



ONTAPの自動化

ONTAP automation

NetApp
February 06, 2025

目次

ONTAPの自動化	1
新機能	2
ONTAP REST APIの新機能	2
ONTAP REST API呼び出しに対する変更点	9
はじめに	11
ONTAP の自動化オプションを理解する	11
REST Webサービスの詳細	12
ONTAP REST APIにアクセスする方法	14
最初のONTAP REST API呼び出し	15
ONTAP REST APIのラボリソース	15
ONTAP REST API	17
REST の実装の詳細	17
RBAC セキュリティ	29
REST リソースの概要	35
ワークフロー	58
ONTAP REST APIワークフローを使用するための準備	58
クラスタ	61
NAS	65
ネットワークング	75
セキュリティ	82
ストレージ	96
サポート	100
SVM	107
ソフトウェアツール	109
Python クライアントライブラリ	109
NetApp PowerShell Toolkitの詳細	113
NetApp Manageability SDKの詳細	113
ONTAPIからREST APIへの移行	115
ONTAPIの無効化とONTAP REST API	115
ONTAP REST APIの移行に関する考慮事項	115
ONTAPIからONTAP REST APIへのマッピング	116
ONTAP REST APIでのパフォーマンスカウンタの使用	116
ONTAP REST APIをサポートするツールとソフトウェア	139
ONTAP REST APIのリファレンス	140
ONTAP APIのリファレンスドキュメントへのオンラインアクセス	140
Swagger UIからONTAP APIのリファレンスドキュメントにアクセス	140
ONTAP REST APIの詳細	141
ブログ記事	141
ビデオ	142

技術トレーニングとイベント	144
ネットアップナレッジベース	144
ONTAP REST APIの法的通知	145
著作権	145
商標	145
特許	145
プライバシーポリシー	145

ONTAPの自動化

新機能

ONTAP REST APIの新機能

ONTAPのリリースごとにONTAP REST APIが更新され、新機能や機能拡張、バグの修正が行われます。



既知の制限事項や問題などの追加情報については、を参照してください ["ONTAP リリースノート"](#)。また、自動化ソフトウェアに影響する可能性のある変更についても、を参照してください ["ONTAP REST API呼び出しに対する変更点"](#)。

ONTAP 9.16.1

ONTAP 9.16.1には、20を超える新しいAPI呼び出しが含まれており、ONTAP REST APIの機能が引き続き拡張されています。これらの機能強化は主にセキュリティに重点が置かれていますが、指標とバケット管理の改善も含まれています。



NetApp ASA R2システム (ASAA1K、ASAA70、およびASAA90) のユーザ向けに公開されるONTAP REST APIは、他のすべてのFAS、AFF、およびASAシステムで提供されるREST APIとは異なります。詳細については、を参照してください ["ASA R2システムでのREST APIのサポート"](#)。

Microsoft Entra IDに対するOAuth 2.0のサポート

OAuth 2.0のサポートは、ONTAP 9.14.1で最初に導入されました。OAuth 2.0の機能は、ONTAP 9.16.1で強化され、標準のOAuth 2.0要求を持つMicrosoft Entra ID認証サーバー(旧Azure AD)をサポートします。次の2つの主な機能が含まれています。

グループをUUIDとして使用するOAuth 2.0

UUIDスタイル値に基づくEntra ID標準グループ要求は、次の2つの新しい機能と10の新しいAPI呼び出しによってサポートされています。

- グループUUIDからグループ名(`/security/groups`へのマッピング)
- UUIDグループとロールのマッピング(`/security/group/role-mapping`)

外部ロールを使用するOAuth 2.0

外部ロールは、ONTAPに定義されたOAuth 2.0 Identifyプロバイダーで定義されます。これらの外部ロールとONTAPロール間のマッピング関係を作成および管理できます。5つの新しいAPI呼び出しが追加されました。

Web認証

Web認証 (WebAuthn) は、公開鍵暗号に基づいてユーザを安全に認証するためのWeb標準です。ONTAPでは、System ManagerおよびONTAP REST APIを使用して、フィッシングに強いMFAの管理をサポートしています。いくつかのエンドポイントに7つの新しいAPI呼び出しが追加されました。

自律型ランサムウェア対策のバージョン管理と更新

ONTAPで使用されるAutonomous Ransomware Protectionパッケージを管理するための2つのAPI呼び出しが新しいエンドポイントに追加されました。Autonomous Ransomware Protectionパッケージのバージョンを表示して更新できます。

qtreeの指標

ONTAP 9.16.1には、オプションのqtree拡張パフォーマンス監視機能が含まれています。この機能を有効にすると、ONTAPはレイテンシの指標や履歴データを含む追加データをキャプチャします。このパフォーマンスデータを取得するための新しいエンドポイントが追加されました。

S3ハケットノ Snapshot

S3バケットのSnapshotを作成および管理できるように、4つの新しいAPI呼び出しが追加されました。各Snapshotは、Snapshot作成時のバケットのイメージです。

ONTAP 9.15.1

ONTAP 9.15.1では、2つの新機能のサポートを含め、ONTAP REST APIの機能が引き続き拡張されています。

TLS経由のNFS

この機能では、3つの新しいエンドポイントを使用できます。これらのAPI呼び出しを問題して、すべてのNFS over TLSインターフェイスの取得、UUIDによる特定のインターフェイスの取得、およびTLSインターフェイスの設定プロパティの更新を行うことができます。これらのAPI呼び出しをまとめて使用すると、`vserver nfs tls interface` CLIコマンド。



ONTAP 9.15.1では、NFS over TLSがパブリックプレビューとして提供されています。プレビュー版として、この機能はONTAP 9.15.1の本番環境ワークロードではサポートされていません。

WindowsバックアップアプリケーションとUNIX形式のシンボリックリンク

WindowsバックアップアプリケーションでUNIX形式のシンボリックリンク (symlink) が検出されると、リンクがトラバースされ、データがONTAPから返されてバックアップされます。ONTAP 9.15.1以降では、シンボリックリンクが指すデータではなくシンボリックリンクをバックアップするオプションも用意されています。これにより、バックアップアプリケーションのパフォーマンスの向上など、いくつかの利点が得られます。エンドポイント `/protocols/cifs/services/{svm.uuid}` が更新され、新しいパラメータがオブジェクトに追加され `backup-symlink-enabled options` しました。

ONTAP 9.14.1

ONTAP 9.14.1リリースには、30以上の新しいAPI呼び出しが含まれており、引き続きONTAP REST APIの機能が拡張されています。これらのエンドポイントは、既存の機能の更新に加えて、いくつかの新しいONTAP機能をサポートします。このリリースでは、主にセキュリティの強化に重点を置いています。NAS、QoS、パフォーマンス指標の改善も含まれています。

セキュリティ

ONTAP 9.14.1で導入された2つの主要なセキュリティ機能があります。Open Authorization (OAuth 2.0) は、ONTAPストレージリソースへのアクセスを制限するために使用できるトークンベースのフレームワークです。REST APIを使用してONTAPにアクセスするクライアントで使用できます。設定は、REST APIを含む任意のONTAP管理インターフェイスを使用して実行できます。ONTAP 9.14.1リリースでは、SSHログインの2要素認証を提供するCisco Duoもサポートされています。Duoは、ONTAPクラスタレベルまたはSVMレベルで動作するように設定できます。これら2つの新機能に加えて、いくつかのエンドポイントが追加され、キーストアの制御が向上しました。

FPolicyの永続的ストレージ

FPolicyは、ONTAPポリシーを管理するためのプラットフォームを提供します。イベントやポリシーエンジ

ンなど、さまざまなコンポーネントや要素のコンテナを提供します。REST APIを使用して、ONTAP FPolicyの設定およびイベント用の永続的ストアを設定および管理できるようになりました。SVMごとに1つの永続的ストアを設定でき、SVM内の複数のポリシーで共有されます。

QoSオプション

クラスタのQoSオプションを取得および設定できるように、2つのエンドポイントが導入されました。たとえば、バックグラウンドタスク用に使用可能なシステム処理リソースの割合を予約できます。

パフォーマンス指標

ONTAPは、システムの動作特性に関する統計情報を保持します。この情報は、テーブルと行で構成されるデータベース形式で表示されます。ONTAP 9.14.1では、ファイバチャネル、iSCSI、LUN、NVMeなど、複数のリソースカテゴリで指標データが追加されました。この追加の指標データにより、ONTAP REST APIは引き続きData ONTAP API（ONTAPIまたはZAPI）と同等になります。

その他の機能拡張

使用する環境に応じて、さらにいくつかの拡張機能が追加されています。これらの新しいエンドポイントを使用すると、SANイニシエータへのアクセスとホストキャッシュ設定の制御が向上し、個々のAutoSupportメッセージにアクセスできるようになります。

ONTAP 9.13.1

ONTAP 9.13.1では、20を超える新しいAPI呼び出しが追加され、引き続きONTAP REST APIの機能が拡張されています。これらのエンドポイントは、ONTAPの新しい機能および既存の機能拡張をサポートします。このリリースでは、セキュリティ、リソース管理、強化されたSVM設定オプション、パフォーマンス指標の改善に重点が置かれています。

リソースタギング

タグを使用してREST APIリソースをグループ化できます。これは、特定のプロジェクトまたは組織グループ内の関連リソースを関連付ける場合に行います。タグを使用すると、リソースをより効果的に整理および追跡できます。

整合グループ

ONTAP 9.13.1では、パフォーマンスカウンタデータの可用性が引き続き拡張されています。この種の統計情報にアクセスして、整合性グループのパフォーマンスと容量の履歴を追跡できるようになりました。さらに、コンシステンシグループ間の親子関係を設定および管理できるように拡張されました。

SVMごとのDNS設定

既存のDNSエンドポイントが拡張され、DNSドメインとサーバの設定を個々のSVMに対して実行できるようになりました。

EMSロールの設定

既存のEMSサポート機能が拡張され、ロールとロールに割り当てられたアクセス制御設定を管理できるようになりました。これにより、ロールの設定に基づいてイベントやメッセージを制限またはフィルタリングできます。

セキュリティ

REST APIを使用して、サインインしてSSHを使用してONTAPにアクセスするアカウントの時間ベースのワンタイムパスワード（TOTP）プロファイルを設定できます。また、キー管理エンドポイントが拡張され、指定したキー管理サーバからのリストア処理が可能になりました。

SVMごとのCIFS設定

既存のCIFSエンドポイントが拡張され、特定のSVMの設定を更新できるようになりました。

S3バケットルール

既存のS3バケットエンドポイントが拡張されてルール定義が追加されました。各ルールはリストオブジェクトであり、バケット内のオブジェクトに対して実行される一連のアクションを定義します。これらのルールをまとめて使用することで、S3バケットのライフサイクルをより適切に管理できます。

ONTAP 9.12.1

ONTAP 9.12.1では、40以上の新しいAPI呼び出しによって、ONTAP REST APIの機能が拡張されています。これらのエンドポイントは、ONTAPの新しい機能および既存の機能拡張をサポートします。このリリースでは、セキュリティ機能とNAS機能の強化に焦点を当てています。

セキュリティの機能拡張

Amazon Web Servicesには、キーなどのシークレット用のセキュアなストレージを提供するキー管理サービスが含まれています。このサービスにはREST APIからアクセスできます。これにより、ONTAPは暗号化キーをクラウドにセキュアに格納できます。また、NetApp Storage Encryptionで使用する認証キーを作成して一覧表示することもできます。

Active Directory

ONTAP クラスタ用に定義されたActive Directoryアカウントを管理できます。これには、新しいアカウントの作成、アカウントの表示、更新、削除などが含まれます。

CIFSグループポリシー

REST APIが強化され、CIFSグループポリシーの作成と管理がサポートされるようになりました。設定情報は、すべてまたは特定のSVMに適用されるグループポリシーオブジェクトによって提供および管理されます。

ONTAP 9.11.1

ONTAP 9.11.1では、引き続きONTAP REST APIの機能が拡張され、約100件の新しいAPI呼び出しが追加されています。これらのエンドポイントは、新しいONTAP機能および既存の機能拡張をサポートします。

きめ細かなRBAC

ONTAPのRole-Based Access Control (RBAC; ロールベースアクセス制御)機能が強化され、さらに細かくアクセスを制御できるようになりました。REST APIを使用すると、従来のロールを使用したり、必要に応じて新しいカスタムロールを作成したりできます。各ロールには1つ以上の権限が関連付けられます。それぞれの権限は、REST API呼び出しまたはCLIコマンドとアクセスレベルを識別します。RESTロールでは、次のような新しいアクセスレベルを使用できます。read_create および read_modify。この拡張機能は、Data ONTAP API (ONTAPIまたはZAPI)と同じ機能を提供し、REST APIへのユーザの移行をサポートします。を参照してください ["RBAC セキュリティ"](#) を参照してください。

パフォーマンスカウンタ

ONTAPの以前のリリースでは、システムの動作特性に関する統計情報が管理されていました。9.11.1リリースでは、この情報が拡張され、REST APIから使用できるようになりました。管理者または自動プロセスは、データにアクセスしてシステムのパフォーマンスを判断できます。カウンタマネージャサブシステムが管理する統計情報は、テーブルと行を使用してデータベース形式で表示されます。この拡張機能により、ONTAP REST APIはData ONTAP API (ONTAPIまたはZAPI)と同等に機能します。

アグリゲートの管理

ONTAP ストレージアグリゲートの管理が強化されました。更新されたRESTエンドポイントを使用して、アグリゲートをオンラインとオフラインに切り替えたり、スペアを管理したりできます。

IPサブネット機能

ONTAP のネットワーク機能が拡張され、IPサブネットのサポートが追加されました。REST APIを使用すると、ONTAP クラスタ内のIPサブネットの設定と管理にアクセスできます。

複数の管理者の検証

複数の管理者による検証機能は、ONTAP のコマンドや操作へのアクセスを保護するための柔軟な認証フレームワークを提供します。制限されたコマンドを識別するルールを定義できます。ユーザから特定のコマンドへのアクセスが要求された場合、必要に応じて、複数のONTAP 管理者に承認を与えることができます。

SnapMirrorの機能拡張

SnapMirror機能は、スケジュール設定など、いくつかの領域で強化されています。ONTAP 9.11.1のDP関係にSnapVault 関係のパリティも追加され、REST APIで使用できるスロットル機能は、Data ONTAP API (ONTAPIまたはZAPI) と同じ値に達しています。これに関連して、Snapshotコピーの一括作成と管理がサポートされます。

ストレージプール

ONTAP ストレージプールへのアクセスを提供するためにいくつかのエンドポイントが追加されています。クラスタ内のストレージプールの作成および一覧表示、特定のプールのIDによる更新および削除がサポートされます。

ネームサービスキャッシュのサポート

ONTAP ネームサービスが強化され、キャッシュがサポートされるようになり、パフォーマンスと耐障害性が向上しています。REST APIを使用してネームサービスキャッシュの設定にアクセスできるようになりました。設定は、ホスト、UNIXユーザ、UNIXグループ、ネットグループなど、複数のレベルで適用できます。

ONTAPIレポートツール

ONTAPIレポートツールを使用すると、お客様やパートナー様が自社の環境でONTAPIを使用する状況を特定する際に役立ちます。このツールは、ONTAPIからONTAP REST APIへの移行を計画しているお客様にとって有益な分析情報を提供します。

ONTAP 9.10.1

ONTAP 9.10.1 では、引き続き ONTAP REST API の機能が拡張されています。ONTAP の新機能と既存の機能拡張をサポートするために、100 以上の新しいエンドポイントが追加されています。次に、REST API の拡張機能の概要を示します。

アプリケーション整合グループ

整合グループは、Snapshot などの特定の処理を実行するときにグループ化される一連のボリュームです。この機能は、単一ボリュームの操作時に、クラッシュ整合性とデータ整合性を暗黙的に拡張したものです。大規模なマルチボリュームワークロードアプリケーションに有効です。

SVM 移行

SVM は、ソースクラスタからデスティネーションクラスタに移行できます。新しいエンドポイントは、一時停止、再開、ステータスの読み出し、移行処理の中止など、すべての機能を制御します。

ファイルのクローニングと管理

ボリュームレベルのファイルクローニングと管理が強化されました。新しい REST エンドポイントでは、ファイルの移動、コピー、およびスプリットの処理がサポートされます。

S3 監査の強化

S3 イベントの監査は、セキュリティの向上によって特定の S3 イベントを追跡してログに記録できるようになりました。S3 監査イベントセクタは、バケット単位で SVM 単位で設定できます。

ランサムウェア防御

ONTAP は、ランサムウェアの脅威を含む可能性のあるファイルを検出しますこれらの疑わしいファイルのリストを取得したり、ボリュームから削除したりできます。

その他のセキュリティ機能強化

既存のプロトコルを拡張し、新しい機能を導入するための一般的なセキュリティ機能がいくつか強化されています。IPSec、キー管理、SSH 設定、およびファイル権限が改善されました。

CIFS ドメインおよびローカルグループ

クラスタレベルおよび SVM レベルで CIFS ドメインのサポートが追加されました。ドメイン設定を取得したり、優先ドメインコントローラを作成および削除したりできます。

ボリューム分析を強化

上位のファイル、ディレクトリ、ユーザをサポートするために、追加のエンドポイントを通じてボリューム分析と指標が拡張されました。

サポートの強化

サポートは、いくつかの新機能によって強化されています。自動アップデートでは、最新のソフトウェアアップデートをダウンロードして適用することで、ONTAP システムを最新の状態に保つことができます。ノードによって生成されたメモリコアダンプを取得および管理することもできます。

ONTAP 9.9.1

ONTAP 9.9.1 では、引き続き ONTAP REST API の機能が拡張されています。SAN ポートセットや vServer ファイルディレクトリのセキュリティなど、既存の ONTAP 機能用の新しい API エンドポイントが追加されました。また、ONTAP 9.9.1 の新しい機能と機能拡張をサポートするためにエンドポイントが追加されました。関連ドキュメントも改善されています。拡張機能の概要を以下に示します。

ONTAPI を ONTAP 9 REST API にマッピングしています

ONTAP 自動化コードを REST API に移行するために、ネットアップでは API マッピングのドキュメントを提供しています。このリファレンスには、ONTAPI コールの一覧と、それぞれの REST API に相当する機能が含まれます。マッピングドキュメントが更新され、ONTAP 9.9.1 の新しい API エンドポイントが追加されました。を参照してください ["ONTAPI から REST API へのマッピング"](#) を参照してください。

ONTAP 9.9.1 の新しいコア機能用の API エンドポイント

ONTAPI API では使用できない ONTAP 9.9.1 の新しい機能のサポートが REST API に追加されました。ネストされた igroup と Google Cloud Key Management Services もサポートされます。

ONTAPI から REST への移行のサポートが改善されました

以前の ONTAPI コールのうち、対応する REST API に相当するものが追加されました。これには、ローカル UNIX ユーザとグループ、クライアント、SAN ポートセット、ボリュームスペース属性を必要とせず、NTFS ファイルセキュリティを管理する作業が含まれます。これらの変更は、更新された ONTAPI から

REST へのマッピングのドキュメントにも含まれます。

オンラインドキュメントが強化されました

ONTAP オンラインドキュメントのリファレンスページに、ONTAP 9.9.1 で新たに追加されたものも含め、各 REST エンドポイントまたはパラメータが導入されたときの ONTAP リリースを示すラベルが追加されました。

ONTAP 9.8

ONTAP 9.8には、ONTAPストレージシステムの導入と管理を自動化する機能を強化するいくつかの新機能が含まれています。また、従来のONTAPI APIからRESTへの移行を支援するためのサポートが強化されています。

ONTAPI を ONTAP 9 REST API にマッピングしています

ONTAPI の自動化を更新するのに役立つように、1 つ以上の入力パラメータを必要とする ONTAPI コールのリストと、それに相当する ONTAP 9 の REST API コールへのマッピングが提供されます。を参照してください "[ONTAPI から REST API へのマッピング](#)" を参照してください。

ONTAP 9.8の新しい機能のAPIエンドポイント

ONTAPIでは使用できない新しいONTAP 9.8機能がREST APIでサポートされるようになりました。これには、ONTAP S3のバケットとサービスのREST APIサポート、SnapMirror Active Sync（旧SnapMirrorビジネス継続性）、ファイルシステム分析が含まれます。

セキュリティ強化のための拡張サポート

セキュリティは、Azure Key Vault、Google Cloud Key Management Services、IPSec、証明書署名要求などの複数のサービスとプロトコルをサポートすることで強化されています。

簡易性を向上するための機能拡張

ONTAP 9.8 では、REST API を使用して、より効率的で最新のワークフローを実現できます。たとえば、ワンクリックでファームウェアのアップデートを複数の種類のファームウェアで利用できるようになりました。

オンラインドキュメントが強化されました

ONTAPオンラインドキュメントページには、9.8の新機能を含む、各RESTエンドポイントまたはパラメータが導入されたONTAPリリースを示すラベルが含まれています。

ONTAPI から REST への移行のサポートが改善されました

以前の ONTAPI コールに対応する REST API に相当する機能が追加されました。既存の ONTAPI コールの代わりに使用する REST エンドポイントを特定する方法については、ドキュメントでも説明しています。

パフォーマンス指標の強化

REST API のパフォーマンス指標が拡張され、いくつかの新しいストレージオブジェクトとネットワークオブジェクトが追加されました。

ONTAP 9.7

ONTAP 9.7 では、ONTAP REST API の機能を拡張するために、以下の 3 つの新しいリソースカテゴリが追加されています。それぞれに複数の REST エンドポイントが含まれています。

- NDMP

- オブジェクトストア
- SnapLock

ONTAP 9.7 では、既存のいくつかのリソースカテゴリに 1 つ以上の新しい REST エンドポイントが導入されています。

- クラスタ
- NAS
- ネットワーキング
- NVMe
- SAN
- セキュリティ
- ストレージ
- サポート

ONTAP 9.6

ONTAP 9.6 は、ONTAP 9.4 で導入された REST API のサポートを大幅に拡張します。ONTAP 9.6 REST API は、ほとんどの ONTAP 設定タスクおよび管理タスクをサポートします。

ONTAP 9.6 の REST API には、次のような重要な領域などがあります。

- クラスタセットアップ
- プロトコルの設定
- プロビジョニング
- パフォーマンスの監視
- データ保護
- アプリケーション対応のデータ管理

ONTAP REST API呼び出しに対する変更点

NetAppでは、製品のメジャーリリースごとにONTAP REST APIの拡張と更新を継続的に行っていきます。これらの更新には、パラメータや使用されているデフォルト値など、既存のAPI呼び出しに対する変更が含まれる場合があります。これらの変更は、REST API にアクセスするソフトウェアに影響する可能性があります。

既存のONTAP REST API呼び出しに対する変更

既存のAPI呼び出しに対する変更は、REST APIにアクセスするソフトウェアに影響する可能性があります。次の表の変更点を確認して、ONTAP自動化環境に影響がないかどうかを判断してください。各エントリには、該当するAPIエンドポイント、変更の説明、および導入されたONTAPリリースが含まれます。

エンドポイント	変更の説明	ONTAP リリース
/security/authentication/duo/groups /security/authentication/duo/profiles	応答のフィールド*_links*は、これらのエンドポイントのデュオグループから削除されました。お客様による推奨されるアクションや回避策はありません。このフィールドは、ONTAPの今後のリリースで追加される予定です。	9.15.1

ONTAP REST APIリファレンスドキュメントのエラー

NetAppはONTAP REST APIを拡張および更新するため、オンラインリファレンスドキュメントでエラーが発生することがあります。これらのエラーは、APIの使用時に混乱を招く可能性があります。通常はONTAP自動化ソフトウェアや環境に影響を与えたり、中断したりすることはありません。

次の表のエラーのリストを確認してください。これは、ONTAP REST APIのリファレンスドキュメントについて理解を深め、ナビゲートするのに役立ちます。各エントリには、該当するAPIエンドポイント、エラーの説明、およびAPIエンドポイントが導入されたONTAPリリースが含まれます。

エンドポイント	変更の説明	ONTAP リリース
/storage/quota/reports	エンドポイントのREST APIのドキュメントでは、*指定子*が有効なフィールドであることが示されています。ただし、このエンドポイントではクォータ指定子はサポートされません。お客様による推奨されるアクションや回避策はありません。このフィールドは、ONTAPの今後のリリースでAPIドキュメントから削除される予定です。	9.6

関連情報

["ONTAP REST APIの新機能"](#)

はじめに

ONTAP の自動化オプションを理解する

ONTAPストレージシステムの導入と管理を自動化するためのオプションがいくつかあります。

ONTAP REST API

ONTAP 9.6 以降 ONTAP には、ストレージシステムの導入と管理を自動化するための基盤となる拡張 REST API が搭載されています。それ以降、REST APIは拡張と成熟を続けています。ONTAP 環境の管理を自動化する際に、推奨される戦略的オプションが提供されるようになりました。

REST APIへのネイティブアクセス

ONTAP REST API には、REST クライアントをサポートする任意のプログラミング言語を使用して直接アクセスできます。代表的な言語の選択肢は、Python、PowerShell、Java です。

RESTを使用するための従来のONTAPIコードの移行

ONTAPI API (Zephyr APIまたはZAPI) は、データストレージの管理タスクと管理タスクの自動化をサポートするためにNetApp ONTAPソフトウェアに付属している独自の呼び出しセットです。APIは含まれていない["NetApp Manageability SDK の使用"](#)ます。ONTAPIインターフェイスは、ONTAPの今後のバージョンでは無効になる予定です。ONTAPI APIを使用する既存のコードがある場合は、ONTAPIから移行することを計画してください。NetAppでは、新しいONTAP REST APIを使用するためのコード変換がサポートされています。詳細については、[を参照してください "ONTAPIからREST APIへの移行"](#)。

クライアントソフトウェアツールキット

NetAppには、ONTAP REST APIを抽象化し、自動化コードの作成を容易にするクライアントツールキットが用意されています。開発言語と環境に適したものを選択してください。

Python クライアントライブラリ

Python クライアントライブラリは、ONTAP REST API にアクセスするスクリプトを記述する際に使用できるパッケージです。接続管理、非同期要求処理、例外処理など、基盤となる複数のサービスをサポートします。Python クライアントライブラリを使用すると、ONTAP の自動化目標をサポートする堅牢なコードを迅速に開発できます。詳細については、[を参照してください "Python クライアントライブラリ"](#)。

PowerShellツールキット

NetApp.ONTAP PowerShell Toolkitを使用すると、WindowsホストからのONTAPクラスタの管理を自動化できます。詳細については、[を参照してください "NetApp PowerShell Toolkitの詳細"](#)。

自動化フレームワーク

複数のフレームワークのいずれかを使用して、自動化コードを作成およびデプロイできます。

Ansible

Ansible は、プロビジョニング、構成管理、アプリケーション導入をサポートするオープンソースのソフトウェアツールです。リリース以降、RedHat が買収して以来、人気が高まってきています。ネットアップは、Ansible 認定モジュールを提供しています。このモジュールを使用すると、ONTAP ストレージシステムの管

理を自動化できます。を参照してください "[詳細はこちら。](#)" および "[ネットアップの Ansible DevOps ソリューション](#)" 追加情報の場合。

BlueXP自動化カタログ

ネットアップ "[BlueXP自動化カタログ](#)" BlueXPのWebユーザインターフェイスから利用できます。このカタログでは、ONTAPの導入と他の製品との統合を自動化するのに役立つパッケージソリューションにアクセスできます。を参照してください "[NetApp自動化](#)" を参照してください。

REST Webサービスの詳細

Representational State Transfer (REST) は、分散 Web アプリケーションの作成に使用される形式です。Web サービス API の設計に適用すると、サーバベースのリソースを公開し、その状態を管理するための一連のテクノロジーが確立されます。主流のプロトコルと標準が使用されており、ONTAP クラスタを管理するための柔軟な基盤が提供されます。



REST で共通のテクノロジーとベストプラクティスは確立されますが、各 API の詳細は開発時の選択内容に応じて異なる場合があります。ライブ環境で使用する前に、ONTAP REST API の設計上の特徴を理解しておく必要があります。

リソースと状態の表示

リソースは、Web ベースシステムの基本コンポーネントです。REST Web サービスアプリケーションを作成する場合、設計の早い段階で次の作業を行います。

- システムまたはサーバベースのリソースの識別

すべてのシステムは、リソースを使用および管理します。リソースには、ファイル、ビジネストランザクション、プロセス、管理エンティティなどがあります。REST Web サービスに基づいてアプリケーションを設計する際に行う最初の作業の 1 つは、リソースを識別することです。

- リソースの状態および関連する状態操作の定義

リソースの状態の数は有限で、リソースは必ずそのいずれかの状態にあります。状態、および状態の変化に影響する関連操作を明確に定義する必要があります。

URI エンドポイント

すべての REST リソースは、明確に定義されたアドレス指定方式を使用して定義および使用可能にする必要があります。リソースが置かれているエンドポイントは、Uniform Resource Identifier (URI) で識別されます。URI は、ネットワーク内の各リソースに一意的な名前を作成するための一般的なフレームワークです。Uniform Resource Locator (URL) は、リソースを識別してアクセスするために Web サービスで使われる URI の一種です。リソースは通常、ファイルディレクトリに似た階層構造で公開されます。

HTTP メッセージ

Hypertext Transfer Protocol (HTTP) は、Web サービスのクライアントとサーバがリソースに関する要求と応答のメッセージを交換する際に使用するプロトコルです。Web サービスアプリケーションの設計の一環として、HTTP メソッドはリソースおよび対応する状態管理アクションにマッピングされます。HTTP はステ

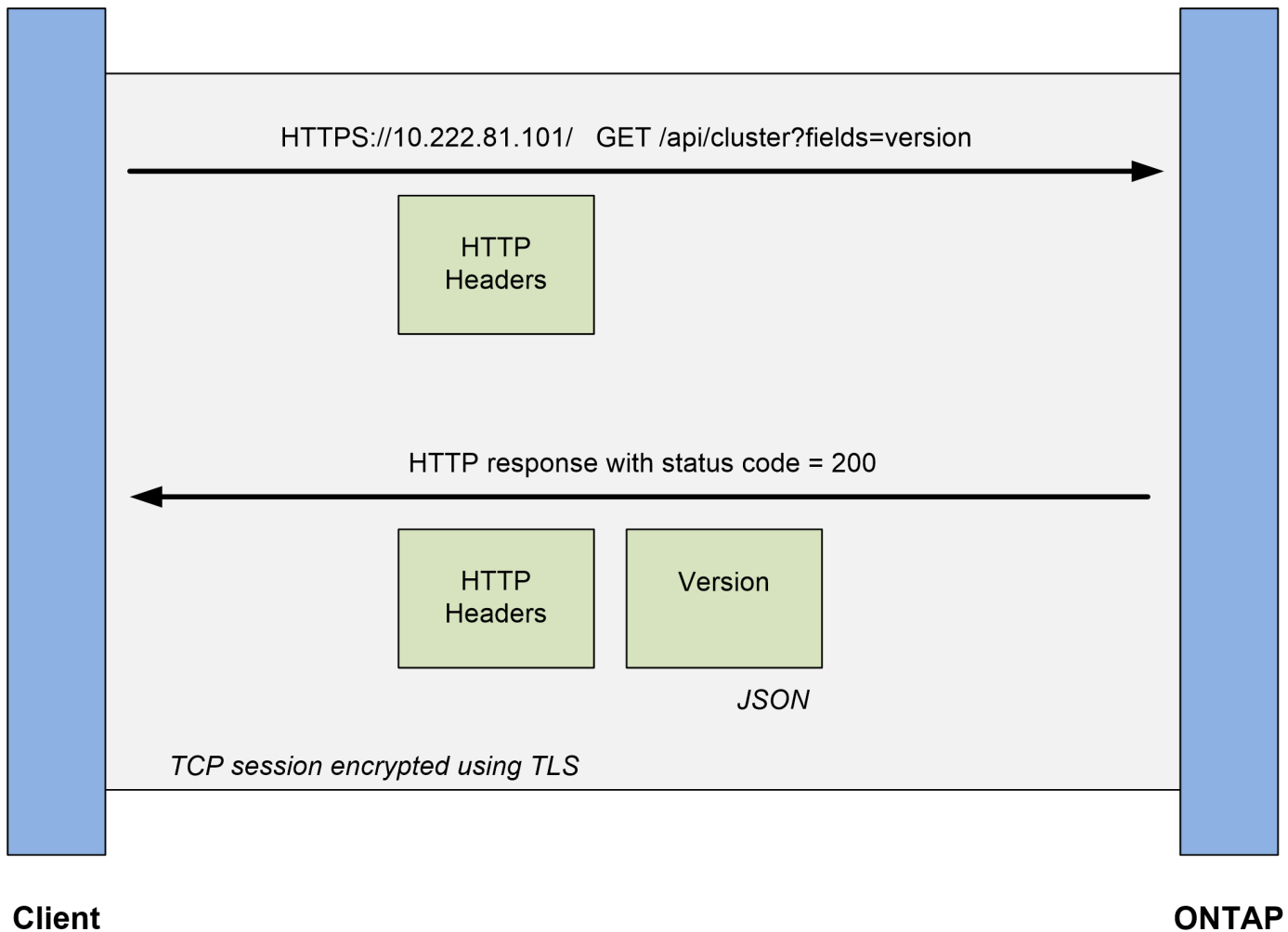
ートレスです。したがって、関連する一連の要求と応答を 1 つのトランザクションの一部として関連付けるには、要求と応答のデータフローで伝送される HTTP ヘッダーに追加情報を含める必要があります。

JSON 形式

Web サービスのクライアントとサーバの間で情報を構造化して転送する方法は複数ありますが、最も広く使用されているのは JavaScript Object Notation (JSON) です。JSON は、単純なデータ構造をプレーンテキストで表すための業界標準であり、リソースについての状態情報の転送に使用されます。ONTAP REST API では、JSON を使用して、各 HTTP 要求と応答の本文で伝送されるデータをフォーマットします。

一般的な REST API トランザクション

すべての API トランザクションは、HTTP 要求と関連する応答で構成されます。この図は、クラスタで使用されている ONTAP ソフトウェアのバージョンを取得する方法を示しています。



HTTP 要求

クライアントからサーバに送信される要求は、次のもので構成されます。

- GET 動詞
- クラスタの URL パス
- クエリパラメータ (フィールド)

- 要求ヘッダー。許可を含みます

HTTP応答

サーバからクライアントに送信される応答は、次のもので構成されます。

- ステータスコード 200
- 応答ヘッダー
- クラスタソフトウェアバージョンを含む応答の本文

ONTAP REST APIにアクセスする方法

ONTAP REST API には、いくつかの方法でアクセスできます。

ネットワークに関する考慮事項

REST API には、次のインターフェイスを通じて接続できます。

- クラスタ管理 LIF
- ノード管理 LIF
- SVM 管理 LIF

使用する LIF は、HTTPS 管理プロトコルをサポートするように設定する必要があります。また、ネットワークのファイアウォール設定で HTTPS トラフィックを許可する必要があります。



必ずクラスタ管理LIFを使用してください。これにより、API要求の負荷がすべてのノードに分散され、オフラインになっているノードや接続の問題が発生しているノードを回避できます。複数のクラスタ管理LIFが設定されている場合は、REST APIへのアクセスに関してすべて同じです。

ONTAP API オンラインドキュメントページ

ONTAP API オンラインドキュメントページに、Web ブラウザを使用する際のアクセスポイントが記載されています。個々の API 呼び出しを直接実行する方法に加え、各呼び出しの入力パラメータやその他のオプションなど、API の詳細な概要も含まれています。API 呼び出しは機能のカテゴリ別に分類されています。を参照してください "[REST リソースの概要](#)" を参照してください。

最新バージョンの API のドキュメントページにアクセスするための URL の形式は次のとおりです。

```
https://<cluster_mgmt_ip_address>/docs/api
```

カスタムのソフトウェアとツール

ONTAP API には、さまざまなプログラミング言語やツールを使用してアクセスできます。代表的なものとしては、Python、Java、Curl、PowerShell などがあります。API を使用するプログラム、スクリプト、またはツールは、REST Web サービスのクライアントとして機能します。プログラミング言語を使用すると、API についての理解が深まり、ONTAP の管理を自動化することもできます。

最新バージョンの API に直接アクセスするためのベース URL の形式は次のとおりです。

https://<cluster_mgmt_ip_address>/api

複数のバージョンがサポートされている場合に特定のバージョンの API にアクセスするには、次の形式の URL を使用します。

https://<cluster_mgmt_ip_address>/api/v1

最初のONTAP REST API呼び出し

簡単なcurlコマンドを問題して、ONTAP REST APIの使用を開始し、使用可能かどうかを確認できます。

作業を開始する前に

ワークステーションでcurlユーティリティを使用できるほか、次のものがが必要です。

- ONTAPクラスタ管理LIFのIPアドレスまたはFQDN
- ONTAP REST APIにアクセスする権限を持つアカウントのONTAPクレデンシャル



クレデンシャルに特殊文字が含まれている場合は、使用しているシェルに応じてカールできる形式にする必要があります。たとえば、各特殊文字の前にバックスラッシュを挿入したり、クレデンシャル文字列全体を二重引用符で囲むことができます。

手順

1. ローカルワークステーションのコマンドラインインターフェイスで、次のコマンドを問題します。

```
curl --request GET \  
"https://$FQDN_IP/api/cluster?fields=version" \  
--user username:password
```

◦ 例 *

```
curl --request GET "https://10.29.186.132/api/cluster?fields=version" --user  
admin:david123
```

完了後

ONTAP のバージョン情報は JSON 形式で表示されます。

ONTAP REST APIのラボリソース

NetAppには、ONTAP REST APIおよびその他の関連する自動化テクノロジーをテストするためのラボ環境が用意されています。

◦ ["ラボオンデマンド"](#) NetAppのお客様とパートナー様が利用できます。サインインしてラボリソースの使用を開始するには、有効なクレデンシャルが必要です。必要に応じて、_REST_またはその他のテクノロジーをラボで検索できます。

また、"[サンプルスクリプトを実行するためのラボオンデマンドの準備](#)"をダウンロードしてご確認ください。

ONTAP REST API

REST の実装の詳細

ONTAP REST APIの動作特性

REST で共通のテクノロジーとベストプラクティスは確立されますが、各 API の詳細は設計内容に応じて異なる場合があります。

要求と応答の API トランザクション

すべての REST API 呼び出しは、ONTAP システムへの HTTP 要求として実行され、クライアントへの関連する応答が生成されます。この要求と応答のペアで API トランザクションが構成されます。API を使用する前に、要求の制御に使用できる入力変数と応答出力の内容を理解しておく必要があります。

CRUD 操作のサポート

ONTAP REST API で使用できる各リソースへのアクセスは CRUD モデルに基づきます。

- 作成
- 読み取り
- 更新
- 削除

一部のリソースでは、一部の処理のみがサポートされます。各リソースの詳細については、ONTAP クラスタで ONTAP API ドキュメントページを参照してください。

オブジェクト ID

各リソースインスタンスまたはオブジェクトには、作成時に一意の識別子が割り当てられます。ほとんどの場合、識別子は 128 ビットの UUID です。これらの識別子は、特定の ONTAP クラスタ内でグローバルに一意です。新しいオブジェクトインスタンスを作成する API 呼び出しを実行すると、関連付けられた ID の値を含む URL が HTTP 応答の場所ヘッダーにある呼び出し元に返されます。リソースインスタンスを以降の呼び出しで参照する際には、この識別子を抽出して使用できます。



オブジェクト識別子の内容と内部構造は、いつでも変更される可能性があります。識別子を使用するのは、該当する API 呼び出しで関連付けられているオブジェクトを参照するときに必要なに応じてのみです。

オブジェクトのインスタンスとコレクション

リソースパスと HTTP メソッドに応じて、API 呼び出しを特定のオブジェクトインスタンスまたはオブジェクトのコレクションに適用できます。

同期操作と非同期操作

ONTAP では、クライアントから受信した HTTP 要求を 2 つの方法で実行します。

同期処理

ONTAP は要求をただちに実行し、成功した場合は HTTP ステータスコード 200 または 201 を返します。

GET、HEAD、OPTIONS の各メソッドを使用する要求は、いずれも常に同期的に実行されます。また、POST、PATCH、DELETE を使用する要求は、完了までに 2 秒かからないと予想される場合は同期的に実行するように設計されています。

非同期処理

非同期要求が有効な場合、ONTAP は要求を処理するバックグラウンドタスクと、タスクのアンカーを設定するジョブオブジェクトを作成します。HTTP ステータス 202 がジョブオブジェクトとともに呼び出し元に返されます。最終的な成功または失敗を確認するには、ジョブの状態を取得する必要があります。

POST、PATCH、DELETE の各メソッドを使用する要求は、完了までに 2 秒以上かかると予想される場合は非同期で実行するように設計されています。



。 `return_timeout` クエリパラメータは非同期API呼び出しで使用でき、非同期呼び出しを同期的に完了するように変換できます。を参照してください ["ジョブオブジェクトを使用した非同期処理"](#) を参照してください。

セキュリティ

REST API のセキュリティは、主に ONTAP で利用可能な既存のセキュリティ機能に基づいています。API で使用されるセキュリティは次のとおりです。

トランスポートレイヤのセキュリティ

クライアントと ONTAP LIF の間でネットワークを介して送信されるすべてのトラフィックは、ONTAP 設定に基づいて TLS を使用して暗号化されます。

クライアント認証

ONTAP System Manager および Network Manageability SDK と同じ認証オプションを ONTAP REST API でも使用できます。

HTTP 認証

HTTP レベルでは、たとえば ONTAP REST API に直接アクセスする場合、次の 2 つの認証オプションがあります。いずれの場合も、HTTP 認証ヘッダーを作成し、各要求に含める必要があります。

オプション	説明
HTTP ベーシック認証	ONTAP のユーザ名とパスワードはコロンで連結されます。文字列は base64 に変換され、要求ヘッダーに含まれます。
OAuth 2.0	ONTAP 9.14 以降では、外部許可サーバからアクセストークンを要求し、それをベアラートークンとして要求ヘッダーに含めることができます。

OAuth 2.0 の詳細と、OAuth 2.0 が ONTAP でどのように実装されているかについては、を参照してください。 ["ONTAP OAuth 2.0 実装の概要"](#)。も参照してください ["ワークフローを使用する準備をします"](#) このサイトで。

ONTAP 許可

ONTAP では、ロールベースの認証モデルが実装されています。ONTAP REST API または API ドキュメントページにアクセスするときは、適切な権限を持つアカウントを使用する必要があります。

ONTAP REST API要求の入力変数

API 呼び出しの処理方法は、HTTP 要求で設定されたパラメータと変数を使用して制御できます。

HTTP メソッド

次の表に、ONTAP REST API でサポートされる HTTP メソッドを示します。



REST エンドポイントのそれぞれですべての HTTP メソッドを使用できるわけではありません。また、PATCH と DELETE はどちらもコレクションで使用できます。詳細については、「[_オブジェクト参照と Access_](#)」を参照してください。

HTTP メソッド	説明
取得	リソースインスタンスまたはコレクションのオブジェクトプロパティを取得します。
投稿 (Post)	指定した入力に基づいて新しいリソースインスタンスを作成します。
パッチ	指定した入力に基づいて既存のリソースインスタンスを更新します。
削除	既存のリソースインスタンスを削除します。
頭部	実質的には GET 要求を発行しますが、HTTP ヘッダーのみを返します。
オプション (Options)	特定のエンドポイントでサポートされる HTTP メソッドを確認します。

パス変数

各REST API呼び出しで使用されるエンドポイントパスには、さまざまな識別子を含めることができます。各IDは特定のリソースインスタンスに対応します。たとえば、クラスタIDやSVM IDなどです。

要求ヘッダー

HTTP 要求には複数のヘッダーを含める必要があります。

コンテンツタイプ

要求の本文に JSON が含まれている場合は、このヘッダーを「application/json」に設定する必要があります。

同意します

このヘッダーは 'application/hal+json' に設定する必要があります代わりに 'application/json' に設定した場合、次のレコードのバッチを取得するために必要なリンクを除き 'HAL' リンクは返されませんヘッダがこれらの2つの値以外のものである場合、応答の「content-type」ヘッダのデフォルト値は「application/hal+json」になります。

承認

base64 文字列としてエンコードされたユーザ名とパスワードを使用するベーシック認証を設定する必要があります。例：

```
Authorization: Basic YWRtaW46cGV0ZXJzb24=。
```

本文を要求します

要求の本文の内容は、それぞれの呼び出しに応じて異なります。HTTP 要求の本文は、次のいずれかで構成されます。

- JSON オブジェクトと入力変数
- JSON オブジェクトが空です

オブジェクトのフィルタリング

GETメソッドを使用してAPI呼び出しを実行する場合、クエリパラメータを使用して、返されるオブジェクトを任意の属性に基づいて制限またはフィルタリングできます。

クエリパラメータの解析と解釈

1つ以上のパラメータのセットをURL文字列の後ろに追加できます。 ? を押します。複数のパラメータを指定した場合、クエリパラメータは & を押します。パラメーター内の各キーと値は、 = を押します。

たとえば、等号を使用して完全に一致する値を指定できます。

```
<field>=<value>
```

より複雑なクエリの場合、追加の演算子は等号の後に配置されます。たとえば、ある値以上の特定のフィールドに基づいてオブジェクトのセットを選択する場合、クエリは次のようになります。

```
<field>=>=<value>
```

フィルタ演算子

上記の例に加えて、値の範囲のオブジェクトを返すための追加の演算子も使用できます。次の表に、ONTAP REST APIでサポートされているフィルタ演算子の概要を示します。



通常、設定されていないフィールドはクエリの照合から除外されます。

演算子	説明
=	等しい
<	より小さい
>	が次の値より大きい
>=	が次の値以下です
>=	が次の値以上である必要があります
!	と等しくない
*	すべてに一致するワイルドカード

また 'null' キーワードまたはその negation!null' をクエリの一部として使用して '特定のフィールドが設定されているかどうかに基づいてオブジェクトのコレクションを返すこともできます

ワークフローの例

このサイトのREST APIワークフローの例を次に示します。

- "ディスクをリスト表示"

次の条件に基づいてフィルタ： state 変数を使用してスペアディスクを選択します。

特定のオブジェクトフィールドを要求しています

デフォルトでは、GET を使用する API 呼び出しを発行すると、オブジェクトを一意に識別する属性のみが HAL 自己リンクとともに返されます。この最小のフィールドセットは、各オブジェクトのキーとして機能し、オブジェクトタイプによって異なります。次の方法で 'fields クエリー・パラメータ' を使用して '追加のオブジェクト・プロパティ' を選択できます

- 共通または標準のフィールド

最もよく使用されるオブジェクトフィールドを取得するには 'fields=*' を指定しますこれらのフィールドは、通常、ローカルサーバメモリに保持されるか、ほとんど処理を必要としません。これらのプロパティは、URL パスキー（UUID）を指定して GET を使用した場合にオブジェクトに対して返されるプロパティと同じです。

- すべてのフィールド

「fields=*」を指定すると、アクセスするために追加のサーバ処理が必要なフィールドも含め、すべてのオブジェクトフィールドが取得されます。

- カスタムフィールドの選択

希望するフィールドを指定するには 'field=<field_name>' を使用します複数のフィールドを要求する場合は、スペースを入れずにカンマで区切る必要があります。



ベストプラクティスとして、必要なフィールドを常に個別に指定することを推奨します。一連の共通フィールドまたはすべてのフィールドを取得するのは、必要な場合だけにしてください。共通として分類され 'fields =*' を使用して返されるフィールドは '内部パフォーマンス分析に基づいてネットアップが決定しますフィールドの分類は、今後のリリースで変更される可能性があります。

出力セット内のオブジェクトのソート

リソースコレクション内のレコードは、オブジェクトによって定義されたデフォルトの順序で返されます。フィールド名とソート方向を指定して 'ORDER BY クエリー・パラメータ' を使用すると '順序を次のように変更' できます

```
order_by=< フィールド名 >asc|desc
```

たとえば、タイプフィールドを降順でソートし、ID を昇順でソートできます。

```
order_by=type desc, id asc
```

次の点に注意してください。

- ソートフィールドを指定しても方向を指定しない場合、値は昇順でソートされます。
- 複数のパラメータを指定する場合は、各フィールドをカンマで区切る必要があります。

オブジェクトのコレクションを取得するときのページ付けです

GET を使用する API 呼び出しを発行して同じタイプのオブジェクトのコレクションにアクセスする場合、ONTAP では 2 つの制約に基づいて可能な限り多くのオブジェクトを返します。これらの各制約は、要求に対する追加のクエリパラメータを使用して制御できます。特定の GET 要求に対する最初の制約に達した時点で要求が終了されるため、返されるレコードの数が制限されます。



すべてのオブジェクトについての処理が完了する前に要求が終了した場合、次のレコードのバッチを取得するために必要なリンクが応答に含まれます。

オブジェクト数の制限

デフォルトでは、ONTAP は GET 要求に対して最大 10、000 個のオブジェクトを返します。この制限は 'max_records' クエリー・パラメータを使用して変更できます例：

```
「 max_records =20`
```

実際に返されるオブジェクトの数は、関連する時間の制約やシステム内のオブジェクトの総数に基づいて、有効な最大数よりも少なくなることがあります。

オブジェクトを読み出す時間を制限しています

デフォルトでは、ONTAP は GET 要求に許可された時間内にできるだけ多くのオブジェクトを返します。デフォルトのタイムアウトは 15 秒です。この制限は、「return_timeout」クエリーパラメータを使用して変更できます。例：

```
re turn _timeout =5
```

実際に返されるオブジェクトの数は、関連するオブジェクト数の制約やシステム内のオブジェクトの総数に基づいて、有効な最大数よりも少なくなることがあります。

結果セットの絞り込み

必要に応じて、これらの 2 つのパラメータを追加のクエリパラメータと組み合わせて、結果セットを絞り込むことができます。たとえば、次の例では、指定した時間のあとに生成された EMS イベントを最大 10 件まで返します。

```
time=> 2018-04-04T15:41:29.140265Z&max_records=10
```

複数の要求を問題で処理して、オブジェクトをページングできます。以降の API 呼び出しでは、前回の結果セットの最新イベントに基づいて新しい時間の値を使用する必要があります。

サイズのプロパティ

一部の API 呼び出しおよびクエリパラメータでは、入力値として数値が使用されます。バイト単位で整数を指定する代わりに、必要に応じて次の表に示すサフィックスを使用できます。

サフィックス	説明
KB	KB キロバイト（1024 バイト）またはキビバイト
MB	MB（KB x 1024 バイト）またはメビバイト
GB	ギガバイト（MB x 1024 バイト）またはギビバイト
容量	TB（GB x 1024 バイト）またはテビバイト

サフィックス	説明
PB	PB ペタバイト (TB x 1024 バイト) またはペビバイト

関連情報

- ["オブジェクトの参照とアクセス"](#)

ONTAP REST APIの応答の解釈

各 API 要求でクライアントへの応答が生成されます。応答を調べて成功したかどうかを確認し、必要に応じて追加データを取得します。

HTTP ステータスコード

ONTAP REST API で使用される HTTP ステータスコードを次に示します。

コード	理由フレーズ	説明
200	わかりました	新しいオブジェクトを作成しない呼び出しが成功したことを示します。
201	作成済み	オブジェクトが作成されました。応答の location ヘッダーにオブジェクトの一意の識別子が含まれます。
202	承認済み	バックグラウンドジョブで要求の実行が開始されましたが、まだ完了していません。
400	無効な要求です	要求の入力が認識されないか不適切です。
401	権限がありません	ユーザ認証に失敗しました。
403	禁止されている	認証エラーによりアクセスが拒否されました。
404	が見つかりません	要求で参照されているリソースが存在しません。
405	メソッドを使用できません	要求の HTTP メソッドがリソースに対してサポートされていません。
409	競合しています	先に別のオブジェクトを作成する必要があるか、要求されたオブジェクトがすでに存在するため、オブジェクトの作成に失敗しました。
500	内部エラー	サーバで一般的な内部エラーが発生しました。

応答ヘッダー

ONTAP によって生成される HTTP 応答には、いくつかのヘッダーが含まれています。

場所

オブジェクトが作成されると、オブジェクトに割り当てられた一意の識別子を含む、新しいオブジェクトへの完全な URL が location ヘッダーに含まれます。

コンテンツタイプ

通常は 'application/hal+json' になります

応答の本文

API 要求の結果として返される応答の本文の内容は、オブジェクト、処理タイプ、および要求の成功または失敗によって異なります。応答は常に JSON 形式になります。

- 単一のオブジェクト

1 つのオブジェクトを要求に基づいて一連のフィールドとともに返すことができます。たとえば、GET では、一意の識別子を使用してクラスタの選択したプロパティを取得できます。

- 複数のオブジェクト

リソースコレクションから複数のオブジェクトを返すことができます。いずれの場合も '一貫性のある形式' が使用されており 'num_records' にはオブジェクト・インスタンスの配列を含むレコードおよびレコードの数が示されますたとえば、特定のクラスタで定義されているノードを取得できます。

- ジョブオブジェクト

API 呼び出しが非同期で処理されると、バックグラウンドタスクのアンカーを設定するジョブオブジェクトが返されます。たとえば、クラスタ構成の更新に使用される PATCH 要求は非同期で処理され、ジョブオブジェクトが返されます。

- エラーオブジェクト

エラーが発生した場合は、常にエラーオブジェクトが返されます。たとえば、クラスタに定義されていないフィールドを変更しようとするエラーが表示されます。

- JSON オブジェクトが空です

場合によっては、データが返されず、応答の本文に空の JSON オブジェクトが含まれることがあります。

HAL リンク

ONTAP REST API では、Hypermedia as the Engine of Application State (HATEOAS) をサポートするメカニズムとして HAL を使用しています。特定のリソースを識別するオブジェクトまたは属性を返す場合、リソースに関する追加の詳細を簡単に見つけて確認できるように HAL 形式のリンクも返されます。

エラー

エラーが発生した場合は、応答の本文でエラーオブジェクトが返されます。

の形式で入力し

エラーオブジェクトの形式は次のとおりです。

```
"error": {
  "message": "<string>",
  "code": <integer>[,
  "target": "<string>"]
}
```

code の値で一般的なエラーの種類やカテゴリを特定し、message で具体的なエラーの内容を確認できます。該当する場合、エラーに関連する特定のユーザ入力ターゲットフィールドに表示されます。

一般的なエラーコード

次の表に、一般的なエラーコードを示します。特定の API 呼び出しについては、追加のエラーコードが含まれる場合があります。

コード		説明
1.	409	同じ識別子のオブジェクトがすでに存在します。
2.	400	フィールドの値が無効であるか、値が指定されていないか、余分なフィールドが指定されています。
3.	400	この処理はサポートされません。
4.	405	指定した識別子のオブジェクトが見つかりません。
6.	403	要求を実行する権限が拒否されました。
8.	409	リソースが使用中です。

ONTAP REST APIを使用した非同期処理

非同期で実行するように設計された API 要求を発行すると、常にジョブオブジェクトが作成されて呼び出し元に返されます。このジョブは、要求を処理するバックグラウンドタスクを記述してアンカーを設定します。HTTP ステータスコードによっては、要求が成功したかどうかを確認するためにジョブの状態を取得する必要があります。

を参照してください ["API リファレンス"](#) 非同期で実行するように設計されている API 呼び出しを確認します。

要求の処理方法を制御する

「return turn_timeout」クエリーパラメータを使用して、非同期 API 呼び出しの処理方法を制御できます。このパラメータを使用した場合の結果には次の 2 つがあります。

要求が完了する前にタイマーが期限切れになります

有効な要求の場合、ONTAP はジョブオブジェクトとともに HTTP ステータスコード 202 を返します。要求が正常に完了したかどうかを確認するには、ジョブの状態を取得する必要があります。

要求は、タイマーが切れる前に完了します

要求が有効で時間切れになる前に正常に完了すると、ONTAP はジョブオブジェクトとともに HTTP ステータスコード 200 を返します。200 は要求が同期的に完了したことを示すため、ジョブの状態を取得する必要はありません。



'return_timeout' パラメータのデフォルト値は 0 秒ですが、パラメータを指定しない場合は、有効な要求に対して常に HTTP ステータスコード 202 が返されます。

API 要求に関連付けられたジョブオブジェクトの照会

HTTP 応答で返されるジョブオブジェクトには、いくつかのプロパティが含まれています。後続の API 呼び出しで state プロパティを照会することで、要求が正常に完了したかどうかを確認できます。ジョブオブジェクトは常に次のいずれかの状態になります。

非終了状態

- キューに登録され
- 実行中です
- 一時停止中

終了状態

- 成功
- 失敗

非同期要求を発行するための一般的な手順

非同期 API 呼び出しを完了する大まかな手順を次に示します。この例では、「return_timeout」パラメータが使用されていないか、バックグラウンドジョブが完了する前に時間が経過していると仮定しています。

1. 問題非同期で実行するように設計された API 呼び出し。
2. 有効な要求を受け入れたことを示す HTTP 応答 202 を受信します。
3. 応答の本文からジョブオブジェクトの識別子を抽出します。
4. タイミンググループ内で、サイクルごとに次の操作を実行します。
 - a. ジョブの現在の状態を取得します。
 - b. ジョブが非終了状態の場合は、もう一度ループを実行します。
5. ジョブが終了状態（success または failure）になったら停止します。

関連情報

- ["クラスタ連絡先を更新"](#)
- ["ジョブインスタンスの取得"](#)

ONTAP REST API オブジェクトの参照とアクセス

ONTAP REST API を通じて公開されたリソースインスタンスまたはオブジェクトは、さまざまな方法で参照およびアクセスできます。

オブジェクトのアクセスパス

オブジェクトにアクセスする際のパスのタイプは大きく分けて 2 つあります。

- プライマリ

オブジェクトが API 呼び出しのプライマリまたは直接のターゲットの場合です。

- 外部

オブジェクトが API 呼び出しのプライマリの参照ではなく、プライマリオブジェクトからリンクされる場合です。つまり、外部またはダウンストリームのオブジェクトであり、プライマリオブジェクトのフィールドを介して参照されます。

UUID を使用したオブジェクトへのアクセス

すべてのオブジェクトには、作成時に一意の識別子が割り当てられます。ほとんどの場合、UUID は 128 ビットです。割り当てられた UUID の値は変更できず、ONTAP 内でリソースへのアクセスと管理に内部的に使用されます。そのため、一般に、UUID はオブジェクトにアクセスするための最も高速で安定した方法となります。

多くのリソースタイプでは、URL のパスキーの一部として UUID の値を指定することで特定のオブジェクトにアクセスできます。たとえば「ノード・インスタンスにアクセスするには `/cluster/nodes/{uuid}`」を使用します

オブジェクトプロパティを使用してオブジェクトにアクセスする

UUID に加え、オブジェクトプロパティを使用してオブジェクトにアクセスすることもできます。ほとんどの場合、name プロパティを使用すると便利です。たとえば、URL 文字列でクエリパラメータを使用すると、ノードインスタンスに名前「`/cluster/nodes?name=node_A_1`」でアクセスできます。クエリパラメータに加えて、プライマリオブジェクトのプロパティを使用して外部オブジェクトにアクセスすることもできます。

UUID の代わりに名前やその他のプロパティを使用してオブジェクトにアクセスできますが、次のような欠点があります。

- 名前のフィールドは変更不可ではないため、変更できます。オブジェクトにアクセスする前にオブジェクトの名前が変更された場合、間違ったオブジェクトが返されるか、オブジェクトアクセスエラーが発生します。



この問題は、外部オブジェクトの POST メソッドまたは PATCH メソッド、またはプライマリオブジェクトの GET メソッドで発生することがあります。

- ONTAP で名前のフィールドを対応する UUID に変換する必要があります。間接アクセスの一種で、パフォーマンス問題になることがあります。

特に、次のいずれかに該当する場合は、パフォーマンスが低下する可能性があります。

- GET メソッドを使用します
- 多数のオブジェクトにアクセスした場合
- 複雑なクエリを使用します

クラスタコンテキストと SVM コンテキスト

いくつかの REST エンドポイントは、クラスタと SVM の両方をサポートします。これらのエンドポイントのいずれかを使用する場合は、「`cope=[SVM|cluster]`」の値を使用して API 呼び出しのコンテキストを指定できます。デュアルコンテキストをサポートするエンドポイントの例としては、IP インターフェイスやセキュリティロールなどがあります。



スコープの値のデフォルト値は、各 API 呼び出しで指定されたプロパティに基づきます。

オブジェクトのコレクションで **PATCH** および **DELETE** を使用する

リソースインスタンスで PATCH または DELETE をサポートする REST エンドポイントは、オブジェクトのコレクションでも同じメソッドをサポートします。唯一の要件は、URL 文字列のクエリパラメータを使用して、少なくとも 1 つのフィールドを指定する必要があることです。コレクションに対して PATCH または DELETE を発行すると、内部的には次のように処理されます。

- クエリベースの GET でコレクションを取得する
- コレクション内の各オブジェクトに対する PATCH または DELETE 呼び出しのシリアルシーケンス

操作のタイムアウトは、デフォルトの 15 秒で「return_timeout」で設定できます。タイムアウトまでに完了しなかった場合は、応答に次のオブジェクトへのリンクが含まれます。処理を続行するには、次のリンクを使用して同じ HTTP メソッドを再発行する必要があります。

ONTAP REST APIを使用したパフォーマンス指標へのアクセス

ONTAP は、選択した SVM ストレージオブジェクトとプロトコルに関するパフォーマンス指標を収集し、REST API を通じてレポートします。このデータを使用して、ONTAP システムのパフォーマンスを監視できます。

特定のストレージオブジェクトまたはプロトコルのパフォーマンスデータは、次の 3 つのカテゴリに分類されます。

- IOPS
- レイテンシ
- スループット

各カテゴリでは、次のタイプのデータを 1 つ以上使用できます。

- 読み取り (R)
- 書き込み (W)
- その他 (O)
- 合計 (T)

次の表に、ONTAP REST API の追加時など、REST API で使用可能なパフォーマンスデータを示します。詳細については、ONTAP システムの REST API オンラインドキュメントページを参照してください。

ストレージオブジェクトまたはプロトコル	IOPS	レイテンシ	スループット	ONTAP リリース
イーサネットポート	該当なし	該当なし	RWT	9.8
FC ポート	RWOT	RWOT	RWT	9.8
IP インターフェイス	該当なし	該当なし	RWT	9.8

ストレージオブジェクトまたはプロトコル	IOPS	レイテンシ	スループット	ONTAP リリース
FC インターフェイス	RWOT	RWOT	RWT	9.8
NVMe ネームスペース	RWOT	RWOT	RWOT	9.8
qtree の統計	未加工 RWOT	該当なし	未加工 RWOT	9.8
Volume FlexCache の略	RWOT	RWOT	RWT	9.8
node -プロセスの利用率	数値としてのプロセス使用率	数値としてのプロセス使用率	数値としてのプロセス使用率	9.8
クラウドボリューム	RWOT	RWOT	適用できません	9.7
LUN	RWOT	RWOT	RWOT	9.7
アグリゲート	RWOT	RWOT	RWOT	9.7
SVM NFS プロトコル	RWOT	RWOT	RWT	9.7
SVM CIFS プロトコル	RWOT	RWOT	RWT	9.7
SVM FCP プロトコル	RWOT	RWOT	RWT	9.7
SVM iSCSI プロトコル	RWOT	RWOT	RWT	9.7
SVM NVMe プロトコル	RWOT	RWOT	RWT	9.7
クラスタ	RWOT	RWOT	RWOT	9.6
個のボリューム	RWOT	RWOT	RWOT	9.6

RBAC セキュリティ

ONTAP REST APIを使用したRBACセキュリティの概要

ONTAP には、堅牢で拡張可能なロールベースアクセス制御（RBAC）機能が搭載されています。各アカウントに異なるロールを割り当てて、REST APIおよびCLIを通じて公開されるリソースへのユーザアクセスを制御することができます。ロールは、ONTAP ユーザごとに異なるレベルの管理アクセスを定義します。



ONTAP RBAC機能は拡張が継続され、ONTAP 9.11.1（およびそれ以降のリリース）で大幅に強化されています。詳細については、およびを参照してください ["RBACの機能拡張の概要"](#) ["ONTAP REST APIの新機能"](#)。

ONTAP ロール

ロールとは、ユーザが実行できるアクションをまとめて定義する権限のセットです。各権限は、特定のアクセスパスと関連するアクセスレベルを識別します。ロールはユーザアカウントに割り当てられ、アクセス制御を決定する際にONTAPによって適用されます。

ロールのタイプ

ロールには2つのタイプがあります。ONTAPの進化に合わせてさまざまな環境に導入、カスタマイズされています。



各タイプのロールを使用する場合、メリットとデメリットがあります。を参照してください "[ロールタイプの比較](#)" を参照してください。

を入力します	説明
REST	RESTロールはONTAP 9.6で導入されたもので、一般にREST APIを使用してONTAPにアクセスするユーザに適用されます。RESTロールを作成すると、従来の_mapping_roleが自動的に作成されます。
伝統的	これらはONTAP 9.6より前のレガシーロールです。ONTAP CLI環境向けに導入された機能で、引き続きRBACのセキュリティの基盤となります。

適用範囲

すべてのロールには、スコープまたはコンテキストがあり、その中で定義および適用されます。スコープによって、特定のロールがどこでどのように使用されるかが決まります。



ONTAP ユーザアカウントにも、ユーザの定義方法と使用方法を決定する同様のスコープがあります。

適用範囲	説明
クラスタ	クラスタスコープのロールは、ONTAP クラスタレベルで定義されます。クラスタレベルのユーザアカウントに関連付けられます。
SVM	SVMスコープのロールは、特定のデータSVMに対して定義されます。ユーザアカウントは同じSVM内のユーザアカウントに割り当てられます。

ロール定義のソース

ONTAP ロールは2つの方法で定義できます。

役割のソース	説明
カスタム	ONTAP 管理者は、カスタムロールを作成できます。これらのロールは、環境やセキュリティの特定の要件に合わせてカスタマイズできます。
組み込み	カスタムロールはより柔軟な設定が可能ですが、クラスタレベルとSVMレベルの両方で使用できる一連の組み込みロールも用意されています。これらのロールは事前定義されており、一般的な管理タスクに使用できます。

ロールマッピングとONTAP 処理

使用しているONTAP リリースに応じて、すべてまたはほぼすべてのREST API呼び出しが1つ以上のCLIコマンドに対応します。RESTロールを作成すると、従来のロールまたはレガシーロールも作成されます。この* Mapped *トラディショナル・ロールは対応するCLIコマンドに基づいており、操作や変更はできません。



リバースロールマッピングはサポートされません。つまり、従来のロールを作成しても、対応するRESTロールは作成されません。

RBACの機能拡張の概要

ONTAP 9のすべてのリリースに、従来のロールが含まれています。RESTロールはあとから導入されたロールで、以降のセクションで説明します。

ONTAP 9.6

REST APIはONTAP 9.6で導入されました。このリリースには、RESTロールも含まれていました。また、RESTロールを作成すると、対応する従来のロールも作成されます。

ONTAP 9.7~9.10.1

9.7から9.10.1までの各ONTAP リリースには、REST APIの機能拡張が含まれています。たとえば、リリースごとにRESTエンドポイントが追加されているとします。ただし、2つのロールタイプの作成と管理は別々に行われています。また、ONTAP 9.10.1では、リソース修飾エンドポイントである、スナップショットRESTエンドポイント「/api/storage/volumes/{voluu}/snapshots」に対するREST RBACサポートが追加されました。

ONTAP 9.11.1

このリリースでは、REST APIを使用して従来のロールを設定および管理できるようになりました。RESTロールの追加のアクセスレベルも追加されました。

ONTAP REST APIでのロールとユーザの操作

基本的なRBAC機能を理解したら、ONTAP のロールとユーザを使用できるようになります。



を参照してください ["RBACワークフロー"](#) ONTAP REST APIでロールを作成して使用する方法的例を次に示します。

管理アクセス

ONTAP ロールは、REST APIまたはコマンドラインインターフェイスを使用して作成および管理できます。アクセスの詳細を以下に示します。

REST API

RBACロールとユーザアカウントを使用するときは、いくつかのエンドポイントを使用できます。表の最初の4つは、ロールの作成と管理に使用されます。最後の2つのは、ユーザアカウントの作成と管理に使用しません。



ONTAP にはオンラインでアクセスできます ["API リファレンス"](#) APIの使用例など、詳細な情報が記載されたドキュメント。

エンドポイント	説明
「/security/roles」を参照してください	このエンドポイントでは、新しいRESTロールを作成できます。また、ONTAP 9.11.1以降では、従来のロールを作成することもできます。この場合、ONTAP は入力パラメータに基づいてロールタイプを決定します。定義済みのロールのリストを取得することもできます。
/security/roles/{owner.UUID}/{name}	クラスタまたはSVMを対象とした特定のロールを取得または削除できます。UUIDの値は、ロールが定義されているSVM（クラスタまたはデータSVM）を示します。名前の値はロールの名前です。
`/security/roles/{owner.UUID}/{name}/privileges`	このエンドポイントでは、特定のロールの権限を設定できます。組み込みのロールは取得できますが、更新することはできません。詳細については、お使いのONTAP リリースのAPIリファレンスドキュメントを参照してください。
/security/roles/{owner.UUID}/{name}/privileges / [path]	特定の権限のアクセスレベルとオプションのクエリ値を取得、変更、および削除できます。詳細については、お使いのONTAP リリースのAPIリファレンスドキュメントを参照してください。
「/security/accounts」	このエンドポイントを使用すると、クラスタまたはSVMを対象とした新しいユーザアカウントを作成できます。アカウントが使用可能になるには、いくつかの種類情報が含まれているか、追加されている必要があります。定義済みのユーザアカウントのリストを取得することもできます。
/security/accounts/{owner.UUID}/{name}	クラスタまたはSVMを対象とした特定のユーザアカウントを取得、変更、および削除できます。UUIDの値は、ユーザが定義されているSVM（クラスタまたはデータSVM）です。名前の値はアカウントの名前です。

コマンドラインインターフェイス

次に、関連するONTAP CLIコマンドについて説明します。すべてのコマンドには、管理者アカウントを使用してクラスタレベルでアクセスします。

コマンドを実行します	説明
「security login」と入力します	ユーザログインを作成および管理するために必要なコマンドが格納されたディレクトリです。
「security login rest-role」と入力します	ユーザログインに関連付けられたRESTロールの作成と管理に必要なコマンドを格納するディレクトリです。
「security login role」と入力します	ユーザログインに関連付けられた従来のロールを作成および管理するために必要なコマンドが格納されたディレクトリです。

ロールの定義

RESTロールと従来のロールは、一連の属性によって定義されます。

所有者と範囲

ロールは、ONTAP クラスタまたはクラスタ内の特定のデータSVMに所有されます。所有者は、ロールの範囲も暗黙的に決定します。

一意の名前

すべてのロールには、スコープ内で一意の名前を付ける必要があります。クラスタロールの名前はONTAP クラスタレベルで一意である必要があります。一方、SVMロールは特定のSVM内で一意である必要があります。



新しいRESTロールの名前は、RESTロールと従来のロールで一意である必要があります。これは、RESTロールを作成すると同じ名前の新しい

権限のセット

すべてのロールには、1つ以上の権限のセットが含まれています。各権限では、特定のリソースまたはコマンドと関連するアクセスレベルが識別されます。

権限

ロールには1つ以上の権限を含めることができます。各特権の定義はタプルであり、特定のリソースまたは操作へのアクセスレベルを確立します。

リソースパス

リソースパスは、RESTエンドポイントまたはCLIコマンド/コマンドディレクトリパスのいずれかとして識別されます。

RESTエンドポイント

RESTロールのターゲットリソースはAPIエンドポイントで特定されました。

CLI コマンド

CLIコマンドは、従来のロールのターゲットを特定します。コマンドディレクトリも指定できます。これにより、すべてのダウンストリームコマンドがONTAP CLI階層に含まれます。

アクセスレベル

アクセスレベルは、特定のリソースパスまたはコマンドに対するロールのアクセスタイプを定義します。アクセスレベルは、事前に定義された一連のキーワードによって識別されます。ONTAP 9.6では3つのアクセスレベルが導入されました。従来のロールとRESTロールの両方に使用できます。また、ONTAP 9.11.1で3つの新しいアクセスレベルが追加されました。これらの新しいアクセスレベルは、RESTロールでのみ使用できません。



アクセスレベルはCRUDモデルに従います。RESTでは、主なHTTPメソッド（POST、GET、PATCH、DELETE）に基づいています。対応するCLI処理は、一般にREST処理（create、show、modify、delete）と対応します。

アクセスレベル	RESTプリミティブ	を追加しました	RESTロールのみ
なし	該当なし	9.6	いいえ
- 読み取り専用	取得	9.6	いいえ
すべて	GET、POST、PATCH、DELETE	9.6	いいえ
READ_CREATE	GET、POST	9.11.1	はい。
READ_MODIFY	取得、パッチ	9.11.1	はい。

アクセスレベル	REST プリミティブ	を追加しました	REST ロールのみ
READ_CREATE _MODIFY	GET、POST、PATCH	9.11.1	はい。

オプションのクエリ

従来のロールを作成する場合、コマンドまたはコマンドディレクトリに適用可能なオブジェクトのサブセットを特定する * query * 値をオプションで指定できます。

組み込みのロールの概要

ONTAP には、クラスタレベルまたはSVMレベルで使用できる事前定義されたロールがいくつか用意されています。

クラスタを対象としたロール

クラスタ内には、複数の組み込みのロールを使用できます。

を参照してください ["クラスタ管理者の事前定義されたロール"](#) を参照してください。

ロール	説明
管理	このロールの管理者には制限のない権限があり、ONTAP システムであらゆる操作を実行できます。クラスタレベルおよびSVMレベルのすべてのリソースを設定できます。
AutoSupport	これは、AutoSupport アカウント専用のロールです。
バックアップ	この特殊な役割は、システムのバックアップが必要なバックアップソフトウェアに適用されます。
SnapLock	これは、SnapLock アカウント専用のロールです。
- 読み取り専用	このロールの管理者は、すべてのデータをクラスタレベルで表示できますが、変更はできません。
なし	管理機能は提供されません。

SVMを対象としたロール

SVMには、SVMスコープで使用できる組み込みのロールがいくつかあります。* vsadmin * は、最も一般的で強力な機能へのアクセスを提供します。特定の管理タスクに応じて、次のような追加のロールが用意されています。

- vsadmin-volume
- vsadmin-protocol のいずれかです
- vsadmin-backup のストレージシステムで
- vsadmin-snaplock
- vsadmin-readonly (読み取り専用)

を参照してください ["SVM 管理者の事前定義されたロール"](#) を参照してください。

ロールタイプの比較

REST *ロールまたは*従来の*ロールを選択する前に、これらの違いを理解しておく必要があります。この2つのロールタイプの比較方法の一部を次に示します。



RBACのユースケースが複雑で高度な場合は、通常は従来のロールを使用します。

ユーザがONTAP にアクセスする方法

ロールを作成する前に、ユーザがONTAP システムにどのようにアクセスするかを理解しておくことが重要です。このロールに基づいて、ロールのタイプを決定できます。

にアクセスします	推奨されるタイプ
REST APIのみ	RESTロールは、REST APIで使用するよう設計されています。
REST APIおよびCLI	対応する従来のロールも作成するRESTロールを定義できます。
CLIのみ	従来のロールを作成できます。

アクセスパスの精度

RESTロールに対して定義されるアクセスパスは、RESTエンドポイントに基づいています。従来のロールのアクセスパスは、CLIコマンドまたはコマンドディレクトリに基づきます。また、オプションのクエリパラメータを従来のロールと一緒に指定することで、コマンドパラメータの値に基づいてアクセスをさらに制限することもできます。

REST リソースの概要

ONTAP REST APIのリソースカテゴリの概要

ONTAP REST APIで使用できるリソースは、カテゴリ別に分類されています。各リソースカテゴリには、簡単な概要と、必要に応じて使用上の追加の考慮事項が含まれています。

この概要で説明するRESTリソースは、製品の最新バージョンに基づいています。以前のリリースで行われた変更の詳細については、を参照してください。"[ONTAP REST APIの新機能](#)"と同様に "[ONTAP リリースノート](#)"。



REST エンドポイントの多くでは、UUID キーをパス文字列の一部として含めることで特定のオブジェクトインスタンスにアクセスできます。ただし、多くの場合、クエリパラメータのプロパティ値を使用してオブジェクトにアクセスすることもできます。

関連情報

- "[API リファレンス](#)"

ONTAP REST APIのアプリケーションリソース

ONTAP アプリケーションリソースの管理に使用できる API 呼び出しを次に示します。

アプリケーションのスナップショット

アプリケーションの Snapshot コピーがサポートされます。Snapshot コピーはいつでも作成またはリストアできます。このリソースタイプは ONTAP 9.6 で導入されました。

アプリケーション

ONTAP アプリケーションは、テンプレート、アプリケーション、コンポーネント、Snapshot コピーなどのタイプに基づいて分類されます。このリソースタイプは ONTAP 9.6 で導入されました。

整合グループ

整合グループは、Snapshot などの特定の処理を実行するときにグループ化される一連のボリュームです。この機能は、単一ボリュームの操作時に、クラッシュ整合性とデータ整合性を暗黙的に拡張したものです。このリソースタイプは ONTAP 9.10 で導入され、9.12 で更新されました。指標のパフォーマンスと容量のデータを取得するエンドポイントが ONTAP 9.13 で追加されました。

整合性グループの Snapshot

これらのエンドポイントを使用して、整合グループの Snapshot をコピー、作成、インベントリ、およびリストアできます。このリソースタイプは ONTAP 9.10 で導入されました。

ONTAP REST APIのクラウドリソース

クラウドのオブジェクトストレージリソースへの接続の管理に使用できる API 呼び出しを次に示します。

ターゲット

ターゲットはクラウド内のオブジェクトストレージリソースを表します。各ターゲットには、ストレージリソースへの接続に必要な設定情報が含まれます。このリソースタイプは ONTAP 9.6 で導入されました。

ONTAP REST APIのクラスタリソース

ONTAP クラスタと関連リソースの管理に使用できる API 呼び出しを次に示します。

容量プール

容量プールのライセンスモデルでは、各クラスタノードのストレージ容量のライセンスを共有プールから取得できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

シャーシ

シャーシは、クラスタをサポートするハードウェアフレームワークです。このリソースタイプは ONTAP 9.6 で導入されました。

クラスタ

ONTAP クラスタには、1 つ以上のノードと、ストレージシステムを定義する関連設定が含まれます。このリソースタイプは ONTAP 9.6 で導入されました。

カウンタテーブル

ONTAP に関するさまざまな統計情報は、カウンタマネージャサブシステムによってキャプチャされます。この情報にアクセスして、システムのパフォーマンスを評価できます。このリソースタイプは ONTAP 9.11 で導入されました。

ファームウェア

ファームウェア更新要求の履歴を取得できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

ジョブ

非同期 REST API 要求は、ジョブによってアンカーが設定されたバックグラウンドタスクを使用して実行されます。このリソースタイプは ONTAP 9.6 で導入されました。

ライセンスインスタンス

各ライセンスは個別のパッケージとして管理できます。このリソースタイプは ONTAP 9.6 で導入されました。

ライセンスマネージャ

ONTAP クラスタに関連付けられている各ライセンスマネージャインスタンスに関する設定やその他の情報を管理できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

ライセンス

ライセンスに基づいて、特定の ONTAP 機能を実装できます。このリソースタイプは ONTAP 9.6 で導入されました。

メディアエーター

MetroCluster に関連付けられているメディアエーターインスタンスの追加や削除を含むメディアエーターを管理できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

MetroCluster

MetroCluster 環境を作成および管理して、スイッチオーバー処理やスイッチバック処理を実行できます。このリソースタイプは ONTAP 9.8 で新たに追加され、9.11 で更新されました。

MetroCluster 診断

MetroCluster 環境で診断処理を実行して、結果を取得できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

MetroCluster DR グループ

MetroCluster DR グループに関連する処理を実行できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

MetroCluster インターコネクト

MetroCluster インターコネクトのステータスを取得できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

MetroCluster ノード

MetroCluster 環境内の個々のノードのステータスを取得できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

MetroCluster 処理

MetroCluster 構成に対して最近実行された処理のリストを取得できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

MetroCluster SVM

MetroCluster 構成内のすべての SVM ペアに関する情報を取得できます。このリソースタイプは ONTAP 9.11.1 で導入されました。

ノード

ONTAP クラスタは 1 つ以上のノードで構成されます。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.8 で更新されました。

NTP キー

信頼できる外部 NTP タイムサーバと ONTAP の間で共有秘密鍵を使用するようにネットワークタイムプロトコル (NTP) を設定できます。このリソースタイプは ONTAP 9.7 で導入されました。

NTP サーバ

外部 NTP サーバやキーなど、ONTAP ネットワークタイムプロトコルを設定するために使用できる API 呼び出しを次に示します。このリソースタイプは ONTAP 9.7 で導入されました。

ピア

ピアオブジェクトはエンドポイントを表し、クラスタピア関係をサポートします。このリソースタイプは ONTAP 9.6 で導入されました。

パフォーマンスカウンタ

ONTAP の以前のリリースでは、システムの動作特性に関する統計情報が管理されていました。9.11.1 リリースでは、この情報が拡張され、REST API から使用できるようになりました。この機能を使用すると、ONTAP REST API (ONTAPI または ZAPI) と同等の機能が Data ONTAP API に近くなります。このリソースタイプは ONTAP 9.11 で導入されました。

リソースタグ

タグを使用して REST API リソースをグループ化できます。これは、特定のプロジェクトまたは組織グループ内の関連リソースを関連付ける場合に行います。タグを使用すると、リソースをより効果的に整理および追跡できます。このリソースタイプは ONTAP 9.13 で導入されました。

スケジュール

スケジュールを使用してタスクの実行を自動化できます。このリソースタイプは ONTAP 9.6 で導入されました。

センサー

これらのエンドポイントを使用して、すべてのプラットフォーム環境センサーに関する詳細を取得できます。このリソースタイプは ONTAP 9.11 で導入されました。

ソフトウェア

ONTAP クラスタには、クラスタソフトウェアプロファイル、ソフトウェアパッケージ情報、およびソフトウェア履歴情報が含まれます。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.8 で更新されました。

ウェブ:

これらのエンドポイントを使用して、Web サービス設定を更新し、現在の設定を取得することができます。このリソースタイプは ONTAP 9.10 で導入されました。

ONTAP REST API のネームサービスリソース

ONTAP でサポートされるネームサービスの管理に使用できる API 呼び出しを次に示します。

キャッシュ

ONTAP ネームサービスは、パフォーマンスと耐障害性を向上させるキャッシュをサポートしています。REST APIを使用してネームサービスキャッシュを設定できるようになりました。設定は、ホスト、UNIX ユーザ、UNIXグループ、ネットグループなど、複数のレベルで適用できます。このリソースタイプはONTAP 9.11で導入されました。

DDNS

Dynamic DNS (DDNS ; 動的 DNS) 情報を表示し、DDNS サブシステムを管理することができます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

DNS

DNS では、ネットワークでの ONTAP クラスタの統合がサポートされます。このリソースタイプはONTAP 9.6で導入され、ONTAP 9.13で拡張されました。

ホストレコード

これらのエンドポイントでは、指定したホスト名の IP アドレスと IP アドレスのホスト名を表示できます。このリソースタイプは ONTAP 9.10 で導入されました。

LDAP

LDAP サーバを使用してユーザ情報を管理できます。このリソースタイプは ONTAP 9.6 で導入されました。

LDAPスキーマ

ONTAP で使用するLDAPスキーマを作成、変更、および一覧表示できます。4つのデフォルトスキーマが含まれています。このリソースタイプはONTAP 9.11で導入されました。

ローカルホスト

これらのエンドポイントを使用して、ホスト名のローカルマッピングを表示および管理できます。このリソースタイプは ONTAP 9.10 で導入されました。

ネームマッピング

ネームマッピングを使用すると、特定のネームドメインから別のネームドメインに ID をマッピングできます。たとえば、CIFS から UNIX、Kerberos から UNIX、UNIX から CIFS に識別子をマッピングできます。このリソースタイプは ONTAP 9.6 で導入されました。

ネットグループファイル

ネットグループファイルの詳細を取得し、SVMのファイルを削除できます。このリソースタイプはONTAP 9.11で導入されました。

NIS

NIS サーバは、ユーザやクライアントワークステーションの認証に使用できます。このリソースタイプは ONTAP 9.6 で導入されました。

UNIX ユーザおよびグループ

ローカル UNIX ユーザおよびグループは、これまでの ONTAP リリースに含まれていました。ただし、REST API のサポートが追加され、ユーザとグループを表示および管理できるようになりました。これらの REST リソースタイプは ONTAP 9.9 で導入され、ONTAP 9.10 で大幅に拡張されました。

ONTAP REST APIのNASリソース

クラスタおよび SVM の CIFS と NFS の設定の管理に使用できる API 呼び出しを次に示します。

Active Directory

ONTAP クラスタ用に定義されたActive Directoryアカウントを管理できます。これには、新しいアカウントの作成、アカウントの表示、更新、削除などが含まれます。このサポートはONTAP 9.12で追加されました。

監査

SVM について、特定の CIFS イベントと NFS イベントをログに記録できます。この情報はセキュリティの向上に役立ちます。このリソースタイプは ONTAP 9.6 で導入されました。

監査ログのリダイレクト

NAS の監査イベントを特定の SVM にリダイレクトできます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

CIFS接続

確立されたCIFS接続のリストを取得できます。このリソースタイプはONTAP 9.11.1で導入されました。

CIFS ドメイン

CIFS ドメインのサポートがクラスタレベルおよび SVM レベルで追加され、いくつかのカテゴリのエンドポイントが用意されています。ドメイン設定を取得したり、優先ドメインコントローラを作成および削除したりできます。このリソースタイプはONTAP 9.10で導入され、ONTAP 9.13で拡張されました。

CIFSグループポリシー

CIFSグループポリシーの作成と管理をサポートするためにエンドポイントが追加されている。設定情報は、すべてまたは特定のSVMに適用されるグループポリシーオブジェクトによって提供および管理されます。このサポートはONTAP 9.12で追加されました。

CIFS ホームディレクトリ検索パス

CIFS サーバ上に SMB ユーザのホームディレクトリを作成すると、ユーザごとに個別の SMB 共有を作成する必要がなくなります。ホームディレクトリ検索パスは、SVM のルートからの絶対パスのセットです。このリソースタイプは ONTAP 9.6 で導入されました。

CIFS ローカルグループ

CIFS サーバでは、共有、ファイル、およびディレクトリのアクセス権を決定する際の許可にローカルグループを使用できます。このリソースタイプは ONTAP 9.9 で導入され、ONTAP 9.10 で大幅に拡張されました。

CIFS NetBIOSの場合

クラスタのNetBIOS接続に関する情報を表示できます。詳細には、IPアドレスと登録されたNetBIOS名が含まれます。この情報は、名前解決に関する問題のトラブルシューティングに役立ちます。このリソースタイプはONTAP 9.11.1で導入されました。

CIFS サービス

CIFS サーバのコアの構成。このリソースタイプはONTAP 9.6で導入され、ONTAP 9.7および9.15で更新されました。

CIFSセッションのファイル

いくつかのフィルタリングオプションに基づいて、CIFSセッションの開いているファイルのリストを取得できます。このリソースタイプはONTAP 9.11.1で導入されました。

CIFS セッション数

この API を使用して、CIFS セッションに関する詳細情報を取得できます。このリソースタイプは、ONTAP 9.8 REST API で導入され、ONTAP 9.9 で拡張されました。

CIFSシャドウコピー

Microsoftリモートボリュームシャドウコピーサービスは、Microsoft VSSの既存機能を拡張したものです。SMB共有のシャドウコピーにも対応するようにVSS機能が拡張されています。この機能は、ONTAP REST APIから使用できるようになりました。このリソースタイプはONTAP 9.11.1で導入されました。

CIFS 共有

CIFS サーバで定義されている SMB 共有。このリソースタイプは ONTAP 9.6 で導入されました。

CIFS 共有 ACL

CIFS 共有のフォルダおよびファイルへのアクセスを制御する Access Control List (ACL ; アクセス制御リスト)。このリソースタイプは ONTAP 9.6 で導入されました。

CIFS UNIX シンボリックリンクマッピング

CIFS クライアントと UNIX クライアントの両方から同じデータストアにアクセスできます。UNIX クライアントでシンボリックリンクを作成した場合、これらのマッピングによって、CIFS クライアント用に別のファイルまたはフォルダへの参照が提供されます。このリソースタイプは ONTAP 9.6 で導入されました。

CIFSユーザおよびグループの一括インポート

新しいREST APIエンドポイントを使用して、CIFSローカルユーザ、グループ、およびグループメンバーシップ情報を一括でインポートしたり、要求のステータスを監視したりできます。このリソースタイプはONTAP 9.11.1で導入されました。

ファイルアクセスのトレース

特定のファイルへのアクセスをトレースするために使用できる API 呼び出しを次に示します。このリソースタイプは ONTAP 9.8 で新たに追加されました。

ファイルセキュリティ権限

これらの API 呼び出しは、特定のファイルまたはフォルダに対して Windows ユーザまたは UNIX ユーザに付与されている有効な権限を表示します。NTFS ファイルセキュリティと監査ポリシーも管理できます。このリソースタイプは、ONTAP 9.8 REST API で導入され、ONTAP 9.9 で大幅に拡張されました。

FPolicy の

FPolicy は、SVM でファイルアクセスイベントの監視と管理に使用されるファイルアクセス通知フレームワークです。このリソースタイプは ONTAP 9.6 で導入されました。

FPolicy 接続

これらのエンドポイントを使用すると、外部 FPolicy サーバの接続ステータス情報を表示および更新できます。このリソースタイプは ONTAP 9.10 で導入されました。

FPolicy エンジン

FPolicy エンジンを使用すると、ファイルアクセス通知を受信する外部サーバを識別できます。このリソースタイプは ONTAP 9.6 で導入されました。

FPolicy イベント

ファイルアクセスの監視方法と生成されるイベントを識別する構成。このリソースタイプは ONTAP 9.6 で導入されました。

FPolicy 永続的ストア

ONTAP FPolicy の設定およびイベント用の永続的ストアを設定および管理できます。SVM ごとに1つの永続的ストアを設定でき、SVM 内の複数のポリシーで共有されます。このリソースタイプは ONTAP 9.14 で導入されました。

FPolicy ポリシー

FPolicy エンジンやイベントなど、FPolicy フレームワークの要素を格納するコンテナ。このリソースタイプは ONTAP 9.6 で導入されました。

ロック

ロックは、多数のクライアントが同じファイルに同時にアクセスしているファイルへの同時アクセスに制限を設けるための同期メカニズムです。これらのエンドポイントを使用して、ロックを取得および削除できます。このリソースタイプは ONTAP 9.10 で導入されました。

NFS 接続クライアントマップ

接続されているクライアントの NFS マップ情報を新しいエンドポイントから取得します。ノード、SVM、および IP アドレスの詳細を取得できます。このリソースタイプは ONTAP 9.11.1 で導入されました。

NFS 接続クライアント

接続されているクライアントとその接続の詳細のリストを表示できます。このリソースタイプは ONTAP 9.7 で導入されました。

NFS エクスポートポリシー

NFS エクスポートに関するルールを含むポリシー。このリソースタイプは ONTAP 9.6 で導入されました。

NFS Kerberos インターフェイス

Kerberos のインターフェイスの設定。このリソースタイプは ONTAP 9.6 で導入されました。

NFS Kerberos Realm に移動します

Kerberos Realm の設定。このリソースタイプは ONTAP 9.6 で導入されました。

TLS 経由の NFS

このリソースを使用すると、NFS over TLS を使用する場合にインターフェイス設定を取得および更新できます。このリソースタイプは ONTAP 9.15 で導入されました。

NFS サービス

NFS サーバのコアの構成。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.7 で更新されました。

オブジェクトストア

S3 イベントの監査は、セキュリティの向上によって特定の S3 イベントを追跡してログに記録できるようになりました。S3 監査イベントセレクタは、バケット単位で SVM 単位で設定できます。このリソースタイプは ONTAP 9.10 で導入されました。

vscan

ウイルスやその他の悪意のあるコードからデータを保護するセキュリティ機能。このリソースタイプは

ONTAP 9.6 で導入されました。

Vscan オンアクセスポリシー

ファイルオブジェクトをクライアントからのアクセス時にアクティブにスキャンする際の Vscan ポリシー。このリソースタイプは ONTAP 9.6 で導入されました。

Vscan オンデマンドポリシー

ファイルオブジェクトをオンデマンドで即座にスキャンするか設定されたスケジュールに従ってスキャンする際の Vscan ポリシー。このリソースタイプは ONTAP 9.6 で導入されました。

Vscan スキャナプール

ONTAP と外部ウイルススキャンサーバの間の接続を管理するために使用される一連の属性。このリソースタイプは ONTAP 9.6 で導入されました。

Vscan サーバステータス

外部ウイルススキャンサーバのステータス。このリソースタイプは ONTAP 9.6 で導入されました。

ONTAP REST APIのNDMPリソース

NDMP サービスの管理に使用できる API 呼び出しを次に示します。

NDMP モード

SVM を対象とした NDMP とノードを対象とした NDMP の動作モードがあります。このリソースタイプは ONTAP 9.7 で導入されました。

NDMP ノード

ノードの NDMP の設定を管理できます。このリソースタイプは ONTAP 9.7 で導入されました。

NDMP セッション

特定の SVM またはノードの NDMP セッションの詳細を取得および削除できます。このリソースタイプは ONTAP 9.7 で導入されました。

NDMP SVM

SVM の NDMP の設定を管理できます。このリソースタイプは ONTAP 9.7 で導入されました。

NDMP SVM ユーザパスワード

SVM のコンテンツ内で、特定の NDMP ユーザのパスワードを生成して取得できます。このリソースタイプは、ONTAP 9.8 REST API で導入され、ONTAP 9.9 で拡張されました。

ONTAP REST APIのネットワークリソース

クラスターで使用される物理ネットワークリソースと論理ネットワークリソースの管理に使用できる API 呼び出しを次に示します。

BGP ピアグループ

Border Gateway Protocol ピアグループを作成および管理できます。このリソースタイプは ONTAP 9.7 で導入されました。

イーサネットブロードキャストドメイン

イーサネットブロードキャストドメインは、同じ物理ネットワークの一部として認識される物理ポートのセットです。ドメイン内のいずれかのポートからパケットがブロードキャストされると、すべてのポートがパケットを受信します。各ブロードキャストドメインは IPspace の一部です。このリソースタイプは ONTAP 9.6 で導入されました。

イーサネットポート

イーサネットポートは、物理ネットワークまたは仮想ネットワークのエンドポイントです。Link Aggregate Group（LAG；リンクアグリゲートグループ）に結合することも、Virtual LAN（VLAN；仮想LAN）を使用して分離することもできます。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.8 で更新されました。

イーサネット・スイッチ・ポート

イーサネットスイッチのポート情報を取得することができます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

イーサネットスイッチ

ONTAP クラスタまたはストレージネットワークに使用されるイーサネットスイッチの設定を取得または変更できます。このリソースタイプは ONTAP 9.8 で新たに追加され、9.11 で更新されました。

ファイバチャネルファブリック

Fibre Channel（FC）ファブリック REST API エンドポイントを使用して、FC ネットワークに関する情報を取得できます。これには、ONTAP クラスタと FC ファブリックの間の接続、ファブリックを構成するスイッチ、アクティブなゾーンセットのゾーンが含まれます。このリソースタイプは ONTAP 9.11 で導入されました。

Fibre Channel インターフェイス

Fibre Channel インターフェイスは、SVM に関連付けられた論理エンドポイントです。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.8 で更新されました。パフォーマンス指標データの取得が ONTAP 9.14 でサポートされるようになりました。

Fibre Channel ポート

Fibre Channel ポートは、Fibre Channel ネットワークへの接続に使用される ONTAP ノード上の物理アダプタです。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.8 で更新されました。パフォーマンス指標データの取得が ONTAP 9.14 でサポートされるようになりました。

HTTP プロキシ

SVM またはクラスタ IPspace の HTTP プロキシを設定できます。このリソースタイプは ONTAP 9.7 で導入されました。

IP インターフェイス

Logical Interface（LIF；論理インターフェイス）は、追加の構成属性を持つ IP アドレスです。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.8 で更新されました。

IP ルート

ルーティングテーブルは、トラフィックを宛先に転送するために使用される IP ルートの集合です。このリソースタイプは ONTAP 9.6 で導入されました。

IP のサービスポリシー

IP サービスポリシーは、特定の LIF で使用可能なサービスを定義します。サービスポリシーは SVM または IPspace のコンテキストで設定できます。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.8 で更新

されました。

IPサブネット

ONTAP のネットワーク機能が拡張され、IPサブネットがサポートされるようになりました。REST APIを使用すると、ONTAP クラスタ内のIPサブネットの設定と管理にアクセスできます。このリソースタイプはONTAP 9.11で導入されました。

IPspace

IPspace は、1 つ以上の SVM をサポートするためのネットワークスペースを作成します。IPspace を相互に分離することで、セキュリティとプライバシーが確保されます。このリソースタイプは ONTAP 9.6 で導入されました。

ONTAP REST APIのNVMeリソース

Non-Volatile Memory Express (NVMe) をサポートするリソースの管理に使用できる API 呼び出しを次に示します。

Fibre Channel ログイン

Fibre Channel ログインは、ONTAP にログインした Fibre Channel イニシエータによって確立された接続を表します。このリソースタイプは ONTAP 9.6 で導入されました。

ネームスペース

NVMe ネームスペースは、NVMe over Fabrics プロトコルを使用して SVM に接続されたホストに提供されるアドレス指定可能な論理ブロックの集まりです。このリソースタイプはONTAP 9.6で導入され、ONTAP 9.8で更新されました。パフォーマンス指標データの取得がONTAP 9.14でサポートされるようになりました。

NVMe インターフェイス

NVMe インターフェイスは、NVMe over Fabrics (NVMe-oF) プロトコルをサポートするように設定されたネットワークインターフェイスです。このリソースタイプは ONTAP 9.6 で導入されました。

NVMe サービス

NVMe サービスは、SVM の NVMe コントローラターゲットのプロパティを定義します。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.7 で更新されました。パフォーマンス指標データの取得がONTAP 9.14でサポートされるようになりました。

NVMe サブシステムコントローラ

NVMe サブシステムコントローラは、ホストとストレージ解決策の間の動的な接続を表します。このリソースタイプは ONTAP 9.6 で導入されました。

NVMe サブシステムマップ

NVMe サブシステムマップは、NVMe ネームスペースと NVMe サブシステムの関連付けです。このリソースタイプは ONTAP 9.6 で導入されました。

NVMe サブシステム

NVMe サブシステムは、NVMe に接続された一連のホストの設定状態とネームスペースアクセス制御を管理します。このリソースタイプは ONTAP 9.6 で導入されました。

ONTAP REST APIでのオブジェクトストアリソース

S3 ベースのオブジェクトストレージへのアクセスに使用できる API 呼び出しを次に示します。

バケット

バケットはオブジェクトのコンテナであり、オブジェクトネームスペースを使用して構成されます。各 S3 オブジェクトサーバに複数のバケットを含めることができます。このリソースタイプは ONTAP 9.7 で導入され、ONTAP 9.8 で更新されました。

バケットのSnapshot

S3バケットのSnapshotを作成および管理できます。この機能は、ONTAP 9.16.1で追加されました。

サービス

サーバやバケットの設定など、ONTAP S3 設定を作成および管理できます。このリソースタイプは ONTAP 9.7 で導入されました。

サービスバケット

バケットはオブジェクトのコンテナであり、オブジェクトネームスペースを使用して構成されます。特定の S3 サーバのバケットを管理できます。このリソースタイプは ONTAP 9.7 で導入されました。

S3バケットルール

S3バケットにルール定義を含めることができます。各ルールはリストオブジェクトであり、バケット内のオブジェクトに対して実行される一連のアクションを定義します。このリソースタイプはONTAP 9.13で導入されました。

S3 グループ

S3 ユーザのグループを作成し、グループレベルでアクセス制御を管理できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

S3 ポリシー

S3 ポリシーを作成してリソースに関連付け、さまざまな権限を定義することができます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

ユーザ

S3 ユーザアカウントは S3 サーバで管理されます。ユーザアカウントはキーのペアに基づいており、ユーザが制御するバケットに関連付けられています。このリソースタイプは ONTAP 9.7 で導入されました。

ONTAP RESTAPIテノSANリソス

Storage Area Network（SAN；ストレージエリアネットワーク）リソースの管理に使用できる API 呼び出しを次に示します。

Fibre Channel ログイン

Fibre Channel ログインは、ONTAP にログインした Fibre Channel イニシエータによって確立された接続を表します。このリソースタイプは ONTAP 9.6 で導入されました。

Fibre Channel Protocol サービス

Fibre Channel Protocol (FCP) サービスは、SVM の Fibre Channel ターゲットのプロパティを定義します。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.7 で更新されました。パフォーマンス指標データの取得が ONTAP 9.14 でサポートされるようになりました。

Fibre Channel WWPN エイリアス

World Wide Port Name (WWPN ; ワールドワイドポート名) は、Fibre Channel ポートを一意に識別する 64 ビットの値です。このリソースタイプは ONTAP 9.6 で導入されました。

igroup 数

イニシエータグループ (igroup) は、ホストイニシエータを識別する Fibre Channel WWPN (World Wide Port Name)、iSCSI IQN (修飾名)、および iSCSI Extended Unique Identifier (EUI) の集まりです。このリソースタイプは、もともと ONTAP 9.6 で導入されたものです。

ネストされた igroup は、ONTAP 9.9 の新機能であり、REST API にもサポートが追加されています。この REST リソースタイプは ONTAP 9.9 で導入されました。

イニシエータ

イニシエータは、ホストエンドポイントを識別する Fibre Channel (FC ; ファイバチャネル) の World Wide Port Name (WWPN ; ワールドワイドポート名)、iSCSI Qualified Name (IQN ; iSCSI 修飾名)、または iSCSI EUI (拡張一意識別子) です。クラスタまたは特定の SVM のイニシエータを取得できます。このリソースタイプは ONTAP 9.14 で導入されました。

iSCSI クレデンシャル

iSCSI クレデンシャルオブジェクトには、イニシエータと ONTAP で使用される認証クレデンシャルが含まれています。このリソースタイプは ONTAP 9.6 で導入されました。

iSCSI サービス

iSCSI サービスは、SVM の iSCSI ターゲットのプロパティを定義します。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.7 で更新されました。パフォーマンス指標データの取得が ONTAP 9.14 でサポートされるようになりました。

iSCSI セッション

iSCSI セッションは、iSCSI イニシエータを iSCSI ターゲットにリンクする 1 つ以上の TCP 接続です。このリソースタイプは ONTAP 9.6 で導入されました。

LUN 属性

LUN 属性は呼び出し元によって定義された名前と値のペアであり、オプションで LUN に格納できます。属性は、アプリケーション固有のメタデータを少量保存するために使用でき、ONTAP で解釈されません。エンドポイントを使用して、LUN の属性を作成、更新、削除、および検出できます。このリソースタイプは ONTAP 9.10 で導入されました。

LUN マップ

LUN マップは、LUN とイニシエータグループの関連付けです。このリソースタイプは ONTAP 9.6 で導入されました。

LUN マップのレポートノード

レポートノードとは、マッピングされた LUN へのネットワークパスが ONTAP の選択的 LUN マップ (SLM) 機能の一部として SAN プロトコルを使用してアドバタイズされるクラスターノードです。新しいエンドポイントを使用すると、LUN マップのレポートノードを追加、削除、および検出できます。このリソースタイプは ONTAP 9.10 で導入されました。

LUN

LUN は、Storage Area Network（SAN；ストレージエリアネットワーク）内のストレージを論理的に表したものです。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.7 で更新されました。パフォーマンス指標データの取得が ONTAP 9.14 でサポートされるようになりました。

ポートセット

ポートセットは、_portset_Storage VM に関連付けられたファイバチャネルまたは iSCSI ネットワークインターフェイスの集まりです。この機能は以前のリリースの ONTAP にも搭載されていましたが、現在は REST API にもサポートが追加されています。この REST リソースタイプは ONTAP 9.9 で導入されました。

VVOL のバインド

VMware の Virtual Volume（VVOL）バインドは、「protocol_endpoint」クラスの LUN と「vvol」クラスの LUN の間の関連付けです。VVOL バインド REST API を使用すると、VVOL バインドを作成、削除、および検出できます。このリソースタイプは ONTAP 9.10 で導入されました。

ONTAP REST APIのセキュリティリソース

これらのAPI呼び出しを使用して、クラスタとSVMのセキュリティ設定を管理できません。

アカウント

クラスタと SVM の一連のユーザアカウントがあります。このリソースタイプは ONTAP 9.6 で導入されました。

アカウント名

対象が指定されたユーザアカウントの構成。このリソースタイプは ONTAP 9.6 で導入されました。

Active Directory プロキシ

Active Directory サーバの SVM アカウント情報を管理できます。このリソースタイプは ONTAP 9.7 で導入されました。

ランサムウェア対策

ONTAP は、ランサムウェアの脅威を含む可能性のあるファイルを検出します。エンドポイントにはいくつかのカテゴリがあります。これらの疑わしいファイルのリストを取得したり、ボリュームから削除したりできます。このリソースタイプは ONTAP 9.10.1 で導入されました。ONTAP 9 でバージョン表示とランサムウェア対策パッケージの更新のサポートが追加されました。16.

監査

監査ログファイルに記録する内容を決定する設定。このリソースタイプは ONTAP 9.6 で導入されました。

監査の送信先

これらの設定は、監査ログ情報をリモートシステムまたは Splunk サーバに転送する方法を制御します。このリソースタイプは ONTAP 9.6 で導入されました。

監査メッセージ

監査ログメッセージを取得できます。このリソースタイプは ONTAP 9.6 で導入されました。

AWS KMS

Amazon Web Services には、キーなどのシークレット用のセキュアなストレージを提供するキー管理サービス

が含まれています。このサービスにはREST APIからアクセスできます。これにより、ONTAP は暗号化キーをクラウドにセキュアに格納できます。また、NetApp Storage Encryptionで使用する認証キーを作成して一覧表示することもできます。このサポートは、ONTAP 9.12で新たに追加されました。

Azure キーバックアップ

この API 呼び出しセットを使用すると、Azure Key Vault を使用して ONTAP 暗号化キーを格納できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

証明書

API 呼び出しを使用して、ONTAP で使用される証明書をインストール、表示、および削除できます。このリソースタイプは ONTAP 9.7 で導入されました。

Cisco Duo

Duoは、SSHログインの2要素認証を提供します。Duoは、ONTAPクラスタレベルまたはSVMレベルで動作するように設定できます。このリソースタイプはONTAP 9.14で導入されました。

クラスタセキュリティ

クラスタ全体のセキュリティの詳細を取得し、特定のパラメータを更新できます。このリソースタイプは ONTAP 9.7 で導入され、ONTAP 9.8 で更新されました。

外部ロール

外部ロールは、OAuth 2.0 Identifyプロバイダーで定義されます。これらの外部ロールとONTAPロール間のマッピング関係を作成および管理できます。このリソースタイプは、ONTAP 9.16で導入されました。

GCP KMS

この API 呼び出しセットを使用すると、Google Cloud Platform Key Management Service を使用して ONTAP 暗号化キーを格納および管理できます。このリソースタイプは、ONTAP 9.8 REST API で最初に導入されました。ただし、この機能は再設計されているため、ONTAP 9.9 で新しいリソースタイプであると見なされます。

グループ

UUIDで表されるグループを含むグループ構成を管理できます。このリソースタイプは、ONTAP 9.16で導入されました。

グループロールのマッピング

グループとロール間のマッピング関係を作成および管理できます。このリソースタイプは、ONTAP 9.16で導入されました。

IPSec

IPSec は、基盤となる IP ネットワーク上の 2 つのエンドポイント間のセキュリティを提供するプロトコルのスイートです。このリソースタイプは ONTAP 9.8 で新たに追加されました。

IPSec CA 証明書

IPSec CA 証明書を追加、削除、および取得できます。このリソースタイプは、ONTAP 9.10 で新たに導入されました。

IPSec ポリシー

この一連の API 呼び出しを使用して、IPSec 展開に有効なポリシーを管理できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

IPsec セキュリティアソシエーション

この一連の API 呼び出しを使用して、IPSec 展開で有効なセキュリティアソシエーションを管理できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

キー管理ツールの設定

これらのエンドポイントを使用すると、キー管理ツールの設定を取得および更新できます。このリソースタイプは、ONTAP 9.10 で新たに導入されました。

キー管理ツール

キー管理ツールを使用すると、ONTAP 内のクライアントモジュールでキーを安全に保管できます。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.7 用に更新されました。認証キーをサポートするために ONTAP 9.12 を使用する更新がもう 1 つありました。リストア機能が ONTAP 9.13 で追加されました。

キーストア

キーストアとは、キー管理ツールのタイプを表します。このリソースタイプは、ONTAP 9.10 で新たに導入されました。ONTAP 9.14 では、強化された制御をサポートするエンドポイントが追加されました。

LDAP 認証

これらの API 呼び出しは、クラスタの LDAP サーバの構成を取得および管理するために使用します。このリソースタイプは ONTAP 9.6 で導入されました。

ログインメッセージ

ONTAP で使用されるログインメッセージを表示および管理するために使用します。このリソースタイプは ONTAP 9.6 で導入されました。

複数の管理者の検証

複数の管理者による検証機能は、ONTAP のコマンドや操作へのアクセスを保護するための柔軟な認証フレームワークを提供します。次の領域でアクセスの定義、要求、および承認をサポートする新しいエンドポイントは 17 個あります。

- ルール
- リクエスト
- 承認グループ

複数の管理者がアクセスを承認するオプションを指定すると、ONTAP および IT 環境のセキュリティが向上します。これらのリソースタイプは ONTAP 9.11 で導入されました。

NIS 認証

これらの設定は、クラスタの NIS サーバの構成を取得および管理するために使用します。このリソースタイプは ONTAP 9.6 で導入されました。

OAuth 2.0

Open Authorization (OAuth 2.0) は、ONTAP ストレージリソースへのアクセスを制限するために使用できるトークンベースのフレームワークです。REST API を使用して ONTAP にアクセスするクライアントで使用できます。このリソースタイプは、ONTAP 9.14 で導入されました。これは ONTAP 9.16 で強化され、Microsoft Entra ID 認証サーバー (旧 Azure AD) と標準の OAuth 2.0 要求をサポートしています。さらに、UUID スタイル値に基づく Entra ID 標準グループ要求は、新しいグループおよびロールマッピング機能によってサポートされています。新しい外部ロールマッピング機能も導入されました。「外部ロール」、「グループ」、および「グループロールマッピング」も参照してください。

パスワード認証

これには、ユーザアカウントのパスワードの変更に使用される API 呼び出しが含まれます。このリソースタイプは ONTAP 9.6 で導入されました。

ロールインスタンスの権限

特定のロールの権限を管理します。このリソースタイプは ONTAP 9.6 で導入されました。

公開鍵による認証

ユーザアカウントの公開鍵の設定に使用できる API 呼び出しを次に示します。このリソースタイプは ONTAP 9.7 で導入されました。

ロール

ロールを使用してユーザアカウントに権限を割り当てることができます。このリソースタイプは ONTAP 9.6 で導入されました。

ロールインスタンス

ロールの特定のインスタンス。このリソースタイプは ONTAP 9.6 で導入されました。

SAML サービスプロバイダ

SAML サービスプロバイダの設定を表示および管理できます。このリソースタイプは ONTAP 9.6 で導入されました。

SSH

これらの呼び出しは、SSH の設定に使用します。このリソースタイプは ONTAP 9.7 で導入されました。

SSH SVMs

これらのエンドポイントを使用すると、すべての SVM の SSH セキュリティ設定を取得できます。このリソースタイプは ONTAP 9.10 で導入されました。

TOTPS

REST API を使用して、サインインして SSH を使用して ONTAP にアクセスするアカウントの時間ベースのワンタイムパスワード (TOTP) プロファイルを設定できます。このリソースタイプは ONTAP 9.13 で導入されました。

Web 認証

Web 認証 (WebAuthn) は、公開鍵暗号に基づいてユーザを安全に認証するための Web 標準です。ONTAP では、System Manager および ONTAP REST API を使用して、フィッシングに抵抗する MFA の管理をサポートしています。この機能は ONTAP 9 で追加されました。16。

ONTAP REST API の SnapLock リソース

これらの API 呼び出しを使用して、ONTAP SnapLock 機能を管理できます。

ログ

SnapLock のログ構造は、ログレコードを含む特定のボリュームのディレクトリとファイルに基づいています。ログファイルは、最大ログサイズに基づいていっぱいになり、アーカイブされます。このリソースタイプは ONTAP 9.7 で導入されました。

コンプライアンスクロック

コンプライアンスクロックは、SnapLock オブジェクトの有効期限を決定します。クロックは REST API の外部で初期化する必要があり、変更することはできません。このリソースタイプは ONTAP 9.7 で導入されました。

イベント保持

SnapLock のイベントベースの保持（EBR）機能を使用して、特定のイベントの発生後にファイルを保持する期間を定義できます。このリソースタイプは ONTAP 9.7 で導入されました。

ファイルの保持と **privileged delete**

SnapLock で作成されたファイルの保持期間を管理できます。必要に応じて、SnapLock エンタープライズボリュームにある期限切れ前の WORM ファイルを削除することもできます。このリソースタイプは ONTAP 9.7 で導入されました。



削除操作を実行する権限を持つ組み込みのロールは vsadmin-snaplock だけです。

ファイルフィンガープリント

タイプや有効期限など、ファイルとボリュームについてのコア情報を表示および管理できます。このリソースタイプは ONTAP 9.7 で導入されました。

リーガルホールド

これらの API 呼び出しは、訴訟プロセスに関連するファイルの管理に使用できます。このリソースタイプは ONTAP 9.7 で導入されました。

ONTAP REST APIのSnapMirrorリソース

SnapMirror データ保護テクノロジーの管理に使用できる API 呼び出しを次に示します。

ポリシー

SnapMirror ポリシーは関係に適用され、各関係の構成属性と動作を制御します。このリソースタイプは ONTAP 9.6 で導入されました。

関係

データの転送に必要な接続を確立する非同期関係と同期関係の両方が含まれます。このリソースタイプは ONTAP 9.6 で導入されました。

関係が転送される

既存の SnapMirror 関係による SnapMirror 転送を管理できます。このリソースタイプは ONTAP 9.6 で導入されました。

ONTAP REST APIのストレージリソース

物理ストレージと論理ストレージの管理に使用できる API 呼び出しを次に示します。

集計指標

特定のアグリゲートの指標の履歴データを取得できます。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.7 で更新されました。

アグリゲートのプレックス

アグリゲート内の WAFL ストレージの物理コピー。このリソースタイプは ONTAP 9.6 で導入されました。

アグリゲート

アグリゲートは 1 つ以上の RAID グループで構成されます。このリソースタイプは ONTAP 9.6 で導入されました。

ブリッジ

クラスタ内のブリッジを取得できます。このリソースタイプは ONTAP 9.9 で導入されました。

ディスク

クラスタ内の物理ディスク。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.7 および 9.8 で更新されました。

ファイルクローン

これらのエンドポイントを使用して、ファイルクローンの作成、スプリットステータスの取得、およびスプリット負荷の管理を行うことができます。ファイルクローニングのエンドポイントリソースは、ONTAP 9.6 で初めて導入され、ONTAP 9.8 で拡張されました。ONTAP 9.10 で再び大幅に拡張されました。

ファイル移動

これらの REST API エンドポイントを使用して、2 つの FlexVol 間または FlexGroup ボリューム内でファイルを移動できます。要求を承認したら、進捗状況とステータスを監視できます。このリソースタイプは ONTAP 9.11.1 で導入されました。

FlexCache

このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.8 で更新されました。

FlexCache の原点

FlexCache は、元のボリュームの永続的なキャッシュです。このリソースタイプは、もともと ONTAP 9.6 で導入されたものです。ONTAP 9.9 REST API によるサポートが強化され、HTTP パッチメソッドによる変更がサポートされるようになりました。

監視対象ファイル

特定のファイルを追加監視用に指定できます。このリソースタイプは ONTAP 9.8 で新たに追加されました。

プール

共有ストレージプールを作成したり、クラスタ内のストレージプールを取得したりできます。このリソースタイプは ONTAP 9.11.1 で導入されました。

ポート

クラスタのストレージポート。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.11.1 で拡張されました。

QoS ポリシー

QoS ポリシーの設定。このリソースタイプは ONTAP 9.6 で導入されました。

QoS オプション

エンドポイントが導入され、クラスタの QoS オプションを取得および設定できるようになりました。たとえば、バックグラウンドタスク用に使用可能なシステム処理リソースの割合を予約できます。このリソースタイプは ONTAP 9.14 で導入されました。

QoS ワークロード

QoS ワークロードとは、QoS によって追跡されるストレージオブジェクトのことです。QoS ワークフローを取得できます。このリソースタイプは ONTAP 9.10 で導入されました。

qtree

これらのAPI呼び出しを使用して、qtree（論理的に分割されたファイルシステムの種類）を管理できます。このリソースタイプは ONTAP 9 で導入されました。6qtree 拡張パフォーマンス監視機能が ONTAP 9.16.1 で追加されました。

クォータレポート

クォータに関するレポート。クォータは、ファイルまたはスペースの使用を制限または追跡するための手法です。このリソースタイプは ONTAP 9.6 で導入されました。

クォータルール

クォータの適用に使用されるルール。このリソースタイプは ONTAP 9.6 で導入され、ONTAP 9.7 で更新されました。

シェルフ

クラスタ内のシェルフ。このリソースタイプは ONTAP 9.6 で導入されました。

Snapshot ポリシー

Snapshot はポリシーに基づいて作成されます。このリソースタイプは ONTAP 9.6 で導入されました。

Snapshot スケジュール

Snapshot スケジュールを制御できます。このリソースタイプは、ONTAP 9.8 で新たに再設計されました。

スイッチ

クラスタ内のスイッチを取得できます。このリソースタイプは ONTAP 9.9 で導入されました。

テープデバイス

クラスタ内のテープデバイスを取得できます。このリソースタイプは ONTAP 9.9 で導入されました。

上位の指標

上位の指標エンドポイントでは、特定の指標でフィルタされたボリュームのアクティビティを確認できます。クライアント、ディレクトリ、ファイル、およびユーザに基づいてフィルタリングを実行できます。このリソースタイプは ONTAP 9.10 で導入されました。

ボリューム効率化ポリシー

ボリューム全体に効率化を設定するために使用できる API 呼び出しを次に示します。このリソースタイプは ONTAP 9.8 で新たに追加されました。

個のボリューム

論理コンテナは、クライアントにデータを提供するために使用されます。このリソースタイプは、元々は ONTAP 9.6 REST API で導入されました。API で使用されるパラメータ値の多くは、ONTAP 9.9 で大幅に拡張されました。これには、スペース管理で使用される値も含まれます。

ボリュームファイル

ボリューム上の特定のディレクトリのファイルとディレクトリのリストを取得できます。このリソースタイプは ONTAP 9.7 で導入され、ONTAP 9.8 で更新されました。

ボリューム Snapshot

ボリュームの Snapshot。このリソースタイプは ONTAP 9.6 で導入されました。

ONTAP REST APIのサポートリソース

クラスタのサポートに使用される ONTAP 機能の管理に使用できる API 呼び出しを次に示します。

アプリケーションログ

スタンドアロンアプリケーションでは、POST要求を発行することで、ONTAP システムにEMSイベントとオプションで生成されたAutoSupport パッケージを記録できます。このリソースタイプはONTAP 9.11.1で導入されました

自動更新

自動更新機能は、最新のソフトウェア更新をダウンロードして適用することで、ONTAP システムを最新の状態に保ちます。この機能は、ステータス、設定、更新など、いくつかのエンドポイントカテゴリでサポートされます。これらのリソースタイプは ONTAP 9.10 で導入されました。

AutoSupport

AutoSupport は、構成やステータスの詳細およびエラーを収集してネットアップに情報を報告します。このリソースタイプは ONTAP 9.6 で導入されました。

AutoSupport メッセージ

各ノードで生成および取得できる AutoSupport メッセージが管理されます。このリソースタイプは ONTAP 9.6 で導入されました。

構成のバックアップ

これらの API を使用して、現在のバックアップ設定を取得および更新できます。このリソースタイプは ONTAP 9.6 で導入されました。

構成のバックアップ処理

構成バックアップファイルを作成、取得、および削除できます。このリソースタイプは ONTAP 9.7 で導入されました。

コアダンプ

これらのエンドポイントを使用して、クラスタまたはノードによって生成されたメモリコアダンプを取得および管理できます。このリソースタイプは ONTAP 9.10 で導入されました。

EMS

Event Management System (EMS ; イベント管理システム) は、イベントを収集して 1 つ以上のデスティネーションに通知を送信します。このリソースタイプは ONTAP 9.6 で導入されました。

EMS デスティネーション

EMS デスティネーションによって、通知の送信方法と送信先が決まります。このリソースタイプは ONTAP 9.6 で導入されました。

EMS デスティネーションインスタンス

EMS デスティネーションインスタンスは、タイプと場所で定義されます。このリソースタイプは ONTAP 9.6 で導入されました。

EMS イベント

クラスタの最新のシステムイベントを収集したものです。このリソースタイプは ONTAP 9.6 で導入されました。

EMS フィルタ

EMS フィルタは、追加の処理が必要なイベントをまとめて識別します。このリソースタイプは ONTAP 9.6 で導入されました。

EMS フィルタインスタンス

EMS フィルタインスタンスは、イベントに適用されるルールの集まりです。このリソースタイプは ONTAP 9.6 で導入されました。

EMS メッセージです

EMS イベントカタログへのアクセスを提供します。このリソースタイプは ONTAP 9.6 で導入されました。

EMS ロールの設定

EMS サポート機能では、ロールとそのロールに割り当てられたアクセス制御設定を管理できます。これにより、ロールの設定に基づいてイベントやメッセージを制限またはフィルタリングできます。このリソースタイプは ONTAP 9.13 で導入されました。

フィルタインスタンスの EMS ルール

EMS フィルタの特定のインスタンスに対するルールのリストを管理できます。このリソースタイプは ONTAP 9.6 で導入されました。

フィルタインスタンスの EMS ルールインスタンス

EMS フィルタの特定のインスタンスに対する個別のルール。このリソースタイプは ONTAP 9.6 で導入されました。

SNMP

クラスタの SNMP およびトラップ操作を有効または無効にできます。このリソースタイプは ONTAP 9.7 で導入されました。

SNMP トラップホスト

SNMP トラップホストは、ONTAP から SNMP トラップを受信するように設定されたシステムです。ホストを取得および定義できます。このリソースタイプは ONTAP 9.7 で導入されました。

SNMP トラップホストインスタンス

特定の SNMP トラップホストを管理できます。このリソースタイプは ONTAP 9.7 で導入されました。

SNMP ユーザ

SNMP ユーザを定義および管理できます。このリソースタイプは ONTAP 9.7 で導入されました。

SNMP ユーザインスタンス

エンジン ID が管理 SVM またはデータ SVM に関連付けられた特定の SNMP ユーザを管理できます。このリソースタイプは ONTAP 9.7 で導入されました。

ONTAP REST API の SVM リソース

Storage Virtual Machine (SVM) の管理に使用できる API 呼び出しを次に示します。

データ移行

SVM は、ソースクラスタからデスティネーションクラスタに移行できます。新しいエンドポイントは、一時停止、再開、ステータスの読み出し、移行処理の中止など、すべての機能を制御します。このリソースタイプは ONTAP 9.10 で導入されました。

ピア権限

SVM ピア関係を有効にするピア権限を割り当てることができます。このリソースタイプは ONTAP 9.6 で導入されました。

ピア

ピア関係で SVM 間の接続を確立します。このリソースタイプは ONTAP 9.6 で導入されました。

SVM

クラスタにバインドされている SVM を管理できます。このリソースタイプは ONTAP 9.6 で導入されました。

上位の指標

特定のSVMインスタンスのその他のパフォーマンス指標データにアクセスできます。リストは4つあり、それぞれがONTAP FlexVol ボリュームとFlexGroup ボリュームの上位のI/Oアクティビティを示しています。リストには次のものがあります

- クライアント
- ディレクトリ
- ファイル
- ユーザ

これらのリソースタイプはONTAP 9.11で導入されました。

ウェブ：

これらのエンドポイントを使用して、各データ SVM の Web サービスセキュリティ設定を更新および取得できます。このリソースタイプは ONTAP 9.10 で導入されました。

ワークフロー

ONTAP REST APIワークフローを使用するための準備

実際のONTAP環境でワークフローを使用する前に、ワークフローの構造と形式を理解しておく必要があります。



使用するワークフローで、ONTAPリリースがすべてのAPI呼び出しをサポートしていることを確認する必要があります。を参照してください "[API リファレンス](#)" を参照してください。

はじめに

`a_workflow_` は、特定の管理タスクまたは目標を達成するために必要な 1 つ以上のステップのシーケンスです。ONTAPワークフローには、各タスクを実行するために必要な主要な手順とパラメータが含まれています。ONTAP自動化環境をカスタマイズするための出発点となります。

ステップタイプ

ONTAPワークフローの各手順は、次のいずれかのタイプです。

- REST API 呼び出し（cURL や JSON の例などの詳細を含む）
- 別のONTAPワークフローの実行または起動
- その他の関連タスク（構成の決定など）

REST API呼び出し

ワークフローの手順のほとんどはREST API呼び出しです。これらの手順では、カールの例やその他の情報を含む一般的な形式を使用します。を参照してください "[API リファレンス](#)" を参照してください。

ワンステップのワークフロー

ワークフローには1つのステップのみを含めることができます。these_single-step_workflows_ は、複数のステップを含むワークフローとは少し異なります。たとえば、明示的なステップ名は削除されます。アクションまたは操作は、ワークフローのタイトルに基づいて明確にする必要があります。

入力変数

ワークフローは、任意のONTAP環境で使用できるように、できるだけ一般的なものするように設計されています。そのため、REST API呼び出しでは、curlサンプルやその他の入力で変数が使用されます。REST API呼び出しは、さまざまなONTAP環境に簡単に適合させることができます。

ベースURL形式

ONTAP REST APIには、curlまたはプログラミング言語から直接アクセスできます。この場合、ベースURLは、ONTAPオンラインドキュメントまたはSystem Managerにアクセスするときに使用するURLとは異なります。

APIに直接アクセスする場合は、ドメインまたはIPアドレスに* api *を追加する必要があります。例：

<https://ontap.demo-example.com/api>

を参照してください ["ONTAP REST APIにアクセスする方法"](#) を参照してください。

共通の入力パラメータ

REST API呼び出しのほとんどでよく使用される入力パラメータがいくつかあります。これらのパラメータは、通常、個々のワークフローでは説明されていません。パラメータをよく理解しておく必要があります。を参照してください ["API 要求を制御する入力変数"](#) を参照してください。

特定のREST API呼び出しに追加のパラメータが必要な場合は、各ワークフローの* curlサンプルの追加の入力パラメータ*に記載されています。

変数の形式

このワークフローの例で使用されているID値やその他の変数は不透明であり、ONTAPクラスタごとに異なる場合があります。例を読みやすくするために、実際の値は使用しません。代わりに変数が使用されます。この方法では、一貫した形式と予約名のセットに基づいて、次のような利点があります。

- curlとjsonのサンプルは読みやすく、わかりやすくなっています。
- すべてのキーワードが同じ形式を使用しているため、すばやく識別できます。
- 値をコピーして再利用することはできないため、セキュリティ上の影響はありません。

変数はBashシェル環境で使用されるようにフォーマットされています。各変数はドル記号で始まり、必要に応じて二重引用符で囲みます。これにより、Bashに認識されるようになります。名前には常に大文字が使用されます。

ここでは、一般的な変数キーワードの一部を示します。このリストは完全なものではなく、必要に応じて追加の変数が使用されます。その意味はコンテキストに基づいて明確になる必要があります。

キーワード	を入力します	説明
\$FQDN_IP	URL	ONTAP管理LIFの完全修飾ドメイン名またはIPアドレス。
\$クラスタID	パス	UUIDv4の値。API処理を実行するONTAPクラスタを識別します。
\$BASIC_AUTH	ヘッダー	HTTPベーシック認証に使用するクレデンシャル文字列。

JSONの入力例

POSTやPATCHを使用するREST API呼び出しなど、一部のREST API呼び出しでは、要求の本文にJSON入力が必要です。JSON入力の例は、わかりやすくするためにcurlの例とは別に表示されています。JSON入力例は、以下で説明するいずれかの方法で使用できます。

ローカルファイルに保存

JSON入力例をファイルにコピーしてローカルに保存できます。curlコマンドは、`--data` ファイル名を示す値を持つパラメータ。@プレフィックス。

curlの例の後に端末に貼り付けます

最初に、カールの例をコピーしてターミナルシェルに貼り付ける必要があります。次に、例を編集して、`--data` 最後のパラメータを置き換えます。 `--data-raw` パラメータ最後に、JSONの例をコピーして貼り付け、更新されたパラメータを使用してcurlコマンドに従うようにします。JSON入力の例では、一重引用符を使用して折り返します。

認証オプション

REST APIで使用できる主な認証手法はHTTPベーシック認証です。ONTAP 9.14以降では、トークンベースの認証と承認でOpen Authorization (OAuth 2.0)フレームワークを使用するオプションもあります。

HTTPベーシック認証

ベーシック認証を使用する場合は、各HTTP要求にユーザクレデンシアルを含める必要があります。クレデンシアルを送信する方法は2つあります。

HTTP要求ヘッダーを作成する

Authorizationヘッダーは手動で作成し、HTTP要求に含めることができます。これは、CLIでcurlコマンドを使用する場合、またはオートメーションコードでプログラミング言語を使用する場合に実行できます。手順の概要は次のとおりです。

1. ユーザとパスワードの値をコロンで連結します。

```
admin:david123
```

2. 文字列全体をbase64に変換します。

```
YWRtaW46ZGF2aWQxMjM=
```

3. 要求ヘッダーを作成します。

```
Authorization: Basic YWRtaW46ZGF2aWQxMjM=
```

ワークフローカールの例には、このヘッダーと変数*\$BASIC_AUTH *が含まれています。このヘッダーは、を使用する前に更新する必要があります。

curlパラメータを使用する

curlを使用する場合のもう1つのオプションは、Authorizationヘッダーを削除し、代わりにcurl *user *パラメータを使用することです。例：

```
--user username:password
```

使用する環境に応じた適切なクレデンシアルに置き換える必要があります。クレデンシアルはbase64でエンコードされていません。このパラメータを指定してcurlコマンドを実行すると、文字列がエンコードされ、Authorizationヘッダーが生成されます。

OAuth 2.0

OAuth 2.0を使用する場合は、外部認可サーバーからアクセストークンを要求し、各HTTPリクエストに含める必要があります。基本的な手順の概要を次に示します。も参照してください ["ONTAP OAuth 2.0実装の概要"](#) OAuth 2.0の詳細とONTAPでの使用方法については、[を参照してください](#)。

ONTAP環境の準備

REST APIを使用してONTAPにアクセスする前に、ONTAP環境を準備して設定する必要があります。手順の概要は次のとおりです。

- ONTAPで保護されるリソースとクライアントを特定する

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/クラスタ

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
フィールド	クエリ	いいえ	返される値を選択します。例： contact および version。

curlの例：クラスタの連絡先情報を取得する

この例では、単一のフィールドを取得する方法を示します。クラスタオブジェクトと設定全体を取得するには、fields クエリパラメータ。

```
curl --request GET \  
--location "https://$FQDN_IP/api/cluster?fields=contact" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 出力例

```
{  
  "contact": "support@company-demo.com"  
}
```

ONTAP REST APIを使用したクラスタ連絡先の更新

クラスタの連絡先情報を更新できます。要求は非同期で処理されるため、関連するバックグラウンドジョブが正常に完了したかどうかを確認する必要があります。

手順1：クラスタの連絡先情報を更新する

API呼び出しを問題して、クラスタの連絡先情報を更新できます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
パッチ	/api/クラスタ

処理のタイプ

非同期

カールの例

```
curl --request PATCH \  
--location "https://$FQDN_IP/api/cluster" \  
--include \  
--header "Content-Type: application/json" \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON の入力例

```
{  
  "contact": "support@company-demo.com"  
}
```

JSON 出力例

ジョブオブジェクトが返されます。次の手順で使用するには、ジョブIDを保存する必要があります。

```
{ "job": {  
  "uuid": "d877f5bb-3aa7-11e9-b6c6-005056a78c89",  
  "_links": {  
    "self": {  
      "href": "/api/cluster/jobs/d877f5bb-3aa7-11e9-b6c6-005056a78c89"  
    }  
  }  
}
```

手順2: ジョブのステータスを取得する

ワークフローを実行 "[ジョブインスタンスの取得](#)" をクリックし、state 値は success。

手順3: クラスタの連絡先情報を確認する

ワークフローを実行 "[クラスタ構成を取得](#)". を設定する必要があります fields クエリパラメータ contact。

ONTAP REST APIを使用したジョブインスタンスの取得

特定のONTAPジョブのインスタンスを取得できます。通常、この操作は、ジョブおよび関連する処理が正常に完了したかどうかを確認するために行います。



ジョブオブジェクトのUUIDが必要です。このUUIDは通常、非同期要求の実行後に指定されます。また、["ジョブオブジェクトを使用した非同期処理"](#) ONTAP内部ジョブを操作する前に。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/cluster/jobs/ {uuid}

処理のタイプ

同期

Curlの例の追加入力パラメータ

すべての REST API 呼び出しに共通するパラメータに加えて、この手順の curl の例では次のパラメータも使用されます。

パラメータ	を入力します	必須	説明
\$JOB_ID	パス	はい。	要求されているジョブを識別するために必要です。

カールの例

```
curl --request GET \  
--location "https://$FQDN_IP/api/cluster/jobs/$JOB_ID" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 出力例

stateの値とその他のフィールドは、返されるジョブオブジェクトに含まれます。この例のジョブは、ONTAP クラスタ更新の一環として実行されました。

```
{
  "uuid": "d877f5bb-3aa7-11e9-b6c6-005056a78c89",
  "description": "PATCH /api/cluster",
  "state": "success",
  "message": "success",
  "code": 0,
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/d877f5bb-3aa7-11e9-b6c6-005056a78c89"
    }
  }
}
```

NAS

ファイルセキュリティ権限

ONTAP REST APIを使用してファイルセキュリティと監査ポリシーを管理するための準備

ONTAP クラスタ内の SVM から使用可能なファイルの権限と監査ポリシーを管理できません。

概要

ONTAP では、システムアクセス制御リスト (SACL) と随意アクセス制御リスト (DACL) を使用してファイルオブジェクトに権限を割り当てます。ONTAP 9.9.1 以降では、REST API で SACL と DACL の権限の管理がサポートされます。API を使用すると、ファイルセキュリティ権限の管理を自動化できます。多くの場合、複数の CLI コマンドや ONTAPI (ZAPI) 呼び出しではなく、1 つの REST API 呼び出しを使用できます。



9.9.1 より前の ONTAP リリースでは、CLI パススルー機能を使用して、SACL および DACL 権限の管理を自動化できます。を参照してください ["移行に関する考慮事項"](#) および ["ONTAP REST API でプライベート CLI パススルーを使用する"](#) を参照してください。

REST API を使用して ONTAP ファイルセキュリティサービスを管理する方法を示すワークフローの例をいくつか紹介します。ワークフローを使用して REST API 呼び出しを実行する前に、["ワークフローを使用する準備をします"](#)。

Python を使用する場合は、スクリプトも参照してください。 ["file_security_permissions.py"](#) ファイルセキュリティアクティビティの一部を自動化する方法の例を参照してください。

ONTAP REST API コマンドと ONTAP CLI コマンドの比較

多くのタスクで、ONTAP REST API を使用する場合、同等の ONTAP CLI コマンドや ONTAPI (ZAPI) 呼び出しよりも少ない呼び出しで済みます。次の表に、API 呼び出しと、各タスクに必要な CLI コマンドを示します。

ONTAP REST API	ONTAP CLI
「 get/protocols/file-security/effected-permissions/ 」	vserver security file-directory show-effectuated-permissions
「 POST/protocols /file-security /permissions/ 」	<ol style="list-style-type: none"> 1. 「 vserver security file-directory ntfs create 」 2. vserver security file-directory ntfs dacl add 3. vserver security file-directory ntfs sacl add 4. 「 vserver security file-directory policy create 」 5. vserver security file-directory policy task add 6. 「 vserver security file-directory apply 」
patch/protocols/file-security/permissions/	vserver security file-directory ntfs modify
'delete/protocols/file-security/permissions/	<ol style="list-style-type: none"> 1. 「 vserver security file-directory ntfs dacl remove 」 2. 「 vserver security file-directory ntfs sacl remove 」

関連情報

- ["ファイル権限を示すPythonスクリプト"](#)
- ["ONTAP REST API を使用してファイルセキュリティ権限を簡単に管理できます"](#)
- ["ONTAP REST API でプライベート CLI パススルーを使用する"](#)

ONTAP REST APIを使用して、ファイルに対して有効な権限を取得する

特定のファイルまたはフォルダに対して現在有効な権限を取得できます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/protocols/file-security/effective-permissions/ {svm.uuid} / {path}

処理のタイプ

同期

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
\$SVM_ID	パス	はい。	これは、ファイルが含まれているSVMのUUIDです。
\$file_path	パス	はい。	ファイルまたはフォルダへのパスです。

カールの例

```
curl --request GET \  
--location "https://$FQDN_IP/api/protocols/file-security/effective-  
permissions/$SVM_ID/$FILE_PATH" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 出力例

```
{
  "svm": {
    "uuid": "cf5f271a-1beb-11ea-8fad-005056bb645e",
    "name": "vs1"
  },
  "user": "administrator",
  "type": "windows",
  "path": "/",
  "share": {
    "path": "/"
  },
  "file_permission": [
    "read",
    "write",
    "append",
    "read_ea",
    "write_ea",
    "execute",
    "delete_child",
    "read_attributes",
    "write_attributes",
    "delete",
    "read_control",
    "write_dac",
    "write_owner",
    "synchronize",
    "system_security"
  ],
  "share_permission": [
    "read",
    "read_ea",
    "execute",
    "read_attributes",
    "read_control",
    "synchronize"
  ]
}
```

ONTAP REST APIを使用したファイルの監査情報の取得

特定のファイルまたはフォルダの監査情報を取得できます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/protocols/file-security/permissions/ {svm.uuid} / {path}

処理のタイプ

同期

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
\$SVM_ID	パス	はい。	これは、ファイルが含まれているSVMのUUIDです。
\$file_path	パス	はい。	ファイルまたはフォルダへのパスです。

カールの例

```
curl --request GET \
--location "https://$FQDN_IP/api/protocols/file-
security/permissions/$SVM_ID/$FILE_PATH" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 出力例

```
{
  "svm": {
    "uuid": "9479099d-5b9f-11eb-9c4e-0050568e8682",
    "name": "vs1"
  },
  "path": "/parent",
  "owner": "BUILTIN\\Administrators",
  "group": "BUILTIN\\Administrators",
  "control_flags": "0x8014",
  "acls": [
    {
      "user": "BUILTIN\\Administrators",
      "access": "access_allow",
      "apply_to": {
        "files": true,
        "sub_folders": true,
        "this_folder": true
      },
      "advanced_rights": {
```



```

    "append_data": true,
    "delete": true,
    "delete_child": true,
    "execute_file": true,
    "full_control": true,
    "read_attr": true,
    "read_data": true,
    "read_ea": true,
    "read_perm": true,
    "write_attr": true,
    "write_data": true,
    "write_ea": true,
    "write_owner": true,
    "synchronize": true,
    "write_perm": true
  },
  "access_control": "file_directory"
},
{
  "user": "BUILTIN\\Users",
  "access": "access_allow",
  "apply_to": {
    "files": true,
    "sub_folders": true,
    "this_folder": true
  },
  "advanced_rights": {
    "append_data": true,
    "delete": true,
    "delete_child": true,
    "execute_file": true,
    "full_control": true,
    "read_attr": true,
    "read_data": true,
    "read_ea": true,
    "read_perm": true,
    "write_attr": true,
    "write_data": true,
    "write_ea": true,
    "write_owner": true,
    "synchronize": true,
    "write_perm": true
  },
  "access_control": "file_directory"
}
],

```

```

    "inode": 64,
    "security_style": "mixed",
    "effective_style": "ntfs",
    "dos_attributes": "10",
    "text_dos_attr": "----D---",
    "user_id": "0",
    "group_id": "0",
    "mode_bits": 777,
    "text_mode_bits": "rwxrwxrwx"
}

```

ONTAP REST APIを使用してファイルに新しい権限を適用する

新しいセキュリティ記述子を特定のファイルまたはフォルダに適用できます。

手順1：新しい権限を適用する

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
投稿 (Post)	/api/protocols/file-security/permissions/ {svm.uuid} / {path}

処理のタイプ

非同期

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
\$SVM_ID	パス	はい。	これは、ファイルが含まれているSVMのUUIDです。
\$file_path	パス	はい。	ファイルまたはフォルダへのパスです。

カールの例

```
curl --request POST --location "https://$FQDN_IP/api/protocols/file-security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include --header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data '{ \"acls\": [ { \"access\": \"access_allow\", \"advanced_rights\": { \"append_data\": true, \"delete\": true, \"delete_child\": true, \"execute_file\": true, \"full_control\": true, \"read_attr\": true, \"read_data\": true, \"read_ea\": true, \"read_perm\": true, \"write_attr\": true, \"write_data\": true, \"write_ea\": true, \"write_owner\": true, \"write_perm\": true }, \"apply_to\": { \"files\": true, \"sub_folders\": true, \"this_folder\": true }, \"user\": \"administrator\" } ], \"control_flags\": \"32788\", \"group\": \"S-1-5-21-2233347455-2266964949-1780268902-69700\", \"ignore_paths\": [ \"/parent/child2\" ], \"owner\": \"S-1-5-21-2233347455-2266964949-1780268902-69304\", \"propagation_mode\": \"propagate\"}'
```

JSON 出力例

```
{
  "job": {
    "uuid": "3015c294-5bbc-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/3015c294-5bbc-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

手順2：ジョブのステータスを取得する

ワークフローを実行 ["ジョブインスタンスの取得"](#) をクリックし、state 値は success。

ONTAP REST APIを使用したセキュリティ記述子情報の更新

特定のセキュリティ記述子を、プライマリ所有者、グループ、制御フラグなど、特定のファイルまたはフォルダに対して更新できます。

手順1：セキュリティ記述子を更新する

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
パッチ	/api/protocols/file-security/permissions/ {svm.uuid} / {path}

処理のタイプ

非同期

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
\$SVM_ID	パス	はい。	これは、ファイルが含まれているSVMのUUIDです。
\$file_path	パス	はい。	ファイルまたはフォルダへのパスです。

カールの例

```
curl --request POST --location "https://$FQDN_IP/api/protocols/file-security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include --header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data '{"control_flags": "32788", "group": "everyone", "owner": "user1"}'
```

JSON 出力例

```
{
  "job": {
    "uuid": "6f89e612-5bbd-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/6f89e612-5bbd-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

手順2：ジョブのステータスを取得する

ワークフローを実行 ["ジョブインスタンスの取得"](#) をクリックし、state 値は success。

ONTAP REST APIを使用してアクセス制御エントリを削除する

特定のファイルまたはフォルダから既存のAccess Control Entry (ACE；アクセス制御エントリ) を削除できます。変更はすべての子オブジェクトに伝播されます。

手順1：ACEの削除

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
削除	/api/protocols/file-security/permissions/ {svm.uuid} / {path}

処理のタイプ

非同期

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
\$SVM_ID	パス	はい。	これは、ファイルが含まれているSVMのUUIDです。
\$file_path	パス	はい。	ファイルまたはフォルダへのパスです。

カールの例

```
curl --request DELETE --location "https://$FQDN_IP/api/protocols/file-security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include --header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data '{ \"access\": \"access_allow\", \"apply_to\": { \"files\": true, \"sub_folders\": true, \"this_folder\": true }, \"ignore_paths\": [ \"/parent/child2\" ], \"propagation_mode\": \"propagate\"}'
```

JSON 出力例

```
{
  "job": {
    "uuid": "3015c294-5bbc-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/3015c294-5bbc-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

手順2：ジョブのステータスを取得する

ワークフローを実行 ["ジョブインスタンスの取得"](#) をクリックし、state 値は success。

ネットワーキング

ONTAP REST APIを使用したIPインターフェイスの一覧表示

クラスタおよびSVMに割り当てられているIP LIFを取得できます。この操作は、ネットワーク設定を確認する場合や、別のLIFを追加する場合に実行します。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/network/ip/interfaces

処理のタイプ

同期

Curlの例の追加入力パラメータ

すべての REST API 呼び出しに共通するパラメータに加えて、この手順の curl の例では次のパラメータも使用されます。

パラメータ	を入力します	必須	説明
フィールド	クエリ	いいえ	関連する設定値の限定されたリストを返します。

curlの例：すべてのLIFをデフォルトの設定値で返す

```
curl --request GET \  
--location "https://$FQDN_IP/api/network/ip/interfaces" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

curlの例：特定の4つの設定値を持つすべてのLIFを返す

```
curl --request GET \  
--location \  
"https://$FQDN_IP/api/network/ip/interfaces?fields=name,scope,svm.name,ip.  
address" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

```
{
  "records": [
    {
      "uuid": "5ded9e38-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsrm-sr027o_mgmt1",
      "ip": {
        "address": "172.29.151.116"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/5ded9e38-999e-11ee-acad-005056ae6bd8"
        }
      }
    },
    {
      "uuid": "bb03c162-999e-11ee-acad-005056ae6bd8",
      "name": "cluster_mgmt",
      "ip": {
        "address": "172.29.186.156"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/bb03c162-999e-11ee-acad-005056ae6bd8"
        }
      }
    },
    {
      "uuid": "c5ffbd03-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsrm-sr027o_data1",
      "ip": {
        "address": "172.29.186.150"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c5ffbd03-999e-11ee-acad-
```

```

005056ae6bd8"
  }
}
},
{
  "uuid": "c6612abe-999e-11ee-acad-005056ae6bd8",
  "name": "sti214-vsrm-sr027o_data2",
  "ip": {
    "address": "172.29.186.151"
  },
  "scope": "svm",
  "svm": {
    "name": "vs0"
  },
  "_links": {
    "self": {
      "href": "/api/network/ip/interfaces/c6612abe-999e-11ee-acad-
005056ae6bd8"
    }
  }
},
{
  "uuid": "c6b21b94-999e-11ee-acad-005056ae6bd8",
  "name": "sti214-vsrm-sr027o_data3",
  "ip": {
    "address": "172.29.186.152"
  },
  "scope": "svm",
  "svm": {
    "name": "vs0"
  },
  "_links": {
    "self": {
      "href": "/api/network/ip/interfaces/c6b21b94-999e-11ee-acad-
005056ae6bd8"
    }
  }
},
{
  "uuid": "c7025322-999e-11ee-acad-005056ae6bd8",
  "name": "sti214-vsrm-sr027o_data4",
  "ip": {
    "address": "172.29.186.153"
  },
  "scope": "svm",
  "svm": {

```



```

    "name": "vs0"
  },
  "_links": {
    "self": {
      "href": "/api/network/ip/interfaces/c7025322-999e-11ee-acad-005056ae6bd8"
    }
  }
},
{
  "uuid": "c752cc66-999e-11ee-acad-005056ae6bd8",
  "name": "sti214-vsimsr027o_data5",
  "ip": {
    "address": "172.29.186.154"
  },
  "scope": "svm",
  "svm": {
    "name": "vs0"
  },
  "_links": {
    "self": {
      "href": "/api/network/ip/interfaces/c752cc66-999e-11ee-acad-005056ae6bd8"
    }
  }
},
{
  "uuid": "c7a03719-999e-11ee-acad-005056ae6bd8",
  "name": "sti214-vsimsr027o_data6",
  "ip": {
    "address": "172.29.186.155"
  },
  "scope": "svm",
  "svm": {
    "name": "vs0"
  },
  "_links": {
    "self": {
      "href": "/api/network/ip/interfaces/c7a03719-999e-11ee-acad-005056ae6bd8"
    }
  }
},
{
  "uuid": "ccd4c59c-999e-11ee-acad-005056ae6bd8",
  "name": "sti214-vsimsr027o_data4_inet6",

```

```

    "ip": {
      "address": "fd20:8b1e:b255:300f::ac5"
    },
    "scope": "svm",
    "svm": {
      "name": "vs0"
    },
    "_links": {
      "self": {
        "href": "/api/network/ip/interfaces/ccd4c59c-999e-11ee-acad-005056ae6bd8"
      }
    }
  },
  {
    "uuid": "d9144c30-999e-11ee-acad-005056ae6bd8",
    "name": "sti214-vsime-sr027o_data6_inet6",
    "ip": {
      "address": "fd20:8b1e:b255:300f::ac7"
    },
    "scope": "svm",
    "svm": {
      "name": "vs0"
    },
    "_links": {
      "self": {
        "href": "/api/network/ip/interfaces/d9144c30-999e-11ee-acad-005056ae6bd8"
      }
    }
  },
  {
    "uuid": "d961c13b-999e-11ee-acad-005056ae6bd8",
    "name": "sti214-vsime-sr027o_data1_inet6",
    "ip": {
      "address": "fd20:8b1e:b255:300f::ac2"
    },
    "scope": "svm",
    "svm": {
      "name": "vs0"
    },
    "_links": {
      "self": {
        "href": "/api/network/ip/interfaces/d961c13b-999e-11ee-acad-005056ae6bd8"
      }
    }
  }
}

```

```

    }
  },
  {
    "uuid": "d9ac8d6a-999e-11ee-acad-005056ae6bd8",
    "name": "sti214-vsim-sr027o_data5_inet6",
    "ip": {
      "address": "fd20:8b1e:b255:300f::ac6"
    },
    "scope": "svm",
    "svm": {
      "name": "vs0"
    },
    "_links": {
      "self": {
        "href": "/api/network/ip/interfaces/d9ac8d6a-999e-11ee-acad-005056ae6bd8"
      }
    }
  },
  {
    "uuid": "d9fc1a3-999e-11ee-acad-005056ae6bd8",
    "name": "sti214-vsim-sr027o_data2_inet6",
    "ip": {
      "address": "fd20:8b1e:b255:300f::ac3"
    },
    "scope": "svm",
    "svm": {
      "name": "vs0"
    },
    "_links": {
      "self": {
        "href": "/api/network/ip/interfaces/d9fc1a3-999e-11ee-acad-005056ae6bd8"
      }
    }
  },
  {
    "uuid": "da4995a0-999e-11ee-acad-005056ae6bd8",
    "name": "sti214-vsim-sr027o_data3_inet6",
    "ip": {
      "address": "fd20:8b1e:b255:300f::ac4"
    },
    "scope": "svm",
    "svm": {
      "name": "vs0"
    },
  },

```

```

    "_links": {
      "self": {
        "href": "/api/network/ip/interfaces/da4995a0-999e-11ee-acad-005056ae6bd8"
      }
    },
    {
      "uuid": "da9e7afd-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsrm-sr027o_cluster_mgmt_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac8"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/da9e7afd-999e-11ee-acad-005056ae6bd8"
        }
      }
    },
    {
      "uuid": "e6db58b4-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsrm-sr027o_mgmt1_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:3008::1a0"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/e6db58b4-999e-11ee-acad-005056ae6bd8"
        }
      }
    }
  ],
  "num_records": 16,
  "_links": {
    "self": {
      "href":
"/api/network/ip/interfaces?fields=name,scope,svm.name,ip.address"
    }
  }
}

```

セキュリティ

アカウント

ONTAP REST APIを使用してアカウントを表示する

アカウントのリストを取得できます。これは、セキュリティ環境を評価するため、または新しいアカウントを作成する前に行うことができます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/security/accounts (/api/security/アカウント)

処理のタイプ

同期

カールの例

```
curl --request GET \  
--location "https://$FQDN_IP/api/security/accounts" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 出力例

```
{
  "records": [
    {
      "owner": {
        "uuid": "642573a8-9d14-11ee-9330-005056aed3de",
        "name": "vs0",
        "_links": {
          "self": {
            "href": "/api/svm/svms/642573a8-9d14-11ee-9330-005056aed3de"
          }
        }
      },
      "name": "vsadmin",
      "_links": {
        "self": {
          "href": "/api/security/accounts/642573a8-9d14-11ee-9330-005056aed3de/vsadmin"
        }
      }
    },
    {
      "owner": {
        "uuid": "fdb6fe29-9d13-11ee-9330-005056aed3de",
        "name": "sti214nscluster-1"
      },
      "name": "admin",
      "_links": {
        "self": {
          "href": "/api/security/accounts/fdb6fe29-9d13-11ee-9330-005056aed3de/admin"
        }
      }
    },
    {
      "owner": {
        "uuid": "fdb6fe29-9d13-11ee-9330-005056aed3de",
        "name": "sti214nscluster-1"
      },
      "name": "autosupport",
      "_links": {
        "self": {
          "href": "/api/security/accounts/fdb6fe29-9d13-11ee-9330-
```

```

005056aed3de/autosupport"
    }
  }
},
"num_records": 3,
"_links": {
  "self": {
    "href": "/api/security/accounts"
  }
}
}
}

```

証明書とキー

ONTAP REST APIを使用してインストールされている証明書を表示する

ONTAP クラスタにインストールされている証明書を表示できます。これは、特定の証明書が使用可能かどうかを確認したり、特定の証明書のIDを取得したりするために実行します。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/security/certificates

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
max_records	クエリ	いいえ	返されるレコードの数を指定します。

curlの例：3つの証明書を返す

```

curl --request GET \
--location "https://$FQDN_IP/api/security/certificates?max_records=3" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"

```

JSON 出力例

```
{
  "records": [
    {
      "uuid": "dad822c2-573c-11ee-a310-005056aecc29",
      "name": "vs0_17866DB5C933E2EA",
      "_links": {
        "self": {
          "href": "/api/security/certificates/dad822c2-573c-11ee-a310-005056aecc29"
        }
      }
    },
    {
      "uuid": "7d8e5570-573c-11ee-a310-005056aecc29",
      "name": "BuypassClass3RootCA",
      "_links": {
        "self": {
          "href": "/api/security/certificates/7d8e5570-573c-11ee-a310-005056aecc29"
        }
      }
    },
    {
      "uuid": "7dbb2191-573c-11ee-a310-005056aecc29",
      "name": "EntrustRootCertificationAuthority",
      "_links": {
        "self": {
          "href": "/api/security/certificates/7dbb2191-573c-11ee-a310-005056aecc29"
        }
      }
    }
  ],
  "num_records": 3,
  "_links": {
    "self": {
      "href": "/api/security/certificates?max_records=3"
    },
    "next": {
      "href": "/api/security/certificates?start.svm_id=sti214nscluster-1&start.uuid=7dbb2191-573c-11ee-a310-005056aecc29&max_records=3"
    }
  }
}
```


ONTAP REST APIを使用した証明書のインストール

署名済みX.509証明書をONTAPクラスタにインストールできます。これは、強力な認証を必要とするONTAP機能またはプロトコルの設定の一環として行うことができます。

作業を開始する前に

インストールする証明書が必要です。また、必要に応じて中間証明書がインストールされていることを確認してください。



以下に示すJSON入力例を使用する前に、 `public_certificate` 環境の証明書を使用して値を設定します。

手順1：証明書をインストールする

API呼び出しを問題して証明書をインストールできます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
投稿 (Post)	/api/security/certificates

cURLの例：ルート**CA**証明書をクラスタレベルでインストールする

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/certificates" \  
--include \  
--header "Content-Type: application/json" \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON の入力例

```
{
  "type": "server_ca",
  "public_certificate":
    "-----BEGIN CERTIFICATE-----
MIID0TCCArkCFGYdznvTVvaY1VZPNfy4yCCyPph6MA0GCSqGSIb3DQEBCwUAMIGk
MQswCQYDVQQGEwJVUzELMAkGA1UECAwCTkMxDDAKBgNVBACMA1JUUDEWMBQGA1UE
CgwNT05UQVAgRXhhbXBsZTETMBEGA1UECwwKT05UQVAgOS4xNDEcMBoGA1UEAwWT
Ki5vbnRhcC1leGFtcGxlLmNvbTEvMC0GCSqGSIb3DQEJARYgZGF2aWQucGV0ZXJz
b25Ab250YXAtZXhhbXBsZS5jb20wHhcNMjMxMDA1MTUyOTE4WhcNMjMxMDA0MTUy
OTE4WjCBpDELMAkGA1UEBhMCMVVMxMzA1BjBGNVBAgMAk5DMQwwCgYDVQQHDANSVFAX
FjAUBGNVBAoMDU9OVEFQIEV4YW1wbGUxEzARBGNVBAcMCK9OVEFQIDkuMTQxHDAa
BgNVBAMMEyoub250YXAtZXhhbXBsZS5jb20xLzAtBgkqhkiG9w0BCQEWIGRhdm1k
LnBlldGVyc29uQG9udGFwLWV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOc
AQ8AMIIBCgKCAQEAXQgy8mhb1Jhkf0D/MBodpZgW0aSp2jGbWJ+Zv2G8BXkp1762
dPHRkv1hnx9JvwkK4Dba05GiCiD5t3gjH/jUQMSFb+VwDbVmubVFnXjkm/4Q7sea
tMtA/ZpQdZbQFZ5RKtdWz7dzZPYEl2x8Q1Jc8Kh7NxERNMtgupGWZzn7mfXKYr4O
N/+vgahIhDibS8YK5rflw6bfmrik9E2D+PEab9DX/1DL5RX4tZ1H2OkyN2UxoBR6
Fq7l6n1Hi/5yR0OilxStN6s07EPoGak+KSlK41q+EcIKRo0bP4mEQp8WMjJuiTkb
5MmeYoIpWEUgJK7S0M6Tp/3bTh2CST3AWxiNxQIDAQABMA0GCSqGSIb3DQEBCwUA
A4IBAQAQABfBqOuR0mYxdfRj930yIiRoDcoMzvo8cHGNUMsuhnlBDnL203qhWEs97s0
mIy6zFMGnyNYa0t4ilcFsGDKP/JuljmYHjvv+2lHWnxHjTo7AOQCnXmQH5swoDbf
o1Vjqz8Oxz+PRJ+PA3dF5/8zqaAR6QreAN/iFR++6nUq1sbbM7w03tthBVMgo/h1
E9I2jVOZsqMFujm2CYfMs4XkZtrYmN6nZA8JcUpDjIWcAVbQYurMnna9r42oS3GB
WB/FE9n+P+FfJyHJ93KGcCXbH5RF2pi3wLlHilbvVuCjLRrhJ8U20I5mZoiXvAbc
IpYuBcuKXLwAarhDEacXttVjC+Bq
-----END CERTIFICATE-----"
}
```

手順2：証明書がインストールされたことを確認する

ワークフローを実行 ["インストールされている証明書を表示"](#) 証明書が利用可能であることを確認します。

RBAC

ONTAP REST APIを使用して**RBAC**を使用するための準備

ONTAP RBAC機能は、環境に応じていくつかの方法で使用できます。このセクションでは、いくつかの一般的なシナリオをワークフローとして紹介します。いずれの場合も、特定のセキュリティおよび管理上の目標に焦点を当てています。

ロールを作成してONTAPユーザアカウントにロールを割り当てる前に、次に示す主なセキュリティ要件とオプションを確認して準備しておく必要があります。また、次のWebサイトで一般的なワークフローの概念を確認してください。 ["ワークフローを使用する準備をします"](#)。

どのONTAP リリースを使用していますか？

ONTAP リリースによって、使用可能なRESTエンドポイントとRBAC機能が決まります。

保護対象のリソースと範囲を特定

保護対象のリソースまたはコマンドとその範囲（クラスタまたはSVM）を特定する必要があります。

ユーザにはどのようなアクセス権が必要ですか。

リソースと範囲を特定したら、許可するアクセスレベルを決定する必要があります。

ユーザはどのように**ONTAP** にアクセスしますか。

ユーザはREST API、CLI、またはその両方を使用してONTAP にアクセスできます。

組み込みの役割の1つで十分か、またはカスタムの役割が必要か。

既存の組み込みロールを使用する方が便利ですが、必要に応じて新しいカスタムロールを作成することもできます。

どのような種類の役割が必要ですか？

セキュリティ要件とONTAP アクセスに基づいて、RESTと従来のどちらのロールを作成するかを選択する必要があります。

ロールの作成

ONTAP REST APIを使用して**SVM**ボリューム処理へのアクセスを制限する

SVM内でのストレージボリュームの管理を制限するロールを定義できます。

このワークフローについて

最初に、クローニングを除くすべての主要なボリューム管理機能へのアクセスを許可するために、トラディショナルロールが作成されます。ロールは次の特性で定義されます。

- GET、CREATE、MODIFY、DELETEなどのCRUDボリューム操作をすべて実行できる
- ボリュームクローンを作成できません

その後、必要に応じてロールを更新できます。このワークフローでは、2番目の手順でロールが変更され、ユーザがボリュームクローンを作成できるようになります。

手順1：ロールを作成する

API呼び出しを問題してRBACロールを作成できます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
投稿（Post）	/api/security/rolesのように入力します

カールの例

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON の入力例

```
{  
  "name": "role1",  
  "owner": {  
    "name": "cluster-1",  
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"  
  },  
  "privileges": [  
    { "path": "volume create", "access": "all" },  
    { "path": "volume delete", "access": "all" }  
  ]  
}
```

手順2：ロールを更新する

API呼び出しを問題して既存のロールを更新できます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
投稿 (Post)	/api/security/rolesのように入力します

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
\$SVM_ID	パス	はい。	これは、ロールの定義が含まれているSVMのUUIDです。
\$ロール名	パス	はい。	更新するSVM内のロールの名前を指定します。

カールの例

```
curl --request POST \  
--location  
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/priveleges" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON の入力例

```
{  
  "path": "volume clone",  
  "access": "all"  
}
```

ONTAP REST APIを使用したデータ保護の管理

ユーザに提供できるデータ保護機能は限られています。

このワークフローについて

従来のロールは、次の特性で定義されます。

- Snapshotの作成と削除、およびSnapMirror関係の更新が可能です
- ボリュームやSVMなどの上位のオブジェクトを作成または変更することはできません

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
投稿 (Post)	/api/security/rolesのように入力します

カールの例

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON の入力例

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    {"path": "volume snapshot create", "access": "all"},
    {"path": "volume snapshot delete", "access": "all"},
    {"path": "volume show", "access": "readonly"},
    {"path": "vserver show", "access": "readonly"},
    {"path": "snapmirror show", "access": "readonly"},
    {"path": "snapmirror update", "access": "all"}
  ]
}
```

ONTAP REST APIを使用したONTAPレポートの生成を許可する

ONTAP レポートを生成する機能をユーザに提供するRESTロールを作成できます。

このワークフローについて

作成されるロールは、次の特性で定義されます。

- 容量とパフォーマンス（ボリューム、qtree、LUN、アグリゲート、ノード、 SnapMirror関係の場合）
- 上位のオブジェクト（ボリュームやSVMなど）を作成または変更できない

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
投稿（Post）	/api/security/rolesのように入力します

カールの例

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON の入力例

```
{
  "name": "rest_role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    {"path": "/api/storage/volumes", "access": "readonly"},
    {"path": "/api/storage/qtrees", "access": "readonly"},
    {"path": "/api/storage/luns", "access": "readonly"},
    {"path": "/api/storage/aggregates", "access": "readonly"},
    {"path": "/api/cluster/nodes", "access": "readonly"},
    {"path": "/api/snapmirror/relationships", "access": "readonly"},
    {"path": "/api/svm/svms", "access": "readonly"}
  ]
}
```

ONTAP REST APIを使用してロールを持つユーザを作成する

このワークフローを使用して、RESTロールを関連付けたユーザを作成できます。

このワークフローについて

このワークフローには、カスタムRESTロールを作成して新しいユーザアカウントに関連付けるために必要な一般的な手順が含まれています。ユーザとロールの両方にSVMスコープがあり、特定のデータSVMに関連付けられています。一部の手順はオプションである場合もあれば、環境に応じて変更する必要がある場合もあります。

手順1：クラスタ内のデータSVMをリストする

次のREST API呼び出しを実行して、クラスタ内のSVMを表示します。各SVMのUUIDと名前が出力に表示されます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/SVM/SVMs

カールの例

```
curl --request GET \  
--location "https://$FQDN_IP/api/svm/svms?order_by=name" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

完了後

リストから必要なSVMを選択し、新しいユーザとロールを作成します。

手順2: SVMに定義されているユーザを表示する

選択したSVMで定義されているユーザを表示するために、次のREST API呼び出しを実行します。SVMは、ownerパラメータを使用して識別できます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/security/accounts (/api/security/アカウント)

カールの例

```
curl --request GET \  
--location "https://$FQDN_IP/api/security/accounts?owner.name=dmp" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

完了後

SVMですでに定義されているユーザに基づいて、新しいユーザの一意の名前を選択します。

手順3: SVMに定義されているRESTロールを表示する

次のREST API呼び出しを実行し、選択したSVMで定義されているロールをリストします。SVMは、ownerパラメータを使用して識別できます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/security/rolesのように入力します

カールの例

```
curl --request GET \  
--location "https://$FQDN_IP/api/security/roles?owner.name=dmp" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

完了後

SVMですでに定義されているロールに基づいて、新しいロールに一意の名前を選択します。

手順4：カスタムRESTロールを作成する

次のREST API呼び出しを実行して、SVMでカスタムのRESTロールを作成します。最初は権限を1つしか持たず、すべてのアクセスが拒否されるようにするために、このロールにはデフォルトのアクセスである* none * が設定されます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
投稿 (Post)	/api/security/rolesのように入力します

カールの例

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON の入力例

```
{  
  "name": "dprole1",  
  "owner": {  
    "name": "dmp",  
    "uuid": "752d96be-f17c-11ec-9d19-005056bbad91"  
  },  
  "privileges": [  
    {"path": "/api", "access": "none"},  
  ]  
}
```

完了後

必要に応じて、手順3をもう一度実行して新しいロールを表示します。ONTAP CLIでもロールを表示できません。

手順5：権限を追加してロールを更新する

必要に応じて権限を追加してロールを変更するには、次のREST API呼び出しを実行します。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
投稿 (Post)	/api/security/roles/ {owner.uuid} / {name} /privileges

curlの例の追加入力パラメータ

この手順のcurlの例では、すべてのREST API呼び出しに共通のパラメータに加えて、次のパラメータも使用しています。

パラメータ	を入力します	必須	説明
\$SVM_ID	パス	はい。	ロールの定義が含まれているSVMのUUID。
\$ロール名	パス	はい。	更新するSVM内のロールの名前を指定します。

カールの例

```
curl --request POST \  
--location \  
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/privileges" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON の入力例

```
{  
  "path": "/api/storage/volumes",  
  "access": "readonly"  
}
```

完了後

必要に応じて、手順3をもう一度実行して新しいロールを表示します。ONTAP CLIでもロールを表示できません。

手順6：ユーザを作成する

ユーザアカウントを作成するには、次のREST API呼び出しを実行します。上で作成したロール*dprole1*は、新しいユーザに関連付けられています。



ロールを指定せずにユーザを作成できます。この場合、ユーザにはデフォルトのロール（admin または vsadmin）ユーザがクラスタスコープとSVMスコープのどちらで定義されているかに応じて変わります。別のロールを割り当てるには、ユーザを変更する必要があります。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
投稿（Post）	/api/security/accounts (/api/security/アカウント)

カールの例

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/accounts" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON の入力例

```
{  
  "owner": {"uuid": "daf84055-248f-11ed-a23d-005056ac4fe6"},  
  "name": "david",  
  "applications": [  
    {"application": "ssh",  
      "authentication_methods": ["password"],  
      "second_authentication_method": "none"}  
  ],  
  "role": "dprole1",  
  "password": "netapp123"  
}
```

完了後

SVM管理インターフェイスにサインインするには、新しいユーザのクレデンシャルを使用します。

ストレージ

ONTAP REST APIを使用してアグリゲートを表示する

クラスタ内のアグリゲートのリストを取得できます。これは、利用率とパフォーマンスを評価するために行うことができます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/API/ストレージ/ディスク

処理のタイプ

同期

Curlの例の追加入力パラメータ

すべての REST API 呼び出しに共通するパラメータに加えて、この手順の curl の例では次のパラメータも使用されます。

パラメータ	を入力します	必須	説明
node.name	クエリ	いいえ	を使用して、各アグリゲートが接続されているノードを特定できます。

curlの例：デフォルトの設定値を使用してすべてのアグリゲートを返す

```
curl --request GET \  
--location "https://$FQDN_IP/api/storage/aggregates" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

curlの例：特定の設定値を持つすべてのアグリゲートを返す

```
curl --request GET \  
--location "https://$FQDN_IP/api/storage/aggregates?fields=node.name" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 出力例

```
{
  "records": [
    {
      "uuid": "760d8137-fc59-47da-906a-cc28db0a1c1b",
      "name": "sti214_vsim_sr027o_aggr1",
      "node": {
        "name": "sti214-vsimsr027o"
      },
      "_links": {
        "self": {
          "href": "/api/storage/aggregates/760d8137-fc59-47da-906a-cc28db0a1c1b"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/storage/aggregates?fields=node.name"
    }
  }
}
```

ONTAP REST APIを使用してディスクを表示する

クラスタ内のディスクのリストを取得できます。この操作は、アグリゲートの作成時に使用する1つ以上のスペアを特定する場合に行います。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/API/ストレージ/ディスク

処理のタイプ

同期

Curlの例の追加入力パラメータ

すべての REST API 呼び出しに共通するパラメータに加えて、この手順の curl の例では次のパラメータも使用されます。

パラメータ	を入力します	必須	説明
状態	クエリ	いいえ	を使用すると、新しいアグリゲートに使用できるスペアディスクを特定できます。

curlの例：すべてのディスクを返す

```
curl --request GET \  
--location "https://$FQDN_IP/api/storage/disks" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

curlの例：スペアディスクを返す

```
curl --request GET \  
--location "https://$FQDN_IP/api/storage/disks?state=spare" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 出力例

```
{
  "records": [
    {
      "name": "NET-1.20",
      "state": "spare",
      "_links": {
        "self": {
          "href": "/api/storage/disks/NET-1.20"
        }
      }
    },
    {
      "name": "NET-1.12",
      "state": "spare",
      "_links": {
        "self": {
          "href": "/api/storage/disks/NET-1.12"
        }
      }
    },
    {
      "name": "NET-1.7",
      "state": "spare",
      "_links": {
        "self": {
          "href": "/api/storage/disks/NET-1.7"
        }
      }
    }
  ],
  "num_records": 3,
  "_links": {
    "self": {
      "href": "/api/storage/disks?state=spare"
    }
  }
}
```

サポート

EMS

ONTAP REST APIを使用してEMSサポートサービスを管理する準備

ONTAPクラスタのイベント管理システム（EMS）処理を設定し、必要に応じてEMSメッセージを取得できます。

概要

ここでは、ONTAP EMSサービスの使用方法を示すワークフローの例をいくつか紹介します。ワークフローを使用してREST API呼び出しを実行する前に、["ワークフローを使用する準備をします"](#)。

Pythonを使用する場合は、スクリプトも参照してください。 ["events.py"](#) EMS関連の一部のアクティビティを自動化する方法の例を参照してください。

ONTAP REST API コマンドと ONTAP CLI コマンドの比較

多くのタスクでは、ONTAP REST APIを使用すると、同等のONTAP CLIコマンドよりも少ない呼び出しで済みます。次の表に、API呼び出しと、各タスクに必要なCLIコマンドを示します。

ONTAP REST API	ONTAP CLI
GET /support/ems	event config show
ポスト/サポート/EMS /デステイネーション	1. イベント通知の送信先を作成します 2. イベント通知は "" を作成します
「 get/support/ems/events 」	「 event log show 」を参照してください
「 POST/support/ems/filters 」と入力します	1. 'event filter create -filter-name <filtername>` 2. 'event filter rule add-filter-name <filtername>`

関連情報

- ["EMSを示すPythonスクリプト"](#)
- ["ONTAP REST API：重大度の高いイベントの通知を自動化します"](#)

ONTAP REST APIを使用したEMSログイベントの一覧表示

すべてのイベント通知メッセージを取得することも、特定の特性を持つメッセージのみを取得することもできます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/support/ems/events

処理のタイプ

同期

Curlの例の追加入力パラメータ

すべての REST API 呼び出しに共通するパラメータに加えて、この手順の curl の例では次のパラメータも使用されます。

パラメータ	を入力します	必須	説明
フィールド	クエリ	いいえ	応答に含める特定のフィールドを要求するために使用されます。
max_records	クエリ	いいえ	1回の要求で返されるレコード数を制限するために使用できます。
LOG_MESSAGE	クエリ	いいえ	特定のテキスト値を検索し、一致するメッセージのみを返します。
message.severity	クエリ	いいえ	返されるメッセージは、次のような特定の重大度のメッセージだけに制限します。 alert。

curlの例:最新のメッセージと名前の値を返す

```
curl --request GET \  
--location \  
"https://$FQDN_IP/api/support/ems/events?fields=message.name&max_records=1" \  
\  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

curlの例:特定のテキストと重大度を含むメッセージを返す

```
curl --request GET \  
--location \  
"https://$FQDN_IP/api/support/ems/events?log_message=*disk*&message.severity=alert" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 出力例

```
{
  "records": [
    {
      "node": {
        "name": "malha-vsimg1",
        "uuid": "da4f9e62-9de3-11ec-976a-005056b369de",
        "_links": {
          "self": {
            "href": "/api/cluster/nodes/da4f9e62-9de3-11ec-976a-005056b369de"
          }
        }
      },
      "index": 4602,
      "time": "2022-03-18T06:37:46-04:00",
      "message": {
        "severity": "alert",
        "name": "raid.autoPart.disabled"
      },
      "log_message": "raid.autoPart.disabled: Disk auto-partitioning is disabled on this system: the system needs a minimum of 4 usable internal hard disks.",
      "_links": {
        "self": {
          "href": "/api/support/ems/events/malha-vsimg1/4602"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/support/ems/events?log_message=*disk*&message.severity=alert&max_records=1"
    },
    "next": {
      "href": "/api/support/ems/events?start.keytime=2022-03-18T06%3A37%3A46-04%3A00&start.node.name=malha-vsimg1&start.index=4602&log_message=*disk*&message.severity=alert"
    }
  }
}
```

ONTAP REST APIを使用したEMS設定の取得

ONTAPクラスタの現在のEMS設定を取得できます。この処理は、設定を更新する前や新しいEMS通知を作成する前に実行します。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/support/ems

処理のタイプ

同期

カールの例

```
curl --request GET \  
--location "https://$FQDN_IP/api/support/ems" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 出力例

```
{  
  "proxy_url": "https://proxyserver.mycompany.com",  
  "proxy_user": "proxy_user",  
  "mail_server": "mail@mycompany.com",  
  "_links": {  
    "self": {  
      "href": "/api/resourcelink"  
    }  
  },  
  "pubsub_enabled": "1",  
  "mail_from": "administrator@mycompany.com"  
}
```

ONTAP REST APIを使用したEMS通知の作成

次のワークフローを使用して、選択したイベントメッセージを受信する新しいEMS通知の送信先を作成できます。

手順1：システム全体のEメール設定を構成する

次のAPI呼び出しを問題して、システム全体のEメール設定を行うことができます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
パッチ	/api/support/ems

処理のタイプ

同期

Curlの例の追加入力パラメータ

すべての REST API 呼び出しに共通するパラメータに加えて、この手順の curl の例では次のパラメータも使用されます。

パラメータ	を入力します	必須	説明
メールの差出人	クエリ	はい。	を設定します。 from フィールドをクリックします。
メールサーバ	クエリ	はい。	ターゲットのSMTPメールサーバを設定します。

カールの例

```
curl --request PATCH \  
--location \  
"https://$FQDN_IP/api/support/ems?mail_from=administrator@mycompany.com&mail_server=mail@mycompany.com" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

手順2：メッセージフィルタを定義する

API呼び出しを問題して、メッセージに一致するフィルタルールを定義できます。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
投稿 (Post)	/api/support/ems/filters

処理のタイプ

同期

Curlの例の追加入力パラメータ

すべての REST API 呼び出しに共通するパラメータに加えて、この手順の curl の例では次のパラメータも使用されます。

パラメータ	を入力します	必須	説明
フィルタ	ボディ (Body)	はい。	フィルタ設定の値が含まれます。

カールの例

```
curl --request POST \
--location "https://$FQDN_IP/api/support/ems/filters" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON の入力例

```
{
  "name": "test-filter",
  "rules.type": ["include"],
  "rules.message_criteria.severities": ["emergency"]
}
```

手順3：メッセージの送信先を作成する

API呼び出しを問題して、メッセージの送信先を作成できません。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
投稿 (Post)	/api/support/ems/destinations

処理のタイプ

同期

Curlの例の追加入力パラメータ

すべての REST API 呼び出しに共通するパラメータに加えて、この手順の curl の例では次のパラメータも使用されます。

パラメータ	を入力します	必須	説明
デスティネーションの設定	ボディ (Body)	はい。	イベントの送信先の値が含まれます。

カールの例

```
curl --request POST \  
--location "https://$FQDN_IP/api/support/ems/destinations" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON の入力例

```
{  
  "name": "test-destination",  
  "type": "email",  
  "destination": "administrator@mycompany.com",  
  "filters.name": ["important-events"]  
}
```

SVM

ONTAP REST APIを使用してSVMを表示する

ONTAPクラスタ内で定義されているStorage Virtual Machine (SVM) をリストできます。この処理は、特定のSVMの識別子を検索する場合や、新しいSVMを作成する前に名前を一意にする場合に実行します。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTP メソッド	パス
取得	/api/SVM/SVMs

カールの例

```
curl --request GET \  
--location "https://$FQDN_IP/api/svm/svms" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 出力例

```
{
  "records": [
    {
      "uuid": "71bd74f8-40dc-11ee-b51a-005056aee9fa",
      "name": "vs0",
      "_links": {
        "self": {
          "href": "/api/svm/svms/71bd74f8-40dc-11ee-b51a-005056aee9fa"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/svm/svms"
    }
  }
}
```

ソフトウェアツール

Python クライアントライブラリ

ONTAP Pythonクライアントライブラリの詳細

NetApp ONTAP Pythonクライアントライブラリは、ONTAP REST APIにアクセスするスクリプトをすばやく記述するためにインストールして使用できるパッケージです。ローカルランタイム環境を使用する前に準備する必要があります。pip_utilityを使用して、Python Package Index (PyPI)サイトからパッケージをインストールできます。

関連情報

- ["ONTAP REST APIの詳細"](#)です。

機能とメリット

Pythonクライアントライブラリを使用すると、ONTAP環境の管理を自動化するための堅牢なコードを迅速に開発できます。次のようないくつかの基盤サービスを提供します。

- 接続管理
- 非同期処理
- 例外処理
- ユニフォームエラーメッセージ

パッケージとドキュメント

NetAppクライアントライブラリパッケージの名前は`_python-python_ONTAP`です。パッケージに関連付けられているバージョンは、ライブラリが生成されたONTAPのメジャーバージョン番号とマイナーバージョン番号、およびONTAPリリース内のクライアントライブラリのマイナーバージョンを組み合わせたものです。たとえば、有効なバージョン番号は9.6.1、9.6.2、9.7.1です。

9.6以降の各ONTAPリリースには、PyPIパッケージと関連ドキュメントが含まれています。インストール要件は各パッケージに含まれており、Python、requests、requests-toolbelt、marshmallowなどのサポートライブラリのバージョンを指定します。

ONTAP 9.16.1

- ["PyPI : NetApp ONTAP 9.16.1"](#)
- ["9.16.1のNetApp PCLドキュメント"](#)

ONTAP 9.15.1

- ["PyPI : NetApp ONTAP 9.15.1"](#)
- ["9.15.1用NetApp PCLドキュメント"](#)

ONTAP 9.14.1

- ["PyPI : NetApp ONTAP 9.14.1"](#)
- ["9.14.1用NetApp PCLドキュメント"](#)

ONTAP 9.13.1

- ["PyPI : NetApp ONTAP 9.13.1"](#)
- ["9.13.1用のNetApp PCLドキュメント"](#)

ONTAP 9.12.1

- ["PyPI : NetApp ONTAP 9.12.1"](#)
- ["9.12.1用NetApp PCLドキュメント"](#)

ONTAP 9.11.1

- ["PyPI : NetApp ONTAP 9.11.1"](#)
- ["9.11.1用のネットアップPCLドキュメント"](#)

ONTAP 9.10.1

- ["PyPI : NetApp ONTAP 9.10.1"](#)
- ["9.10.1用のネットアップ PCL ドキュメント"](#)

ONTAP 9.9.1

- ["PyPI : NetApp ONTAP 9.9.1"](#)
- ["9.9.1のNetApp PCLドキュメント"](#)

ONTAP 9.8

- ["PyPI : NetApp ONTAP 9.8"](#)
- ["9.8用NetApp PCLドキュメント"](#)

ONTAP 9.7

- ["PyPI : NetApp ONTAP 9.7"](#)
- ["9.7用NetApp PCLドキュメント"](#)

ONTAP 9.6

- ["PyPI : NetApp ONTAP 9.6"](#)

- ["NetApp PCLドキュメント \(9.6\) "](#)

コードサンプル

NetAppは、コードサンプルやその他の有用な情報を含むGitHubリポジトリを管理しています。python クライアント・ライブラリを使用してサンプルにアクセスするには、`_examples_folder` に移動します。詳細については、GitHubの次の場所を参照してください。

- ["ONTAP REST Python GitHub リポジトリ"](#)
- ["ONTAP REST Pythonクライアントライブラリの例"](#)

Pythonクライアントライブラリを使用してクラスタ構成を取得するスクリプト

次のスクリプトは、Python クライアントライブラリの使用方法の簡単な例を示しています。CLI で Python 3 を使用してスクリプトを実行すると、ONTAP クラスタ構成を取得できます。

```

##-----
#
# Description: Python script to retrieve the cluster configuration.
#
# Usage example:
#
# python3 get_cluster.py
#
#
# (C) Copyright 2025 NetApp, Inc.
#
# This sample code is provided AS IS, with no support or warranties of
# any kind, including but not limited for warranties of merchantability
# or fitness of any kind, expressed or implied. Permission to use,
# reproduce, modify and create derivatives of the sample code is granted
# solely for the purpose of researching, designing, developing and
# testing a software application product for use with NetApp products,
# provided that the above copyright notice appears in all copies and
# that the software application product is distributed pursuant to terms
# no less restrictive than those set forth herein.
#
##-----
# For reading the password from the commandline
from getpass import getpass
# Global configuration for the library
from netapp_ontap import config
# Support for the connection to ONTAP
from netapp_ontap import HostConnection
# Specific API needed for this script
from netapp_ontap.resources import Cluster
# Create connection to the ONTAP management LIF
# (add verify=False if the certificate your cluster is serving is not
trusted)
conn = HostConnection(
    "<mgmt_ip>", username="admin", password=getpass("ONTAP admin password:
"),
)
# Set connection as the default for all API calls
config.CONNECTION = conn
# Create new cluster object
clus = Cluster()
# Issue REST API call
clus.get()
# Display the cluster configuration
print(clus)

```

NetApp PowerShell Toolkitの詳細

NetAppは、ONTAPストレージシステムの管理に使用できるPowerShellをサポートしています。

概要

PowerShellは、ONTAPクラスタの管理を自動化するもう1つのオプションです。

PowerShell

PowerShellは、タスクの自動化と構成管理に使用できるMicrosoftのプログラミング言語です。これには、コマンドラインシェル環境とスクリプト言語が含まれています。

NetApp ONTAP PowerShellツールキット

The NetAppの略。ONTAP PowerShell Toolkitには、NetApp ONTAP用のPowerShellモジュールが含まれています。このツールキットは、NetApp AFFおよびFASシステム、コモディティハードウェア、クラウドなど、さまざまな環境で実行されるONTAPをサポートします。このモジュールには、Windowsホストでのストレージ管理をまとめてサポートする2,400以上のコマンドレットが含まれています。

ダウンロードしてインストールします

NetApp ONTAP PowerShellツールキットのダウンロードとインストールには、2つのオプションがあります。

ネットアップサポート

PowerShellツールキットはNetApp Support Siteからダウンロードできます。

["NetAppの略。ONTAP PowerShellツールキット"](#)

PowerShellギャラリー

PowerShellツールキットは、PowerShell Galleryからダウンロードできます。

["NetAppの略。ONTAP PowerShellツールキット"](#)

NetApp Manageability SDKの詳細

NetAppマネージャビリティSDKには、ONTAPストレージを監視および管理するアプリケーションを開発するための一連のONTAPI API呼び出しが用意されています。OnCommand Workflow Automationパッケージとともに、SDKはONTAPシステムの管理を自動化するための取り組みをサポートします。



NetApp Manageability SDKとOnCommand Workflow Automationは引き続きサポートされていますが、ONTAP REST APIは、ONTAPシステムを自動化する際に推奨される戦略的テクノロジーです。を参照してください ["ONTAPI無効化"](#) を参照してください。

SDKをダウンロード

NetApp Manageability SDKは、NetApp Support Siteからダウンロードできます。SDKは、Python、PowerShell、C、C++など、クライアント側で複数の言語をサポートしています。Java、C#、VB。 ネット

とルビーNetApp Manageability SDKの詳細と、お使いのバージョンのONTAPでのサポート方法については、Interoperability Matrix Toolを参照してください。

OnCommand Workflow Automationを使用

また、SDKに付属のAPIを使用して、スクリプトを記述せずに管理タスクを自動化することもできます。OnCommand Workflow Automation（OnCommand WFA）には、管理タスクを導入して実行するためのワークフローがあらかじめパッケージ化されています。

関連情報

- ["NetApp Support Site"](#)
- ["NetApp Interoperability Matrix Tool で確認できます"](#)
- ["NetApp Manageability SDKドキュメント"](#)
- ["OnCommand Workflow Automationのドキュメント"](#)

ONTAPIからREST APIへの移行

ONTAPIの無効化とONTAP REST API

ONTAPI API (ZAPI) は、NetApp ONTAPソフトウェアに含まれている独自の呼び出しの元々のセットです。このAPIは、Network Manageability SDKを通じて提供され、データストレージの管理タスクと管理タスクの自動化をサポートします。ONTAPIインターフェイスは、ONTAPの今後のバージョンでは無効になる予定です。ONTAPIを使用している場合は、ONTAP REST APIへの移行を計画する必要があります。

関連情報

- ["ONTAPの自動化オプションを理解する"](#)
- ["CPC-00410 ONTAPI \(ZAPI\) の延期に関する販売終了のお知らせ"](#)
- ["CPCでのZAPIからONTAP REST APIへの変換に関するFAQ"](#)

ONTAP REST APIの移行に関する考慮事項

ONTAPI API (ZAPI) またはONTAP CLIからONTAP REST APIに移行する前に、いくつかの点を考慮する必要があります。

一般的な設計上の違い

ONTAP REST API とコマンドラインインターフェイスでは、設計が根本的に異なります。CLIのコマンドおよびパラメータは、REST API 呼び出しに直接マッピングされません。また、似ているように見えても、入力パラメータの詳細が異なる場合があります。たとえば、数値の単位はバイト数またはサフィックス (KB など) を使用して指定できます。を参照してください ["API 要求を制御する入力変数"](#) および ["API リファレンス"](#) を参照してください。

データ SVM は REST API を通じて公開されます

ONTAP では、いくつかのタイプの Storage Virtual Machine (SVM) がサポートされています。ただし、ONTAP REST API を通じて直接公開されるのはデータ SVM だけです。クラスタとノードについての構成情報は REST API で使用できますが、クラスタとノードは別々の SVM として扱われません。

REST API を使用して ONTAP CLI にアクセスします

ONTAPI API および CLI ユーザーが ONTAP REST API に移行できるように、ONTAP には ONTAP CLI にアクセスするための REST エンドポイントが用意されています。このパススルー機能を使用して、任意の CLI コマンドを実行できます。REST エンドポイントの使用は AutoSupport データに返されます。これにより、NetApp は REST API のギャップを特定し、ONTAP の今後のリリースで改善を行うことができます。

CLI コマンドを問題するには、次のルールに基づいて適切に形成された REST API 呼び出しを行う必要があります。

- リソースパス
- フィールド名

- HTTP メソッド

CLIアクセスのベースリソースパスは次のとおりです。 /private/cli。 REST API を使用した CLI へのアクセスの詳細については、 [ONTAP API オンラインドキュメントページ](#)を参照してください。 NetAppは、コードサンプルやその他の有用な情報を含む[GitHubリポジトリ](#)も維持しています。を参照してください ["ONTAP REST Python GitHub リポジトリ - CLI パススルーサンプル"](#) を参照してください。

ONTAPI での SnapDiff の可用性に対する変更

ONTAP 9.10.1 以降では、 SnapDiff v1 および v2 ONTAPI コールを呼び出すことはできません。 SnapDiff v1 または v2 の ONTAPI コールを呼び出すサードパーティ製アプリケーションは、 ONTAP 9.10.1 以降では機能しません。 ONTAP ユーザは、 ONTAP 9.10.1 にアップグレードする前に、バックアップアプリケーションで SnapDiff v3 REST 呼び出しがサポートされていることを確認する必要があります。

ONTAP の各リリースで利用できる SnapDiff API は次のとおりです。

- ONTAP 9.7 以前のリリース： v1 および v2 （ ONTAPI のみ）
- ONTAP 9.8 – 9.9.1： v1、 v2、 v3 （ ONTAPI と REST API の両方）
- .10.1以降： v3のみ（ONTAP 9のみ）

サポートはリリースごとに異なる時点で撤回されました。これには、ONTAP 9.10.1 P11以降、9.11.1 P7以降、9.12.1 GA以降が含まれます。詳細については、 [を参照してください "ONTAP リリースノート"](#)。

ONTAPIをREST APIのギャップに送信する

NetAppは、お客様のONTAPIからONTAP REST APIへの移行をサポートすることをお約束します。 REST API に何か欠けているものがある場合は、お知らせください。これらのギャップおよび他の考えをで提出できる ["ONTAPIからREST APIへ"](#) ページ

ONTAPIからONTAP REST APIへのマッピング

ONTAP REST APIには、ほとんどの領域のONTAPIに相当する機能が含まれています。 ネットアップでは、 ONTAPIコールとそれに対応するREST API呼び出しのマッピングについて説明したドキュメントを提供しています。

最新のドキュメントにはオンラインでアクセスでき ["ONTAP ONTAPIからRESTへのマッピング"](#)ます。 ONTAPリリースに基づく以前のバージョンのドキュメントにアクセスするためのバージョンセレクトも用意されています。

ONTAP REST APIでのパフォーマンスカウンタの使用

ONTAP カウンタマネージャは、各ONTAP システムのパフォーマンスに関する広範な情報を保持します。このデータは、_パフォーマンスカウンタのセットとしてエクスポートされます。これを使用して、ONTAP システムのパフォーマンスを評価し、パフォーマンス目標を達成することができます。

ONTAP パフォーマンスカウンタにアクセスします

ONTAP パフォーマンスカウンタには、ONTAP コマンドラインインターフェイスと2つの異なるAPIを使用してアクセスできます。



ONTAP REST APIは、ONTAP 環境の管理を自動化する際に推奨される戦略的オプションです。

ONTAPI API

ONTAPI APIは、NetApp Network Manageability SDKで使用できます。ONTAPIを使用する場合、パフォーマンスカウンタは一連のオブジェクト内に定義されます。各オブジェクトは、システムの物理コンポーネントまたは仮想コンポーネントに対応します。システム構成に基づいて、各オブジェクトに1つ以上のインスタンスが存在できます。

たとえば、ONTAP システムに4本の物理ディスクがある場合、のインスタンスは4つになります `disk` オブジェクトごとに固有のパフォーマンスカウンタのセットがあります。ONTAPIを使用して、各ディスクインスタンスの個々のカウンタにアクセスできます。

ONTAP REST API

ONTAP 9.11.1以降では、REST APIを使用してパフォーマンスデータにアクセスすることもできます。この場合、パフォーマンスカウンタは、ONTAPIオブジェクトに相当するテーブルに編成されています。各テーブル行は、ONTAPIオブジェクトのインスタンスに相当します。

たとえば、ONTAP システムに4本の物理ディスクがある場合、が表示されます `disk` テーブルには4つの行が含まれます。行ごとに個別にアクセスでき、その行のフィールドまたは列として使用できるパフォーマンスカウンタのセットが含まれています。

REST API を使用するための準備を行う

ONTAP REST APIを使用してパフォーマンスカウンタにアクセスする前に、準備をしておく必要があります。

パフォーマンスカウンタを表にまとめました

ONTAPIオブジェクトの一部をONTAP REST APIから使用でき、テーブルとして表示されます。たとえば、ONTAPI * `hostadapter` オブジェクトは、**REST API**で `host_adapter` *テーブルとして表示されます。システム内の各ホストアダプタは、固有のパフォーマンスカウンタのセットを持つ行です。

インスタンス名	パフォーマンスカウンタ					
HOST_ADAPTER_1	total_read_ops_1	total_write_ops_1	bytes_read_1	bytes_writted_1	max_link_data_rate_1	RSCN count_1
host_adapter_2	total_read_ops_2	total_write_ops_2	bytes_read_2	bytes_writted_2	max_link_data_rate-2です	RSCN count_2
host_adapter_3	total_read_ops_3	total_write_ops_3	bytes_read_3.	Byte_Writted_3	max_link_data_rate-3の値です	RSCN count_3

RESTエンドポイントの概要

ONTAP のパフォーマンスカウンタと関連テーブルにアクセスするために使用できる主要なエンドポイントは4つあります。



各RESTエンドポイントは読み取り専用アクセスを提供し、* GET * HTTPメソッドのみをサポートします。を参照してください ["API リファレンス"](#) を参照してください。

- `*/cluster/counter/tables *`

カウンタテーブルとそのスキーマ定義のコレクションを返します。

- `/cluster/counter/tables / {name}`

単一の名前付きカウンタテーブルに関する情報を返します。

- `*/cluster/counter/tables / {counter_name} / rows *`

名前付きカウンタテーブルから行のコレクションを返します。

- `/cluster/counter/tables / {counter_name} / rows / {id}`

名前付きカウンタテーブルの特定の行を返します。

ONTAPIからREST APIへの移行

ネットアップでは、ONTAPIからONTAP REST APIに自動化コードを移行する広範なサポートを提供しています。これには、特定のONTAPIオブジェクトのREST APIで使用可能な同等のパフォーマンスカウンタテーブルを識別するためのマッピングドキュメントが含まれます。

最新のドキュメントにはオンラインでアクセスでき ["ONTAPパフォーマンスカウンタのマッピング"](#) ます。ONTAPリリースに基づく以前のバージョンのドキュメントにアクセスするためのバージョンセレクトも用意されています。

ONTAP REST APIの使用を開始する

次の例は、REST APIを使用してONTAP のパフォーマンスカウンタにアクセスする方法を示しています。これには、使用可能なテーブルのリストを取得し、テーブル構造を確認する作業が含まれます。

作業を開始する前に

例を使用する前に、次の情報を確認してください。

ONTAP クレデンシャル

パスワードを含むONTAP 管理者アカウントが必要です。

クラスタ管理IP

ONTAP システムに設定されたクラスタ管理IPアドレスが必要です。

すべてのAPI呼び出しでGETメソッドを使用します

以下に示すすべての例は、HTTP GETメソッドを使用して情報を取得する場合にのみ使用できます。

変数置換

各カールの例には、大文字と角かっこで囲まれたテキストで示される1つ以上の変数が含まれています。これらの変数は、環境に応じて実際の値に置き換えてください。

例はエンドポイントに一致します

以下の一連の例は、パフォーマンスカウンタの取得に使用できるRESTエンドポイントの使用方法を示しています。を参照してください [RESTエンドポイントの概要](#) を参照してください。

例1：すべてのパフォーマンスカウンタテーブル

このREST API呼び出しは、使用可能なすべてのカウンタマネージャテーブルを検出するために使用できません。

カールの例

```
curl --request GET --user admin:<PASSWORD>  
'https://<ONTAP_IP_ADDRESS>/api/cluster/counter/tables'
```

```
{
  "records": [
    {
      "name": "copy_manager",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/copy_manager"
        }
      }
    },
    {
      "name": "copy_manager:constituent",
      "_links": {
        "self": {
          "href":
"/api/cluster/counter/tables/copy_manager%3Aconstituent"
        }
      }
    },
    {
      "name": "disk",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/disk"
        }
      }
    },
    {
      "name": "disk:constituent",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/disk%3Aconstituent"
        }
      }
    },
    {
      "name": "disk:raid_group",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/disk%3Araid_group"
        }
      }
    }
  ],
}
```

```
{
  "name": "external_cache",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/external_cache"
    }
  }
},
{
  "name": "fcp",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/fcp"
    }
  }
},
{
  "name": "fcp:node",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/fcp%3Anode"
    }
  }
},
{
  "name": "fcp_lif",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/fcp_lif"
    }
  }
},
{
  "name": "fcp_lif:node",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/fcp_lif%3Anode"
    }
  }
},
{
  "name": "fcp_lif:port",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/fcp_lif%3Aport"
    }
  }
}
```

```

    }
  },
  {
    "name": "fcp_lif:svm",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/fcp_lif%3Asvm"
      }
    }
  },
  {
    "name": "fcvi",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/fcvi"
      }
    }
  },
  {
    "name": "headroom_aggregate",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/headroom_aggregate"
      }
    }
  },
  {
    "name": "headroom_cpu",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/headroom_cpu"
      }
    }
  },
  {
    "name": "host_adapter",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/host_adapter"
      }
    }
  },
  {
    "name": "iscsi_lif",
    "_links": {
      "self": {

```

```

        "href": "/api/cluster/counter/tables/iscsi_lif"
    }
}
},
{
    "name": "iscsi_lif:node",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/iscsi_lif%3Anode"
        }
    }
},
{
    "name": "iscsi_lif:svm",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/iscsi_lif%3Asvm"
        }
    }
},
{
    "name": "lif",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/lif"
        }
    }
},
{
    "name": "lif:svm",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/lif%3Asvm"
        }
    }
},
{
    "name": "lun",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/lun"
        }
    }
},
{
    "name": "lun:constituent",

```

```

    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/lun%3Aconstituent"
      }
    }
  },
  {
    "name": "lun:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/lun%3Anode"
      }
    }
  },
  {
    "name": "namespace",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/namespace"
      }
    }
  },
  {
    "name": "namespace:constituent",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/namespace%3Aconstituent"
      }
    }
  },
  {
    "name": "nfs_v4_diag",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/nfs_v4_diag"
      }
    }
  },
  {
    "name": "nic_common",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/nic_common"
      }
    }
  }
},

```

```

{
  "name": "nvmf_lif",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/nvmf_lif"
    }
  }
},
{
  "name": "nvmf_lif:constituent",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/nvmf_lif%3Aconstituent"
    }
  }
},
{
  "name": "nvmf_lif:node",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/nvmf_lif%3Anode"
    }
  }
},
{
  "name": "nvmf_lif:port",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/nvmf_lif%3Aport"
    }
  }
},
{
  "name": "object_store_client_op",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/object_store_client_op"
    }
  }
},
{
  "name": "path",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/path"
    }
  }
}

```



```

    }
  },
  {
    "name": "processor",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/processor"
      }
    }
  },
  {
    "name": "processor:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/processor%3Anode"
      }
    }
  },
  {
    "name": "qos",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/qos"
      }
    }
  },
  {
    "name": "qos:constituent",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/qos%3Aconstituent"
      }
    }
  },
  {
    "name": "qos:policy_group",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/qos%3Apolicy_group"
      }
    }
  },
  {
    "name": "qos_detail",
    "_links": {
      "self": {

```

```

        "href": "/api/cluster/counter/tables/qos_detail"
    }
}
},
{
    "name": "qos_detail_volume",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/qos_detail_volume"
        }
    }
},
{
    "name": "qos_volume",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/qos_volume"
        }
    }
},
{
    "name": "qos_volume:constituent",
    "_links": {
        "self": {
            "href":
"/api/cluster/counter/tables/qos_volume%3Aconstituent"
        }
    }
},
{
    "name": "qtree",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/qtree"
        }
    }
},
{
    "name": "qtree:constituent",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/qtree%3Aconstituent"
        }
    }
},
{

```

```

    "name": "svm_cifs",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_cifs"
      }
    }
  },
  {
    "name": "svm_cifs:constituent",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_cifs%3Aconstituent"
      }
    }
  },
  {
    "name": "svm_cifs:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_cifs%3Anode"
      }
    }
  },
  {
    "name": "svm_nfs_v3",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v3"
      }
    }
  },
  {
    "name": "svm_nfs_v3:constituent",
    "_links": {
      "self": {
        "href":
"/api/cluster/counter/tables/svm_nfs_v3%3Aconstituent"
      }
    }
  },
  {
    "name": "svm_nfs_v3:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v3%3Anode"
      }
    }
  }
}

```

```

    }
  },
  {
    "name": "svm_nfs_v4",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v4"
      }
    }
  },
  {
    "name": "svm_nfs_v41",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v41"
      }
    }
  },
  {
    "name": "svm_nfs_v41:constituent",
    "_links": {
      "self": {
        "href":
"/api/cluster/counter/tables/svm_nfs_v41%3Aconstituent"
      }
    }
  },
  {
    "name": "svm_nfs_v41:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v41%3Anode"
      }
    }
  },
  {
    "name": "svm_nfs_v42",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v42"
      }
    }
  },
  {
    "name": "svm_nfs_v42:constituent",
    "_links": {

```

```

    "self": {
      "href":
"/api/cluster/counter/tables/svm_nfs_v42%3Aconstituent"
    }
  },
  {
    "name": "svm_nfs_v42:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v42%3Anode"
      }
    }
  },
  {
    "name": "svm_nfs_v4:constituent",
    "_links": {
      "self": {
        "href":
"/api/cluster/counter/tables/svm_nfs_v4%3Aconstituent"
      }
    }
  },
  {
    "name": "svm_nfs_v4:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v4%3Anode"
      }
    }
  },
  {
    "name": "system",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/system"
      }
    }
  },
  {
    "name": "system:constituent",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/system%3Aconstituent"
      }
    }
  }
}

```

```

},
{
  "name": "system:node",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/system%3Anode"
    }
  }
},
{
  "name": "token_manager",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/token_manager"
    }
  }
},
{
  "name": "volume",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/volume"
    }
  }
},
{
  "name": "volume:node",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/volume%3Anode"
    }
  }
},
{
  "name": "volume:svm",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/volume%3Asvm"
    }
  }
},
{
  "name": "waf1",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/waf1"
    }
  }
}

```

```

    }
  },
  {
    "name": "waf1_comp_aggr_vol_bin",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/waf1_comp_aggr_vol_bin"
      }
    }
  },
  {
    "name": "waf1_hya_per_aggregate",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/waf1_hya_per_aggregate"
      }
    }
  },
  {
    "name": "waf1_hya_sizer",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/waf1_hya_sizer"
      }
    }
  }
],
"num_records": 71,
"_links": {
  "self": {
    "href": "/api/cluster/counter/tables"
  }
}
}
}

```

例2：特定のテーブルに関する概要情報

このREST API呼び出しを使用して、特定のテーブルの概要とメタデータを表示できます。出力には、表の目的と各パフォーマンスカウンタに含まれるデータのタイプが表示されます。この例では、* host_adapter * テーブルを使用します。

カールの例

```
curl --request GET --user admin:<PASSWORD>  
'https://<ONTAP_IP_ADDRESS>/api/cluster/counter/tables/host_adapter'
```



```
{
  "name": "host_adapter",
  "description": "The host_adapter table reports activity on the Fibre Channel, Serial Attached SCSI, and parallel SCSI host adapters the storage system uses to connect to disks and tape drives.",
  "counter_schemas": [
    {
      "name": "bytes_read",
      "description": "Bytes read through a host adapter",
      "type": "rate",
      "unit": "per_sec"
    },
    {
      "name": "bytes_written",
      "description": "Bytes written through a host adapter",
      "type": "rate",
      "unit": "per_sec"
    },
    {
      "name": "max_link_data_rate",
      "description": "Max link data rate in Kilobytes per second for a host adapter",
      "type": "raw",
      "unit": "kb_per_sec"
    },
    {
      "name": "node.name",
      "description": "System node name",
      "type": "string",
      "unit": "none"
    },
    {
      "name": "rscn_count",
      "description": "Number of RSCN(s) received by the FC HBA",
      "type": "raw",
      "unit": "none"
    },
    {
      "name": "total_read_ops",
      "description": "Total number of reads on a host adapter",
      "type": "rate",
      "unit": "per_sec"
    }
  ],
}
```

```
{
  "name": "total_write_ops",
  "description": "Total number of writes on a host adapter",
  "type": "rate",
  "unit": "per_sec"
}
],
"_links": {
  "self": {
    "href": "/api/cluster/counter/tables/host_adapter"
  }
}
}
```

例3：特定のテーブル内のすべての行

このREST API呼び出しを使用して、テーブルのすべての行を表示できます。これは、カウンタマネージャオブジェクトのインスタンスが存在することを示します。

カールの例

```
curl --request GET --user admin:<PASSWORD>
'https://<ONTAP_IP_ADDRESS>/api/cluster/counter/tables/host_adapter/rows'
```

JSON 出力例

```
{
  "records": [
    {
      "id": "dmp-adapter-01",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/host_adapter/rows/dmp-adapter-01"
        }
      }
    },
    {
      "id": "dmp-adapter-02",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/host_adapter/rows/dmp-adapter-02"
        }
      }
    }
  ],
  "num_records": 2,
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/host_adapter/rows"
    }
  }
}
```

例4：特定のテーブル内の単一の行

このREST API呼び出しは、特定のカウンタマネージャインスタンスのパフォーマンスカウンタ値を表で表示する際に使用できます。この例では、いずれかのホストアダプタのパフォーマンスデータが要求されます。

カールの例

```
curl --request GET --user admin:<PASSWORD>
'https://<ONTAP_IP_ADDRESS>/api/cluster/counter/tables/host_adapter/rows/dmp-adapter-01'
```

JSON 出力例



```

{
  "counter_table": {
    "name": "host_adapter"
  },
  "id": "dmp-adapter-01",
  "properties": [
    {
      "name": "node.name",
      "value": "dmp-node-01"
    }
  ],
  "counters": [
    {
      "name": "total_read_ops",
      "value": 25098
    },
    {
      "name": "total_write_ops",
      "value": 48925
    },
    {
      "name": "bytes_read",
      "value": 1003799680
    },
    {
      "name": "bytes_written",
      "value": 6900961600
    },
    {
      "name": "max_link_data_rate",
      "value": 0
    },
    {
      "name": "rscn_count",
      "value": 0
    }
  ],
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/host_adapter/rows/dmp-adapter-01"
    }
  }
}

```

ONTAP REST APIをサポートするツールとソフトウェア

ネットアップでは、ONTAPIからONTAP REST APIへの移行をサポートするために、サンプルのPythonスクリプトとその他の関連ソフトウェアを提供しています。これらのサンプルの中で最も重要なものを以下に説明します。



すべてのPythonコードサンプルはGitHubリポジトリで入手でき ["NetApp ONTAP REST Python"](#) ます。また、に記載されているリソースも確認して ["ONTAP REST APIの詳細"](#) ください。

ONTAPI使用状況レポートツール

ONTAPI使用状況レポートツールは、ネットアップのプロフェッショナルサービス、お客様、パートナー様が自社のONTAP 環境でのONTAPIの使用状況を確認できるように設計されています。スクリプトは、次の表に示す3つのユースケースに対応しています。

スクリプト	説明
apache_scraper.py	ONTAP ノードに対して発行されたONTAPIコールを検索するためのApacheログスクレーパー
session_stats.py	ONTAP からセッション統計データを取得するCLISクリプト
zapi_to_rest.py	渡されたONTAPI呼び出しと属性のRESTの詳細を抽出するスクリプト

にアクセスできます ["ONTAPI使用状況レポートツール"](#) をダウンロードしてご確認ください。Aも参照してください。 ["デモ"](#) レポート作成ツールとその使用方法について説明します。

プライベートCLIパススルー

REST APIは、ONTAP で利用可能な機能を幅広く提供します。ただし、REST APIを使用してONTAP CLIに直接アクセスすると便利な場合があります。

この機能の概要については、を参照してください ["REST API を使用して ONTAP CLI にアクセスします"](#) 。 Pythonのサンプルについては、を参照してください ["REST CLIパススルーのサンプル"](#) 。

Python クライアントライブラリ

Pythonクライアントライブラリは、Pythonを使用してONTAP REST APIにアクセスするためにインストールして使用できるパッケージです。ONTAP 環境を自動化するための堅牢なコードを迅速に開発できます。Pythonクライアントライブラリの詳細については、を参照してください ["Python クライアントライブラリ"](#) 。

ONTAP PowerShellツールキット

NetApp.ONTAP PowerShell Toolkitは、2、400を超えるコマンドレットを含むモジュールで、ローカルPowerShell環境を強化します。Windowsホスト用のコードを迅速に開発して、ONTAPの導入を自動化できます。詳細については、を参照してください ["NetApp PowerShell Toolkitの詳細"](#) 。

ONTAP REST APIのリファレンス

APIリファレンスには、ONTAP REST API呼び出しの詳細（HTTPメソッド、入力パラメータ、応答など）が記載されています。このリファレンスは、REST API を使用して自動化アプリケーションを開発する場合に役立ちます。



ONTAPリリースに基づいて、いくつかのサイトのいずれかでREST APIのリファレンスドキュメントにアクセスできます。同等のドキュメントのコピーは、ローカルのONTAPシステムのSwagger UIから入手できます。

ONTAP APIのリファレンスドキュメントへのオンラインアクセス

最新のドキュメントにはオンラインでアクセスでき "[ONTAP REST APIリファレンス](#)"ます。ONTAPリリースに基づく以前のバージョンのドキュメントにアクセスするためのバージョンセレクタも用意されています。

Swagger UIからONTAP APIのリファレンスドキュメントにアクセス

ONTAP REST APIのドキュメントには、ローカルのONTAPシステムのSwagger UIからアクセスできます。

作業を開始する前に

次の情報が必要です。

- ONTAP クラスタ管理 LIF の IP アドレスまたはホスト名
- ONTAP REST API にアクセスする権限を持つアカウントのユーザ名とパスワード

手順

1. ブラウザに URL を入力し、**Enter** キーを押します。

https://<ip_address>/docs/api

2. ONTAP アカウントを使用してサインインします。

ONTAP API ドキュメントページが表示され、主要なリソースカテゴリ別に分類された API 呼び出しが下部に表示されます。

3. 個々の API 呼び出しの例として、`* cluster *` カテゴリまでスクロールし、`* get/cluster *` をクリックします。

ONTAP REST APIの詳細

ONTAPストレージシステムの導入と管理を自動化するための参考資料がいくつか用意されています。

ブログ記事

ブログ記事は、主題に基づいていくつかのセクションに配置されています。

全般

- 現在のONTAP自動化テクノロジーの概要です。

["自動化の新たな標準"](#)

- Ansible for ONTAP 自動化を初めて使用する方には、この作業を始めることをお勧めします。

["ネットアップと Ansible の使用： Ansible のインストール"](#)

- ONTAP REST APIを使用してファイルセキュリティと権限を管理する方法について説明します。

["ONTAP REST API を使用してファイルセキュリティ権限を簡単に管理できます"](#)

- ONTAPイベントを監視して、システムアクティビティを常に把握できます。これらのイベントの設定と管理は、REST APIを使用して自動化できます。

["ONTAP REST API：重大度の高いイベントの通知を自動化します"](#)

- REST APIを使用して、RBACセキュリティ環境の一部としてロールとアクセスレベルを設定できます。

["ONTAP REST APIを使用したロールベースアクセス制御（RBAC）"](#)

- コーヒーブレークウィズREST（6エピソード）：

- ["ONTAP REST APIの基礎"](#)
- ["ONTAP RESTAPIノキノウ"](#)
- ["Postmanを使用したONTAP RESTのハンズオン"](#)
- ["ONTAPI（ZAPI）レポートツール"](#)
- ["プライベートCLIパススルー"](#)
- ["ONTAPストレージの自動化をシンプルにする5つの魔法の機能！"](#)

Python クライアントライブラリ

- NetAppがONTAP REST APIにアクセスするためにGitHubで提供しているPythonサンプルスクリプトの使用方法的紹介です。

["ONTAP REST API PythonサンプルスクリプトがGitHubで利用可能になりました!"](#)

- このブログでは、ONTAP Pythonクライアントライブラリの機能を簡単に紹介します。

["PythonクライアントライブラリでONTAP REST APIの利用を簡易化"](#)

- これは、Pythonクライアントライブラリの使用を開始するための3部構成のブログです。
 - ["パート1"](#)
 - ["パート2"](#)
 - ["パート3"](#)

REST APIへの移行

- ネットアップでは、マッピングドキュメントを使用して、独自のONTAPI APIからONTAP REST APIへの移行をサポートしています。

["ONTAPI から REST へのマッピング"](#)

- REST APIをベースにしたONTAP 自動化環境の変革に役立つテクノロジーがいくつかあります。

["ONTAPIから自動化をONTAP REST APIに変換します"](#)

- CLIおよびONTAP ユーザーがONTAP REST APIに移行できるように、ONTAP には、すべてのCLIコマンドへのアクセスに使用できるプライベートREST APIエンドポイントが用意されています。

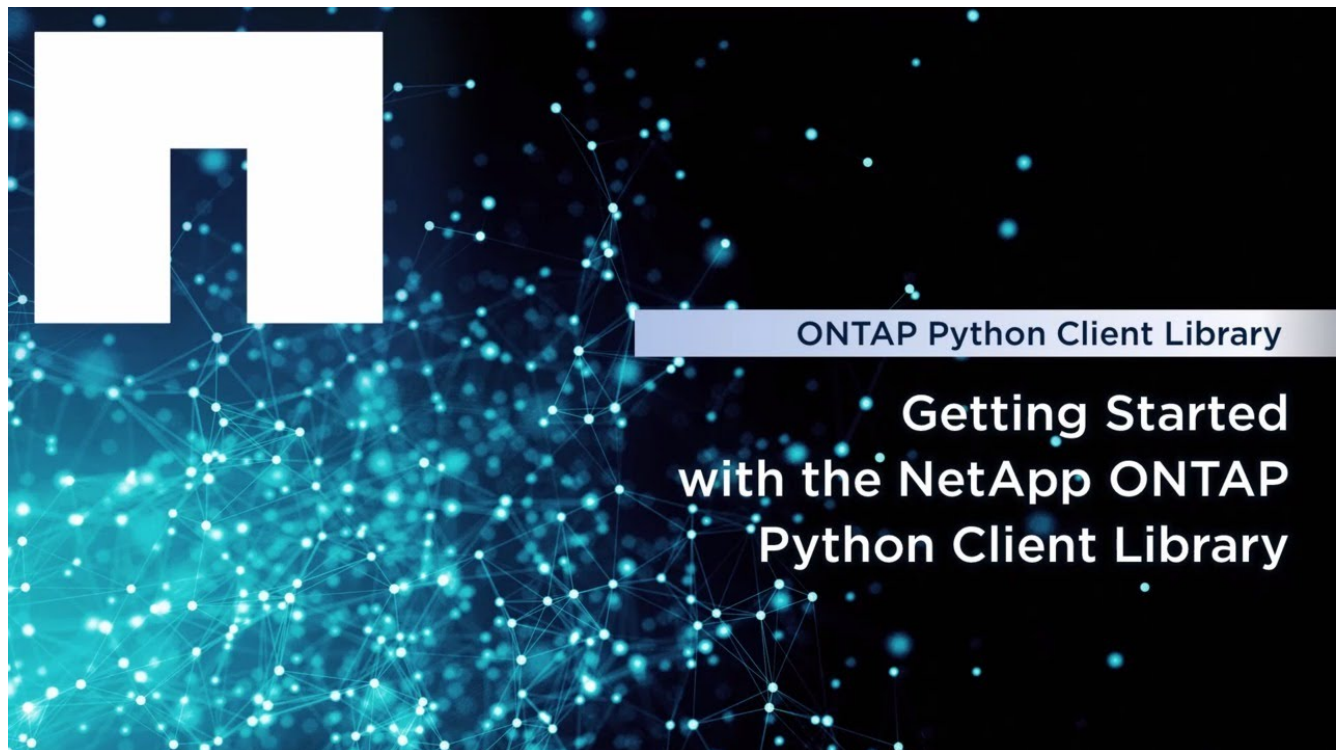
["ONTAP REST API でプライベート CLI パススルーを使用する"](#)

- ネットアップは、お客様やパートナー様がONTAP REST APIへの移行を支援するツールを提供しています。

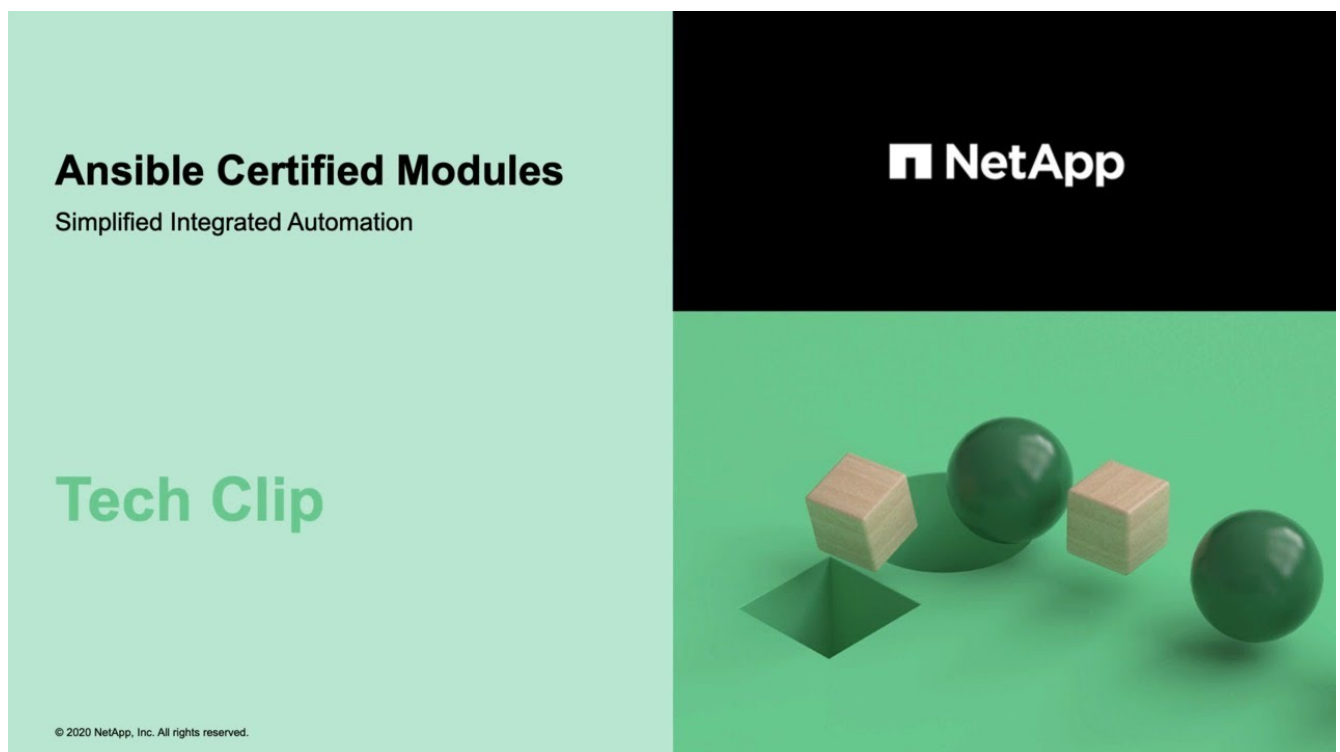
["ONTAPI使用状況レポートツールを使用したONTAPI \(ZAPI\) からの移行"](#)

ビデオ

- NetApp Pythonクライアントライブラリの入門と、ライブラリを使用してコードを書き始める方法を紹介합니다。



- Ansible認定モジュールをご覧ください。



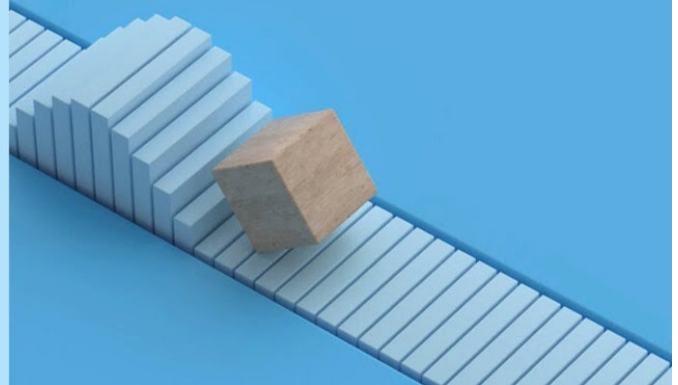
Ansible Certified Modules

Simplified Integrated Automation

Use Case

© 2020 NetApp, Inc. All rights reserved.

 NetApp



- NetApp TechComm TVのビデオコレクション。

["NetApp ONTAP管理の自動化"](#)

技術トレーニングとイベント

- INSIGHT 2022プレゼンテーション (26分)

["ONTAP REST APIによるONTAPストレージ管理の刷新"](#)

- INSIGHT 2021プレゼンテーション (31分)

["NetApp ONTAP : REST APIを使用した時間の節約と簡易化"](#)

- NetAppラーニングサービス。

["ONTAP REST APIとAnsibleを使用してストレージ管理を自動化"](#)

ネットアップナレッジベース

- ONTAP REST APIで問題が発生した場合は、NetAppに報告できます。

["ONTAP REST APIおよびONTAP REST API Pythonクライアントライブラリに関する問題の報告方法"](#)

- ONTAP REST APIの機能ギャップが見つかった場合は、APIの新しい機能を要求できます。

["ONTAP REST APIの機能を要求する方法"](#)

ONTAP REST APIの法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

商標

NetApp、NetApp のロゴ、および NetApp の商標ページに記載されているマークは、NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

<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/"](https://www.netapp.com/company/legal/privacy-policy/)

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

商標に関する情報

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