



データ分類を展開する

NetApp Data Classification

NetApp
February 11, 2026

目次

データ分類を展開する	1
どのNetApp Data Classification展開を使用する必要がありますか?	1
NetApp Consoleを使用してクラウドにNetApp Data Classificationを導入する	1
クイック スタート	2
コンソールエージェントを作成する	2
前提条件	3
クラウドでデータ分類を展開	6
インターネットにアクセスできるホストにNetApp Data Classificationをインストールする	8
クイック スタート	10
コンソールエージェントを作成する	10
Linuxホストシステムを準備する	11
データ分類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	13
必要なポートがすべて有効になっていることを確認します	14
Linuxホストにデータ分類をインストールする	15
インターネットにアクセスできない Linux ホストにNetApp Data Classificationをインストールする	19
LinuxホストがNetApp Data Classificationをインストールする準備ができていることを確認します	19
はじめに	19
コンソールエージェントを作成する	20
ホストの要件を確認する	20
データ分類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	22
必要なポートがすべて有効になっていることを確認します	23
データ分類の前提条件スクリプトを実行する	23

データ分類を展開する

どのNetApp Data Classification展開を使用する必要がありますか？

NetApp Data Classification はさまざまな方法で導入できます。どの方法がニーズに合っているかを学びます。

データ分類は次の方法で展開できます。

- ["コンソールを使用してクラウドにデプロイする"](#)。コンソールは、コンソール エージェントと同じクラウド プロバイダー ネットワークにデータ分類インスタンスを展開します。
- ["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する"](#)。インターネットにアクセスできるネットワーク内の Linux ホスト、またはクラウド内の Linux ホストに Data Classification をインストールします。このタイプのインストールは、オンプレミスにあるデータ分類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に適したオプションですが、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オンプレミス サイトの Linux ホストにインストールする"](#)プライベート モード とも呼ばれます。インストール スクリプトを使用するこのタイプのインストールでは、コンソール SaaS レイヤーへの接続はありません。



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

インターネットにアクセスできる Linux ホストへのインストールと、インターネットにアクセスできない Linux ホストへのオンプレミス インストールの両方で、インストール スクリプトが使用されます。スクリプトは、システムと環境が前提条件を満たしているかどうかを確認することから始まります。前提条件が満たされている場合は、インストールが開始されます。データ分類のインストールを実行せずに前提条件を検証したい場合は、前提条件のみをテストする別のソフトウェア パッケージをダウンロードできます。

。 ["Linuxホストがデータ分類をインストールする準備ができていることを確認します"](#)。

NetApp Consoleを使用してクラウドにNetApp Data Classificationを導入する

NetApp Consoleを使用して、クラウドにNetApp Data Classification を導入できます。コンソールは、コンソール エージェントと同じクラウド プロバイダー ネットワークにデータ分類インスタンスを展開します。

また、["インターネットにアクセスできる Linux ホストにデータ分類をインストールする"](#)。このタイプのインストールは、オンプレミスにあるデータ分類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に適したオプションですが、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

以下の手順に従ってすぐに開始するか、残りのセクションまでスクロールして詳細を確認してください。

1

コンソールエージェントを作成する

コンソール エージェントがまだない場合は作成します。見る["AWSでコンソールエージェントを作成する"](#)、["Azureでコンソールエージェントを作成する"](#)、 または["GCP でコンソール エージェントを作成する"](#)。

また、["オンプレミスにコンソールエージェントをインストールする"](#)ネットワーク内の Linux ホストまたはクラウド内の Linux ホスト上。

2

前提条件

お使いの環境が前提条件を満たしていることを確認してください。これには、インスタンスの外向きインターネットアクセス、ConsoleエージェントとData Classification間のポート443での接続などが含まれます。[完全なリストを見る](#)。

3

データ分類を展開する

インストール ウィザードを起動して、データ分類インスタンスをクラウドにデプロイします。

コンソールエージェントを作成する

コンソール エージェントがまだない場合は、クラウド プロバイダーにコンソール エージェントを作成します。見る ["AWSでコンソールエージェントを作成する"](#)または ["Azureでコンソールエージェントを作成する"](#)、または ["GCP でコンソール エージェントを作成する"](#)。ほとんどの場合、データ分類を有効化する前にコンソールエージェントをセットアップしておく必要があります。 ["コンソール機能にはコンソールエージェントが必要です"](#)ただし、今すぐ設定する必要がある場合もあります。

特定のクラウド プロバイダーにデプロイされたコンソール エージェントを使用する必要があるシナリオがいくつかあります。

- AWS のCloud Volumes ONTAPまたはAmazon FSx for ONTAPバケット内のデータをスキャンする場合は、AWS のコンソールエージェントを使用します。
- Azure のCloud Volumes ONTAPまたはAzure NetApp Filesでデータをスキャンする場合は、Azure のコンソール エージェントを使用します。
 - Azure NetApp Filesの場合、スキャンするボリュームと同じリージョンにデプロイする必要があります。
- GCP のCloud Volumes ONTAPでデータをスキャンする場合は、GCP のコンソール エージェントを使用します。

これらのクラウド コンソール エージェントのいずれかを使用すると、オンプレミスのONTAPシステム、NetAppファイル共有、およびデータベースをスキャンできます。

また、 ["オンプレミスにコンソールエージェントをインストールする"](#)ネットワークまたはクラウド内の Linux ホスト上。オンプレミスでデータ分類をインストールする予定のユーザーの中には、オンプレミスでコンソール エージェントをインストールすることを選択する場合もあります。

使用する必要がある状況があるかもしれません ["複数のコンソールエージェント"](#)。



データ分類では、スキャンできるデータの量に制限はありません。各コンソール エージェントは、500 TiB のデータのスキャンと表示をサポートします。500TiB以上のデータをスキャンするには、["別のコンソールエージェントをインストールする"](#)それから["別のデータ分類インスタンスをデプロイする"](#)。+ コンソール UI には、単一のコネクタからのデータが表示されます。複数のコンソールエージェントからデータを表示するヒントについては、["複数のコンソールエージェントを操作する"](#)。

政府地域支援

データ分類は、コンソール エージェントが政府リージョン (AWS GovCloud、Azure Gov、または Azure DoD) にデプロイされている場合にサポートされます。この方法で展開する場合、データ分類には次の制限があります。

["政府地域におけるコンソールエージェントの導入について学習します"](#)。

前提条件

クラウドにデータ分類を展開する前に、次の前提条件を確認して、サポートされている構成があることを確認してください。クラウドにデータ分類を展開すると、コンソール エージェントと同じサブネットに配置されます。

データ分類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

データ分類には、アウトバウンドのインターネット アクセスが必要です。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 サーバーを使用している場合は、データ分類インスタンスに次のエンドポイントに接続するための送信インターネット アクセスがあることを確認してください。プロキシは非透過である必要があります。透過プロキシは現在サポートされていません。

データ分類を AWS、Azure、GCP のいずれに展開するかに応じて、以下の適切な表を確認してください。

AWSに必要なエンドポイント

エンドポイント	目的
https://api.console.netapp.com	NetAppアカウントを含むコンソール サービスとの通信。
https://netapp-cloud-account.auth0.com https://auth0.com	集中ユーザー認証のためのコンソール Web サイトとの通信。
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://dseasb33srrrn.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を提供します。
https://kinesis.us-east-1.amazonaws.com	NetApp 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	データ分類を有効にして、マニフェストとテンプレートにアクセスしてダウンロードし、ログとメトリックを送信できるようにします。

Azureに必要なエンドポイント

エンドポイント	目的
https://api.console.netapp.com	NetAppアカウントを含むコンソール サービスとの通信。
https://netapp-cloud-account.auth0.com https://auth0.com	集中ユーザー認証のためのコンソール Web サイトとの通信。
https://support.compliance.api.console.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srrrn.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を提供し、ログとメトリックを送信します。
https://support.compliance.api.console.netapp.com/	NetApp 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。

GCP に必要なエンドポイント

エンドポイント	目的
https://api.console.netapp.com	NetAppアカウントを含むコンソール サービスとの通信。
https://netapp-cloud-account.auth0.com https://auth0.com	集中ユーザー認証のためのコンソール Web サイトとの通信。

エンドポイント	目的
https://support.compliance.api.console.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を提供し、ログとメトリックを送信します。
https://support.compliance.api.console.netapp.com/	NetApp 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。

データ分類に必要な権限があることを確認する

データ分類に、リソースをデプロイし、データ分類インスタンスのセキュリティ グループを作成するための権限があることを確認します。

- ["Google Cloud の権限"](#)
- ["AWS 権限"](#)
- ["Azure のアクセス許可"](#)

コンソールエージェントがデータ分類にアクセスできることを確認する

コンソール エージェントとデータ分類インスタンス間の接続を確認します。コンソール エージェントのセキュリティ グループは、ポート 443 経由のデータ分類インスタンスとの間の受信トラフィックと送信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、データ分類インスタンスのデプロイが可能になり、コンプライアンス タブとガバナンス タブで情報を表示できるようになります。データ分類は、AWS および Azure の政府リージョンでサポートされています。

AWS および AWS GovCloud のデプロイメントには、追加の受信および送信セキュリティ グループ ルールが必要です。見る ["AWS のコンソールエージェントのルール"](#)詳細については。

Azure および Azure Government の展開には、追加の受信および送信セキュリティ グループ ルールが必要です。見る ["Azure のコンソール エージェントのルール"](#)詳細については。

データ分類を継続して実行できるようにする

データを継続的にスキャンするには、データ分類インスタンスをオンのままにしておく必要があります。

データ分類への**Web**ブラウザ接続を確保する

データ分類を有効にした後、ユーザーがデータ分類インスタンスに接続しているホストからコンソール インターフェイスにアクセスすることを確認します。

データ分類インスタンスは、インデックス付けされたデータがインターネットからアクセスできないようにするためにプライベート IP アドレスを使用します。そのため、コンソールにアクセスするために使用する 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 プロバイダーへの直接接続 (VPN など) から行うことも、データ分類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もできます。

vCPUの制限を確認する

クラウド プロバイダーの vCPU 制限によって、必要な数のコアを持つインスタンスのデプロイが許可されていることを確認します。コンソール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確認する"](#)。

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

クラウドでデータ分類を展開

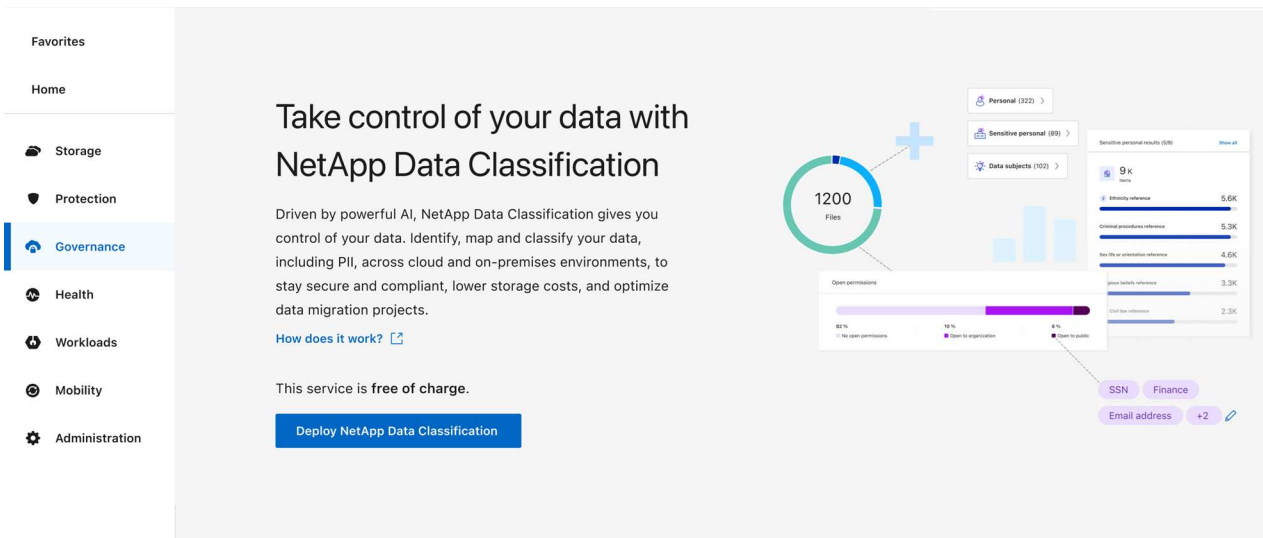
クラウドにデータ分類のインスタンスをデプロイするには、次の手順に従います。コンソール エージェントはクラウドにインスタンスを展開し、そのインスタンスにデータ分類ソフトウェアをインストールします。

デフォルトのインスタンスタイプが利用できない地域では、データ分類は["代替インスタンスタイプ"](#)。

AWSにデプロイ

手順

1. データ分類のメイン ページから、オンプレミスまたはクラウドでの分類の展開 を選択します。

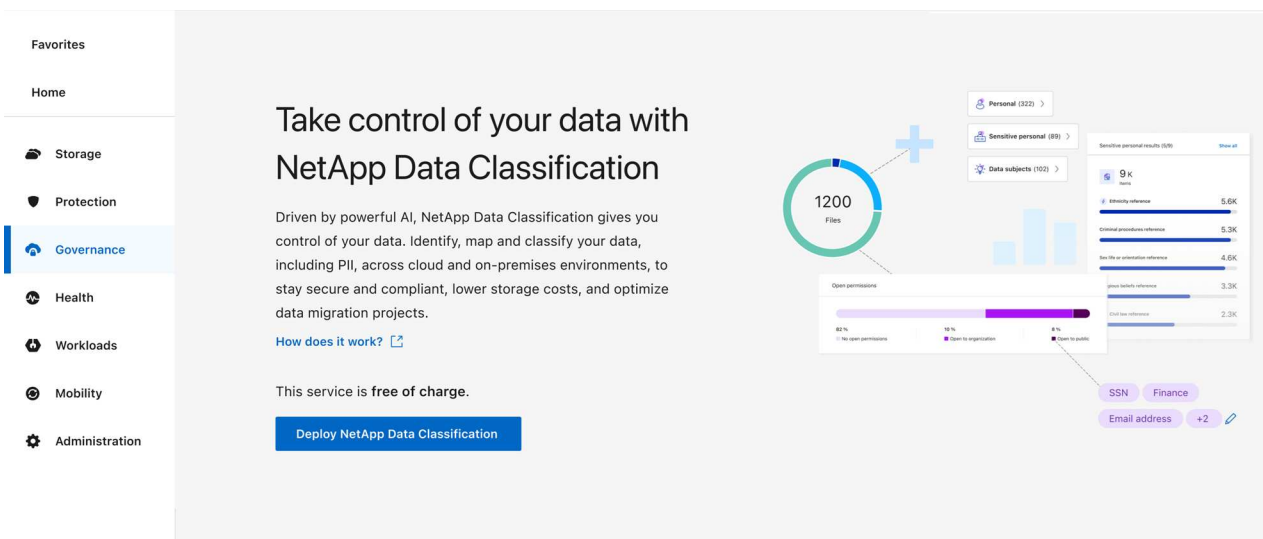


2. インストール ページで、デプロイ > デプロイ を選択して、「大」インスタンス サイズを使用し、クラウド デプロイ ウィザードを起動します。
3. ウィザードは、展開手順を実行する際の進行状況を表示します。入力が必要な場合、または問題が発生した場合には、プロンプトが表示されます。
4. インスタンスがデプロイされ、データ分類がインストールされたら、[構成に進む] を選択して [構成] ページに移動します。

Azureにデプロイする

手順

1. データ分類のメイン ページから、オンプレミスまたはクラウドでの分類の展開 を選択します。



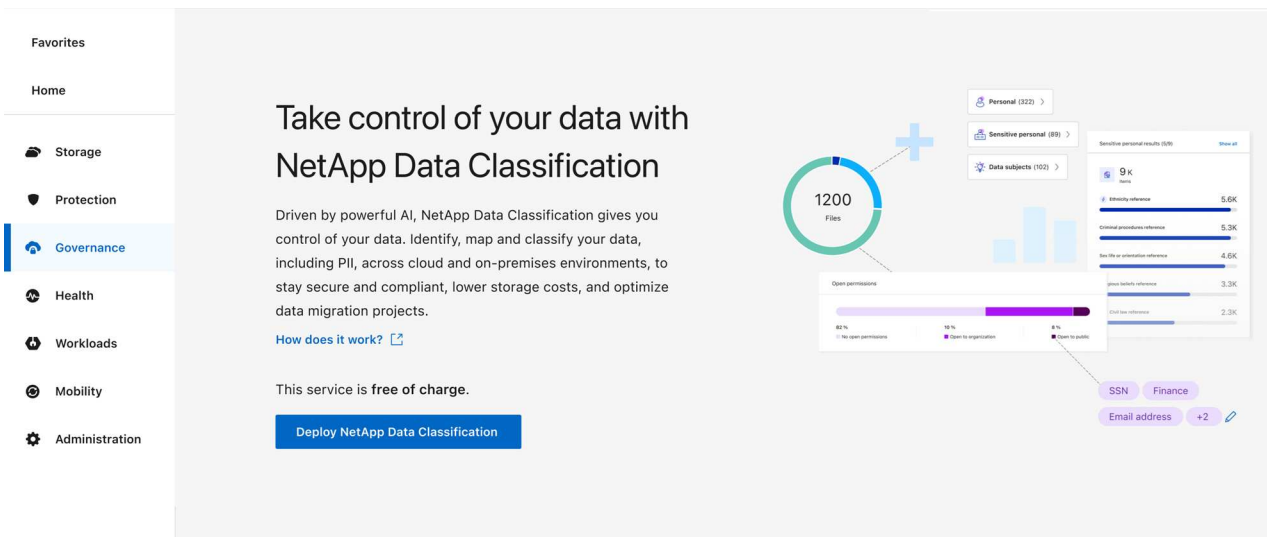
2. デプロイ を選択して、クラウド デプロイ ウィザードを起動します。

3. ウィザードは、展開手順を実行する際の進行状況を表示します。問題が発生すると停止し、入力を求められます。
4. インスタンスがデプロイされ、データ分類がインストールされたら、[構成に進む] を選択して [構成] ページに移動します。

Google Cloud にデプロイ

手順

1. データ分類のメイン ページから、ガバナンス > 分類 を選択します。
2. *オンプレミスまたはクラウドでの分類の展開*を選択します。



3. デプロイ を選択して、クラウド デプロイ ウィザードを起動します。
4. ウィザードは、展開手順を実行する際の進行状況を表示します。問題が発生すると停止し、入力を求められます。
5. インスタンスがデプロイされ、データ分類がインストールされたら、[構成に進む] を選択して [構成] ページに移動します。

結果

コンソールは、クラウド プロバイダーにデータ分類インスタンスをデプロイします。

インスタンスがインターネットに接続されている限り、コンソール エージェントとデータ分類ソフトウェアへのアップグレードは自動的に行われます。

次は何？

構成ページから、スキャンするデータ ソースを選択できます。

インターネットにアクセスできるホストにNetApp Data Classificationをインストールする

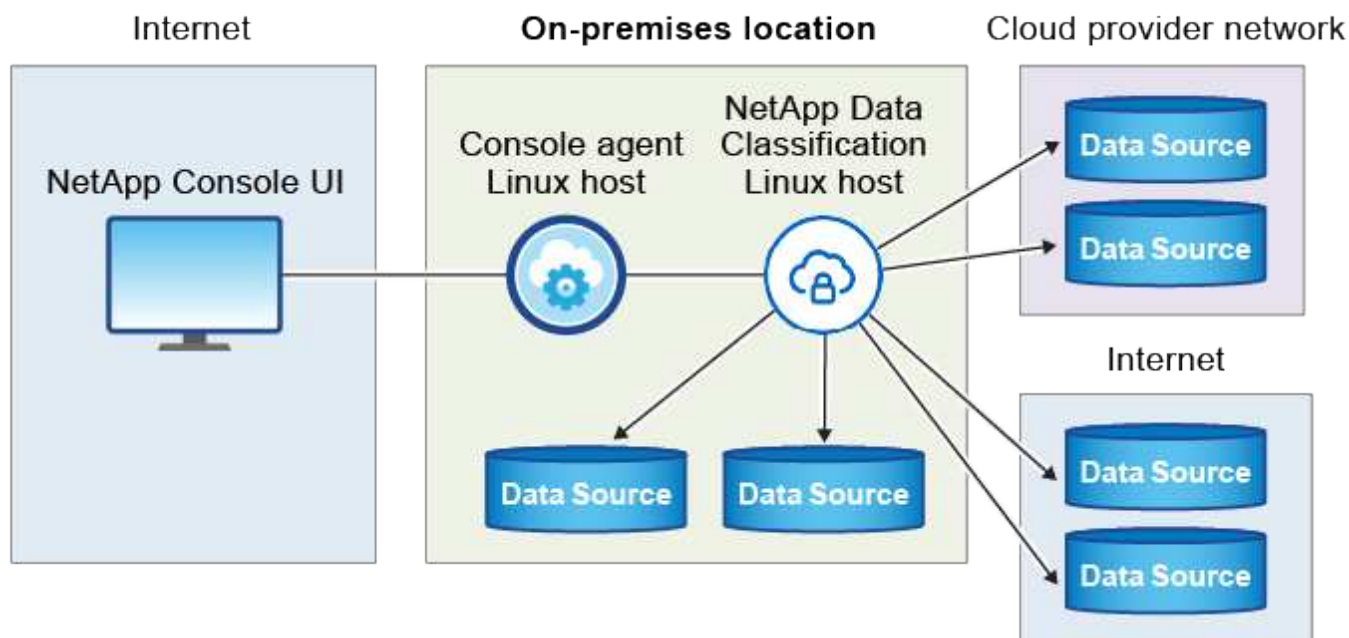
ネットワーク内の Linux ホストまたはインターネットにアクセスできるクラウド内の Linux ホストにNetApp Data Classification を展開するには、ネットワークまたはクラウド

ドに Linux ホストを手動で展開する必要があります。

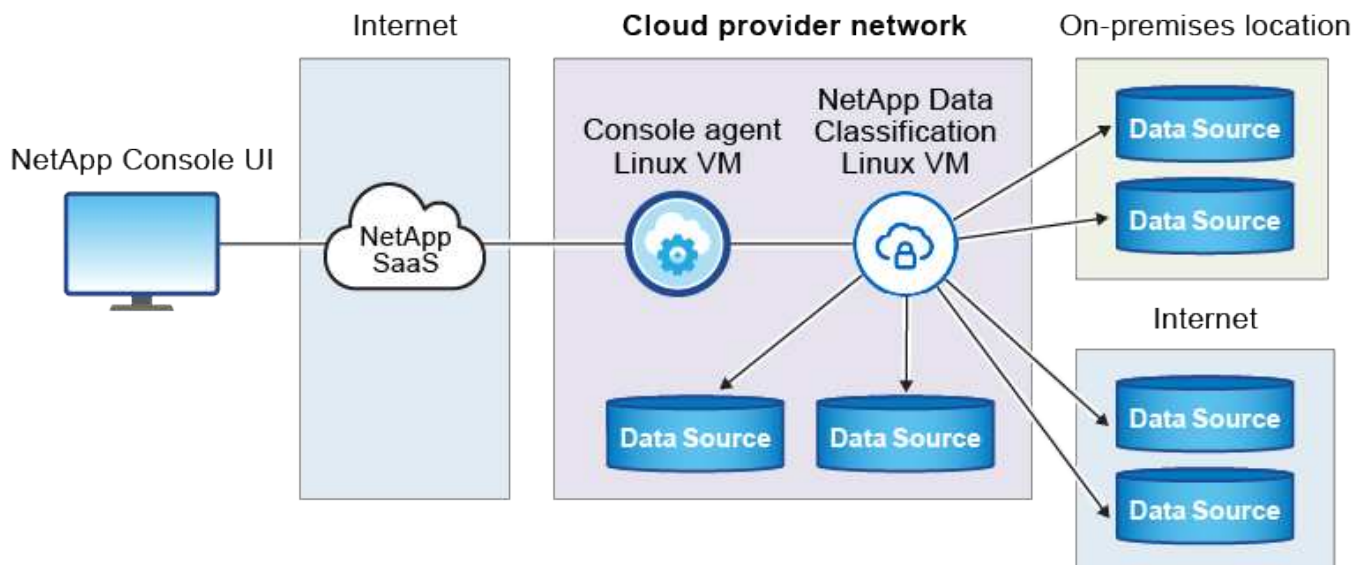
オンプレミス インストールは、オンプレミスにあるデータ分類インスタンスを使用してオンプレミスのONTAPシステムをスキャンする場合に適したオプションです。これは必須ではありません。どのインストール方法を選択しても、ソフトウェアは同じように機能します。

データ分類のインストール スクリプトは、システムと環境が必要な前提条件を満たしているかどうかを確認することから始まります。前提条件がすべて満たされている場合は、インストールが開始されます。データ分類のインストールの実行とは別に前提条件を検証したい場合は、前提条件のみをテストする別のソフトウェアパッケージをダウンロードできます。["Linuxホストがデータ分類をインストールする準備ができているかどうかを確認する方法をご覧ください"](#)。

社内の Linux ホストへの一般的なインストールには、次のコンポーネントと接続が含まれます。



クラウド内の Linux ホストへの一般的なインストールには、次のコンポーネントと接続が含まれます。



クイック スタート

以下の手順に従ってすぐに開始するか、残りのセクションまでスクロールして詳細を確認してください。

1

コンソールエージェントを作成する

コンソールエージェントがまだない場合は、"[コンソールエージェントをオンプレミスに展開する](#)"ネットワーク内の Linux ホスト上、またはクラウド内の Linux ホスト上。

クラウド プロバイダーを使用してコンソール エージェントを作成することもできます。見る "[AWSでコンソールエージェントを作成する](#)"、"[Azureでコンソールエージェントを作成する](#)"、または "[GCP でコンソールエージェントを作成する](#)"。

2

前提条件を確認する

ご使用の環境が前提条件を満たしていることを確認してください。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 経由のコンソール エージェントとデータ分類間の接続などが含まれます。[完全なリストを見る](#)。

また、以下の要件を満たすLinuxシステムも必要です。[以下の要件](#)。

3

データ分類をダウンロードして展開する

NetAppサポート サイトから Cloud Data Classification ソフトウェアをダウンロードし、使用する予定の 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データ分類インスタンスをデプロイします。

コンソールエージェントを作成する

Data Classification をインストールして使用する前に、コンソール エージェントが必要です。ほとんどの場合、データ分類を有効化する前にコンソールエージェントをセットアップしておく必要があります。["コンソール機能にはコンソールエージェントが必要です"](#)ただし、今すぐ設定する必要がある場合もあります。

クラウドプロバイダー環境で作成するには、"[AWSでコンソールエージェントを作成する](#)"、"[Azureでコンソールエージェントを作成する](#)"、または "[GCP でコンソール エージェントを作成する](#)"。

特定のクラウド プロバイダーにデプロイされたコンソール エージェントを使用する必要があるシナリオがいくつかあります。

- AWS のCloud Volumes ONTAPまたはAmazon FSx for ONTAPでデータをスキャンする場合は、AWS のコンソールエージェントを使用します。
- Azure のCloud Volumes ONTAPまたはAzure NetApp Filesでデータをスキャンする場合は、Azure のコンソール エージェントを使用します。

Azure NetApp Filesの場合、スキャンするボリュームと同じリージョンにデプロイする必要があります。

- GCP のCloud Volumes ONTAPでデータをスキャンする場合は、GCP のコンソール エージェントを使用します。

オンプレミスのONTAPシステム、NetAppファイル共有、データベース アカウントは、これらのクラウド コ

ンソール エージェントのいずれかを使用してスキャンできます。

また、"[コンソールエージェントをオンプレミスに展開する](#)"ネットワーク内の Linux ホストまたはクラウド内の Linux ホスト上。オンプレミスで Data Classification をインストールする予定のユーザーの中には、オンプレミスでコンソール エージェントをインストールすることを選択する場合があります。

Data Classification をインストールするときは、コンソール エージェント システムの IP アドレスまたはホスト名が必要になります。オンプレミスでコンソール エージェントをインストールした場合は、この情報が得られます。コンソール エージェントがクラウドに展開されている場合は、コンソールからこの情報を確認できます。ヘルプ アイコンを選択し、次に サポート、コンソール エージェント を選択します。

Linuxホストシステムを準備する

データ分類ソフトウェアは、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上で実行する必要があります。Linux ホストはネットワーク内またはクラウド内に配置できます。

データ分類を実行し続けることができることを確認します。データ分類マシンは、データを継続的にスキャンするためにオンのままにしておく必要があります。

- データ分類は専用ホスト上で実行する必要があります。ホストは、他のアプリケーションやウイルス対策などのサードパーティ製ソフトウェアと共有することはできません。
- データ分類でスキャンする予定のデータ セットに合わせてサイズを選択します。

システムサイズ	CPU	RAM (スワップメモリを無効にする必要があります)	ディスク
特大	CPU×32	128GBのRAM	• / に 1 TiB SSD、または /opt に 100 GiB 利用可能 • /var/lib/docker で 895 GiB が利用可能 • /tmp に 5 GiB • Podman の場合、/var/tmp に 30 GB
大きい	CPU×16	64GBのRAM	• / に 500 GiB SSD、または /opt に 100 GiB 利用可能 • /var/lib/docker または Podman /var/lib/containers で 400 GiB が利用可能 • /tmp に 5 GiB • Podman の場合、/var/tmp に 30 GB

- データ分類インストール用にクラウドにコンピューティング インスタンスをデプロイする場合は、上記の「大規模」システム要件を満たすシステムを使用することをお勧めします。
 - **Amazon Elastic Compute Cloud (Amazon EC2)** インスタンスタイプ: 「m6i.4xlarge」。["その他のAWSインスタンスタイプを見る"](#)。

- **Azure VM** サイズ: 「Standard_D16s_v3」 。 ["その他のAzureインスタンスタイプを見る"](#) 。
- **GCP** マシンタイプ: 「n2-standard-16」 。 ["その他の GCP インスタンスタイプを見る"](#) 。
- **UNIX** フォルダ権限: 次の最低限の UNIX 権限が必要です。

フォルダ	最小限の権限
/tmp	rwXrwxrwt
/opt	rwXr-Xr-X
/var/lib/docker	rwX-----
/usr/lib/systemd/システム	rwXr-Xr-X

- **オペレーティング・システム** :
 - 次のオペレーティング システムでは、Docker コンテナ エンジンを使用する必要があります。
 - Red Hat Enterprise Linux バージョン 7.8 および 7.9
 - Ubuntu 22.04 (データ分類バージョン 1.23 以上が必要)
 - Ubuntu 24.04 (データ分類バージョン 1.23 以上が必要)
 - 次のオペレーティング システムでは、Podman コンテナ エンジンを使用する必要があります、データ分類バージョン 1.30 以上が必要です。
 - Red Hat Enterprise Linux バージョン 8.8、8.10、9.0、9.1、9.2、9.3、9.4、9.5、および 9.6。
 - ホスト システムで Advanced Vector Extensions (AVX2) を有効にする必要があります。
- **Red Hat サブスクリプション管理**: ホストは Red Hat サブスクリプション管理に登録されている必要があります。登録されていない場合、システムはリポジトリにアクセスできず、インストール中に必要なサードパーティ製ソフトウェアを更新できません。
- **追加ソフトウェア**: Data Classification をインストールする前に、ホストに次のソフトウェアをインストールする必要があります。
 - 使用している OS に応じて、次のいずれかのコンテナ エンジンを実インストールする必要があります。
 - Docker Engine バージョン 19.3.1 以上。 ["インストール手順を見る"](#) 。
 - Podman バージョン 4 以上。 Podmanをインストールするには、次のように入力します。(sudo yum install podman netavark -y) 。
- **Python バージョン 3.6 以上**。 ["インストール手順を見る"](#) 。
- **NTP** に関する考慮事項: NetApp、データ分類システムをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。データ分類システムとコンソール エージェント システムの間で時刻を同期する必要があります。
- **Firewalldの考慮事項**: 使用を計画している場合 firewalld、データ分類をインストールする前に有効にすることをお勧めします。設定するには次のコマンドを実行します `firewalld` データ分類と互換性があるように:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

追加のデータ分類ホストをスキャナー ノードとして使用することを計画している場合は、この時点で次のルールをプライマリ システムに追加します。

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

有効化または更新するたびにDockerまたはPodmanを再起動する必要があることに注意してください。
`firewalld`設定。



データ分類ホスト システムの IP アドレスは、インストール後に変更することはできません。

データ分類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

データ分類には、アウトバウンドのインターネット アクセスが必要です。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 サーバーを使用している場合は、データ分類インスタンスに次のエンドポイントに接続するための送信インターネット アクセスがあることを確認してください。

エンドポイント	目的
https://api.console.netapp.com	NetAppアカウントを含むコンソールとの通信。
https://netapp-cloud-account.auth0.com https://auth0.com	集中ユーザー認証のためのコンソール Web サイトとの通信。
https://support.compliance.api.bluelxp.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を提供し、ログとメトリックを送信します。
https://support.compliance.api.bluelxp.netapp.com/	NetApp 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	docker インストールの前提条件パッケージを提供します。
http://packages.ubuntu.com/ http://archive.ubuntu.com	Ubuntu インストールの前提条件となるパッケージを提供します。

必要なポートがすべて有効になっていることを確認します

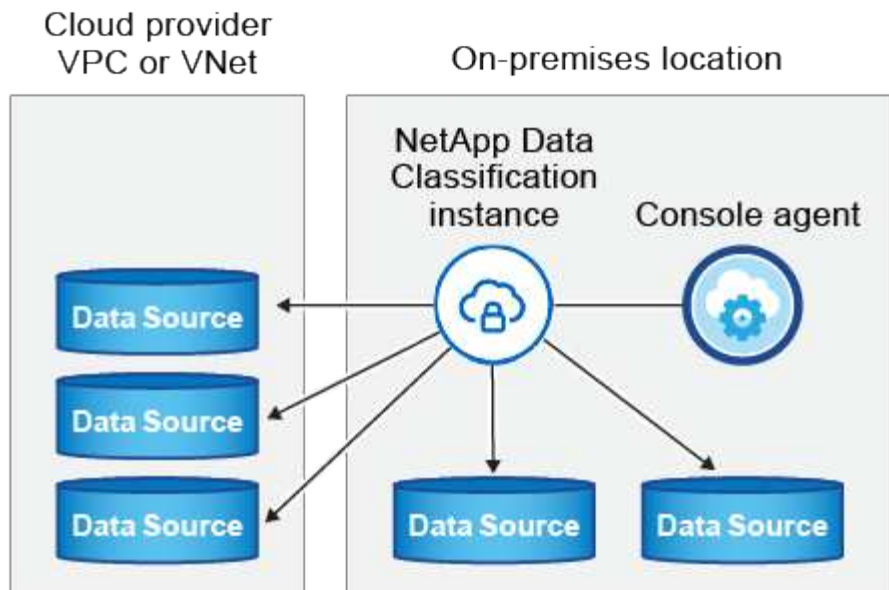
コンソール エージェント、データ分類、Active Directory、およびデータ ソース間の通信に必要なすべてのポートが開いていることを確認する必要があります。

接続タイプ	ポート	説明
コンソールエージェント <> データ分類	8080 (TCP)、443 (TCP)、 および 80。9000	コンソール エージェントのファイアウォールまたはルーティング ルールでは、ポート 443 経由のデータ分類インスタンスとの間の受信トラフィックと送信トラフィックを許可する必要があります。コンソールでインストールの進行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。Linux ホストでファイアウォールが使用されている場合、Ubuntu サーバー内の内部プロセスにはポート 9000 が必要です。
コンソールエージェント <> ONTAP クラスタ (NAS)	443 (TCP)	コンソールは、HTTPS を使用して ONTAP クラスタを検出します。カスタム ファイアウォール ポリシーを使用する場合は、次の要件を満たす必要があります。 • コンソール エージェント ホストは、ポート 443 経由の送信 HTTPS アクセスを許可する必要があります。コンソール エージェントがクラウド内にある場合、すべての送信通信は事前定義されたファイアウォールまたはルーティング ルールによって許可されます。 • ONTAP クラスタは、ポート 443 経由の着信 HTTPS アクセスを許可する必要があります。デフォルトの「mgmt」ファイアウォール ポリシーでは、すべての IP アドレスからの受信 HTTPS アクセスが許可されます。このデフォルト ポリシーを変更した場合、または独自のファイアウォール ポリシーを作成した場合は、HTTPS プロトコルをそのポリシーに関連付け、コンソール エージェント ホストからのアクセスを有効にする必要があります。

接続タイプ	ポート	説明
データ分類 <> ONTAP クラスタ	• NFSの場合 - 111 (TCP\UDP) および 2049 (TCP\UDP) • CIFSの場合 - 139 (TCP\UDP) および 445 (TCP\UDP)	データ分類には、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のファイアウォールまたはルーティング ルールは、データ分類インスタンスからの受信接続を許可する必要があります。 次のポートがデータ分類インスタンスに対して開いていることを確認します。 • NFSの場合 - 111と2049 • CIFSの場合 - 139および445 NFS ボリュームのエクスポート ポリシーでは、データ分類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。
データ分類 <> Active Directory	389 (TCP & UDP)、636 (TCP)、3268 (TCP)、および 3269 (TCP)	社内のユーザー用に Active Directory がすでに設定されている必要があります。さらに、データ分類では、CIFS ボリュームをスキャンするために Active Directory 資格情報が必要です。 Active Directory の情報が必要です: • DNSサーバーのIPアドレス、または複数のIPアドレス • サーバーのユーザー名とパスワード • ドメイン名（アクティブディレクトリ名） • セキュアLDAP（LDAPS）を使用しているかどうか • LDAP サーバー ポート (通常、LDAP の場合は 389、セキュア LDAP の場合は 636)

Linuxホストにデータ分類をインストールする

通常の構成では、ソフトウェアを単一のホスト システムにインストールします。[ここでその手順をご覧ください](#)。



見るLinuxホストシステムの準備そして前提条件の確認データ分類を展開する前に、要件の完全なリストを確認してください。

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



現在、データ分類では、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、S3 バケット、Azure NetApp Files、または FSx for ONTAP をスキャンできません。このような場合には、クラウドに別のコンソールエージェントとデータ分類のインスタンスを展開し、"[コネクタ間の切り替え](#)"さまざまなデータ ソース用。

一般的な構成の単一ホストインストール

単一のオンプレミス ホストにデータ分類ソフトウェアをインストールする場合は、要件を確認し、次の手順に従ってください。

["このビデオを見る"](#)Data Classification のインストール方法を確認します。

Data Classification をインストールすると、すべてのインストール アクティビティがログに記録されることに注意してください。インストール中に問題が発生した場合は、インストール監査ログの内容を表示できます。それは、`/opt/netapp/install_logs/`。

開始する前に

- Linuxシステムが[ホスト要件](#)。
- システムに 2 つの前提条件ソフトウェア パッケージ (Docker Engine または Podman、および Python 3) がインストールされていることを確認します。
- Linux システムでルート権限を持っていることを確認してください。
- インターネットへのアクセスにプロキシを使用している場合:
 - プロキシ サーバー情報 (IP アドレスまたはホスト名、接続ポート、接続スキーム: https または http、ユーザー名とパスワード) が必要になります。
 - プロキシが TLS インターセプションを実行している場合は、TLS CA 証明書が保存されている Data

Classification Linux システム上のパスを知っておく必要があります。

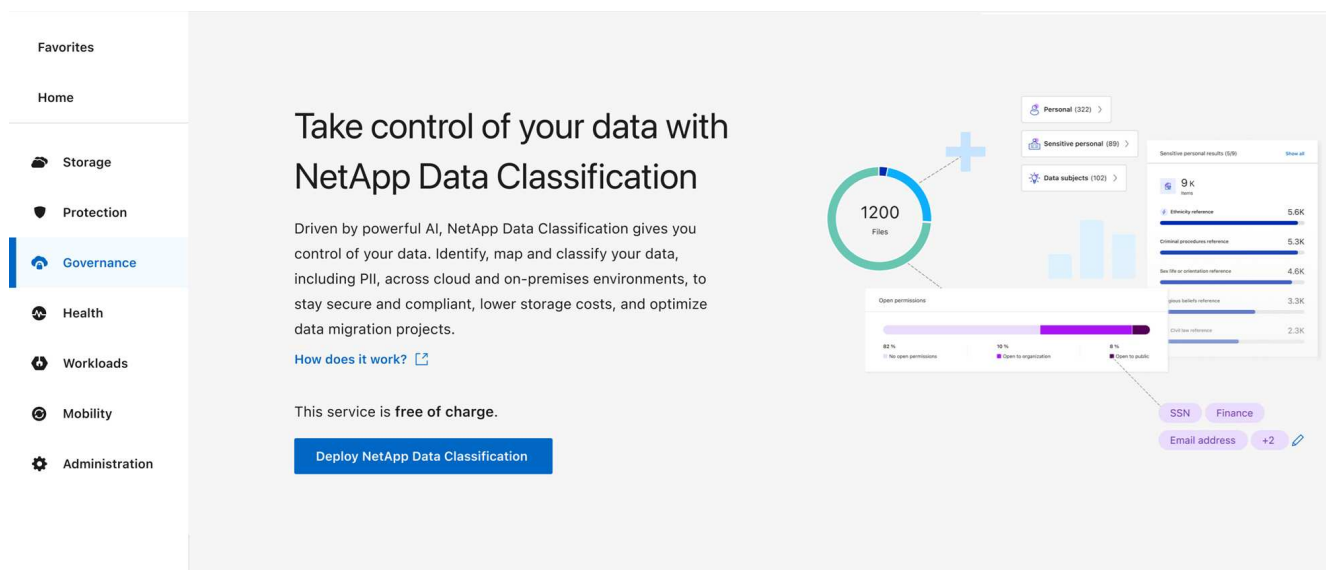
- プロキシは非透過である必要があります。データ分類は現在、透過プロキシをサポートしていません。
- ユーザーはローカル ユーザーである必要があります。ドメイン ユーザーはサポートされていません。
- オフライン環境が要件を満たしていることを確認する[権限と接続性](#)。

手順

1. データ分類ソフトウェアを以下からダウンロードしてください。"[NetAppサポート サイト](#)"。選択するファイルの名前は **DATASENSE-INSTALLER-<version>.tar.gz** です。
2. 使用する予定のLinuxホストにインストーラファイルをコピーします（`scp`または他の方法）。
3. ホスト マシン上でインストーラ ファイルを解凍します。例:

```
tar -xzf DATASENSE-INSTALLER-V1.25.0.tar.gz
```

4. コンソールで、***ガバナンス > 分類***を選択します。
5. ***オンプレミスまたはクラウドでの分類の展開***を選択します。



6. クラウドで準備したインスタンスにデータ分類をインストールするか、オンプレミスで準備したインスタンスにデータ分類をインストールするかに応じて、適切な デプロイ オプションを選択してデータ分類のインストールを開始します。
7. オンプレミスでのデータ分類の展開 ダイアログが表示されます。提供されたコマンドをコピーします（例：`sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`）を作成し、テキスト ファイルに貼り付けて、後で使用することもできます。次に、[閉じる]を選択してダイアログを閉じます。
8. ホスト マシンで、コピーしたコマンドを入力して一連のプロンプトに従うか、必要なすべてのパラメーターを含む完全なコマンドをコマンド ライン引数として指定することもできます。

インストーラーは、インストールを正常に実行するためにシステムとネットワークの要件が満たされているかどうかを確認するための事前チェックを実行することに注意してください。"[このビデオを見る](#)"事前チェックのメッセージとその意味を理解する。

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。
a. 手順 7 からコピーしたコマンドを貼り付けます。 <pre>sudo ./install.sh -a <account_id> -c <client_id> -t <user_token></pre> クラウドインスタンス（オンプレミスではない）にインストールする場合は、<code>--manual -cloud-install <cloud_provider></code>。 b. コンソール エージェント システムからアクセスできるように、データ分類ホスト マシンの IP アドレスまたはホスト名を入力します。 c. データ分類システムからアクセスできるように、コンソール エージェント 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。 d. プロンプトに従ってプロキシの詳細を入力します。コンソール エージェントがすでにプロキシを使用している場合は、データ分類はコンソール エージェントが使用するプロキシを自動的に使用するため、ここでこの情報を再度入力する必要はありません。	あるいは、必要なホストとプロキシの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。 <pre>sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --manual-cloud-install <cloud_provider> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy -user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir></pre>

変数値:

- `account_id` = NetApp アカウント ID
- `client_id` = コンソール エージェントのクライアント ID（クライアント ID に「clients」というサフィックスがない場合は追加します）
- `user_token` = JWT ユーザー アクセストークン
- `ds_host` = データ分類 Linux システムの IP アドレスまたはホスト名。
- `cm_host` = コンソール エージェント システムの IP アドレスまたはホスト名。
- `cloud_provider` = クラウドインスタンスにインストールする場合は、クラウドプロバイダーに応じて「AWS」、「Azure」、または「Gcp」を入力します。
- `proxy_host` = ホストがプロキシ サーバーの背後にある場合のプロキシ サーバーの IP またはホスト名。
- `proxy_port` = プロキシ サーバーに接続するためのポート (デフォルトは 80)。
- `proxy_scheme` = 接続スキーム: https または http (デフォルトは http)。
- `proxy_user` = 基本認証が必要な場合に、プロキシ サーバーに接続するための認証済みユーザー。ユーザーはローカル ユーザーである必要があります。ドメイン ユーザーはサポートされていません。
- `proxy_password` = 指定したユーザー名のパスワード。
- `ca_cert_dir` = 追加の TLS CA 証明書バンドルを含むデータ分類 Linux システム上のパス。プロキシが TLS インターセプションを実行している場合にのみ必要です。

結果

Data Classification インストーラーは、パッケージをインストールし、インストールを登録し、Data Classification 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 マシンとコンソール エージェント インスタンスの間にポート 8080 経由の接続がある場合は、コンソールの [データ分類] タブにインストールの進行状況が表示されます。

次は何？

構成ページから、スキャンするデータ ソースを選択できます。

インターネットにアクセスできない Linux ホストにNetApp Data Classificationをインストールする

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 Linux ホストにNetApp Data Classification をインストールすることを、プライベート モード と呼びます。インストール スクリプトを使用するこのタイプのインストールでは、NetApp ConsoleSaaS レイヤーに接続できません。



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

LinuxホストがNetApp Data Classificationをインストールする準備ができていることを確認します

Linux ホストにNetApp Data Classification を手動でインストールする前に、オプションでホスト上でスクリプトを実行し、Data Classification をインストールするための前提条件がすべて満たされていることを確認します。このスクリプトは、ネットワーク内の Linux ホストまたはクラウド内の Linux ホストで実行できます。ホストはインターネットに接続することも、インターネットにアクセスできないサイト (ダーク サイト) に存在することもできます。

データ分類インストール スクリプトには、環境が要件を満たしていることを確認するためのテスト スクリプトが含まれています。インストール スクリプトを実行する前に、このスクリプトを個別に実行して、Linux ホストの準備状況を確認できます。

はじめに

以下のタスクを実行します。

- 必要に応じて、コンソール エージェントがまだインストールされていない場合はインストールします。コンソール エージェントがインストールされていなくてもテスト スクリプトを実行できますが、スクリプトはコンソール エージェントとデータ分類ホスト マシン間の接続をチェックするため、コンソール エージェントを使用することをお勧めします。
- ホスト マシンを準備し、すべての要件を満たしていることを確認します。

- データ分類ホスト マシンからのアウトバウンド インターネット アクセスを有効にします。
- すべてのシステムで必要なすべてのポートが有効になっていることを確認します。
- 前提条件テスト スクリプトをダウンロードして実行します。

コンソールエージェントを作成する

Data Classification をインストールして使用する前に、コンソール エージェントが必要です。ただし、コンソール エージェントなしで前提条件スクリプトを実行することは可能です。

あなたはできる ["オンプレミスにコンソールエージェントをインストールする"](#) ネットワーク内の Linux ホストまたはクラウド内の Linux ホスト上。コンソール エージェントがオンプレミスにインストールされている場合は、データ分類をオンプレミスにインストールすることもできます。

クラウド プロバイダー環境でコンソール エージェントを作成するには、以下を参照してください。

- ["AWSでコンソールエージェントを作成する"](#)
- ["Azureでコンソールエージェントを作成する"](#)
- ["GCP でコンソール エージェントを作成する"](#)

前提条件スクリプトを実行するときは、コンソール エージェント システムの IP アドレスまたはホスト名が必要です。オンプレミスでコンソール エージェントをインストールした場合は、この情報が得られます。コンソール エージェントがクラウドに展開されている場合は、コンソールからこの情報を確認できます。ヘルプアイコンを選択してから [サポート] を選択し、[エージェントと監査] セクションで [エージェントに移動] を選択します。

ホストの要件を確認する

データ分類ソフトウェアは、特定のオペレーティング システム要件、RAM 要件、およびソフトウェア要件を満たすホスト上で実行する必要があります。

- データ分類は専用ホスト上で実行する必要があります。ホストは、他のアプリケーションやウイルス対策などのサードパーティ製ソフトウェアと共有することはできません。
- データ分類でスキャンする予定のデータ セットに合わせてサイズを選択します。

システムサイズ	CPU	RAM (スワップメモリを無効にする必要があります)	ディスク
特大	CPU×32	128GBのRAM	• / に 1 TiB SSD、または /opt に 100 GiB 利用可能 • /var/lib/docker で 895 GiB が利用可能 • /tmp に 5 GiB • Podman の場合、/var/tmp に 30 GB

システムサイズ	CPU	RAM (スワップメモリを無効にする必要があります)	ディスク
大きい	CPU×16	64GBのRAM	• / に 500 GiB SSD、または /opt に 100 GiB 利用可能 • /var/lib/docker または Podman /var/lib/containers で 400 GiB が利用可能 • /tmp に 5 GiB • Podman の場合、/var/tmp に 30 GB

- データ分類インストール用にクラウドにコンピューティング インスタンスをデプロイする場合は、上記の「大規模」システム要件を満たすシステムを使用することをお勧めします。
 - **Amazon Elastic Compute Cloud (Amazon EC2)** インスタンスタイプ: 「m6i.4xlarge」。["その他のAWSインスタンスタイプを見る"](#)。
 - **Azure VM** サイズ: 「Standard_D16s_v3」。["その他のAzureインスタンスタイプを見る"](#)。
 - **GCP** マシンタイプ: 「n2-standard-16」。["その他の GCP インスタンスタイプを見る"](#)。
- **UNIX** フォルダ権限: 次の最低限の UNIX 権限が必要です。

フォルダ	最小限の権限
/tmp	rwXrwxrwt
/opt	rwXr-Xr-X
/var/lib/docker	rwX-----
/usr/lib/systemd/システム	rwXr-Xr-X

- オペレーティング・システム：
 - 次のオペレーティング システムでは、Docker コンテナ エンジンを使用する必要があります。
 - Red Hat Enterprise Linux バージョン 7.8 および 7.9
 - Ubuntu 22.04 (データ分類バージョン 1.23 以上が必要)
 - Ubuntu 24.04 (データ分類バージョン 1.23 以上が必要)
 - 次のオペレーティング システムでは、Podman コンテナ エンジンを使用する必要があり、データ分類バージョン 1.30 以上が必要です。
 - Red Hat Enterprise Linux バージョン 8.8、8.10、9.0、9.1、9.2、9.3、9.4、9.5、および 9.6。
 - ホスト システムで Advanced Vector Extensions (AVX2) を有効にする必要があります。
- **Red Hat** サブスクリプション管理: ホストは Red Hat サブスクリプション管理に登録されている必要があります。登録されていない場合、システムはリポジトリにアクセスできず、インストール中に必要なサードパーティ製ソフトウェアを更新できません。
- 追加ソフトウェア: Data Classification をインストールする前に、ホストに次のソフトウェアをインストールする必要があります。

- 使用している OS に応じて、次のいずれかのコンテナ エンジンをインストールする必要があります。
 - Docker Engine バージョン 19.3.1 以上。 ["インストール手順を見る"](#)。
 - Podman バージョン 4 以上。Podmanをインストールするには、次のように入力します。(sudo yum install podman netavark -y)。
- Python バージョン 3.6 以上。 ["インストール手順を見る"](#)。
 - **NTP** に関する考慮事項: NetApp、データ分類システムをネットワーク タイム プロトコル (NTP) サービスを使用するように構成することを推奨しています。データ分類システムとコンソール エージェント システムの間で時刻を同期する必要があります。
- **Firewalld**の考慮事項: 使用を計画している場合 firewalld、データ分類をインストールする前に有効にすることをお勧めします。設定するには次のコマンドを実行します `firewalld` データ分類と互換性があるように:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

追加のデータ分類ホストをスキャナー ノードとして使用することを計画している場合 (分散モデル)、この時点で次のルールをプライマリ システムに追加します。

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

有効化または更新するたびにDockerまたはPodmanを再起動する必要があることに注意してください。
`firewalld` 設定。

データ分類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

データ分類には、アウトバウンドのインターネット アクセスが必要です。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 サーバーを使用している場合は、データ分類インスタンスに次のエンドポイントに接続するための送信インターネット アクセスがあることを確認してください。



このセクションは、インターネットに接続できないサイトにインストールされたホスト システムでは必要ありません。

エンドポイント	目的
https://api.console.netapp.com	NetAppアカウントを含むコンソール サービスとの通信。
https://netapp-cloud-account.auth0.com https://auth0.com	集中ユーザー認証のためのコンソール Web サイトとの通信。

エンドポイント	目的
https://support.compliance.api.console.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を提供し、ログとメトリックを送信します。
https://support.compliance.api.console.netapp.com/	NetApp 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	docker インストールの前提条件パッケージを提供します。
http://packages.ubuntu.com/ http://archive.ubuntu.com	Ubuntu インストールの前提条件となるパッケージを提供します。

必要なポートがすべて有効になっていることを確認します

コンソール エージェント、データ分類、Active Directory、およびデータ ソース間の通信に必要なすべてのポートが開いていることを確認する必要があります。

接続タイプ	ポート	説明
コンソールエージェント <> データ分類	8080 (TCP)、443 (TCP)、 および 80。9000	コンソール エージェントのファイアウォールまたはルーティング ルールでは、ポート 443 経由のデータ分類インスタンスとの間の受信トラフィックと送信トラフィックを許可する必要があります。コンソールでインストールの進行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。Linux ホストでファイアウォールが使用されている場合、Ubuntu サーバー内の内部プロセスにはポート 9000 が必要です。
コンソールエージェント <> ONTAP クラスタ (NAS)	443 (TCP)	コンソールは、HTTPS を使用して ONTAP クラスタを検出します。カスタム ファイアウォール ポリシーを使用する場合、コンソール エージェント ホストはポート 443 経由の送信 HTTPS アクセスを許可する必要があります。コンソール エージェントがクラウド内にある場合、すべての送信通信は事前定義されたファイアウォールまたはルーティング ルールによって許可されます。

データ分類の前提条件スクリプトを実行する

データ分類の前提条件スクリプトを実行するには、次の手順に従います。

["このビデオを見る"](#)前提条件スクリプトを実行して結果を解釈する方法を確認します。

開始する前に

- Linux システムが [ホスト要件](#)。
- システムに 2 つの前提条件ソフトウェア パッケージ (Docker Engine または Podman、および Python 3)

がインストールされていることを確認します。

- Linux システムでルート権限を持っていることを確認してください。

手順

1. データ分類の前提条件スクリプトを以下からダウンロードします。"[NetAppサポート サイト](#)"。選択するファイルの名前は **standalone-pre-requisite-tester-<version>** です。
2. 使用する予定のLinuxホストにファイルをコピーします（`scp`または他の方法）。
3. スクリプトを実行するための権限を割り当てます。

```
chmod +x standalone-pre-requisite-tester-v1.25.0
```

4. 次のコマンドを使用してスクリプトを実行します。

```
./standalone-pre-requisite-tester-v1.25.0 <--darksite>
```

インターネットにアクセスできないホストでスクリプトを実行する場合にのみ、オプション "--darksite" を追加します。ホストがインターネットに接続されていない場合、特定の前提条件テストはスキップされます。

5. スクリプトは、データ分類ホスト マシンの IP アドレスの入力を求めます。
 - IP アドレスまたはホスト名を入力します。
6. スクリプトは、コンソール エージェントがインストールされているかどうかを尋ねます。
 - コンソール エージェントがインストールされていない場合は、**N** と入力します。
 - コンソール エージェントがインストールされている場合は、「**Y**」と入力します。次に、テスト スクリプトがこの接続をテストできるように、コンソール エージェントの IP アドレスまたはホスト名を入力します。
7. スクリプトはシステム上でさまざまなテストを実行し、進行中に結果を表示します。終了すると、セッションのログを次のファイルに書き込みます。prerequisites-test-<timestamp>.log`ディレクトリ内` /opt/netapp/install_logs。

結果

すべての前提条件テストが正常に実行された場合、準備ができたらホストに Data Classification をインストールできます。

問題が発見された場合は、修正が「推奨」または「必須」として分類されます。推奨される問題は通常、データ分類のスキャンと分類のタスクの実行速度を低下させる項目です。これらの項目は修正する必要はありませんが、対処することをお勧めします。

「必須」の問題がある場合は、問題を修正して、前提条件テスト スクリプトを再度実行する必要があります。

著作権に関する情報

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

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

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

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

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

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

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

商標に関する情報

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