー名を指定し、パスワードまたは SSH 公開キーで認証することを選択します。 VM に接続するために選択した認証方法を使用します。

"Azure ドキュメント: VM への SSH 接続"

Google Cloud

Google Cloud でエージェントを作成するときに認証方法を指定することはできません。ただし、Google Cloud Console または Google Cloud CLI (gcloud) を使用して Linux VM インスタンスに接続できます。

"Google Cloud ドキュメント: Linux VM への接続"

エージェントの**IP**アドレスを変更する

必要に応じて、クラウド プロバイダーによって割り当てられたエージェント インスタンスの内部 IP アドレスとパブリック IP アドレスを変更できます。

手順

1. クラウド プロバイダーの指示に従って、エージェント インスタンスのローカル IP アドレスまたはパブリック IP アドレス (あるいはその両方) を変更します。
2. エージェント インスタンスを再起動して、新しいパブリック IP アドレスをコンソールに登録します。
3. プライベート IP アドレスを変更した場合は、 Cloud Volumes ONTAP構成ファイルのバックアップ場所を更新して、バックアップがエージェントの新しいプライベート IP アドレスに送信されるようにします。

   各Cloud Volumes ONTAPシステムのバックアップ場所を更新します。

   a. Cloud Volumes ONTAP CLI から、権限レベルを高度に設定します。

   ```
   set -privilege advanced
   ```

   b. 現在のバックアップ ターゲットを表示するには、次のコマンドを実行します。

   ```
   system configuration backup settings show
   ```

   c. バックアップ ターゲットの IP アドレスを更新するには、次のコマンドを実行します。

   ```
   system configuration backup settings modify -destination <target-
   location>
   ```

エージェントの**URI**を編集する

エージェントの Uniform Resource Identifier (URI) を追加および削除できます。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、コンソール エージェントのアクション メニューを選択し、*エージェントの編集*を選択します。

   編集するには、コンソール エージェントがアクティブである必要があります。

3. エージェント URI を表示するには、エージェント **URI** バーを展開します。
4. URI を追加および削除し、[適用] を選択します。

コンソールエージェント用の **VCenter** または **ESXi** ホストを維持する

コンソール エージェントを展開した後、既存の VCenter または ESXi ホストに変更を加えることができます。たとえば、コンソール エージェントをホストする VM インスタンスの CPU または RAM を増やすことができます。

VM Web コンソールを使用して次のメンテナンス タスクを実行します。

- ディスクサイズを増やす
- エージェントを再起動する
- 静的ルートを更新する
- 検索ドメインを更新する

制限事項

コンソール経由でのエージェントのアップグレードはまだサポートされていません。さらに、IP アドレス、DNS、ゲートウェイに関する情報のみを表示できます。

VMメンテナンスコンソールにアクセスする

VSphere クライアントからメンテナンス コンソールにアクセスできます。

手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。

メインユーザーのパスワードを変更する

パスワードを変更することができます `maint`ユーザー。

手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `1`表示するには `System Configuration`メニュー。
6. 入力 `1`メンテナンス ユーザーのパスワードを変更し、画面の指示に従います。

VMインスタンスのCPUまたはRAMを増やす

コンソール エージェントをホストする VM インスタンスの CPU または RAM を増やすことができます。

VCenter または ESXi ホストで VM インスタンス設定を編集し、メンテナンス コンソールを使用して変更を適用します。

VSphereクライアントでの手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. VM インスタンスを右クリックし、[設定の編集] を選択します。
4. /opt または /var パーティションに使用されるハード ドライブの領域を増やします。
   a. /opt に使用されるハード ドライブの領域を増やすには、ハード ディスク **2** を選択します。
   b. /var に使用されるハードドライブの容量を増やすには、ハード ディスク **3** を選択します。
5. 変更を保存します。

メンテナンスコンソールの手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `1 to view the `System Configuration`メニュー。
6. 入力 `2`画面上の指示に従います。コンソールは新しい設定をスキャンし、パーティションのサイズを増やします。

エージェントVMのネットワーク設定を表示する

VSphere クライアントでエージェント VM のネットワーク設定を表示して、ネットワークの問題を確認またはトラブルシューティングします。次のネットワーク設定は表示のみ可能で、更新はできません: IP アドレスと DNS の詳細。

手順

1. VSphere クライアントを開き、VCenter にログインします。

2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `2`表示するには `Network Configuration`メニュー。
6. 対応するネットワーク設定を表示するには、1 ～ 6 の数字を入力します。

エージェント**VM**の静的ルートを更新する

必要に応じて、エージェント VM の静的ルートを追加、更新、または削除します。

手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `2`表示するには `Network Configuration`メニュー。
6. 入力 `7`静的ルートを更新し、画面の指示に従います。
7. Enterキーを押します。
8. 必要に応じて、追加の変更を加えます。
9. 入力 `9`変更をコミットします。

エージェント**VM**のドメイン検索設定を更新する

エージェント VM の検索ドメイン設定を更新できます。

手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `2``表示するには `Network Configuration`メニュー。
6. 入力 `8`ドメイン検索設定を更新し、画面の指示に従います。
7. Enterキーを押します。
8. 必要に応じて、追加の変更を加えます。
9. 入力 `9`変更をコミットします。

エージェント診断ツールにアクセスする

コンソール エージェントの問題をトラブルシューティングするための診断ツールにアクセスします。 NetApp サポートは、問題のトラブルシューティング時にこれを実行するように依頼する場合があります。

手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `3`サポートと診断メニューを表示します。
6. 入力 `1`診断ツールにアクセスし、画面上の指示に従います。 + たとえば、すべてのエージェント サービスが実行されていることを確認できます。"コンソールエージェントのステータスを確認する" 。

エージェント診断ツールにリモートでアクセスする

Putty などのツールを使用して、診断ツールにリモートでアクセスできます。ワンタイム パスワードを割り当てて、エージェント VM への SSH アクセスを有効にします。

SSH アクセスにより、コピー アンド ペーストなどの高度なターミナル機能が有効になります。

手順

1. VSphere クライアントを開き、VCenter にログインします。
2. コンソール エージェントをホストする VM インスタンスを選択します。
3. **Web** コンソールの起動 を選択します。
4. VM インスタンスの作成時に指定したユーザー名とパスワードを使用して、VM インスタンスにログインします。ユーザー名は `maint`パスワードは、VM インスタンスの作成時に指定したパスワードです。
5. 入力 `3`表示するには `Support and Diagnostics`メニュー。
6. 入力 `2`診断ツールにアクセスし、画面上の指示に従って 24 時間で期限が切れるワンタイム パスワードを設定します。
7. PuttyなどのSSHツールを使用して、ユーザー名でエージェントVMに接続します。 `diag`および設定したワンタイムパスワード。

Webベースのコンソールアクセス用に**CA**署名証明書をインストールする

NetApp Consoleを制限モードで使用する場合、クラウド リージョンまたはオンプレミスに展開されているコンソール エージェント仮想マシンからユーザー インターフェイスにアクセスできます。デフォルトでは、コンソールは自己署名 SSL 証明書を使用して、コンソール エージェント上で実行されている Web ベースのコンソールへの安全な HTTPS アクセスを提供します。

ビジネスで必要な場合は、証明機関 (CA) によって署名された証明書をインストールできます。これにより、自己署名証明書よりも優れたセキュリティ保護が提供されます。証明書をインストールすると、ユーザーが Web ベースのコンソールにアクセスするときに、コンソールは CA 署名付き証明書を使用します。

HTTPS証明書をインストールする

コンソール エージェント上で実行されている Web ベースのコンソールに安全にアクセスするために、CA によって署名された証明書をインストールします。

タスク概要

次のいずれかのオプションを使用して証明書をインストールできます。

- コンソールから証明書署名要求 (CSR) を生成し、証明書要求を CA に送信して、CA 署名証明書をコンソール エージェントにインストールします。

  コンソールが CSR を生成するために使用するキー ペアは、コンソール エージェントに内部的に保存されます。コンソール エージェントに証明書をインストールすると、コンソールは同じキー ペア (秘密キー) を自動的に取得します。

- すでに持っている CA 署名付き証明書をインストールします。

  このオプションを選択すると、CSR はコンソールを通じて生成されません。 CSR を別途生成し、秘密鍵を外部に保存します。証明書をインストールするときに、コンソールに秘密キーを提供します。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、コンソール エージェントのアクション メニューを選択し、*HTTPS セットアップ*を選択します。

   編集するには、コンソール エージェントがアクティブである必要があります。

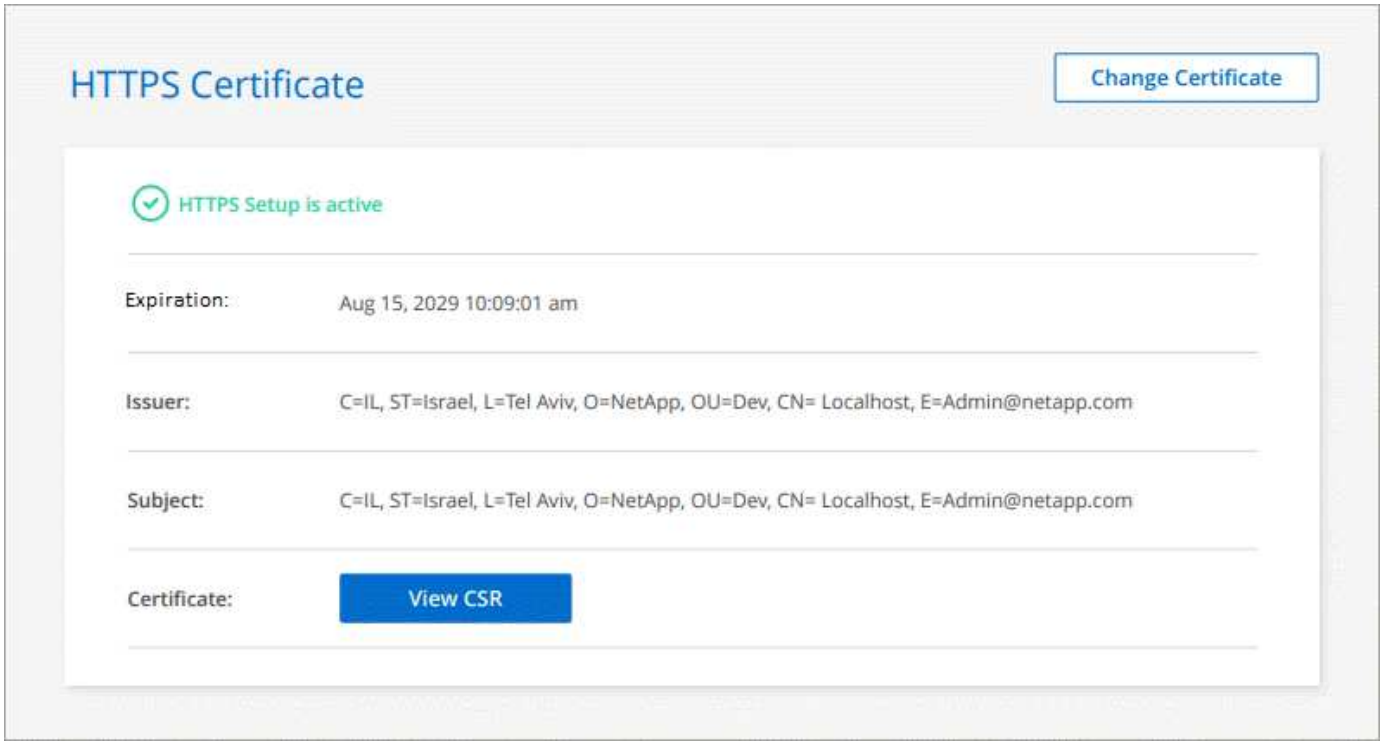
3. HTTPS セットアップ ページで、証明書署名要求 (CSR) を生成するか、独自の CA 署名証明書をインストールして証明書をインストールします。

オプション	説明
CSRを生成する	a. コンソール エージェント ホストのホスト名または DNS (共通名) を入力し、[CSR の生成] を選択します。 コンソールに証明書署名要求が表示されます。 b. CSR を使用して、SSL 証明書要求を CA に送信します。 証明書には、Privacy Enhanced Mail (PEM) Base-64 エンコード X.509 形式を使用する必要があります。 c. 証明書ファイルをアップロードし、[インストール] を選択します。

オプション	説明
独自のCA署名証明書をインストールする	a. *CA 署名証明書のインストール*を選択します。 b. 証明書ファイルと秘密キーの両方をロードし、[インストール] を選択します。 証明書には、Privacy Enhanced Mail (PEM) Base-64 エンコード X.509 形式を使用する必要があります。

結果

コンソール エージェントは、CA 署名証明書を使用して安全な HTTPS アクセスを提供するようになりました。次の画像は、安全なアクセス用に構成されたエージェントを示しています。



コンソールの**HTTPS**証明書を更新する

安全なアクセスを確保するには、エージェントの HTTPS 証明書が期限切れになる前に更新する必要があります。証明書の有効期限が切れる前に更新しないと、ユーザーが HTTPS を使用して Web コンソールにアクセスしたときに警告が表示されます。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、コンソール エージェントのアクション メニューを選択し、*HTTPS セットアップ*を選択します。

   有効期限を含む証明書の詳細が表示されます。
3. *証明書の変更*を選択し、手順に従って CSR を生成するか、独自の CA 署名証明書をインストールします。

プロキシサーバーを使用するようにコンソールエージェントを構成する

企業ポリシーでインターネットへのすべての通信にプロキシ サーバーの使用が求められている場合は、そのプロキシ サーバーを使用するようにエージェントを構成する必要があります。インストール時にコンソール エージェントがプロキシ サーバーを使用するように構成しなかった場合は、いつでもそのプロキシ サーバーを使用するようにコンソール エージェントを構成できます。

エージェントのプロキシ サーバーは、パブリック IP または NAT ゲートウェイなしでアウトバウンドのインターネット アクセスを可能にします。プロキシ サーバーは、Cloud Volumes ONTAPシステムではなく、コンソール エージェントに対してのみ送信接続を提供します。

Cloud Volumes ONTAPシステムにアウトバウンド インターネット アクセスがない場合、コンソールはコンソール エージェントのプロキシ サーバーを使用するようにシステムを構成します。コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認する必要があります。コンソール エージェントを展開した後、このポートを開きます。

コンソール エージェント自体に送信インターネット接続がない場合、 Cloud Volumes ONTAPシステムは構成されたプロキシ サーバーを使用できません。

サポートされている構成

- Cloud Volumes ONTAPシステムにサービスを提供するエージェントでは、透過プロキシ サーバーがサポートされています。 Cloud Volumes ONTAPでNetAppデータ サービスを使用する場合は、透過プロキシ サーバーを使用できるCloud Volumes ONTAP専用のエージェントを作成します。
- 明示的なプロキシ サーバーは、 Cloud Volumes ONTAPシステムを管理するエージェントやNetAppデータ サービスを管理するエージェントを含むすべてのエージェントでサポートされています。
- HTTP と HTTPS。
- プロキシ サーバーはクラウドまたはネットワーク内に配置できます。

> プロキシを設定したら、プロキシの種類を変更することはできません。プロキシ タイプを変更する必要がある場合は、コンソール エージェントを削除し、新しいプロキシ タイプで新しいエージェントを追加します。

コンソールエージェントで明示的なプロキシを有効にする

プロキシ サーバーを使用するようにコンソール エージェントを構成すると、そのエージェントとそれが管理するCloud Volumes ONTAPシステム (HA メディエーターを含む) はすべてプロキシ サーバーを使用します。

この操作により、コンソール エージェントが再起動されます。続行する前に、コンソール エージェントがアイドル状態であることを確認してください。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、コンソール エージェントのアクション メニューを選択し、*エージェントの編集*を選択します。

   編集するには、コンソール エージェントがアクティブである必要があります。

3. *HTTP プロキシ構成*を選択します。
4. 構成タイプ フィールドで 明示的なプロキシ を選択します。
5. *プロキシを有効にする*を選択します。
6. 構文を使用してサーバーを指定します http://address:portまたは https://address:port
7. サーバーに基本認証が必要な場合は、ユーザー名とパスワードを指定します。

   次の点に注意してください。

   - ユーザーはローカル ユーザーまたはドメイン ユーザーになります。
   - ドメインユーザーの場合は、\ の ASCII コードを次のように入力する必要があります: domain-name%92user-name

     例: netapp%92proxy

   - コンソールは @ 文字を含むパスワードをサポートしていません。
8. *保存*を選択します。

コンソールエージェントの透過プロキシを有効にする

Cloud Volumes ONTAPのみが、コンソール エージェントでの透過プロキシの使用をサポートしています。Cloud Volumes ONTAPに加えてNetAppデータ サービスを使用する場合は、データ サービス用またはCloud Volumes ONTAP用として別のエージェントを作成する必要があります。

透過プロキシを有効にする前に、次の要件が満たされていることを確認してください。

- エージェントは、透過プロキシ サーバーと同じネットワークにインストールされます。
- プロキシ サーバーで TLS 検査が有効になっています。
- 透過プロキシ サーバーで使用されている証明書と一致する PEM 形式の証明書があります。
- Cloud Volumes ONTAP以外のNetAppデータ サービスにはコンソール エージェントを使用しないでください。

既存のエージェントを透過プロキシ サーバーを使用するように構成するには、コンソール エージェント ホストのコマンド ラインから使用できるコンソール エージェント メンテナンス ツールを使用します。

プロキシ サーバーを構成すると、コンソール エージェントが再起動します。続行する前に、コンソール エージェントがアイドル状態であることを確認してください。

手順

プロキシ サーバーの PEM 形式の証明書ファイルがあることを確認します。証明書がない場合は、ネットワーク管理者に問い合わせて取得してください。

1. コンソール エージェント ホストでコマンド ライン インターフェイスを開きます。
2. コンソール エージェント メンテナンス ツール ディレクトリに移動します。
   `/opt/application/netapp/service-manager-2/agent-maint-console`

3. 透過プロキシを有効にするには、次のコマンドを実行します。 `/home/ubuntu/<certificate-file>.pem`プロキシ サーバーのディレクトリと証明書ファイルの名前です。

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

証明書ファイルが PEM 形式であり、コマンドと同じディレクトリに存在することを確認するか、証明書ファイルへのフルパスを指定します。

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

コンソールエージェントの透過プロキシを変更する

コンソールエージェントの既存の透過プロキシサーバーを更新するには、 `proxy update`コマンドを使用して透過プロキシサーバーを削除するか、 `proxy remove`指示。詳細については、次のドキュメントを参照してください。"エージェントメンテナンスコンソール" 。

プロキシを設定したら、プロキシの種類を変更することはできません。プロキシ タイプを変更する必要がある場合は、コンソール エージェントを削除し、新しいプロキシ タイプで新しいエージェントを追加します。

インターネットへのアクセスが失われた場合は、コンソールエージェントプロキシを更新します。

ネットワークのプロキシ構成が変更されると、エージェントはインターネットにアクセスできなくなる可能性があります。たとえば、誰かがプロキシ サーバーのパスワードを変更したり、証明書を更新したりした場合などです。この場合、コンソール エージェント ホストから直接 UI にアクセスし、設定を更新する必要があります。コンソール エージェント ホストへのネットワーク アクセスがあり、コンソールにログインできることを確認します。

直接**API**トラフィックを有効にする

コンソール エージェントがプロキシ サーバーを使用するように構成した場合は、コンソール エージェントで直接 API トラフィックを有効にして、プロキシを経由せずに API 呼び出しをクラウド プロバイダー サービスに直接送信できます。AWS、Azure、または Google Cloud で実行されているエージェントはこのオプションをサポートしています。

Cloud Volumes ONTAPで Azure Private Links を無効にしてサービス エンドポイントを使用する場合は、直接 API トラフィックを有効にします。そうしないと、トラフィックは適切にルーティングされません。

"Cloud Volumes ONTAPで Azure Private Link またはサービス エンドポイントを使用する方法の詳細"

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、コンソール エージェントのアクション メニューを選択し、*エージェントの編集*を選択します。

   編集するには、コンソール エージェントがアクティブである必要があります。

3. *直接 API トラフィックのサポート*を選択します。
4. チェックボックスを選択してオプションを有効にし、[保存] を選択します。

Amazon EC2 インスタンスで IMDSv2 の使用を必須にする

NetApp Consoleは、コンソール エージェントとCloud Volumes ONTAP (HA 展開のメディエーターを含む) を使用して、Amazon EC2 インスタンス メタデータ サービス バージョン 2 (IMDSv2) をサポートします。ほとんどの場合、IMDSv2 は新しい EC2 インスタンスで自動的に構成されます。 IMDSv1 は 2024 年 3 月より前に有効化されました。セキュリティ ポリシーで必要な場合は、EC2 インスタンスで IMDSv2 を手動で設定する必要がある場合があります。

開始する前に

- コンソール エージェントのバージョンは 3.9.38 以降である必要があります。
- Cloud Volumes ONTAP は次のいずれかのバージョンを実行している必要があります。
  - 9.12.1 P2（またはそれ以降のパッチ）
  - 9.13.0 P4（またはそれ以降のパッチ）
  - 9.13.1 またはこのリリース以降のバージョン
- この変更を行うには、Cloud Volumes ONTAPインスタンスを再起動する必要があります。
- これらの手順では、応答ホップ制限を 3 に変更する必要があるため、AWS CLI を使用する必要があります。

タスク概要

IMDSv2 は脆弱性に対する保護を強化します。 "IMDSv2 の詳細については、AWS セキュリティブログをご覧ください。"

インスタンス メタデータ サービス (IMDS) は、EC2 インスタンスで次のように有効化されます。

- コンソールから、またはコンソールを使用して新しいコンソールエージェントを展開する場合 "Terraform スクリプト"、IMDSv2 は EC2 インスタンスでデフォルトで有効になっています。
- AWS で新しい EC2 インスタンスを起動し、コンソールエージェントソフトウェアを手動でインストールすると、IMDSv2 もデフォルトで有効になります。
- AWS Marketplace からコンソールエージェントを起動すると、IMDSv1 がデフォルトで有効になります。EC2 インスタンスで IMDSv2 を手動で設定できます。
- 既存のコンソールエージェントの場合、IMDSv1 は引き続きサポートされますが、必要に応じて EC2 インスタンスで IMDSv2 を手動で設定することもできます。
- Cloud Volumes ONTAPの場合、新規インスタンスと既存インスタンスで IMDSv1 がデフォルトで有効になっています。必要に応じて、EC2 インスタンスで IMDSv2 を手動で設定することもできます。

手順

1. コンソール エージェント インスタンスで IMDSv2 の使用を必須にします。
   a. コンソール エージェントの Linux VM に接続します。

AWS でコンソール エージェント インスタンスを作成したときに、AWS アクセス キーとシークレット キーを指定しました。このキー ペアを使用してインスタンスに SSH 接続できます。 EC2 Linux インスタンスのユーザー名は ubuntu です (2023 年 5 月より前に作成されたコンソールエージェントの場合、ユーザー名は ec2-user でした)。

"AWS ドキュメント: Linux インスタンスに接続する"

b. AWS CLI をインストールします。

"AWS ドキュメント: AWS CLI の最新バージョンをインストールまたは更新する"

c. 使用 `aws ec2 modify-instance-metadata-options`IMDSv2 の使用を必須にし、PUT 応答のホップ制限を 3 に変更するコマンド。

例

```
aws ec2 modify-instance-metadata-options \
    --instance-id <instance-id> \
    --http-put-response-hop-limit 3 \
    --http-tokens required \
    --http-endpoint enabled
```

その `http-tokens`パラメータは IMDSv2 を必須に設定します。いつ `http-tokens`必須の場合は、 `http-endpoint`有効にします。

2. Cloud Volumes ONTAPインスタンスで IMDSv2 の使用を必須にします。
   a. に行く "Amazon EC2 コンソール"
   b. ナビゲーション ペインから、[インスタンス] を選択します。
   c. Cloud Volumes ONTAPインスタンスを選択します。
   d. *アクション > インスタンス設定 > インスタンスメタデータオプションの変更*を選択します。
   e. インスタンス メタデータ オプションの変更 ダイアログ ボックスで、以下を選択します。
      - インスタンス メタデータ サービス の場合は、有効 を選択します。
      - *IMDSv2*の場合は*必須*を選択します。
      - *保存*を選択します。
   f. HA メディエーターを含む他のCloud Volumes ONTAPインスタンスに対しても、これらの手順を繰り返します。
   g. "Cloud Volumes ONTAPインスタンスを停止して起動する"

結果

コンソール エージェント インスタンスとCloud Volumes ONTAPインスタンスが IMDSv2 を使用するように構成されました。

コンソールエージェントのアップグレードを管理する

標準モードまたは制限モードを使用する場合、コンソール エージェントがソフトウェア更新を取得するためのアウトバウンド インターネット アクセスを持っている限り、NetApp Consoleはコンソール エージェントを最新リリースに自動的にアップグレードします。

コンソール エージェントのアップグレードを手動で管理する必要がある場合は、標準モードまたは制限モードの自動アップグレードを無効にすることができます。

自動アップグレードを無効にする

コンソール エージェントの自動アップグレードを無効にするには、2 つの手順を実行します。まず、コンソール エージェントが正常で最新の状態であることを確認する必要があります。次に、構成ファイルを編集して自動アップグレードをオフにします。

自動アップグレードを無効にできるのは、コンソール エージェント バージョン 3.9.48 以降を使用している場合のみです。

エージェントの健全性を確認する

エージェントが安定しており、エージェント VM 上で実行されているすべてのコンテナが正常に動作していることを確認する必要があります。自動アップグレードを無効にすると、エージェント VM は新しいサービスまたはアップグレード パッケージのチェックを停止します。

コンソール エージェントを確認するには、次のいずれかのコマンドを使用します。すべてのサービスのステータスは「実行中」になっている必要があります。そうでない場合は、自動アップグレードを無効にする前にNetAppサポートにお問い合わせください。

Docker (Ubuntu および **VCenter** のデプロイメント用**)**

```
docker ps -a
```

ポッドマン

```
podman ps -a
```

エージェントの自動アップグレードを無効にする

自動アップグレードを無効にするには、*com/opt/application/netapp/service-manager-2/config.json* ファイルで *isUpgradeDisabled* フラグを設定します。デフォルトでは、このフラグは false に設定されており、エージェントは自動的にアップグレードされます。自動アップグレードを無効にするには、このフラグを true に設定できます。この手順を完了する前に、JSON 構文を理解しておく必要があります。

自動アップグレードを再度有効にするには、次の手順に従い、*isUpgradeDisabled* フラグを false に設定します。

手順

1. エージェントが最新かつ正常であることを確認してください。

2. 変更を元に戻せるように、*/opt/application/netapp/service-manager-2/config.json* ファイルのバックアップコピーを作成します。
3. */opt/application/netapp/service-manager-2/config.json* ファイルを編集し、*isUpgradeDisabled* フラグの値を true に変更します。

```
  "isUpgradeDisabled": true,
```

4. ファイルを保存します。
5. 次のコマンドを実行して、サービス マネージャー 2 サービスを再起動します。

```
systemctl restart netapp-service-manager.service
```

6. 次のコマンドを実行し、エージェントのステータスが *active(running)* と表示されていることを確認します: _

```
systemctl status netapp-service-manager.service
_
```

コンソールエージェントをアップグレードする

アップグレード プロセス中にコンソール エージェントを再起動する必要があるため、アップグレード中はNetApp Consoleは使用できません。

手順

1. コンソールエージェントソフトウェアを以下からダウンロードします。 "NetAppサポート サイト" 。
2. インストーラーを Linux ホストにコピーします。
3. スクリプトを実行するための権限を割り当てます。

```
chmod +x /path/NetApp-Console-Agent-Offline-<version>
```

<version> は、ダウンロードしたコンソール エージェントのバージョンです。

4. インストール スクリプトを実行します。

```
sudo /path/NetApp-Console-Agent-Offline-<version>
```

ここで、<version> はダウンロードしたエージェントのバージョンです。

5. アップグレードが完了したら、管理 > サポート > エージェント に移動してエージェントのバージョンを確認できます。

複数のコンソールエージェントを操作する

複数のコンソール エージェントを使用する場合は、コンソールから直接それらのコンソール エージェントを切り替えて、関連付けられているシステムを表示できます。

コンソールエージェントを切り替える

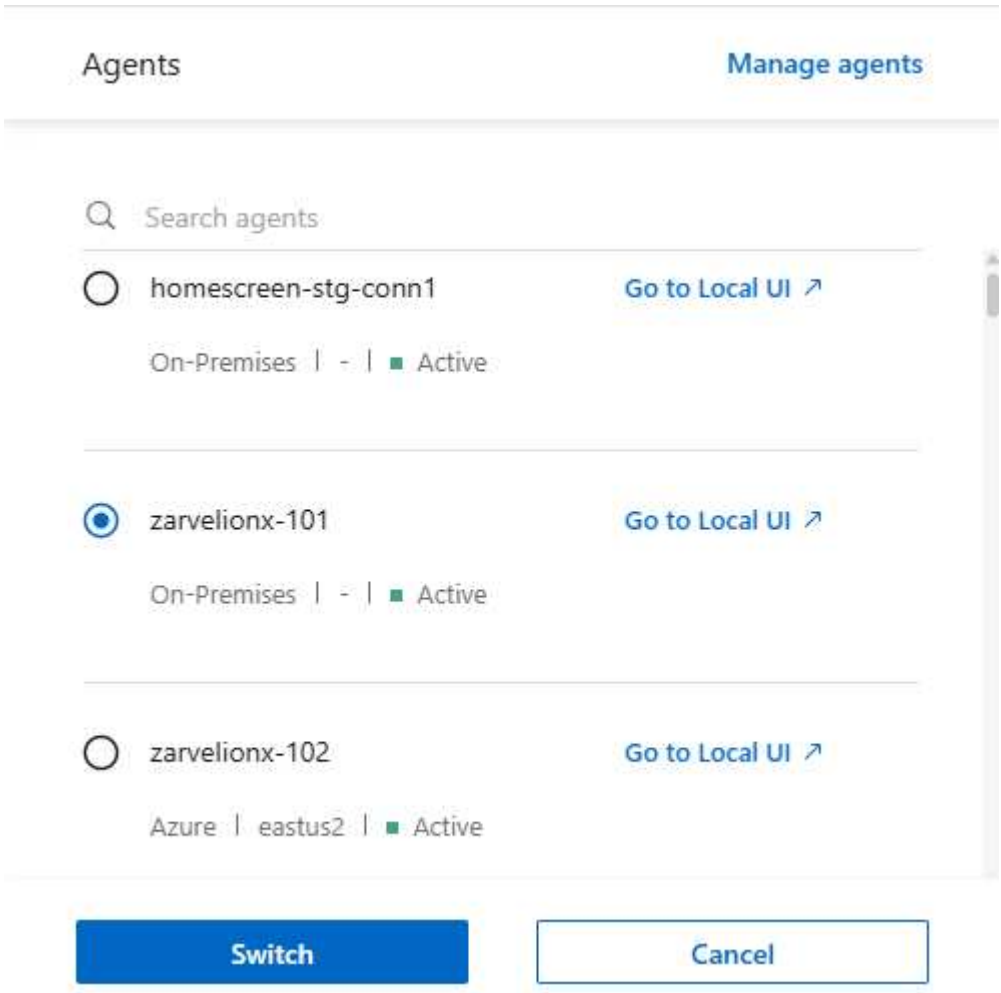
複数のコンソール エージェントがある場合は、それらを切り替えて、特定のエージェントに関連付けられているシステムを表示できます。

たとえば、マルチクラウド環境では、AWS にエージェントが 1 つあり、Google Cloud に別のエージェントがある場合があります。これらのエージェントを切り替えて、それぞれのクラウド環境内のCloud Volumes ONTAPシステムを管理します。

このオプションは、エージェントのローカル UI からNetApp Consoleを表示するときには使用できません。

手順

1. コンソールエージェントアイコン（ ）をクリックすると、利用可能なエージェントのリストが表示されます。



結果

コンソールが更新され、選択したエージェントに関連付けられているシステムが表示されます。

災害復旧構成を設定する

災害復旧の目的で、複数のコンソール エージェントを使用して同時にシステムを管理できます。 1 つのコンソール エージェントがダウンした場合は、他のエージェントに切り替えてシステムをすぐに管理できます。

手順

1. コンソール エージェントで管理する他のコンソール エージェントに切り替えます。
2. 既存のシステムを発見する。
   - "既存のCloud Volumes ONTAPシステムをコンソールに追加する"
   - "ONTAPクラスタの検出"
3. Cloud Volumes ONTAPシステムを管理している場合は、容量管理モードを 手動モード に調整します。

   競合の問題を回避するには、メインのコンソール エージェントのみを 自動モード に設定する必要があります。

   "容量管理モードの詳細"

コンソールエージェントのトラブルシューティング

コンソール エージェントの問題をトラブルシューティングするには、自分で問題を確認するか、 NetAppサポートに問い合わせて、システム ID、エージェント バージョン、または最新のAutoSupportメッセージを尋ねられることがあります。

NetAppサポートサイトのアカウントをお持ちの場合は、"NetAppナレッジベース。"

一般的なエラーメッセージと解決策

次の表に、一般的なエラー メッセージとその解決方法を示します。

エラー メッセージ	説明	何をするか
コンソールエージェントUIを読み込めません	エージェントのインストールに失敗しました	• Service Manager サービスがアクティブであることを確認します。 • すべてのコンテナが実行されていることを確認します。 • ファイアウォールがポート 8888 でのサービスへのアクセスを許可していることを確認してください。 • 問題が解決しない場合は、サポートにお問い合わせください。

エラー メッセージ	説明	何をするか
NetAppエージェントUIにアクセスできません	このメッセージは、エージェントの IP アドレスにアクセスしようとしたときに表示されます。エージェントに適切なネットワーク アクセスがない場合や不安定な場合は、初期化に失敗する可能性があります。	• コンソール エージェントに接続します。 • サービスマネージャサービスを確認する • エージェントに必要なネットワーク アクセス権があることを確認します。"必要なネットワーク アクセス エンドポイントの詳細について説明します。"
エージェント設定を読み込めません	エージェント設定ページにアクセスしようとすると、コンソールにこのメッセージが表示されます。	• OCCM コンテナが実行中であり、動作しているかどうかを確認します。 • 問題が解決しない場合は、サポートにお問い合わせください。
エージェントのサポート情報を読み込めません。	エージェントがサポート アカウントにアクセスできない場合、このメッセージが表示されます。	• *。

コンソールエージェントのステータスを確認する

コンソール エージェントを確認するには、次のいずれかのコマンドを使用します。すべてのサービスのステータスは「実行中」になっている必要があります。そうでない場合は、 NetAppサポートにお問い合わせください。

コンソール エージェント診断へのアクセスの詳細については、次のトピックを参照してください。

- "コンソール エージェントのステータスを確認する (Linux ホスト展開の場合)"
- "コンソール エージェントのステータスを確認する (VCenter 展開の場合)"

Docker (Ubuntu および VCenter のデプロイメント用)

```
docker ps -a
```

Podman (RedHat Enterprise Linux デプロイメント用)

```
podman ps -a
```

コンソールエージェントのバージョンを表示する

コンソール エージェントのバージョンを表示してアップグレードを確認するか、 NetApp の担当者と共有してください。

手順

1. *管理 > サポート > エージェント*を選択します。

   コンソールのページ上部にバージョンが表示されます。

ネットワークアクセスを確認する

コンソール エージェントに必要なネットワーク アクセスがあることを確認します。"必要なネットワーク アクセス ポイントの詳細について説明します。"

コンソールエージェントのインストールに関する問題

インストールに失敗した場合は、レポートとログを表示して問題を解決してください。

次のディレクトリにあるコンソール エージェント ホストから、JSON 形式の検証レポートと構成ログに直接アクセスすることもできます。

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- 新しいエージェントの展開では、 NetApp は次のエンドポイントをチェックします。"ここに記載" 。アップグレードに使用した以前のエンドポイントを使用している場合、この構成チェックはエラーで失敗します。"ここに記載" 。 NetAppは、現在のエンドポイントへのアクセスを許可し、以前のエンドポイントへのアクセスをブロックするようにファイアウォールルールを更新することを推奨します。"ネットワークをアップデートする方法を学ぶ" 。
- ファイアウォールのエンドポイントを更新しても、既存のエージェントは引き続き動作します。

手動インストールの構成チェックを無効にする

インストール中に送信接続を検証する構成チェックを無効にする必要がある場合があります。例えば：

- Government Cloud 環境にエージェントを手動でインストールする場合は、構成チェックを無効にする必要があります。無効にしないと、インストールは失敗します。
- エージェントのアップグレードに以前のエンドポイント リストを引き続き使用している場合は、これらのチェックを無効にすることもできます。

手順

com/opt/application/netapp/service-manager-2/config.json ファイルで *skipConfigCheck* フラグを設定することで、構成チェックを無効にします。デフォルトでは、このフラグは false に設定されており、構成チェックによってエージェントの送信アクセスが検証されます。チェックを無効にするには、このフラグを true に設定します。この手順を完了する前に、JSON 構文を理解しておく必要があります。

構成チェックを再度有効にするには、次の手順に従い、*skipConfigCheck* フラグを false に設定します。

手順

1. コンソール エージェント ホストに root または sudo 権限でアクセスします。
2. 変更を元に戻せるように、*/opt/application/netapp/service-manager-2/config.json* ファイルのバックアップコピーを作成します。
3. 次のコマンドを実行して、サービス マネージャー 2 サービスを停止します。

```
systemctl stop netapp-service-manager.service
```

1. */opt/application/netapp/service-manager-2/config.json* ファイルを編集し、*skipConfigCheck* フラグの値を true に変更します。

```
  "skipConfigCheck": true,
```

2. ファイルを保存します。
3. 次のコマンドを実行して、サービス マネージャー 2 サービスを再起動します。

```
systemctl restart netapp-service-manager.service
```

アップグレードに使用されたエンドポイントでのインストールの失敗

まだ使用している場合は"以前のエンドポイント"エージェントのアップグレードに使用すると、検証が失敗し、エラーが発生します。これを回避するには、検証エージェント構成 チェックボックスをオフにするか、VCenter にインストールするときに構成チェックをスキップします。

NetAppは、ファイアウォールルールを更新して、"現在のエンドポイント"ご都合の良い時に。"エンドポイントを更新する方法を学ぶ" 。

唯一のエラーが以前のエンドポイントに関連していることを確認してください。

- https://bluexpinfraprod.eastus2.data.azurecr.io
- https://bluexpinfraprod.azurecr.io

他にエラーがある場合は、続行する前に解決する必要があります。

NetAppサポートと連携する

コンソール エージェントの問題を解決できない場合は、 NetAppサポートにお問い合わせください。 NetAppサポートでは、コンソール エージェント ID を要求したり、コンソール エージェント ログがまだない場合はそれを送信するよう要求したりすることがあります。

コンソールエージェント**ID**を見つける

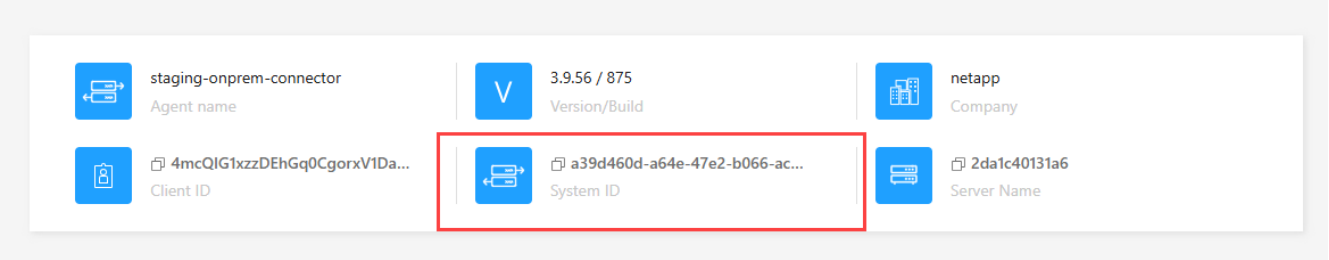
作業を開始するには、コンソール エージェントのシステム ID が必要になる場合があります。 ID は通常、ライセンスとトラブルシューティングの目的で使用されます。

手順

1. *管理 > サポート > エージェント*を選択します。

   システム ID はページの上部にあります。

   例



2. ID にマウスを合わせてクリックするとコピーできます。

AutoSupportメッセージをダウンロードまたは送信する

問題が発生した場合、 NetApp はトラブルシューティングのためにAutoSupportメッセージをNetAppサポートに送信するように依頼することがあります。

NetApp Consoleは、負荷分散のため、 AutoSupportメッセージを送信するのに最大 5 時間かかります。緊急の場合は、ファイルをダウンロードして手動で送信してください。

手順

1. *管理 > サポート > エージェント*を選択します。
2. NetAppサポートに情報を送信する方法に応じて、次のいずれかのオプションを選択します。
   a. AutoSupportメッセージをローカル マシンにダウンロードするオプションを選択します。その後、優先する方法を使用してNetAppサポートに送信できます。
   b. **Send AutoSupport** を選択すると、メッセージがNetAppサポートに直接送信されます。

Google Cloud NAT ゲートウェイ使用時のダウンロード失敗を修正

コンソール エージェントは、 Cloud Volumes ONTAPのソフトウェア アップデートを自動的にダウンロードします。 Google Cloud NAT ゲートウェイを使用している場合、設定によりダウンロードが失敗する可能性があります。ソフトウェア イメージを分割する部分の数を制限することで、この問題を修正できます。この手順は API を使用して完了する必要があります。

手順

1. 次の JSON を本文として、PUT リクエストを /occm/config に送信します。

```
{
  "maxDownloadSessions": 32
}
```

   maxDownloadSessions の値は 1 または 1 より大きい任意の整数にすることができます。値が 1 の場合、ダウンロードされたイメージは分割されません。

32 は例の値であることに注意してください。値は NAT 構成と同時セッションの数によって異なります。

"/occm/config API呼び出しの詳細"

NetAppナレッジベースからヘルプを入手する

"NetAppサポートチームが作成したトラブルシューティング情報を表示します" 。

コンソールエージェントをアンインストールして削除する

問題をトラブルシューティングしたり、ホストから完全に削除したりするには、コンソール エージェントをアンインストールします。実行する必要がある手順は、使用している展開モードによって異なります。環境からコンソール エージェントを削除したら、コンソールからも削除できます。

"NetApp Consoleの導入モードについて学ぶ" 。

標準モードまたは制限モードを使用している場合はエージェントをアンインストールします

標準モードまたは制限モードを使用している場合 (つまり、エージェント ホストに送信接続がある場合)、以下の手順に従ってエージェントをアンインストールする必要があります。

手順

1. エージェントの Linux VM に接続します。
2. Linux ホストから、アンインストール スクリプトを実行します。

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   silent は確認を求めることなくスクリプトを実行します。

コンソールからコンソールエージェントを削除する

コンソール エージェントが非アクティブな場合は、エージェントのリストから削除できます。エージェント仮想マシンを削除した場合、またはエージェント ソフトウェアをアンインストールした場合に、この操作を行う可能性があります。

コンソール エージェントを削除する場合は、次の点に注意してください。

- このアクションでは仮想マシンは削除されません。
- このアクションは元に戻すことはできません。コンソール エージェントを削除すると、再度追加することはできません。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、非アクティブなエージェントのアクション メニューを選択し、*エージェントの削除*を選択します。
3. 確認のためにエージェントの名前を入力し、「削除」を選択します。

コンソールエージェントのデフォルト構成

コンソール エージェントを展開する前に、その構成について詳しく確認してください。

インターネットアクセスを備えたデフォルト構成

次の構成の詳細は、 NetApp Consoleから、クラウド プロバイダーのマーケットプレイスからコンソール エージェントを展開した場合、またはインターネットにアクセスできるオンプレミスの Linux ホストにコンソール エージェントを手動でインストールした場合に適用されます。

AWS の詳細

コンソールまたはクラウド プロバイダーのマーケットプレイスからコンソール エージェントを展開した場合は、次の点に注意してください。

- EC2 インスタンスタイプは t3.2xlarge です。
- イメージのオペレーティング システムは Ubuntu 22.04 LTS です。

  オペレーティング システムには GUI が含まれていません。システムにアクセスするには端末を使用する必要があります。

- インストールには、必要なコンテナ オーケストレーション ツールである Docker Engine が含まれます。
- EC2 Linux インスタンスのユーザー名は ubuntu です (2023 年 5 月より前に作成されたエージェントの場合、ユーザー名は ec2-user です)。
- デフォルトのシステム ディスクは 100 GiB gp2 ディスクです。

Azureの詳細

コンソールまたはクラウド プロバイダーのマーケットプレイスからコンソール エージェントを展開した場合は、次の点に注意してください。

- VM タイプは Standard_D8s_v3 です。
- イメージのオペレーティング システムは Ubuntu 22.04 LTS です。

  オペレーティング システムには GUI が含まれていません。システムにアクセスするには端末を使用する必要があります。

- インストールには、必要なコンテナ オーケストレーション ツールである Docker Engine が含まれます。
- デフォルトのシステム ディスクは 100 GiB のプレミアム SSD ディスクです。

Google Cloudの詳細

コンソールからコンソール エージェントを展開した場合は、次の点に注意してください。

- VM インスタンスは n2-standard-8 です。
- イメージのオペレーティング システムは Ubuntu 22.04 LTS です。

  オペレーティング システムには GUI が含まれていません。システムにアクセスするには端末を使用する必要があります。

- インストールには、必要なコンテナ オーケストレーション ツールである Docker Engine が含まれます。
- デフォルトのシステム ディスクは 100 GiB の SSD 永続ディスクです。

インストールフォルダ

エージェントのインストール フォルダーは次の場所にあります。

/opt/application/netapp/cloudmanager

ログ ファイル

ログ ファイルは次のフォルダーに保存されます。

- /opt/application/netapp/cloudmanager/log または
- /opt/application/netapp/service-manager-2/logs (新しい 3.9.23 インストール以降)

  これらのフォルダー内のログには、コンソール エージェントに関する詳細が記録されます。

- /opt/application/netapp/cloudmanager/docker_occm/data/log

  このフォルダー内のログには、クラウド サービスと、コンソール エージェントで実行されるコンソール サービスに関する詳細が記録されます。

コンソールエージェントサービス

- コンソール エージェント サービスの名前は occm です。
- occm サービスは MySQL サービスに依存します。

  MySQL サービスがダウンしている場合は、occm サービスもダウンします。

ポート

エージェントは Linux ホスト上で次のポートを使用します。

- HTTPアクセスの場合は80
- HTTPSアクセスの場合は443

インターネットアクセスなしのデフォルト設定

インターネットにアクセスできないオンプレミスの Linux ホストにコンソール エージェントを手動でインストールした場合は、次の構成が適用されます。"このインストールオプションの詳細" 。

- エージェントのインストール フォルダーは次の場所にあります。

  /opt/application/netapp/ds

- ログ ファイルは次のフォルダーに保存されます。

  /var/lib/docker/volumes/ds_occmdata/_data/log

このフォルダー内のログには、コンソール エージェントと Docker イメージに関する詳細が記録されます。

- すべてのサービスはDockerコンテナ内で実行されています

  サービスはdockerランタイムサービスの実行に依存しています

- エージェントは Linux ホスト上で次のポートを使用します。
  - HTTPアクセスの場合は80
  - HTTPSアクセスの場合は443

ONTAP Advanced View（ONTAP System Manager）のONTAP権限を適用する

デフォルトでは、コンソール エージェントの認証情報により、ユーザーは詳細ビュー (ONTAP System Manager) にアクセスできます。代わりに、ユーザーにONTAP認証情報の入力を求めることもできます。これにより、ユーザーが Cloud Volumes ONTAP とONTAPオンプレミス クラスターの両方でONTAPクラスターを操作するときに、ユーザーのONTAP権限が確実に適用されます。

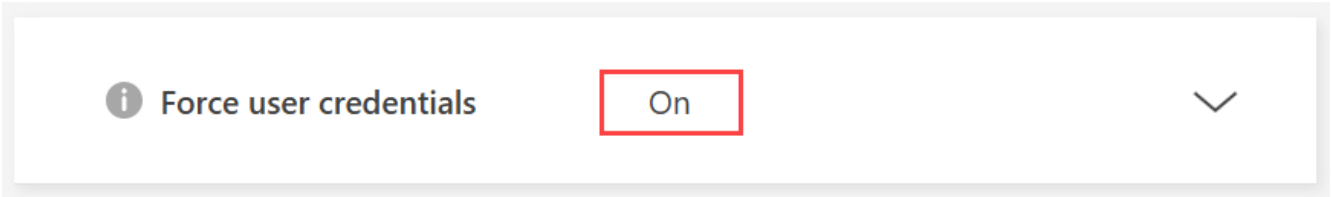
コンソール エージェントの設定を編集するには、組織管理者のロールが必要です。

手順

1. *管理 > エージェント*を選択します。
2. *概要*ページで、コンソール エージェントのアクション メニューを選択し、*エージェントの編集*を選択します。

   編集するには、コンソール エージェントがアクティブである必要があります。

3. *資格情報の強制*オプションを展開します。
4. *資格情報の強制*オプションを有効にするにはチェックボックスをオンにして、*保存*を選択します。
5. *資格情報の強制*オプションが有効になっていることを確認します。



資格情報とサブスクリプション

AWS

NetApp Consoleの **AWS** 認証情報と権限について学習します

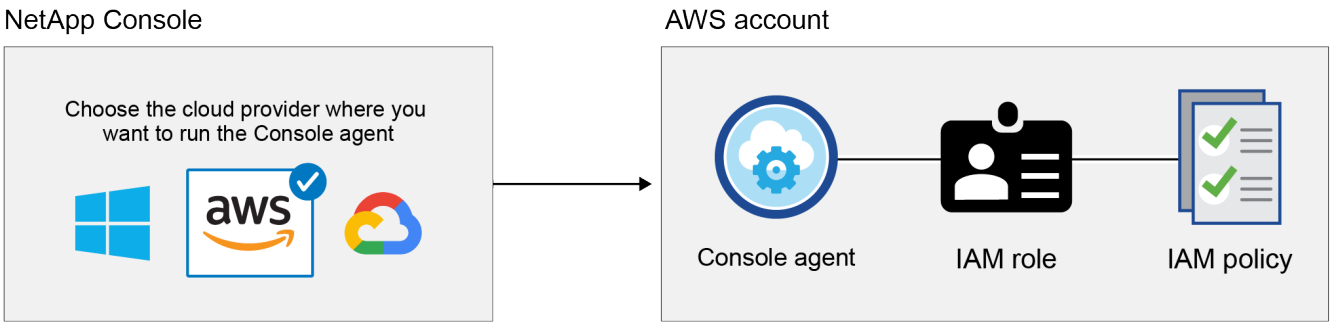
NetApp ConsoleがAWS 認証情報を使用してユーザーに代わってアクションを実行する

方法と、それらの認証情報がマーケットプレイスのサブスクリプションとどのように関連付けられるかについて説明します。これらの詳細を理解しておくと、NetApp Console で 1 つ以上の AWS アカウントの認証情報を管理するときに役立ちます。たとえば、追加の AWS 認証情報をいつ追加する必要があるかについて学習したい場合があります。

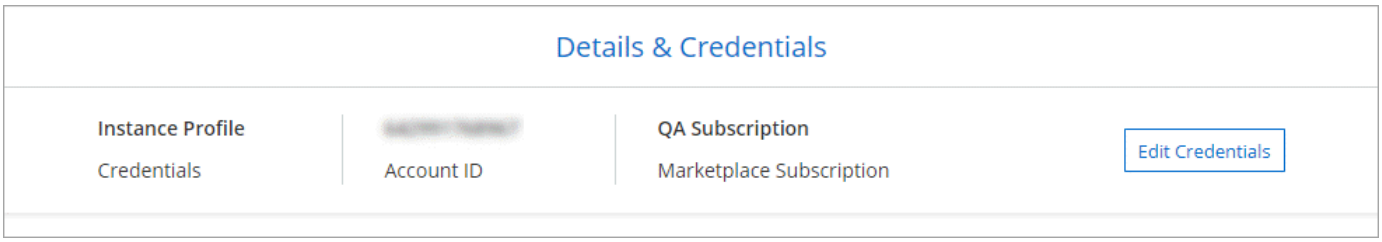
初期AWS認証情報

コンソールからコンソールエージェントをデプロイする場合は、IAM ロールの ARN または IAM ユーザーのアクセスキーを指定する必要があります。認証方法には、AWS にコンソールをデプロイするための権限が必要です。必要な権限は、link:task-install-agent-aws-the Console.html#console-permissions-aws[AWS のエージェント展開ポリシー]に記載されています。

コンソールが AWS でコンソールエージェントインスタンスを起動すると、インスタンスの IAM ロールとインスタンスプロファイルが作成されます。また、コンソールエージェントにその AWS アカウント内のリソースとプロセスを管理するための権限を付与するポリシーも添付します。"コンソールが権限をどのように使用するかを確認します" 。



新しいCloud Volumes ONTAPシステムを追加すると、コンソールはデフォルトで次の AWS 認証情報を選択します。



初期の AWS 認証情報を使用してすべてのCloud Volumes ONTAPシステムを展開するか、追加の認証情報を追加することができます。

追加のAWS認証情報

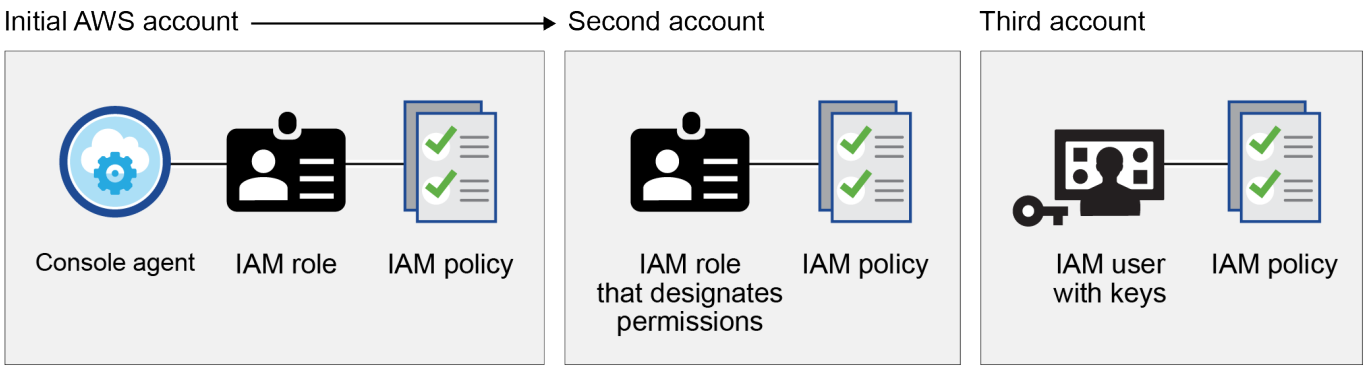
次の場合には、コンソールに追加の AWS 認証情報を追加する必要があるかもしれません。

- 既存のコンソールエージェントを追加のAWSアカウントで使用するには
- 特定のAWSアカウントに新しいエージェントを作成するには
- FSx for ONTAPファイルシステムを作成および管理するには

詳細については、以下のセクションを確認してください。

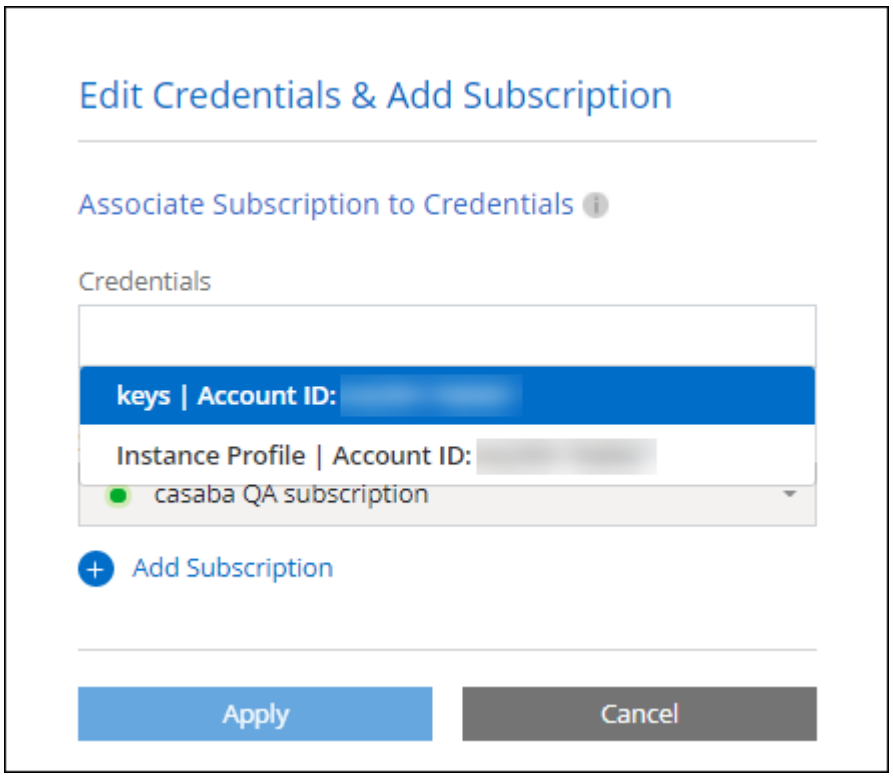
別の **AWS** アカウントでコンソールエージェントを使用するには、**AWS** 認証情報を追加します。

追加の AWS アカウントでコンソールを使用する場合は、IAM ユーザーの AWS キーまたは信頼できるアカウントのロールの ARN を提供できます。次の図は、信頼できるアカウントの IAM ロールを通じて権限を提供するアカウントと、IAM ユーザーの AWS キーを通じて権限を提供するアカウントの 2 つの追加アカウントを示しています。



次に、IAM ロールの Amazon リソースネーム (ARN) または IAM ユーザーの AWS キーを指定して、アカウント認証情報をコンソールに追加します。

たとえば、新しいCloud Volumes ONTAPシステムを作成するときに、資格情報を切り替えることができます。



"既存のエージェントに AWS 認証情報を追加する方法を学びます。"

コンソールエージェントを作成するには**AWS**認証情報を追加します

コンソールに新しい AWS 認証情報を追加すると、コンソールエージェントを作成するために必要な権限が付与されます。

"コンソールエージェントを作成するためにコンソールにAWS認証情報を追加する方法を学びます"

FSx for ONTAPに AWS 認証情報を追加する

FSx for ONTAPシステムを作成および管理するために必要な権限を付与するには、コンソールに AWS 認証情報を追加します。

"Amazon FSx for ONTAPのコンソールに AWS 認証情報を追加する方法を学びます"

資格情報とマーケットプレイスのサブスクリプション

コンソールエージェントに追加する認証情報は、AWS Marketplace サブスクリプションに関連付ける必要があります。これにより、 Cloud Volumes ONTAPの料金を時間単位 (PAYGO) で支払うことができ、その他のNetAppデータ サービスに対しても、年間契約で支払うことができます。"AWSサブスクリプションを関連付ける方法を学ぶ" 。

AWS 認証情報とマーケットプレイスサブスクリプションについては、次の点に注意してください。

- AWS 認証情報のセットに関連付けることができるのは、1 つの AWS Marketplace サブスクリプションのみです。
- 既存のマーケットプレイスサブスクリプションを新しいサブスクリプションに置き換えることができます

FAQ

次の質問は、資格情報とサブスクリプションに関連しています。

AWS 認証情報を安全にローテーションするにはどうすればよいですか?

上のセクションで説明したように、コンソールでは、コンソールエージェントインスタンスに関連付けられたIAM ロール、信頼できるアカウントでの IAM ロールの引き受け、または AWS アクセスキーの提供など、いくつかの方法で AWS 認証情報を提供できます。

最初の 2 つのオプションでは、コンソールは AWS セキュリティ トークン サービスを使用して、常にローテーションする一時的な認証情報を取得します。このプロセスはベストプラクティスであり、自動かつ安全です。

コンソールに AWS アクセスキーを提供する場合は、コンソールで定期的にキーを更新してキーをローテーションする必要があります。これは完全に手動のプロセスです。

Cloud Volumes ONTAPシステムの AWS Marketplace サブスクリプションを変更できますか?

はい、できます。認証情報セットに関連付けられている AWS Marketplace サブスクリプションを変更すると、既存および新規のすべてのCloud Volumes ONTAPシステムに新しいサブスクリプションの料金が課金されます。

"AWSサブスクリプションを関連付ける方法を学ぶ" 。

それぞれ異なるマーケットプレイスサブスクリプションを持つ複数の AWS 認証情報を追加できますか?

同じ AWS アカウントに属するすべての AWS 認証情報は、同じ AWS Marketplace サブスクリプションに関連付けられます。

異なる AWS アカウントに属する複数の AWS 認証情報がある場合、それらの認証情報は、同じ AWS Marketplace サブスクリプションまたは異なるサブスクリプションに関連付けることができます。

既存の**Cloud Volumes ONTAP**システムを別の **AWS** アカウントに移動できますか**?**

いいえ、 Cloud Volumes ONTAPシステムに関連付けられている AWS リソースを別の AWS アカウントに移動することはできません。

マーケットプレイスの展開とオンプレミスの展開では資格情報はどのように機能しますか**?**

上記のセクションでは、コンソールからのコンソール エージェントの推奨展開方法について説明しています。 AWS Marketplace から AWS にエージェントをデプロイし、独自の Linux ホストにコンソールエージェント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。

Marketplace を使用する場合も、同様の方法で権限が提供されます。 IAM ロールを手動で作成して設定し、追加のアカウントに権限を付与するだけです。

オンプレミス展開の場合、コンソールに IAM ロールを設定することはできませんが、AWS アクセスキーを使用して権限を付与することはできます。

権限の設定方法については、次のページを参照してください。

- 標準モード
  - "AWS Marketplace デプロイメントの権限を設定する"
  - "オンプレミス展開の権限を設定する"
- 制限モード
  - "制限モードの権限を設定する"

NetApp Consoleの **AWS** 認証情報とマーケットプレイス サブスクリプションを管理する

AWS 認証情報を追加および管理して、 NetApp Consoleから AWS アカウント内のクラウド リソースを展開および管理できるようにします。複数の AWS Marketplace サブスクリプションを管理する場合は、[認証情報] ページから各サブスクリプションを異なる AWS 認証情報に割り当てることができます。

概要

AWS 認証情報を既存のコンソールエージェントに追加することも、コンソールに直接追加することもできます。

- 既存のエージェントにAWS認証情報を追加する

  クラウド リソースを管理するには、コンソール エージェントに AWS 認証情報を追加します。コンソールエージェントにAWS認証情報を追加する方法を学びます 。

- コンソールエージェントを作成するためにコンソールにAWS認証情報を追加する

  コンソールに新しい AWS 認証情報を追加すると、コンソールエージェントを作成するために必要な権限が付与されます。NetApp ConsoleにAWS認証情報を追加する方法を学びます 。

- FSx for ONTAPのコンソールに AWS 認証情報を追加する

  FSx for ONTAPを作成および管理するには、コンソールに新しい AWS 認証情報を追加します。 "FSx for ONTAPの権限を設定する方法を学びます"

資格情報をローテーションする方法

NetApp Consoleを使用すると、エージェント インスタンスに関連付けられた IAM ロール、信頼できるアカウントでの IAM ロールの引き受け、または AWS アクセス キーの提供など、いくつかの方法で AWS 認証情報を提供できます。"AWS の認証情報と権限について詳しく見る" 。

最初の 2 つのオプションでは、コンソールは AWS セキュリティ トークン サービスを使用して、常にローテーションする一時的な認証情報を取得します。このプロセスは自動かつ安全であるため、ベストプラクティスです。

コンソールで更新して、AWS アクセスキーを手動でローテーションします。

コンソールエージェントに追加の資格情報を追加する

コンソールエージェントに追加の AWS 認証情報を追加して、パブリッククラウド環境内のリソースとプロセスを管理するために必要な権限を付与します。別のアカウントの IAM ロールの ARN を提供するか、AWS アクセスキーを提供することができます。

コンソールを使い始めたばかりの方は、"NetApp ConsoleがAWS認証情報と権限を使用する方法を学ぶ" 。

権限を付与する

コンソールエージェントに AWS 認証情報を追加する前に、権限を付与します。権限により、コンソールエージェントはその AWS アカウント内のリソースとプロセスを管理できるようになります。信頼できるアカウントのロールの ARN または AWS キーを使用して、アクセス許可を付与できます。

> コンソールからコンソールエージェントを展開した場合、コンソールエージェントを展開したアカウントの AWS 認証情報が自動的に追加されます。これにより、リソースを管理するために必要な権限が確保されます。"AWS の認証情報と権限について学ぶ" 。

選択肢

- 別のアカウントの IAM ロールを引き受けて権限を付与する
- AWSキーを提供して権限を付与する

別のアカウントの **IAM** ロールを引き受けて権限を付与する

IAM ロールを使用して、コンソールエージェントインスタンスをデプロイしたソース AWS アカウントと他の AWS アカウントの間に信頼関係を設定できます。次に、信頼できるアカウントの IAM ロールの ARN をコンソールに提供します。

コンソール エージェントがオンプレミスにインストールされている場合、この認証方法は使用できません。AWS キーを使用する必要があります。

手順

1. コンソール エージェントに権限を付与するターゲット アカウントの IAM コンソールに移動します。

2. [アクセス管理] で、**[ロール] > [ロールの作成]** を選択し、手順に従ってロールを作成します。

   必ず次のことを行ってください。

   - *信頼されたエンティティタイプ*で、*AWS アカウント*を選択します。
   - 別の **AWS** アカウント を選択し、コンソールエージェントインスタンスが存在するアカウントの ID を入力します。
   - の内容をコピーして貼り付けて必要なポリシーを作成します。"コンソールエージェントのIAMポリシー" 。

3. 後でコンソールに貼り付けることができるように、IAM ロールのロール ARN をコピーします。

結果

アカウントには必要な権限があります。コンソールエージェントに資格情報を追加できるようになりました 。

AWSキーを提供して権限を付与する

コンソールに IAM ユーザーの AWS キーを提供する場合は、そのユーザーに必要な権限を付与する必要があります。コンソール IAM ポリシーは、コンソールが使用できる AWS アクションとリソースを定義します。

コンソール エージェントがオンプレミスにインストールされている場合は、この認証方法を使用する必要があります。 IAM ロールは使用できません。

手順

1. IAMコンソールから、以下の内容をコピーして貼り付けることでポリシーを作成します。"コンソールエージェントのIAMポリシー" 。

   "AWSドキュメント: IAMポリシーの作成"

2. ポリシーを IAM ロールまたは IAM ユーザーにアタッチします。

   - "AWSドキュメント: IAMロールの作成"
   - "AWSドキュメント: IAMポリシーの追加と削除"

結果

アカウントには必要な権限があります。コンソールエージェントに資格情報を追加できるようになりました 。

資格情報を追加する

AWS アカウントに必要な権限を付与したら、そのアカウントの認証情報を既存のエージェントに追加できます。これにより、同じエージェントを使用してそのアカウントでCloud Volumes ONTAPシステムを起動できるようになります。

```
 New credentials in your cloud provider may take a few minutes to become
available. Then, add the credentials.
```
.手順
. 上部のナビゲーション バーを使用して、資格情報を追加するコンソール
エージェントを選択します。
. 左側のナビゲーション バーで、*管理 > 資格情報* を選択します。
. *組織の資格情報*ページで、*資格情報の追加*を選択し、ウィザードの手順に従います。

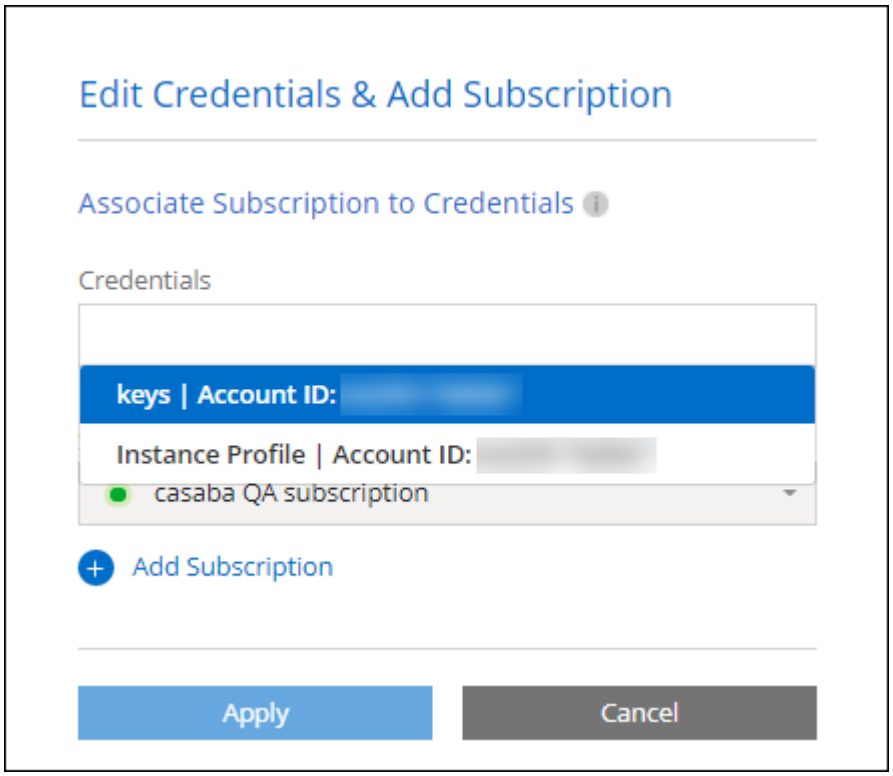
+
.. 資格情報の場所: **Amazon Web Services >** エージェント*を選択します。
**.. ***認証情報の定義: 信頼できる IAM ロールの ARN (Amazon リソース名) を指定するか、AWS アクセスキーとシークレットキーを入力します。
.. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。

+
時間単位の料金 (PAYGO) または年間契約でサービス料金を支払うには、AWS 認証情報を AWS Marketplace サブスクリプションに関連付ける必要があります。

a. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

結果

コンソールにシステムを追加するときに、[詳細と資格情報] ページから別の資格情報セットに切り替えることができるようになりました。



コンソールエージェントの作成に必要な権限を付与する IAM ロールの ARN を指定して、AWS 認証情報を追加します。新しいエージェントを作成するときに、これらの資格情報を選択できます。

IAMロールを設定する

NetApp Consoleのソフトウェア サービス (SaaS) レイヤーがロールを引き受けることができる IAM ロールを設定します。

手順

1. ターゲットアカウントの IAM コンソールに移動します。
2. [アクセス管理] で、**[ロール] > [ロールの作成]** を選択し、手順に従ってロールを作成します。

   必ず次のことを行ってください。

   - *信頼されたエンティティタイプ*で、*AWS アカウント*を選択します。
   - *別のAWSアカウント*を選択し、 NetApp ConsoleSaaSのIDを入力します：952013314444
   - 特にAmazon FSx for NetApp ONTAPの場合は、信頼関係 ポリシーを編集して "AWS": "arn:aws:iam::952013314444:root" を含めます。

     たとえば、ポリシーは次のようになります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

   +
   参照"AWS Identity and Access Management (IAM) ドキュメント" IAM でのクロスアカウント リソース アクセスの詳細については、こちらをご覧ください。

   - コンソール エージェントを作成するために必要な権限を含むポリシーを作成します。
     - "FSx for ONTAPに必要な権限を表示する"
     - "エージェント展開ポリシーを表示する"
3. 次のステップでコンソールに貼り付けることができるように、IAM ロールのロール ARN をコピーします。

結果

IAM ロールに必要な権限が付与されました。コンソールに追加できるようになりました 。

資格情報を追加する

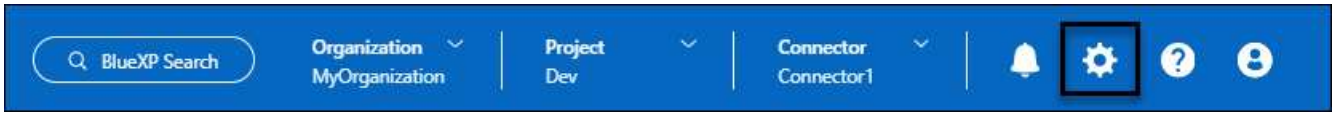
IAM ロールに必要な権限を付与したら、ロール ARN をコンソールに追加します。

開始する前に

IAM ロールを作成したばかりの場合は、使用できるようになるまでに数分かかることがあります。資格情報をコンソールに追加する前に、数分お待ちください。

手順

1. *管理 > 資格情報*を選択します。



2. 組織の資格情報 または アカウントの資格情報 ページで、資格情報の追加 を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: *Amazon Web Services > NetApp Console*を選択します。
   b. 認証情報の定義: IAM ロールの ARN (Amazon リソース名) を指定します。
   c. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

Amazon FSx for ONTAPのコンソールに認証情報を追加する

詳細については、 "Amazon FSx for ONTAPのコンソールドキュメント"

AWSサブスクリプションを設定する

AWS 認証情報を追加したら、その認証情報を使用して AWS Marketplace サブスクリプションを設定できます。サブスクリプションを使用すると、Cloud Volumes ONTAP の料金を時間単位 (PAYGO) または年間契約で支払うことができ、その他のデータ サービスに対しても支払うことができます。

認証情報を追加した後に AWS Marketplace サブスクリプションを構成するシナリオは 2 つあります。

- 資格情報を最初に追加したときに、サブスクリプションを構成しませんでした。
- AWS 認証情報に設定されている AWS Marketplace サブスクリプションを変更します。

  現在のマーケットプレイス サブスクリプションを新しいサブスクリプションに置き換えると、既存のCloud Volumes ONTAPシステムとすべての新しいシステムのマーケットプレイス サブスクリプションが変更されます。

開始する前に

サブスクリプションを構成する前に、コンソール エージェントを作成する必要があります。"コンソールエージェントの作成方法を学ぶ" 。

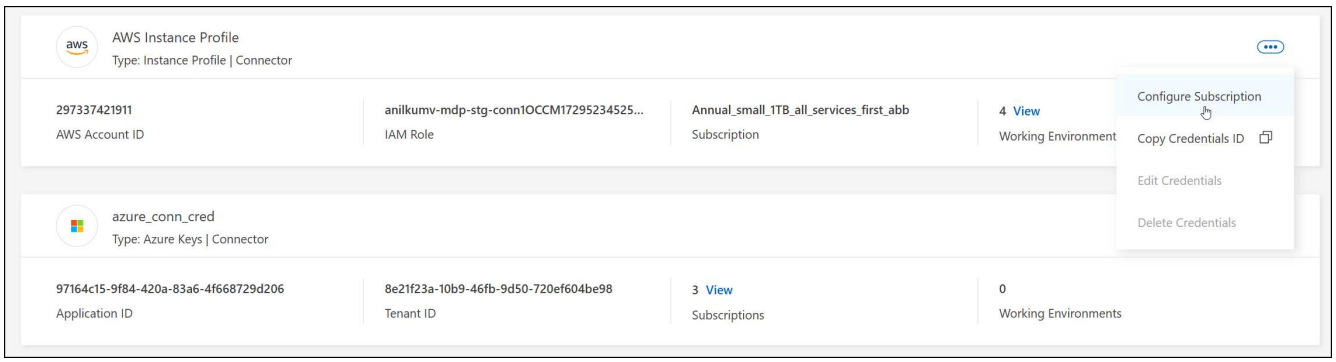
次のビデオは、AWS Marketplace からNetApp Intelligent Servicesをサブスクライブする手順を示しています。

AWS MarketplaceからNetApp Intelligent Servicesをサブスクライブする

手順

1. *管理 > 資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. コンソール エージェントに関連付けられている資格情報のセットのアクション メニューを選択し、[サブスクリプションの構成] を選択します。

   コンソール エージェントに関連付けられている資格情報を選択する必要があります。マーケットプレイス サブスクリプションを、 NetApp Consoleに関連付けられている資格情報に関連付けることはできません。



4. 資格情報を既存のサブスクリプションに関連付けるには、ドロップダウン リストからサブスクリプションを選択し、[構成] を選択します。
5. 認証情報を新しいサブスクリプションに関連付けるには、[サブスクリプションの追加] > [続行] を選択し、AWS Marketplace の手順に従います。

   a. *購入オプションを表示*を選択します。

   b. *購読*を選択します。

   c. *アカウントを設定*を選択します。

      NetApp Consoleにリダイレクトされます。

   d. *サブスクリプションの割り当て*ページから:

      - このサブスクリプションを関連付けるコンソール組織またはアカウントを選択します。
      - 既存のサブスクリプションを置き換える フィールドで、1 つの組織またはアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        コンソールは、組織またはアカウント内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

   他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。

   ◦ *保存*を選択します。

AWS Marketplace からサブスクライブする場合、プロセスの最後のステップは、サブスクリプションを組織に関連付けることです。この手順を完了しなかった場合、組織またはアカウントでサブスクリプションを使用できません。

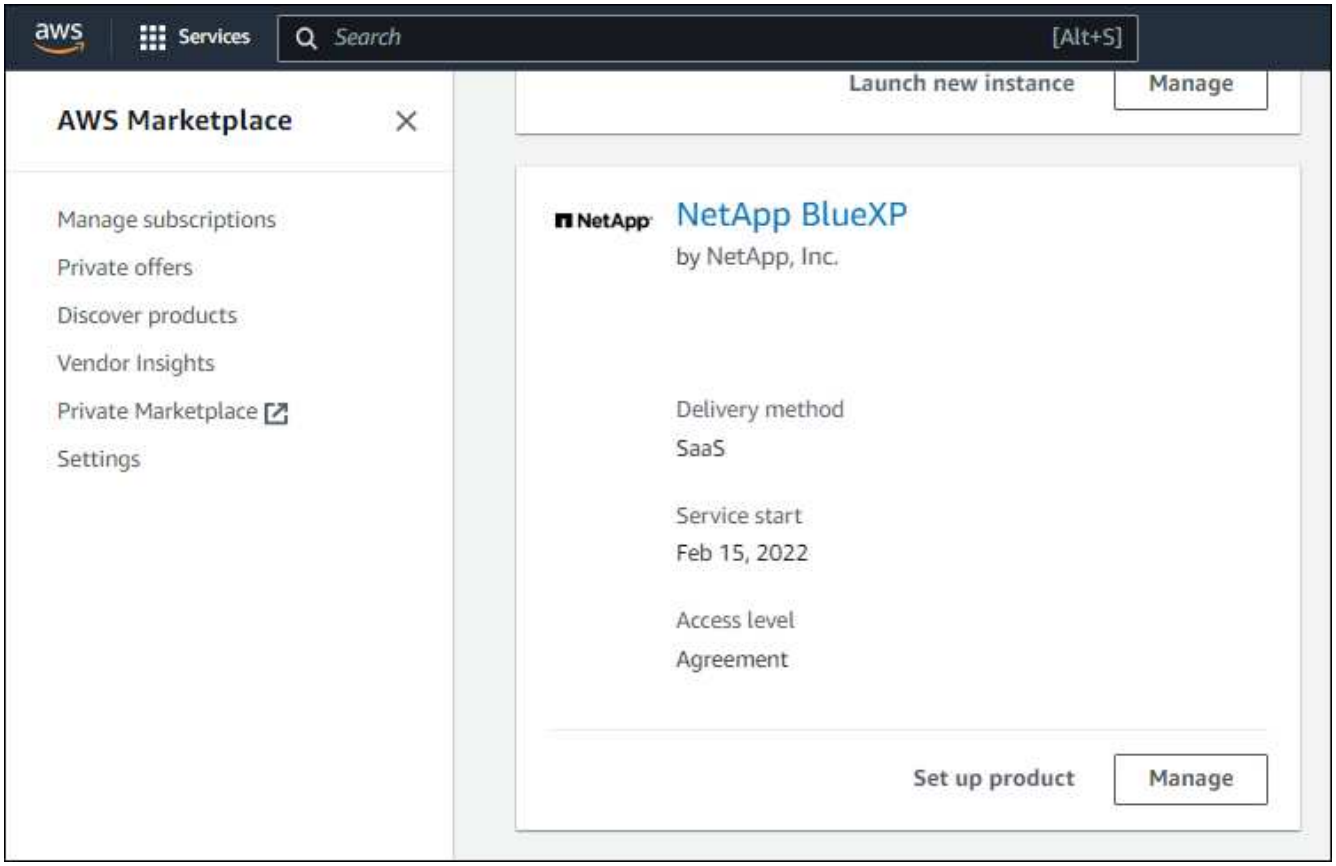
- "コンソールの展開モードについて学ぶ"
- "コンソールのIDとアクセス管理について学ぶ"

AWS Marketplace からNetAppインテリジェント データ サービスにサブスクライブしたが、サブスクリプションをアカウントに関連付ける手順を忘れた場合は、以下の手順に従ってください。

手順

1. サブスクリプションをコンソールの組織またはアカウントに関連付けていないことを確認します。
   a. ナビゲーション メニューから、*管理 >Licenses and subscriptions*を選択します。
   b. *サブスクリプション*を選択します。
   c. サブスクリプションが表示されていないことを確認します。

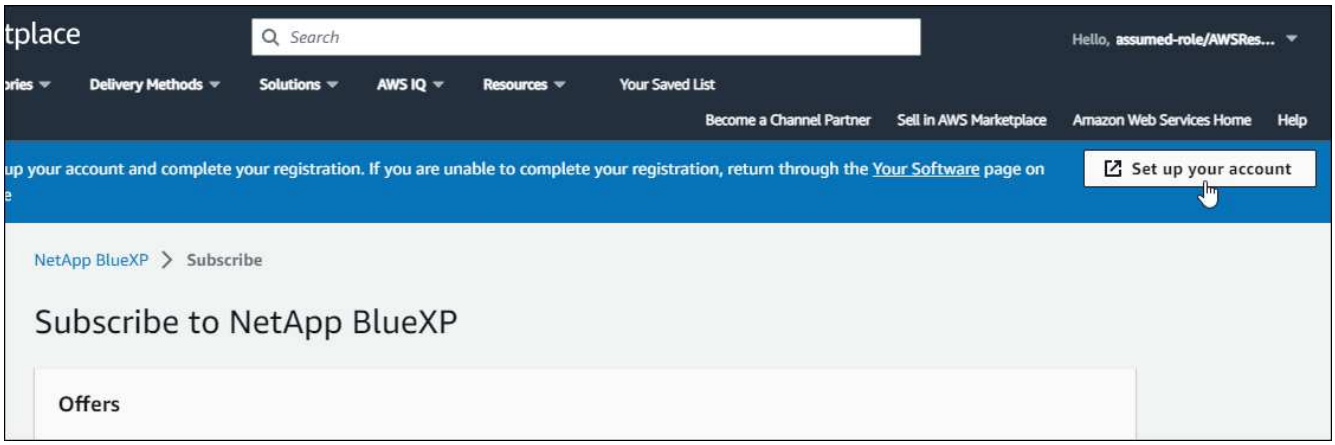
      現在表示している組織またはアカウントに関連付けられているサブスクリプションのみが表示されます。サブスクリプションが表示されない場合は、次の手順に進みます。
2. AWS コンソールにログインし、*AWS Marketplace サブスクリプション*に移動します。
3. サブスクリプションを見つけます。



4. *製品のセットアップ*を選択します。

サブスクリプション オファー ページは、新しいブラウザ タブまたはウィンドウに読み込まれます。

5. *アカウントを設定*を選択します。



netapp.com の サブスクリプションの割り当て ページが新しいブラウザ タブまたはウィンドウに読み込まれます。

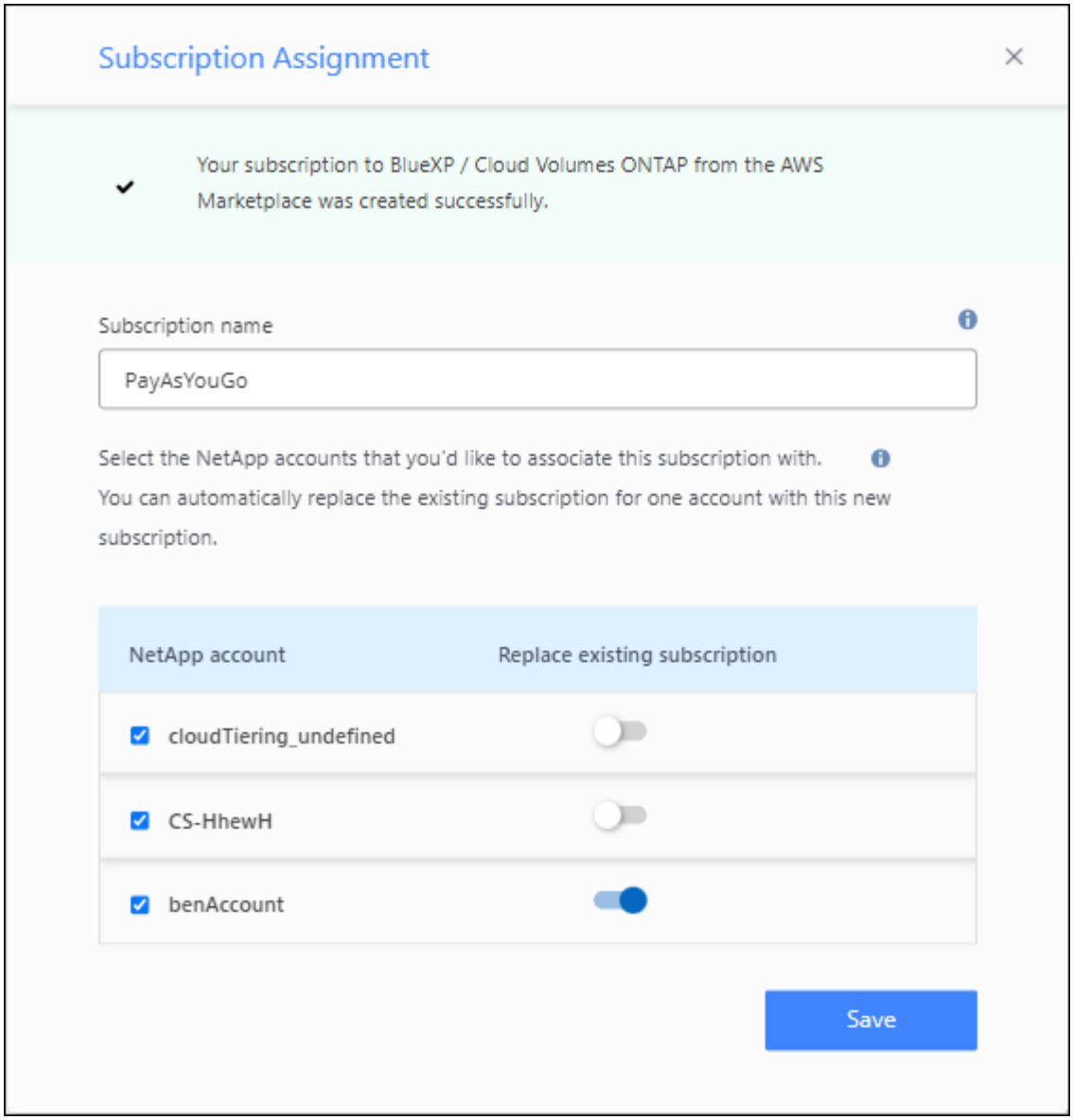
最初にコンソールにログインするように求められる場合があります。

6. *サブスクリプションの割り当て*ページから:

   - このサブスクリプションを関連付けるコンソール組織またはアカウントを選択します。
   - 既存のサブスクリプションを置き換える フィールドで、1 つの組織またはアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

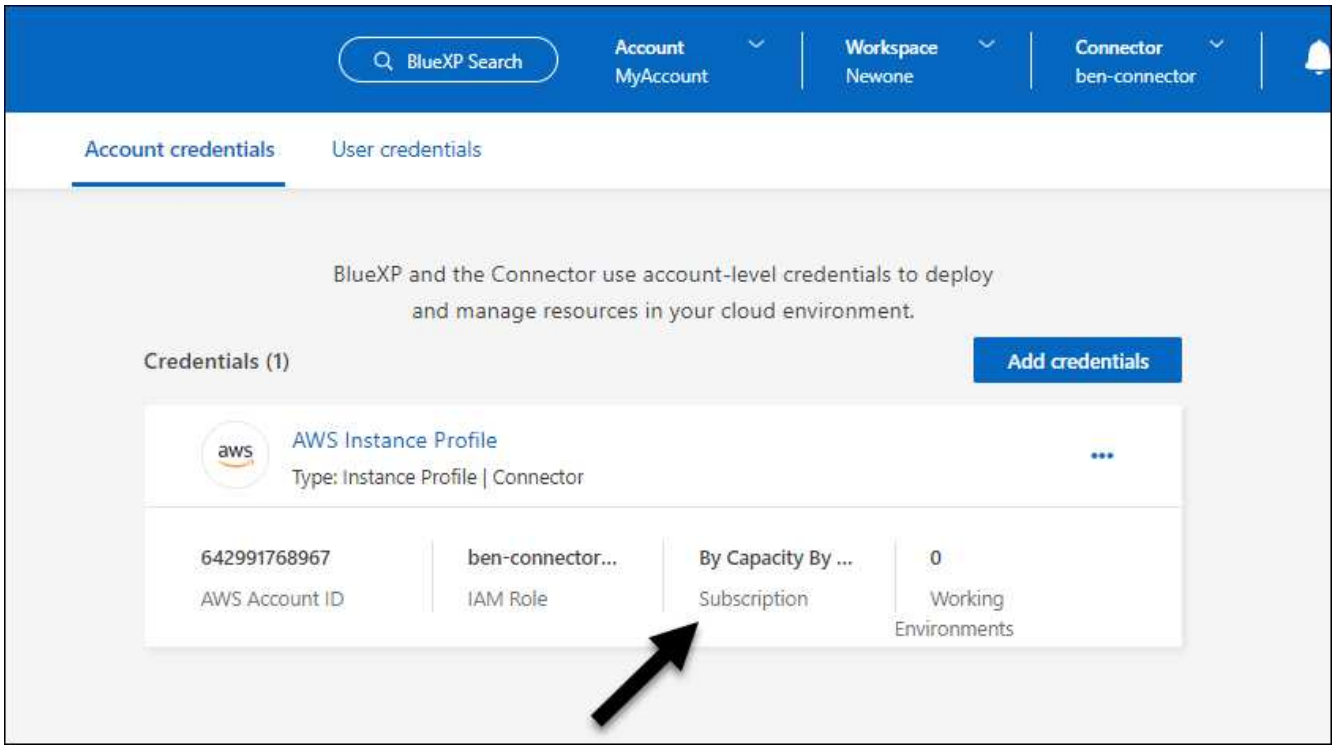
     コンソールは、組織またはアカウント内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

     他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。



7. サブスクリプションが組織またはアカウントに関連付けられていることを確認します。
   a. ナビゲーション メニューから、*管理 > ライセンスとサブスクリプション*を選択します。
   b. *サブスクリプション*を選択します。
   c. サブスクリプションが表示されていることを確認します。
8. サブスクリプションが AWS 認証情報に関連付けられていることを確認します。
   a. コンソールの右上にある設定アイコンを選択し、*資格情報*を選択します。
   b. *組織の認証情報*ページで、サブスクリプションが AWS 認証情報に関連付けられていることを確認します。

      ここに例があります。



資格情報を編集する

アカウントの種類 (AWS キーまたはロールの引き受け) を変更したり、名前を編集したり、認証情報自体 (キーまたはロール ARN) を更新したりして、AWS 認証情報を編集します。

コンソールエージェントインスタンスまたはAmazon FSx for ONTAPインスタンスに関連付けられているインスタンスプロファイルの認証情報を編集することはできません。 FSx for ONTAPインスタンスの資格情報の名前のみを変更できます。

手順

1. *管理 > 資格情報*を選択します。
2. 組織の資格情報 または アカウントの資格情報 ページで、資格情報セットのアクション メニューを選択し、資格情報の編集 を選択します。
3. 必要な変更を加えて、[適用] を選択します。

資格情報を削除する

資格情報セットが不要になった場合は、削除できます。システムに関連付けられていない資格情報のみを削除できます。

コンソール エージェント インスタンスに関連付けられているインスタンス プロファイルの資格情報を削除することはできません。

手順

1. *管理 > 資格情報*を選択します。
2. 組織の資格情報 または アカウントの資格情報 ページで、資格情報セットのアクション メニューを選択し、資格情報の削除 を選択します。

3. *削除*を選択して確認します。

Azure

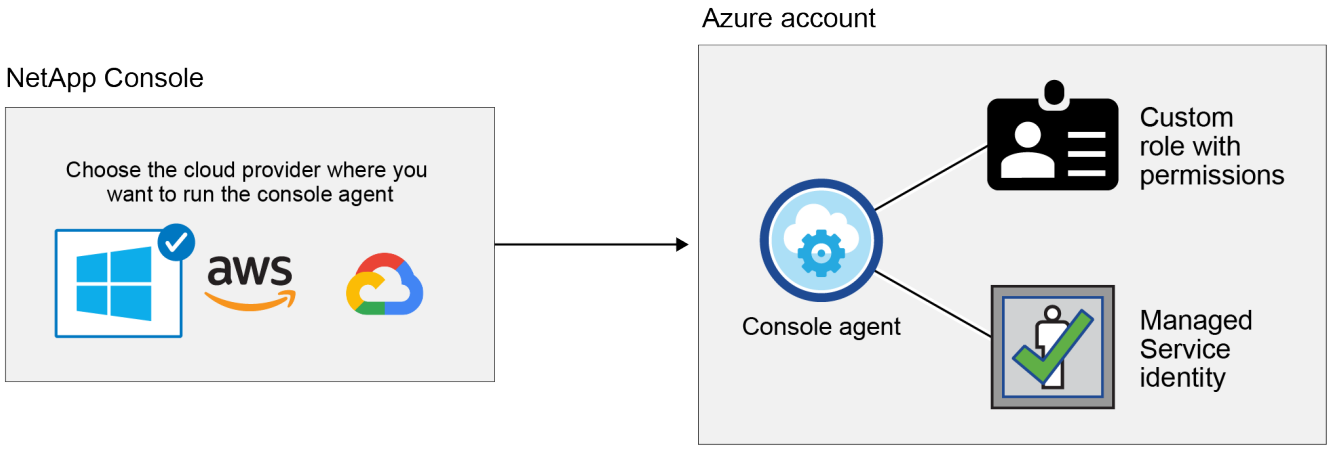
NetApp Consoleの Azure 資格情報と権限について学習します

NetApp ConsoleがAzure 資格情報を使用してユーザーに代わってアクションを実行する方法と、それらの資格情報がマーケットプレイスのサブスクリプションと関連付けられる方法について説明します。これらの詳細を理解しておくと、1 つ以上の Azure サブスクリプションの資格情報を管理するときに役立ちます。たとえば、コンソールに追加の Azure 資格情報を追加するタイミングを知りたい場合があります。

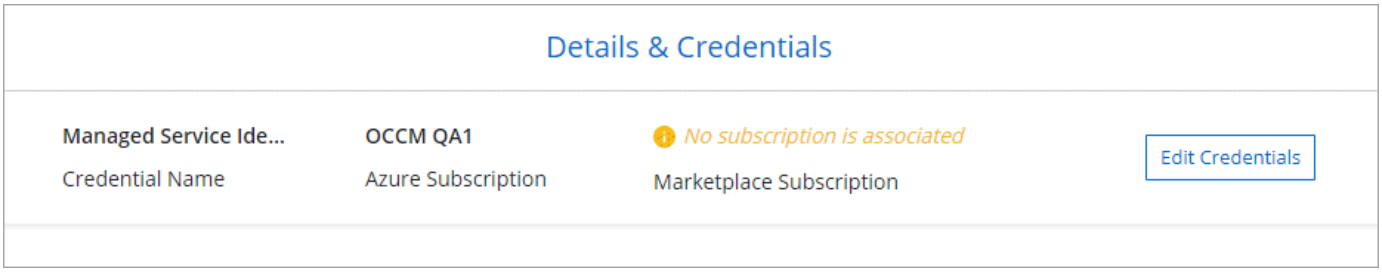
初期の Azure 資格情報

コンソールからコンソール エージェントを展開する場合は、コンソール エージェント仮想マシンを展開する権限を持つ Azure アカウントまたはサービス プリンシパルを使用する必要があります。必要な権限は、"Azure のエージェント展開ポリシー" 。

コンソールがAzureにコンソールエージェント仮想マシンを展開すると、 "システム割り当てマネージドID"仮想マシン上でカスタム ロールを作成し、それを仮想マシンに割り当てます。このロールは、その Azure サブスクリプション内のリソースとプロセスを管理するために必要な権限をコンソールに提供します。"コンソールが権限をどのように使用するかを確認します" 。



Cloud Volumes ONTAP用に新しいシステムを作成する場合、コンソールはデフォルトで次の Azure 資格情報を選択します。



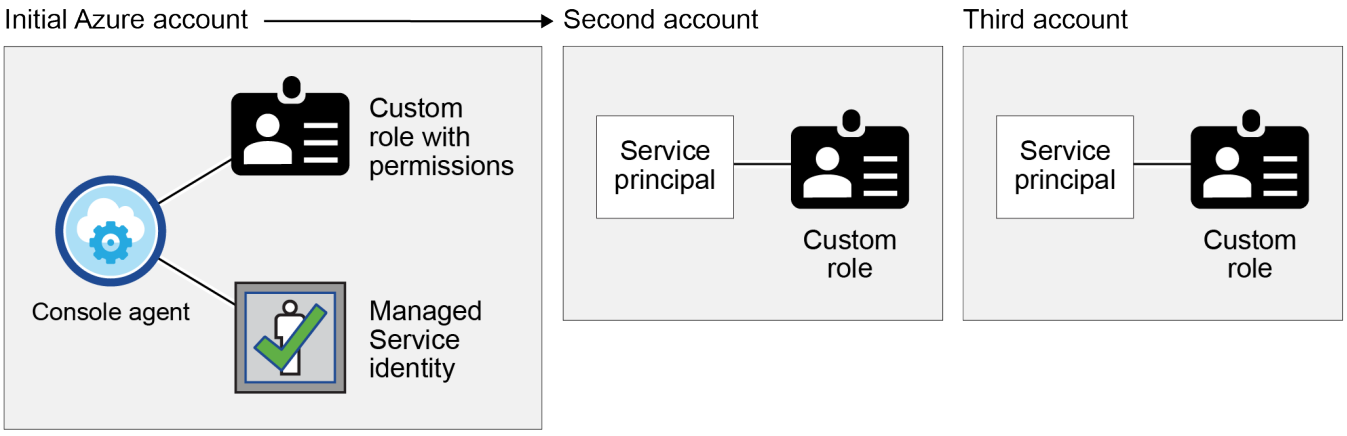
初期の Azure 資格情報を使用してすべてのCloud Volumes ONTAPシステムを展開することも、追加の資格情報を追加することもできます。

マネージド ID 用の追加の Azure サブスクリプション

コンソール エージェント VM に割り当てられたシステム割り当てマネージド ID は、コンソール エージェントを起動したサブスクリプションに関連付けられています。別のAzureサブスクリプションを選択する場合は、"マネージドIDをそれらのサブスクリプションに関連付ける" 。

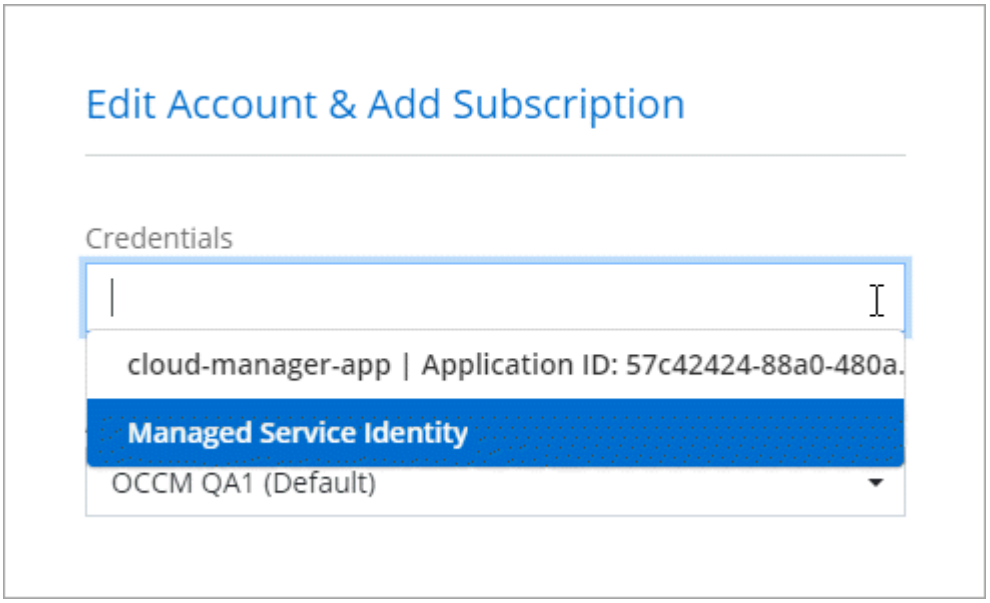
追加のAzure資格情報

コンソールで異なるAzure資格情報を使用する場合は、必要な権限を付与する必要があります。"Microsoft Entra ID でサービス プリンシパルを作成して設定する" Azure アカウントごとに。次の図は、それぞれサービス プリンシパルと、アクセス許可を提供するカスタム ロールが設定された 2 つの追加アカウントを示しています。



そうすると"コンソールにアカウント資格情報を追加する"AD サービス プリンシパルに関する詳細を提供します。

たとえば、新しいCloud Volumes ONTAPシステムを作成するときに、資格情報を切り替えることができます。



資格情報とマーケットプレイスのサブスクリプション

コンソール エージェントに追加する資格情報は、Azure Marketplace サブスクリプションに関連付ける必要が

あります。これにより、 Cloud Volumes ONTAPの料金を時間単位 (PAYGO) またはNetAppデータ サービス、あるいは年間契約で支払うことができます。

"Azureサブスクリプションを関連付ける方法を学ぶ" 。

Azure 資格情報とマーケットプレース サブスクリプションについては、次の点に注意してください。

- Azure 資格情報のセットに関連付けることができるのは、1 つの Azure Marketplace サブスクリプションのみです。
- 既存のマーケットプレイスサブスクリプションを新しいサブスクリプションに置き換えることができます

FAQ

次の質問は、資格情報とサブスクリプションに関連しています。

Cloud Volumes ONTAPシステムの **Azure Marketplace** サブスクリプションを変更できますか**?**

はい、できます。 Azure 資格情報のセットに関連付けられている Azure Marketplace サブスクリプションを変更すると、既存および新しいすべてのCloud Volumes ONTAPシステムに新しいサブスクリプションに対して課金されます。

"Azureサブスクリプションを関連付ける方法を学ぶ" 。

それぞれ異なるマーケットプレイス サブスクリプションを持つ複数の **Azure** 資格情報を追加できますか**?**

同じ Azure サブスクリプションに属するすべての Azure 資格情報は、同じ Azure Marketplace サブスクリプションに関連付けられます。

異なる Azure サブスクリプションに属する複数の Azure 資格情報がある場合、それらの資格情報は、同じ Azure Marketplace サブスクリプションまたは異なるマーケットプレイス サブスクリプションに関連付けることができます。

既存の**Cloud Volumes ONTAP**システムを別の **Azure** サブスクリプションに移動できますか**?**

いいえ、 Cloud Volumes ONTAPシステムに関連付けられている Azure リソースを別の Azure サブスクリプションに移動することはできません。

マーケットプレイスの展開とオンプレミスの展開では資格情報はどのように機能しますか**?**

上記のセクションでは、コンソールからのコンソール エージェントの推奨展開方法について説明しています。 Azure Marketplace から Azure にコンソール エージェントをデプロイし、独自の Linux ホストにコンソール エージェント ソフトウェアをインストールすることもできます。

Marketplace を使用する場合は、コンソール エージェント VM とシステム割り当てマネージド ID にカスタム ロールを割り当てることでアクセス許可を付与することも、Microsoft Entra サービス プリンシパルを使用することもできます。

オンプレミス展開の場合、コンソール エージェントのマネージド ID を設定することはできませんが、サービス プリンシパルを使用してアクセス許可を付与することはできます。

権限の設定方法については、次のページを参照してください。

- 標準モード
  - "Azure Marketplace のデプロイの権限を設定する"
  - "オンプレミス展開の権限を設定する"
- 制限モード
  - "制限モードの権限を設定する"

NetApp Consoleの **Azure** 資格情報とマーケットプレイス サブスクリプションを管理する

Azure 資格情報を追加および管理して、 NetApp ConsoleがAzure サブスクリプション内のクラウド リソースを展開および管理するために必要な権限を持つようにします。複数の Azure Marketplace サブスクリプションを管理する場合は、[資格情報] ページから各サブスクリプションを異なる Azure 資格情報に割り当てることができます。

概要

コンソールで追加の Azure サブスクリプションと資格情報を追加するには、2 つの方法があります。

1. 追加の Azure サブスクリプションを Azure マネージド ID に関連付けます。
2. 異なる Azure 資格情報を使用してCloud Volumes ONTAPをデプロイするには、サービス プリンシパルを使用して Azure 権限を付与し、その資格情報をコンソールに追加します。

追加の **Azure** サブスクリプションをマネージド **ID** に関連付ける

コンソールを使用すると、Cloud Volumes ONTAPをデプロイする Azure 資格情報と Azure サブスクリプションを選択できます。マネージドIDプロファイルに別のAzureサブスクリプションを選択することはできません。 "マネージドID"それらのサブスクリプションで。

タスク概要

マネージドIDとは"最初のAzureアカウント"コンソールからコンソール エージェントを展開する場合。コンソール エージェントを展開すると、コンソールはコンソール エージェント仮想マシンにコンソール オペレータ ロールを割り当てます。

手順

1. Azure ポータルにログインします。
2. サブスクリプション サービスを開き、 Cloud Volumes ONTAPをデプロイするサブスクリプションを選択します。
3. アクセス制御 **(IAM)** を選択します。
   a. 追加 > ロールの割り当ての追加 を選択し、権限を追加します。
      - コンソールオペレーター ロールを選択します。

        コンソール オペレータは、コンソール エージェント ポリシーで提供されるデフォルト名です。ロールに別の名前を選択した場合は、代わりにその名前を選択します。

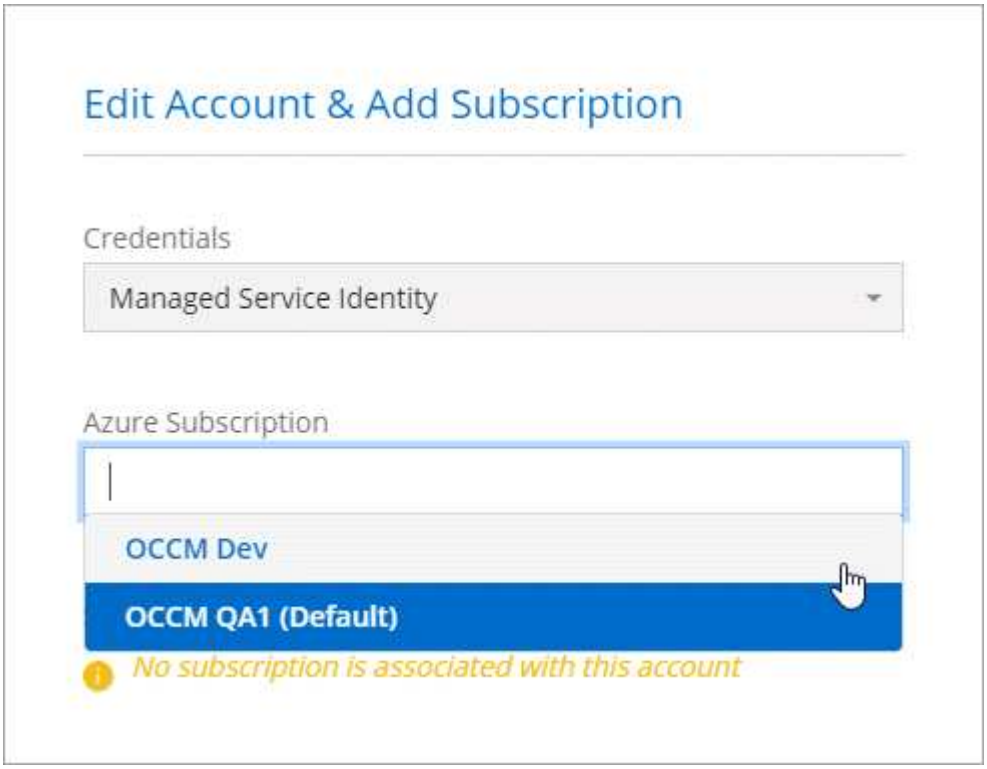
      - *仮想マシン*へのアクセスを割り当てます。

- コンソール エージェント仮想マシンが作成されたサブスクリプションを選択します。
- コンソール エージェント仮想マシンを選択します。
- *保存*を選択します。

4. 追加のサブスクリプションについては、これらの手順を繰り返します。

結果

新しいシステムを作成するときに、マネージド ID プロファイルに対して複数の Azure サブスクリプションから選択できるようになりました。



NetApp Consoleに **Azure** 資格情報を追加する

コンソールからコンソール エージェントを展開すると、コンソールは必要なアクセス許可を持つ仮想マシン上でシステム割り当てのマネージド ID を有効にします。 Cloud Volumes ONTAPの新しいシステムを作成するときに、コンソールはデフォルトでこれらの Azure 資格情報を選択します。

既存のシステムにコンソール エージェント ソフトウェアを手動でインストールした場合、資格情報の初期セットは追加されません。"Azure の資格情報と権限について学習する" 。

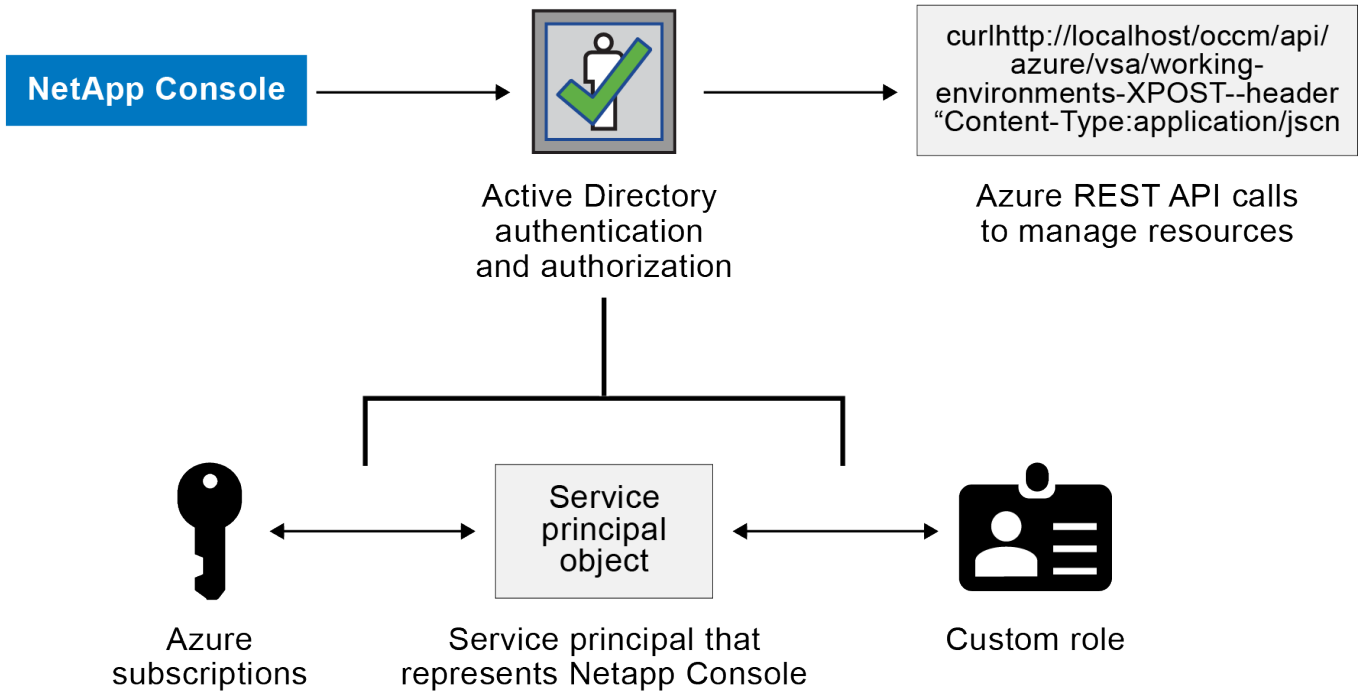
異なる Azure 資格情報を使用してCloud Volumes ONTAPをデプロイする場合は、Azure アカウントごとに Microsoft Entra ID でサービス プリンシパルを作成して設定し、必要な権限を付与する必要があります。その後、新しい資格情報をコンソールに追加できます。

サービス プリンシパルを使用して **Azure** 権限を付与する

コンソールには、Azure でアクションを実行するための権限が必要です。 Microsoft Entra ID でサービス プリンシパルを作成して設定し、コンソールに必要な Azure 資格情報を取得することで、Azure アカウントに必要な権限を付与できます。

タスク概要

次の図は、コンソールが Azure で操作を実行するための権限を取得する方法を示しています。 1 つ以上の Azure サブスクリプションに関連付けられたサービス プリンシパル オブジェクトは、Microsoft Entra ID のコンソールを表し、必要なアクセス許可を許可するカスタム ロールに割り当てられます。



手順

1. Microsoft Entra アプリケーションを作成する 。
2. [アプリケーションをロールに割り当てる] 。
3. Windows Azure サービス管理 API 権限を追加する 。
4. アプリケーションIDとディレクトリIDを取得する 。
5. [クライアントシークレットを作成する] 。

Microsoft Entra アプリケーションを作成する

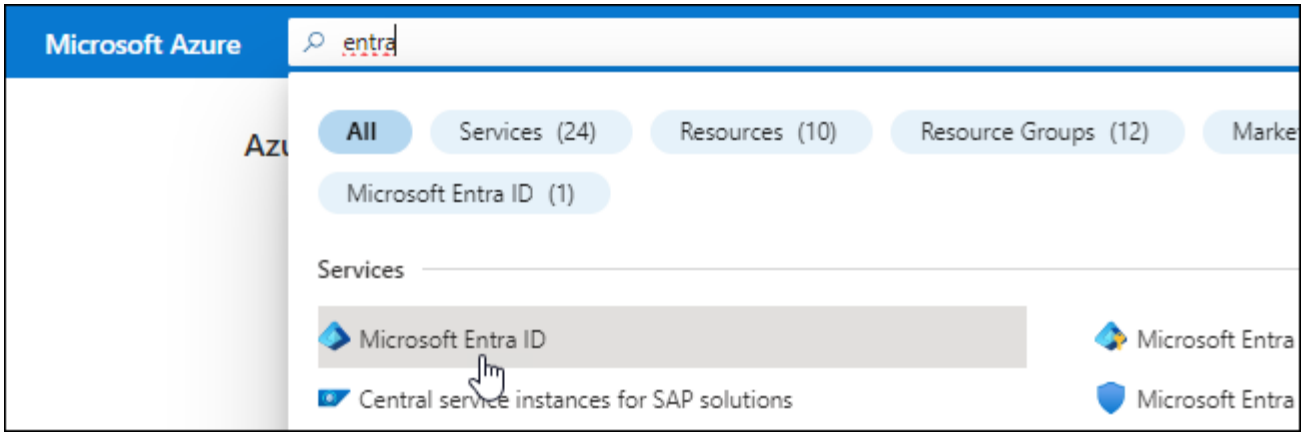
コンソールがロールベースのアクセス制御に使用できる Microsoft Entra アプリケーションとサービス プリンシパルを作成します。

手順

1. Azure で Active Directory アプリケーションを作成し、そのアプリケーションをロールに割り当てるためのアクセス許可があることを確認します。

   詳細については、 "Microsoft Azure ドキュメント: 必要な権限"

2. Azure ポータルから、**Microsoft Entra ID** サービスを開きます。



3. メニューで*アプリ登録*を選択します。
4. *新規登録*を選択します。
5. アプリケーションの詳細を指定します。
   - 名前: アプリケーションの名前を入力します。
   - アカウント タイプ: アカウント タイプを選択します (いずれのタイプもNetApp Consoleで使用できます)。
   - リダイレクト **URI**: このフィールドは空白のままにすることができます。
6. *登録*を選択します。

   AD アプリケーションとサービス プリンシパルを作成しました。

アプリケーションをロールに割り当てる

サービス プリンシパルを 1 つ以上の Azure サブスクリプションにバインドし、カスタムの「コンソール オペレーター」ロールを割り当てて、コンソールに Azure での権限を与える必要があります。

手順

1. カスタム ロールを作成します。

   Azure ポータル、Azure PowerShell、Azure CLI、または REST API を使用して、Azure カスタム ロールを作成できます。次の手順は、Azure CLI を使用してロールを作成する方法を示しています。別の方法をご希望の場合は、 "Azureドキュメント"

   a. の内容をコピーします"コンソールエージェントのカスタムロール権限"JSON ファイルに保存します。
   b. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、JSON ファイルを変更します。

      ユーザーがCloud Volumes ONTAPシステムを作成する各 Azure サブスクリプションの ID を追加する必要があります。

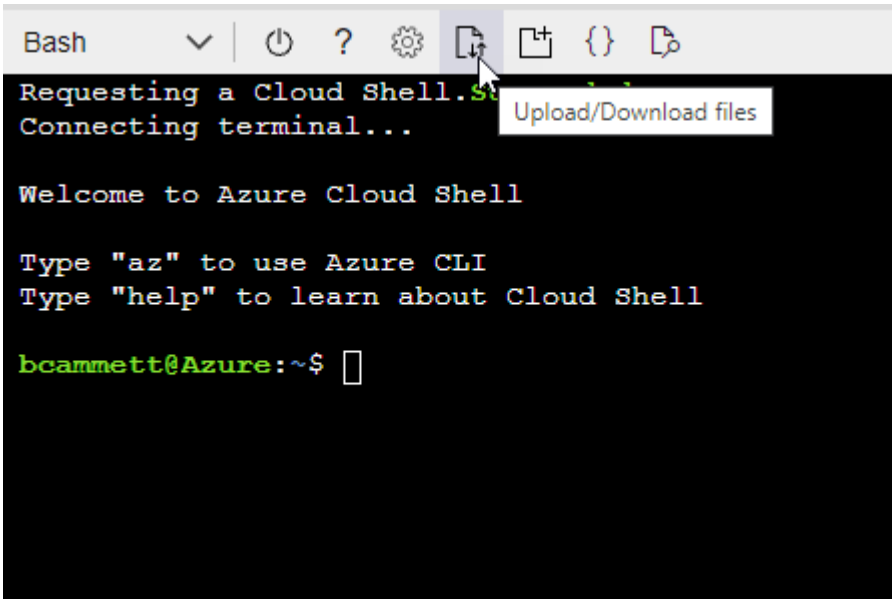
      例

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

c. JSON ファイルを使用して、Azure でカスタム ロールを作成します。

次の手順では、Azure Cloud Shell で Bash を使用してロールを作成する方法について説明します。

- 始める "Azure クラウド シェル"Bash 環境を選択します。
- JSON ファイルをアップロードします。



- Azure CLI を使用してカスタム ロールを作成します。

```
az role definition create --role-definition Connector_Policy.json
```

これで、コンソール エージェント仮想マシンに割り当てることができる、コンソール オペレーターと呼ばれるカスタム ロールが作成されます。

2. アプリケーションをロールに割り当てます。

a. Azure ポータルから、サブスクリプション サービスを開きます。

b. サブスクリプションを選択します。

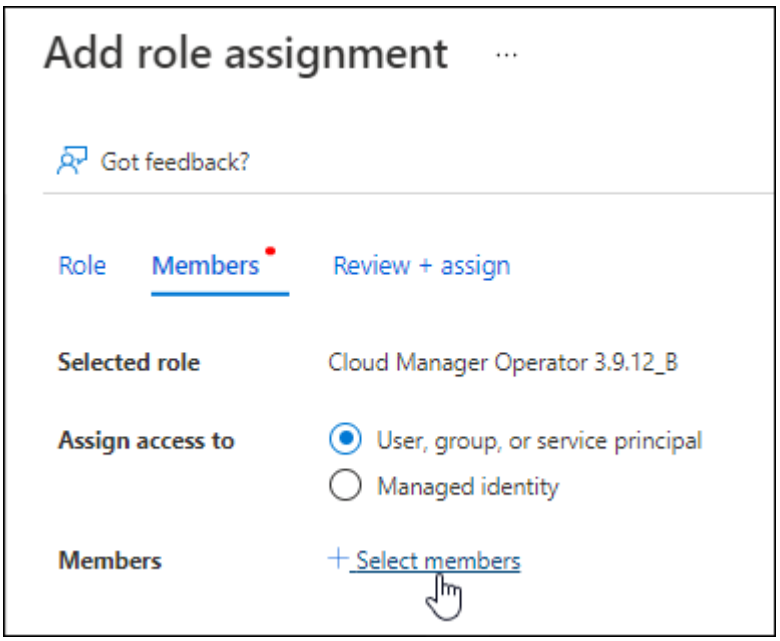
c. アクセス制御 **(IAM) >** 追加 **>** ロール割り当ての追加 を選択します。

d. *役割*タブで、*コンソールオペレーター*役割を選択し、*次へ*を選択します。

e. *メンバー*タブで、次の手順を実行します。

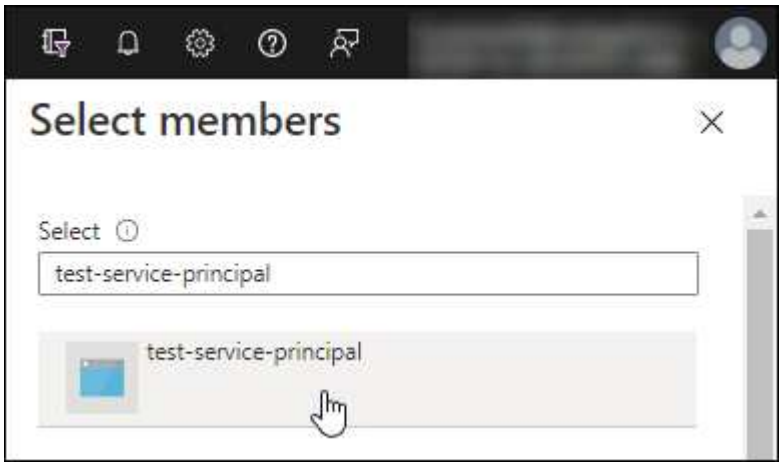
- *ユーザー、グループ、またはサービス プリンシパル*を選択したままにします。

- *メンバーを選択*を選択します。



- アプリケーションの名前を検索します。

  次に例を示します。



- アプリケーションを選択し、[選択] を選択します。
- *次へ*を選択します。

f. *レビュー + 割り当て*を選択します。

これで、サービス プリンシパルに、コンソール エージェントをデプロイするために必要な Azure アクセス許可が付与されました。

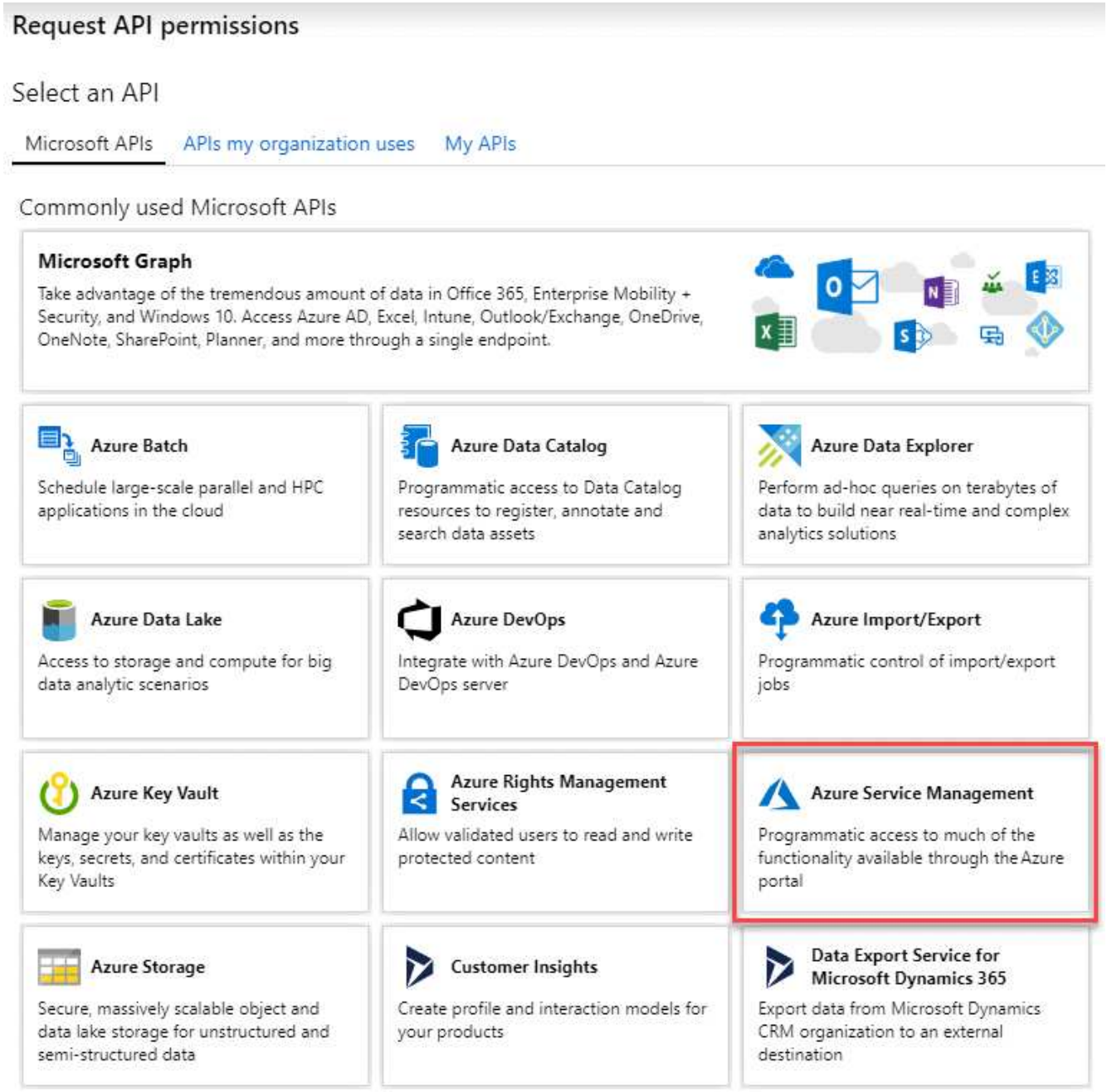
複数の Azure サブスクリプションからCloud Volumes ONTAPをデプロイする場合は、サービス プリンシパルを各サブスクリプションにバインドする必要があります。 NetApp Consoleでは、 Cloud Volumes ONTAP をデプロイするときに使用するサブスクリプションを選択できます。

Windows Azure サービス管理 API 権限を追加する

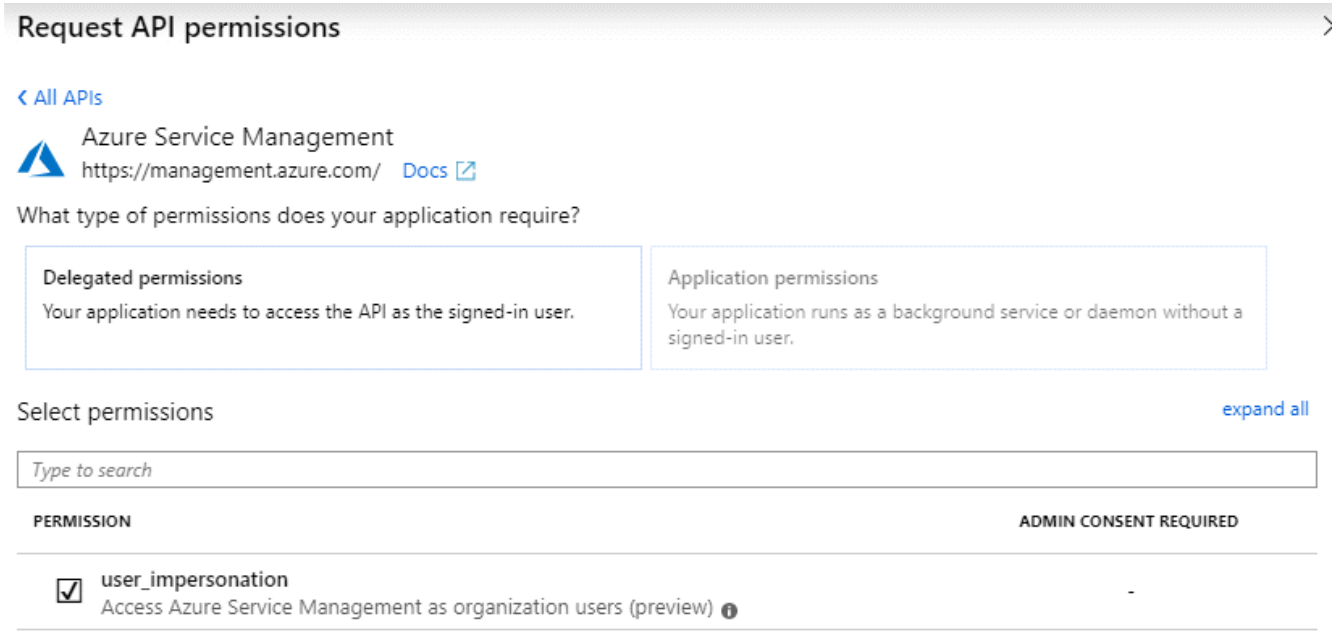
サービス プリンシパルに「Windows Azure サービス管理 API」権限を割り当てる必要があります。

手順

1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. **API** 権限 **>** 権限の追加 を選択します。
3. **Microsoft API** の下で、**Azure Service Management** を選択します。



4. 組織ユーザーとして **Azure** サービス管理にアクセスする を選択し、権限の追加 を選択します。

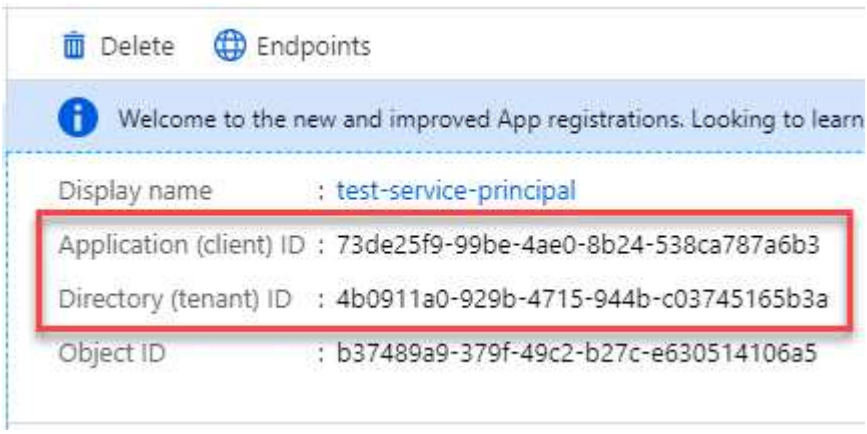


アプリケーション**ID**とディレクトリ**ID**を取得する

Azure アカウントをコンソールに追加するときは、アプリケーションのアプリケーション (クライアント) ID とディレクトリ (テナント) ID を指定する必要があります。コンソールは ID を使用してプログラムでサインインします。

手順

1. **Microsoft Entra ID** サービスで、アプリの登録 を選択し、アプリケーションを選択します。
2. アプリケーション **(**クライアント**) ID** と ディレクトリ **(**テナント**) ID** をコピーします。



Azure アカウントをコンソールに追加するときは、アプリケーションのアプリケーション (クライアント) ID とディレクトリ (テナント) ID を指定する必要があります。コンソールは ID を使用してプログラムでサインインします。

クライアントシークレットを作成する

クライアント シークレットを作成し、その値をコンソールに提供して、Microsoft Entra ID による認証を行います。

手順

1. **Microsoft Entra ID** サービスを開きます。
2. *アプリ登録*を選択し、アプリケーションを選択します。
3. *証明書とシークレット > 新しいクライアント シークレット*を選択します。
4. シークレットの説明と期間を指定します。
5. *追加*を選択します。
6. クライアント シークレットの値をコピーします。

結果

これでサービス プリンシパルが設定され、アプリケーション (クライアント) ID、ディレクトリ (テナント) ID、およびクライアント シークレットの値がコピーされているはずです。 Azure アカウントを追加するときに、コンソールにこの情報を入力する必要があります。

コンソールに資格情報を追加する

Azure アカウントに必要な権限を付与したら、そのアカウントの資格情報をコンソールに追加できます。この手順を完了すると、さまざまな Azure 資格情報を使用してCloud Volumes ONTAP を起動できるようになります。

開始する前に

クラウド プロバイダーでこれらの資格情報を作成したばかりの場合は、使用できるようになるまでに数分かかることがあります。資格情報をコンソールに追加する前に、数分お待ちください。

開始する前に

コンソール設定を変更する前に、コンソール エージェントを作成する必要があります。"コンソールエージェントの作成方法を学ぶ" 。

手順

1. *管理 > 資格情報*を選択します。
2. *資格情報の追加*を選択し、ウィザードの手順に従います。
   a. 資格情報の場所: **Microsoft Azure >** エージェント を選択します。
   b. 資格情報の定義: 必要な権限を付与する Microsoft Entra サービス プリンシパルに関する情報を入力します。
      - アプリケーション（クライアント）ID
      - ディレクトリ（テナント）ID

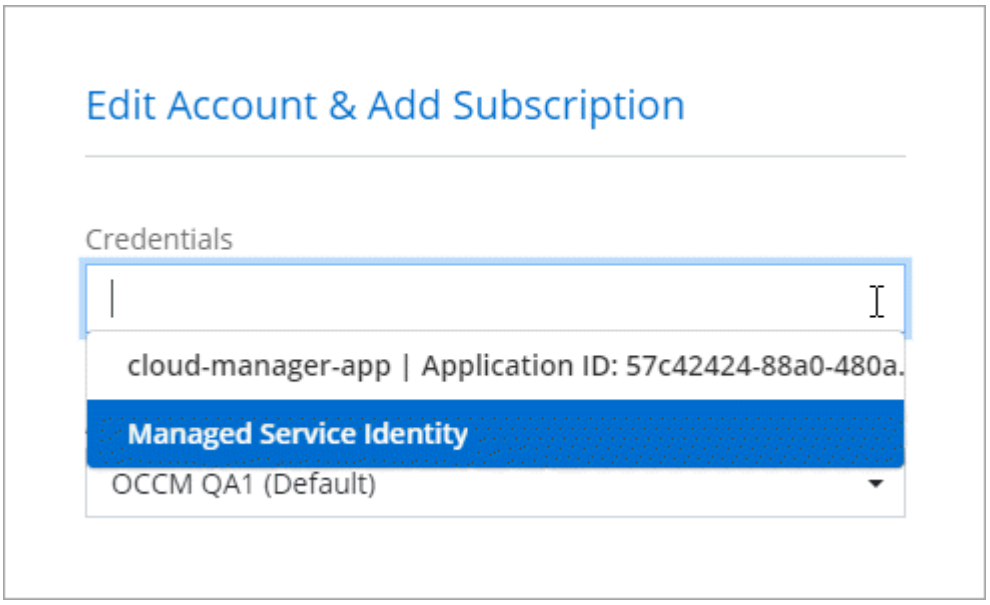
- クライアントシークレット

c. マーケットプレイス サブスクリプション: 今すぐサブスクライブするか、既存のサブスクリプションを選択して、マーケットプレイス サブスクリプションをこれらの資格情報に関連付けます。

d. 確認: 新しい資格情報の詳細を確認し、[追加] を選択します。

結果

詳細と資格情報ページから別の資格情報セットに切り替えることができます "コンソールにシステムを追加するとき"



既存の資格情報を管理する

Marketplace サブスクリプションを関連付けたり、資格情報を編集したり、削除したりすることで、コンソールに既に追加した Azure 資格情報を管理します。

Azure Marketplace サブスクリプションを資格情報に関連付ける

Azure 資格情報をコンソールに追加したら、Azure Marketplace サブスクリプションをそれらの資格情報に関連付けることができます。サブスクリプションを使用すると、従量課金制のCloud Volumes ONTAPシステムを作成し、 NetAppデータ サービスにアクセスできます。

コンソールに資格情報を追加した後に、Azure Marketplace サブスクリプションを関連付けるシナリオは 2 つあります。

- 資格情報をコンソールに最初に追加したときに、サブスクリプションを関連付けませんでした。
- Azure 資格情報に関連付けられている Azure Marketplace サブスクリプションを変更します。

  現在のマーケットプレイス サブスクリプションを置き換えると、既存および新しいCloud Volumes ONTAPシステム用に更新されます。

手順

1. *管理 > 資格情報*を選択します。

2. *組織の資格情報*を選択します。
3. コンソール エージェントに関連付けられている資格情報のセットのアクション メニューを選択し、[サブスクリプションの構成] を選択します。

   コンソール エージェントに関連付けられている資格情報を選択する必要があります。マーケットプレイス サブスクリプションを、 NetApp Consoleに関連付けられている資格情報に関連付けることはできません。

4. 資格情報を既存のサブスクリプションに関連付けるには、ドロップダウン リストからサブスクリプションを選択し、[構成] を選択します。
5. 資格情報を新しいサブスクリプションに関連付けるには、[サブスクリプションの追加] > [続行] を選択し、Azure Marketplace の手順に従います。

   a. プロンプトが表示されたら、Azure アカウントにログインします。
   b. *購読*を選択します。
   c. フォームに記入し、「購読」を選択します。
   d. サブスクリプションプロセスが完了したら、「今すぐアカウントを構成」を選択します。

      NetApp Consoleにリダイレクトされます。

   e. *サブスクリプションの割り当て*ページから:

      - このサブスクリプションを関連付けるコンソール組織またはアカウントを選択します。
      - 既存のサブスクリプションを置き換える フィールドで、1 つの組織またはアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

        コンソールは、組織またはアカウント内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

      他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。

      - *保存*を選択します。

        次のビデオでは、Azure Marketplace からサブスクライブする手順を示します。

Azure Marketplace からNetApp Intelligent Servicesをサブスクライブする

資格情報を編集する

コンソールで Azure 資格情報を編集します。たとえば、サービス プリンシパル アプリケーションに新しいシークレットが作成された場合は、クライアント シークレットを更新できます。

手順

1. *管理 > 資格情報*を選択します。
2. *組織の資格情報*を選択します。

3. 資格情報セットのアクション メニューを選択し、[資格情報の編集] を選択します。
4. 必要な変更を加えて、[適用] を選択します。

資格情報を削除する

資格情報セットが不要になった場合は、削除できます。システムに関連付けられていない資格情報のみを削除できます。

手順

1. *管理 > 資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. *組織の資格情報*ページで、資格情報セットのアクション メニューを選択し、*資格情報の削除*を選択します。
4. *削除*を選択して確認します。

Google Cloud

Google Cloud プロジェクトと権限について学ぶ

NetApp ConsoleがGoogle Cloud 認証情報を使用してユーザーに代わってアクションを実行する方法と、それらの認証情報がマーケットプレイスのサブスクリプションとどのように関連付けられるかについて説明します。これらの詳細を理解しておくと、1 つ以上の Google Cloud プロジェクトの認証情報を管理するときに役立ちます。たとえば、コンソール エージェント VM に関連付けられているサービス アカウントについて知りたい場合があります。

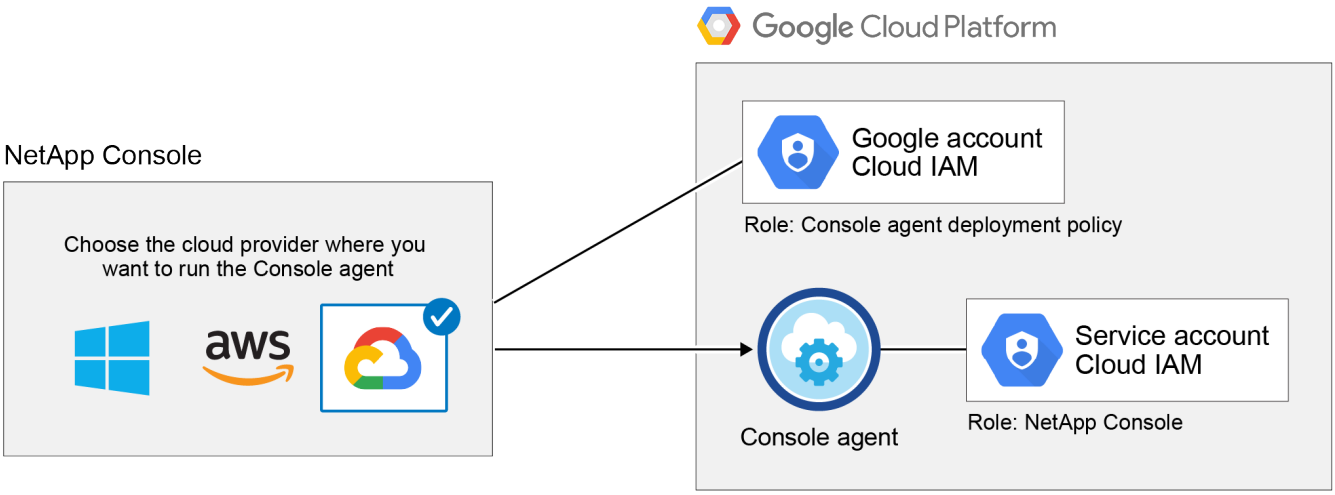
NetApp Consoleのプロジェクトと権限

コンソールを使用して Google Cloud プロジェクト内のリソースを管理する前に、まずコンソール エージェントをデプロイする必要があります。エージェントは、オンプレミスまたは別のクラウド プロバイダーで実行することはできません。

コンソール エージェントをコンソールから直接展開する前に、次の 2 セットの権限を設定する必要があります。

1. コンソールからコンソール エージェント VM インスタンスを起動する権限を持つ Google アカウントを使用して、コンソール エージェントを展開する必要があります。
2. コンソールエージェントを展開する際には、 "サービスアカウント" VM インスタンス用。コンソールは、サービス アカウントから権限を取得して、 Cloud Volumes ONTAPシステムの作成と管理、 NetAppバックアップとリカバリを使用したバックアップの管理などを行います。権限は、サービス アカウントにカスタム ロールを添付することによって提供されます。

次の図は、上記の 1 および 2 で説明した許可要件を示しています。



権限の設定方法については、次のページを参照してください。

- "標準モードの Google Cloud 権限を設定する"
- "制限モードの権限を設定する"

資格情報とマーケットプレイスのサブスクリプション

Google Cloud にコンソール エージェントをデプロイすると、コンソールは、コンソール エージェントが存在するプロジェクト内の Google Cloud サービス アカウントのデフォルトの認証情報セットを作成します。Cloud Volumes ONTAPおよびNetAppデータサービスの料金を支払うには、これらの認証情報を Google Cloud Marketplace サブスクリプションに関連付ける必要があります。

"Google Cloud Marketplace サブスクリプションを関連付ける方法を学びます" 。

Google Cloud の認証情報とマーケットプレイスのサブスクリプションについては、次の点に注意してください。

- コンソール エージェントに関連付けることができるのは、Google Cloud 認証情報の 1 セットのみです。
- 認証情報に関連付けることができるのは、Google Cloud Marketplace サブスクリプション 1 つだけです。
- 既存のマーケットプレイスサブスクリプションを新しいサブスクリプションに置き換えることができます

Cloud Volumes ONTAPプロジェクト

Cloud Volumes ONTAP は、コンソール エージェントと同じプロジェクトに存在することも、別のプロジェクトに存在することもできます。 Cloud Volumes ONTAP を別のプロジェクトにデプロイするには、まずそのプロジェクトにコンソール エージェントのサービス アカウントとロールを追加する必要があります。

- "サービスアカウントの設定方法を学ぶ"
- "Google Cloud でCloud Volumes ONTAPをデプロイし、プロジェクトを選択する方法を学びます"

NetApp Consoleの **Google Cloud** 認証情報とサブスクリプションを管理する

マーケットプレイス サブスクリプションを関連付け、サブスクリプション プロセスをトラブルシューティングすることで、コンソール エージェント VM インスタンスに関連付けられている Google Cloud 認証情報を管理できます。これら両方のタスクにより、マ

ーケットプレイスのサブスクリプションを使用してデータ サービスの支払いができるようになります。

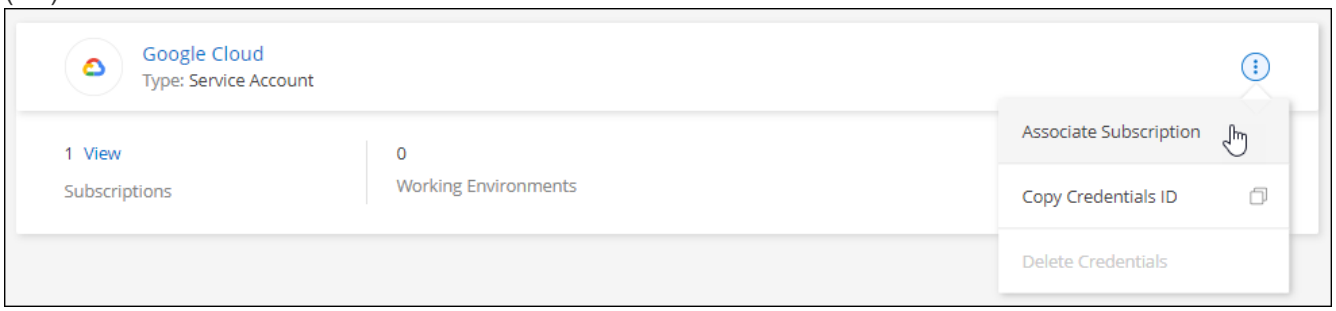
Marketplace サブスクリプションを **Google Cloud** 認証情報に関連付ける

Google Cloud にコンソール エージェントをデプロイすると、コンソールによって、コンソール エージェント VM インスタンスに関連付けられたデフォルトの認証情報セットが作成されます。これらの認証情報に関連付けられている Google Cloud Marketplace サブスクリプションはいつでも変更できます。このサブスクリプションを使用すると、従量課金制のCloud Volumes ONTAPシステムを作成し、他のデータ サービスを使用できるようになります。

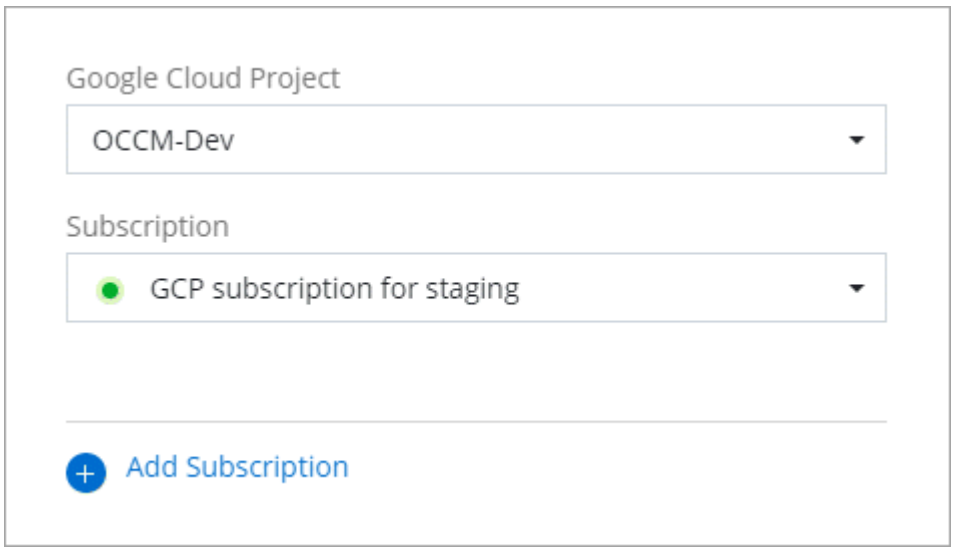
現在のマーケットプレイス サブスクリプションを新しいサブスクリプションに置き換えると、既存のCloud Volumes ONTAPシステムとすべての新しいシステムのマーケットプレイス サブスクリプションが変更されます。

手順

1. *管理 > *資格情報*を選択します。
2. *組織の資格情報*を選択します。
3. コンソール エージェントに関連付けられている資格情報のセットのアクション メニューを選択し、[サブスクリプションの構成] を選択します。 +新しいスクリーンショットが必要です (TS)



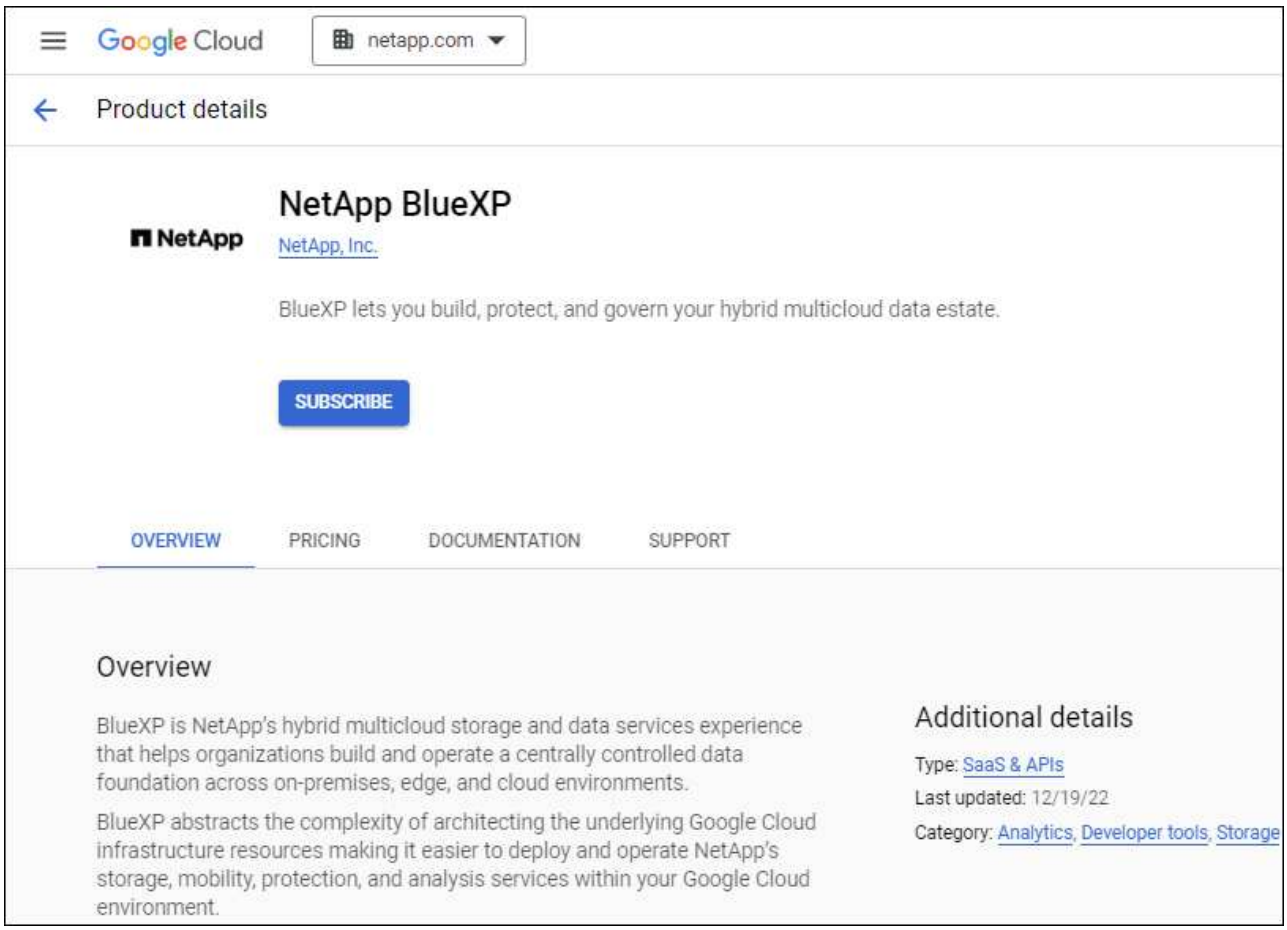
4. 選択した認証情報を使用して既存のサブスクリプションを構成するには、ドロップダウン リストから Google Cloud プロジェクトとサブスクリプションを選択し、[構成] を選択します。



5. まだサブスクリプションをお持ちでない場合は、[サブスクリプションを追加] > [続行] を選択し、Google Cloud Marketplace の手順に従います。

次の手順を完了する前に、Google Cloud アカウントの課金管理者権限とNetApp Consoleのログイン権限の両方があることを確認してください。

a. リダイレクトされたら "Google Cloud Marketplace のNetApp Intelligent Servicesページ"上部のナビゲーション メニューで正しいプロジェクトが選択されていることを確認します。



b. *購読*を選択します。

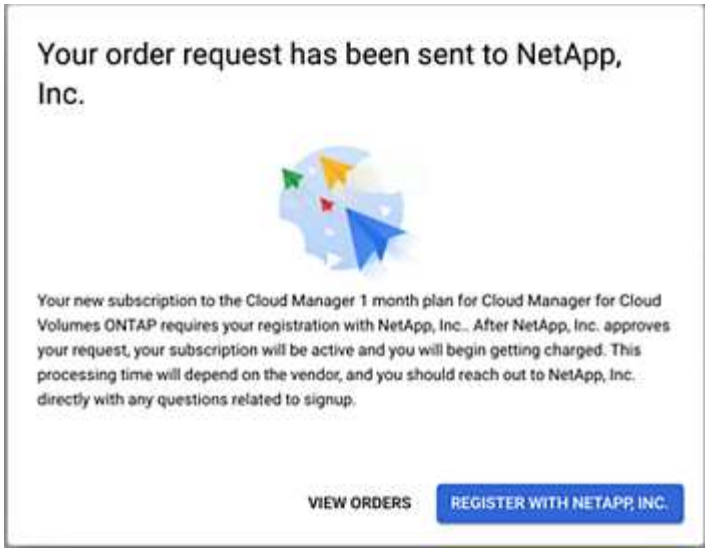
c. 適切な請求先アカウントを選択し、利用規約に同意します。

d. *購読*を選択します。

この手順により、転送リクエストがNetAppに送信されます。

e. ポップアップダイアログボックスで、* NetApp, Inc.に登録*を選択します。

Google Cloud サブスクリプションをコンソールの組織またはアカウントにリンクするには、この手順を完了する必要があります。このページからリダイレクトされ、コンソールにサインインするまで、サブスクリプションをリンクするプロセスは完了しません。



f. サブスクリプションの割り当て ページの手順を完了します。

> 組織内の誰かが既に請求先アカウントからマーケットプレイスサブスクリプションを利用している場合は、次のページにリダイレクトされます。 "NetApp Console内のCloud Volumes ONTAPページ"その代わり。予期しない事態が発生した場合は、 NetAppの営業チームにお問い合わせください。 Google では、Google 請求先アカウントごとに 1 つのサブスクリプションのみ有効になります。

- このサブスクリプションを関連付けるコンソール組織またはアカウントを選択します。
- 既存のサブスクリプションを置き換える フィールドで、1 つの組織またはアカウントの既存のサブスクリプションをこの新しいサブスクリプションに自動的に置き換えるかどうかを選択します。

  コンソールは、組織またはアカウント内のすべての資格情報の既存のサブスクリプションをこの新しいサブスクリプションに置き換えます。資格情報のセットがサブスクリプションに関連付けられたことがない場合、この新しいサブスクリプションはそれらの資格情報に関連付けられません。

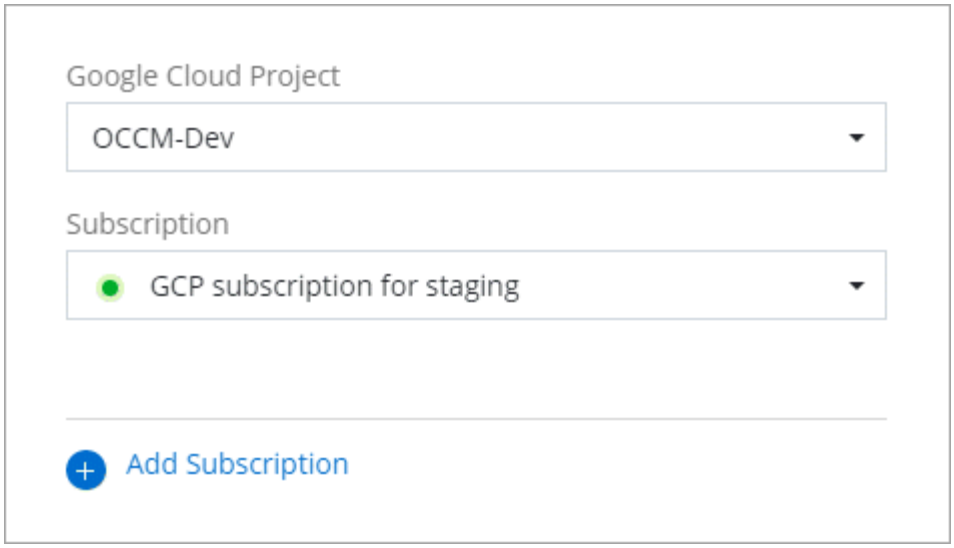
他のすべての組織またはアカウントについては、これらの手順を繰り返して、サブスクリプションを手動で関連付ける必要があります。

- *保存*を選択します。

  次のビデオでは、Google Cloud Marketplace からサブスクライブする手順を示します。

Google Cloud Marketplace から登録する

a. このプロセスが完了したら、コンソールの [資格情報] ページに戻り、この新しいサブスクリプションを選択します。

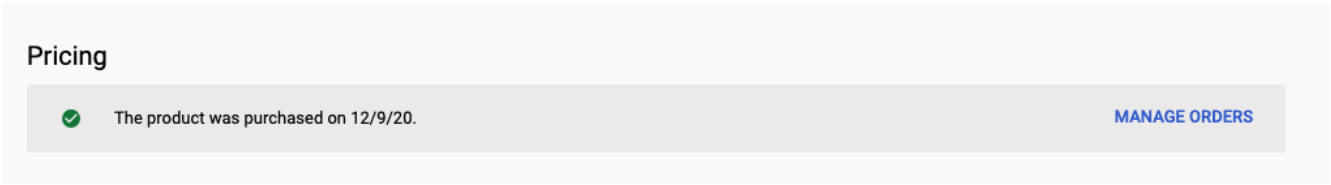


マーケットプレイスのサブスクリプションプロセスのトラブルシューティング

Google Cloud Marketplace を通じてNetAppデータ サービスにサブスクライブすると、権限が間違っていたり、誤ってコンソールへのリダイレクトに従わなかったりしたために、断片化されることがあります。このような場合は、次の手順に従ってサブスクリプション プロセスを完了してください。

手順

1. に移動 "Google Cloud Marketplace のNetAppページ"注文の状態を確認します。ページに「プロバイダーで管理」と表示されている場合は、下にスクロールして「注文の管理」を選択します。



◦ 注文に緑色のチェックマークが表示され、これが予期しない場合は、同じ請求アカウントを使用している組織内の他のユーザーがすでにサブスクライブしている可能性があります。これが予期しないものである場合、またはこのサブスクリプションの詳細が必要な場合は、 NetApp の営業チームにお問い合わせください。

◦ 注文に時計と「保留中」ステータスが表示されている場合は、マーケットプレイス ページに戻り、「プロバイダーで管理」を選択して、上記に記載されているプロセスを完了します。

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 アカウントを関連付けることもサポートされています。"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。

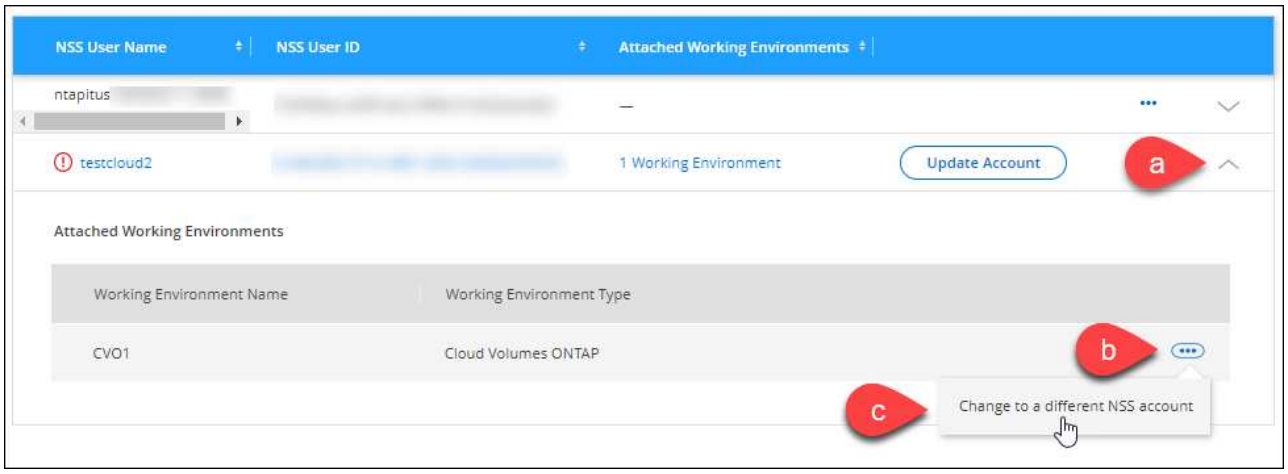
システムを別のNSSアカウントに接続する

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

コンソールで使用しなくなった 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ログインに関連付けられた資格情報を管理する

コンソールで実行したアクションに応じて、 ONTAP資格情報とNetAppサポート サイト (NSS) 資格情報がユーザー ログインに関連付けられている場合があります。関連付けた資格情報を表示および管理できます。たとえば、これらの資格情報のパスワードを変更する場合は、コンソールでパスワードを更新する必要があります。

ONTAP認証情報

コンソールでONTAPクラスターを検出するには、ユーザーはONTAP管理者の認証情報が必要です。ただし、ONTAP System Manager へのアクセスは、コンソール エージェントを使用しているかどうかによって異なります。

コンソールエージェントなし

ユーザーは、クラスタのONTAP System Manager にアクセスするために、 ONTAP認証情報を入力するよう求められます。ユーザーはこれらの資格情報をコンソールに保存することを選択できます。これにより、毎回資格情報を入力する必要がなくなります。ユーザー資格情報はそれぞれのユーザーのみに表示され、「ユーザー資格情報」ページから管理できます。

コンソールエージェントを使用

デフォルトでは、ユーザーはONTAP System Manager にアクセスするためにONTAP認証情報を入力するように求められません。ただし、コンソール管理者（組織管理者ロールを持つ）は、ユーザーにONTAP認証情報の入力を求めるようにコンソールを設定できます。この設定を有効にすると、ユーザーは毎回ONTAP認証情報を入力する必要があります。

"詳細情報"

NSS認証情報

NetApp Consoleログインに関連付けられた NSS 資格情報により、サポート登録、ケース管理、およびDigital Advisorへのアクセスが可能になります。

- サポート > リソース にアクセスしてサポートに登録すると、NSS 資格情報をログインに関連付けるように求められます。

  これにより、組織またはアカウントがサポートに登録され、サポート資格が有効になります。サポートに

登録し、サポート資格を有効にするには、組織内の 1 人のユーザーのみがNetAppサポート サイト アカウントをログインに関連付ける必要があります。これが完了すると、リソース ページにアカウントがサポートに登録されていることが表示されます。

"サポート登録方法を学ぶ"

- 管理 > サポート > ケース管理 にアクセスすると、まだ入力していない場合は NSS 資格情報を入力するように求められます。このページでは、NSS アカウントおよび会社に関連付けられたサポート ケースを作成および管理できます。
- コンソールでDigital Advisorにアクセスすると、NSS 資格情報を入力してDigital Advisorにログインするように求められます。

ログインに関連付けられている NSS アカウントについては、次の点に注意してください。

- アカウントはユーザーレベルで管理されるため、ログインした他のユーザーには表示されません。
- Digital Advisorおよびサポート ケース管理に関連付けられる NSS アカウントは、ユーザーごとに 1 つだけです。
- NetAppサポート サイト アカウントをCloud Volumes ONTAPシステムに関連付ける場合は、自分が所属する組織に追加された NSS アカウントからのみ選択できます。

  NSS アカウント レベルの資格情報は、ログインに関連付けられている NSS アカウントとは異なります。NSS アカウント レベルの認証情報を使用すると、BYOL を使用してCloud Volumes ONTAPをデプロイし、PAYGO システムを登録し、ソフトウェアをアップグレードできます。

  "NetApp Console組織またはアカウントで NSS 認証情報を使用する方法の詳細" 。

ユーザー資格情報を管理する

ユーザー名とパスワードを更新するか、資格情報を削除して、ユーザー資格情報を管理します。

手順

1. *管理 > 資格情報*を選択します。
2. *ユーザー資格情報*を選択します。
3. まだユーザー資格情報がない場合は、「**NSS** 資格情報の追加」を選択して、 NetAppサポート サイト アカウントを追加できます。
4. [アクション] メニューから次のオプションを選択して、既存の資格情報を管理します。
   - 資格情報の更新: アカウントのユーザー名とパスワードを更新します。
   - 資格情報の削除: コンソール ログインに関連付けられている NSS アカウントを削除します。

NetApp Consoleの操作を監視する

コンソールが実行している操作のステータスを監視して、対処する必要がある問題があるかどうかを確認できます。監査ページや通知センターからステータスを確認したり、電子メールに通知を送信したりすることができます。

この表では、監査ページと通知センターの機能を比較して詳しく説明しています。

通知センター	監査ページ
イベントとアクションの高レベルのステータスを表示します	さらなる調査のために各イベントまたはアクションの詳細を提供します
現在のログイン セッションのステータスを表示します (ログオフ後は通知センターに情報は表示されません)	過去1か月間のステータスを維持
ユーザーインターフェースで開始されたアクションのみを表示します	UI または API からのすべてのアクションを表示します
ユーザーが開始したアクションを表示します	ユーザーが開始したものかシステムが開始したものかを問わず、すべてのアクションを表示します
重要度で結果をフィルタリング	サービス、アクション、ユーザー、ステータスなどでフィルタリング
ユーザーや他のユーザーに電子メール通知を送信する機能を提供します	メール機能なし

監査ページからユーザーアクティビティを監査する

監査ページには、ユーザーが組織またはアカウントを管理するために実行したアクションが表示されます。これには、ユーザーの関連付け、システムの作成、エージェントの作成などの管理アクションが含まれます。

監査ページを使用して、アクションを実行したユーザーやそのステータスを識別します。

手順

1. *管理 > 監査*を選択します。
2. 表の上にあるフィルターを使用して、表に表示されるアクションを変更します。

   たとえば、サービス フィルターを使用して特定のサービスに関連するアクションを表示したり、ユーザー フィルターを使用して特定のユーザー アカウントに関連するアクションを表示したりできます。

監査ページから監査ログをダウンロードする

監査ページから監査ログを CSV ファイルにダウンロードできます。これにより、組織内でユーザーが実行するアクションを記録できるようになります。 CSV ファイルには、監査ページのフィルターや表示されている列に関係なく、ダウンロードした CSV ファイルのすべての列が含まれます。

手順

1. *監査*ページで、テーブルの右上隅にあるダウンロード アイコンを選択します。

通知センターを使用してアクティビティを監視する

通知はコンソールの操作を追跡して成功を確認します。これらを使用すると、現在のログイン セッション中に開始した多くのコンソール アクションのステータスを表示できます。すべてのコンソール サービスが通知センターに情報を報告するわけではありません。

通知ベル（  ）をクリックします。ベル内の小さなバブルの色は、アクティブな最高レベルの重大度通知を示します。したがって、赤いバブルが表示された場合は、確認する必要がある重要な通知があることを意味し

ます。

また、特定の種類の通知を電子メールで送信するようにコンソールを構成することもできます。これにより、システムにログインしていない場合でも重要なシステム アクティビティについて通知を受けることができます。電子メールは、組織に属するすべてのユーザー、または特定の種類のシステム アクティビティを認識する必要があるその他の受信者に送信できます。方法を見るメール通知設定を設定する。

通知センターとアラートの比較

通知センターを使用すると、開始した操作のステータスを表示したり、特定の種類のシステム アクティビティに関するアラート通知を設定したりできます。一方、アラートを使用すると、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ONTAPストレージ環境の問題や潜在的なリスクを確認できます。

"NetApp Consoleアラートの詳細"

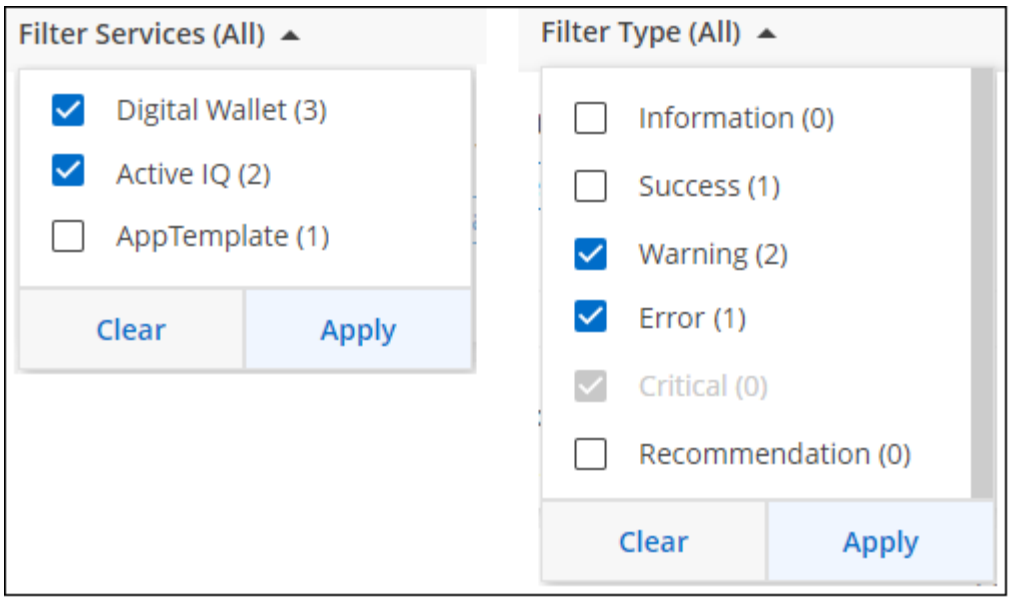
通知タイプ

コンソールは通知を次のカテゴリに分類します。

通知の種類	説明
致命的	問題が発生しており、すぐに対処しないとサービスが停止する可能性があります。
エラー	アクションまたはプロセスは失敗して終了しました。または、修正アクションが実行されないと、失敗につながる可能性があります。
警告	重大な重大度に達しないように注意する必要がある問題。この重大度の通知ではサービスの中断は発生しないため、即時の修正アクションは必要ない可能性があります。
推奨事項	システムまたは特定のサービスを改善するためのアクションを実行するためのシステム推奨事項。例: コスト削減、新しいサービスの提案、推奨されるセキュリティ構成など。
情報	アクションまたはプロセスに関する追加情報を提供するメッセージ。
成功	アクションまたはプロセスが正常に完了しました。

通知をフィルタリングする

デフォルトでは、すべてのアクティブな通知が通知センターに表示されます。表示される通知をフィルタリングして、自分にとって重要な通知だけを表示することができます。 「サービス」と通知の「タイプ」でフィルタリングできます。



たとえば、コンソール操作の「エラー」と「警告」の通知のみを表示する場合は、それらのエントリを選択すると、それらの種類の通知のみが表示されます。

通知を閉じる

通知を表示する必要がなくなった場合は、ページから通知を削除できます。通知は個別に、または一度にすべて閉じることができます。

すべての通知を閉じるには、通知センターで[すべて閉じる]を選択します。

個々の通知を閉じるには、通知の上にカーソルを移動し、[閉じる] を選択します。

メール通知設定を設定する

特定の種類の通知を電子メールで送信できるため、ログインしていないときでも重要なシステム アクティビティについて通知を受けることができます。電子メールは、組織またはアカウントに属するすべてのユーザー、または特定の種類のシステム アクティビティを認識する必要があるその他の受信者に送信できます。

- コンソールは、エージェント、ライセンスとサブスクリプション、 NetApp Copy and Sync、およびNetApp Backup and Recoveryに関する電子メール通知を送信します。
- コンソール エージェントがインターネットにアクセスできないサイトにインストールされている場合、電子メール通知の送信はサポートされません。

通知センターで設定したフィルターによって、電子メールで受信する通知の種類が決まるわけではありません。デフォルトでは、すべての組織管理者はすべての「重要」および「推奨事項」通知のメールを受信します。これらの通知はすべてのサービスに渡されるため、エージェントやNetApp Backup and Recoveryなどの特定のサービスについてのみ通知を受信するように選択することはできません。

他のすべてのユーザーと受信者は通知メールを受信しないように設定されているため、追加のユーザーに対して通知設定を構成する必要があります。

通知設定をカスタマイズするには、組織管理者の役割が必要です。

手順

1. *管理 > 通知設定*を選択します。
2. *組織ユーザー*または*追加の受信者*を選択します。

   追加の受信者 ページでは、コンソール組織のメンバーである人々に通知するようにコンソールを設定できます。

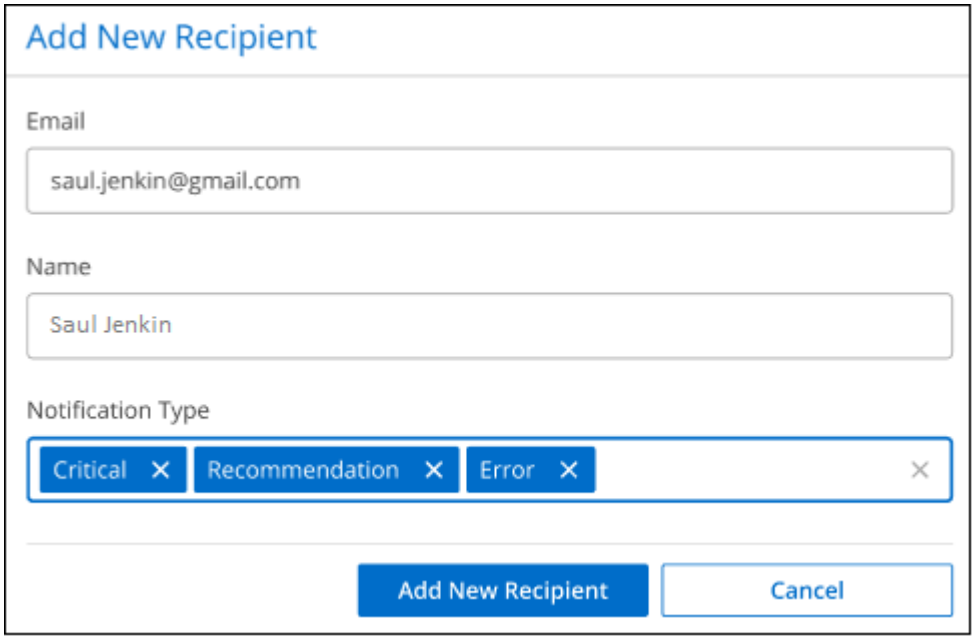
3. 組織ユーザー ページまたは 追加受信者 ページから 1 人または複数のユーザーを選択し、送信する通知の種類を選択します。
   - 1 人のユーザーに対して変更を行うには、そのユーザーの [通知] 列のメニューを選択し、送信する通知の種類をチェックして、[適用] を選択します。
   - 複数のユーザーに対して変更を行うには、各ユーザーのボックスをオンにし、「電子メール通知の管理」を選択し、送信する通知の種類をオンにして、「適用」を選択します。

追加のメール受信者を追加する

組織ユーザー ページに表示されるユーザーは、組織またはアカウント内のユーザーから自動的に入力されます。コンソールへのアクセス権を持たないが、特定の種類のアラートや通知について通知を受ける必要がある他のユーザーまたはグループの電子メール アドレスを [追加の受信者] ページに追加できます。

手順

1. *通知設定*ページから、*新しい受信者を追加*を選択します。



2. 名前、メールアドレスを入力し、受信者が受信する通知の種類を選択して、「新しい受信者を追加」を選択します。

参照

エージェントメンテナンスコンソール

コンソールエージェントメンテナンスコンソール

コンソール エージェント メンテナンス コンソールを使用して、透過プロキシ サーバーを使用するようにコンソール エージェントを構成できます。

エージェントメンテナンスコンソールにアクセスする

コンソール エージェント ホストからメンテナンス コンソールにアクセスできます。次のディレクトリに移動します。

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

透過プロキシコマンド

エージェント メンテナンス コンソールには、透過プロキシ サーバーを使用するようにエージェントを構成するコマンドが用意されています。

現在の透過プロキシ構成を表示する

現在の透過プロキシ構成を表示するには、次のコマンドを使用します。

```
./agent-maint-console proxy get
```

透過プロキシサーバーを追加する

透過プロキシサーバーを追加するには、次のコマンドを使用します。 `/home/ubuntu/myCA1.pem`プロキシ サーバーの証明書ファイルへのパスです。証明書ファイルは PEM 形式である必要があります。

```
./agent-maint-console proxy add -c /home/ubuntu/myCA1.pem
```

証明書ファイルがコマンドと同じディレクトリにあることを確認するか、証明書ファイルへの完全パスを指定します。

透過プロキシサーバーの証明書を更新する

透過プロキシサーバーの証明書を更新するには、次のコマンドを使用します。 `/home/ubuntu/myCA1.pem`プロキシ サーバーの新しい証明書ファイルへのパスです。証明書ファイルは PEM 形式である必要があります。

```
./agent-maint-console proxy update -c /home/ubuntu/myCA1.pem
```

証明書ファイルがコマンドと同じディレクトリにあることを確認するか、証明書ファイルへの完全パスを指定します。

透過プロキシサーバーを削除する

透過プロキシ サーバーを削除するには、次のコマンドを使用します。

```
./agent-maint-console proxy remove
```

任意のコマンドのヘルプを表示する

コマンドのヘルプを表示するには、 `--help`コマンドに。たとえば、 `proxy add`コマンドを実行するには、次のコマンドを使用します。

```
./agent-maint-console proxy add --help
```

権限

NetApp Consoleの権限の概要

NetApp Consoleの機能とサービスを使用するには、コンソールがクラウド環境で操作を実行できるように権限を付与する必要があります。このページのリンクを使用して、目標に応じて必要な権限にすばやくアクセスします。

AWS 権限

NetApp Consoleには、コンソールエージェントと個々のサービスに対する AWS 権限が必要です。

コンソールエージェント

目標	説明	リンク
コンソールからコンソールエージェントを展開する	コンソールからコンソールエージェントを作成するユーザーには、AWS にインスタンスをデプロイするための特定の権限が必要です。	"AWS権限を設定する"
コンソールエージェントに権限を付与する	コンソールがコンソールエージェントをデプロイすると、AWS アカウント内のリソースとプロセスを管理するために必要なアクセス許可を提供するポリシーがインスタンスにアタッチされます。 AWS Marketplaceからコンソールエージェントをデプロイする場合、コンソールエージェントを手動でインストールする場合、または"コンソールエージェントにAWS認証情報を追加する"。また、後続のリリースで新しい権限が追加された場合、ポリシーが最新であることを確認する必要があります。	"コンソールエージェントのAWS権限"

NetApp Backup and Recovery

目標	説明	リンク
NetApp Backup and Recoveryを使用してオンプレミスのONTAPクラスターを Amazon S3 にバックアップする	ONTAPボリュームでバックアップをアクティブ化するときに、NetApp Backup and Recovery、特定の権限を持つ IAM ユーザーのアクセス キーとシークレットを入力するように求められます。	"バックアップ用のS3権限を設定する"

Cloud Volumes ONTAP

目標	説明	リンク
Cloud Volumes ONTAPノードに権限を付与する	AWS の各Cloud Volumes ONTAPノードに IAM ロールを添付する必要があります。 HA メディエーターについても同様です。デフォルトのオプションでは、コンソールで IAM ロールが自動的に作成されますが、コンソールでシステムを作成するときに独自のロールを使用することもできます。	"IAMロールを自分で設定する方法を学ぶ"

NetApp Copy and Sync

目標	説明	リンク
AWSにデータブローカーをデプロイする	データブローカーをデプロイするために使用する AWS ユーザー アカウントには、特定の権限が必要です。	"AWS にデータブローカーをデプロイするために必要な権限"
データブローカーに権限を付与する	NetApp Copy and Sync がデータ ブローカーを展開すると、データ ブローカー インスタンスの IAM ロールが作成されます。必要に応じて、独自の IAM ロールを使用してデータ ブローカーをデプロイすることもできます。	"AWS データブローカーで独自の IAM ロールを使用するための要件"
手動でインストールされたデータブローカーの AWS アクセスを有効にする	S3 バケットを含む同期関係でデータ ブローカーを使用する場合は、AWS アクセス用に Linux ホストを準備する必要があります。データブローカーをインストールするときは、プログラムによるアクセスと特定の権限を持つ IAM ユーザーに AWS キーを提供する必要があります。	"AWSへのアクセスを有効にする"

ONTAP向け FSx

目標	説明	リンク
FSx for ONTAP の作成と管理	Amazon FSx for NetApp ONTAPシステムを作成または管理するには、コンソールに必要な権限を付与する IAM ロールの ARN を指定して、AWS 認証情報をコンソールに追加する必要があります。	"FSx 用の AWS 認証情報を設定する方法を学ぶ"

NetApp Cloud Tiering

目標	説明	リンク
オンプレミスのONTAPクラスターを Amazon S3 に階層化する	NetApp Cloud Tiering to AWS を有効にすると、ウィザードによってアクセス キーとシークレット キーの入力が求められます。これらの認証情報はONTAPクラスターに渡され、 ONTAP はデータを S3 バケットに階層化できるようになります。	"階層化のためのS3権限を設定する"

Azure のアクセス許可

コンソールには、コンソール エージェントと個々のサービスに対する Azure アクセス許可が必要です。

コンソールエージェント

目標	説明	リンク
コンソールからコンソールエージェントを展開する	コンソールからコンソール エージェントを展開する場合は、Azure にコンソール エージェント VM を展開する権限を持つ Azure アカウントまたはサービス プリンシパルを使用する必要があります。	"Azure の権限を設定する"
コンソールエージェントに権限を付与する	コンソールが Azure にコンソール エージェント VM を展開すると、その Azure サブスクリプション内のリソースとプロセスを管理するために必要なアクセス許可を提供するカスタム ロールが作成されます。 マーケットプレイスからコンソールエージェントを起動する場合、コンソールエージェントを手動でインストールする場合、または"コンソールエージェントにAzure資格情報を追加する"。 また、後続のリリースで新しい権限が追加された場合、ポリシーが最新であることを確認する必要があります。	"コンソールエージェントの Azure 権限"

NetApp Backup and Recovery

目標	説明	リンク
Cloud Volumes ONTAP をAzure BLOB ストレージにバックアップする	NetApp Backup and Recoveryを使用してCloud Volumes ONTAPをバックアップする場合、次のシナリオでコンソール エージェントに権限を追加する必要があります。 • 「検索と復元」機能を使用したい • 顧客管理暗号鍵（CMEK）を使用したい	• "バックアップとリカバリを使用して、 Cloud Volumes ONTAP データを Azure Blob ストレージにバックアップします。"
オンプレミスのONTAPクラスターを Azure BLOB ストレージにバックアップする	NetApp Backup and Recoveryを使用してオンプレミスのONTAP クラスターをバックアップする場合は、「検索と復元」機能を使用するために、コンソール エージェントに権限を追加する必要があります。	"バックアップとリカバリを使用してオンプレミスのONTAPデータを Azure Blob ストレージにバックアップする"

NetAppコピーと同期

目標	説明	リンク
Azureにデータブローカーをデプロイする	データ ブローカーをデプロイするために使用する Azure ユーザー アカウントには、必要なアクセス許可が必要です。	"Azure にデータ ブローカーをデプロイするために必要な権限"

Google Cloud の権限

コンソールでは、コンソール エージェントと個々のサービスに対する Google Cloud 権限が必要です。

コンソールエージェント

目標	説明	リンク
コンソールからコンソールエージェントを展開する	コンソールからコンソール エージェントをデプロイする Google Cloud ユーザーには、Google Cloud にコンソール エージェントをデプロイするための特定の権限が必要です。	"コンソールエージェントを作成するための権限を設定する"
コンソールエージェントに権限を付与する	コンソール エージェント VM インスタンスのサービス アカウントには、日常的な操作のための特定の権限が必要です。展開中に、サービス アカウントをコンソール エージェントに関連付ける必要があります。また、後続のリリースで新しい権限が追加された場合、ポリシーが最新であることを確認する必要があります。	"コンソールエージェントの権限を設定する"

NetApp Backup and Recovery

目標	説明	リンク
Cloud Volumes ONTAPをGoogle Cloudにバックアップする	NetApp Backup and Recoveryを使用してCloud Volumes ONTAPをバックアップする場合、次のシナリオでコンソール エージェントに権限を追加する必要があります。 • 「検索と復元」機能を使用したい • 顧客管理暗号鍵（CMEK）を使用したい	• "バックアップとリカバリを使用して、 Cloud Volumes ONTAP データを Google Cloud Storage にバックアップします。" • "CMEK の権限"
オンプレミスのONTAPクラスタを Google Cloud にバックアップする	NetApp Backup and Recoveryを使用してオンプレミスのONTAP クラスターをバックアップする場合は、「検索と復元」機能を使用するために、コンソール エージェントに権限を追加する必要があります。	"バックアップとリカバリを使用してオンプレミスのONTAPデータを Google Cloud Storage にバックアップする"

NetApp Copy and Sync

目標	説明	リンク
Google Cloud にデータブローカーをデプロイする	データ ブローカーをデプロイする Google Cloud ユーザーに必要な権限があることを確認します。	"Google Cloud にデータブローカーをデプロイするために必要な権限"
手動でインストールされたデータブローカーの Google Cloud アクセスを有効にする	Google Cloud Storage バケットを含む同期関係でデータ ブローカーを使用する予定の場合は、Google Cloud アクセス用に Linux ホストを準備する必要があります。データ ブローカーをインストールするときは、特定の権限を持つサービス アカウントのキーを指定する必要があります。	"Google Cloudへのアクセスを有効にする"

StorageGRID権限

コンソールには、2 つのサービスに対するStorageGRID権限が必要です。

NetApp Backup and Recovery

目標	説明	リンク
オンプレミスのONTAPクラスターをStorageGRIDにバックアップする	StorageGRID をONTAPクラスターのバックアップ ターゲットとして準備する場合、 NetApp Backup and Recovery、特定の権限を持つ IAM ユーザーのアクセス キーとシークレットを入力するように求められます。	"StorageGRIDをバックアップターゲットとして準備する"

NetApp Cloud Tiering

目標	説明	リンク
オンプレミスのONTAPクラスターをStorageGRIDに階層化	NetApp Cloud Tiering をStorageGRIDに設定する場合は、Cloud Tiering に S3 アクセス キーと秘密キーを提供する必要があります。クラウド階層化では、キーを使用してバケットにアクセスします。	"StorageGRIDへの階層化を準備する"

コンソールエージェントのAWS権限

NetApp ConsoleがAWS でコンソール エージェント インスタンスを起動すると、そのインスタンスにポリシーがアタッチされ、その AWS アカウント内のリソースとプロセスを管理するための権限がエージェントに付与されます。エージェントは、権限を使用して、EC2、S3、CloudFormation、IAM、キー管理サービス (KMS) などの複数の AWS サービスへの API 呼び出しを実行します。

IAMポリシー

以下の IAM ポリシーは、AWS リージョンに基づいてパブリッククラウド環境内のリソースとプロセスを管理するためにコンソールエージェントに必要な権限を提供します。

次の点に注意してください。

- コンソールから直接標準 AWS リージョンにコンソールエージェントを作成すると、コンソールはエージ

ェントにポリシーを自動的に適用します。

- AWS Marketplace からエージェントをデプロイする場合、Linux ホストにエージェントを手動でインストールする場合、またはコンソールに追加の AWS 認証情報を追加する場合は、ポリシーを自分で設定する必要があります。
- いずれの場合も、後続のリリースで新しい権限が追加されるため、ポリシーが最新であることを確認する必要があります。新しい権限が必要な場合は、リリース ノートに記載されます。
- 必要に応じて、IAMを使用してIAMポリシーを制限することができます。 `Condition`要素。 "AWS ドキュメント: 条件要素"
- これらのポリシーの使用方法の詳細な手順については、次のページを参照してください。
  - "AWS Marketplace デプロイメントの権限を設定する"
  - "オンプレミス展開の権限を設定する"
  - "制限モードの権限を設定する"

必要なポリシーを表示するには、地域を選択してください。

標準地域

標準リージョンの場合、権限は 2 つのポリシーに分散されます。 AWS の管理ポリシーの最大文字サイズ制限により、2 つのポリシーが必要になります。

ポリシー1

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DescribeTags",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:CreatePlacementGroup",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DescribeVpcs",
```

```
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteRoute",
                "ec2:DeletePlacementGroup",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeVolumesModifications",
                "ec2:ModifyVolume",
                "cloudformation:CreateStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "cloudformation:DeleteStack",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:ListInstanceProfiles",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DeleteInstanceProfile",
                "iam:GetRolePolicy",
                "iam:GetRole",
                "sts:DecodeAuthorizationMessage",
                "sts:AssumeRole",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketPolicy",
                "s3:GetBucketAcl",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:PutObject",
                "s3:ListAllMyBuckets",
```

```
                "s3:GetObject",
                "s3:GetEncryptionConfiguration",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "fsx:Describe*",
                "fsx:List*",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "cvoServicePolicy"
        },
        {
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "kms:List*",
                "kms:Describe*",
                "ec2:DescribeVpcEndpoints",
                "kms:ListAliases",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
```

```
                "glue:BatchDeletePartition"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "backupPolicy"
        },
        {
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:DeleteBucket",
                "s3:GetObjectVersionTagging",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:PutObjectVersionTagging",
                "s3:PutObjectRetention",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::netapp-backup-*"
            ],
            "Effect": "Allow",
            "Sid": "backupS3Policy"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteBucket"
            ],
            "Resource": [
                "arn:aws:s3:::fabric-pool*"
            ],
            "Effect": "Allow",
            "Sid": "fabricPoolS3Policy"
        },
        {
            "Action": [
                "ec2:DescribeRegions"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "fabricPoolPolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/netapp-adc-manager": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
```

```
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume",
                "ec2:StopInstances",
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        }
```

```
    ]
}
```

ポリシー**2**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "tag:getResources",
                "tag:getTagKeys",
                "tag:getTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "tagServicePolicy"
        }
    ]
}
```

GovCloud（米国）リージョン

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListInstanceProfiles",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "ec2:ModifyVolumeAttribute",
                "sts:DecodeAuthorizationMessage",
                "ec2:DescribeImages",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstances",
                "iam:PassRole",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
```

```
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:StopInstances",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:CreateBucket",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
```

```
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::fabric-pool*"
            ]
        },
        {
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::netapp-backup-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
```

```
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

秘密の地域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
```

```
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
```

```
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

極秘地域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
```

```
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
```

```
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

AWS権限の使用方法

次のセクションでは、各NetApp Console管理サービスまたはデータ サービスに対して権限がどのように使用されるかについて説明します。この情報は、必要な場合にのみ権限を付与するように企業ポリシーで定められている場合に役立ちます。

Amazon FSx for ONTAP

コンソールエージェントは、 Amazon FSx for ONTAPファイルシステムを管理するために次の API リクエストを行います。

- ec2:インスタンスの説明
- ec2:インスタンスステータスの説明
- ec2:インスタンス属性の説明
- ec2:ルートテーブルの説明
- ec2:画像の説明
- ec2:タグの作成
- ec2:ボリュームの説明
- ec2:セキュリティグループの説明

- ec2:ネットワークインターフェースの説明
- ec2:サブネットの説明
- ec2:Vpcs の説明
- ec2:Dhcpオプションの説明
- ec2:スナップショットの説明
- ec2:キーペアの説明
- ec2:リージョンの説明
- ec2:タグの説明
- ec2:IamInstanceProfileAssociations の説明
- ec2:予約済みインスタンスの提供内容の説明
- ec2:Vpcエンドポイントの説明
- ec2:Vpcs の説明
- ec2:ボリュームの変更の説明
- ec2:配置グループの説明
- kms:リスト*
- kms:説明*
- kms:許可の作成
- kms:エイリアスのリスト
- fsx:説明*
- fsx:リスト*

Amazon S3 バケット検出

コンソールエージェントは、Amazon S3 バケットを検出するために次の API リクエストを行います。

s3:暗号化設定の取得

NetApp Backup and Recovery

エージェントは、Amazon S3 内のバックアップを管理するために次の API リクエストを行います。

- s3:GetBucketLocation
- s3:すべてのバケットをリスト
- s3:リストバケット
- s3:バケットの作成
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:バケットバージョンのリスト

- s3:GetBucketAcl
- s3:PutBucketパブリックアクセスブロック
- kms:リスト*
- kms:説明*
- s3:GetObject
- ec2:Vpcエンドポイントの説明
- kms:エイリアスのリスト
- s3:PutEncryptionConfiguration

検索と復元方法を使用してボリュームとファイルを復元する場合、エージェントは次の API 要求を行います。

- s3:バケットの作成
- s3:オブジェクトの削除
- s3:オブジェクトバージョンの削除
- s3:GetBucketAcl
- s3:リストバケット
- s3:バケットバージョンのリスト
- s3:リストバケットマルチパートアップロード
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketパブリックアクセスブロック
- s3:マルチパートアップロードの中止
- s3:ListMultipartUploadParts
- athena:クエリ実行の開始
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- グルー:データベースの作成
- グルー:CreateTable
- グルー:バッチ削除パーティション

ボリュームのバックアップに DataLock とNetApp Ransomware Resilienceを使用する場合、エージェントは次の API 要求を行います。

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl

- s3:オブジェクトのタグ付け
- s3:オブジェクトの削除
- s3:オブジェクトのタグ付けを削除
- s3:GetObjectRetention
- s3:オブジェクトバージョンタグ付けの削除
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:タグによるバケットのリスト
- s3:GetBucketTagging
- s3:オブジェクトバージョンの削除
- s3:バケットバージョンのリスト
- s3:リストバケット
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketバージョン管理
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:バイパスガバナンス保持
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Cloud Volumes ONTAPバックアップにソースボリュームに使用しているものとは異なる AWS アカウントを使用する場合、エージェントは次の API リクエストを実行します。

- s3:PutBucketポリシー
- s3:PutBucketOwnershipControls

分類

エージェントは、NetApp Data Classificationを展開するために次の API 要求を行います。

- ec2:インスタンスの説明
- ec2:インスタンスステータスの説明
- ec2:インスタンスの実行
- ec2:インスタンスの終了

- ec2:タグの作成
- ec2:ボリュームの作成
- ec2:ボリュームのアタッチ
- ec2:セキュリティグループの作成
- ec2:セキュリティグループの削除
- ec2:セキュリティグループの説明
- ec2:ネットワークインターフェースの作成
- ec2:ネットワークインターフェースの説明
- ec2:ネットワークインターフェースの削除
- ec2:サブネットの説明
- ec2:Vpcs の説明
- ec2:スナップショットの作成
- ec2:リージョンの説明
- cloudformation:スタックの作成
- cloudformation:スタックの削除
- cloudformation:スタックの説明
- cloudformation:スタックイベントの説明
- iam:インスタンスプロファイルにロールを追加
- ec2:Iamインスタンスプロファイルの関連付け
- ec2:IamInstanceProfileAssociations の説明

NetApp Data Classificationを使用する場合、エージェントは次の API 要求を行って S3 バケットをスキャンします。

- iam:インスタンスプロファイルにロールを追加
- ec2:Iamインスタンスプロファイルの関連付け
- ec2:IamInstanceProfileAssociations の説明
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:すべてのバケットをリスト
- s3:リストバケット
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3:オブジェクトの削除

- s3:オブジェクトバージョンの削除
- s3:PutObject
- sts:役割を担う

Cloud Volumes ONTAP

エージェントは、AWS でCloud Volumes ONTAP をデプロイおよび管理するために、次の API リクエストを行います。

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
Cloud Volumes ONTAPインスタンスのIAMロールとインスタンスプロファイルを作成および管理します	iam:ListInstanceProfiles	はい	はい	いいえ
	iam:CreateRole	はい	いいえ	いいえ
	iam:DeleteRole	いいえ	はい	はい
	iam:PutRolePolicy	はい	いいえ	いいえ
	iam:インスタンスプロファイルの作成	はい	いいえ	いいえ
	iam:DeleteRolePolicy	いいえ	はい	はい
	iam:インスタンスプロファイルにロールを追加	はい	いいえ	いいえ
	iam:インスタンスプロファイルからロールを削除	いいえ	はい	はい
	iam:インスタンスプロファイルの削除	いいえ	はい	はい
	iam:PassRole	はい	いいえ	いいえ
	ec2:Iamインスタンスプロファイルの関連付け	はい	はい	いいえ
	ec2:IamInstanceProfileAssociations の説明	はい	はい	いいえ
	ec2:IamInstanceProfileの関連付けを解除	いいえ	はい	いいえ
認証ステータスメッセージをデコードする	sts:DecodeAuthorizationMessage	はい	はい	いいえ
アカウントで利用可能な指定されたイメージ（AMI）について説明します	ec2:画像の説明	はい	はい	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
VPC 内のルートテーブルについて説明します（HA ペアの場合のみ必要）	ec2:ルートテーブルの説明	はい	いいえ	いいえ
インスタンスの停止、起動、監視	ec2:インスタンスの開始	はい	はい	いいえ
	ec2:インスタンスの停止	はい	はい	いいえ
	ec2:インスタンスの説明	はい	はい	いいえ
	ec2:インスタンスステータスの説明	はい	はい	いいえ
	ec2:インスタンスの実行	はい	いいえ	いいえ
	ec2:インスタンスの終了	いいえ	いいえ	はい
	ec2:インスタンス属性の変更	いいえ	はい	いいえ
サポートされているインスタンスタイプで拡張ネットワークが有効になっていることを確認します	ec2:インスタンス属性の説明	いいえ	はい	いいえ
メンテナンスとコスト配分に使用される「WorkingEnvironment」および「WorkingEnvironmentId」タグでリソースにタグを付ける	ec2:タグの作成	はい	はい	いいえ
Cloud Volumes ONTAPがバックエンドストレージとして使用するEBSボリュームを管理する	ec2:ボリュームの作成	はい	はい	いいえ
	ec2:ボリュームの説明	はい	はい	はい
	ec2:ボリューム属性の変更	いいえ	はい	はい
	ec2:ボリュームのアタッチ	はい	はい	いいえ
	ec2:ボリュームの削除	いいえ	はい	はい
	ec2:ボリュームのデタッチ	いいえ	はい	はい

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
Cloud Volumes ONTAPのセキュリティ グループの作成と管理	ec2:セキュリティグループの作成	はい	いいえ	いいえ
	ec2:セキュリティグループの削除	いいえ	はい	はい
	ec2:セキュリティグループの説明	はい	はい	はい
	ec2:セキュリティグループの出力を取り消す	はい	いいえ	いいえ
	ec2:セキュリティグループ出力の承認	はい	いいえ	いいえ
	ec2:セキュリティグループイングレスの承認	はい	いいえ	いいえ
	ec2:セキュリティグループの入力を取り消す	はい	はい	いいえ
ターゲットサブネットでCloud Volumes ONTAPのネットワークインターフェースを作成および管理する	ec2:ネットワークインターフェースの作成	はい	いいえ	いいえ
	ec2:ネットワークインターフェースの説明	はい	はい	いいえ
	ec2:ネットワークインターフェースの削除	いいえ	はい	はい
	ec2:ネットワークインターフェース属性の変更	いいえ	はい	いいえ
宛先サブネットとセキュリティグループのリストを取得する	ec2:サブネットの説明	はい	はい	いいえ
	ec2:Vpcs の説明	はい	はい	いいえ
Cloud Volumes ONTAPインスタンスのDNSサーバーとデフォルトのドメイン名を取得します	ec2:Dhcpオプションの説明	はい	いいえ	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
Cloud Volumes ONTAPの EBS ボリュームのスナップショットを作成します	ec2:スナップショットの作成	はい	はい	いいえ
	ec2:スナップショットの削除	いいえ	はい	はい
	ec2:スナップショットの説明	いいえ	はい	いいえ
AutoSupportメッセージに添付されているCloud Volumes ONTAPコンソールをキャプチャします。	ec2:GetConsoleOutput	はい	はい	いいえ
利用可能なキーペアのリストを取得する	ec2:キーペアの説明	はい	いいえ	いいえ
利用可能なAWSリージョンのリストを取得する	ec2:リージョンの説明	はい	はい	いいえ
Cloud Volumes ONTAPインスタンスに関連付けられたリソースのタグを管理する	ec2:タグを削除	いいえ	はい	はい
	ec2:タグの説明	いいえ	はい	いいえ
AWS CloudFormation テンプレートのスタックを作成および管理する	cloudformation:スタックの作成	はい	いいえ	いいえ
	cloudformation:スタックの削除	はい	いいえ	いいえ
	cloudformation:スタックの説明	はい	はい	いいえ
	cloudformation:スタックイベントの説明	はい	いいえ	いいえ
	cloudformation:テンプレートの検証	はい	いいえ	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
Cloud Volumes ONTAPシステムがデータ階層化の容量層として使用するS3 バケットを作成および管理します	s3:バケットの作成	はい	はい	いいえ
	s3:バケットの削除	いいえ	はい	はい
	s3:GetLifecycleConfiguration	いいえ	はい	いいえ
	s3:PutLifecycleConfiguration	いいえ	はい	いいえ
	s3:PutBucketTagging	いいえ	はい	いいえ
	s3:バケットバージョンのリスト	いいえ	はい	いいえ
	s3:GetBucketPolicyStatus	いいえ	はい	いいえ
	s3:GetBucketPublicAccessBlock	いいえ	はい	いいえ
	s3:GetBucketAcl	いいえ	はい	いいえ
	s3:GetBucketPolicy	いいえ	はい	いいえ
	s3:PutBucketパブリックアクセスブロック	いいえ	はい	いいえ
	s3:GetBucketTagging	いいえ	はい	いいえ
	s3:GetBucketLocation	いいえ	はい	いいえ
	s3:すべてのバケットをリスト	いいえ	いいえ	いいえ
	s3:リストバケット	いいえ	はい	いいえ
AWS Key Management Service (KMS) を使用してCloud Volumes ONTAPのデータ暗号化を有効にする	kms:リスト*	はい	はい	いいえ
	kms:再暗号化*	はい	いいえ	いいえ
	kms:説明*	はい	はい	いいえ
	kms:許可の作成	はい	はい	いいえ
	kms:プレーンテキストなしでデータキーを生成する	はい	はい	いいえ
単一の AWS アベイラビリティゾーン内の 2 つの HA ノードとメディエーターの AWS スプレッド配置グループを作成および管理します。	ec2:配置グループの作成	はい	いいえ	いいえ
	ec2:配置グループの削除	いいえ	はい	はい

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
レポートを作成する	fsx:説明*	いいえ	はい	いいえ
	fsx:リスト*	いいえ	はい	いいえ
Amazon EBS エラスティックボリューム機能をサポートするアグリゲートを作成および管理します	ec2:ボリュームの変更の説明	いいえ	はい	いいえ
	ec2:ボリュームの変更	いいえ	はい	いいえ
アベイラビリティゾーンがAWSローカルゾーンであるかどうかを確認し、すべてのデプロイメントパラメータが互換性があるかどうかを検証します。	ec2:アベイラビリティゾーンの説明	はい	いいえ	はい

変更ログ

権限が追加または削除されると、以下のセクションでその旨を記録します。

2024年9月9日

NetApp ConsoleはNetAppエッジ キャッシングと Kubernetes クラスターの検出および管理をサポートしなくなったため、標準リージョンのポリシー #2 から権限が削除されました。

ポリシーから削除された権限を表示する

```
        {
            "Action": [
                "ec2:DescribeRegions",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "iam:GetInstanceProfile"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "K8sServicePolicy"
        },
        {
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudwatch:GetMetricStatistics",
                "cloudformation:ListStacks"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "GFCservicePolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GFCInstance": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
```

2024年5月9日

Cloud Volumes ONTAPには次の権限が必要になりました。

ec2:アベイラビリティゾーンの説明

2023年6月6日

Cloud Volumes ONTAPには次の権限が必要になりました。

kms:プレーンテキストなしでデータキーを生成する

2023年2月14日

NetApp Cloud Tieringには次の権限が必要になりました。

ec2:Vpcエンドポイントの説明

コンソールエージェントの**Azure**権限

NetApp ConsoleがAzure でコンソール エージェントを起動すると、その Azure サブスクリプション内のリソースとプロセスを管理するための権限をエージェントに提供するカスタム ロールが VM にアタッチされます。エージェントは、アクセス許可を使用して、複数の Azure サービスへの API 呼び出しを実行します。

エージェントに対してこのカスタム ロールを作成する必要があるかどうかは、エージェントをどのように展開したかによって異なります。

NetApp Consoleからの導入

コンソールを使用してAzureにエージェント仮想マシンを展開すると、 "システム割り当てマネージドID"仮想マシン上でカスタム ロールを作成し、それを仮想マシンに割り当てます。このロールは、その Azure サブスクリプション内のリソースとプロセスを管理するために必要な権限をコンソールに提供します。エージェントがアップグレードされると、ロールの権限は最新の状態に保たれます。エージェントに対してこのロールを作成したり、更新を管理したりする必要はありません。

手動でのデプロイまたは**Azure Marketplace**からのデプロイ

Azure Marketplace からエージェントをデプロイする場合、または Linux ホストにエージェントを手動でインストールする場合は、カスタム ロールを自分で設定し、変更を加えてそのアクセス許可を維持する必要があります。

以降のリリースで新しい権限が追加されるので、ロールが最新であることを確認する必要があります。新しい権限が必要な場合は、リリース ノートに記載されます。

- これらのポリシーの使用方法の詳細な手順については、次のページを参照してください。
  - "Azure Marketplace のデプロイの権限を設定する"
  - "オンプレミス展開の権限を設定する"
  - "制限モードの権限を設定する"

```
{
    "Name": "Console Operator",
    "Actions": [
                    "Microsoft.Compute/disks/delete",
```

```
                    "Microsoft.Compute/disks/read",
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Compute/locations/operations/read",
                    "Microsoft.Compute/locations/vmSizes/read",
                    "Microsoft.Resources/subscriptions/locations/read",
                    "Microsoft.Compute/operations/read",
                    "Microsoft.Compute/virtualMachines/instanceView/read",
                    "Microsoft.Compute/virtualMachines/powerOff/action",
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/restart/action",
                    "Microsoft.Compute/virtualMachines/deallocate/action",
                    "Microsoft.Compute/virtualMachines/start/action",
                    "Microsoft.Compute/virtualMachines/vmSizes/read",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/images/read",
                    "Microsoft.Network/locations/operationResults/read",
                    "Microsoft.Network/locations/operations/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
                    "Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Resources/deployments/operations/read",
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Resources/deployments/write",
                    "Microsoft.Resources/resources/read",

"Microsoft.Resources/subscriptions/operationresults/read",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
```

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
                    "Microsoft.Storage/checknameavailability/read",
                    "Microsoft.Storage/operations/read",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/read",
                    "Microsoft.Storage/storageAccounts/delete",
                    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/usages/read",
                    "Microsoft.Compute/snapshots/write",
                    "Microsoft.Compute/snapshots/read",
                    "Microsoft.Compute/availabilitySets/write",
                    "Microsoft.Compute/availabilitySets/read",
                    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
                    "Microsoft.Network/loadBalancers/read",
                    "Microsoft.Network/loadBalancers/write",
                    "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
                    "Microsoft.Network/loadBalancers/probes/read",
                    "Microsoft.Network/loadBalancers/probes/join/action",
                    "Microsoft.Authorization/locks/*",
                    "Microsoft.Network/routeTables/join/action",
                    "Microsoft.NetApp/netAppAccounts/read",
                    "Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
                    "Microsoft.Network/privateEndpoints/write",
```

```
"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",

"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
                    "Microsoft.Network/privateEndpoints/read",
                    "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
                    "Microsoft.Network/virtualNetworks/join/action",
                    "Microsoft.Network/privateDnsZones/A/write",
                    "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Insights/Metrics/Read",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Compute/virtualMachines/extensions/delete",
                    "Microsoft.Compute/virtualMachines/extensions/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/networkSecurityGroups/delete",
                    "Microsoft.Resources/deployments/delete",
                    "Microsoft.Compute/diskEncryptionSets/read",
                    "Microsoft.Compute/snapshots/delete",
                    "Microsoft.Network/privateEndpoints/delete",
                    "Microsoft.Compute/availabilitySets/delete",
                    "Microsoft.KeyVault/vaults/read",
                    "Microsoft.KeyVault/vaults/accessPolicies/write",
                    "Microsoft.Compute/diskEncryptionSets/write",
                    "Microsoft.KeyVault/vaults/deploy/action",
                    "Microsoft.Compute/diskEncryptionSets/delete",
                    "Microsoft.Resources/tags/read",
                    "Microsoft.Resources/tags/write",
                    "Microsoft.Resources/tags/delete",
                    "Microsoft.Network/applicationSecurityGroups/write",
                    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",
```

```
                    "Microsoft.Network/applicationSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete",
                    "Microsoft.Synapse/workspaces/write",
                    "Microsoft.Synapse/workspaces/read",
                    "Microsoft.Synapse/workspaces/delete",
                    "Microsoft.Synapse/register/action",
                    "Microsoft.Synapse/checkNameAvailability/action",
                    "Microsoft.Synapse/workspaces/operationStatuses/read",
                    "Microsoft.Synapse/workspaces/firewallRules/read",

"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
                    "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.Compute/images/write",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
                    "Microsoft.Compute/virtualMachineScaleSets/write",
                    "Microsoft.Compute/virtualMachineScaleSets/read",
                    "Microsoft.Compute/virtualMachineScaleSets/delete"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Console Permissions",
    "IsCustom": "true"
}
```

Azure の権限の使用方法

次のセクションでは、各NetAppストレージ システムおよびデータ サービスに対する権限の使用方法について説明します。この情報は、必要な場合にのみ権限を付与するように企業ポリシーで定められている場合に役立ちます。

Azure NetApp Files

NetApp Data Classification を使用してAzure NetApp Filesデータをスキャンすると、エージェントは次の API 要求を行います。

- Microsoft. NetApp/netAppAccounts/read
- Microsoft. NetApp/netAppAccounts/capacityPools/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/delete

NetApp Backup and Recovery

コンソール エージェントは、NetApp Backup and Recoveryに対して次の API 要求を行います。

- Microsoft.Storage/storageAccounts/listkeys/アクション
- Microsoft.Storage/storageAccounts/読み取り
- Microsoft.Storage/ストレージアカウント/書き込み
- Microsoft.Storage/storageAccounts/blobServices/containers/読み取り
- Microsoft.Storage/storageAccounts/listAccountSas/アクション
- Microsoft.KeyVault/vaults/読み取り
- Microsoft.KeyVault/vaults/accessPolicies/書き込み
- Microsoft.Network/ネットワークインターフェイス/読み取り
- Microsoft.Resources/サブスクリプション/場所/読み取り
- Microsoft.Network/仮想ネットワーク/読み取り
- Microsoft.Network/virtualNetworks/サブネット/読み取り
- Microsoft.Resources/サブスクリプション/リソースグループ/読み取り
- Microsoft.Resources/サブスクリプション/リソースグループ/リソース/読み取り
- Microsoft.Resources/サブスクリプション/リソースグループ/書き込み
- Microsoft.Authorization/locks/*
- Microsoft.Network/privateEndpoints/書き込み
- Microsoft.Network/privateEndpoints/読み取り
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/書き込み
- Microsoft.Network/仮想ネットワーク/参加/アクション
- Microsoft.Network/privateDnsZones/A/書き込み
- Microsoft.Network/privateDnsZones/読み取り
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/読み取り
- Microsoft.Network/ネットワークインターフェイス/削除
- Microsoft.Network/ネットワークセキュリティグループ/削除
- Microsoft.Resources/デプロイメント/削除
- Microsoft.ManagedIdentity/userAssignedIdentities/割り当て/アクション

検索と復元機能を使用するとき、エージェントは次の API リクエストを行います。

- Microsoft.Synapse/ワークスペース/書き込み
- Microsoft.Synapse/ワークスペース/読み取り
- Microsoft.Synapse/ワークスペース/削除
- Microsoft.Synapse/登録/アクション

- Microsoft.Synapse/checkNameAvailability/アクション
- Microsoft.Synapse/ワークスペース/操作ステータス/読み取り
- Microsoft.Synapse/ワークスペース/ファイアウォールルール/読み取り
- Microsoft.Synapse/ワークスペース/replaceAllIpFirewallRules/アクション
- Microsoft.Synapse/ワークスペース/操作結果/読み取り
- Microsoft.Synapse/ワークスペース/プライベートエンドポイント接続承認/アクション

NetApp Data Classification

データ分類を使用する場合、エージェントは次の API リクエストを行います。

アクション	セットアップに使用しますか?	日常業務に使用されますか?
Microsoft.Compute/場所/操作/読み取り	はい	はい
Microsoft.Compute/場所/vmSizes/読み取り	はい	はい
Microsoft.Compute/操作/読み取り	はい	はい
Microsoft.Compute/virtualMachines/instanceView/読み取り	はい	はい
Microsoft.Compute/virtualMachines/powerOff/アクション	はい	いいえ
Microsoft.Compute/仮想マシン/読み取り	はい	はい
Microsoft.Compute/virtualMachines/再起動/アクション	はい	いいえ
Microsoft.Compute/virtualMachines/start/action	はい	いいえ
Microsoft.Compute/virtualMachines/vmSizes/読み取り	いいえ	はい
Microsoft.Compute/仮想マシン/書き込み	はい	いいえ
Microsoft.Compute/images/読み取り	はい	はい
Microsoft.Compute/ディスク/削除	はい	いいえ
Microsoft.Compute/ディスク/読み取り	はい	はい
Microsoft.Compute/ディスク/書き込み	はい	いいえ
Microsoft.Storage/checknameavailability/読み取り	はい	はい
Microsoft.Storage/操作/読み取り	はい	はい

アクション	セットアップに使用しますか?	日常業務に使用されますか?
Microsoft.Storage/storageAccounts/listkeys/アクション	はい	いいえ
Microsoft.Storage/storageAccounts/読み取り	はい	はい
Microsoft.Storage/ストレージアカウント/書き込み	はい	いいえ
Microsoft.Storage/storageAccounts/blobServices/containers/読み取り	はい	はい
Microsoft.Network/ネットワークインターフェイス/読み取り	はい	はい
Microsoft.Network/ネットワークインターフェイス/書き込み	はい	いいえ
Microsoft.Network/ネットワークインターフェイス/参加/アクション	はい	いいえ
Microsoft.Network/ネットワークセキュリティグループ/読み取り	はい	はい
Microsoft.Network/ネットワークセキュリティグループ/書き込み	はい	いいえ
Microsoft.Resources/サブスクリプション/場所/読み取り	はい	はい
Microsoft.Network/場所/操作結果/読み取り	はい	はい
Microsoft.Network/場所/操作/読み取り	はい	はい
Microsoft.Network/仮想ネットワーク/読み取り	はい	はい
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/読み取り	はい	はい
Microsoft.Network/virtualNetworks/サブネット/読み取り	はい	はい
Microsoft.Network/virtualNetworks/サブネット/virtualMachines/読み取り	はい	はい
Microsoft.Network/virtualNetworks/virtualMachines/読み取り	はい	はい
Microsoft.Network/virtualNetworks/サブネット/参加/アクション	はい	いいえ
Microsoft.Network/virtualNetworks/サブネット/書き込み	はい	いいえ
Microsoft.Network/routeTables/join/アクション	はい	いいえ

アクション	セットアップに使用しますか?	日常業務に使用されますか?
Microsoft.Resources/デプロイメント/運用/読み取り	はい	はい
Microsoft.Resources/デプロイメント/読み取り	はい	はい
Microsoft.Resources/デプロイメント/書き込み	はい	いいえ
Microsoft.Resources/リソース/読み取り	はい	はい
Microsoft.Resources/サブスクリプション/操作結果/読み取り	はい	はい
Microsoft.Resources/サブスクリプション/リソースグループ/削除	はい	いいえ
Microsoft.Resources/サブスクリプション/リソースグループ/読み取り	はい	はい
Microsoft.Resources/サブスクリプション/リソースグループ/リソース/読み取り	はい	はい
Microsoft.Resources/サブスクリプション/リソースグループ/書き込み	はい	いいえ

Cloud Volumes ONTAP

エージェントは、Azure でCloud Volumes ONTAP をデプロイおよび管理するために、次の API 要求を行います。

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
VMの作成と管理	Microsoft.Compute/場所/操作/読み取り	はい	はい	いいえ
	Microsoft.Compute/場所/vmSizes/読み取り	はい	はい	いいえ
	Microsoft.Resources/サブスクリプション/場所/読み取り	はい	いいえ	いいえ
	Microsoft.Compute/操作/読み取り	はい	はい	いいえ
	Microsoft.Compute/virtualMachines/instanceView/読み取り	はい	はい	いいえ
	Microsoft.Compute/virtualMachines/powerOff/アクション	はい	はい	いいえ
	Microsoft.Compute/仮想マシン/読み取り	はい	はい	いいえ
	Microsoft.Compute/virtualMachines/再起動/アクション	はい	はい	いいえ
	Microsoft.Compute/virtualMachines/start/action	はい	はい	いいえ
	Microsoft.Compute/virtualMachines/割り当て解除/アクション	いいえ	はい	はい
	Microsoft.Compute/virtualMachines/vmSizes/読み取り	いいえ	はい	いいえ
	Microsoft.Compute/仮想マシン/書き込み	はい	はい	いいえ
	Microsoft.Compute/仮想マシン/削除	はい	はい	はい
	Microsoft.Resources/デプロイメント/削除	はい	いいえ	いいえ
VHDからの展開を有効にする	Microsoft.Compute/images/読み取り	はい	いいえ	いいえ
	Microsoft.Compute/images/書き込み	はい	いいえ	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
ターゲットサブネット内のネットワークインターフェースの作成と管理	Microsoft.Network/ネットワークインターフェイス/読み取り	はい	はい	いいえ
	Microsoft.Network/ネットワークインターフェイス/書き込み	はい	はい	いいえ
	Microsoft.Network/ネットワークインターフェイス/参加/アクション	はい	はい	いいえ
	Microsoft.Network/ネットワークインターフェイス/削除	はい	はい	いいえ
ネットワーク セキュリティ グループの作成と管理	Microsoft.Network/ネットワークセキュリティグループ/読み取り	はい	はい	いいえ
	Microsoft.Network/ネットワークセキュリティグループ/書き込み	はい	はい	いいえ
	Microsoft.Network/ネットワークセキュリティグループ/参加/アクション	はい	いいえ	いいえ
	Microsoft.Network/ネットワークセキュリティグループ/削除	いいえ	はい	はい

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
リージョン、ターゲット VNet、サブネットに関するネットワーク情報を取得し、VM を VNet に追加します。	Microsoft.Network/場所/操作結果/読み取り	はい	はい	いいえ
	Microsoft.Network/場所/操作/読み取り	はい	はい	いいえ
	Microsoft.Network/仮想ネットワーク/読み取り	はい	いいえ	いいえ
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/読み取り	はい	いいえ	いいえ
	Microsoft.Network/virtualNetworks/サブネット/読み取り	はい	はい	いいえ
	Microsoft.Network/virtualNetworks/サブネット/virtualMachines/読み取り	はい	はい	いいえ
	Microsoft.Network/virtualNetworks/virtualMachines/読み取り	はい	はい	いいえ
	Microsoft.Network/virtualNetworks/サブネット/参加/アクション	はい	はい	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
リソース グループの作成と管理	Microsoft.Resources/デプロイメント/運用/読み取り	はい	はい	いいえ
	Microsoft.Resources/デプロイメント/読み取り	はい	はい	いいえ
	Microsoft.Resources/デプロイメント/書き込み	はい	はい	いいえ
	Microsoft.Resources/リソース/読み取り	はい	はい	いいえ
	Microsoft.Resources/サブスクリプション/操作結果/読み取り	はい	はい	いいえ
	Microsoft.Resources/サブスクリプション/リソースグループ/削除	はい	はい	はい
	Microsoft.Resources/サブスクリプション/リソースグループ/読み取り	いいえ	はい	いいえ
	Microsoft.Resources/サブスクリプション/リソースグループ/リソース/読み取り	はい	はい	いいえ
	Microsoft.Resources/サブスクリプション/リソースグループ/書き込み	はい	はい	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
Azure ストレージ アカウントとディスクを管理する	Microsoft.Compute/ディスク/読み取り	はい	はい	はい
	Microsoft.Compute/ディスク/書き込み	はい	はい	いいえ
	Microsoft.Compute/ディスク/削除	はい	はい	はい
	Microsoft.Storage/checknameavailability/読み取り	はい	はい	いいえ
	Microsoft.Storage/操作/読み取り	はい	はい	いいえ
	Microsoft.Storage/storageAccounts/listkeys/アクション	はい	はい	いいえ
	Microsoft.Storage/storageAccounts/読み取り	はい	はい	いいえ
	Microsoft.Storage/storageAccounts/削除	いいえ	はい	はい
	Microsoft.Storage/ストレージアカウント/書き込み	はい	はい	いいえ
	Microsoft.Storage/使用状況/読み取り	いいえ	はい	いいえ
BLOB ストレージへのバックアップとストレージ アカウントの暗号化を有効にする	Microsoft.Storage/storageAccounts/blobServices/containers/読み取り	はい	はい	いいえ
	Microsoft.KeyVault/vaults/読み取り	はい	はい	いいえ
	Microsoft.KeyVault/vaults/accessPolicies/書き込み	はい	はい	いいえ
データ階層化のために VNet サービス エンドポイントを有効にする	Microsoft.Network/virtualNetworks/サブネット/書き込み	はい	はい	いいえ
	Microsoft.Network/routeTables/join/アクション	はい	はい	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
Azure 管理スナップショットの作成と管理	Microsoft.Compute/スナップショット/書き込み	はい	はい	いいえ
	Microsoft.Compute/スナップショット/読み取り	はい	はい	いいえ
	Microsoft.Compute/スナップショット/削除	いいえ	はい	はい
	Microsoft.Compute/ディスク/beginGetAccess/アクション	いいえ	はい	いいえ
可用性セットの作成と管理	Microsoft.Compute/availabilitySets/書き込み	はい	いいえ	いいえ
	Microsoft.Compute/availabilitySets/読み取り	はい	いいえ	いいえ
マーケットプレイスからのプログラムによる展開を可能にする	Microsoft.MarketplaceOrdering/オファータイプ/発行者/オファー/プラン/契約/読み取り	はい	いいえ	いいえ
	Microsoft.MarketplaceOrdering/オファータイプ/パブリッシャー/オファー/プラン/契約/書き込み	はい	はい	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
HAペアのロードバランサを管理する	Microsoft.Network/ロードバランサー/読み取り	はい	はい	いいえ
	Microsoft.Network/ロードバランサー/書き込み	はい	いいえ	いいえ
	Microsoft.Network/loadBalancers/削除	いいえ	はい	はい
	Microsoft.Network/loadBalancers/backendAddressPools/読み取り	はい	いいえ	いいえ
	Microsoft.Network/loadBalancers/backendAddressPools/参加/アクション	はい	いいえ	いいえ
	Microsoft.Network/loadBalancers/frontendIPConfigurations/読み取り	はい	はい	いいえ
	Microsoft.Network/loadBalancers/loadBalancingRules/読み取り	はい	いいえ	いいえ
	Microsoft.Network/loadBalancers/プローブ/読み取り	はい	いいえ	いいえ
	Microsoft.Network/loadBalancers/プローブ/参加/アクション	はい	いいえ	いいえ
Azure ディスクのロックの管理を有効にする	Microsoft.Authorization/locks/*	はい	はい	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
サブネット外に接続できない場合にHAペアのプライベートエンドポイントを有効にする	Microsoft.Network/privateEndpoints/書き込み	はい	はい	いいえ
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/アクション	はい	いいえ	いいえ
	Microsoft.Storage/storageAccounts/privateEndpointConnections/読み取り	はい	はい	はい
	Microsoft.Network/privateEndpoints/読み取り	はい	はい	はい
	Microsoft.Network/privateDnsZones/書き込み	はい	はい	いいえ
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/書き込み	はい	はい	いいえ
	Microsoft.Network/仮想ネットワーク/参加/アクション	はい	はい	いいえ
	Microsoft.Network/privateDnsZones/A/書き込み	はい	はい	いいえ
	Microsoft.Network/privateDnsZones/読み取り	はい	はい	いいえ
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/読み取り	はい	はい	いいえ
基盤となる物理ハードウェアに応じて、一部の VM 展開に必要	Microsoft.Resources/デプロイメント/操作ステータス/読み取り	はい	はい	いいえ
デプロイメントの失敗または削除の場合にリソース グループからリソースを削除する	Microsoft.Network/privateEndpoints/削除	はい	はい	いいえ
	Microsoft.Compute/availabilitySets/削除	はい	はい	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
API を使用する際に顧客管理の暗号化キーの使用を有効にする	Microsoft.Compute/diskEncryptionSets/読み取り	はい	はい	はい
	Microsoft.Compute/diskEncryptionSets/書き込み	はい	はい	いいえ
	Microsoft.KeyVault/vaults/deploy/action	はい	いいえ	いいえ
	Microsoft.Compute/diskEncryptionSets/削除	はい	はい	はい
HA ペアのアプリケーション セキュリティ グループを構成して、HA インターコネクトとクラスタ ネットワーク NIC を分離します。	Microsoft.Network/アプリケーションセキュリティグループ/書き込み	いいえ	はい	いいえ
	Microsoft.Network/applicationSecurityGroups/読み取り	いいえ	はい	いいえ
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/アクション	いいえ	はい	いいえ
	Microsoft.Network/ネットワークセキュリティグループ/セキュリティルール/書き込み	はい	はい	いいえ
	Microsoft.Network/applicationSecurityGroups/削除	いいえ	はい	はい
	Microsoft.Network/ネットワークセキュリティグループ/セキュリティルール/削除	いいえ	はい	はい
Cloud Volumes ONTAPリソースに関連付けられたタグの読み取り、書き込み、削除	Microsoft.Resources/タグ/読み取り	いいえ	はい	いいえ
	Microsoft.Resources/タグ/書き込み	はい	はい	いいえ
	Microsoft.Resources/タグ/削除	はい	いいえ	いいえ
作成時にストレージアカウントを暗号化する	Microsoft.ManagedIdentity/userAssignedIdentities/割り当て/アクション	はい	はい	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
Cloud Volumes ONTAPの特定のゾーンを指定するには、柔軟なオーケストレーション モードで仮想マシン スケール セットを使用します。	Microsoft.Compute/仮想マシンスケールセット/書き込み	はい	いいえ	いいえ
	Microsoft.Compute/仮想マシンスケールセット/読み取り	はい	いいえ	いいえ
	Microsoft.Compute/virtualMachineScaleSets/削除	いいえ	いいえ	はい

階層化

NetApp Cloud Tieringをセットアップすると、エージェントは次の API 要求を行います。

- Microsoft.Storage/storageAccounts/listkeys/アクション
- Microsoft.Resources/サブスクリプション/リソースグループ/読み取り
- Microsoft.Resources/サブスクリプション/場所/読み取り

コンソール エージェントは、日常の操作のために次の API 要求を行います。

- Microsoft.Storage/storageAccounts/blobServices/containers/読み取り
- Microsoft.Storage/storageAccounts/managementPolicies/読み取り
- Microsoft.Storage/storageAccounts/managementPolicies/書き込み
- Microsoft.Storage/storageAccounts/読み取り

変更ログ

権限が追加または削除されると、以下のセクションでその旨を記録します。

2024年9月9日

コンソールでは Kubernetes クラスターの検出と管理がサポートされなくなったため、次の権限が JSON ポリシーから削除されました。

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/アクション
- Microsoft.ContainerService/managedClusters/読み取り

2024年8月22日

仮想マシン スケール セットのCloud Volumes ONTAPサポートに必要なため、次の権限が JSON ポリシーに追加されました。

- Microsoft.Compute/仮想マシンスケールセット/書き込み
- Microsoft.Compute/仮想マシンスケールセット/読み取り
- Microsoft.Compute/virtualMachineScaleSets/削除

2023年12月5日

ボリューム データを Azure Blob ストレージにバックアップする場合、 NetApp Backup and Recoveryでは次の権限は不要になりました。

- Microsoft.Compute/仮想マシン/読み取り
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/割り当て解除/アクション
- Microsoft.Compute/virtualMachines/拡張機能/削除
- Microsoft.Compute/仮想マシン/削除

これらの権限は他のコンソール ストレージ サービスに必要なので、他のストレージ サービスを使用している場合は、エージェントのカスタム ロールに引き続き残ります。

2023年5月12日

Cloud Volumes ONTAP管理に必要なため、次の権限が JSON ポリシーに追加されました。

- Microsoft.Compute/images/書き込み
- Microsoft.Network/loadBalancers/frontendIPConfigurations/読み取り

次の権限は不要になったため、JSON ポリシーから削除されました。

- Microsoft.Storage/storageAccounts/blobServices/コンテナー/書き込み
- Microsoft.Network/publicIPAddresses/削除

2023年3月23日

データ分類には「Microsoft.Storage/storageAccounts/delete」アクセス許可は不要になりました。

この権限は、Cloud Volumes ONTAPでも必要です。

2023年1月5日

次の権限が JSON ポリシーに追加されました。

- Microsoft.Storage/storageAccounts/listAccountSas/アクション
- Microsoft.Synapse/ワークスペース/プライベートエンドポイント接続承認/アクション

  これらの権限は、NetApp Backup and Recoveryに必要です。

- Microsoft.Network/loadBalancers/backendAddressPools/参加/アクション

  この権限は、Cloud Volumes ONTAP のデプロイメントに必要です。

コンソール エージェントの **Google Cloud** 権限

NetApp Consoleには、Google Cloud でアクションを実行するための権限が必要です。

これらの権限は、 NetAppが提供するカスタム ロールに含まれています。エージェントがこれらの権限を使用して何を行うかを理解する必要があります。

サービスアカウントの権限

以下に示すカスタムロールは、コンソール エージェントが Google Cloud ネットワーク内のリソースとプロセスを管理するために必要な権限を提供します。

このカスタム ロールを、コンソール エージェント VM に接続されるサービス アカウントに適用する必要があります。

- "標準モードの Google Cloud 権限を設定する"
- "制限モードの権限を設定する"

また、後続のリリースで新しい権限が追加された場合、ロールが最新であることを確認する必要があります。新しい権限が必要な場合は、リリース ノートに記載されます。

```
title: NetApp Console agent
description: Permissions for the service account associated with the
Console agent instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
```

```
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.instanceGroups.get
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
```

```
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
```

Google Cloud の権限の使用方法

アクション	目的
- compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	Cloud Volumes ONTAPのディスクを作成および管理します。
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Cloud Volumes ONTAPのファイアウォール ルールを作成します。
- compute.globalOperations.get	操作のステータスを取得します。
- compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	VM インスタンスのイメージを取得します。
- compute.instances.attachDisk - compute.instances.detachDisk	Cloud Volumes ONTAPにディスクを接続および切断します。

アクション	目的
- compute.instances.create - compute.instances.delete	Cloud Volumes ONTAP VMインスタンスを作成および削除します。
- compute.instances.get	VM インスタンスを一覧表示します。
- compute.instances.getSerialPortOutput	コンソールログを取得します。
- compute.instances.list	ゾーン内のインスタンスのリストを取得します。
- compute.instances.setDeletionProtection	インスタンスに削除保護を設定します。
- compute.instances.setLabels	ラベルを追加します。
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	Cloud Volumes ONTAPのマシンタイプを変更します。
- compute.instances.setMetadata	メタデータを追加します。
- compute.instances.setTags	ファイアウォール ルールのタグを追加します。
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Cloud Volumes ONTAP を起動および停止します。
- compute.machineTypes.get	クォータをチェックするためのコア数を取得します。
- compute.projects.get	複数のプロジェクトをサポートします。
- compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels	永続ディスクのスナップショットを作成および管理します。
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - compute.zoneOperations.get - compute.zones.get - compute.zones.list	新しいCloud Volumes ONTAP仮想マシンインスタンスを作成するために必要なネットワーク情報を取得します。
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifests.list - deploymentmanager.operations.get - deploymentmanager.operations.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.types.get - deploymentmanager.types.list	Google Cloud Deployment Manager を使用してCloud Volumes ONTAP仮想マシン インスタンスをデプロイします。
- logging.logEntries.list - logging.privateLogEntries.list	スタック ログ ドライブを取得します。
- リソースマネージャー.プロジェクト.取得	複数のプロジェクトをサポートします。

アクション	目的
- ストレージバケットの作成 - ストレージバケットの削除 - ストレージバケットの取得 - ストレージバケットの一覧表示 - ストレージバケットの更新	データ階層化用の Google Cloud Storage バケットを作成および管理します。
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyRings.list	Cloud Volumes ONTAPで Cloud Key Management Service の顧客管理暗号化キーを使用する。
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects.get - storage.objects.list	Cloud Volumes ONTAPインスタンスにサービス アカウントを設定します。このサービス アカウントは、Google Cloud Storage バケットへのデータ階層化の権限を付与します。
- アドレスリストを計算する	HA ペアを展開するときにリージョン内のアドレスを取得します。
- compute.backendServices.create - compute.regionBackendServices.create - compute.regionBackendServices.get - compute.regionBackendServices.list	HA ペアでトラフィックを分散するためのバックエンド サービスを設定します。
- compute.networks.updatePolicy	HA ペアの VPC とサブネットにファイアウォール ルールを適用します。
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	NetApp Data Classification を有効にします。
- compute.instanceGroups.get - compute.addresses.get - compute.instances.updateNetworkInterface	Cloud Volumes ONTAP HA ペアでストレージ VM を作成および管理します。
- 監視.timeSeries.リスト - ストレージ.バケット.getIamPolicy	Google Cloud Storage バケットに関する情報を検出します。
- cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.getIamPolicy - cloudkms.cryptoKeys.list - cloudkms.cryptoKeys.setIamPolicy - cloudkms.keyRings.get - cloudkms.keyRings.getIamPolicy - cloudkms.keyRings.list - cloudkms.keyRings.setIamPolicy	デフォルトの Google 管理暗号化キーを使用する代わりに、 NetApp Backup and Recoveryアクティベーション ウィザードで独自の顧客管理キーを選択します。

変更ログ

権限が追加または削除されると、以下のセクションでその旨を記録します。

2023/02/06

このポリシーに次の権限が追加されました:

- compute.instances.updateNetworkInterface

この権限はCloud Volumes ONTAPに必要です。

2023/01/27

次の権限がポリシーに追加されました:

- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

これらの権限は、NetApp Backup and Recoveryに必要です。

ポート

AWS のコンソールエージェントのセキュリティグループルール

エージェントの AWS セキュリティグループには、インバウンドルールとアウトバウンドルールの両方が必要です。 NetApp Consoleは、コンソールからコンソール エージェントを作成すると、このセキュリティ グループを自動的に作成します。他のすべてのインストール オプションに対して、このセキュリティ グループを設定する必要があります。

インバウンドルール

プロトコル	ポート	目的
SSH	22	エージェントホストへのSSHアクセスを提供します
HTTP	80	• クライアントのWebブラウザからローカルユーザーインターフェースへのHTTPアクセスを提供します • Cloud Volumes ONTAPのアップグレードプロセス中に使用されます
HTTPS	443	ローカル ユーザー インターフェイスへの HTTPS アクセスとNetApp Data Classificationインスタンスからの接続を提供します。
TCP	3128	Cloud Volumes ONTAPにインターネット アクセスを提供します。デプロイ後にこのポートを手動で開く必要があります。

アウトバウンドルール

エージェントの定義済みセキュリティ グループは、すべての送信トラフィックを開きます。それが許容できる場合は、基本的な送信ルールに従ってください。より厳格なルールが必要な場合は、高度な送信ルールを使用します。

基本的なアウトバウンドルール

エージェントの定義済みセキュリティ グループには、次の送信ルールが含まれています。

プロトコル	ポート	目的
すべてのTCP	全て	すべての送信トラフィック
すべてUDP	全て	すべての送信トラフィック

高度なアウトバウンドルール

送信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、エージェントによる送信通信に必要なポートのみを開くことができます。

送信元 IP アドレスはエージェント ホストです。

サービス	プロトコル	ポート	デスティネーション	目的
API呼び出しとAutoSupport	HTTPS	443	アウトバウンドインターネットとONTAPクラスタ管理 LIF	AWS、 ONTAP、NetApp Data ClassificationへのAPI呼び出し、およびNetAppへのAutoSupportメッセージの送信
API呼び出し	TCP	3000	ONTAP HAメディエーター	ONTAP HAメディエーターとの通信
	TCP	8080	データ分類	デプロイメント中にデータ分類インスタンスにプローブする
DNS	UDP	53	DNS	コンソールによるDNS解決に使用

Azure のコンソール エージェント セキュリティ グループ ルール

エージェントの Azure セキュリティ グループには、受信規則と送信規則の両方が必要です。 NetApp Consoleは、コンソールからコンソール エージェントを作成すると、このセキュリティ グループを自動的に作成します。その他のインストール オプションについては、このセキュリティ グループを手動で設定する必要があります。

インバウンドルール

プロトコル	ポート	目的
SSH	22	エージェントホストへのSSHアクセスを提供します

プロトコル	ポート	目的
HTTP	80	• クライアントのWebブラウザからローカルユーザーインターフェースへのHTTPアクセスを提供します • Cloud Volumes ONTAPのアップグレードプロセス中に使用されます
HTTPS	443	クライアントのWebブラウザからローカルユーザーインターフェースへのHTTPSアクセスと、 NetApp Data Classificationインスタンスからの接続を提供します。
TCP	3128	Cloud Volumes ONTAPにインターネット アクセスを提供し、AutoSupportメッセージをNetAppサポートに送信します。デプロイ後にこのポートを手動で開く必要があります。 "エージェントがAutoSupportメッセージのプロキシとしてどのように使用されるかを学びます"

アウトバウンドルール

エージェントの定義済みセキュリティ グループは、すべての送信トラフィックを開きます。それが許容できる場合は、基本的な送信ルールに従ってください。より厳格なルールが必要な場合は、高度な送信ルールを使用します。

基本的なアウトバウンドルール

エージェントの定義済みセキュリティ グループには、次の送信ルールが含まれています。

プロトコル	ポート	目的
すべてのTCP	全て	すべての送信トラフィック
すべてUDP	全て	すべての送信トラフィック

高度なアウトバウンドルール

送信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、エージェントによる送信通信に必要なポートのみを開くことができます。

送信元 IP アドレスはエージェント ホストです。

サービス	プロトコル	ポート	デスティネーション	目的
API呼び出しとAutoSupport	HTTPS	443	アウトバウンドインターネットとONTAPクラスタ管理 LIF	Azure、 ONTAP、NetApp Data ClassificationへのAPI呼び出し、およびNetAppへのAutoSupportメッセージの送信
API呼び出し	TCP	8080	データ分類	デプロイメント中にデータ分類インスタンスにプローブする
DNS	UDP	53	DNS	コンソールによるDNS解決に使用

Google Cloud のエージェント ファイアウォール ルール

エージェントの Google Cloud ファイアウォール ルールには、受信ルールと送信ルールの両方が必要です。 NetApp Consoleからコンソール エージェントを作成すると、このセキュリティ グループが自動的に作成されます。その他のインストール オプションの場合は、このセキュリティ グループを手動で設定する必要があります。

インバウンドルール

プロトコル	ポート	目的
SSH	22	エージェントホストへのSSHアクセスを提供します
HTTP	80	• クライアントのWebブラウザからローカルユーザーインターフェースへのHTTPアクセスを提供します • Cloud Volumes ONTAPのアップグレードプロセス中に使用されます
HTTPS	443	クライアントのWebブラウザからローカルユーザーインターフェースへのHTTPSアクセスを提供します
TCP	3128	Cloud Volumes ONTAPにインターネット アクセスを提供します。デプロイ後にこのポートを手動で開く必要があります。

アウトバウンドルール

エージェントの事前定義されたファイアウォール ルールにより、すべての送信トラフィックが開かれます。許容できる場合は基本的な送信ルールに従います。より厳しい要件の場合は、高度な送信ルールを使用します。

基本的なアウトバウンドルール

エージェントの定義済みファイアウォール ルールには、次の送信ルールが含まれます。

プロトコル	ポート	目的
すべてのTCP	全て	すべての送信トラフィック
すべてUDP	全て	すべての送信トラフィック

高度なアウトバウンドルール

送信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、エージェントによる送信通信に必要なポートのみを開くことができます。

送信元 IP アドレスはエージェント ホストです。

サービス	プロトコル	ポート	デスティネーション	目的
API呼び出しとAutoSupport	HTTPS	443	アウトバウンドインターネットとONTAPクラスタ管理 LIF	Google Cloud、ONTAP、 NetApp Data ClassificationへのAPI呼び出し、およびNetAppへのAutoSupportメッセージの送信
API呼び出し	TCP	8080	データ分類	デプロイメント中にデータ分類インスタンスにプローブする
DNS	UDP	53	DNS	データ分類によるDNS解決に使用される

オンプレミスのコンソールエージェントのポート

コンソール エージェントは、オンプレミスの Linux ホストに手動でインストールされる場合、受信 ポートを使用します。計画の際にはこれらのポートを参照してください。

これらの受信ルールは、すべてのNetApp Console展開モードに適用されます。

プロトコル	ポート	目的
HTTP	80	• クライアントのWebブラウザからローカルユーザーインターフェースへのHTTPアクセスを提供します • Cloud Volumes ONTAPのアップグレードプロセス中に使用されます
HTTPS	443	クライアントのWebブラウザからローカルユーザーインターフェースへのHTTPSアクセスを提供します

3.9.55 以前に必要なネットワーク アクセス ポイント

このトピックでは、 NetApp Console4.0.0 リリースより前のバージョンのNetApp

Consoleコンソール標準モード、 NetApp Consoleエージェント、およびNetAppデータ サービスのアウトバウンド インターネット アクセス、および必要なエンドポイントに接続する機能に必要なネットワーク アクセスについて詳しく説明します。コンソールとインストールするエージェントに、機能プロパティへの適切なネットワーク アクセスがあることを確認する必要があります。

NetApp Consoleに SaaS (Software as a Service) としてアクセスするコンピューターと、オンプレミスまたはクラウドにインストールするコンソール エージェントのネットワーク アクセスを設定する必要があります。Cloud Volumes ONTAPなどの特定のNetAppデータ サービスには追加のエンドポイントが必要になる場合もあります。

エンドポイント リストを **4.0.0** 以降の改訂リストに更新します。

バージョン 4.0.0 以降、コンソール エージェントに必要なエンドポイントが少なくなります。 4.0.0 より前の既存のデプロイメントは引き続きサポートされます。 4.0.0 以降にアップグレードした後、都合の良いときに古いエンドポイントを許可リストから削除できます。

NetApp、改訂されたエンドポイント リストを使用するようにファイアウォール ルールを更新することをお勧めします。改訂されたリストは小さくなったため、より安全になり、管理も容易になりました。

レビュー"4.0.0以降でサポートされているエンドポイント"

手順

1. エンドポイントをホワイトリストに登録する"4.0.0 以降でサポートされているエンドポイント"。
2. 次のコマンドを実行して、各エージェントのサービス マネージャー 2 サービスを再起動します。

```
systemctl restart netapp-service-manager.service
```

3. 次のコマンドを実行し、エージェントのステータスが *active(running)* と表示されていることを確認します: _

```
systemctl status netapp-service-manager.service
```

4. 許可リストから古いエンドポイントを削除します。

NetApp Consoleが接続するエンドポイント

NetApp Consoleにアクセスする各コンピューターは、以下にリストされているエンドポイントに接続されている必要があります。

システムは、次の 2 つのシナリオでこれらのエンドポイントに接続します。

- アクセスしているコンピュータから "NetApp Console"サービスとしてのソフトウェア (SaaS) として。
- エージェント ホストに直接アクセスするコンピュータから、ログインして設定するか、エージェント ホストからコンソールにアクセスします。

エンドポイント	目的
https://support.netapp.com https://mysupport.netapp.com	ライセンス情報を取得し、 AutoSupportメッセージをNetAppサポートに送信します。
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com	NetApp Console内で機能とサービスを提供します。
次の 2 つのエンドポイント セットから選択します。 • オプション1（推奨） https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • オプション2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 NetApp、ランサムウェア耐性またはバックアップとリカバリを使用していない限り、より安全なオプション 1 のエンドポイントをファイアウォールで許可し、オプション 2 のエンドポイントを禁止することを推奨しています。これらのエンドポイントについては、次の点に注意してください。 • オプション 1 エンドポイントは 3.9.47 以降でサポートされます。 3.9.47 より前のリリースでは下位互換性がサポートされていません。 • コンソール エージェントは、まずオプション 2 のエンドポイントとの接続を開始します。これらのエンドポイントにアクセスできない場合は、オプション 1 のエンドポイントに自動的に接続します。 • コンソール エージェントをNetApp Backup and Recoveryまたは Ransomware Resilience と併用する場合、システムはオプション 1 のエンドポイントをサポートしません。オプション 2 のエンドポイントを許可し、オプション 1 を禁止します。

コンソールエージェントが接続するエンドポイント

コンソール エージェントをオンプレミスまたはクラウドにインストールし、エンドポイントに接続してコンソールによって開始されたアクションを完了します。

コンソール エージェントは、 NetApp Consoleと同じエンドポイントにアクセスできる必要があります。また、エージェントをクラウド プロバイダーに導入する場合は追加のエンドポイントにもアクセスできる必要があります。

AWS のエージェントエンドポイント

これらのエンドポイントは、4.0.0 より前のコンソール エージェントに適用されます。

エンドポイント	目的
AWS サービス (amazonaws.com): CloudFormation Elastic Compute Cloud (EC2) Identity and Access Management (IAM) Key Management Service (KMS) Security Token Service (STS) Simple Storage Service (S3)	AWS 内のリソースを管理します。正確なエンドポイントは、使用している AWS リージョンによって異なります。ライセンス情報を取得し、 AutoSupportメッセージをNetAppサポートに送信する方法については、AWS のドキュメントを参照してください。
https://support.netapp.com https://mysupport.netapp.com	ライセンス情報を取得し、 AutoSupportメッセージをNetAppサポートに送信します。
次の 2 つのエンドポイント セットから選択します。 • オプション1（推奨） https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • オプション2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 NetApp、ランサムウェア耐性またはバックアップとリカバリを使用していない限り、より安全なオプション 1 のエンドポイントをファイアウォールで許可し、オプション 2 のエンドポイントを禁止することを推奨しています。これらのエンドポイントについては、次の点に注意してください。 • オプション 1 エンドポイントは 3.9.47 以降でサポートされます。 3.9.47 より前のリリースでは下位互換性がサポートされていません。 • コンソール エージェントは、まずオプション 2 のエンドポイントとの接続を開始します。これらのエンドポイントにアクセスできない場合は、オプション 1 のエンドポイントに自動的に接続します。 • コンソール エージェントをNetApp Backup and Recoveryまたは Ransomware Resilience と併用する場合、システムはオプション 1 のエンドポイントをサポートしません。オプション 2 のエンドポイントを許可し、オプション 1 を禁止します。

Azureのエージェントエンドポイント

これらのエンドポイントは、4.0.0 より前のコンソール エージェントに適用されます。

エンドポイント	目的
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Azure パブリック リージョン内のリソースを管理します。
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Azure China リージョンのリソースを管理します。
https://support.netapp.com https://mysupport.netapp.com	ライセンス情報を取得し、 AutoSupportメッセージをNetAppサポートに送信します。

エンドポイント	目的
次の 2 つのエンドポイント セットから選択します。 • オプション1（推奨） https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • オプション2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 NetApp、ランサムウェア耐性またはバックアップとリカバリを使用していない限り、より安全なオプション 1 のエンドポイントをファイアウォールで許可し、オプション 2 のエンドポイントを禁止することを推奨しています。これらのエンドポイントについては、次の点に注意してください。 • オプション 1 エンドポイントは 3.9.47 以降でサポートされます。 3.9.47 より前のリリースでは下位互換性がサポートされていません。 • コンソール エージェントは、まずオプション 2 のエンドポイントとの接続を開始します。これらのエンドポイントにアクセスできない場合は、オプション 1 のエンドポイントに自動的に接続します。 • コンソール エージェントをNetApp Backup and Recoveryまたは Ransomware Resilience と併用する場合、システムはオプション 1 のエンドポイントをサポートしません。オプション 2 のエンドポイントを許可し、オプション 1 を禁止します。

Google Cloud のエージェント エンドポイント

これらのエンドポイントは、4.0.0 より前のコンソール エージェントに適用されます。

エンドポイント	目的
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/project	Google Cloud 内のリソースを管理します。
https://support.netapp.com https://mysupport.netapp.com	ライセンス情報を取得し、 AutoSupportメッセージをNetAppサポートに送信します。

エンドポイント	目的
次の 2 つのエンドポイント セットから選択します。 • オプション1（推奨） https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • オプション2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 NetApp、より安全なオプション 1 のエンドポイントをファイアウォールで許可し、オプション 2 のエンドポイントを禁止することを推奨しています。これらのエンドポイントについては、次の点に注意してください。 • コンソール エージェントの 3.9.47 リリース以降、システムはオプション 1 にリストされているエンドポイントをサポートします。コンソール エージェントの以前のリリースでは、下位互換性はサポートされていません。 • コンソール エージェントは、最初にオプション 2 のエンドポイントに接続します。これらのエンドポイントにアクセスできない場合は、オプション 1 のエンドポイントに自動的に接続します。 • コンソール エージェントをNetApp Backup and Recoveryまたは Ransomware Resilience と併用する場合、システムはオプション 1 のエンドポイントをサポートしません。オプション 2 のエンドポイントを許可し、オプション 1 を禁止します。

オンプレミスのエージェントエンドポイント

エンドポイント	目的
https://support.netapp.com https://mysupport.netapp.com	ライセンス情報を取得し、 AutoSupportメッセージをNetAppサポートに送信します。
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
次の 2 つのエンドポイント セットから選択します。 • オプション1（推奨） https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • オプション2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 NetApp、ランサムウェア耐性またはバックアップとリカバリを使用していない限り、より安全なオプション 1 のエンドポイントをファイアウォールで許可し、オプション 2 のエンドポイントを禁止することを推奨しています。これらのエンドポイントについては、次の点に注意してください。 • オプション 1 エンドポイントは 3.9.47 以降でサポートされます。 3.9.47 より前のリリースでは下位互換性がサポートされていません。 • コンソール エージェントは、まずオプション 2 のエンドポイントとの接続を開始します。これらのエンドポイントにアクセスできない場合は、オプション 1 のエンドポイントに自動的に接続します。 • コンソール エージェントをNetApp Backup and Recoveryまたは Ransomware Resilience と併用する場合、システムはオプション 1 のエンドポイントをサポートしません。オプション 2 のエンドポイントを許可し、オプション 1 を禁止します。

知識とサポート

サポートに登録する

NetApp Consoleとそのストレージ ソリューションおよびデータ サービスに固有のテクニカル サポートを受けるには、サポート登録が必要です。 Cloud Volumes ONTAPシステムの主要なワークフローを有効にするには、サポート登録も必要です。

サポートに登録しても、クラウド プロバイダー ファイル サービスに対するNetAppサポートは有効になりません。クラウド プロバイダーのファイル サービス、そのインフラストラクチャ、またはサービスを使用するソリューションに関連するテクニカル サポートについては、その製品のドキュメントの「ヘルプの取得」を参照してください。

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

サポート登録の概要

サポート資格を有効にするには、次の 2 つの登録形式があります。

- NetApp Consoleアカウントのシリアル番号 (コンソールの [サポート リソース] ページにある 20 桁の 960xxxxxxxxx シリアル番号) を登録します。

  これは、コンソール内のすべてのサービスに対する単一のサポート サブスクリプション ID として機能します。各コンソール アカウントを登録する必要があります。

- クラウド プロバイダーのマーケットプレイスで、サブスクリプションに関連付けられたCloud Volumes ONTAPシリアル番号を登録します (これらは 20 桁の 909201xxxxxxxx シリアル番号です)。

  これらのシリアル番号は一般に *PAYGO* シリアル番号 と呼ばれ、 Cloud Volumes ONTAP の導入時にNetApp Consoleによって生成されます。

両方のタイプのシリアル番号を登録すると、サポート チケットの開設やケースの自動生成などの機能が有効になります。登録は、以下の説明に従ってNetAppサポート サイト (NSS) アカウントをコンソールに追加することで完了します。

NetAppサポートのためにNetApp Consoleを登録する

サポートに登録し、サポート資格を有効にするには、 NetApp Consoleアカウントの 1 人のユーザーがNetAppサポート サイト アカウントをコンソール ログインに関連付ける必要があります。 NetAppサポートに登録する方法は、 NetAppサポート サイト (NSS) アカウントをすでにお持ちかどうかによって異なります。

NSSアカウントをお持ちの既存顧客

NSS アカウントをお持ちのNetApp のお客様の場合は、コンソールからサポートに登録するだけです。

手順

1. 管理 > *資格情報*を選択します。
2. *ユーザー資格情報*を選択します。
3. **NSS** 資格情報の追加 を選択し、 NetAppサポート サイト (NSS) の認証プロンプトに従います。
4. 登録プロセスが成功したことを確認するには、[ヘルプ] アイコンを選択し、[サポート] を選択します。

   リソース ページには、コンソール アカウントがサポートに登録されていることが表示されます。

   他のコンソール ユーザーは、ログインにNetAppサポート サイト アカウントを関連づけていない場合、同じサポート登録ステータスを表示しないことに注意してください。ただし、これはあなたのアカウントがサポートに登録されていないことを意味するものではありません。組織内の 1 人のユーザーがこれらの手順を実行していれば、アカウントは登録済みになります。

既存の顧客だが**NSS**アカウントがない

既存のNetApp顧客であり、既存のライセンスとシリアル番号を持っているものの、NSS アカウントを持っていない場合は、NSS アカウントを作成し、それをコンソール ログインに関連付ける必要があります。

手順

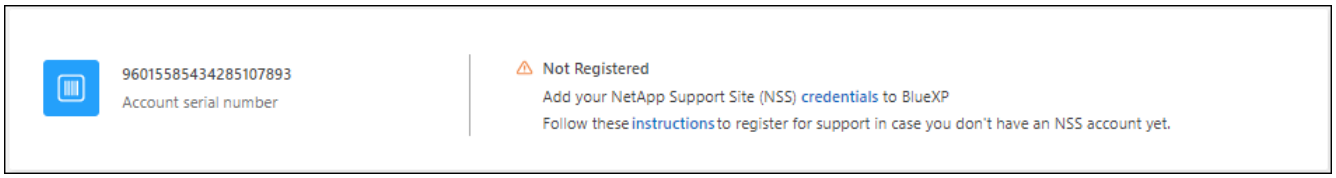
1. NetAppサポートサイトのアカウントを作成するには、 "NetAppサポートサイト ユーザー登録フォーム"
   a. 適切なユーザー レベル (通常は * NetApp顧客/エンド ユーザー*) を選択してください。
   b. 上記で使用したコンソール アカウントのシリアル番号 (960xxxx) を必ずシリアル番号フィールドにコピーしてください。これにより、アカウント処理が高速化されます。
2. 以下の手順を実行して、新しいNSSアカウントをコンソールログインに関連付けます。NSSアカウントをお持ちの既存顧客 。

NetAppの新着情報

NetAppを初めて使用し、NSS アカウントをお持ちでない場合は、以下の手順に従ってください。

手順

1. コンソールの右上にあるヘルプ アイコンを選択し、サポート を選択します。
2. サポート登録ページからアカウント ID シリアル番号を見つけます。



3. 移動先 "NetAppのサポート登録サイト"私は登録済みの**NetApp**顧客ではありません を選択します。
4. 必須フィールド（赤いアスタリスクが付いているフィールド）に入力します。
5. 製品ライン フィールドで、**Cloud Manager** を選択し、該当する請求プロバイダーを選択します。
6. 上記の手順 2 からアカウントのシリアル番号をコピーし、セキュリティ チェックを完了して、NetApp のグローバル データ プライバシー ポリシーを読んだことを確認します。

   この安全な取引を完了するために、指定されたメールボックスに電子メールが直ちに送信されます。検証

メールが数分以内に届かない場合は、必ずスパム フォルダーを確認してください。

7. メール内からアクションを確認します。

   確認すると、リクエストがNetAppに送信され、 NetAppサポート サイトのアカウントを作成することが推奨されます。

8. NetAppサポートサイトのアカウントを作成するには、 "NetAppサポートサイト ユーザー登録フォーム"
   a. 適切なユーザー レベル (通常は * NetApp顧客/エンド ユーザー*) を選択してください。
   b. 上記で使用したアカウントのシリアル番号 (960xxxx) を必ずシリアル番号フィールドにコピーしてください。これにより処理速度が向上します。

終了後の操作

このプロセス中に、 NetAppから連絡が来るはずです。これは、新規ユーザー向けの 1 回限りのオンボーディング演習です。

NetAppサポートサイトのアカウントを取得したら、以下の手順を実行して、アカウントをコンソールログインに関連付けます。NSSアカウントをお持ちの既存顧客 。

Cloud Volumes ONTAPサポートに NSS 認証情報を関連付ける

Cloud Volumes ONTAPの次の主要なワークフローを有効にするには、 NetAppサポート サイトの認証情報をコンソール アカウントに関連付ける必要があります。

- 従量課金制のCloud Volumes ONTAPシステムをサポート対象として登録する

  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。

- 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。

- 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

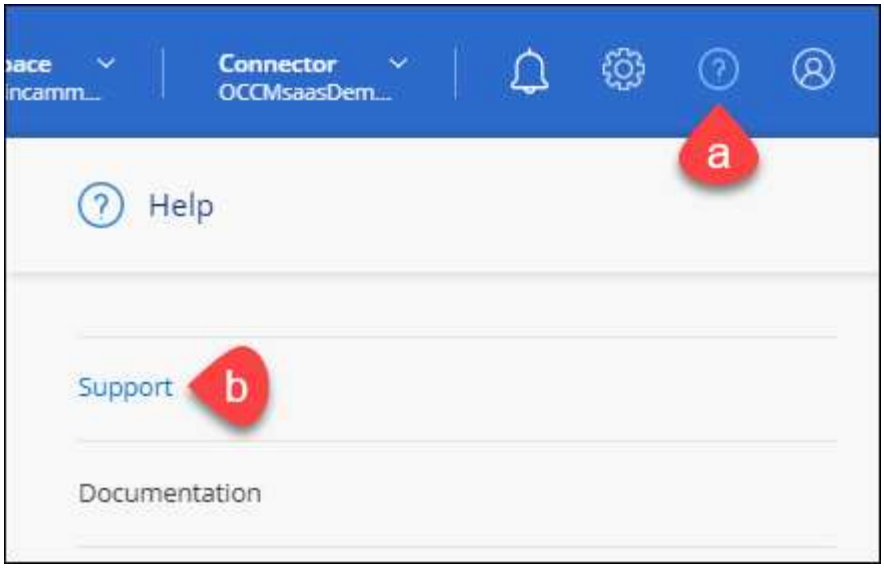
NSS 資格情報をNetApp Consoleアカウントに関連付けることは、コンソール ユーザー ログインに関連付けられている NSS アカウントとは異なります。

これらの NSS 資格情報は、特定のコンソール アカウント ID に関連付けられています。コンソール組織に属するユーザーは、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。

- 顧客レベルのアカウントをお持ちの場合は、1 つ以上の NSS アカウントを追加できます。
- パートナー アカウントまたは再販業者アカウントをお持ちの場合は、1 つ以上の NSS アカウントを追加できますが、顧客レベルのアカウントと一緒に追加することはできません。

手順

1. コンソールの右上にあるヘルプ アイコンを選択し、サポート を選択します。



2. *NSS管理 > NSSアカウントの追加*を選択します。
3. 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。

4. 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て、認証プロセスを実行します。

   これらのアクションにより、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 NSS アカウントを使用できるようになります。

   次の点に注意してください。

   - NSS アカウントは顧客レベルのアカウントである必要があります (ゲスト アカウントや一時アカウントではありません)。顧客レベルの NSS アカウントを複数持つことができます。
   - パートナー レベルのアカウントの場合、NSS アカウントは 1 つだけ存在できます。顧客レベルの NSS アカウントを追加しようとしたときに、パートナー レベルのアカウントが存在する場合は、次のエラー メッセージが表示されます。

     「異なるタイプの NSS ユーザーがすでに存在するため、このアカウントでは NSS 顧客タイプは許可されません。」

   既存の顧客レベルの NSS アカウントがあり、パートナー レベルのアカウントを追加しようとする場合も同様です。

   - 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。

ヘルプを受ける

NetApp は、 NetApp Consoleとそのクラウド サービスをさまざまな方法でサポートします。ナレッジ ベース (KB) 記事やコミュニティ フォーラムなど、豊富な無料のセルフ サポート オプションが 24 時間 365 日ご利用いただけます。サポート登録には、Webチケットによるリモートテクニカルサポートも含まれます。

クラウドプロバイダーのファイルサービスのサポートを受ける

クラウド プロバイダーのファイル サービス、そのインフラストラクチャ、またはサービスを使用するソリューションに関連するテクニカル サポートについては、その製品のドキュメントを参照してください。

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

NetAppとそのストレージ ソリューションおよびデータ サービスに固有のテクニカル サポートを受けるには、以下に説明するサポート オプションを使用してください。

セルフサポートオプションを使用する

以下のオプションは、24 時間 365 日無料でご利用いただけます。

- ドキュメント

  現在表示しているNetApp Consoleのドキュメント。

- "ナレッジベース"

  NetAppナレッジベースを検索して、問題のトラブルシューティングに役立つ記事を見つけます。

- "コミュニティ"

  NetApp Consoleコミュニティに参加して、進行中のディスカッションをフォローしたり、新しいディスカッションを作成したりできます。

NetAppサポートでケースを作成する

上記のセルフ サポート オプションに加えて、サポートを有効にした後は、 NetAppサポート スペシャリストと協力して問題を解決することもできます。

始める前に

- *ケースの作成*機能を使用するには、まずNetAppサポート サイトの資格情報をコンソール ログインに関連付ける必要があります。 "コンソールログインに関連付けられた資格情報を管理する方法を学びます" 。
- シリアル番号を持つONTAPシステムのケースを開く場合は、NSS アカウントがそのシステムのシリアル番号に関連付けられている必要があります。

手順

1. NetApp Consoleで、[ヘルプ] > [サポート] を選択します。
2. *リソース*ページで、テクニカル サポートの下にある利用可能なオプションのいずれかを選択します。

   a. 電話で誰かと話したい場合は、「電話する」を選択してください。電話をかけることができる電話番号をリストした netapp.com のページに移動します。

   b. NetAppサポート スペシャリストとのチケットを開くには、[ケースを作成] を選択します。

      - サービス: 問題が関連付けられているサービスを選択します。たとえば、* NetApp Console* は、コンソール内のワークフローまたは機能に関するテクニカル サポートの問題に固有の場合です。
      - システム: ストレージに該当する場合は、* Cloud Volumes ONTAP* または **On-Prem** を選択し、関連する作業環境を選択します。

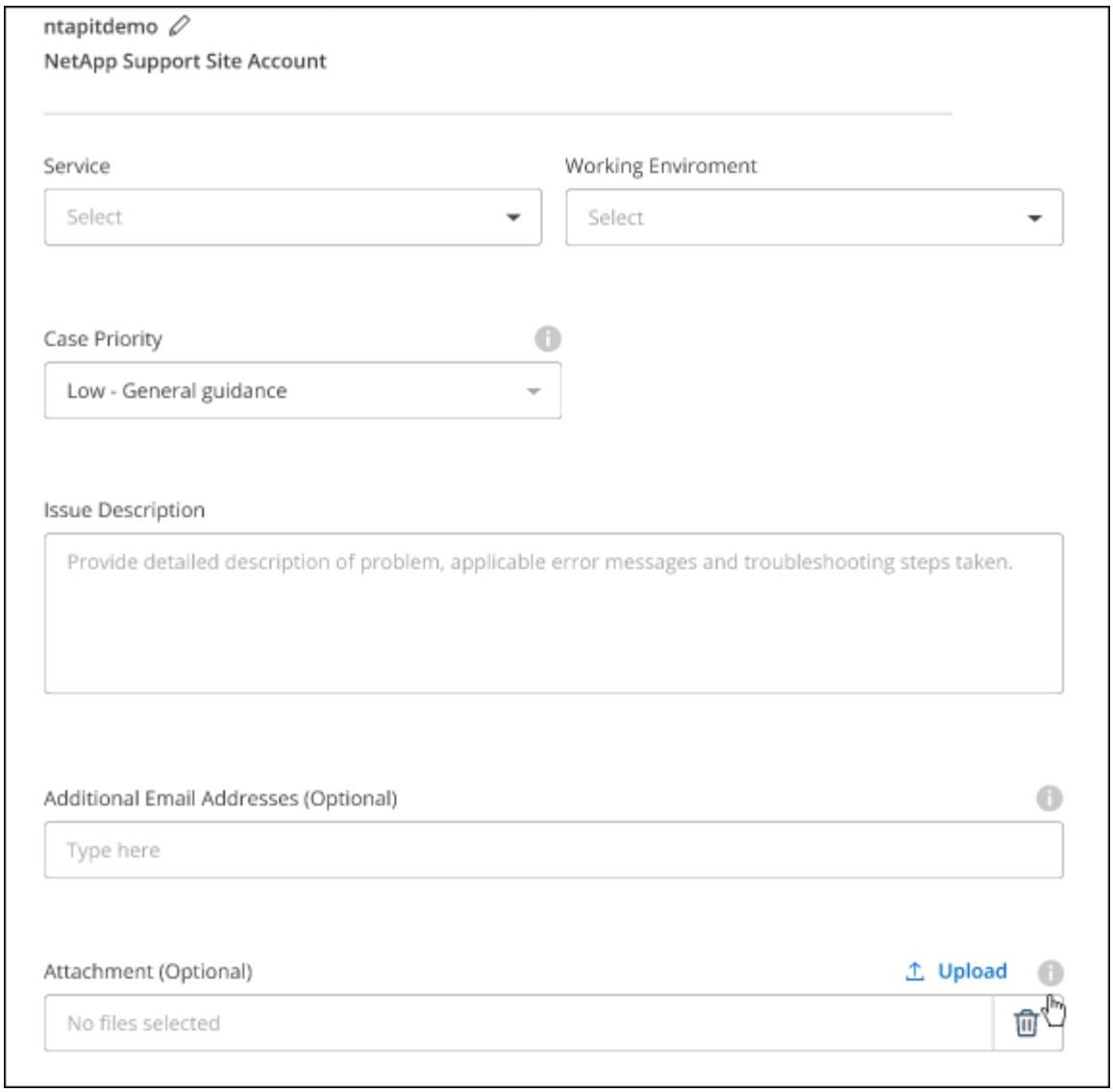
        システムのリストは、コンソール組織と、上部のバナーで選択したコンソール エージェントの範囲内にあります。

      - ケースの優先度: ケースの優先度 (低、中、高、重大) を選択します。

        これらの優先順位の詳細を確認するには、フィールド名の横にある情報アイコンの上にマウスを置きます。

      - 問題の説明: 該当するエラー メッセージや実行したトラブルシューティング手順など、問題の詳細な説明を入力します。
      - 追加のメールアドレス:この問題を他の人に知らせたい場合は、追加のメールアドレスを入力してください。
      - 添付ファイル **(**オプション**)**: 一度に 1 つずつ、最大 5 つの添付ファイルをアップロードします。

        添付ファイルはファイルごとに 25 MB までに制限されます。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、csv です。



終了後の操作

サポート ケース番号を示すポップアップが表示されます。 NetAppサポート スペシャリストがお客様のケースを確認し、すぐにご連絡いたします。

サポート ケースの履歴については、設定 > タイムライン を選択し、「サポート ケースの作成」というアクションを探します。右端のボタンを使用すると、アクションを展開して詳細を表示できます。

ケースを作成しようとすると、次のエラー メッセージが表示される場合があります。

「選択したサービスに対してケースを作成する権限がありません」

このエラーは、NSS アカウントとそれに関連付けられているレコード会社が、NetApp Consoleアカウントのシリアル番号のレコード会社と同じではないことを意味している可能性があります (つまり、 960xxxx) または作業環境のシリアル番号。次のいずれかのオプションを使用してサポートを求めることができます。

- 非技術的なケースを提出する https://mysupport.netapp.com/site/help

サポートケースを管理する

アクティブなサポート ケースと解決済みのサポート ケースをコンソールから直接表示および管理できます。NSS アカウントおよび会社に関連付けられたケースを管理できます。

次の点に注意してください。

- ページ上部のケース管理ダッシュボードには、次の 2 つのビューがあります。
  - 左側のビューには、指定したユーザー NSS アカウントによって過去 3 か月間に開かれたケースの合計が表示されます。
  - 右側のビューには、ユーザーの NSS アカウントに基づいて、会社レベルで過去 3 か月間に開かれたケースの合計が表示されます。

  表の結果には、選択したビューに関連するケースが反映されます。
- 関心のある列を追加または削除したり、優先度やステータスなどの列の内容をフィルタリングしたりできます。その他の列は並べ替え機能のみを提供します。

  詳細については、以下の手順をご覧ください。
- ケースごとに、ケースメモを更新したり、まだ「クローズ」または「クローズ保留中」ステータスになっていないケースをクローズしたりする機能を提供します。

手順

1. NetApp Consoleで、[ヘルプ] > [サポート] を選択します。
2. *ケース管理*を選択し、プロンプトが表示されたら、NSS アカウントをコンソールに追加します。

   ケース管理 ページには、コンソール ユーザー アカウントに関連付けられている NSS アカウントに関連するオープン ケースが表示されます。これは、**NSS** 管理 ページの上部に表示される NSS アカウントと同じです。
3. 必要に応じて、テーブルに表示される情報を変更します。
   - *組織のケース*の下で*表示*を選択すると、会社に関連付けられているすべてのケースが表示されます。
   - 正確な日付範囲を選択するか、別の期間を選択して日付範囲を変更します。
   - 列の内容をフィルタリングします。
   - 表に表示される列を変更するには、次に、表示する列を選択します。
4. 既存のケースを管理するには、利用可能なオプションのいずれかを選択します。
   - ケースを表示: 特定のケースに関する詳細をすべて表示します。
   - ケースノートを更新: 問題に関する追加の詳細を入力するか、*ファイルのアップロード*を選択して最大 5 つのファイルを添付します。

     添付ファイルはファイルごとに 25 MB までに制限されます。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、csv です。
   - ケースを閉じる: ケースを閉じる理由の詳細を入力し、[ケースを閉じる] を選択します。

法律上の表示

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲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。

"https://www.netapp.com/company/legal/trademarks/"

特許

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシー ポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、 NetAppソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が提供されます。

"NetApp Consoleに関するお知らせ"

著作権に関する情報

商標に関する情報