



データ分類の管理

NetApp Data Classification

NetApp
February 11, 2026

目次

データ分類の管理	1
NetApp Data Classification スキャンから特定のディレクトリを除外する	1
サポートされているデータソース	1
スキャンから除外するディレクトリを定義する	1
例	2
フォルダ名の特殊文字をエスケープする	3
現在の除外リストを表示する	4
NetApp Data Classification で組織に公開されている追加のグループIDを定義します。	4
グループIDに「組織に公開」権限を追加する	4
現在のグループIDのリストを表示する	5
NetApp Data Classification で古いデータ定義をカスタマイズする	5
NetApp Data Classification からデータソースを削除する	6
システムのスキャンを無効にする	6
データ分類からデータベースを削除する	6
データ分類からファイル共有のグループを削除する	7
NetApp Data Classification をアンインストールする	7
クラウドプロバイダーからデータ分類をアンインストールする	7
オンプレミス展開からデータ分類をアンインストールする	8

データ分類の管理

NetApp Data Classification スキャンから特定のディレクトリを除外する

NetApp Data Classification で特定のディレクトリをスキャンから除外する場合は、これらのディレクトリ名を構成ファイルに追加できます。この変更を適用すると、データ分類エンジンはそれらのディレクトリをスキャンから除外します。



デフォルトでは、データ分類スキャンでは、ボリューム内のソースと同一のボリューム スナップショット データが除外されます。

サポートされているデータソース

データ分類スキャンから特定のディレクトリを除外することは、次のデータ ソースの NFS および CIFS 共有でサポートされています。

- オンプレミスのONTAP
- Cloud Volumes ONTAP
- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- 一般的なファイル共有

スキャンから除外するディレクトリを定義する

ディレクトリを分類スキャンから除外する前に、データ分類システムにログインして、構成ファイルを編集し、スクリプトを実行する必要があります。方法を見る["データ分類システムにログインする"](#)Linux マシンにソフトウェアを手動でインストールしたか、インスタンスをクラウドに展開したかによって異なります。

考慮事項

- データ分類システムごとに最大 50 個のディレクトリ パスを除外できます。
- ディレクトリ パスを除外すると、スキャン時間に影響する可能性があります。

手順

1. データ分類システムで、「/opt/netapp/config/custom_configuration」に移動し、ファイルを開きます。
data_provider.yaml。
2. 「exclude:」行の下に「data_providers」セクションに、除外するディレクトリ パスを入力します。例えば：

```
exclude:
- "folder1"
- "folder2"
```

このファイル内の他の部分を変更しないでください。

3. ファイルへの変更を保存します。
4. 「/opt/netapp/Datasense/tools/customer_configuration/data_providers」に移動し、次のスクリプトを実行します。

```
update_data_providers_from_config_file.sh
```

+ このコマンドは、スキャンから除外するディレクトリを分類エンジンにコミットします。

結果

以降のすべてのデータスキャンでは、指定されたディレクトリのスキャンは除外されます。

同じ手順を使用して、除外リストの項目を追加、編集、または削除できます。スクリプトを実行して変更をコミットすると、修正された除外リストが更新されます。

例

構成1:

名前のどこかに「folder1」が含まれるすべてのフォルダーは、すべてのデータソースから除外されます。

```
data_providers:
  exclude:
    - "folder1"
```

除外されるパスの予想される結果:

- /CVO1/フォルダ1
- /CVO1/フォルダ1名
- /CVO1/フォルダ10
- /CVO1/*フォルダ1
- /CVO1/+フォルダ1名
- /CVO1/notfolder10
- /CVO22/フォルダ1
- /CVO22/フォルダ1名
- /CVO22/フォルダ10

除外されないパスの例:

- /CVO1/*フォルダ
- /CVO1/フォルダ名
- /CVO22/*フォルダ20

構成2:

名前の先頭にのみ「*folder1」が含まれるすべてのフォルダーが除外されます。

```
data_providers:
  exclude:
    - "\\*folder1"
```

除外されるパスの予想される結果:

- /CVO/*フォルダ1
- /CVO/*フォルダ1名
- /CVO/*フォルダ10

除外されないパスの例:

- /CVO/フォルダ1
- /CVO/フォルダ1名
- /CVO/not*folder10

構成3:

データ ソース「CVO22」内の、名前のどこかに「folder1」が含まれるすべてのフォルダーが除外されます。

```
data_providers:
  exclude:
    - "CVO22/folder1"
```

除外されるパスの予想される結果:

- /CVO22/フォルダ1
- /CVO22/フォルダ1名
- /CVO22/フォルダ10

除外されないパスの例:

- /CVO1/フォルダ1
- /CVO1/フォルダ1名
- /CVO1/フォルダ10

フォルダ名の特殊文字をエスケープする

フォルダー名に次のいずれかの特殊文字が含まれており、そのフォルダー内のデータをスキャン対象から除外する場合は、フォルダー名の前にエスケープシーケンス \\ を使用する必要があります。

```
., +, *, ?, ^, $, (, ), [, ], {, }, |
```

例えば:

ソース内のパス: /project/*not_to_scan

除外ファイルの構文: "*not_to_scan"

現在の除外リストを表示する

内容は `data_provider.yaml` 設定ファイルは、実行後に実際にコミットされたものと異なる可能性があります。`update_data_providers_from_config_file.sh` スクリプト。データ分類スキャンから除外したディレクトリの現在のリストを表示するには、「/opt/netapp/Datasense/tools/customer_configuration/data_providers」から次のコマンドを実行します。

```
get_data_providers_configuration.sh
```

NetApp Data Classificationで組織に公開されている追加のグループIDを定義します。

グループ ID (GID) が NFS ファイル共有内のファイルまたはフォルダーに関連付けられると、そのファイルまたはフォルダーのアクセス許可 (組織に公開されているかどうかなど) が定義されます。一部の GID が最初に「組織に公開」権限レベルで設定されていない場合は、その権限を GID に追加して、その GID が添付されているすべてのファイルとフォルダーが「組織に公開」されているとみなされるようにすることができます。

この変更を行った後、NetApp Data Classificationによってファイルとフォルダが再スキャンされると、これらのグループ ID が添付されているすべてのファイルとフォルダの [調査の詳細] ページにこの権限が表示され、ファイル権限を表示するレポートにも表示されます。

この機能を有効にするには、データ分類システムにログインして、構成ファイルを編集し、スクリプトを実行する必要があります。方法を見る["データ分類システムにログインする"](#)Linux マシンにソフトウェアを手動でインストールしたか、インスタンスをクラウドに展開したかによって異なります。

グループIDに「組織に公開」権限を追加する

このタスクを開始する前に、グループ ID 番号 (GID) が必要です。

手順

1. データ分類システムで、「/opt/netapp/config/custom_configuration」に移動し、ファイルを開きます。
data_provider.yaml。
2. 「organization_group_ids: []」の行にグループIDを追加します。例えば：

```
organization_group_ids: [1014, 1015, 21, 2021, 1013, 2020, 1018, 1019]
```

このファイルの他の部分は変更しないでください。

3. ファイルへの変更を保存します。
4. 「/opt/netapp/Datasense/tools/customer_configuration/data_providers」に移動し、次のスクリプトを実行します。

```
update_data_providers_from_config_file.sh
```

このコマンドは、変更されたグループ ID 権限を分類エンジンにコミットします。

結果

データのその後のすべてのスキャンでは、これらのグループ ID が添付されているファイルまたはフォルダーが「組織に公開」として識別されます。

同じ手順を使用して、グループ ID のリストを編集し、過去に追加したグループ ID を削除できます。スクリプトを実行して変更をコミットすると、修正されたグループ ID のリストが更新されます。

現在のグループIDのリストを表示する

内容は `data_provider.yaml` 設定ファイルは、実行後に実際にコミットされたものと異なる可能性があります。`update_data_providers_from_config_file.sh` スクリプト。データ分類に追加したグループ ID の現在のリストを表示するには、「/opt/netapp/Datasense/tools/customer_configuration/data_providers」から次のコマンドを実行します。

```
get_data_providers_configuration.sh
```

NetApp Data Classificationで古いデータ定義をカスタマイズする

NetApp Data Classification は古いデータを識別し、節約の機会とガバナンスのリスクを特定するのに役立ちます。古いデータの定義は組織のコンテキストによって異なる可能性があるため、データ分類で古いデータを定義する方法をカスタマイズできます。

古いデータは、最終アクセス または 最終変更 された日時に基づいて定義できます。選択できる期間は 6 か月前から 10 年前までです。

デフォルトでは、データが最後に変更されてから 3 年前であれば古いデータとみなされます。

古いデータを定義する

1. ランサムウェア耐性で、[構成] を選択します。
2. 構成ページで、古いデータ定義 の見出しまでスクロールします。
3. ファイル プロパティ ドロップダウン メニューで、最終アクセス または 最終変更 に基づいて古いデータを定義するかどうかを選択します。
4. 古いデータ定義の期間を選択します。

Scanner Groups

Search

Scanner Group: default

1 Scanner nodes

Host Name	IP	Status	Last Active Time	Error
ip-10-128-0-46.us-west-2.compute.internal		ACTIVE	2025-08-31 08:24	

Activate Slow Scan

Stale data definition

Define how your organization identifies stale data for insights and reporting

File property

Last Modified

Time period

3 Years ago

Save

Current definition: Files **modified** more than **3 years ago** will be marked as stale

Uninstall Data Classification


5. 保存を選択します。

NetApp Data Classificationからデータソースを削除する

必要に応じて、NetApp Data Classification による 1 つ以上のシステム、データベース、またはファイル共有グループのスキャンを停止できます。

システムのスキャンを無効にする

スキャンを非アクティブ化すると、データ分類はシステム上のデータをスキャンしなくなり、インデックス付けされた分析情報がデータ分類インスタンスから削除されます。システム自体のデータは削除されません。


1. _Configuration_ ページから、 システムの行のボタンをクリックし、*データ分類を非アクティブ化*します。



システムを選択するときに、[サービス] パネルからシステムのスキャンを無効にすることもできます。

データ分類からデータベースを削除する


特定のデータベースをスキャンする必要がなくなった場合は、データ分類インターフェースからそのデータベースを削除し、すべてのスキャンを停止できます。

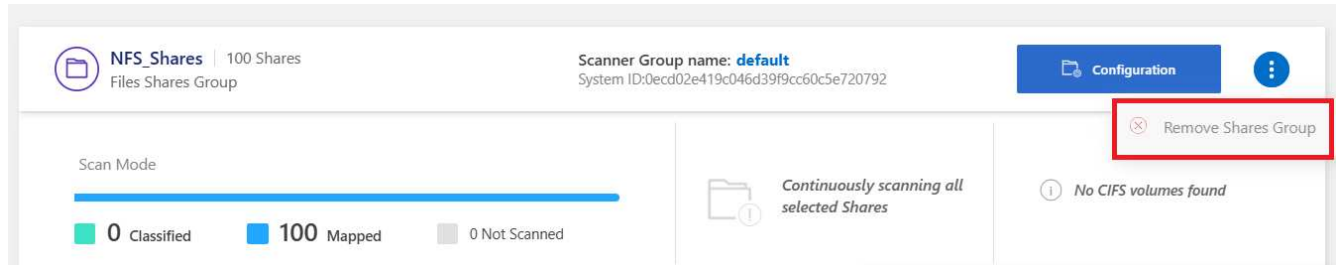
1. _Configuration_ ページから、 データベースの行のボタンをクリックし、*DB サーバーの削除*をクリックします。

データ分類からファイル共有のグループを削除する

ファイル共有グループからユーザー ファイルをスキャンする必要がなくなった場合は、データ分類インターフェースからファイル共有グループを削除し、すべてのスキャンを停止できます。

手順

1. Configuration ページから、 ファイル共有グループの行にあるボタンをクリックし、*ファイル共有グループの削除*をクリックします。



2. 確認ダイアログから*共有グループの削除*を選択します。

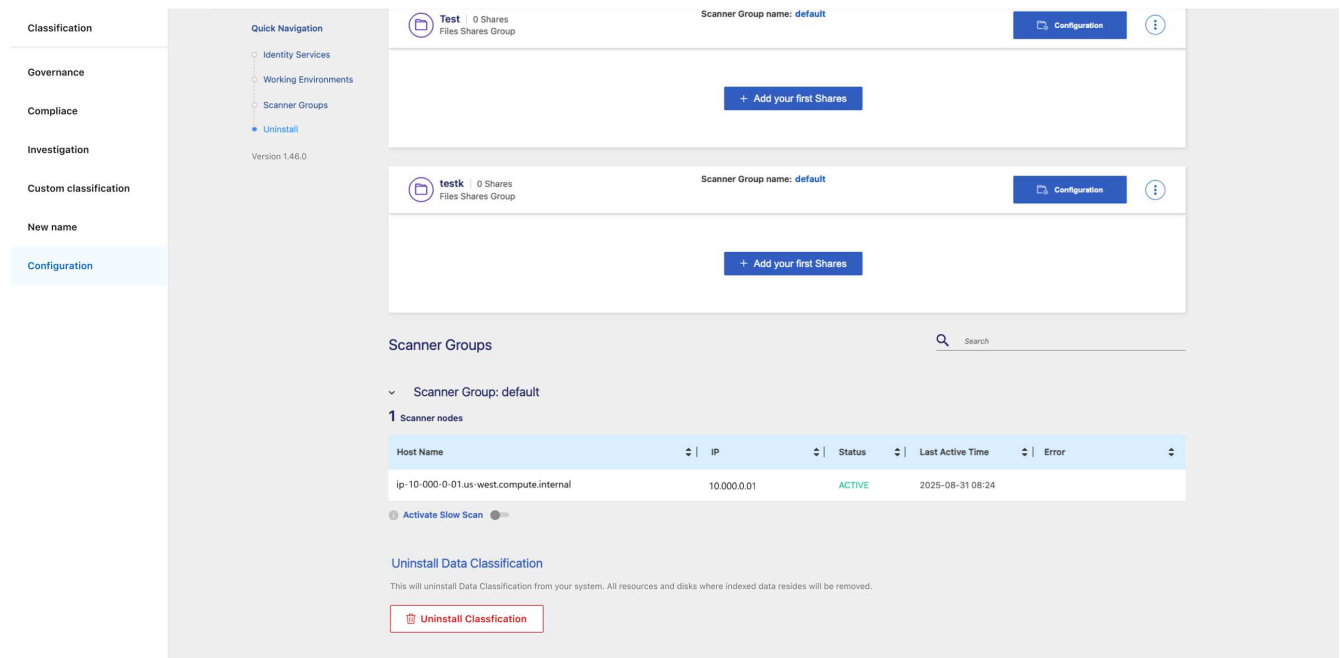
NetApp Data Classificationをアンインストールする

問題のトラブルシューティングを行ったり、ホストからソフトウェアを完全に削除したりするために、NetApp Data Classificationをアンインストールすることができます。インスタンスを削除すると、インデックス付けされたデータが存在する関連ディスクも削除されるため、データ分類によってスキャンされたすべての情報が完全に削除されます。

使用する必要がある手順は、データ分類をクラウドに展開したか、オンプレミス ホストに展開したかによって異なります。

クラウドプロバイダーからデータ分類をアンインストールする

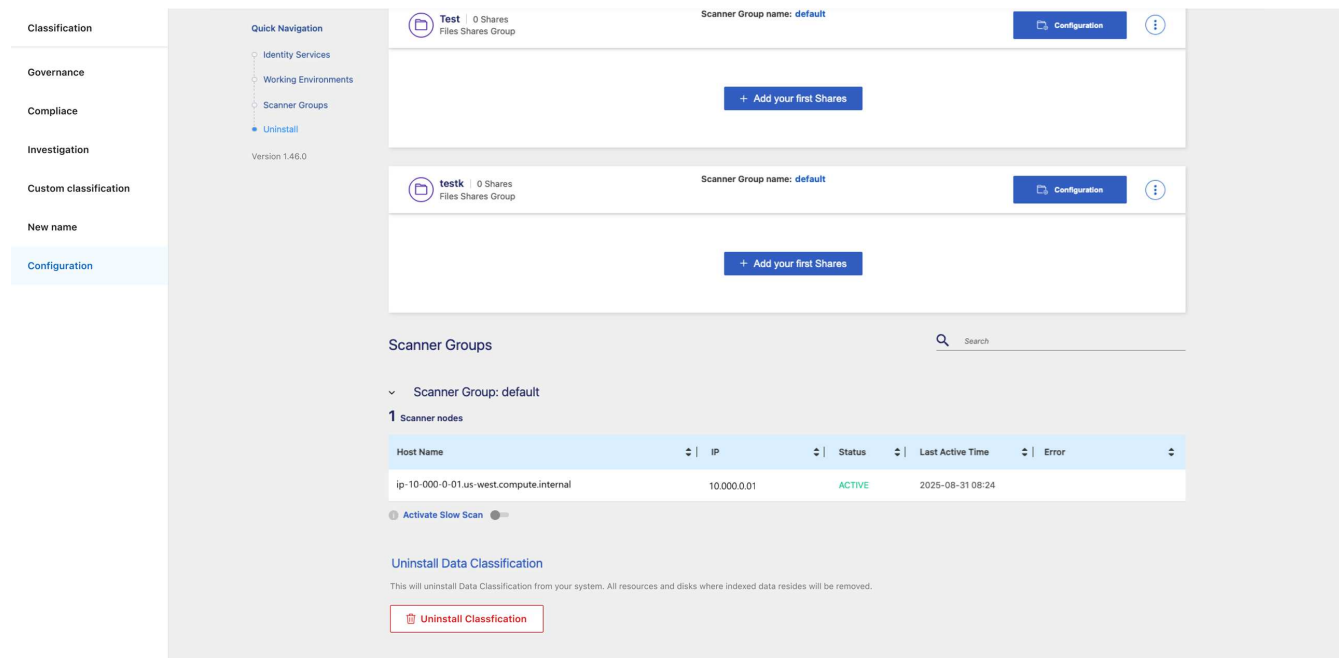
1. データ分類から構成を選択します。
2. 構成ページの下部で、[Uninstall Classification] を選択します。



3. ダイアログで「uninstall」と入力して、コンソール エージェントからデータ分類インスタンスの切断を続行します。確認するにはアンインストールを選択します。
4. [Uninstall Classification] ダイアログで、「uninstall」と入力して、コンソール エージェントからデータ分類インスタンスを切断することを確認し、[Uninstall] を選択します。
5. アンインストール プロセスを完了するには、クラウド プロバイダーのコンソールに移動し、データ分類インスタンスを削除します。インスタンスの名前は *CloudCompliance* となり、生成されたハッシュ (UUID) が連結されます。例: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

オンプレミス展開からデータ分類をアンインストールする

1. データ分類から構成を選択します。
2. 構成ページの下部で、[Uninstall Classification] を選択します。



3. ダイアログで「uninstall」と入力して、コンソール エージェントからデータ分類インスタンスの切断を続行します。確認するにはアンインストールを選択します。
4. ホストからソフトウェアをアンインストールするには、`cleanup.sh` データ分類ホスト マシン上のスクリプト。例:

```
cleanup.sh
```

スクリプトは `/install/light_probe/onprem_installer/cleanup.sh` ディレクトリ。方法を見る["データ分類ホストマシンにログインする"](#)。

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。