



はじめに

Cloud Data Sense

NetApp
May 12, 2022

目次

はじめに	1
クラウドデータの意味をご確認ください	1
クラウドデータの導入センス	7
データソースでスキャンをアクティブ化します	27
Active Directory と Cloud Data Sense を統合	69
クラウドデータセンスのライセンスをセットアップする	72
クラウドデータの意味についてよく寄せられる質問	78

はじめに

クラウドデータの意味をご確認ください

Cloud Data Sense は、社内のオンプレミスデータソースやクラウドデータソース、作業環境をスキャンしてデータをマッピング、分類し、プライベート情報を特定する、Cloud Manager のデータガバナンスサービスです。これにより、セキュリティとコンプライアンスのリスクを軽減し、ストレージコストを削減し、データ移行プロジェクトを支援できます。

["Cloud Data Sense のユースケースについて説明します"](#)。

の機能

Cloud Data Sense には、コンプライアンスの取り組みに役立つツールがいくつか用意されています。データセンスを使用すると、次のことができます。

- 個人識別情報（PII）の識別
- GDPR、CCPA、PCI、HIPAA の各プライバシー規制の要件に応じて、さまざまな機密情報の範囲を特定します
- データサブジェクトアクセス要求への応答（dsar）
- ファイルに特定のが含まれている場合は、Cloud Manager ユーザに E メールで通知します PII（この基準は、を使用して定義します ["ポリシー"](#)）
- 表示と変更 ["Azure Information Protection（AIP）ラベル"](#) ファイルに保存できます
- ファイルにカスタムタグを追加し（「移動が必要」など）、Cloud Manager ユーザを割り当てて、ユーザがファイルの更新を所有できるようにします
- ファイルをコピー、移動、および削除します

クラウドデータセンスには、ガバナンスの取り組みに役立つツールも用意されています。Cloud Data Sense を使用すると、次のことが可能になります。

- 古いデータ、ビジネス以外のデータ、重複するファイル、開いている権限を持つファイル、システム内の大容量ファイルを特定します。

この情報を使用して、一部のファイルを低コストのオブジェクトストレージに移動、削除、または階層化するかどうかを決定できます。

- データのサイズ、および移動前に機密情報が含まれているデータがないかどうかを確認する。

これは、オンプレミスの場所からクラウドにデータを移行する場合に便利です。

サポートされている作業環境とデータソース

Cloud Data Sense では、次のような作業環境やデータソースからデータをスキャンできます。

- 作業環境： *

- Cloud Volumes ONTAP（AWS、Azure、GCP に導入）
- オンプレミスの ONTAP クラスタ
- Azure NetApp Files の特長
- ONTAP 対応の Amazon FSX
- Amazon S3
- データソース：*
- ネットアップ以外のファイル共有
- オブジェクトストレージ（S3 プロトコルを使用）
- データベース
- OneDrive アカウント
- SharePoint アカウント
- Google ドライブ アカウント

Data Sense は、NFS バージョン 3.x、4.0、4.1、および CIFS バージョン 1.x、2.0、2.1、3.0 をサポートしています。

コスト

- クラウドデータセンスの使用コストは、スキャンするデータの量によって異なります。データをスキャンする、Cloud Manager ワークスペース内の最初の 1TB のデータは無料です。これには、すべての作業環境とデータソースのすべてのデータが含まれます。この時点以降もデータのスキャンを続行するには、AWS、Azure、GCP Marketplace、またはネットアップの BYOL ライセンスのサブスクリプションが必要です。を参照してください ["価格設定"](#) を参照してください。

["Cloud Data Sense のライセンスを取得する方法について説明します"](#)。

- クラウドにクラウドデータセンスをインストールするには、クラウドインスタンスを導入する必要があります。その場合、クラウドインスタンスが導入されているクラウドプロバイダから料金が発生します。を参照してください [各クラウドに導入されるインスタンスのタイプ プロバイダ](#)。データセンスをオンプレミスシステムにインストールしても、コストはかかりません。
- Cloud Data Senseを使用するには、Cloud Manager Connectorを導入しておく必要があります。多くの場合、Cloud Manager で他のストレージとサービスを使用しているため、すでにコネクタが用意されています。Connector インスタンスを使用すると、導入先のクラウドプロバイダから料金が発生します。を参照してください ["クラウドプロバイダごとに導入されるインスタンスのタイプ"](#)。コネクタをオンプレミスシステムにインストールしても、コストはかかりません。

データ転送コスト

データ転送のコストは設定によって異なります。Cloud Data Sense インスタンスとデータソースが同じアベイラビリティゾーンとリージョンにある場合は、データ転送コストは発生しない。ただし、Cloud Volumes ONTAP システムや S3 バケットなどのデータソースが `_different_` Availability Zone またはリージョンにある場合は、クラウドプロバイダにデータ転送コストが請求されます。詳細については、次のリンクを参照してください。

- ["AWS：Amazon EC2 価格設定"](#)
- ["Microsoft Azure：Bandwidth Pricing Details 』"](#)

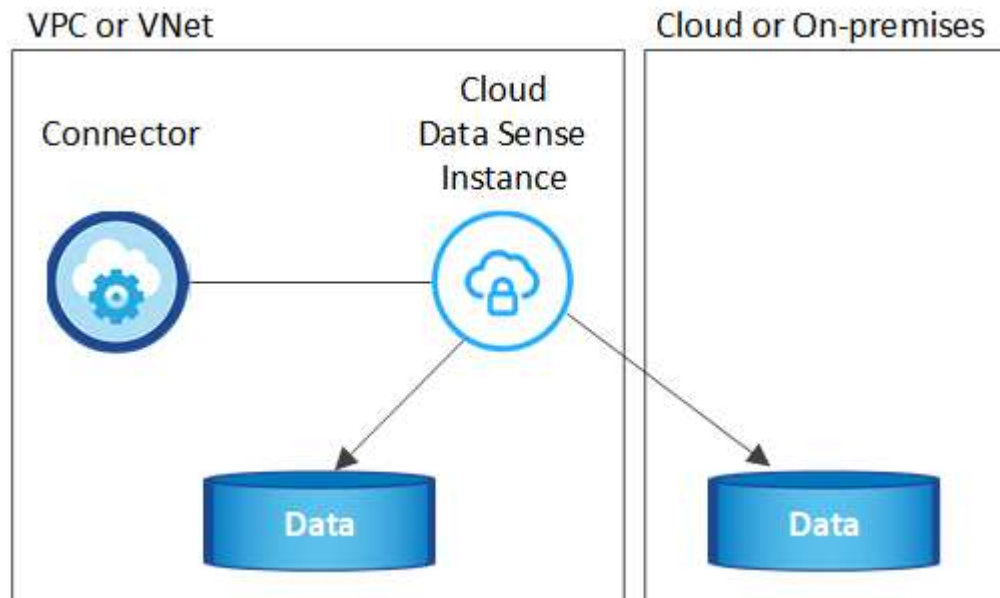
- ["Google Cloud : ストレージ転送サービスの価格"](#)

Cloud Data Sense インスタンス

クラウドにデータセンスを導入すると、Cloud Manager はコネクタと同じサブネットにインスタンスを導入します。"[コネクタの詳細については、こちらをご覧ください。](#)"



コネクタがオンプレミスにインストールされている場合は、要求内の最初の Cloud Volumes ONTAP システムと同じ VPC または VNet にクラウドデータセンスインスタンスを導入します。データセンスはオンプレミスにもインストールできます。



デフォルトのインスタンスについては、次の点に注意してください。

- AWS では、Cloud Data Sense はで実行されます ["m5.mc2\[インスタンス\]"](#) 500 GB の gp2 ディスクです。オペレーティングシステムイメージは Amazon Linux 2 (Red Hat 7.3.1) です。

m5.mcd を使用できない領域では、代わりに m4.mcd インスタンスに対してデータセンスを実行します。

- Azure では、Cloud Data Sense はで実行されます ["Standard_D16s_v3 VM"](#) 512 GB ディスクオペレーティングシステムのイメージは CentOS 7.8 です。
- GCP では、Cloud Data Sense はで実行されます ["N2-standard-16 VM"](#) 512 GB の標準パーシステントディスクオペレーティングシステムイメージは CentOS 7.9 です。

n2-dstandard-16 を使用できない地域では、データセンスは n2D-standard-16 または n1-standard-16 VM で実行されます。

- インスタンスの名前は *CloudCompliance_with* で、生成されたハッシュ (UUID) を連結しています。例：
_CloudCompliance-16bb6564-38ad-40802-9a92-36f5fd2f71c7
- コネクタごとに展開されるデータセンスインスタンスは 1 つだけです。
- データセンスソフトウェアのアップグレードは、インスタンスがインターネットにアクセスできるかぎり自動化されます。



Cloud Data Sense がデータを継続的にスキャンするため、インスタンスは常時実行している必要があります。

小さいインスタンスタイプを使用しています

CPU の数と RAM の数が少ないシステムには Data Sense を導入できますが、このような低パフォーマンスのシステムを使用する場合はいくつかの制限事項があります。

システムサイズ	仕様	制限
Extra Large (デフォルト)	CPU × 16 、 64GB RAM 、 500GB SSD	なし
中	CPU × 8 、 32GB RAM 、 200GB SSD	スキャンに時間がかかり、スキャンできるファイルは最大 100 万個です。
小規模	CPU × 8 、 16GB RAM 、 100GB SSD	「中」と同じ制限に加えて、特定する機能 "データ主体名" 内部ファイルは無効です。

クラウドにデータセンスを導入する場合は、ng-contact-data-sense@netapp.com に電子メールを送信して、これらの小規模なシステムのいずれかを使用する場合のサポートを依頼してください。これらの小規模なクラウド構成を導入するには、弊社と協力する必要があります。

データセンスをオンプレミスで導入する場合は、小さい仕様の Linux ホストを使用するだけです。ネットアップにお問い合わせいただく必要はありません。

Cloud Data Sense の仕組み

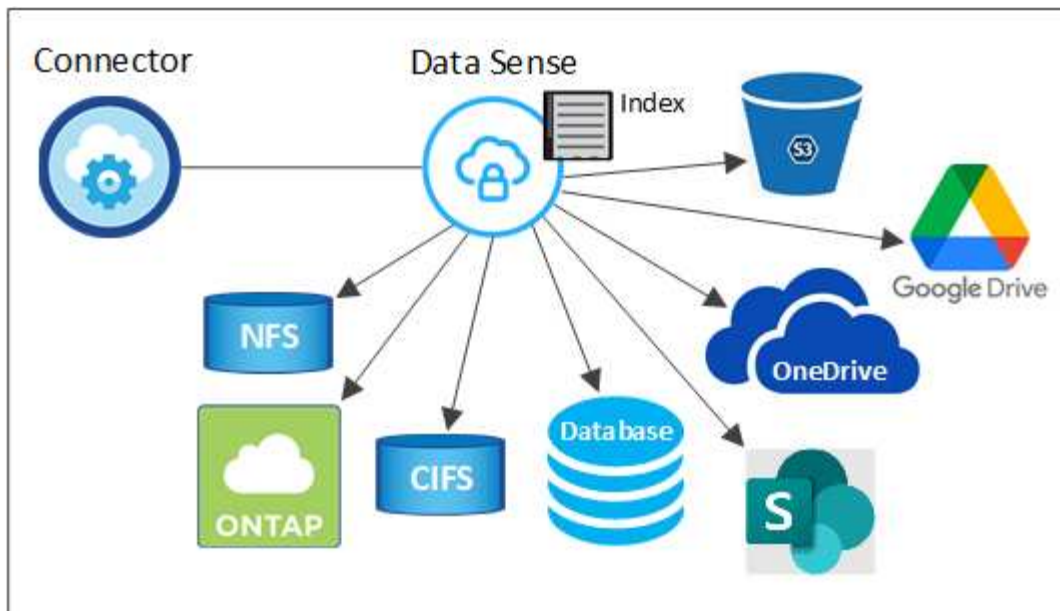
Cloud Data Sense の概要は次のようになります。

1. Cloud Manager でデータセンスのインスタンスを導入します。
2. 概要マッピングまたは詳細レベルスキャンは、1 つ以上の作業環境またはデータソースで有効にします。
3. データセンスは、AI 学習プロセスを使用してデータをスキャンします。
4. 提供されているダッシュボードとレポートツールを使用して、コンプライアンスとガバナンスの取り組みを支援します。

スキャンの動作

Cloud Data Sense を有効にして、スキャンするボリューム、バケット、データベーススキーマ、OneDrive または SharePoint のユーザデータを選択すると、データのスキャンがただちに開始され、個人データや機密データが識別されます。組織のデータをマッピングし、各ファイルを分類して、データ内のエンティティと定義済みパターンを特定して抽出します。スキャンの結果は、個人情報、機密性の高い個人情報、データカテゴリ、およびファイルタイプのインデックスです。

データセンスは、NFS ボリュームと CIFS ボリュームをマウントすることで、他のクライアントと同様にデータに接続します。NFS ボリュームには読み取り専用で自動的にアクセスされますが、CIFS ボリュームをスキャンするためには Active Directory のクレデンシャルを指定する必要があります。



初回スキャン後は、データを継続的にスキャンして、増分変更を検出します（そのため、インスタンスの実行を維持することが重要です）。

スキャンは、ボリュームレベル、バケットレベル、データベーススキーマレベル、OneDrive ユーザレベル、SharePoint サイトレベルで有効または無効にできます。

マッピングスキャンと分類スキャンの違いは何ですか

Cloud Data Sense を使用すると、選択した作業環境やデータソースに対して、一般的な「マッピング」スキャンを実行できます。マッピングではデータの概要のみが示され、分類ではデータの詳細なスキャンが提供されます。データソースでは、ファイルにアクセスしてデータを参照できないため、マッピングは短時間で完了します。

多くのユーザは、この機能を気に入っています。たとえば、より多くの調査が必要なデータソースをすばやくスキャンして特定したうえで、必要なデータソースやボリュームに対してのみ分類スキャンを有効にする必要があるからです。

次の表に、いくつかの相違点を示します。

フィーチャー（Feature）	分類	マッピング
スキャン速度	遅い	高速
ファイルタイプと使用済み容量のリスト	はい。	はい。
ファイル数と使用済み容量	はい。	はい。
ファイルの経過時間とサイズ	はい。	はい。
を実行する機能 "データマッピングレポート"	はい。	はい。
[データ調査] ページでファイルの詳細を確認します	はい。	いいえ
ファイル内の名前を検索します	はい。	いいえ
作成 "ポリシー" カスタムの検索結果が表示されます	はい。	いいえ

フィーチャー（Feature）	分類	マッピング
AIP ラベルおよびステータスタグを使用してデータを分類します	はい。	いいえ
ソースファイルをコピー、削除、および移動します	はい。	いいえ
他のレポートを実行できます	はい。	いいえ

Cloud Data がインデックス化する情報

データセンズは、カテゴリを収集してインデックスを作成し、データ（ファイル）に割り当てます。データセンズインデックスには、次のデータが含まれます。

標準メタデータ

Cloud Data Sense は、ファイルの種類、サイズ、作成日、変更日など、ファイルに関する標準的なメタデータを収集します。

個人データ

メールアドレス、識別番号、クレジットカード番号など、個人を特定できる情報。"[個人データの詳細については、こちらをご覧ください](#)"。

機密性の高い個人データ

GDPR やその他のプライバシー規制で定義されている、健康データ、民族的起源、政治的見解などの機密情報の特殊な種類。"[機密性の高い個人データの詳細をご覧ください](#)"。

カテゴリ

Cloud Data Sense は、スキャンしたデータをさまざまなタイプのカテゴリに分割します。カテゴリは、各ファイルのコンテンツとメタデータの AI 分析に基づくトピックです。"[カテゴリの詳細については、こちらをご覧ください](#)"。

タイプ（Types）

Cloud Data Sense は、スキャンしたデータをファイルタイプ別に分類します。"[タイプの詳細については、こちらをご覧ください](#)"。

名前エンティティ認識

Cloud Data Sense は、AI を使用して、ドキュメントから自然な人物の名前を抽出します。"[データ主体のアクセスリクエストへの対応について説明します](#)"。

ネットワークの概要

Cloud Manager は、コネクタインスタンスからのインバウンド HTTP 接続を可能にするセキュリティグループを使用して、Cloud Data Sense インスタンスを導入します。

SaaS モードで Cloud Manager を使用する場合は、Cloud Manager への接続に HTTPS が使用され、ブラウザと Data Sense インスタンス間で送信されるプライベートデータはエンドツーエンドの暗号化で保護されます。つまり、ネットアップとサードパーティがこのデータを読み取ることはできません。

アウトバウンドルールは完全にオープンです。データセンズソフトウェアをインストールしてアップグレードし、使用率指標を送信するには、インターネットアクセスが必要です。

ネットワーク要件が厳しい場合は、["Cloud Data が接触するエンドポイントについて説明します"](#)。

コンプライアンス情報へのユーザアクセス

各ユーザには、Cloud Manager 内と Cloud Data Sense 内で異なる機能が割り当てられています。

- *** アカウント管理者 *** は、コンプライアンス設定を管理し、すべての作業環境のコンプライアンス情報を表示できます。
- *** ワークスペース管理者 *** は、アクセス権を持つシステムについてのみ、コンプライアンス設定を管理し、コンプライアンス情報を表示できます。ワークスペース管理者が Cloud Manager の作業環境にアクセスできない場合は、[データセンス] タブに作業環境のコンプライアンス情報が表示されません。
- **コンプライアンスビューア *** の役割を持つユーザーは、アクセス権を持つシステムのコンプライアンス情報を表示し、レポートを生成することのみができます。これらのユーザは、ボリューム、バケット、またはデータベーススキーマのスキャンを有効または無効にすることはできません。これらのユーザーは、ファイルのコピー、移動、または削除もできません。

["Cloud Manager のロールに関する詳細情報"](#) そして方法 ["特定のロールのユーザを追加します"](#)。

クラウドデータの導入センス

クラウドにクラウドデータセンスを導入

クラウドデータセンスをクラウドに導入するには、いくつかの手順を実行します。

また、次のことも可能です ["インターネットにアクセスできる Linux ホストに Data Sense を導入する"](#)。オンプレミスの ONTAP システムもオンプレミスにある Data Sense インスタンスを使用してオンプレミスの システムをスキャンする場合は、インストールのタイプを選択することをお勧めしますが、これは必須ではありません。どのインストール方法を選択しても、ソフトウェアはまったく同じように機能します。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

コネクタがない場合は、ここでコネクタを作成します。を参照してください ["AWS でコネクタを作成する"](#)、["Azure でコネクタを作成する"](#)または ["GCP でコネクタを作成する"](#)。

また可能です ["コネクタをオンプレミスに導入"](#) 自社ネットワーク内またはクラウド内の Linux ホスト

環境が前提条件を満たしていることを確認します。これには、インスタンスのアウトバウンドインターネットアクセス、ポート 443 を介したコネクタとクラウドデータセンスの接続などが含まれます。 [すべてのリストを参照してください](#)。

デフォルトの構成では、Cloud Data Sense インスタンス用に 16 個の vCPU が必要です。を参照してください ["インスタンスタイプの詳細"](#)。

インストールウィザードを起動して、クラウドに Cloud Data Sense インスタンスを導入します。

Cloud Data Sense によってスキャンされる最初の 1TB のデータは、Cloud Manager に無料で保存されています。そのあともデータのスキャンを続行するには、クラウドプロバイダ Marketplace での Cloud Manager

のサブスクリプション、または NetApp からの BYOL ライセンスが必要です。

コネクタを作成します

コネクタがない場合は、クラウドプロバイダでコネクタを作成します。を参照してください ["AWS でコネクタを作成する"](#) または ["Azure でコネクタを作成する"](#) または ["GCP でコネクタを作成する"](#)。ほとんどの場合、Cloud Data Sense を有効にする前にコネクタをセットアップしておくことができます ["Cloud Manager の機能にはコネクタが必要です"](#)ただし、ここで設定する必要がある場合もあります。

特定のクラウドプロバイダに導入されているコネクタを使用する必要がある場合は、次のような状況があります。

- AWS、Amazon FSX for ONTAP、または AWS S3 バケット内の Cloud Volumes ONTAP のデータをスキャンするときは、AWS のコネクタを使用します。
- Azure または Azure NetApp Files で Cloud Volumes ONTAP 内のデータをスキャンする場合は、Azure のコネクタを使用します。
- GCP の Cloud Volumes ONTAP でデータをスキャンする場合は、GCP のコネクタを使用します。

オンプレミスの ONTAP システム、ネットアップ以外のファイル共有、汎用の S3 オブジェクトストレージ、データベース、OneDrive フォルダ、SharePoint アカウント、Google ドライブ アカウントは、これらのクラウドコネクタのいずれかを使用している場合にスキャンできます。

また、次のことも可能です ["コネクタをオンプレミスに導入"](#) 自社ネットワーク内またはクラウド内の Linux ホストデータセンスをオンプレミスにインストールする予定のユーザによっては、Connector をオンプレミスにインストールすることもできます。

ご覧のように、を使用する必要がある状況もあります ["複数のコネクタ"](#)。



Azure NetApp Files ボリュームのスキャンを計画している場合は、スキャンするボリュームと同じリージョンに導入する必要があります。

前提条件を確認する

クラウドに Cloud Data Sense を導入する前に、以下の前提条件を確認し、サポートされている構成であることを確認してください。

Cloud Data Sense からのアウトバウンドインターネットアクセスを有効にする

Cloud Data Sense では、アウトバウンドのインターネットアクセスが必要。仮想ネットワークまたは物理ネットワークでインターネットアクセスにプロキシサーバを使用している場合は、Data sense インスタンスにアウトバウンドのインターネットアクセスがあり、次のエンドポイントに接続できることを確認します。クラウドにデータセンスを導入すると、コネクタと同じサブネットに配置されます。

AWS、Azure、GCP のいずれに Cloud Data Sense を導入しているかに応じて、次の表を参照してください。

- AWS 環境に必要なエンドポイント： *

エンドポイント	目的
https://cloudmanager.cloud.netapp.com	ネットアップアカウントを含む Cloud Manager サービスとの通信

エンドポイント	目的
¥ https://netapp-cloud-account.auth0.com ¥ https://auth0.com	NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	ソフトウェアイメージ、マニフェスト、およびテンプレートにアクセスできます。
\ https://kinesis.us-east-1.amazonaws.com	ネットアップが監査レコードからデータをストリーミングできるようにします。
¥ https://cognito-idp.us-east-1.amazonaws.com ¥ https://cognito-identity.us-east-1.amazonaws.com ¥ https://user-feedback-store-prod.s3.us-west-2.amazonaws.com ¥ https://customer-data-production.s3.us-west-2.amazonaws.com	Cloud Data Sense を使用して、マニフェストやテンプレートにアクセスしてダウンロードしたり、ログや指標を送信したりできます。

- Azure と GCP の導入に必要なエンドポイント： *

エンドポイント	目的
\ https://cloudmanager.cloud.netapp.com	ネットアップアカウントを含む Cloud Manager サービスとの通信
¥ https://netapp-cloud-account.auth0.com ¥ https://auth0.com	NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。
https://support.compliance.cloudmanager.cloud.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	ソフトウェアイメージ、マニフェスト、テンプレートへのアクセス、およびログとメトリックの送信を提供します。
\ https://support.compliance.cloudmanager.cloud.netapp.com/	ネットアップが監査レコードからデータをストリーミングできるようにします。

Cloud Manager に必要な権限が割り当てられていることを確認します

Cloud Manager に、リソースを導入する権限と、Cloud Data Sense インスタンス用のセキュリティグループを作成する権限があることを確認します。最新の Cloud Manager 権限は、で確認できます ["ネットアップが提供するポリシー"](#)。

vCPU の制限を確認してください

クラウドプロバイダの vCPU 制限によって、16 コアのインスタンスの導入が許可されていることを確認してください。Cloud Manager が実行されているリージョン内の関連するインスタンスファミリーの vCPU 制限を確認する必要があります。 ["必要なインスタンスタイプを参照してください"](#)。

vCPU の制限の詳細については、次のリンクを参照してください。

- ["AWS のドキュメント：Amazon EC2 サービスクォータ"](#)
- ["Azure のドキュメント：「仮想マシンの vCPU クォータ」"](#)
- ["Google Cloud のドキュメント：リソースクォータ"](#)

CPU 数と RAM 容量が少ないシステムには Data Sense を導入できますが、これらのシステムの使用には制限があります。を参照してください ["小さいインスタンスタイプを使用しています"](#) を参照してください。

Cloud Manager Connector が Cloud Data Sense にアクセスできることを確認する

コネクタと Cloud Data Sense インスタンス間の接続を確認します。コネクタのセキュリティグループは、Data Sense インスタンスとの間でポート 443 経由のインバウンドおよびアウトバウンドトラフィックを許可する必要があります。この接続により、データセンスインスタンスの展開が可能になり、[コンプライアンス（Compliance）] タブと [ガバナンス（Governance）] タブで情報を表示できます。Cloud Data Sense は、AWS や Azure の政府機関でサポートされています。

AWS と AWS GovCloud を導入する場合は、追加のインバウンドおよびアウトバウンドのルールが必要です。を参照してください ["AWS のコネクタのルール"](#) を参照してください。

Azure と Azure Government の環境には、追加のインバウンドルールとアウトバウンドルールが必要です。を参照してください ["Azure のコネクタのルール"](#) を参照してください。

クラウドデータを常に運用しておく必要があります

データを継続的にスキャンするには、Cloud Data Sense インスタンスがオンのままになっている必要があります。

Web ブラウザから Cloud Data Sense への接続を確認する

Cloud Data Sense を有効にしたら、データセンスインスタンスに接続されているホストから Cloud Manager のインターフェイスにユーザがアクセスすることを確認する。

データセンスインスタンスは、プライベート IP アドレスを使用して、インデックス付きデータがインターネットにアクセスできないようにします。そのため、Cloud Manager へのアクセスに使用する Web ブラウザは、そのプライベート IP アドレスに接続する必要があります。この接続は、クラウドプロバイダ（VPN など）への直接接続、またはデータセンスインスタンスと同じネットワーク内にあるホストから行うことができます。

クラウドにデータを導入するメリット

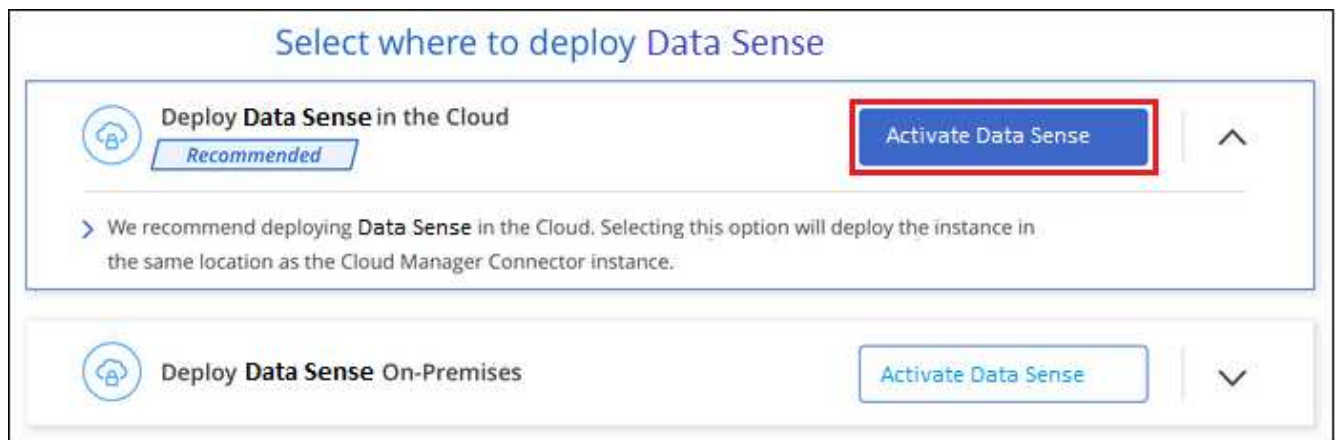
クラウドデータセンスのインスタンスをクラウドに導入するには、次の手順を実行します。

手順

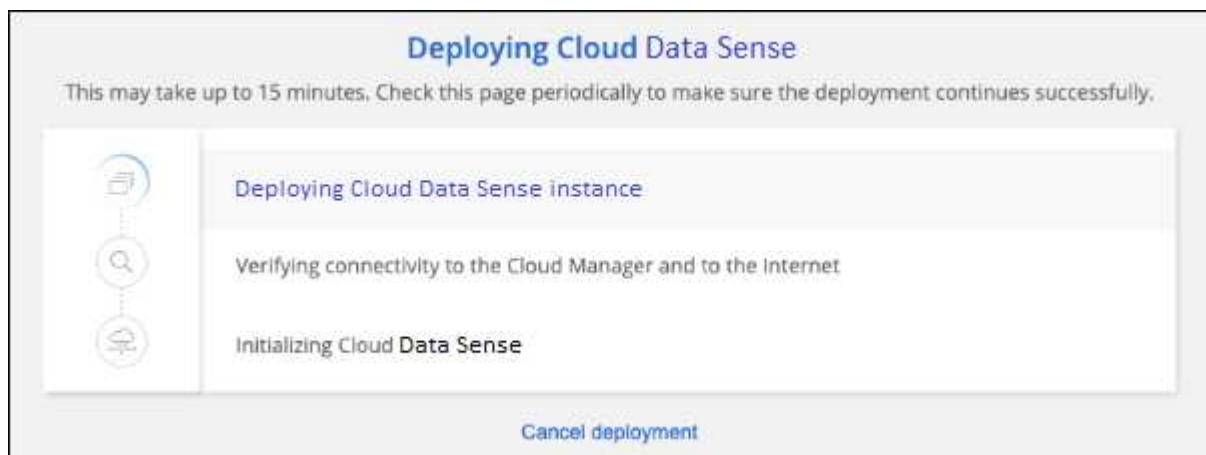
1. Cloud Manager で、* Data sense * をクリックします。
2. [データセンスを活動化（Activate Data sense）] をクリックし



3. Activate Data Sense * をクリックして、クラウド導入ウィザードを開始します。



4. 導入手順が完了すると、ウィザードに進捗状況が表示されます。問題が発生すると停止し、入力を求められます。



5. インスタンスが配備されたら、* 設定に進む * をクリックして _Configuration_page に移動します。

Cloud Manager によってクラウドデータ検出インスタンスがクラウドプロバイダに導入されます。

設定ページで、スキャンするデータソースを選択できます。

また可能です ["クラウドデータセンスのライセンスをセットアップする"](#) 現時点では、データ量が 1TB を超えるまでは料金は発生しません。

インターネットにアクセス可能な Linux ホストに Cloud Data Sense を導入する

ネットワーク内またはクラウド内でインターネットにアクセスできる Linux ホストに Cloud Data Sense を導入するには、いくつかの手順を実行します。

オンプレミスにあるデータセンスインスタンスを使用してオンプレミスの ONTAP システムをスキャンする場合は、オンプレミスインストールを選択することをお勧めします。ただしこれは必須ではありません。どのインストール方法を選択しても、ソフトウェアはまったく同じように機能します。

また、次のことも可能です ["インターネットにアクセスできないオンプレミスサイトにデータセンスを導入する"](#) 完全にセキュアなサイトに。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

コネクタがない場合は、ここでコネクタを作成します。を参照してください ["AWS でコネクタを作成する"](#)、["Azure でコネクタを作成する"](#)または ["GCP でコネクタを作成する"](#)。

また可能です ["コネクタをオンプレミスに導入"](#) 自社ネットワーク内またはクラウド内の Linux ホスト

環境が前提条件を満たしていることを確認します。これには、インスタンスのアウトバウンドインターネットアクセス、ポート 443 を介したコネクタとクラウドデータセンスの接続などが含まれます。 [すべてのリストを参照してください](#)。

とを満たす Linux システムも必要です [次の要件があります](#)。

ネットアップサポートサイトから Cloud Data Sense ソフトウェアをダウンロードし、使用する Linux ホストにインストーラファイルをコピーします。次に、インストールウィザードを起動し、プロンプトに従って Data Sense インスタンスを展開します。

Cloud Data Sense によってスキャンされる最初の 1TB のデータは、Cloud Manager に無料で保存されています。そのあともデータのスキャンを続行するには、クラウドプロバイダ Marketplace またはネットアップの BYOL ライセンスのサブスクリプションが必要です。

コネクタを作成します

コネクタがない場合は、クラウドプロバイダでコネクタを作成します。を参照してください ["AWS でコネクタを作成する"](#) または ["Azure でコネクタを作成する"](#)または ["GCP でコネクタを作成する"](#)。ほとんどの場合、Cloud Data Sense を有効にする前にコネクタをセットアップしておくことができます ["Cloud Manager の機能にはコネクタが必要です"](#)ただし、ここで設定する必要がある場合もあります。

特定のクラウドプロバイダに導入されているコネクタを使用する必要がある場合は、次のような状況があります。

- AWS、Amazon FSX for ONTAP、または AWS S3 バケット内の Cloud Volumes ONTAP のデータをスキャンするときは、AWS のコネクタを使用します。

- Azure または Azure NetApp Files で Cloud Volumes ONTAP 内のデータをスキャンする場合は、Azure のコネクタを使用します。
- GCP の Cloud Volumes ONTAP でデータをスキャンする場合は、GCP のコネクタを使用します。

オンプレミスのONTAP システムでは、ネットアップ以外のファイル共有、汎用のS3オブジェクトストレージ、データベース、OneDriveフォルダ、SharePointアカウント、Googleドライブアカウントを、これらのクラウドコネクタのいずれかを使用してスキャンできます。

また、次のことも可能です ["コネクタをオンプレミスに導入"](#) 自社ネットワーク内またはクラウド内の Linux ホストデータセンスをオンプレミスにインストールする予定のユーザによっては、Connector をオンプレミスにインストールすることもできます。

ご覧のように、を使用する必要がある状況もあります ["複数のコネクタ"](#)。



Azure NetApp Files ボリュームのスキャンを計画している場合は、スキャンするボリュームと同じリージョンに導入する必要があります。

Linux ホストシステムを準備

データセンسوフトウェアは、特定のオペレーティングシステム要件、RAM 要件、ソフトウェア要件などを満たすホストで実行する必要があります。データセンスは、他のアプリケーションと共有されるホストではサポートされません。ホストは専用のホストである必要があります。

- オペレーティングシステム： Red Hat Enterprise Linux または CentOS バージョン 8.0 または 8.1
 - OS が Docker エンジンを実装している必要があります（必要に応じて、`_firewalld_service` を無効にするなど）。
- Disk： 500GiB の SSD を /、またはで使えます
 - 100 GiB は /opt で利用できます
 - /var で 400GiB の可用性を確保
 - /tmp 上で 5 GiB
- RAM： 64GB（ホストでスワップメモリを無効にする必要があります）
- CPU： 16 コア

CPU 数と RAM 容量が少ないシステムには Data Sense を導入できますが、これらのシステムの使用には制限があります。を参照してください ["小さいインスタンスタイプを使用しています"](#) を参照してください。

- Red Hat Enterprise Linux システムは、Red Hat サブスクリプション管理に登録する必要があります。登録されていないと、インストール時に必要なサードパーティ製ソフトウェアを更新するためのリポジトリにアクセスできません。
- 次のソフトウェアがホストにインストールされている必要があります。ホストにソフトウェアがまだ存在しない場合は、インストーラによってソフトウェアがインストールされます。
 - Docker Engine バージョン 19 以降。 ["インストール手順を確認します"](#)。
 - Python 3 バージョン 3.6 以降。 ["インストール手順を確認します"](#)。

Cloud Manager と Data Sense の前提条件を確認

Linux システムに Cloud Data Sense を導入する前に、次の前提条件を確認し、サポートされている構成であることを確認してください。

Cloud Data Sense からのアウトバウンドインターネットアクセスを有効にする

Cloud Data Sense では、アウトバウンドのインターネットアクセスが必要。仮想ネットワークまたは物理ネットワークでインターネットアクセスにプロキシサーバを使用している場合は、Data sense インスタンスにアウトバウンドのインターネットアクセスがあり、次のエンドポイントに接続できることを確認します。

エンドポイント	目的
\ https://cloudmanager.cloud.netapp.com	ネットアップアカウントを含む Cloud Manager サービスとの通信
¥ https://netapp-cloud-account.auth0.com ¥ https://auth0.com	NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。
https://support.compliance.cloudmanager.cloud.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	ソフトウェアイメージ、マニフェスト、テンプレートへのアクセス、およびログとメトリックの送信を提供します。
\ https://support.compliance.cloudmanager.cloud.netapp.com/	ネットアップが監査レコードからデータをストリーミングできるようにします。
¥ https://github.com/docker ¥ https://download.docker.com ¥ http://mirror.centos.org ¥ http://mirrorlist.centos.org ¥ http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	インストールの前提条件パッケージを提供します。

Cloud Manager に必要な権限が割り当てられていることを確認します

Cloud Manager に、リソースを導入する権限と、Cloud Data Sense インスタンス用のセキュリティグループを作成する権限があることを確認します。最新の Cloud Manager 権限は、で確認できます "[ネットアップが提供するポリシー](#)"。

Cloud Manager Connector が Cloud Data Sense にアクセスできることを確認する

コネクタと Cloud Data Sense インスタンス間の接続を確認します。コネクタのセキュリティグループは、Data Sense インスタンスとの間でポート 443 経由のインバウンドおよびアウトバウンドトラフィックを許可する必要があります。

この接続により、データセンスインスタンスの展開が可能になり、[コンプライアンス (Compliance)] タブと [ガバナンス (Governance)] タブで情報を表示できます。

Cloud Manager でインストールの進捗状況を確認できるように、ポート 8080 が開いていることを確認してください。

クラウドデータを常に運用しておく必要があります

データを継続的にスキャンするには、Cloud Data Sense インスタンスがオンのままになっている必要があります。

Web ブラウザから Cloud Data Sense への接続を確認する

Cloud Data Sense を有効にしたら、データセンスインスタンスに接続されているホストから Cloud Manager のインターフェイスにユーザがアクセスすることを確認する。

データセンスインスタンスは、プライベート IP アドレスを使用して、インデックス付きデータがインターネットにアクセスできないようにします。そのため、Cloud Manager へのアクセスに使用する Web ブラウザは、そのプライベート IP アドレスに接続する必要があります。この接続は、クラウドプロバイダ（VPN など）への直接接続、またはデータセンスインスタンスと同じネットワーク内にあるホストから行うことができます。

オンプレミスにデータセンスを導入

一般的な構成では、ソフトウェアを 1 台のホストシステムにインストールします。 [これらの手順を参照してください](#)。

ペタバイト規模のデータをスキャンする大規模な構成では、複数のホストを含めて処理能力を追加できます。 [これらの手順を参照してください](#)。

を参照してください [Linux ホストシステムの準備](#) および [前提条件の確認](#) Cloud Data Sense を導入する前に、要件の一覧を確認してください。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。



Cloud Data Sense は、ソフトウェアがオンプレミスにインストールされている場合、現在 S3 バケット、Azure NetApp Files、または FSX for ONTAP をスキャンできない。このような場合は、クラウドとに別のコネクタとデータセンスのインスタンスを導入する必要があります "[コネクタを切り替えます](#)" データソースごとに異なる。

一般的な構成でのシングルホストインストール

単一のオンプレミスホストに Data Sense ソフトウェアをインストールする場合は、次の手順を実行します。

必要なもの

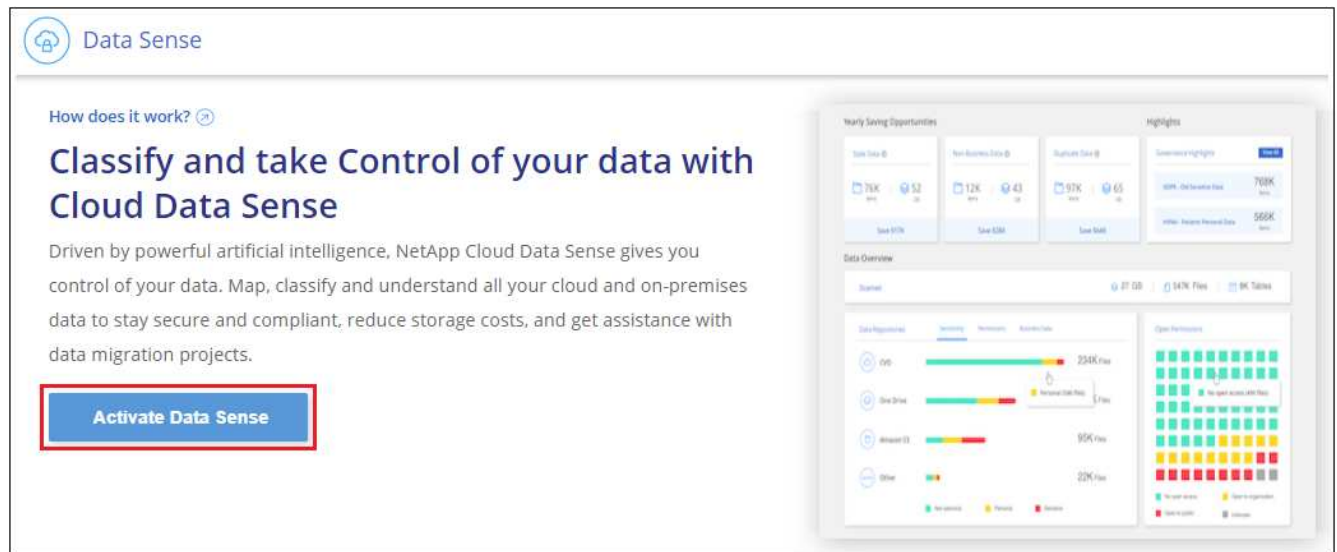
- Linux システムが満たしていることを確認します [ホストの要件](#)。
- （オプション）システムに、前提条件となる 2 つのソフトウェアパッケージ（Docker Engine と Python 3）がインストールされていることを確認します。このソフトウェアがシステムにインストールされていない場合は、インストーラによってインストールされます。
- Linux システムに対する root 権限があることを確認してください。
- プロキシを使用していて、TLS 代行受信を実行している場合は、TLS CA 証明書が保存されている Data Sense Linux システム上のパスを確認する必要があります。
- オフライン環境が要件を満たしていることを確認します [権限と接続](#)。

手順

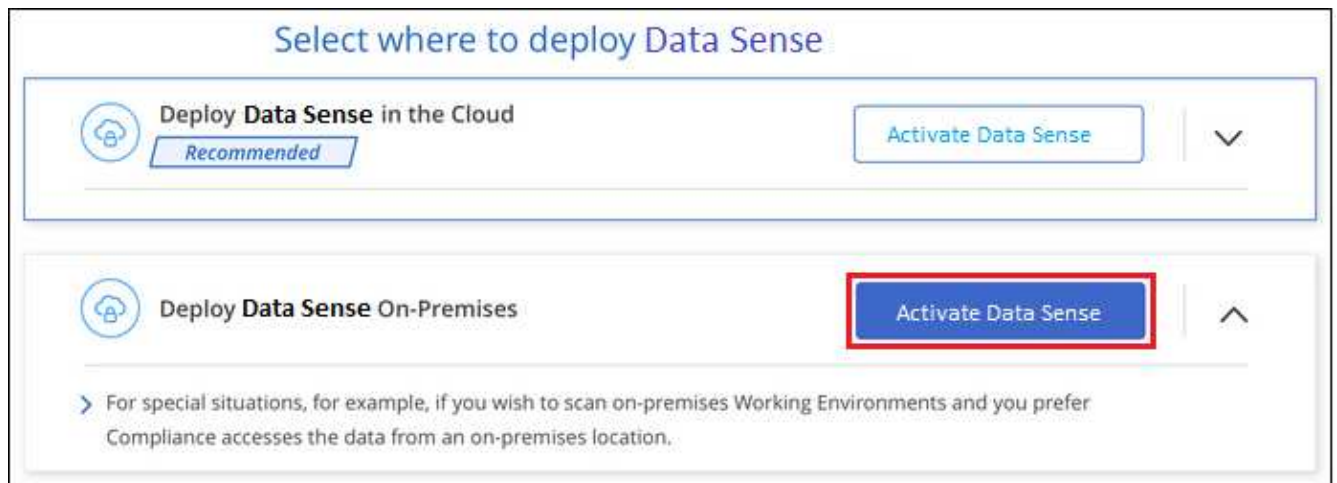
1. から Cloud Data Sense ソフトウェアをダウンロードします "[ネットアップサポートサイト](#)"。選択するフ

ファイルの名前は * cc_onpm_installer_<バージョン>.tar.gz * です。

2. 使用する Linux ホストにインストーラファイルをコピーします (cp またはその他の方法を使用)。
3. Cloud Manager で、 * Data sense * をクリックします。
4. [データセンスを活動化 (Activate Data sense)] をクリックし



5. Activate Data Sense * をクリックして、オンプレミス導入ウィザードを開始します。



6. _Deploy Data Sense on Premises_ Dialog で、提供されたコマンドをコピーしてテキストファイルに貼り付け、後で使用できるようにして、 * Close * をクリックします。例：

「sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq」と入力します

7. ホストマシンでインストーラファイルを解凍します。次に例を示します。

```
tar -xzf cc_onprem_installer_1.10.0.tar.gz
```

8. インストーラからプロンプトが表示されたら、一連のプロンプトに必要な値を入力するか、インストーラに必要なパラメータをコマンドライン引数として指定することができます。

プロンプトに従ってパラメータを入力します。	完全なコマンドを入力します。
<p>a. 手順 6 からコピーした情報を貼り付けます。 'UDO./install.sh -a <account_id>-c <agent_id>-t<token>`</p> <p>b. コネクタインスタンスからアクセスできるように、Data Sense ホストマシンの IP アドレスまたはホスト名を入力します。</p> <p>c. Cloud Manager Connector ホストマシンの IP アドレスまたはホスト名を入力して、Data Sense インスタンスからアクセスできるようにします。</p> <p>d. プロンプトが表示されたら、プロキシの詳細を入力Cloud Manager ですでにプロキシが使用されている場合は、Cloud Manager が使用するプロキシが Data Sense で自動的に使用されるため、ここでもう一度入力する必要はありません。</p>	<p>また、必要なホストパラメータとプロキシパラメータを指定して、コマンド全体を事前に作成することもできます。 <code>sudo ./install.sh -a <account_id> -c <agent_id> -t <token> -host <ds_host> --proxy-host <cm_host> --proxy-host <proxy_host> -proxy-port <proxy-dir password> -proxy-password-dir <proxy-password></code></p>

変数値：

- ° `_account_id _` = ネットアップアカウント ID
- ° `_agent_id _` = コネクタ ID
- ° `_ctoken _` = JWT ユーザートークン
- ° `ds_host` = Data Sense Linux システムの IP アドレスまたはホスト名
- ° `cm_host`= Cloud Manager Connector システムの IP アドレスまたはホスト名。
- ° `proxy_host` = ホストがプロキシサーバの背後にある場合は、プロキシサーバの IP 名またはホスト名。
- ° `proxy_port`= プロキシサーバに接続するポート（デフォルトは 80 ）です。
- ° `proxy_scheme`= 接続方式： https または http （デフォルト http ）。
- ° `proxy_user`= ベーシック認証が必要な場合、プロキシサーバに接続するための認証されたユーザ。
- ° `proxy_password` = 指定したユーザ名のパスワード。
- ° `ca_cert_dir`= 追加の TLS CA 証明書バンドルを含む Data Sense Linux システム上のパス。プロキシが TLS 代行受信を実行している場合にのみ必要です。

Cloud Data Sense インストーラは、パッケージのインストール、Docker のインストール、インストールの登録、および Data Sense のインストールを行います。インストールには 10~20 分かかります。

ホストマシンとコネクタインスタンス間のポート 8080 を介した接続がある場合、Cloud Manager の Data sense タブにインストールの進行状況が表示されます。

設定ページで、スキャンするデータソースを選択できます。

また可能です ["クラウドデータセンスのライセンスをセットアップする"](#) 現時点では、データ量が 1TB を超えるまでは料金は発生しません。

ペタバイト規模のデータをスキャンする大規模な構成では、複数のホストを含めて処理能力を追加できます。複数のホストシステムを使用する場合、プライマリシステムは `_Managernode_name` と呼ばれ、追加の処理能力を提供する追加システムは `_Scanner Node_` と呼ばれます。

複数のオンプレミスホストに Data Sense ソフトウェアをインストールする場合は、次の手順を実行します。

必要なもの

- Manager ノードと Scanner ノードのすべての Linux システムが、を満たしていることを確認します [ホストの要件](#)。
- (オプション) システムに、前提条件となる 2 つのソフトウェアパッケージ (Docker Engine と Python 3) がインストールされていることを確認します。このソフトウェアがシステムにインストールされていない場合は、インストーラによってインストールされます。
- Linux システムに対する root 権限があることを確認してください。
- 環境が要件を満たしていることを確認します [権限と接続](#)。
- 使用するスキャナードホストの IP アドレスを確認しておく必要があります。
- すべてのホストで次のポートとプロトコルを有効にする必要があります。

ポート	プロトコル	説明
2377	TCP	クラスタ管理通信
7946	tcp 、 udp です	ノード間通信
4789	UDP	オーバーレイネットワークトラフィック
50	ESP	暗号化された IPsec オーバーレイネットワーク (ESP) トラフィック
111	tcp 、 udp です	ホスト間でファイルを共有するための NFS サーバ (各スキャナードからマネージャードに必要)
2049	tcp 、 udp です	ホスト間でファイルを共有するための NFS サーバ (各スキャナードからマネージャードに必要)

手順

1. の手順 1~7 を実行します [シングルホストインストール](#) マネージャード。
2. 手順 8 で示したように、インストーラからプロンプトが表示されたら、一連のプロンプトに必要な値を入力するか、必要なパラメータをコマンドライン引数としてインストーラに指定することができます。

シングルホストのインストールで使える変数に加えて、新しいオプション `* -n <Node_IP> *` を使用してスキャナードの IP アドレスを指定します。複数のスキャナードの IP はカンマで区切って指定します。

たとえば、次のコマンドは 3 つのスキャナードを追加します。 `'sudo ./install.sh -a <account_id>-c <agent_id>-t <token> --host <ds_host> --manager-host <cm_host> * -n <node-ip1> 、 <node-ip2> 、 <node-ip3>*-proxy-proxy-proxy-host-pproxy-pxe-password</password>`

3. マネージャードのインストールが完了する前に、スキャナードに必要なインストールコマンドがダイアログに表示されます。コマンドをコピーし、テキストファイルに保存します。例：

```
sudo ./node_install.sh -m 10.11.12.13-t ふぁいる EF-1u69m1-1s35212`
```

4. 各 * スキャナノードホストで：

- データセンスインストーラファイル（* cc_onpm_installer_<バージョン>.tar.gz *）をホストマシンにコピーします（「cp」などの方法を使用）。
- インストーラファイルを解凍します。
- 手順 3 でコピーしたコマンドを貼り付けて実行します。

すべてのスキャナノードでインストールが完了し、それらのノードがマネージャノードに参加したら、マネージャノードのインストールも完了します。

Cloud Data Sense インストーラがパッケージ、Docker のインストールを完了し、インストールを登録します。インストールには 10~20 分かかります。

設定ページで、スキャンするデータソースを選択できます。

また可能です ["クラウドデータセンスのライセンスをセットアップする"](#) 現時点では、データ量が 1TB を超えるまでは料金は発生しません。

クラウドデータをオンプレミスに導入しても、インターネットアクセスは不要

インターネットにアクセスできないオンプレミスサイトのホストに Cloud Data Sense を導入するには、いくつかの手順を実行します。このタイプのインストールは、セキュアなサイトに最適です。

また、次のことも可能です ["インターネットにアクセス可能なオンプレミスサイトにデータセンスを導入"](#)。

サポートされているデータソース

この方法でインストールすると（「オフライン」または「ダーク」サイトと呼ばれることもあります）、データ検出でスキャンできるのは、オンプレミスサイトに対してもローカルなデータソースのデータのみです。現時点では、Data Sense は次のローカルデータソースをスキャンできます。

- オンプレミスの ONTAP システム
- データベーススキーマ
- ネットアップ以外の NFS または CIFS ファイル共有
- Simple Storage Service （S3）プロトコルを使用するオブジェクトストレージ

Cloud Manager を非常にセキュアにインストールする必要があるが、OneDrive アカウントまたは SharePoint アカウントからローカルデータをスキャンする場合は、Data Sense オフラインインストーラを使用して、選択したいいくつかのエンドポイントへのインターネットアクセスを提供できます。を参照してください [SharePoint と OneDrive の特別な要件](#) を参照してください。

現在、データセンスがダークサイトに導入されている場合、Cloud Volumes ONTAP、Azure NetApp Files、ONTAP 用 FSX、AWS S3、または Google ドライブのアカウントのスキャンはサポートされません。

制限

ほとんどのデータセンシブ機能は、インターネットにアクセスできないサイトに導入されている場合に機能します。ただし、インターネットアクセスを必要とする特定の機能はサポートされていません。たとえば、次のような機能があります。

- Microsoft Azure Information Protection (AIP) ラベルの管理
- 特定の重大ポリシーが結果を返すときに Cloud Manager ユーザに E メールアラートを送信する
- さまざまなユーザに対する Cloud Manager ロールの設定 (Account Admin や Compliance Viewer など)
- Cloud Sync を使用したソースファイルのコピーと同期
- ユーザからのフィードバックを受け取る
- Cloud Manager からのソフトウェアの自動アップグレード

Cloud Manager Connector と Data Sense は、新しい機能を有効にするために、定期的な手動アップグレードを必要とします。Data Sense バージョンは、Data Sense UI ページの下部に表示されます。を確認します ["Cloud Data Sense リリースノート"](#) 各リリースの新機能と、それらの機能が必要かどうかを確認できます。次に、の手順を実行します [データセンシブソフトウェアをアップグレードします](#)。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

オフラインのオンプレミスサイトにコネクタがまだインストールされていない場合は、["コネクタを配置します"](#) Linux ホストの場合は、

Linux システムが満たしていることを確認します [ホストの要件](#) 必要なソフトウェアがすべてインストールされていること、およびオフライン環境が要件を満たしていることを確認します [権限と接続](#)。

ネットアップサポートサイトから Cloud Data Sense ソフトウェアをダウンロードし、使用する Linux ホストにインストーラファイルをコピーします。次に、インストールウィザードを起動し、プロンプトに従って Cloud Data Sense インスタンスを導入します。

Cloud Data Sense によってスキャンされる最初の 1TB のデータは、Cloud Manager に無料で保存されています。そのあともデータのスキャンを続行するには、ネットアップの BYOL ライセンスが必要です。

Cloud Manager Connector をインストール

オフラインのオンプレミスサイトに Cloud Manager Connector がインストールされていない場合は、["コネクタを配置します"](#) オフラインサイトの Linux ホスト

Linux ホストシステムを準備

データセンシブソフトウェアは、特定のオペレーティングシステム要件、RAM 要件、ソフトウェア要件などを満たすホストで実行する必要があります。データセンシブは、他のアプリケーションと共有されるホストではサポートされません。ホストは専用のホストである必要があります。

- オペレーティングシステム：Red Hat Enterprise Linux または CentOS バージョン 8.0 または 8.1
 - OS が Docker Engine をインストールできる必要があります (必要に応じて、_firewalld_service を無

効にするなど）。

- Disk : 500GiB の SSD を /、またはで使用できます
 - 100 GiB は /opt で利用できます
 - /var で 400GiB の可用性を確保
 - /tmp 上で 5 GiB
- RAM : 64GB (ホストでスワップメモリを無効にする必要があります)
- CPU : 16 コア

CPU 数と RAM 容量が少ないシステムには Data Sense を導入できますが、これらのシステムの使用には制限があります。を参照してください "[小さいインスタンスタイプを使用しています](#)" を参照してください。

Data Sense をインストールする前に、次のソフトウェアをホストにインストールする必要があります。

- Docker Engine バージョン 19 以降。 "[インストール手順を確認します](#)".
- Python 3 バージョン 3.6 以降。 "[インストール手順を確認します](#)".

Cloud Manager と Data Sense の前提条件を確認

Cloud Data Sense を導入する前に、次の前提条件を確認し、サポートされている構成であることを確認してください。

- Cloud Manager に、リソースを導入する権限と、 Cloud Data Sense インスタンス用のセキュリティグループを作成する権限があることを確認します。
- Cloud Manager Connector がデータセンスインスタンスにアクセスできることを確認します。コネクタのセキュリティグループは、 Data Sense インスタンスとの間でポート 443 経由のインバウンドおよびアウトバウンドトラフィックを許可する必要があります。

この接続により、データセンスインスタンスの展開が可能になり、コンプライアンスとガバナンスの情報を表示できます。

Cloud Manager でインストールの進捗状況を確認できるように、ポート 8080 が開いていることを確認してください。

- クラウドデータを常に運用しておく必要がありますデータを継続的にスキャンするには、 Cloud Data Sense インスタンスがオンのままになっている必要があります。
- Web ブラウザから Cloud Data Sense への接続を確認するCloud Data Sense を有効にしたら、データセンスインスタンスに接続されているホストから Cloud Manager のインターフェイスにユーザがアクセスすることを確認する。

データセンスインスタンスは、プライベート IP アドレスを使用して、インデックス付きデータが他のユーザーにアクセスできないようにします。そのため、 Cloud Manager へのアクセスに使用する Web ブラウザは、そのプライベート IP アドレスに接続する必要があります。この接続は、データセンスインスタンスと同じネットワーク内にあるホストから確立できます。

SharePoint と OneDrive の特別な要件

Cloud Manager と Data Sense がインターネットにアクセスできないサイトに導入されている場合は、SharePoint アカウントと OneDrive アカウントでローカルファイルをスキャンできます。そのためには、選択したいいくつかのエンドポイントへのインターネットアクセスが提供されています。

エンドポイント	目的
¥ login.microsoft.com ¥ graph.microsoft.com	選択したオンラインサービスにログインするための Microsoft サーバとの通信。
\ https://cloudmanager.cloud.netapp.com	ネットアップアカウントを含む Cloud Manager サービスとの通信

cloudmanager.cloud.netapp.com へのアクセスは、これらの外部サービスへの初期接続時にのみ必要です。

データセンスの導入

一般的な構成では、ソフトウェアを 1 台のホストシステムにインストールします。"[これらの手順を参照してください](#)"。

ペタバイト規模のデータをスキャンする大規模な構成では、複数のホストを含めて処理能力を追加できます。"[これらの手順を参照してください](#)"。

一般的な構成でのシングルホストインストール

オフライン環境で単一のオンプレミスホストに Data Sense ソフトウェアをインストールする場合は、次の手順を実行します。

必要なもの

- Linux システムが満たしていることを確認します [ホストの要件](#)。
- 前提条件となる 2 つのソフトウェアパッケージ（Docker Engine と Python 3）がインストールされていることを確認します。
- Linux システムに対する root 権限があることを確認してください。
- オフライン環境が要件を満たしていることを確認します [権限と接続](#)。

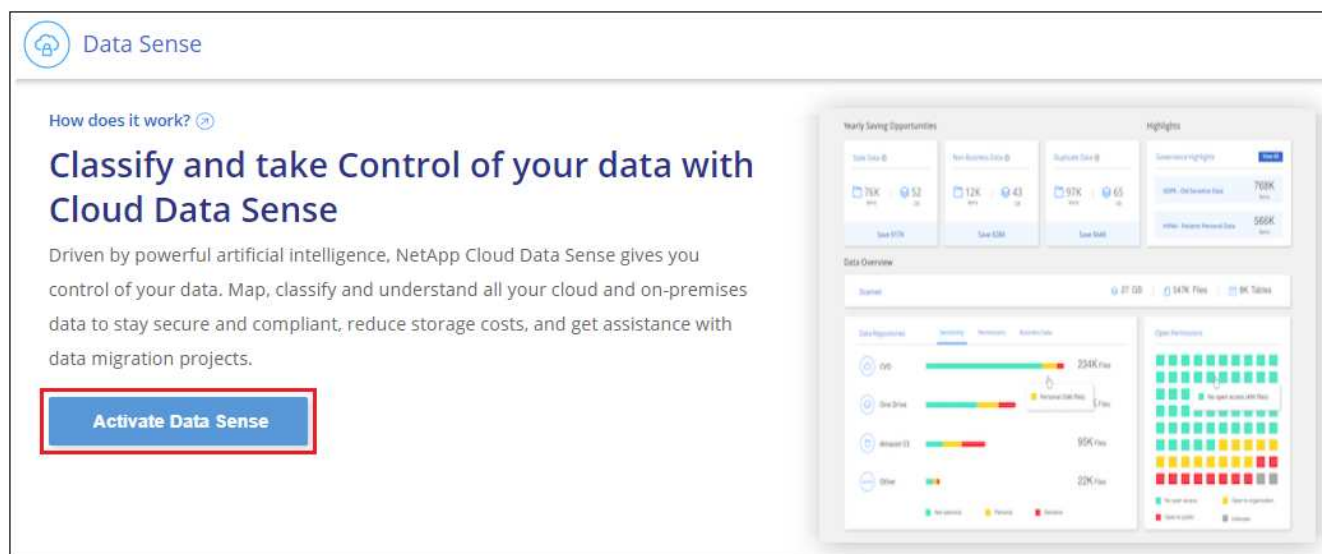
手順

1. インターネットに接続されたシステムで、から Cloud Data Sense ソフトウェアをダウンロードします "[ネットアップサポートサイト](#)"。選択するファイルの名前は * DataSense - offline-bundle-<version>.tar.gz * です。
2. ダークサイトで使用する Linux ホストにインストーラバンドルをコピーします。
3. ホストマシンでインストーラバンドルを解凍します。次に例を示します。

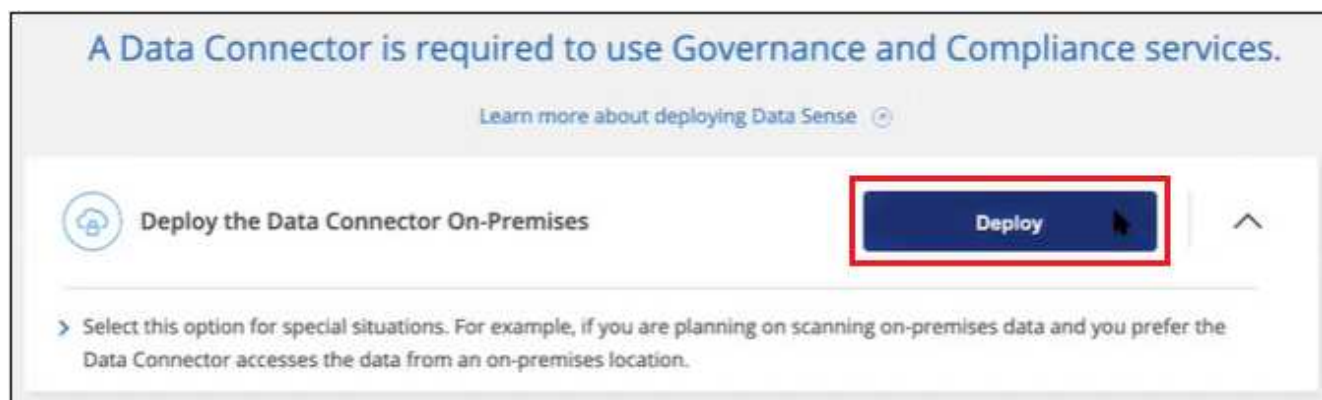
```
tar -xzf DataSense-offline-bundle-v1.10.0.tar.gz
```

これにより、必要なソフトウェアと実際のインストールファイル * cc_onpm_installer_<version>.tar.gz * が抽出されます。

- Cloud Manager を起動し、* Data Sense * タブをクリックします。
- [データセンスを活動化 (Activate Data sense)] をクリックし



- [Deploy *] をクリックして、オンプレミス展開ウィザードを開始します。



- _Deploy Data Sense on Premises_ Dialog で、提供されたコマンドをコピーしてテキストファイルに貼り付け、後で使用できるようにして、* Close * をクリックします。例：

```
「 sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq — darksite
```

- ホストマシンでインストールファイルを解凍します。次に例を示します。

```
tar -xzf cc_onprem_installer_1.10.0.tar.gz
```

- インストーラからプロンプトが表示されたら、一連のプロンプトに必要な値を入力するか、インストーラに必要なパラメータをコマンドライン引数として指定することができます。

プロンプトに従ってパラメータを入力します。	完全なコマンドを入力します。
<p>a. 手順 7 からコピーした情報を貼り付けます。 '<code>UDO./ install.sh -a <account_id> -c <agent_id> -t <token> --darksite</code></p> <p>b. コネクタインスタンスからアクセスできるように、Data Sense ホストマシンの IP アドレスまたはホスト名を入力します。</p> <p>c. Cloud Manager Connector ホストマシンの IP アドレスまたはホスト名を入力して、Data Sense インスタンスからアクセスできるようにします。</p>	<p>また、必要なホストパラメータとして、「<code>sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <DS_host> --manager-host <cm_host> --no-proxy --darksite</code>」を事前に指定して、コマンド全体を作成することもできます</p>

変数値：

- `_account_id` = ネットアップアカウント ID
- `_agent_id` = コネクタ ID
- `_ctoken` = JWT ユーザートークン
- `ds_host` = Data Sense Linux システムの IP アドレスまたはホスト名
- `cm_host` = Cloud Manager Connector システムの IP アドレスまたはホスト名。

Data Sense インストーラは、パッケージをインストールし、インストールを登録し、Data Sense をインストールします。インストールには 10~20 分かかります。

ホストマシンとコネクタインスタンス間のポート 8080 を介した接続がある場合、Cloud Manager の Data sense タブにインストールの進行状況が表示されます。

設定ページからローカルを選択できます ["オンプレミスの ONTAP クラスタ"](#) および ["データベース"](#) をスキャンします。

また可能です ["クラウドデータセンスを使用する BYOL ライセンスをセットアップする"](#) 現時点では、デジタルウォレットのページから入手できます。データ量が 1TB を超えるまでは料金は発生しません。

大規模構成向けのマルチホストインストール

ペタバイト規模のデータをスキャンする大規模な構成では、複数のホストを含めて処理能力を追加できます。複数のホストシステムを使用する場合、プライマリシステムは `_Managernode_name` と呼ばれ、追加の処理能力を提供する追加システムは `_Scanner Node_` と呼ばれます。

オフライン環境で複数のオンプレミスホストに Data Sense ソフトウェアをインストールする場合は、次の手順を実行します。

必要なもの

- Manager ノードと Scanner ノードのすべての Linux システムが、を満たしていることを確認します [ホストの要件](#)。
- 前提条件となる 2 つのソフトウェアパッケージ（Docker Engine と Python 3）がインストールされていることを確認します。
- Linux システムに対する root 権限があることを確認してください。

- オフライン環境が要件を満たしていることを確認します [権限と接続](#)。
- 使用するスキャナードホストの IP アドレスを確認しておく必要があります。
- すべてのホストで次のポートとプロトコルを有効にする必要があります。

ポート	プロトコル	説明
2377	TCP	クラスタ管理通信
7946	tcp 、 udp です	ノード間通信
4789	UDP	オーバーレイネットワークトラフィック
50	ESP	暗号化された IPsec オーバーレイネットワーク（ESP）トラフィック
111	tcp 、 udp です	ホスト間でファイルを共有するための NFS サーバ（各スキャナードからマネージャードに必要）
2049	tcp 、 udp です	ホスト間でファイルを共有するための NFS サーバ（各スキャナードからマネージャードに必要）

手順

1. から手順 1~8 を実行します ["シングルホストインストール"](#) マネージャード。
2. 手順 9 に示すように、インストーラからプロンプトが表示されたら、一連のプロンプトで必要な値を入力するか、必要なパラメータをコマンドライン引数としてインストーラに指定することができます。

シングルホストのインストールで使用できる変数に加えて、新しいオプション `* -n <Node_IP> *` を使用してスキャナードの IP アドレスを指定します。複数のノードの IP をカンマで区切って指定します。

たとえば、次のコマンドは 3 つのスキャナードを追加します。 `'sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <DS_host> --manager-host <cm_host> * -n <node-ip1> 、 <node-ip2> 、 <node-dark3> *-no-proxy-site`

3. マネージャードのインストールが完了する前に、スキャナードに必要なインストールコマンドがダイアログに表示されます。コマンドをコピーし、テキストファイルに保存します。例：

```
sudo ./node_install.sh -m 10.11.12.13-t ふぁいる EF-1u69m1-1s35212`
```

4. 各 * スキャナードホストで：
 - a. データセンズインストーラファイル（ `* cc_onpm_installer_<バージョン>.tar.gz *` ）をホストマシンにコピーします。
 - b. インストーラファイルを解凍します。
 - c. 手順 3 でコピーしたコマンドを貼り付けて実行します。

すべてのスキャナードでインストールが完了し、それらのノードがマネージャードに参加したら、マネージャードのインストールも完了します。

Cloud Data Sense インストーラがパッケージのインストールを完了し、インストールを登録します。インストールには 15 ～ 25 分かかる場合があります。

設定ページからローカルを選択できます ["オンプレミスの ONTAP クラスタ"](#) および local です ["データベース"](#)

をスキャンします。

また可能です ["クラウドデータセンスを使用する BYOL ライセンスをセットアップする"](#) 現時点では、デジタルウォレットのページから入手できます。データ量が 1TB を超えるまでは料金は発生しません。

Data Sense ソフトウェアをアップグレードする

データセンスソフトウェアは定期的に新しい機能で更新されるため、定期的に新しいバージョンをチェックして最新のソフトウェアや機能を使用していることを確認する必要があります。自動的にアップグレードを実行するためのインターネット接続がないため、Data Sense ソフトウェアを手動でアップグレードする必要があります。

作業を開始する前に

- データセンスソフトウェアは、一度に 1 つのメジャーバージョンをアップグレードできます。たとえば、バージョン 1.9.x がインストールされている場合は、1.10.x にのみアップグレードできますいくつかのメジャーバージョンがサポートされている場合は、ソフトウェアを何度もアップグレードする必要があります。
- オンプレミスコネクタソフトウェアが最新バージョンにアップグレードされていることを確認します。 "[コネクタのアップグレード手順を参照してください](#)"。

手順

1. インターネットに接続されたシステムで、から Cloud Data Sense ソフトウェアをダウンロードします ["ネットアップサポートサイト"](#)。選択するファイルの名前は * DataSense - offline-bundle-<version>.tar.gz * です。
2. ダークサイトにデータセンスをインストールした Linux ホストにソフトウェアバンドルをコピーします。
3. ホストマシンでソフトウェアバンドルを解凍します。次に例を示します。

```
tar -xvf DataSense-offline-bundle-v1.10.0.tar.gz
```

これにより、インストールファイル * cc_onpm_installer_<バージョン>.tar.gz * が抽出されます。

4. ホストマシンでインストールファイルを解凍します。次に例を示します。

```
tar -xzf cc_onprem_installer_1.10.0.tar.gz
```

これにより、アップグレードスクリプト * START_ダーク site_upgrade.sh * および必要なサードパーティ製ソフトウェアが抽出されます。

5. ホストマシンでアップグレードスクリプトを実行します。次に例を示します。

```
start_darksite_upgrade.sh
```

データセンスソフトウェアはホスト上でアップグレードされます。更新には 5 ～ 10 分かかる場合があります。

非常に大規模な構成のスキャン用に複数のホストシステムに Data Sense を導入している場合は、スキャナノ

ードをアップグレードする必要はありません。

ソフトウェアが更新されたことを確認するには、Data Sense UI ページの下部にあるバージョンを確認します。

データソースでスキャンをアクティブ化します

Cloud Volumes ONTAP とオンプレミス **ONTAP** 向けのクラウドデータサービスの導入を開始する方法をご紹介します

Cloud Data Sense を使用して、Cloud Volumes ONTAP とオンプレミスの ONTAP ボリュームのスキャンを開始するには、いくつかの手順を実行します。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

ボリュームをスキャンする前に、Cloud Manager でシステムを作業環境として追加する必要があります。

- Cloud Volumes ONTAP システムの場合、これらの作業環境はすでに Cloud Manager で使用可能になっている必要があります
- オンプレミスの ONTAP システムでは、**"ONTAP クラスタは Cloud Manager で検出する必要があります"**

"クラウドデータの導入センス" インスタンスが展開されていない場合。

[* データセンス *] をクリックし、[* 構成 *] タブを選択して、特定の作業環境でボリュームのコンプライアンススキャンを有効にします。

Cloud Data Sense が有効になったので、すべてのボリュームにアクセスできることを確認します。

- クラウドデータセンスインスタンスには、各 Cloud Volumes ONTAP サブネットまたはオンプレミスの ONTAP システムへのネットワーク接続が必要です。
- Cloud Volumes ONTAP のセキュリティグループは、データセンスインスタンスからのインバウンド接続を許可する必要があります。
- これらのポートが Data Sense インスタンスに対して開いていることを確認します。
 - NFS –ポート 111 および 2049。
 - CIFS の場合 - ポート 139 および 445
- NFS ボリュームエクスポートポリシーで、データセンスインスタンスからのアクセスを許可する必要があります。
- CIFS ボリュームをスキャンするには、Active Directory クレデンシャルが必要です。

コンプライアンス * > * 構成 * > * CIFS クレデンシャルの編集 * をクリックし、クレデンシャルを入力します。

スキャンするボリュームを選択または選択解除すると、Cloud Data Sense でスキャンが開始または停止します。

スキャンするデータソースを検出しています

スキャンするデータソースがまだ Cloud Manager 環境にない場合は、ここでキャンバスに追加できます。

Cloud Volumes ONTAP システムは、Cloud Manager のキャンバスですでに使用できるようになっている必要があります。オンプレミスの ONTAP システムには、が必要です ["これらのクラスタは Cloud Manager で検出されます"](#)。

Cloud Data Sense インスタンスの導入

導入済みのインスタンスがない場合は Cloud Data Sense を導入

インターネット経由でアクセス可能な Cloud Volumes ONTAP およびオンプレミス ONTAP システムをスキャンする場合は、を実行します ["クラウドにクラウドデータセンスを導入"](#) または ["インターネットにアクセスできるオンプレミスの場所"](#)。

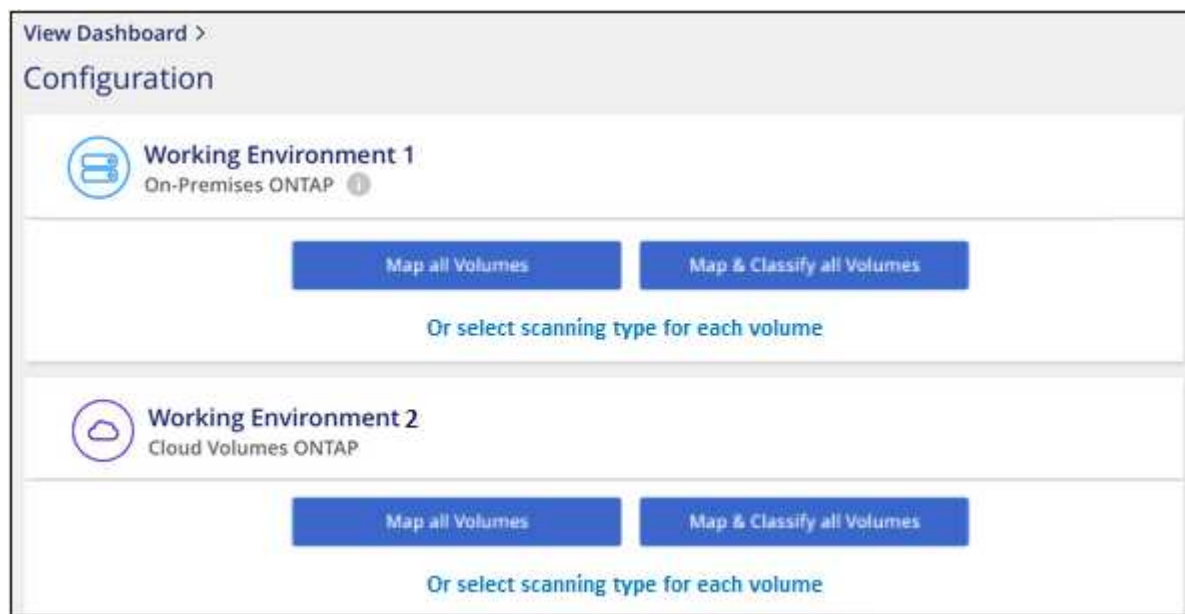
インターネットにアクセスできないデータサイトにインストールされているオンプレミスの ONTAP システムをスキャンする場合は、を実行する必要があります ["クラウドデータセンスは、インターネットにアクセスできないオンプレミス環境に導入できます"](#)。そのため、Cloud Manager Connector をオンプレミスと同じ場所に導入する必要があります。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

作業環境でクラウドデータを有効に活用

クラウドデータセンスは、Cloud Volumes ONTAP システム（AWS、Azure、GCP）とオンプレミスの ONTAP クラスタで有効にすることができます。

1. Cloud Manager の上部で、* Data Sense * をクリックし、* Configuration * タブを選択します。



クリーンショット。"]

タブのス

2. 各作業環境でボリュームをスキャンする方法を選択します。 ["マッピングおよび分類スキャンについて説明します"](#)：

- すべてのボリュームをマップするには、* すべてのボリュームをマップ * をクリックします。
- すべてのボリュームをマップして分類するには、* すべてのボリュームをマップして分類 * をクリックします。
- 各ボリュームのスキャンをカスタマイズするには、「*」をクリックするか、各ボリュームのスキャンタイプを選択してから、マッピングまたは分類するボリュームを選択します。

を参照してください [ボリュームのコンプライアンススキャンの有効化と無効化](#) を参照してください。

3. 確認ダイアログボックスで、[* 承認] をクリックして、ボリュームのスキャンを開始するデータセンスを設定します。

Cloud Data Sense により、作業環境で選択したボリュームのスキャンが開始されます。結果は、Cloud Data Sense が最初のスキャンを完了するとすぐに Compliance ダッシュボードに表示されます。所要時間はデータ量によって異なります。数分から数時間かかる場合もあります。

Cloud Data Sense がボリュームにアクセスできることの確認

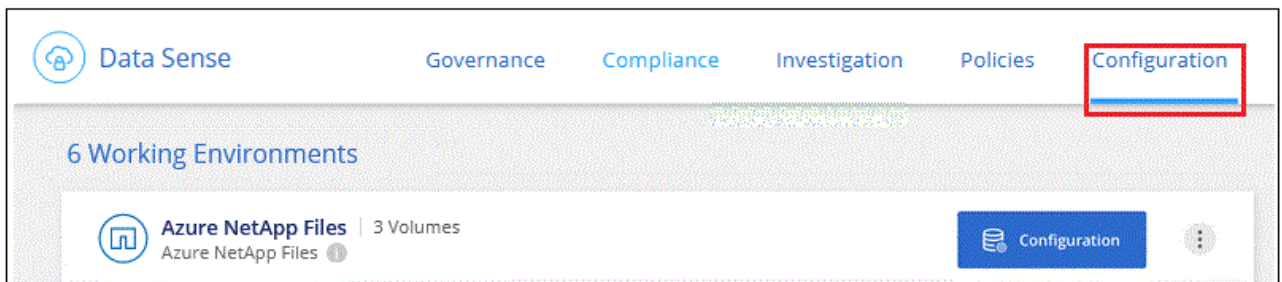
ネットワーク、セキュリティグループ、およびエクスポートポリシーを確認して、Cloud Data Sense でボリュームにアクセスできることを確認します。CIFS ボリュームにアクセスできるようにするには、CIFS クレデンシャルをデータセンスに指定する必要があります。

手順

1. クラウドデータセンスインスタンスと、Cloud Volumes ONTAP またはオンプレミスの ONTAP クラスターのボリュームを含む各ネットワークとの間にネットワーク接続が確立されていることを確認します。
2. Cloud Volumes ONTAP のセキュリティグループがデータセンスインスタンスからのインバウンドトラフィックを許可していることを確認します。

データセンスインスタンスの IP アドレスからのトラフィックのセキュリティグループを開くか、仮想ネットワーク内からのすべてのトラフィックのセキュリティグループを開くことができます。

3. 次のポートがデータセンスインスタンスに対して開いていることを確認します。
 - NFS - ポート 111 および 2049。
 - CIFS の場合 - ポート 139 および 445
4. NFS ボリュームのエクスポートポリシーに、各ボリュームのデータにアクセスできるように Data sense インスタンスの IP アドレスが含まれていることを確認します。
5. CIFS を使用する場合は、CIFS ボリュームをスキャンできるように、Active Directory クレデンシャルを使用したデータセンスを設定します。
 - a. Cloud Manager の上部で、* Data Sense * をクリックします。
 - b. [* 構成 *] タブをクリックします。

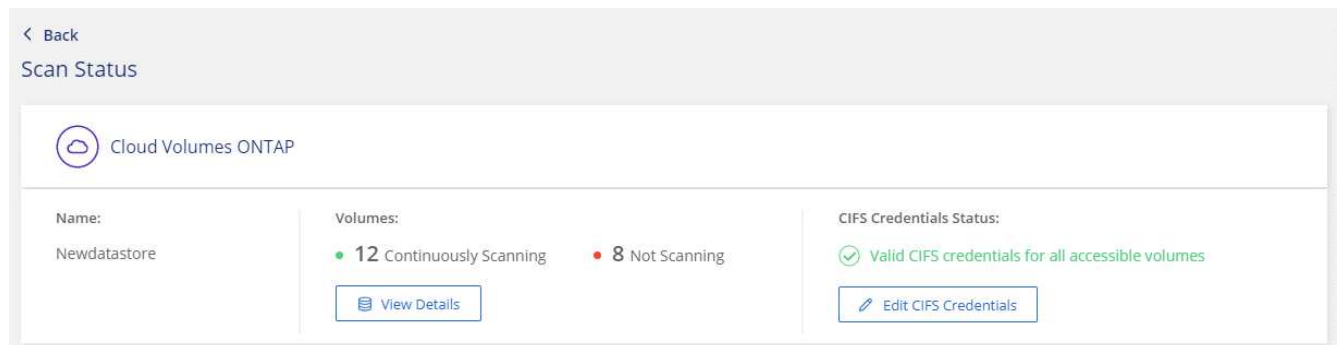


ボタンを示す [遵守] タブのスクリーンショット。"]

- c. 各作業環境について、* CIFS 資格情報の編集 * をクリックし、システム上の CIFS ボリュームにアクセスするために必要なユーザー名とパスワードを入力します。

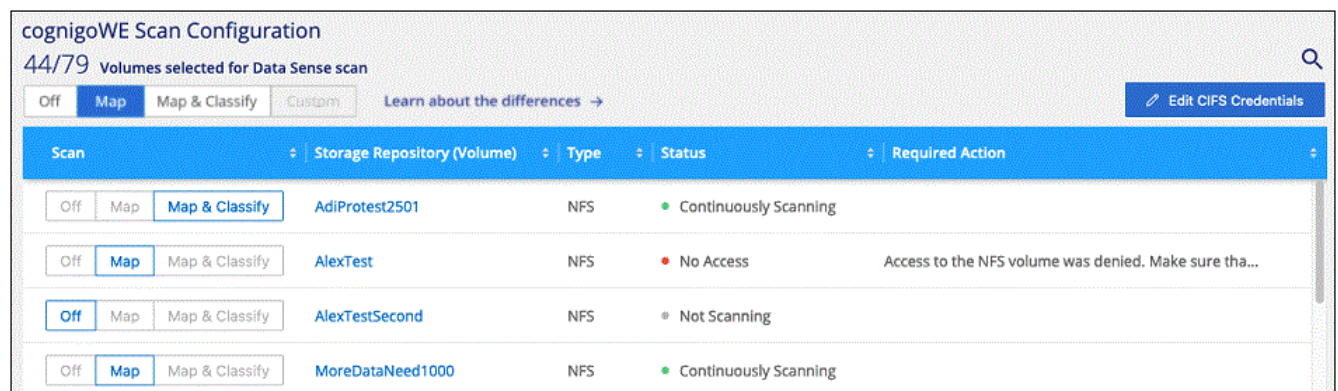
クレデンシャルは読み取り専用ですが、管理者のクレデンシャルを指定することで、データセンスは昇格された権限が必要なデータを読み取ることができます。クレデンシャルは Cloud Data Sense インスタンスに保存されます。

クレデンシャルを入力すると、すべての CIFS ボリュームが認証されたことを示すメッセージが表示されます。



6. _Configuration_page で、*View Details * をクリックして、各 CIFS および NFS ボリュームのステータスを確認し、エラーを修正します。

たとえば、次の図は 4 つのボリュームを示しています。1 つは、データセンスインスタンスとボリュームの間のネットワーク接続の問題が原因でクラウドデータセンスでスキャンできないボリュームです。



ボリュームのコンプライアンススキャンの有効化と無効化

設定ページからは、作業環境でマッピング専用スキャンまたはマッピングおよび分類スキャンをいつでも開始または停止できます。マッピングのみのスキャンからマッピングおよび分類スキャンに変更することもできま

す。また、マッピングのみのスキャンからマッピングおよび分類スキャンに変更することもできます。すべてのボリュームをスキャンすることを推奨します。

cognitoWE Scan Configuration					
44/79 Volumes selected for Data Sense scan					
<div> Off Map Map & Classify Custom Learn about the differences → Edit CIFS Credentials </div>					
Scan	Storage Repository (Volume)	Type	Status	Required Action	
Off Map Map & Classify	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...	
Off Map Map & Classify	AdiProtest2501	NFS	Continuously Scanning		
Off Map Map & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...	
Off Map Map & Classify	AlexTestSecond	NFS	Not Scanning		
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously Scanning		

終了：	手順：
ボリュームに対してマッピングのみのスキャンを有効にします	ボリューム領域で、* マップ * をクリックします
ボリュームでフルスキャンを有効にします	ボリューム領域で、* マップと分類 * をクリックします
ボリュームのスキャンを無効にします	ボリューム領域で、* オフ * をクリックします
すべてのボリュームでマッピングのみのスキャンを有効にします	見出し領域で、* マップ * をクリックします
すべてのボリュームでフルスキャンを有効にします	見出し領域で、* マップと分類 * をクリックします
すべてのボリュームでスキャンを無効にします	見出し領域で、* Off * をクリックします



作業環境に追加された新しいボリュームは、見出し領域で * Map * または * Map & Classify * の設定を行った場合にのみ自動的にスキャンされます。見出し領域で * Custom * または * Off * に設定すると、作業環境に追加する新しいボリュームごとに、マッピングまたはフルスキャンを有効にする必要があります。

データ保護ボリュームをスキャンしています

デフォルトでは、データ保護（DP）ボリュームは外部から公開されておらず、クラウドデータセンスでアクセスできないため、スキャンされません。オンプレミスの ONTAP システムまたは Cloud Volumes ONTAP システムからの SnapMirror 処理のデスティネーションボリュームです。

最初は、ボリュームリストでこれらのボリュームを Type* DP * でスキャンしていないステータス * および必要なアクション _* DP ボリュームへのアクセスを有効にします *。

'Working Environment Name' Configuration

22/28 Volumes selected for compliance scan

Enable Access to DP Volumes [Edit CIFS Credentials](#)

Off **Map** Map & Classify Custom [Learn about the differences](#) →

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	VolumeName1	DP	Not Scanning	Enable access to DP Volumes ⓘ
Off Map Map & Classify	VolumeName2	NFS	Continuously Scanning	
Off Map Map & Classify	VolumeName3	CIFS	Not Scanning	

これらのデータ保護ボリュームをスキャンする場合は、次の手順を実行します。

1. ページ上部の * DP ボリュームへのアクセスを有効にする * をクリックします。
2. 確認メッセージを確認し、もう一度「* DP ボリュームへのアクセスを有効にする *」をクリックします。
 - ソース ONTAP システムで最初に NFS ボリュームとして作成されたボリュームが有効になります。
 - ソース ONTAP システムで最初に CIFS ボリュームとして作成されたボリュームでは、それらの DP ボリュームをスキャンするために CIFS クレデンシャルを入力する必要があります。Cloud Data Sense で CIFS ボリュームをスキャンするためにすでに Active Directory のクレデンシャルを入力している場合は、それらのクレデンシャルを使用できます。また、別の管理クレデンシャルを指定することもできます。

Provide Active Directory Credentials

☒ Use existing CIFS Scanning Credentials (user1@domain2) ☐ Use Custom Credentials

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

Enable Access to DP Volumes Cancel

Provide Active Directory Credentials

☐ Use existing CIFS Scanning Credentials (user1@domain2) ☒ Use Custom Credentials

Username ⓘ Password ⓘ

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

Enable Access to DP Volumes Cancel

3. スキャンする各 DP ボリュームをアクティブ化します [他のボリュームも有効にした場合と同じです](#)。

有効にすると、スキャン対象としてアクティブ化された各 DP ボリュームから NFS 共有が作成されます。共有エクスポートポリシーでは、データセンスインスタンスからのアクセスのみが許可されます。

- ・ 注： DP ボリュームへのアクセスを最初に有効にしたときに CIFS データ保護ボリュームがない場合は、あとで追加しても、CIFS DP の有効化ボタン * が設定ページの上部に表示されます。このボタンをクリックして、CIFS DP ボリュームへのアクセスを有効にする CIFS クレデンシャルを追加します。



Active Directory クレデンシャルは、最初の CIFS DP ボリュームの Storage VM にのみ登録されているため、その SVM 上のすべての DP ボリュームがスキャンされます。他の SVM 上のボリュームには Active Directory クレデンシャルが登録されないため、これらの DP ボリュームはスキャンされません。

Azure NetApp Files 向けクラウドデータセンスの導入を開始する方法をご確認ください

Azure NetApp Files 向けクラウドデータセンスの導入を開始するには、いくつかの手順を実行します。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

Azure NetApp Files ボリュームをスキャンする前に、["構成を検出するには、Cloud Manager が設定されている必要があります"](#)。

["Cloud Manager に Cloud Data Sense を導入"](#) インスタンスが展開されていない場合。

コンプライアンス * をクリックし、* 構成 * タブを選択して、特定の作業環境でボリュームのコンプライアンススキャンを有効にします。

Cloud Data Sense が有効になったので、すべてのボリュームにアクセスできることを確認します。

- クラウドデータセンスインスタンスには、各 Azure NetApp Files サブネットへのネットワーク接続が必要です。
- これらのポートが Data Sense インスタンスに対して開いていることを確認します。
 - NFS –ポート 111 および 2049。
 - CIFS の場合 - ポート 139 および 445
- NFS ボリュームエクスポートポリシーで、データセンスインスタンスからのアクセスを許可する必要があります。
- CIFS ボリュームをスキャンするには、Active Directory クレデンシャルが必要です。

コンプライアンス * > * 構成 * > * CIFS クレデンシャルの編集 * をクリックし、クレデンシャルを入力します。

スキャンするボリュームを選択または選択解除すると、Cloud Data Sense でスキャンが開始または停止します。

スキャンする **Azure NetApp Files** システムを検出しています

スキャンする Azure NetApp Files システムがまだ作業環境として Cloud Manager にはない場合は、この時点でキャンバスに追加できます。

["Cloud Manager で Azure NetApp Files システムを検出する方法をご覧ください"](#)。

Cloud Data Sense インスタンスの導入

["クラウドデータの導入センス"](#) インスタンスが展開されていない場合。

Azure NetApp Files ボリュームをスキャンするときは、データセンスをクラウドに導入する必要があります。また、スキャンするボリュームと同じリージョンに導入する必要があります。

- ・注：* オンプレミスの場所にクラウドデータセンスを導入することは、Azure NetApp Files ボリュームのスキャンでは現在サポートされていません。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

作業環境でクラウドデータを有効に活用

Azure NetApp Files ボリュームでクラウドデータセンスを有効にすることができます。

1. Cloud Manager の上部で、* Data Sense * をクリックし、* Configuration * タブを選択します。



タブのスク

リーンショット。"]

2. 各作業環境でボリュームをスキャンする方法を選択します。"[マッピングおよび分類スキャンについて説明します](#)"：
 - すべてのボリュームをマップするには、* すべてのボリュームをマップ * をクリックします。
 - すべてのボリュームをマップして分類するには、* すべてのボリュームをマップして分類 * をクリックします。
 - 各ボリュームのスキャンをカスタマイズするには、「*」をクリックするか、各ボリュームのスキャンタイプを選択してから、マッピングまたは分類するボリュームを選択します。

を参照してください [ボリュームのコンプライアンススキャンの有効化と無効化](#) を参照してください。

3. 確認ダイアログボックスで、[* 承認] をクリックして、ボリュームのスキャンを開始するデータセンスを設定します。

Cloud Data Sense により、作業環境で選択したボリュームのスキャンが開始されます。結果は、Cloud Data Sense が最初のスキャンを完了するとすぐに Compliance ダッシュボードに表示されます。所要時間はデータ量によって異なります。数分から数時間かかる場合もあります。

Cloud Data Sense がボリュームにアクセスできることの確認

ネットワーク、セキュリティグループ、およびエクスポートポリシーを確認して、Cloud Data Sense でボリュームにアクセスできることを確認します。CIFS ボリュームにアクセスできるようにするには、CIFS クレデンシャルをデータセン스에指定する必要があります。

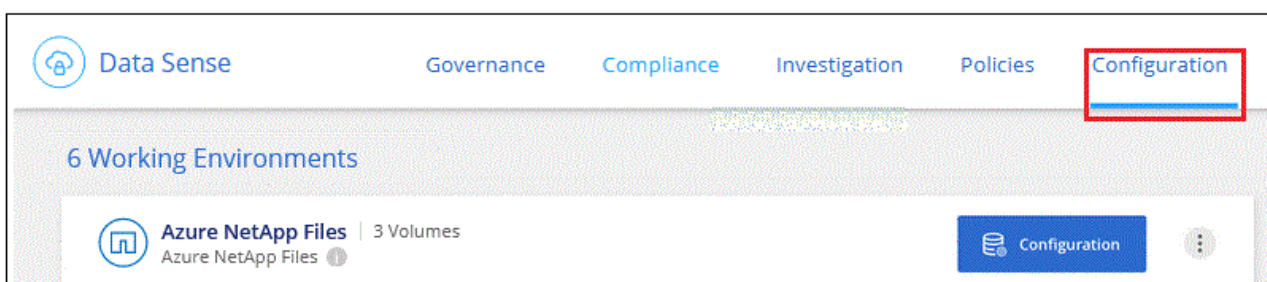
手順

1. クラウドデータセンスインスタンスと、Azure NetApp Files 用のボリュームを含む各ネットワークの間にネットワーク接続が確立されていることを確認します。



Azure NetApp Files の場合、Cloud Data Sense は Cloud Manager と同じリージョンにあるボリュームのみをスキャンできます。

2. 次のポートがデータセンシブインスタンスに対して開いていることを確認します。
 - NFS –ポート 111 および 2049。
 - CIFS の場合 - ポート 139 および 445
3. NFS ボリュームのエクスポートポリシーに、各ボリュームのデータにアクセスできるように Data sense インスタンスの IP アドレスが含まれていることを確認します。
4. CIFS を使用する場合は、CIFS ボリュームをスキャンできるように、Active Directory クレデンシャルを使用したデータセンシブを設定します。
 - a. Cloud Manager の上部で、* Data Sense * をクリックします。
 - b. [* 構成 *] タブをクリックします。

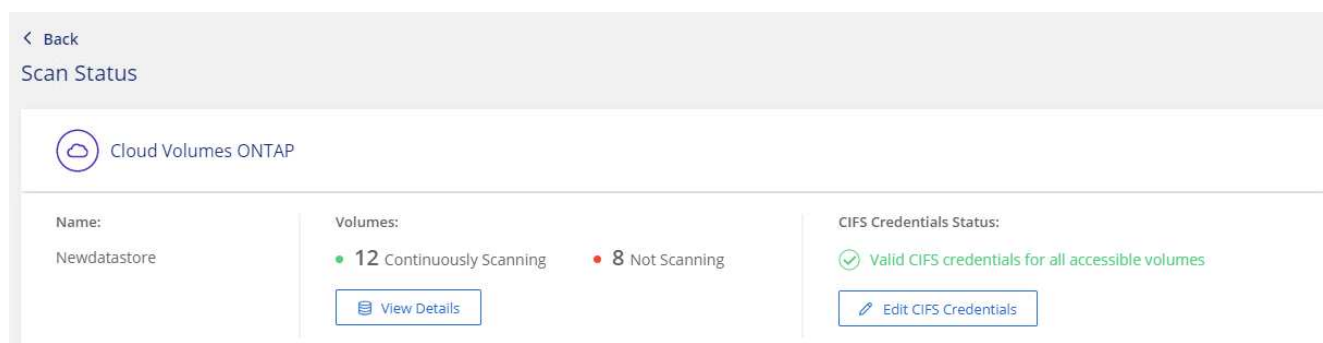


ボタンを示す [遵守] タブのスクリーンショット。"]

- c. 各作業環境について、* CIFS 資格情報の編集 * をクリックし、システム上の CIFS ボリュームにアクセスするために必要なユーザー名とパスワードを入力します。

クレデンシャルは読み取り専用ですが、管理者のクレデンシャルを指定することで、データセンシブは昇格された権限が必要なデータを読み取ることができます。クレデンシャルは Cloud Data Sense インスタンスに保存されます。

クレデンシャルを入力すると、すべての CIFS ボリュームが認証されたことを示すメッセージが表示されます。



5. _Configuration_page で、*View Details * をクリックして、各 CIFS および NFS ボリュームのステータスを確認し、エラーを修正します。

たとえば、次の図は 4 つのボリュームを示しています。1 つは、データセンシブインスタンスとボリュームの間のネットワーク接続の問題が原因でクラウドデータセンシブでスキャンできないボリュームです。

cognitoWE Scan Configuration				
44/79 Volumes selected for Data Sense scan				
<div> Off Map Map & Classify Custom Learn about the differences → Edit CIFS Credentials </div>				
Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	AdiProtest2501	NFS	Continuously Scanning	
Off Map Map & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
Off Map Map & Classify	AlexTestSecond	NFS	Not Scanning	
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously Scanning	

ボリュームのコンプライアンススキャンの有効化と無効化

設定ページからは、作業環境でマッピング専用スキャンまたはマッピングおよび分類スキャンをいつでも開始または停止できます。マッピングのみのスキャンからマッピングおよび分類スキャンに変更することもできます。また、マッピングのみのスキャンからマッピングおよび分類スキャンに変更することもできます。すべてのボリュームをスキャンすることを推奨します。

cognitoWE Scan Configuration				
44/79 Volumes selected for Data Sense scan				
<div> Off Map Map & Classify Custom Learn about the differences → Edit CIFS Credentials </div>				
Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
Off Map Map & Classify	AdiProtest2501	NFS	Continuously Scanning	
Off Map Map & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
Off Map Map & Classify	AlexTestSecond	NFS	Not Scanning	
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously Scanning	

終了：	手順：
ボリュームに対してマッピングのみのスキャンを有効にします	ボリューム領域で、 * マップ * をクリックします
ボリュームでフルスキャンを有効にします	ボリューム領域で、 * マップと分類 * をクリックします
ボリュームのスキャンを無効にします	ボリューム領域で、 * オフ * をクリックします
すべてのボリュームでマッピングのみのスキャンを有効にします	見出し領域で、 * マップ * をクリックします
すべてのボリュームでフルスキャンを有効にします	見出し領域で、 * マップと分類 * をクリックします
すべてのボリュームでスキャンを無効にします	見出し領域で、 * Off * をクリックします



作業環境に追加された新しいボリュームは、見出し領域で * Map * または * Map & Classify * の設定を行った場合にのみ自動的にスキャンされます。見出し領域で * Custom * または * Off * に設定すると、作業環境に追加する新しいボリュームごとに、マッピングまたはフルスキャンを有効にする必要があります。

Amazon FSX for ONTAP のクラウドデータセンスを今すぐ始めましょう

クラウドデータセンスを使用した Amazon FSX for ONTAP ボリュームのスキャンを開始するには、いくつかの手順を実行します。

作業を開始する前に

- データセンスを導入および管理するには、AWS にアクティブなコネクタが必要です。
- 作業環境の作成時に選択したセキュリティグループは、Cloud Data Sense インスタンスからのトラフィックを許可する必要があります。関連付けられたセキュリティグループは、FSX for ONTAP ファイルシステムに接続されている ENI を使用して検索し、AWS 管理コンソールを使用して編集できます。

"Linux インスタンス用の AWS セキュリティグループ"

"Windows インスタンス用の AWS セキュリティグループ"

"AWS Elastic Network Interface (ENI) "

クイックスタート

以下の手順を実行してすぐに作業を開始するか、下にスクロールして詳細を確認してください。

FSX で ONTAP ボリュームをスキャンする前に、**"ボリュームが設定された FSX 作業環境が必要です"**。

"Cloud Manager に Cloud Data Sense を導入" インスタンスが展開されていない場合。

[* データセンス *] をクリックし、[* 構成 *] タブを選択して、特定の作業環境でボリュームのコンプライアンススキャンを有効にします。

Cloud Data Sense が有効になったので、すべてのボリュームにアクセスできることを確認します。

- クラウドデータセンスインスタンスには、ONTAP サブネットの各 FSX へのネットワーク接続が必要です。
- 次のポートがデータセンスインスタンスに対して開いていることを確認します。
 - NFS –ポート 111 および 2049。
 - CIFS の場合 - ポート 139 および 445
- NFS ボリュームエクスポートポリシーで、データセンスインスタンスからのアクセスを許可する必要があります。
- CIFS ボリュームをスキャンするには、Active Directory クレデンシャルが必要です。+ コンプライアンス * > * 構成 * > * CIFS クレデンシャルの編集 * をクリックし、クレデンシャルを入力します。

スキャンするボリュームを選択または選択解除すると、Cloud Data Sense でスキャンが開始または停止します。

スキャンする **ONTAP** ファイルシステムの **FSX** を検出します

スキャンする FSX for ONTAP ファイルシステムが作業環境としてまだ Cloud Manager にはない場合は、この時点でキャンバスに追加できます。

"Cloud Manager で ONTAP ファイルシステムの FSX を検出または作成する方法については、[を参照してください](#)。"

Cloud Data Sense インスタンスの導入

"クラウドデータの導入センス" インスタンスが展開されていない場合。

Connector for AWS とスキャン対象の FSX ボリュームと同じ AWS ネットワークに Data Sense を導入する必要があります。

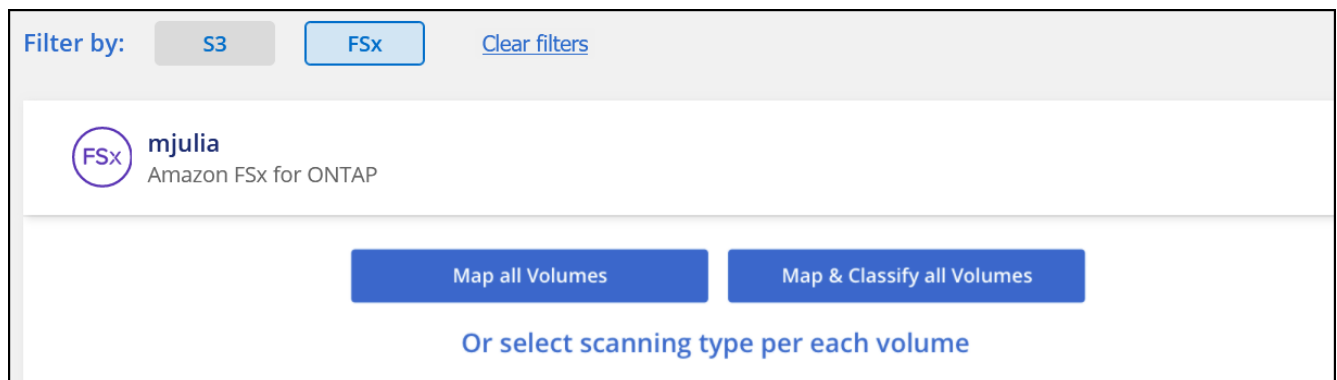
- ・注：* オンプレミスの場所にクラウドデータセンスを導入することは、現在 FSX ボリュームのスキャンではサポートされていません。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

作業環境でクラウドデータを有効に活用

ONTAP ボリュームの FSX に対してクラウドデータセンスを有効にすることができます。

1. Cloud Manager の上部で、* Data Sense * をクリックし、* Configuration * タブを選択します。



タブのスクリーンショット。"]

2. 各作業環境でボリュームをスキャンする方法を選択します。"[マッピングおよび分類スキャンについて説明します](#)"：
 - すべてのボリュームをマップするには、* すべてのボリュームをマップ * をクリックします。
 - すべてのボリュームをマップして分類するには、* すべてのボリュームをマップして分類 * をクリックします。
 - 各ボリュームのスキャンをカスタマイズするには、「*」をクリックするか、各ボリュームのスキャンタイプを選択してから、マッピングまたは分類するボリュームを選択します。

を参照してください [ボリュームのコンプライアンススキャンの有効化と無効化](#) を参照してください。

3. 確認ダイアログボックスで、[* 承認] をクリックして、ボリュームのスキャンを開始するデータセンスを設定します。

Cloud Data Sense により、作業環境で選択したボリュームのスキャンが開始されます。結果は、Cloud Data Sense が最初のスキャンを完了するとすぐに Compliance ダッシュボードに表示されます。所要時間はデータ量によって異なります。数分から数時間かかる場合もあります。

Cloud Data Sense がボリュームにアクセスできることの確認

ネットワーク、セキュリティグループ、およびエクスポートポリシーを確認して、Cloud Data Sense でボリュームにアクセスできることを確認します。

CIFS ボリュームにアクセスできるようにするには、CIFS クレデンシャルをデータセンスに指定する必要があります。

手順

1. _Configuration_page で、**View Details** をクリックしてステータスを確認し、エラーを修正します。

たとえば、次の図は、データセンスインスタンスとボリュームの間のネットワーク接続の問題が原因で、ボリュームの Cloud Data Sense によるスキャンができないことを示しています。

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	jrmclone	NFS	No Access	Check network connectivity between the Data Sense ...

2. クラウドデータセンスインスタンスと各ネットワークの間に、FSX for ONTAP のボリュームを含むネットワーク接続があることを確認します。



FSX for ONTAP の場合、Cloud Data Sense は Cloud Manager と同じリージョンのボリュームのみをスキャンできます。

3. 次のポートがデータセンスインスタンスに対して開いていることを確認します。
 - NFS –ポート 111 および 2049。
 - CIFS の場合 - ポート 139 および 445
4. NFS ボリュームのエクスポートポリシーに Data Sense インスタンスの IP アドレスが含まれていて、各ボリュームのデータにアクセスできることを確認します。
5. CIFS を使用する場合は、CIFS ボリュームをスキャンできるように、Active Directory クレデンシャルを使用したデータセンスを設定します。
 - a. Cloud Manager の上部で、* Data Sense * をクリックします。
 - b. [* 構成 *] タブをクリックします。
 - c. 各作業環境について、* CIFS 資格情報の編集 * をクリックし、システム上の CIFS ボリュームにアクセスするために必要なユーザー名とパスワードを入力します。

クレデンシャルは読み取り専用ですが、管理者のクレデンシャルを指定することで、データセンスは昇格された権限が必要なデータを読み取ることができます。クレデンシャルは Cloud Data Sense インスタンスに保存されます。

クレデンシャルを入力すると、すべての CIFS ボリュームが認証されたことを示すメッセージが表示されます。

ボリュームのコンプライアンススキャンの有効化と無効化

設定ページからは、作業環境でマッピング専用スキャンまたはマッピングおよび分類スキャンをいつでも開始または停止できます。マッピングのみのスキャンからマッピングおよび分類スキャンに変更することもできます。また、マッピングのみのスキャンからマッピングおよび分類スキャンに変更することもできます。すべてのボリュームをスキャンすることを推奨します。

cognigoWE Scan Configuration

44/79 Volumes selected for Data Sense scan

Off

Map

Map & Classify

Custom

Learn about the differences →

Edit CIFS Credentials

Scan	Storage Repository (Volume)	Type	Status	Required Action
<div>Off</div> <div>Map</div> <div>Map & Classify</div>	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<div>Off</div> <div>Map</div> <div>Map & Classify</div>	AdiProtest2501	NFS	Continuously Scanning	
<div>Off</div> <div>Map</div> <div>Map & Classify</div>	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<div>Off</div> <div>Map</div> <div>Map & Classify</div>	AlexTestSecond	NFS	Not Scanning	
<div>Off</div> <div>Map</div> <div>Map & Classify</div>	MoreDataNeed1000	NFS	Continuously Scanning	

終了：	手順：
ボリュームに対してマッピングのみのスキャンを有効にします	ボリューム領域で、 * マップ * をクリックします
ボリュームでフルスキャンを有効にします	ボリューム領域で、 * マップと分類 * をクリックします
ボリュームのスキャンを無効にします	ボリューム領域で、 * オフ * をクリックします
すべてのボリュームでマッピングのみのスキャンを有効にします	見出し領域で、 * マップ * をクリックします
すべてのボリュームでフルスキャンを有効にします	見出し領域で、 * マップと分類 * をクリックします
すべてのボリュームでスキャンを無効にします	見出し領域で、 * Off * をクリックします

i

作業環境に追加された新しいボリュームは、見出し領域で * Map * または * Map & Classify * の設定を行った場合にのみ自動的にスキャンされます。見出し領域で * Custom * または * Off * に設定すると、作業環境に追加する新しいボリュームごとに、マッピングまたはフルスキャンを有効にする必要があります。

データ保護ボリュームをスキャンしています

デフォルトでは、データ保護（DP）ボリュームは外部から公開されておらず、クラウドデータセンスでアクセスできないため、スキャンされません。これは、ONTAP ファイルシステムの FSX からの SnapMirror 処理のデスティネーションボリュームです。

最初は、ボリュームリストでこれらのボリュームを Type* DP * でスキャンしていないステータス * および必要なアクション _ * DP ボリュームへのアクセスを有効にします *。

'Working Environment Name' Configuration

22/28 Volumes selected for compliance scan

Enable Access to DP Volumes Edit CIFS Credentials

Off Map Map & Classify Custom Learn about the differences →

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	VolumeName1	DP	Not Scanning	Enable access to DP Volumes ⓘ
Off Map Map & Classify	VolumeName2	NFS	Continuously Scanning	
Off Map Map & Classify	VolumeName3	CIFS	Not Scanning	

これらのデータ保護ボリュームをスキャンする場合は、次の手順を実行します。

1. ページ上部の * DP ボリュームへのアクセスを有効にする * をクリックします。
2. 確認メッセージを確認し、もう一度「* DP ボリュームへのアクセスを有効にする *」をクリックします。
 - ONTAP ファイルシステムのソース FSX で NFS ボリュームとして最初に作成されたボリュームが有効になります。
 - ONTAP ファイルシステム用のソース FSX で CIFS ボリュームとして最初に作成されたボリュームでは、これらの DP ボリュームをスキャンするために CIFS クレデンシャルを入力する必要があります。Cloud Data Sense で CIFS ボリュームをスキャンするためにすでに Active Directory のクレデンシャルを入力している場合は、それらのクレデンシャルを使用できます。また、別の管理クレデンシャルを指定することもできます。

Provide Active Directory Credentials

☒ Use existing CIFS Scanning Credentials (user1@domain2) ☐ Use Custom Credentials

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

Enable Access to DP Volumes Cancel

Provide Active Directory Credentials

☐ Use existing CIFS Scanning Credentials (user1@domain2) ☒ Use Custom Credentials

Username ⓘ Password ⓘ

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

Enable Access to DP Volumes Cancel

3. スキャンする各 DP ボリュームをアクティブ化します **他のボリュームも有効にした場合と同じです。**

有効にすると、スキャン対象としてアクティブ化された各 DP ボリュームから NFS 共有が作成されます。共有エクスポートポリシーでは、データセンシブインスタンスからのアクセスのみが許可されます。

- ・注： DP ボリュームへのアクセスを最初に有効にしたときに CIFS データ保護ボリュームがない場合は、あとで追加しても、CIFS DP の有効化ボタン * が設定ページの上部に表示されます。このボタンをクリックして、CIFS DP ボリュームへのアクセスを有効にする CIFS クレデンシャルを追加します。



Active Directory クレデンシャルは、最初の CIFS DP ボリュームの Storage VM にのみ登録されているため、その SVM 上のすべての DP ボリュームがスキャンされます。他の SVM 上のボリュームには Active Directory クレデンシャルが登録されないため、これらの DP ボリュームはスキャンされません。

Amazon S3 向けのクラウドデータセンスの導入

Cloud Data Sense は、Amazon S3 バケットをスキャンして、S3 オブジェクトストレージに格納されている個人データや機密データを特定することができます。Cloud Data Sense は、NetApp 解決策用に作成されたバケットかどうかに関係なく、アカウント内の任意のバケットをスキャンできます。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

IAM ロールの準備やデータセンスから S3 への接続の設定など、クラウド環境がクラウドデータセンスの要件を満たしていることを確認します。 [すべてのリストを参照してください](#)。

"クラウドデータの導入センス" インスタンスが展開されていない場合。

Amazon S3 作業環境を選択し、* Enable * をクリックして、必要な権限を含む IAM ロールを選択します。

スキャンするバケットを選択すると、Cloud Data Sense によってスキャンが開始されます。

S3 の前提条件の確認

S3 バケットのスキャンに固有の要件を次に示します。

Cloud Data Sense インスタンス用の IAM ロールを設定する

Cloud Data Sense では、アカウント内の S3 バケットに接続してスキャンするための権限が必要です。以下の権限を含む IAM ロールを設定します。Amazon S3 作業環境でデータの意味を有効にすると、Cloud Manager から IAM ロールを選択するよう求められます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

Cloud Data Sense から Amazon S3 への接続を提供する

Cloud Data Sense は Amazon S3 への接続を必要としている。この接続を確立する最善の方法は、VPC エンドポイントを介して S3 サービスに接続することです。手順については、を参照してください ["AWS のドキュメント：「Creating a Gateway Endpoint」](#)。

VPC エンドポイントを作成するときは、Cloud Data Sense インスタンスに対応するリージョン、VPC、およびルーティングテーブルを選択してください。S3 エンドポイントへのトラフィックを有効にする発信 HTTPS ルールを追加するには、セキュリティグループも変更する必要があります。そうしないと、データセンスで S3 サービスに接続できません。

問題が発生した場合は、を参照してください ["AWS のサポートナレッジセンター：ゲートウェイ VPC エンドポイントを使用して S3 バケットに接続できないのはなぜですか。"](#)

別の方法として、NAT ゲートウェイを使用して接続を提供する方法があります。



インターネット経由で S3 にアクセスするためにプロキシを使用することはできません。

Cloud Data Sense インスタンスの導入

"Cloud Manager に Cloud Data Sense を導入" インスタンスが展開されていない場合。

AWS に導入されているコネクタを使用してインスタンスを導入する必要があります。これにより、Cloud Manager はこの AWS アカウント内の S3 バケットを自動的に検出し、Amazon S3 作業環境に表示します。

- ・注：* クラウドデータセンスをオンプレミスの場所に導入することは、現在 S3 バケットのスキャンではサポートされていません。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

S3 作業環境でのデータセンスのアクティブ化

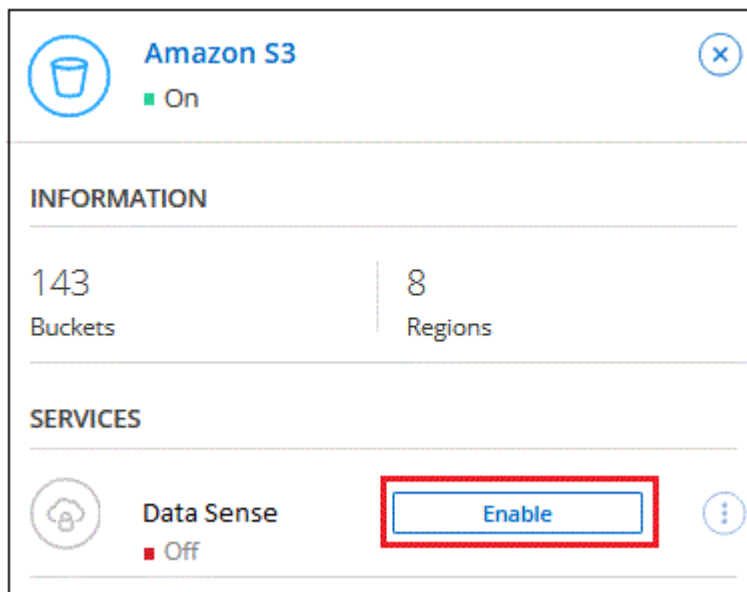
前提条件を確認したら、Amazon S3 で Cloud Data Sense を有効にします。

手順

1. Cloud Manager の上部にある * Canvas * をクリックします。
2. Amazon S3 作業環境を選択します。



3. 右側の [データセンス] ペインで、[Enable] をクリックします。



4. プロンプトが表示されたら、を持つ Cloud Data Sense インスタンスに IAM ロールを割り当てます [必要な権限](#)。

Assign an AWS IAM Role for Cloud Data Sense

To enable **Cloud Data Sense** on Amazon S3 buckets, select an existing IAM Role. Make sure that your AWS IAM Role has the permission defined in the [Policy Requirements](#).

Select IAM Role

occm

VPC Endpoint for Amazon S3 Required

A VPC endpoint to the Amazon S3 service is required so **Data Sense** can securely scan the data.

Alternatively, ensure that the **Data Sense** instance has direct access to the internet via a NAT Gateway or Internet Gateway.

Free for the 1st TB


Over 1 TB you pay only for what you use. [Learn more about pricing.](#)

Enable

Cancel

5. **[Enable]** をクリックします。



また、作業環境のコンプライアンススキャンを有効にすることもできます Configuration ページでをクリックします  ボタンを押して、[データセンスを活動化（Activate Data Sense）] を選択

Cloud Manager によって、インスタンスに IAM ロールが割り当てられます。

S3 バケットでの準拠スキャンの有効化と無効化

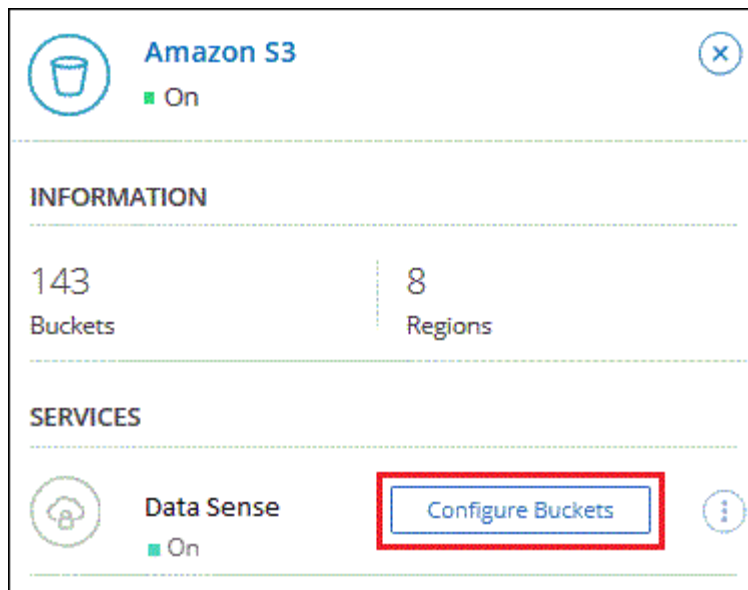
Cloud Manager が Amazon S3 で Cloud Data Sense を有効にしたら、次の手順でスキャンするバケットを設定します。

スキャンする S3 バケットを含む AWS アカウントで Cloud Manager を実行している場合は、そのバケットが検出され、Amazon S3 作業環境に表示されます。

クラウドデータセンスも可能です [別々の AWS アカウントにある S3 バケットをスキャンします](#)。

手順

1. Amazon S3 作業環境を選択します。
2. 右側のペインで、* バケットの設定 * をクリックします。



3. バケットでマッピング専用スキャン、またはマッピングスキャンと分類スキャンを有効にします。

Amazon S3 Configuration			
15/28 Buckets in Scan Scope.			
Scan	Bucket Name	Status	Required Action
Off Map Map & Classify	BucketName1	● Not Scanning	Add Credentials
Off Map Map & Classify	BucketName2	● Continuously Scanning	
Off Map Map & Classify	BucketName3	● Not Scanning	

終了：	手順：
バケットでマッピングのみのスキャンを有効にする	[* マップ *] をクリックします
バケットでフルスキャンを有効にします	[マップと分類 *] をクリックします
バケットに対するスキャンを無効にする	[* Off *] をクリックします

Cloud Data Sense は、有効にした S3 バケットのスキャンを開始します。エラーが発生した場合は、エラーを修正するために必要なアクションとともに、[ステータス] 列に表示されます。

追加の **AWS** アカウントからバケットをスキャンする

別の AWS アカウントを使用している S3 バケットをスキャンするには、そのアカウントから既存の Cloud Data Sense インスタンスにアクセスするロールを割り当てます。

手順

1. S3 バケットをスキャンするターゲット AWS アカウントに移動し、* 別の AWS アカウント * を選択して IAM ロールを作成します。

Create role

1

2

3

4

Select type of trusted entity


 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID*

**Options**

- ☐ Require external ID (Best practice when a third party will assume this role)
- ☐ Require MFA 

必ず次の手順を実行してください。

- Cloud Data Sense インスタンスが存在するアカウントの ID を入力します。
- 最大 CLI / API セッション期間 * を 1 時間から 12 時間に変更し、変更を保存してください。
- クラウドデータセンス IAM ポリシーを関連付けます。必要な権限があることを確認します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

2. データセンスインスタンスが存在するソース AWS アカウントに移動し、インスタンスに関連付けられている IAM ロールを選択します。
 - a. 最大 CLI / API セッション期間 * を 1 時間から 12 時間に変更し、変更を保存してください。
 - b. [* ポリシーの適用 *] をクリックし、[ポリシーの作成 *] をクリックします。
 - c. 「STS : AssumeRole」アクションを含むポリシーを作成し、ターゲットアカウントで作成したロールの ARN を指定します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-ID>:role/<ADDITIONAL_ROLE_NAME>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

Cloud Data Sense インスタンスプロファイルアカウントが追加の AWS アカウントにアクセスできるようになりました。

3. Amazon S3 Configuration * ページに移動し、新しい AWS アカウントが表示されます。Cloud Data Sense が新しいアカウントの作業環境を同期し、この情報を表示するまでに数分かかる場合があります。



4. [Activate Data Sense & Select Buckets] をクリックして、スキャンするバケットを選択します。

Cloud Data Sense は、有効にした新しい S3 バケットのスキャンを開始します。

データベーススキーマをスキャンしています

Cloud Data Sense でデータベーススキーマのスキャンを開始するには、いくつかの手順を実行します。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

データベースがサポートされていること、およびデータベースへの接続に必要な情報があることを確認します。

"クラウドデータの導入センス" インスタンスが展開されていない場合。

アクセスするデータベースサーバを追加します。

スキャンするスキーマを選択します。

前提条件の確認

Cloud Data Sense を有効にする前に、次の前提条件を確認し、サポートされている構成であることを確認します。

サポートされるデータベース

Cloud Data Sense では、次のデータベースからスキーマをスキャンできます。

- Amazon リレーショナルデータベースサービス（Amazon RDS）
- MongoDB
- MySQL
- Oracle の場合
- PostgreSQL
- SAP HANA のサポート
- SQL Server（MSSQL）



統計収集機能*は、データベースで有効にする必要があります*。

データベースの要件

Cloud Data Sense インスタンスに接続されているデータベースは、どこでホストしているかに関係なく、すべてスキャンできます。データベースに接続するには、次の情報が必要です。

- IP アドレスまたはホスト名
- ポート
- サービス名（Oracle データベースにアクセスする場合のみ）
- スキーマへの読み取りアクセスを許可するクレデンシャル

ユーザー名とパスワードを選択する場合は、スキャンするすべてのスキーマとテーブルに対する完全な読み取り権限を持つユーザーを選択することが重要です。必要なすべての権限を持つクラウドデータセンスシステム専用のユーザを作成することを推奨します。

- 注：MongoDB では、読み取り専用の管理者ロールが必要です。

Cloud Data Sense インスタンスの導入

導入済みのインスタンスがない場合は Cloud Data Sense を導入

インターネット経由でアクセス可能なデータベーススキーマをスキャンする場合は、を実行します **"クラウドにクラウドデータセンスを導入"** または **"インターネットにアクセス可能なオンプレミスの場所にデータセンスを導入"**。

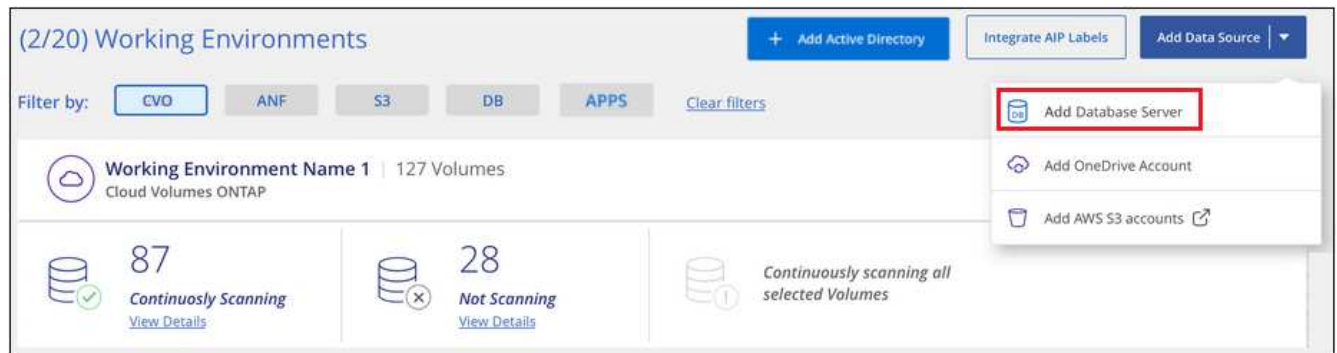
インターネットにアクセスできないダークサイトにインストールされているデータベーススキーマをスキャンする場合は、が必要です **"クラウドデータセンスは、インターネットにアクセスできないオンプレミス環境に導入できます"**。そのため、Cloud Manager Connector をオンプレミスと同じ場所に導入する必要があります。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

データベースサーバを追加しています

スキーマが存在するデータベース・サーバを追加します。

1. [作業環境の構成] ページで、[* データソースの追加 > データベースサーバーの追加 *] をクリックします。



2. データベースサーバを識別するために必要な情報を入力します。
 - a. データベースタイプを選択します。
 - b. データベースに接続するポートおよびホスト名または IP アドレスを入力します。
 - c. Oracle データベースの場合は、サービス名を入力します。
 - d. Cloud Data Sense がサーバにアクセスできるように、クレデンシャルを入力します。
 - e. [Add DB Server*] をクリックします。

Add DB Server

To activate Compliance on Databases, first add a Database Server. After this step, you'll be able to select which Database Schemas you would like to activate Compliance for.

Database

Database Type

Host Name or IP Address

Port

Service Name

Credentials

Username

Password

ページのスクリーンシ

ョット。"]

データベースが作業環境のリストに追加されます。

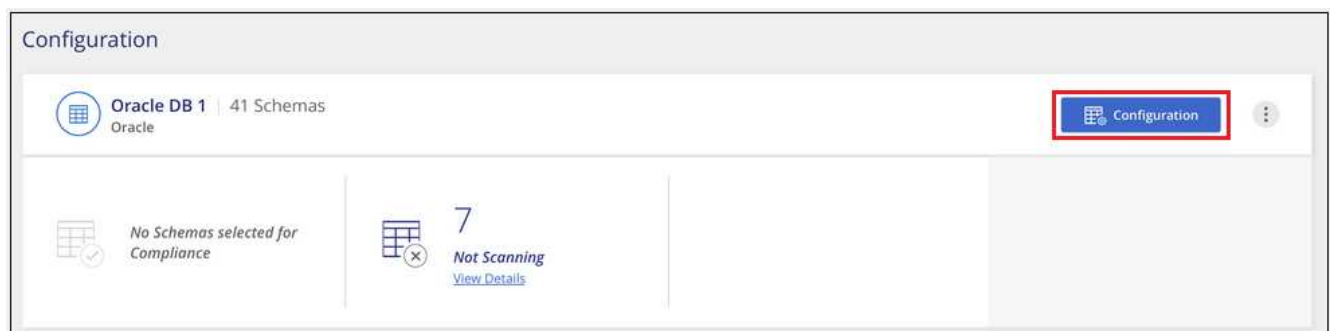
データベーススキーマでの準拠スキャンの有効化と無効化

スキーマのフルスキャンは、いつでも停止または開始できます。



データベーススキーマに対してマッピングのみのスキャンを選択するオプションはありません。

1. `_Configuration_page` で、設定するデータベースの **Configuration** ボタンをクリックします。



2. スライダを右に移動して、スキャンするスキーマを選択します。

'Working Environment Name' Configuration			
28/28 Schemas selected for compliance scan		Edit Credentials	
Scan	Schema Name	Status	Required Action
<input type="checkbox"/>	DB1 - SchemaName1	Not Scanning	Add Credentials ⓘ
<input type="checkbox"/>	DB1 - SchemaName2	Continuously Scanning	
<input type="checkbox"/>	DB1 - SchemaName3	Continuously Scanning	
<input type="checkbox"/>	DB1 - SchemaName4	Continuously Scanning	

ページのスクリーンショット。"]

Cloud Data Sense は、有効にしたデータベーススキーマのスキャンを開始します。エラーが発生した場合は、エラーを修正するために必要なアクションとともに、[ステータス]列に表示されます。

OneDrive アカウントをスキャンしています

いくつかの手順を実行して、クラウドデータセンスを使用した OneDrive フォルダのファイルのスキャンを開始します。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

OneDrive アカウントにログインするための管理者資格情報があることを確認してください。

"クラウドデータの導入センス" インスタンスが展開されていない場合。

Admin ユーザクレデンシャルを使用して、アクセスする OneDrive アカウントにログインし、新しい作業環境として追加します。

スキャンするユーザのリストを OneDrive アカウントから追加し、スキャンのタイプを選択します。一度に最大 100 人のユーザを追加できます。

OneDrive の要件を確認する

Cloud Data Sense を有効にする前に、次の前提条件を確認し、サポートされている構成であることを確認します。

- ユーザのファイルに読み取りアクセスを提供する OneDrive for Business アカウントの管理者ログインクレデンシャルが必要です。
- OneDrive フォルダをスキャンするすべてのユーザーに対して、電子メールアドレスの行区切りリストが必要です。

Cloud Data Sense インスタンスの導入

導入済みのインスタンスがない場合は Cloud Data Sense を導入

データセンスは、のいずれかです "クラウドに導入" または "インターネットにアクセスできるオンプレミスの場所"。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

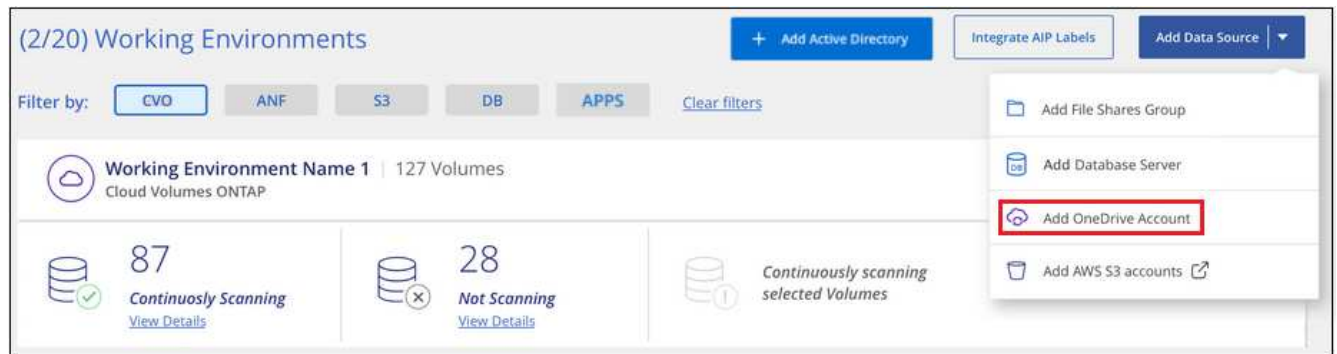
データセンスは、の場合もあります "インターネットにアクセスできないオンプレミスの場所に導入されている"。ただし、ローカルの OneDrive ファイルをスキャンするには、いくつかの一部のエンドポイントへのインターネットアクセスを提供する必要があります。 "必要なエンドポイントのリストを参照してください"。

OneDrive アカウントを追加します

ユーザファイルが存在する OneDrive アカウントを追加します。

手順

1. [作業環境の構成] ページで、[* データソースの追加 >]、[OneDrive アカウントの追加 *] の順にクリックします。



ボタンをクリックできる [スキャン構成] ページのスクリーンショット。"]

2. [OneDrive アカウントの追加] ダイアログで、[* OneDrive にサインイン] をクリックします。
3. 表示される Microsoft ページで、OneDrive アカウントを選択し、必要な管理者ユーザーとパスワードを入力してから、[Accept] をクリックして、Cloud Data Sense がこのアカウントからデータを読み取ることを許可します。

OneDrive アカウントが作業環境の一覧に追加されます。

OneDrive ユーザーをコンプライアンススキャンに追加する

個々の OneDrive ユーザーまたはすべての OneDrive ユーザーを追加して、ファイルを Cloud Data Sense でスキャンすることができます。

手順

1. [Configuration] ページで、OneDrive アカウントの [* 構成 *] ボタンをクリックします。



2. この OneDrive アカウントに初めてユーザーを追加する場合は、[* 最初の OneDrive ユーザーを追加する *] をクリックします。



OneDrive アカウントからユーザーを追加する場合は、[* OneDrive ユーザーの追加 *] をクリックします。



ボタンを示すスクリーンショット。"]

3. ファイルをスキャンするユーザーの電子メールアドレスを 1 行に 1 つ追加し（セッションあたり最大 100 件）、[ユーザーの追加] をクリックします。



ページのスクリーンショット。"]

確認ダイアログに、追加されたユーザの数が表示されます。

ダイアログに追加できなかったユーザが表示される場合は、この情報を記録して問題を解決します。修正した E メールアドレスを使用してユーザを再追加できる場合もあります。

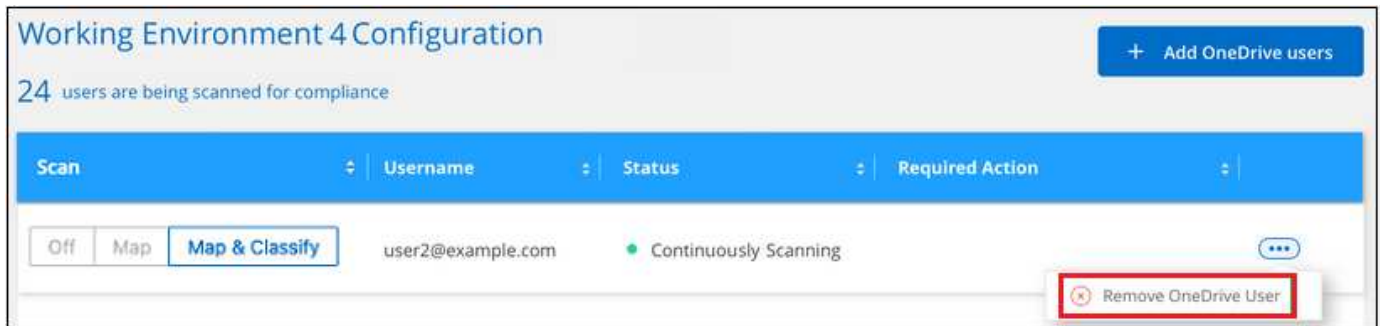
4. ユーザファイルに対して、マッピング専用スキャン、またはマッピングおよび分類スキャンをイネーブルにします。

終了：	手順：
ユーザファイルに対してマッピングのみのスキャンを有効にします	[* マップ *] をクリックします
ユーザファイルのフルスキャンを有効にします	[マップと分類 *] をクリックします
ユーザファイルのスキャンを無効にします	[* Off *] をクリックします

Cloud Data Sense によって、追加したユーザのファイルのスキャンが開始され、その結果がダッシュボードやその他の場所に表示されます。

OneDrive ユーザーをコンプライアンススキャンから削除します

ユーザが会社から退出した場合や、E メールアドレスが変更された場合、個々の OneDrive ユーザがいつでもファイルをスキャンできないようにすることができます。[構成] ページで [OneDrive ユーザーの削除] をクリックします。



できることに注意してください **"データセンズからOneDriveアカウント全体を削除します"** OneDriveアカウントからユーザーデータをスキャンする必要がなくなった場合。

SharePoint アカウントをスキャンしています

Cloud Data Sense を使用して、SharePoint アカウント内のファイルのスキャンを開始するには、いくつかの手順を実行します。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

SharePoint アカウントにログインするための管理者資格情報があり、スキャンする SharePoint サイトの URL があることを確認します。

"クラウドデータの導入センズ" インスタンスが展開されていない場合。

管理者ユーザーの資格情報を使用して、アクセスする SharePoint アカウントにログインし、新しいデータソース / 作業環境として追加します。

SharePoint アカウントでスキャンする SharePoint サイト URL のリストを追加し、スキャンの種類を選択します。一度に最大 100 個の URL を追加できます。

SharePoint の要件を確認する

以下の前提条件を確認して、SharePoint アカウントで Cloud Data Sense を有効にする準備ができていることを確認します。

- すべての SharePoint サイトへの読み取りアクセスを提供する SharePoint アカウントの管理者ログインクレデンシャルが必要です。
- スキャンするすべてのデータについて、SharePoint サイトの URL の行区切りリストが必要です。

Cloud Data Sense インスタンスの導入

導入済みのインスタンスがない場合は Cloud Data Sense を導入

データセンズは、のいずれかです **"クラウドに導入"** または **"インターネットにアクセスできるオンプレミスの場所"**。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動

化されます。

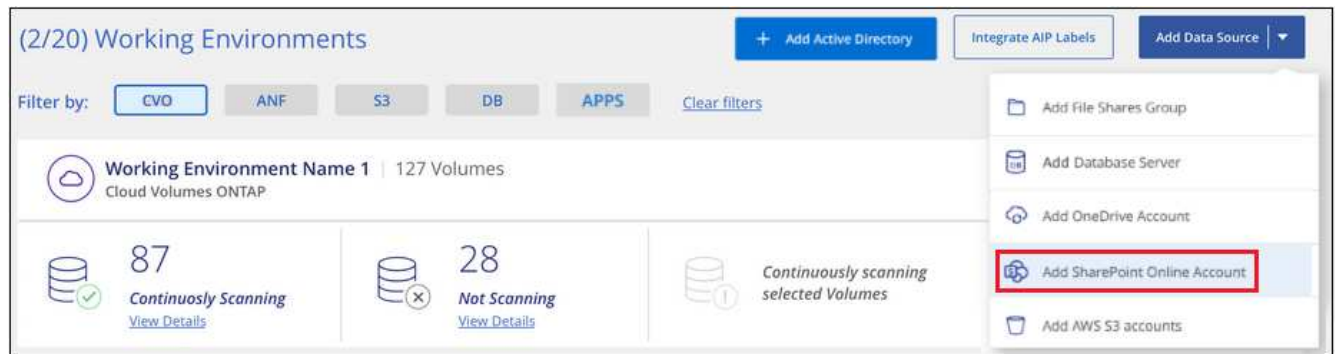
データセンシブは、の場合もあります ["インターネットにアクセスできないオンプレミスの場所に導入されている"](#)。ただし、ローカルの SharePoint ファイルをスキャンするには、いくつかの選択したエンドポイントへのインターネットアクセスを提供する必要があります。 ["必要なエンドポイントのリストを参照してください"](#)。

SharePoint アカウントを追加しています

ユーザーファイルが存在する SharePoint アカウントを追加します。

手順

1. [作業環境の構成] ページで、[* データソースの追加 > SharePoint Online アカウントの追加 *] をクリックします。



ページのスクリーンショット。"]

2. [SharePoint Online アカウントの追加] ダイアログで、[* SharePoint にサインインする *] をクリックします。
3. 表示される Microsoft ページで、SharePoint アカウントを選択し、必要な管理者ユーザーとパスワードを入力してから、*Accept* をクリックして Cloud Data Sense がこのアカウントからデータを読み取することを許可します。

SharePoint アカウントが作業環境のリストに追加されます。

SharePoint サイトをコンプライアンススキャンに追加する

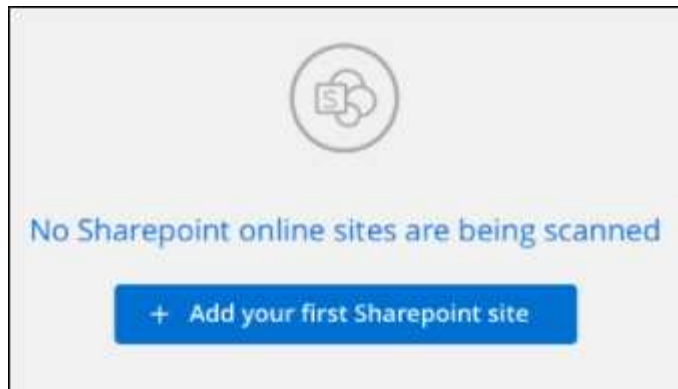
個々の SharePoint サイト、またはアカウント内のすべての SharePoint サイトを追加して、関連するファイルが Cloud Data Sense によってスキャンされるようにすることができます。

手順

1. [Configuration] ページで、SharePoint アカウントの [Configuration] ボタンをクリックします。



2. この SharePoint アカウントのサイトを初めて追加する場合は、[* 最初の SharePoint サイトを追加する *] をクリックします。

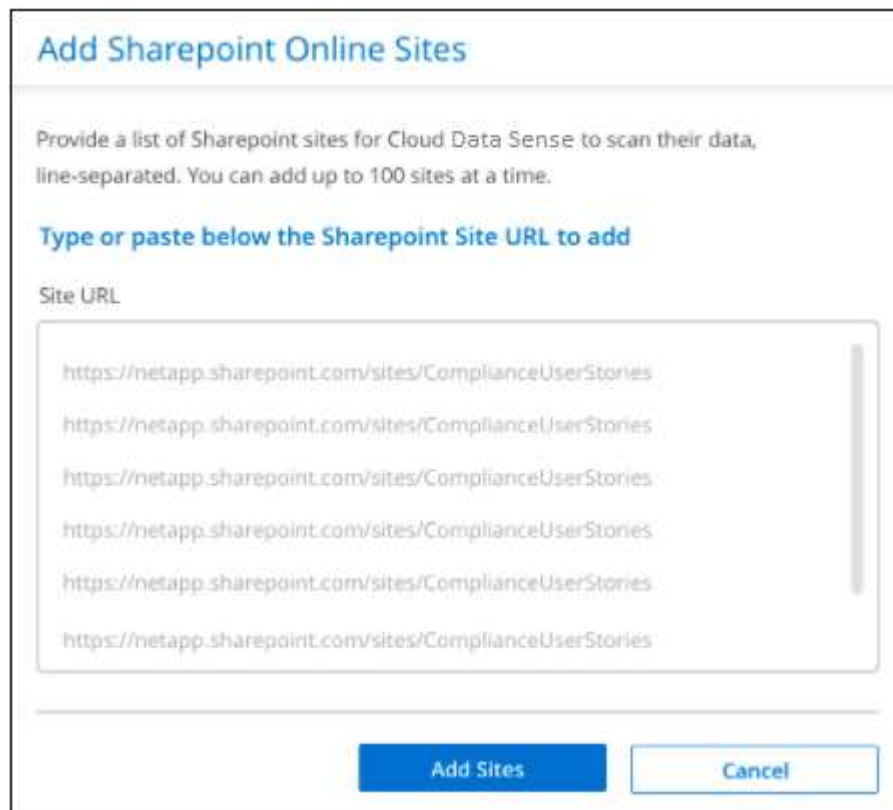


ボタンを示すスクリーンショット。"]

SharePoint アカウントからユーザーを追加する場合は、[* SharePoint サイトの追加 *]をクリックします。



3. スキャンするファイルがあるサイトの URL を 1 行に 1 つ追加し（セッションあたり最大 100 URL ）、[サイトの追加] をクリックします。



確認ダイアログに追加されたサイトの数が表示されます。

ダイアログに追加できなかったサイトが表示された場合は、問題を解決できるようにこの情報を記録します。場合によっては、URL を修正してサイトを再追加することができます。

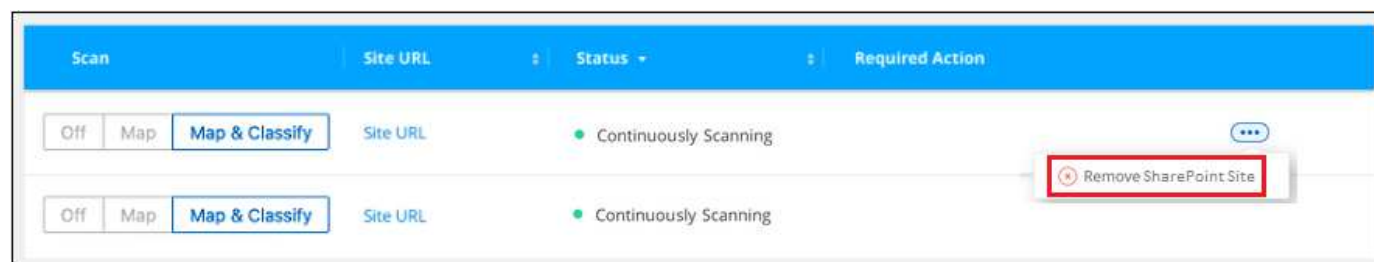
4. SharePoint サイト内のファイルに対して、マッピングのみのスキャン、またはマッピングと分類スキャンを有効にします。

終了：	手順：
ファイルのマッピングのみのスキャンを有効にします	[* マップ *] をクリックします
ファイルのフルスキャンを有効にします	[マップと分類 *] をクリックします
ファイルのスキャンを無効にします	[* Off *] をクリックします

Cloud Data Sense によって、追加した SharePoint サイトのファイルのスキャンが開始され、結果がダッシュボードやその他の場所に表示されます。

SharePoint サイトをコンプライアンススキャンから削除します

今後 SharePoint サイトを削除する場合や、SharePoint サイト内のファイルをスキャンしない場合は、個々の SharePoint サイトのファイルがいつでもスキャンされないようにすることができます。[構成] ページで [SharePoint サイトの削除] をクリックします。



できることに注意してください "[SharePoint アカウント全体をデータセンスから削除します](#)" SharePoint アカウントからユーザーデータをスキャンする必要がなくなった場合。

Google ドライブアカウントをスキャンしています

Cloud Data Sense を使用して、Google Drive アカウントのユーザーファイルのスキャンを開始するには、いくつかの手順を実行します。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

Google ドライブアカウントにログインするための管理者資格情報があることを確認します。

"[クラウドデータの導入センス](#)" インスタンスが展開されていない場合。

Admin ユーザーのクレデンシャルを使用して、アクセスする Google Drive アカウントにログインし、新しいデータソースとして追加します。

ユーザファイルで実行するスキャンのタイプ（マッピングまたはマッピングおよび分類）を選択します。

Googleドライブの要件を確認する

以下の前提条件を確認して、Google DriveアカウントでCloud Data Senseを有効にする準備ができていることを確認します。

- ・ ユーザのファイルへの読み取りアクセスを提供するGoogle Driveアカウントの管理者ログインクレデンシャルが必要です

現在の制限

次のデータセンス機能は、Googleドライブファイルでは現在サポートされていません。

- ・ [データ調査]ページでファイルを表示している場合、ボタンバーのアクションはアクティブになりません。ファイルのコピー、移動、削除などはできません。
- ・ Googleドライブ内のファイル内で権限を識別できないため、[調査] ページに権限情報は表示されません。

Cloud Data Sense の導入

導入済みのインスタンスがない場合は Cloud Data Sense を導入

データセンスは、のいずれかです "[クラウドに導入](#)" または "[インターネットにアクセスできるオンプレミスの場所](#)"。

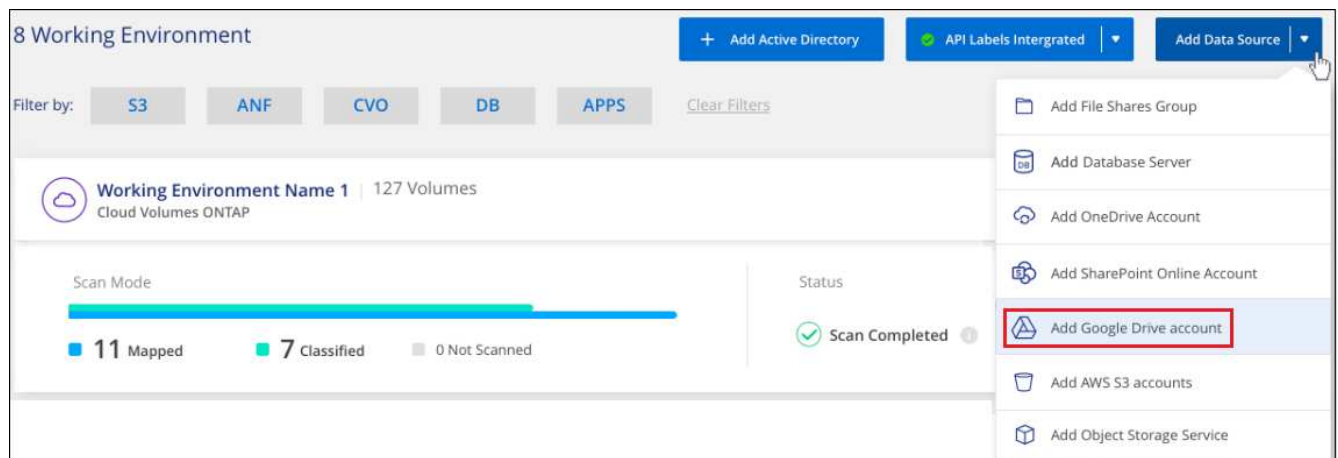
Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

Google Driveアカウントを追加しています

ユーザーファイルが存在するGoogleドライブアカウントを追加します。複数のユーザーからファイルをスキャンする場合は、ユーザーごとにこの手順を実行する必要があります。

手順

1. [作業環境の構成]ページで、[データソースの追加>* Googleドライブアカウントの追加*]をクリックします。



2. [Googleドライブアカウントの追加]ダイアログで、[Googleドライブへのサインイン*]をクリックします。
3. 表示されたGoogleページで、Googleドライブアカウントを選択し、必要な管理者ユーザーとパスワードを入力してから、* Accept *をクリックしてCloud Data Senseがこのアカウントからデータを読み取することを許可します。

Googleドライブアカウントが作業環境のリストに追加されます。

ユーザデータのスキャンタイプを選択しています

ユーザデータに対してCloud Data Senseが実行するスキャンのタイプを選択します。

手順

1. _Configuration_pageで、Google Driveアカウントの* Configuration *ボタンをクリックします。



2. Google Driveアカウントのファイルに対して、マッピング専用スキャンまたはマッピングおよび分類スキャンを有効にします。



終了：	手順：
ファイルのマッピングのみのスキャンを有効にします	[* マップ *] をクリックします
ファイルのフルスキャンを有効にします	[マップと分類 *] をクリックします
ファイルのスキャンを無効にします	[* Off *] をクリックします

Cloud Data Senseは、追加したGoogle Driveアカウントのファイルのスキャンを開始し、その結果がダッシュボードやその他の場所に表示されます。

Googleドライブアカウントをコンプライアンススキャンから削除しています

1人のユーザーのGoogleドライブファイルのみが1つのGoogleドライブアカウントの一部であるため、ユーザーのGoogleドライブアカウントからのファイルのスキャンを停止する場合は、次の手順を実行します ["データセンサからGoogleドライブアカウントを削除します"](#)。

ファイル共有をスキャンしています

NetApp 以外の NFS または CIFS ファイル共有を Cloud Data Sense で直接スキャンす

るには、いくつかの手順を実行します。これらのファイル共有は、オンプレミスでもクラウドでもかまいません。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

CIFS（SMB）共有の場合は、共有にアクセスするためのクレデンシャルがあることを確認しておきます。

"クラウドデータの導入センス" インスタンスが展開されていない場合。

このグループは、スキャンするファイル共有のコンテナであり、これらのファイル共有の作業環境名として使用されます。

スキャンするファイル共有のリストを追加し、スキャンのタイプを選択します。一度に最大 100 個のファイル共有を追加できます。

ファイル共有の要件の確認

Cloud Data Sense を有効にする前に、次の前提条件を確認し、サポートされている構成であることを確認します。

- 共有は、クラウド内やオンプレミスなど、どこでもホストできます。ネットアップ以外のストレージシステム上のファイル共有です。
- データセンスインスタンスと共有の間にネットワーク接続が必要です。
- これらのポートが Data Sense インスタンスに対して開いていることを確認します。
 - NFS –ポート 111 および 2049。
 - CIFS の場合 - ポート 139 および 445
- 追加する共有のリストは、「<host_name> : /<share_path>`」の形式で指定する必要があります。共有は個別に入力することも、スキャンするファイル共有の行区切りリストを指定することもできます。
- CIFS（SMB）共有の場合は、共有への読み取りアクセスを提供する Active Directory クレデンシャルがあることを確認します。管理者クレデンシャルが推奨されるのは、Cloud Data Sense で管理者権限が必要なデータをスキャンする必要がある場合です。

Cloud Data Sense インスタンスの導入

導入済みのインスタンスがない場合は Cloud Data Sense を導入

インターネット経由でアクセス可能な、ネットアップ以外の NFS または CIFS ファイル共有をスキャンする場合は、を実行します **"クラウドにクラウドデータセンスを導入"** または **"インターネットにアクセス可能なオンプレミスの場所にデータセンスを導入"**。

インターネットにアクセスできないダークサイトにインストールされているネットアップ以外の NFS または CIFS ファイル共有をスキャンする場合は、が必要です **"クラウドデータセンスは、インターネットにアクセスできないオンプレミス環境に導入できます"**。そのため、Cloud Manager Connector をオンプレミスと同じ場所に導入する必要があります。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動

化されます。

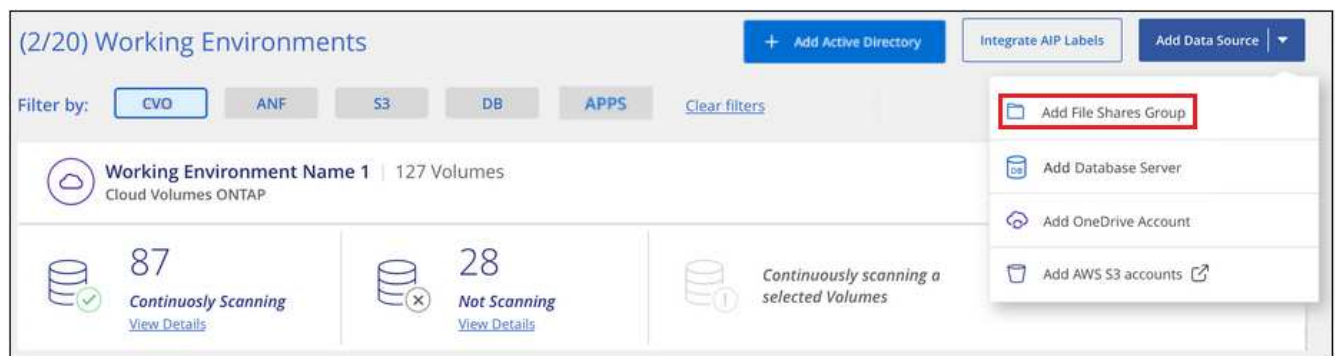
ファイル共有のグループを作成します

ファイル共有を追加する前に、「group」というファイル共有を追加する必要があります。グループはスキャンするファイル共有のコンテナであり、グループ名はそれらのファイル共有の作業環境名として使用されます。

同じグループ内に NFS 共有と CIFS 共有を混在させることはできますが、1つのグループ内のすべての CIFS ファイル共有で同じ Active Directory クレデンシャルを使用する必要があります。異なるクレデンシャルを使用する CIFS 共有を追加する場合は、一意のクレデンシャルセットごとに個別のグループを作成する必要があります。

手順

1. [作業環境の構成] ページで、[* データソースの追加 > ファイル共有グループの追加 *] をクリックします。



2. [ファイル共有グループの追加] ダイアログで、共有グループの名前を入力し、[続行] をクリックします。

新しいファイル共有グループが作業環境のリストに追加されます。

グループへのファイル共有の追加

ファイル共有グループにファイル共有を追加すると、これらの共有内のファイルが Cloud Data Sense によってスキャンされます。共有は、「<host_name> : /<share_path>」の形式で追加します。

個々のファイル共有を追加することも、スキャンするファイル共有を 1 行で区切って指定することもできます。一度に最大 100 個の共有を追加できます。

NFS 共有と CIFS 共有を 1 つのグループに追加する場合は、NFS 共有を追加してから CIFS 共有を再度追加するまで、このプロセスを 2 回実行する必要があります。

手順

1. 作業環境ページで、ファイル共有グループの * 構成 * ボタンをクリックします。



2. このファイル共有グループのファイル共有を初めて追加する場合は、* 最初の共有を追加 * をクリックします。



ボタンを

示すスクリーンショット。"]

既存のグループにファイル共有を追加する場合は、* 共有の追加 * をクリックします。



ボタンを示すスクリーンショット。"]

3. 追加するファイル共有のプロトコルを選択し、スキャンするファイル共有を 1 行に 1 つ追加して、「* Continue *」をクリックします。

CIFS（SMB）共有を追加する場合は、共有への読み取りアクセスを提供する Active Directory クレデンシャルを入力する必要があります。admin クレデンシャルが優先されます。

追加された共有の数が確認ダイアログに表示されます。

ダイアログに追加できなかった共有が表示された場合は、問題を解決できるようにこの情報を記録しておきます。修正したホスト名または共有名を使用して共有を再追加できる場合があります。

4. 各ファイル共有で、マッピング専用スキャン、またはマッピングスキャンと分類スキャンを有効にします。

終了：	手順：
ファイル共有でマッピングのみのスキャンを有効にします	[* マップ *] をクリックします
ファイル共有でフルスキャンを有効にします	[マップと分類 *] をクリックします
ファイル共有でのスキャンを無効にします	[* Off *] をクリックします

Cloud Data Sense によって、追加したファイル共有内のファイルのスキャンが開始され、その結果がダッシュボードやその他の場所に表示されます。

準拠スキャンからのファイル共有の削除

特定のファイル共有をスキャンする必要がなくなった場合は、個々のファイル共有を削除して、ファイルがいつでもスキャンされるようにすることができます。[構成] ページで [共有の削除] をクリックします。



S3 プロトコルを使用するオブジェクトストレージをスキャンしています

Cloud Data Sense で、オブジェクトストレージ内のデータのスキャンを開始するには、いくつかの手順を実行します。データセンスは、Simple Storage Service（S3）プロトコルを使用する任意の Object Storage サービスからデータをスキャンできます。具体的には、NetApp StorageGRID、IBM Cloud Object Store、Azure Blob（MinIO を使用）、Linode、B2 Cloud Storage、Amazon S3 などです。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

オブジェクトストレージサービスに接続するには、エンドポイント URL が必要です。

Cloud Data Sense でバケットにアクセスできるように、オブジェクトストレージプロバイダからアクセスキーとシークレットキーを入手する必要があります。

"クラウドデータの導入センス" インスタンスが展開されていない場合。

オブジェクトストレージサービスをクラウドデータセンスに追加します。

スキャンするバケットを選択すると、Cloud Data Sense によってスキャンが開始されます。

オブジェクトストレージ要件の確認

Cloud Data Sense を有効にする前に、次の前提条件を確認し、サポートされている構成であることを確認します。

- オブジェクトストレージサービスに接続するには、エンドポイント URL が必要です。
- データセンスでバケットにアクセスできるようにするには、オブジェクトストレージプロバイダからアクセスキーとシークレットキーを取得する必要があります。
- Azure Blob のサポートにはを使用する必要があります "MinIO サービス"。

Cloud Data Sense インスタンスの導入

導入済みのインスタンスがない場合は Cloud Data Sense を導入

インターネット経由でアクセス可能な S3 オブジェクトストレージからデータをスキャンする場合は、を実行

します "クラウドにクラウドデータセンスを導入" または "インターネットにアクセス可能なオンプレミスの場所にデータセンスを導入"。

インターネットにアクセスできないダークサイトにインストールされている S3 オブジェクトストレージからデータをスキャンする場合は、が必要です "クラウドデータセンスは、インターネットにアクセスできないオンプレミス環境に導入できます"。そのため、Cloud Manager Connector をオンプレミスと同じ場所に導入する必要があります。

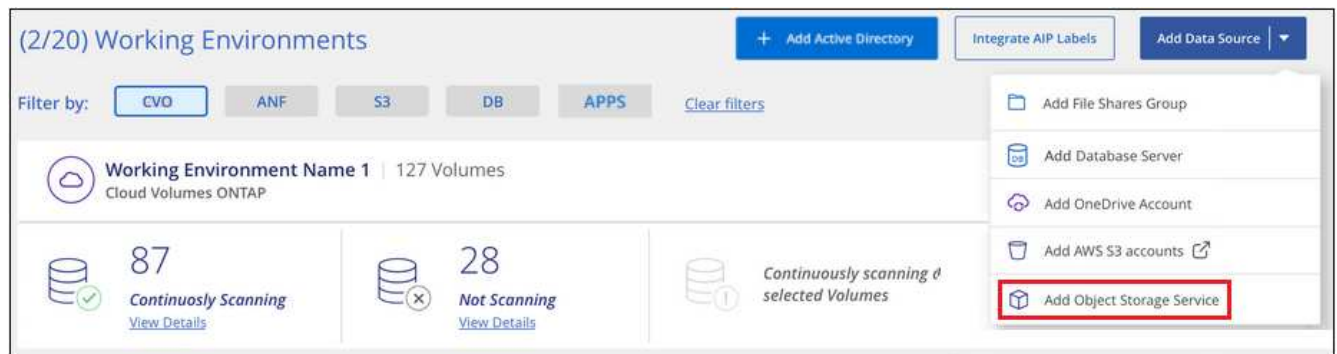
Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

Cloud Data Sense へのオブジェクトストレージサービスの追加

オブジェクトストレージサービスを追加します。

手順

1. [作業環境の構成] ページで、[* データソースの追加 > オブジェクトストレージサービスの追加 *] をクリックします。



2. Add Object Storage Service ダイアログで、オブジェクトストレージサービスの詳細を入力し、* Continue * をクリックします。
 - a. 作業環境に使用する名前を入力します。この名前には、接続先のオブジェクトストレージサービスの名前を指定する必要があります。
 - b. エンドポイントの URL を入力してオブジェクトストレージサービスにアクセスします。
 - c. Cloud Data Sense がオブジェクトストレージ内のバケットにアクセスできるように、アクセスキーとシークレットキーを入力します。

Add Object Storage Service

Cloud Data Sense can scan data from any Object Storage service which uses the S3 protocol. This includes NetApp StorageGRID, IBM Object Store, and more.

To continue, enter the following information. In the next steps you'll need to select the buckets you want to scan.

Name the Working Environment	Endpoint URL
<input type="text" value="object_myIBM"/>	<input type="text" value="http://my.endpoint.com"/>
Access Key	Secret Key
<input type="text" value="AJUKD0574NDJG86795"/>	<input type="text" value="....."/>

新しいオブジェクトストレージサービスが作業環境のリストに追加されます。

オブジェクトストレージバケットでの準拠スキャンの有効化と無効化

オブジェクトストレージサービスで Cloud Data Sense を有効にしたら、次の手順でスキャンするバケットを設定します。Data Sense は、これらのバケットを検出し、作成した作業環境に表示します。

手順

1. 設定ページで、Object Storage Service 作業環境の * 設定 * をクリックします。

(1/20) Working Environments

Filter by:

CVO
ANF
S3
DB
APPS
OB.STG

Rstor Integrated | 41 Buckets
Object Storage Service

23
Continuously Scanning
[View Details](#)

All Buckets selected for Compliance

Continuously scanning all selected Buckets

2. バケットでマッピング専用スキャン、またはマッピングスキャンと分類スキャンを有効にします。

Rstor Integrated Configuration			
3/55 Buckets selected for Compliance scan			
Scan	Storage Repository (Bucket) ↓↑	Status ↓↑	Required Action ↓↑
Off Map Map & Classify	logs-759995470648-us-east-1	● Not Scanning	
Off Map Map & Classify	logs-759995470648-us-west-2	● Not Scanning	
Off Map Map & Classify	carstock	● Continuously Scanning	

終了：	手順：
バケットでマッピングのみのスキャンを有効にする	[* マップ *] をクリックします
バケットでフルスキャンを有効にします	[マップと分類 *] をクリックします
バケットに対するスキャンを無効にする	[* Off *] をクリックします

Cloud Data Sense は、有効にしたバケットのスキャンを開始します。エラーが発生した場合は、エラーを修正するために必要なアクションとともに、[ステータス] 列に表示されます。

Active Directory と Cloud Data Sense を統合

グローバル Active Directory をクラウドデータセンスと統合すると、ファイル所有者や、ファイルにアクセスできるユーザーやグループについてデータセンスがレポートする結果を高めることができます。

一部のデータソース（以下に記載）を設定する場合、CIFS ボリュームをスキャンするデータセンスを設定するためには、Active Directory のクレデンシャルを入力する必要があります。この統合により、データセンスとファイル所有者、およびそれらのデータソースに存在するデータの権限の詳細が提供されます。これらのデータソースに対して入力した Active Directory は、ここで入力したグローバル Active Directory クレデンシャルと異なる場合があります。データセンスは、統合されたすべての Active Directory でユーザと権限の詳細を確認します。

この統合により、データセンスの良い場所で追加情報 を利用できるようになります。

- 「ファイル所有者」を使用できます。"フィルタ" [調査] ペインで、ファイルのメタデータの結果を確認できます。SID（セキュリティ ID）を含むファイル所有者ではなく、実際のユーザ名が入力されます。
- を参照してください "フルファイル権限" 各ファイルについて、[すべてのアクセス許可の表示] ボタンをクリックします。
- を参照してください "ガバナンスダッシュボード" を選択すると、[アクセス許可] パネルに、データに関するより詳細な情報が表示されます。



ローカルユーザの SID および不明なドメインの SID は、実際のユーザ名に変換されません。

サポートされているデータソース

Active Directory と Cloud Data Sense との統合により、次のデータソース内からデータを識別できます。

- オンプレミスの ONTAP システム
- Cloud Volumes ONTAP
- Azure NetApp Files の特長
- FSX for ONTAP の略
- 他社の CIFS ファイル共有（NFS ファイル共有ではない）

データベーススキーマ、OneDriveアカウント、SharePointアカウント、Googleドライブアカウント、Amazon S3アカウント、または、Simple Storage Service（S3）プロトコルを使用するObject Storageの略。

Active Directory サーバに接続しています

データセンスを導入し、データソースでスキャンを有効化したら、Active Directory とデータセンスを統合できます。Active Directory には、DNS サーバの IP アドレスまたは LDAP サーバの IP アドレスを使用してアクセスできます。

Active Directory のクレデンシャルは読み取り専用ですが、管理者のクレデンシャルを指定することで、データセンスは昇格された権限を必要とするすべてのデータを読み取ることができます。クレデンシャルは Cloud Data Sense インスタンスに保存されます。

要件

- 社内のユーザに対して Active Directory がすでに設定されている必要があります。
- Active Directory の次の情報が必要です。
 - DNS サーバの IP アドレス、または複数の IP アドレス

または

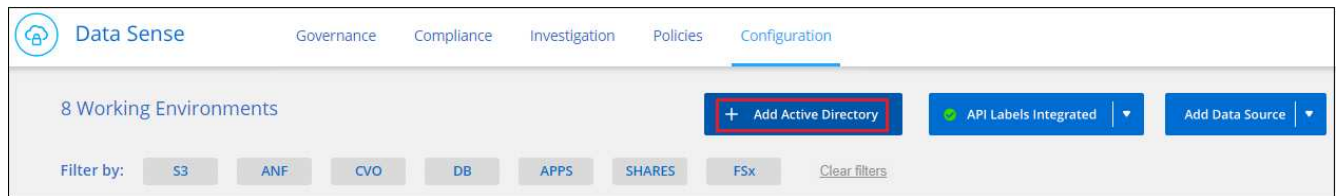
LDAP サーバの IP アドレス、または複数の IP アドレス

- サーバーにアクセスするためのユーザー名とパスワード
 - ドメイン名（Active Directory 名）
 - セキュアな LDAP（LDAPS）を使用しているかどうか
 - LDAP サーバポート（通常は LDAP では 389、セキュア LDAP では 636）
- Data Sense インスタンスによるアウトバウンド通信用に、次のポートが開いている必要があります。

プロトコル	ポート	宛先	目的
TCP および UDP	389	Active Directory	LDAP
TCP	636	Active Directory	LDAP over SSL
TCP	3268	Active Directory	グローバルカタログ
TCP	3269	Active Directory	SSL 経由のグローバルカタログ

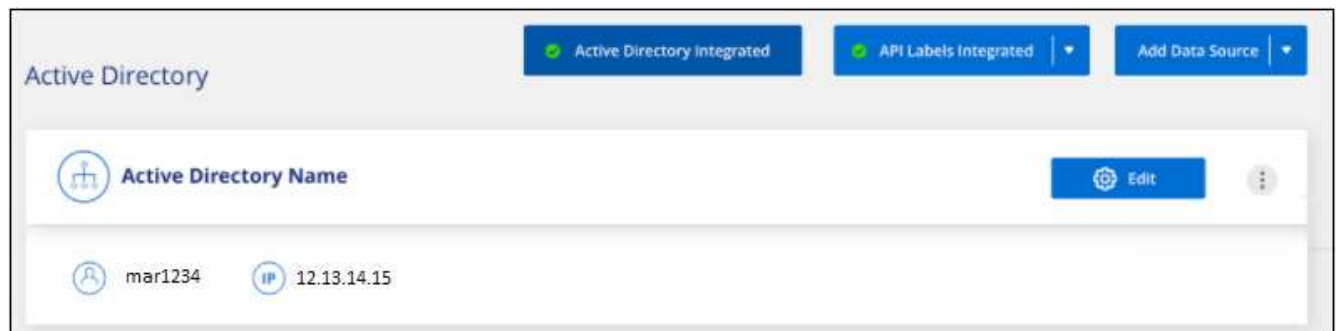
手順

1. Cloud Data Sense Configuration（クラウドデータセンス設定）ページで、* Add Active Directory *（Active Directory の追加）をクリックします。



2. Active Directory への接続ダイアログで、Active Directory の詳細を入力し、* 接続 * をクリックします。
必要に応じて、* IP の追加 * をクリックすると、複数の IP アドレスを追加できます。

データセンスは Active Directory に統合され、新しいセクションが [構成] ページに追加されます。



Active Directory 統合の管理

Active Directory 統合の値を変更する必要がある場合は、* Edit * ボタンをクリックして変更を行います。

不要になった統合は、をクリックして削除することもできます [設定] ボタン] ボタンをクリックして、 * Active Directory を削除 * をクリックします。

クラウドデータセンスのライセンスをセットアップする

Cloud Data Sense によってスキャンされる、Cloud Manager のワークスペース内の最初の 1TB のデータは無料です。そのあとも引き続きデータをスキャンするには、ネットアップの BYOL ライセンス、またはクラウドプロバイダのマーケットプレイスからの Cloud Manager サブスクリプションが必要です。

さらに読む前に、いくつかのメモを記入してください。

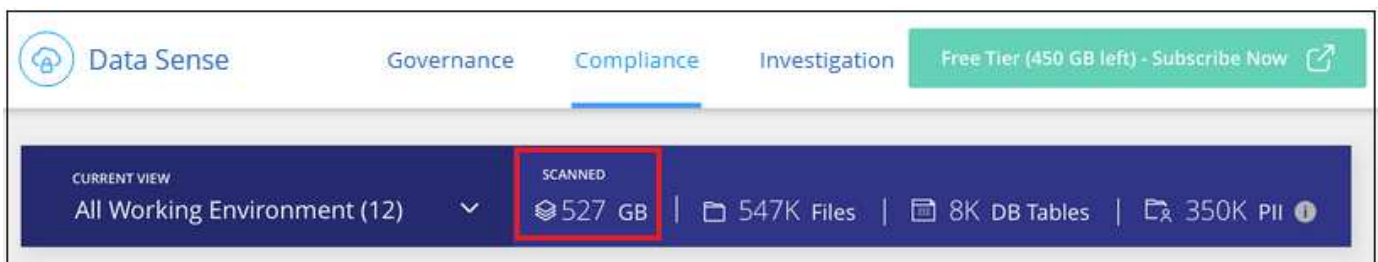
- クラウドプロバイダのマーケットプレイスで Cloud Manager の従量課金制（PAYGO）サブスクリプションにすでに登録している場合は、Cloud Data Sense も自動的にサブスクライブされます。再度登録する必要はありません。
- Cloud Data Sense Bring Your Own License（BYOL；お客様所有のライセンス）は、スキャンを計画しているワークスペース内のすべての作業環境およびデータソースで利用できるフローティングライセンスです。Digital Wallet にアクティブなサブスクリプションが表示されます。

"Cloud Data Sense に関連するライセンスとコストの詳細については、[こちらをご覧ください](#)。"

クラウドデータ従量課金制のサブスクリプションを使用

クラウドプロバイダのマーケットプレイスから従量課金制のサブスクリプションを購入すると、Cloud Volumes ONTAP システムや、クラウドデータセンスの多数のクラウドデータサービスのライセンスを取得できます。

いつでもサブスクライブでき、データ量が 1TB を超えるまでは料金は発生しません。データセンスダッシュボードからスキャンされているデータの総容量を常に確認できます。また、[今すぐサブスクライブ] ボタンを使用すると、準備が整ったときに簡単にサブスクライブできます。



ボタン。"]

これらの手順は、_Account Admin_role 権限を持つユーザが実行する必要があります。

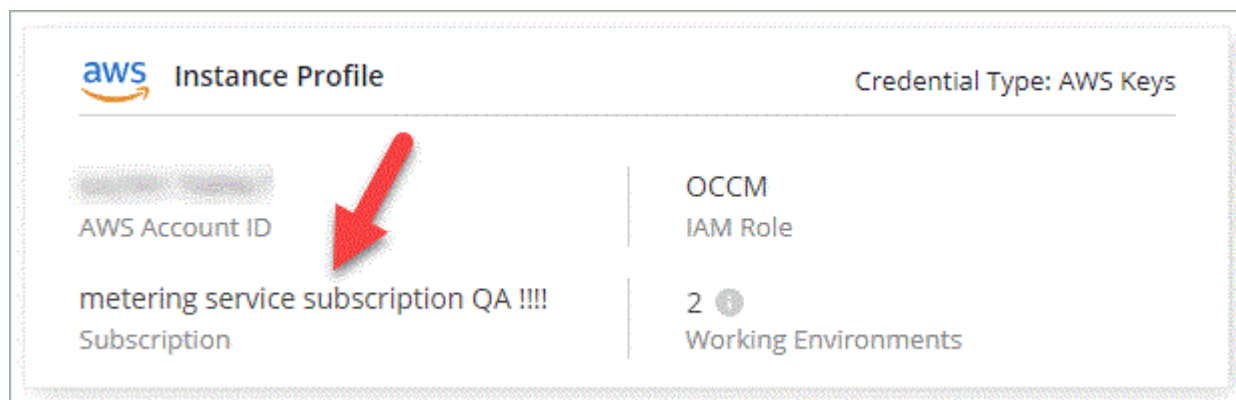
1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、* クレデンシャル * を選択します。



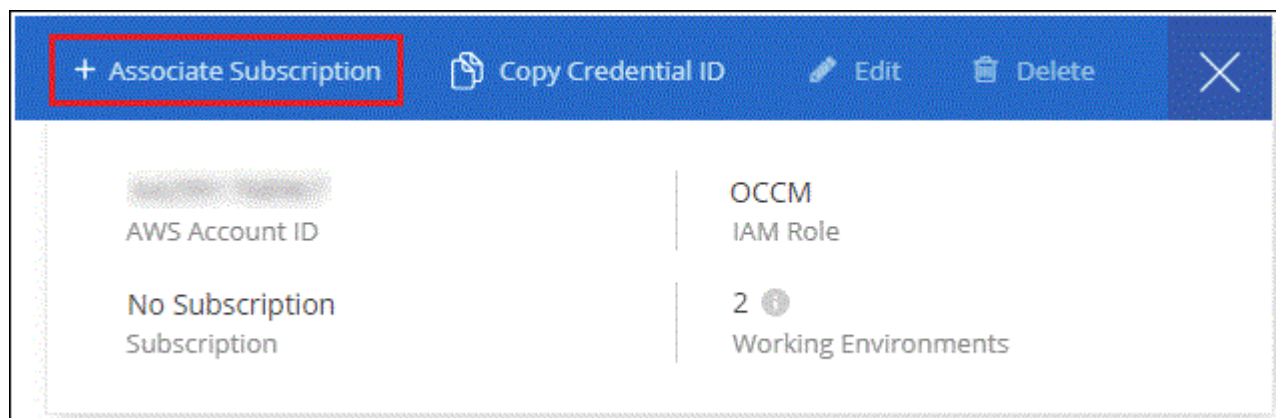
2. AWS インスタンスプロファイル、Azure Managed Service Identity、Google Project のクレデンシャルを検索します。

サブスクリプションは、インスタンスプロファイル、マネージドサービス ID、または Google プロジェクトに追加する必要があります。充電ができない。

すでにサブスクリプション（AWS の場合は以下を参照）をお持ちの場合、設定はすべて済みです。他に必要な機能はありません。



3. まだサブスクリプションをお持ちでない場合は、資格情報の上にカーソルを置いてアクションメニューをクリックし、*サブスクリプションの関連付け*をクリックします。



4. 既存のサブスクリプションを選択し、[* アソシエイト *]をクリックするか、[* サブスクリプションの追加 *]をクリックして、手順を実行します。

次のビデオでは、を関連付ける方法を示します "AWS Marketplace" AWS サブスクリプションへのサブスクリプション：

▶ https://docs.netapp.com/ja-jp/cloud-manager-data-sense//media/video_subscribing_aws.mp4 (video)

次のビデオでは、を関連付ける方法を示します "Azure Marketplace で入手できます" Azure サブスクリプションへのサブスクリプション：

▶ https://docs.netapp.com/ja-jp/cloud-manager-data-sense//media/video_subscribing_azure.mp4 (video)

次のビデオでは、を関連付ける方法を示します "GCP Marketplace" GCP サブスクリプションへのサブスクリプション：

クラウドデータセンス BYOL ライセンスを使用する

ネットアップが提供するお客様所有のライセンスには、1年、2年、3年の期間があります。BYOL * Cloud Data Sense * ライセンスは、フローティング ライセンスで、* すべての作業環境とデータソースで合計容量が共有され、初期ライセンス付与と更新が容易になります。

クラウドデータセンスライセンスをお持ちでない場合は、こちらからお問い合わせください。

- mailto : ng-contact-data-sense@netapp.com ? subject = ライセンス [ライセンスを購入するために電子メールを送信]。
- Cloud Manager の右下にあるチャットアイコンをクリックして、ライセンスを申請してください。

使用しない Cloud Volumes ONTAP 用の未割り当てのノードベースライセンスがある場合は、必要に応じて、ドル同等かつ同じ有効期限を持つ Cloud Data Sense ライセンスに変換できます。"詳細については、[こちらをご覧ください](#)"。

Cloud Manager の Digital Wallet ページを使用して、Cloud Data Sense BYOL ライセンスを管理します。新しいライセンスを追加したり、既存のライセンスを更新したりできます。

Cloud Data Sense ライセンスファイル入手します

Cloud Data Sense ライセンスを購入したら、Cloud Data Sense シリアル番号と NSS アカウントを入力するか、NLF ライセンスファイルをアップロードして、Cloud Manager でライセンスをアクティブ化します。次の手順は、NLF ライセンスファイルを取得する方法を示しています。

インターネットにアクセスできないオンプレミスサイトのホストに Cloud Data Sense を導入した場合は、インターネットに接続されたシステムからライセンスファイルを取得する必要があります。シリアル番号と NSS アカウントを使用してライセンスをアクティブ化することは、ダークサイトへのインストールには使用できません。

手順

1. にサインインします "ネットアップサポートサイト" [システム]、[ソフトウェアライセンス] の順にクリックします。
2. Cloud Data Sense ライセンスのシリアル番号を入力します。

Serial #	Cluster SN	License Name	License Key	Host ID	Value	End Date
4810		SUBS-CLD-DAT-SENSE-TB-2Y	Get NetApp License File		100	12/31/9998

3. [* License Key] で、[* Get NetApp License File*] をクリックします。
4. Cloud Manager アカウント ID (サポートサイトではテナント ID と呼ばれます) を入力し、* Submit * をクリックしてライセンスファイルをダウンロードします。

Get License

SERIAL NUMBER: 4810

LICENSE: SUBS-CLD-DAT-SENSE-TB-2Y

SALES ORDER: 3005

TENANT ID:

Example: account-xxxxxxx

[Cancel](#) [Submit](#)

Cloud Manager アカウント ID は、Cloud Manager の上部にある「* Account *」ドロップダウンを選択し、アカウントの横にある「* Manage Account *」をクリックすると確認できます。アカウント ID は、[概要] タブにあります。

Cloud Data Sense BYOL ライセンスをアカウントに追加します

Cloud Manager アカウント用の Cloud Data Sense ライセンスを購入したら、そのライセンスを Cloud Manager に追加して Data Sense サービスを使用できるようにする必要があります。

手順

1. [すべてのサービス]、[デジタルウォレット]、[データサービスライセンス] の順にクリックします。
2. [ライセンスの追加] をクリックします。
3. ライセンスの追加 ダイアログで、ライセンス情報を入力し、* ライセンスの追加 * をクリックします。
 - データセンスライセンスのシリアル番号があり、NSS アカウントを知っている場合は、* シリアル番号を入力 * オプションを選択してその情報を入力します。

お使いのネットアップサポートサイトのアカウントがドロップダウンリストにない場合は、["NSS アカウントを Cloud Manager に追加します"](#)。

 - データセンスライセンスファイル（ダークサイトにインストールする場合に必要）がある場合は、* ライセンスファイルのアップロード * オプションを選択し、プロンプトに従ってファイルを添付します。

Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

☒ Enter Serial Number
 ☐ Upload License File

Serial Number

NetApp Support Site Account

☐ Enter Serial Number
 ☒ Upload License File

To install a license, follow these instructions:

- Obtain the license file from the "System > Software Licenses" tab at [NetApp Support Site](#). You will need to provide your cloud service serial number and Cloud Manager Account ID.
- Click Upload File and then select the file.

Upload License File

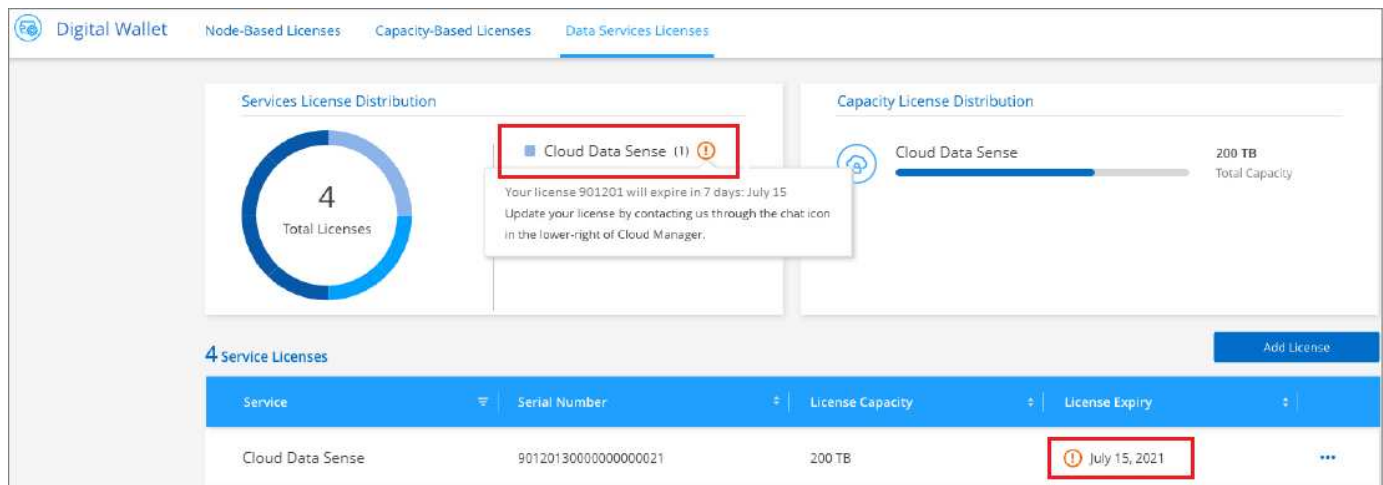
Cloud Manager によってライセンスが追加され、Cloud Data Sense サービスがアクティブになります。

クラウドデータ使用ライセンスを更新します

ライセンス期間が有効期限に近づいている場合や、ライセンスで許可されている容量が上限に達している場合は、Cloud Data Sense で通知が送信されます。



このステータスは、デジタルウォレットにも表示されます。



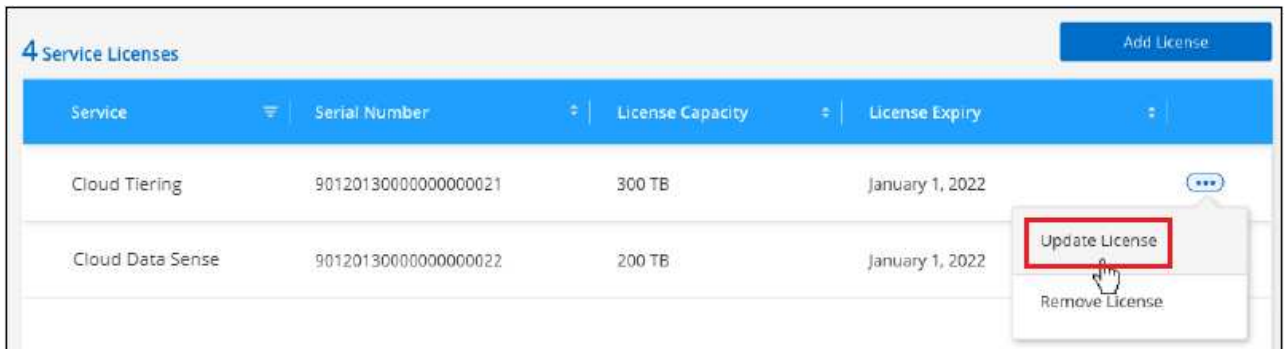
Cloud Data Sense ライセンスは、期限が切れる前に更新できるため、スキャンしたデータへのアクセスが中断されることはありません。

手順

- Cloud Manager の右下にあるチャットアイコンをクリックして、特定のシリアル番号の Cloud Data Sense ライセンスの期間延長または容量の追加をリクエストします。mailto : ng-contact-data-sense@netapp.com ? subject= Licensing [ライセンスの更新をリクエストするメールを送信] もできます。

ライセンスの支払いが完了し、ネットアップサポートサイトに登録されると、Cloud Manager はデジタルウォレットとデータサービスのライセンスページのライセンスを自動的に更新し、5 分から 10 分で変更が反映されます。

2. Cloud Manager がライセンスを自動更新できない場合（ダークサイトにインストールした場合など）は、ライセンスファイルを手動でアップロードする必要があります。
 - a. 可能です [ライセンスファイルをネットアップサポートサイトから入手します](#)。
 - b. [データサービスライセンス] タブの [デジタルウォレット] ページで、をクリックします [...](#) アイコン"] 更新するサービスシリアル番号の場合は、 [* ライセンスの更新 *] をクリックします。



ボタンを選択するスクリーンショット。"]

- c. [_Update License_page](#) で、ライセンスファイルをアップロードし、 [* ライセンスの更新 *](#) をクリックします。

Cloud Manager によってライセンスが更新され、Cloud Data Sense サービスが引き続きアクティブになるようになります。

BYOL ライセンスに関する考慮事項

クラウドデータセンス BYOL ライセンスを使用している場合、スキャンするすべてのデータのサイズが容量の上限に近づいているかライセンスの有効期限に近づいているときに、Cloud Manager のデータセンス UI およびデジタルウォレット UI に警告が表示されます。次の警告が表示されます。

- スキャンするデータ量がライセンスで許可された容量の 80% に達したとき、および制限に達したときに再度スキャンします
- ライセンスの有効期限が切れる 30 日前と、ライセンスの有効期限が切れたあとに再度有効になります

Cloud Manager インターフェイスの右下にあるチャットアイコンを使用して、警告が表示されたときにライセンスを更新してください。

ライセンスの有効期限が切れてもデータセンスは実行されますが、ダッシュボードへのアクセスはブロックされるため、スキャンしたデータに関する情報を表示できません。スキャンするボリューム数を減らして容量の使用量をライセンスの上限までにする場合は、[_Configuration_page](#) だけを使用できます。

BYOL ライセンスを更新すると、Cloud Manager はデジタルウォレットのライセンスを自動的に更新し、すべてのダッシュボードにフルアクセスできるようになります。Cloud Manager がセキュアなインターネット接続経由でライセンスファイルにアクセスできない場合（ダークサイトにインストールされている場合など）は、手動でファイルを入手して Cloud Manager にアップロードできます。手順については、[を参照してください](#) [Cloud Data Sense ライセンスを更新する方法](#)。



使用しているアカウントに BYOL ライセンスと PAYGO の両方のサブスクリプションがある場合、BYOL ライセンスの期限が切れたときに Data Sense が PAYGO サブスクリプションに移行することはありません。BYOL ライセンスを更新する必要があります。

クラウドデータの意味についてよく寄せられる質問

この FAQ は、質問に対する簡単な回答を探している場合に役立ちます。

Cloud Data Sense サービス

以下の質問は、クラウドデータの意味についての一般的な理解を示しています。

クラウドデータの意味

クラウドデータセンスは、人工知能（AI）ベースのテクノロジーを使用して、データの状況を把握し、ストレージシステム全体で機密データを特定するクラウドサービスです。システムは、Cloud Manager Canvasに追加した作業環境や、データが意味するさまざまな種類のデータソースからネットワーク経由でアクセスできる環境にすることができます。 [以下の一覧を参照してください。](#)

Cloud Data Sense は、事前定義されたパラメータ（機密情報の種類やカテゴリなど）を提供し、GDPR、CCPA、HIPAA などのデータプライバシーと機密性に関する新しいデータコンプライアンス規制に対応します。

クラウドデータが適している理由

Cloud Data Sense は、データを活用して以下のことを支援します。

- データコンプライアンスやプライバシーの規制に準拠
- 従来型システムからクラウドへデータを移行
- データ保持ポリシーに準拠
- GDPR、CCPA、HIPAA、その他のデータプライバシー規制の要件に応じて、データ主体に応じて特定のデータを容易に検索し、レポートを作成できます。

クラウドデータの意味でよく使用されるユースケースはどれですか？

- 個人識別情報（PII）を識別します。
- GDPR および CCPA のプライバシー規制の要件に応じて、さまざまな機密情報の範囲を特定します。
- データプライバシーに関する新しい規制や今後の規制に対応できます。

["Cloud Data Sense のユースケースについて詳しくは、こちらをご覧ください"](#)。

クラウドデータはどのように動作するのでしょうか。

Cloud Data Sense は、Cloud Manager システムやストレージシステムと並行して、もう 1 つの人工知能レイヤを導入します。次に、ボリューム、バケット、データベース、その他のストレージアカウントのデータをスキャンして、見つかったデータ分析のインデックスを作成します。データセンスは、正規表現やパターンマッチングを中心に構築される代替ソリューションとは対照的に、人工知能と自然言語処理の両方を活用します。Cloud Data Sense は、AI を使用してデータをコンテキストに基づいて把握し、正確な検出と分類を行います。

す。AIは、最新のデータタイプと拡張性を考慮して設計されているため、この目的はAIによって推進されます。また、データコンテキストを理解して、強力な正確な検出と分類を提供します。

["Cloud Data Sense の仕組みの詳細はこちらをご覧ください"](#)。

Cloud Data Sense はどのくらいの頻度でデータをスキャンしますか？

データが頻繁に変更されるため、Cloud Data Sense は、データに影響を与えることなくデータを継続的にスキャンします。データの初回スキャンには時間がかかる場合がありますが、その後のスキャンでは差分変更のみがスキャンされるため、システムのスキャン時間が短縮されます。

["スキャンの仕組みを説明します"](#)。

データスキャンは、ストレージシステムとデータにほとんど影響を与えません。ただし、影響が非常に小さい場合でも、低速スキャンを実行するようにデータセンスを設定できます。["スキャン速度を下げる方法を参照してください"](#)。

Cloud Data Senseがサポートしている導入モデルを教えてください。

通常、Cloud Data SenseはSaaSモデルを使用して導入されます。このモデルでは、Cloud Managerのインターフェイスからサービスが有効になります。Cloud Data Senseを導入すると、オンプレミス、クラウド、ハイブリッド環境など、ほぼすべての場所にあるシステムをスキャンしてレポートを作成できます。セキュアなインストールの場合、Cloud ManagerとCloud Data Senseは「ダークサイト」モデルで導入できます。ダークサイトは、オンプレミスのパッケージとしてインストールされ、外部ネットワーク接続は必要ありません。

ブラウザとデータセンスの間で送信されたプライベートデータに誰でもアクセスできますか。

いいえブラウザとデータセンスインスタンスの間で送信されるプライベートデータはエンドツーエンドの暗号化によって保護されるため、ネットアップとサードパーティが読み取ることはできません。データセンスは、アクセスをリクエストして承認しない限り、データや結果をネットアップと共有しません。

Cloud Data Sense はレポートを提供していますか？

はい。Cloud Data Sense が提供する情報は、組織内の他の関係者にも関係があるため、レポートを作成して分析情報を共有することができます。Data Sense で使用できるレポートは次のとおりです。

プライバシーリスクアセスメントレポート

データからプライバシーに関する情報を収集し、プライバシーリスクスコアを取得します。["詳細はこちら"](#)。

Data Subject Access Request レポート

データサブジェクトの特定の名前または個人 ID に関する情報を含むすべてのファイルのレポートを抽出できます。["詳細はこちら"](#)。

PCI DSS レポート

クレジットカード情報のファイルへの配布を識別するのに役立ちます。["詳細はこちら"](#)。

HIPAA レポート

健全性情報がファイルにどのように分散されているかを確認できます。["詳細はこちら"](#)。

データマッピングレポート

作業環境内のファイルのサイズと数について説明します。これには、使用容量、データの経過時間、データのサイズ、ファイルタイプが含まれます。"詳細はこちら。"。

特定の情報タイプに関するレポート

個人データや機密性の高い個人データを含む、特定されたファイルの詳細を含むレポートを利用できます。カテゴリおよびファイルタイプ別に分類されたファイルを表示することもできます。"詳細はこちら。"。

スキャンのパフォーマンスは変化しますか？

スキャンのパフォーマンスは、環境内のネットワーク帯域幅と平均ファイルサイズによって異なります。また、（クラウドまたはオンプレミスの）ホストシステムのサイズ特性にも左右されます。を参照してください "Cloud Data Sense インスタンス" および "Cloud Data Sense の導入" を参照してください。

新しいデータソースを最初に追加するときに、「分類」のフルスキャンではなく「マッピング」スキャンのみを実行するように選択することもできます。データソースでは、ファイルにアクセスしてデータを参照できないため、マッピングは短時間で完了します。"マッピングスキャンと分類スキャンの違いを参照してください。"

クラウドデータセンスを有効にする方法

まず、Cloud Manager に Cloud Data Sense のインスタンスを導入する必要があります。インスタンスの実行が完了したら、既存の作業環境、データベース、およびその他のデータソースに対して、* Data Sense *タブからサービスを有効にするか、特定の作業環境を選択してサービスを有効にすることができます。

"開始方法をご確認ください"。



データソースでCloud Data Senseをアクティブにすると、すぐに初期スキャンが実行されます。スキャン結果はすぐ後に表示されます。

クラウドデータセンスを無効にする方法

データセンス構成ページでは、個々の作業環境、データベース、ファイル共有グループ、OneDrive アカウント、SharePoint アカウントをスキャンできないようにすることができます。

"詳細はこちら。"。



クラウドデータセンスインスタンスを完全に削除するには、クラウドプロバイダのポータルまたはオンプレミスの場所から手動でデータセンスインスタンスを削除します。

ONTAP ボリュームでデータ階層化が有効になっている場合、どうなりますか？

コールドデータをオブジェクトストレージに階層化する ONTAP システムでは、クラウドデータの意味を有効にすることができます。データ階層化が有効になっている場合、データセンスは、ディスクにあるすべてのデータと、オブジェクトストレージに階層化されたコールドデータをスキャンします。

コンプライアンススキャンはコールドデータを加熱しません — コールドデータを保存し、オブジェクトストレージに階層化します

Cloud Data Sense は、自分の組織に通知を送信できますか？

はい。ポリシー機能と一緒に、ポリシーの結果が返されたときに Cloud Manager のユーザ（日単位、週単位、または月単位）に E メールアラートを送信して、データを保護するための通知を受け取ることができます。の詳細を確認してください ["ポリシー"](#)。

また、[ガバナンス] ページと [調査] ページからステータスレポートをダウンロードして、組織内で共有することもできます。

組織のニーズに合わせてサービスをカスタマイズできますか。

Cloud Data Sense は、すぐに使用できる分析情報をデータに提供します。これらの分析情報を抽出して、組織のニーズに活用できます。

また、「 * Data Fusion * 」機能を使用すると、スキャンしているデータベース内の特定の列にある条件に基づいて、すべてのデータをデータセンススキャンできます。基本的には、独自のカスタム個人データ型を作成できます。

["詳細はこちら"](#)。

ファイルに埋め込まれた **AIP** ラベルを使用して **Cloud Data Sense** を実行できますか。

はい。加入している場合、Cloud Data Sense がスキャンしているファイルで AIP ラベルを管理できます ["Azure 情報保護（AIP）"](#)。既にファイルに割り当てられているラベルを表示したり、ファイルにラベルを追加したり、既存のラベルを変更したりできます。

["詳細はこちら"](#)。

クラウドデータの意味に関する情報を特定のユーザに制限できますか。

はい。Cloud Data Sense は Cloud Manager と完全に統合されています。Cloud Manager ユーザは、ワークスペースの権限に基づいて表示可能な作業環境の情報のみを表示できます。

また、特定のユーザーがデータセンス設定を管理することなくデータセンススキャン結果を表示できるようにするには、これらのユーザーに `_Cloud Compliance Viewer_role` を割り当てることができます。

["詳細はこちら"](#)。

サポートされているクラウドプロバイダを教えてください。

Cloud Data Sense は Cloud Manager の一部として機能し、AWS、Azure、GCP をサポートします。これにより、異なるクラウドプロバイダ間で統一されたプライバシー可視性を実現できます。

ソースシステムとデータタイプのタイプ

スキャン可能なストレージのタイプ、およびスキャンするデータのタイプに関連する情報を次に示します。

データセンスでスキャンできるデータソースを教えてください。

Cloud Data Senseでは、Cloud Manager Canvasに追加した作業環境や、データがネットワーク経由でアクセスできるさまざまな種類のデータソースからデータをスキャンできます。

- 作業環境：*
- Cloud Volumes ONTAP（AWS、Azure、GCP に導入）
- オンプレミスの ONTAP クラスター
- Azure NetApp Files の特長
- ONTAP 対応の Amazon FSX
- Amazon S3
- データソース：*
- ネットアップ以外のファイル共有
- オブジェクトストレージ（S3 プロトコルを使用）
- データベース（Amazon RDS、MongoDB、MySQL、Oracle、PostgreSQL、SAP HANA、SQL Server など）
- OneDrive アカウント
- SharePoint アカウント
- Googleドライブアカウント

Data Sense は、NFS バージョン 3.x、4.0、4.1、および CIFS バージョン 1.x、2.0、2.1、3.0 をサポートしています。

インターネットにアクセスできないサイトにデータセンスをインストールすると、どのデータソースをスキャンできますか。

データセンスでスキャンできるのは、ローカルのデータソースからオンプレミスのサイトへのデータのみです。現時点では、「ダーク」サイトで次のローカルデータソースをスキャンできます。

- オンプレミスの ONTAP システム
- データベーススキーマ
- ネットアップ以外の NFS または CIFS ファイル共有
- Simple Storage Service（S3）プロトコルを使用するオブジェクトストレージ

サポートされているファイルタイプはどれですか。

Cloud Data Senseは、すべてのファイルをスキャンしてカテゴリやメタデータに関する分析情報を検索し、ダッシュボードのファイルタイプセクションにすべてのファイルタイプを表示します。

データセンスが個人識別情報（PII）を検出した場合、またはdsar検索を実行した場合、次のファイル形式のみがサポートされます。

「+.csv」、「.dcm」、「.dom」、「.DOC」、「.DOCX」、.json、.pdf、.PPTX、.rtf、.TXT、.XLS、.xlsx、Docs、Sheets、Slides +`

Cloud Dataでは、どのような種類のデータやメタデータをキャプチャできますか？

Cloud Data Senseを使用すると、データソースに対して全般的な「マッピング」スキャンまたは完全な「分類」スキャンを実行できます。マッピングではデータの概要のみが示され、分類ではデータの詳細なスキャンが提供されます。データソースでは、ファイルにアクセスしてデータを参照できないため、マッピングは短時

間で完了します。

- データマッピングスキャン：

データセンスはメタデータのみをスキャンします。これは、全体的なデータ管理とガバナンス、プロジェクトの迅速な範囲設定、非常に大規模な環境、優先順位付けに役立ちます。データマッピングはメタデータに基づいており、*高速*スキャンとみなされます。

高速スキャンの後、データマッピングレポートを生成できます。このレポートは、企業データソースに保存されているデータの概要を示しており、リソースの使用率、移行、バックアップ、セキュリティ、コンプライアンスの各プロセスに関する決定に役立ちます。

- データ分類（ディープ）スキャン。

お客様の環境全体で、標準プロトコルと読み取り専用アクセス権を使用してデータセンススキャンを実行します。一部のファイルは、ビジネスに関連する機密データ、プライベート情報、ランサムウェアに関連する問題の有無をチェックして開きます。

フルスキャンの後にデータに適用できるデータ検出機能が多数あります。たとえば、[データ調査]ページでのデータの表示とリファイン、ファイル内での名前の検索、ソースファイルのコピー、移動、削除などです。

ライセンスとコスト

Cloud Data Senseを使用するためのライセンスとコストに関する質問を次に示します。

クラウドデータのコストはどれくらいですか？

クラウドデータセンスの使用コストは、スキャンするデータの量によって異なります。データをスキャンする、Cloud Manager ワークスペース内の最初の 1TB のデータは無料です。この制限に達すると、1TBを超えるデータのスキャンを続行するために次のいずれかが必要になります。

- クラウドプロバイダまたはからCloud Manager Marketplaceに登録するためのサブスクリプション
- ネットアップが提供するお客様所有のライセンス（BYOL）

を参照してください ["価格設定"](#) を参照してください。

BYOLの容量制限に達した場合はどうなりますか？

BYOLの容量制限に達すると、データセンスは引き続き実行されますが、ダッシュボードへのアクセスはブロックされるため、スキャンしたデータに関する情報を表示することはできません。スキャンするボリューム数を減らして容量の使用率をライセンスの上限まで下げる場合は、設定ページのみが表示されます。データセンスへのフルアクセスを回復するには、BYOLライセンスを更新する必要があります。

コネクタの展開

Cloud Manager Connectorに関連する質問を次に示します。

コネクタは何ですか？

Connectorは、クラウドアカウント内またはオンプレミスでコンピューティングインスタンス上で実行される

ソフトウェアで、Cloud Managerによるクラウドリソースのセキュアな管理を可能にします。クラウドデータセンスを使用するには、コネクタを導入する必要があります。

コネクタはどこに取り付ける必要がありますか？

- AWS、Amazon FSX for ONTAP、またはAWS S3 バケット内の Cloud Volumes ONTAP のデータをスキャンするときは、AWS のコネクタを使用します。
- Azure または Azure NetApp Files で Cloud Volumes ONTAP 内のデータをスキャンする場合は、Azure のコネクタを使用します。
- GCP の Cloud Volumes ONTAP でデータをスキャンする場合は、GCP のコネクタを使用します。
- オンプレミスのONTAP システム、ネットアップ以外のファイル共有、汎用のS3オブジェクトストレージ、データベース、OneDriveフォルダ、SharePointアカウント、Google Driveアカウント内のデータをスキャンする場合、これらのクラウド環境ではコネクタを使用できます。

そのため、これらの場所の多くにデータがある場合は、を使用する必要があります ["複数のコネクタ"](#)。

コネクタを自分のホストに導入できますか。

はい。可能です ["コネクタをオンプレミスに導入"](#) 自社ネットワーク内またはクラウド内の Linux ホストオンプレミスにデータセンスを導入する場合は、オンプレミスにもコネクタをインストールできますが、必須ではありません。

インターネットにアクセスできないセキュアなサイトはどうでしょうか。

はい、サポートされています。可能です ["インターネットにアクセスできないオンプレミスのLinuxホストにコネクタを導入します"](#)。その上で、オンプレミスのONTAP クラスタやその他のローカルデータソースを検出し、データセンスを使用してデータをスキャンすることができます。

データセンスの導入

以下の質問は、個別のData Senseインスタンスに関連しています。

クラウドデータセンスにはどのようなタイプのインスタンスまたは **VM** が必要ですか。

いつ ["クラウドに導入"](#)：

- AWS では、Cloud Data Sense は、500 GB の gp2 ディスクを使用する m5.-m構築 インスタンスで実行されます。
- Azure では、Cloud Data Sense は、512 GB のディスクを搭載した Standard_D16s_v3 VM で実行されます。
- GCP では、クラウドデータセンスは、512 GB の標準永続ディスクを搭載した n2 標準の -16 VM で実行されます。

CPU 数と RAM 容量が少ないシステムには Data Sense を導入できますが、これらのシステムの使用には制限があります。を参照してください ["小さいインスタンスタイプを使用しています"](#) を参照してください。

["Cloud Data Sense の仕組みの詳細はこちらをご覧ください"](#)。

データセンスを自分のホストに導入できますか。

はい。データセンスソフトウェアは、ネットワーク内またはクラウド内でインターネットにアクセスできる Linux ホストにインストールできます。すべてが同じように機能し、Cloud Manager を使用してスキャンの設定と結果を引き続き管理できます。を参照してください ["クラウドデータセンスをオンプレミスに導入"](#) を参照してください。

インターネットにアクセスできないセキュアなサイトはどうでしょうか。

はい、サポートされています。可能です ["インターネットにアクセスできないオンプレミスサイトにデータセンスを導入する"](#) 完全にセキュアなサイトに。

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.