



クラウドデータセンスを活用 Cloud Data Sense

NetApp
April 04, 2022

目次

| | |
|--------------------------------------|----|
| クラウドデータセンスを活用 | 1 |
| 組織に保存されているデータに関するガバナンスの詳細を表示する | 1 |
| 組織に保存されているデータのコンプライアンスの詳細を表示する | 5 |
| プライベートデータを整理する | 16 |
| プライベートデータの管理 | 32 |
| Data Fusion を使用して個人データ識別子を追加する | 44 |
| コンプライアンスレポートの表示 | 47 |
| データ主体アクセス要求に応答します | 53 |
| プライベートデータのカテゴリ | 55 |
| Cloud Data Sense からのデータソースの削除 | 61 |

クラウドデータセンスを活用

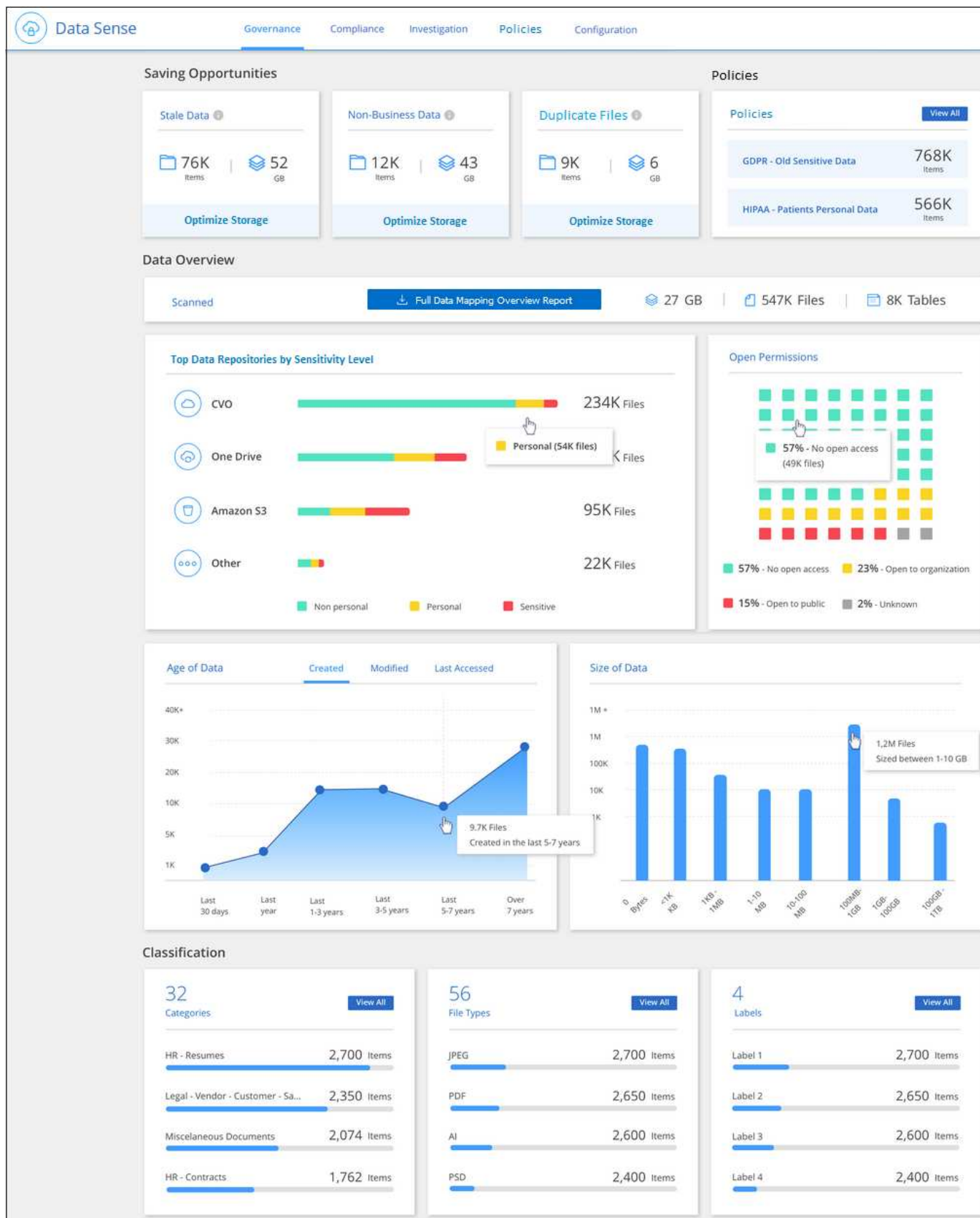
組織に保存されているデータに関するガバナンスの詳細を表示する

組織のストレージリソース上のデータに関連するコストを管理できます。Cloud Data Sense は、古いデータ、ビジネス以外のデータ、重複するファイル、および非常に大きなファイルをシステム内で特定するため、一部のファイルを削除するか、低コストのオブジェクトストレージに階層化するかを判断できます。

また、オンプレミスの場所からクラウドにデータを移行する予定の場合は、移動前にデータのサイズと、機密情報が含まれているデータの有無を確認できます。

Governance ダッシュボード

Governance ダッシュボードには情報が表示されるため、ストレージリソースに保存されているデータの効率性を高め、コストを管理できます。



機会の節約

_Saving Opportunities 領域内の項目を調査して、削除または階層化してより安価なオブジェクトストレージ

にする必要があるデータがないかどうかを確認できます。各項目をクリックすると、[調査] ページにフィルタリングされた結果が表示されます。

- **Stale Data**- 3 年前に最後に変更されたデータ。
- * ビジネス以外のデータ * - カテゴリまたはファイルタイプに基づいて、ビジネスに関連していないと見なされるデータ。これには、次のもの
 - アプリケーションデータ
 - 音声
 - 実行可能ファイル
 - イメージ
 - ログ
 - ビデオ
 - その他（一般的な「その他」カテゴリ）
- * 重複ファイル * - スキャンしているデータソース内の他の場所に複製されているファイル。 ["表示される重複ファイルの種類を確認します"](#)。

検索結果が最も多いポリシーです

_Policy_area でポリシーの名前をクリックすると、その結果が [調査] ページに表示されます。[すべて表示 *] をクリックして、使用可能なすべてのポリシーのリストを表示します。

をクリックします ["こちらをご覧ください"](#) ポリシーの詳細については、を参照してください。

データの概要

スキャンされているすべてのデータの概要。ボタンをクリックして、すべての作業環境とデータソースの使用容量、データの使用年数、データのサイズ、ファイルタイプを含む完全なデータマッピングレポートをダウンロードします。を参照してください ["データマッピングレポート"](#) を参照してください。

データの機密性に基づいて上位のデータリポジトリが表示されます

Top Data Repositories by Sensitivity Level 領域には、最も機密性の高い項目を含む上位 4 つのデータリポジトリ（作業環境およびデータソース）が表示されます。各作業環境の棒グラフは、次のように分割されています。

- 非個人データ
- 個人データ
- 機密性の高い個人データ

各セクションにカーソルを合わせると、各カテゴリの項目の総数を確認できます。

各領域をクリックすると、[調査] ページにフィルタリングされた結果が表示され、詳細を調査できます。

オープンアクセス権のタイプ別に一覧表示されるデータ

Open Permissions 領域には、スキャンされるすべてのファイルに存在する各タイプの権限の割合が表示されます。このチャートには、次の種類の権限が表示されます。

- オープンアクセスがありません
- 組織に開く（Open to Organization）
- [パブリック]に移動します
- 不明なアクセスです

各セクションにカーソルを合わせると、各カテゴリのファイルの総数が表示されます。各領域をクリックすると、[調査] ページにフィルタリングされた結果が表示され、詳細を調査できます。

データの経過時間とデータのサイズのグラフ

_Age および _Size Graphs の項目を調査して、削除または階層化してコストの低いオブジェクトストレージにする必要のあるデータがないかどうかを確認することができます。

グラフの特定のポイントにカーソルを合わせると、そのカテゴリのデータの経過時間やサイズの詳細を確認できます。クリックすると、その年齢またはサイズの範囲でフィルタされたすべてのファイルが表示されます。

- *Age of Data グラフ *- データが作成された時刻、アクセスされた最終時刻、またはデータが変更された最終時刻に基づいてデータを分類します。
- * データサイズグラフ *- サイズに基づいてデータを分類します。

最も識別されているデータ分類

_Classification_area には '最も識別されたリストが表示されます **"カテゴリ"**、**"ファイルの種類"**および **"AIP ラベル"** をスキャンしたデータに保存します。

カテゴリ

カテゴリを使用すると、保有している情報の種類を表示して、データの状況を把握することができます。たとえば、「履歴書」や「従業員契約書」などのカテゴリには機密データを含めることができます。結果を調査すると、従業員契約が安全でない場所に保存されていることがわかります。その後、その問題を修正できます。

を参照してください **"カテゴリ別にファイルを表示します"** を参照してください。

ファイルの種類

ファイルタイプを確認すると、特定のファイルタイプが正しく保存されない可能性があるため、機密データを制御するのに役立ちます。

を参照してください **"ファイルタイプを表示しています"** を参照してください。

AIP ラベル

Azure Information Protection（AIP）に加入している場合は、コンテンツにラベルを適用することで、ドキュメントとファイルを分類して保護できます。ファイルに割り当てられている最も使用されている AIP ラベルを確認すると、ファイルで最も使用されているラベルを確認できます。

を参照してください **"AIP ラベル"** を参照してください。

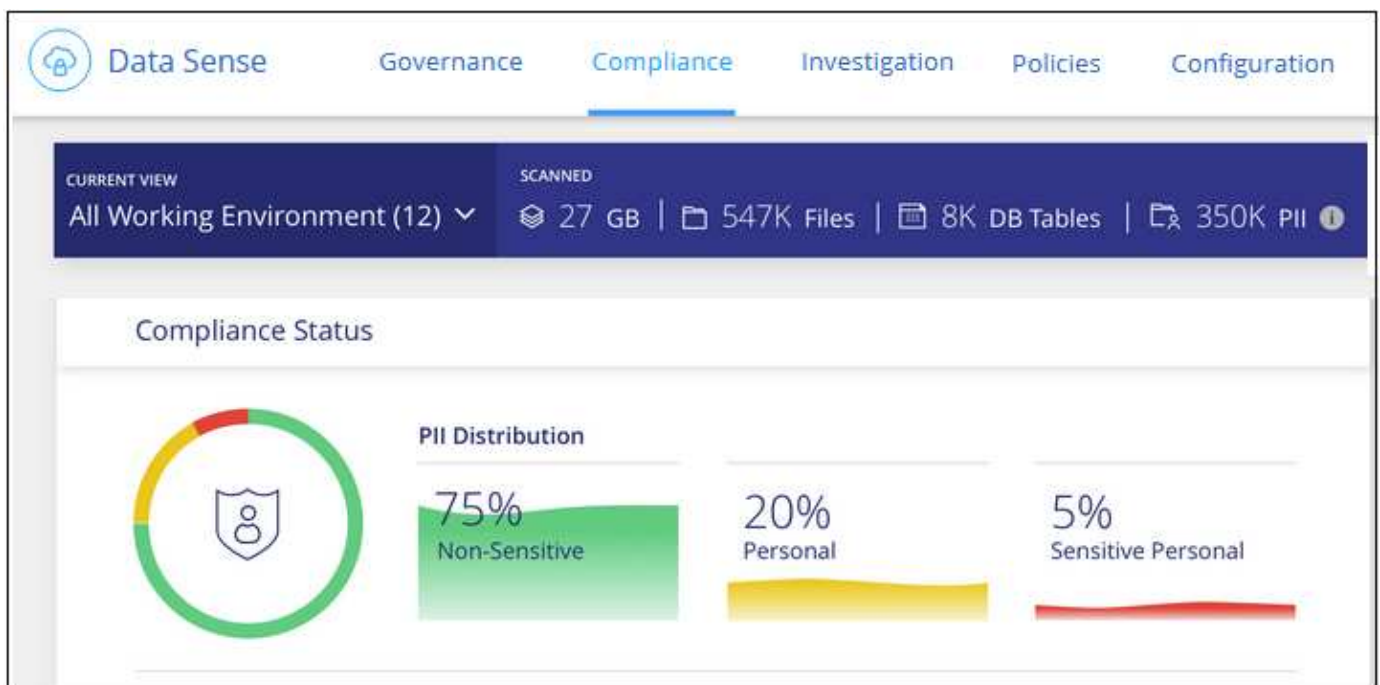
組織に保存されているデータのコンプライアンスの詳細を表示する

組織内の個人データと機密性の高い個人データに関する詳細を表示することで、個人データを管理できます。また、クラウドデータで見つかったカテゴリやファイルタイプを確認することで、データを可視化することもできます。



このセクションで説明する機能は、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。

デフォルトでは、Cloud Data Sense ダッシュボードには、すべての作業環境とデータベースのコンプライアンスデータが表示されます。



一部の作業環境のデータだけを表示する場合は、[それらの作業環境を選択します](#)。

また、[データ調査] ページから結果をフィルタリングして、結果のレポートを CSV ファイルとしてダウンロードすることもできます。を参照してください [\[データ調査\] ページでデータをフィルタリングします](#) を参照してください。

個人データを含むファイルを表示する

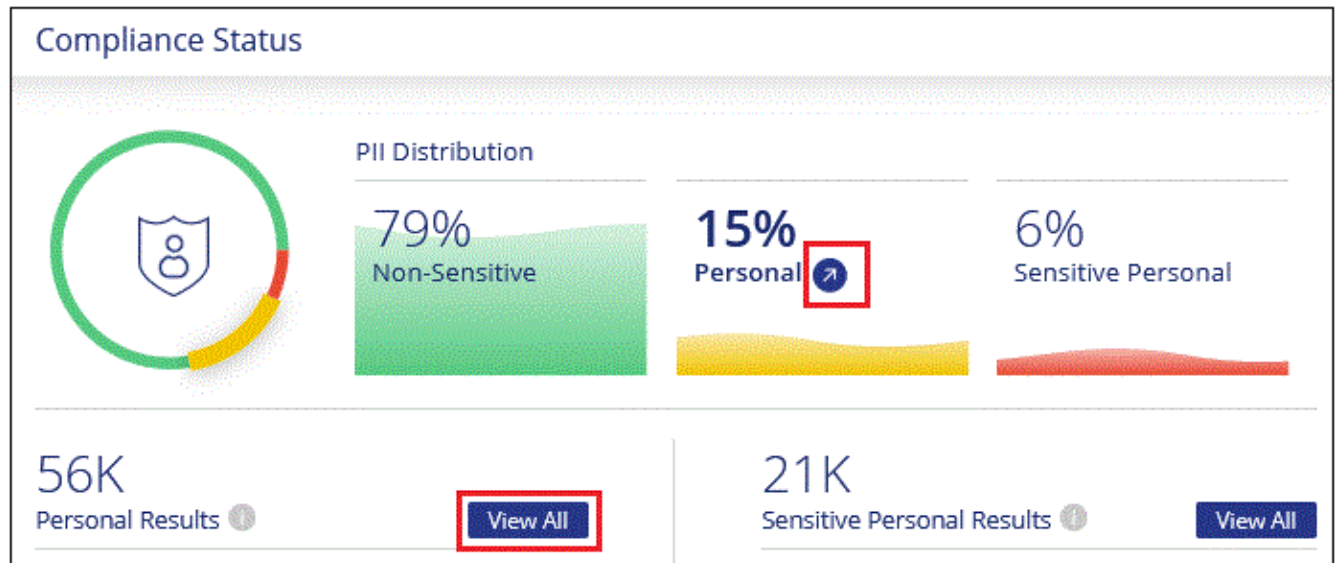
Cloud Data Sense は、データ内の特定の単語、文字列、パターン（Regex）を自動的に識別します。たとえば、個人識別情報（PII）、クレジットカード番号、社会保障番号、銀行口座番号、パスワード、その他。"[すべてのリストを参照してください](#)"。

また、スキャン対象のデータベースサーバを追加した場合、Data Fusion の機能を使用してファイルをスキャンし、データベースから一意の識別子がこれらのファイルまたは他のデータベースのいずれに存在するかを特定できます。を参照してください "[Data Fusion を使用して個人データ識別子を追加する](#)" を参照してください。

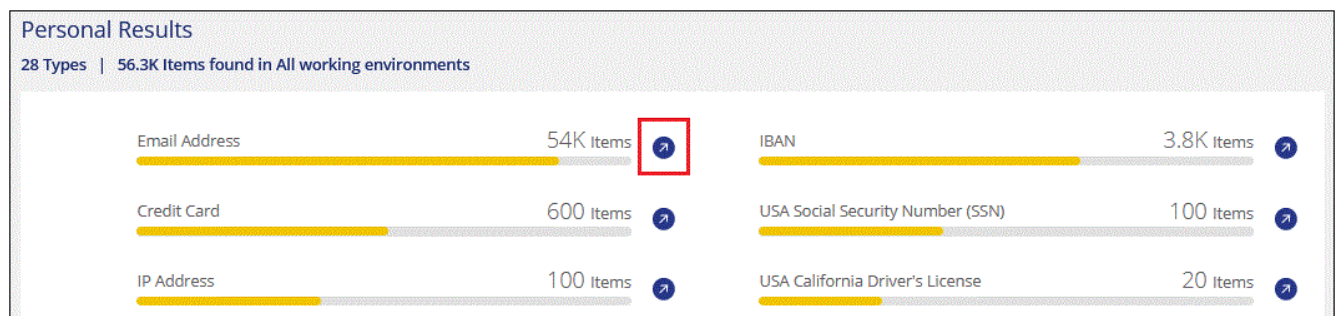
一部のタイプの個人データについては、データセンスは「近接性検証」を使用してその結果を検証します。検証は、見つかった個人データに近接した1つまたは複数の定義済みキーワードを検索することによって行われます。たとえば、データセンスは米国を識別しますソーシャルセキュリティ番号（SSN）は、ITの横に近接語（SSN_or_social_security など）が表示されている場合、SSNとして表示されます。["個人データのテーブル"](#) データセンスがプロキシミティ検証を使用する場合に表示されます

手順

1. Cloud Manager の上部で、* Data Sense * をクリックし、* Compliance * タブをクリックします。
2. すべての個人データの詳細を調査するには、個人データの割合の横にあるアイコンをクリックします。



3. 特定の種類の個人データの詳細を調査するには、[* すべて表示 *] をクリックしてから、特定の種類の個人データの [調査結果 *] アイコン（電子メールアドレスなど）をクリックします。



4. 特定のファイルの検索、ソート、詳細の展開、* 調査結果 * をクリックしてマスクされた情報を表示、またはファイルリストをダウンロードして、データを調査します。



機密性の高い個人データを含むファイルを表示する

クラウドデータセンスは、などのプライバシー規制によって定義された、特別な種類の機密情報を自動的に識別します **"GDPR の第 9、10 記事"**。たとえば、人の健康、民族の起源、性的指向に関する情報などです。 **"すべてのリストを参照してください"**。

Cloud Data Sense は、人工知能（AI）、自然言語処理（NLP）、機械学習（ML）、コグニティブコンピューティング（CC）を使用して、スキャンするコンテンツの意味を理解し、エンティティを抽出してそれに応じて分類します。

たとえば、機密性の高い GDPR データカテゴリの 1 つは民族起源です。データセンスは NLP の能力を持つため、「ジョージ・メキシカン」と書かれた文（GDPR の第 9 条に規定されている機密データを示す文）と「ジョージ・メキシカン料理を食べている文（George is exican food）」の違いを区別することができます。



機密性の高い個人データをスキャンする場合は、英語のみがサポートされます。言語のサポートは、あとで追加されます。

手順

1. Cloud Manager の上部で、* Data Sense * をクリックし、* Compliance * タブをクリックします。
2. 機密性の高い個人データの詳細を調べるには、個人データの割合の横にあるアイコンをクリックします。



3. 特定のタイプの機密個人データの詳細を調べるには、[*すべて表示*] をクリックし、特定のタイプの機密個人データの [調査結果 *] アイコンをクリックします。



4. 特定のファイルの検索、ソート、詳細の展開、* 調査結果 * をクリックしてマスクされた情報を表示、またはファイルリストをダウンロードして、データを調査します。

カテゴリ別にファイルを表示します

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。"[カテゴリのリストを参照してください](#)"。

カテゴリを使用すると、保有している情報の種類を表示して、データの状況を把握することができます。たとえば、履歴書や従業員契約などのカテゴリには機密データを含めることができます。結果を調査すると、従業員契約が安全でない場所に保存されていることがわかります。その後、その問題を修正できます。



英語、ドイツ語、およびスペイン語は、カテゴリでサポートされています。言語のサポートは、あとで追加されます。

手順

1. Cloud Manager の上部で、* Data Sense * をクリックし、* Compliance * タブをクリックします。
2. メイン画面から上位 4 つのカテゴリのいずれかの * 調査結果 * アイコンを直接クリックするか、* すべて表示 * をクリックして、いずれかのカテゴリのアイコンをクリックします。



3. 特定のファイルの検索、ソート、詳細の展開、* 調査結果 * をクリックしてマスクされた情報を表示、またはファイルリストをダウンロードして、データを調査します。

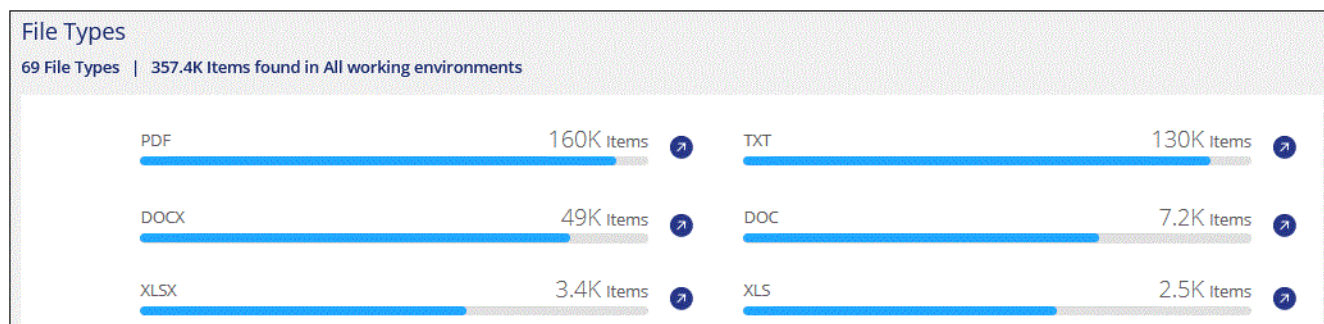
ファイルタイプ別にファイルを表示する

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。ファイルタイプを確認すると、特定のファイルタイプが正しく保存されない可能性があるため、機密データを制御するのに役立ちます。["ファイルタイプのリストを参照してください"](#)。

たとえば '組織に関する非常に機密性の高い情報を含む CAD ファイルを保存する場合がありますセキュリティで保護されていない場合は、権限を制限するか、ファイルを別の場所に移動することで、機密データを制御できます。


手順

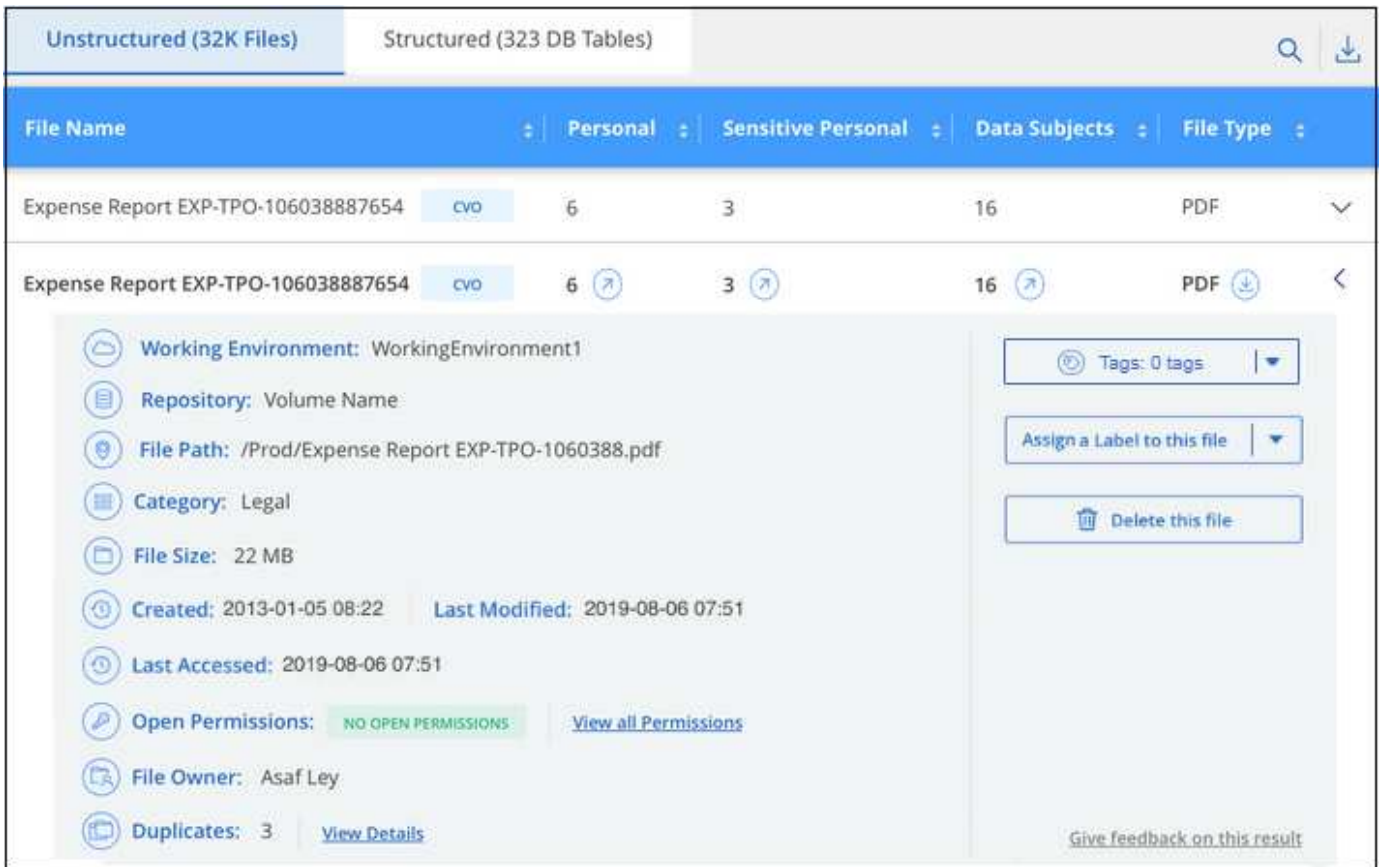
1. Cloud Manager の上部で、* Data Sense * をクリックし、* Compliance * タブをクリックします。
2. メイン画面で上位 4 つのファイルタイプのうちの 1 つに対応する * 調査結果 * アイコンをクリックするか、* すべて表示 * をクリックして、任意のファイルタイプのアイコンをクリックします。



3. 特定のファイルの検索、ソート、詳細の展開、* 調査結果 * をクリックしてマスクされた情報を表示、またはファイルリストをダウンロードして、データを調査します。

ファイルメタデータを表示しています

[データ調査結果] ペインで、をクリックできます  をクリックすると、単一のファイルについてファイルのメタデータが表示されます。



ページのファイルのメタデータの詳細を示すスクリーンショット。"]

ファイルが存在する作業環境とボリュームを表示するだけでなく、メタデータには、ファイル権限、ファイルの所有者、このファイルの重複がないかどうか、および AIP ラベルが割り当てられている場合など、より多くの情報が表示されます ["クラウドデータセンスで AIP を統合"](#)。この情報は、を計画している場合に役立ちます ["ポリシーを作成します"](#) データのフィルタリングに使用できるすべての情報が表示されます。

すべてのデータソースについて、すべての情報が表示されるわけではなく、そのデータソースに適した情報だけが表示されることに注意してください。たとえば、ボリューム名、権限、および AIP ラベルは、データベースファイルには関係ありません。

単一のファイルの詳細を表示する場合は、ファイルに対していくつかの操作を実行できます。

- ファイルは任意の NFS 共有に移動またはコピーできます。を参照してください ["ソースファイルを NFS 共有に移動しています"](#) および ["ソースファイルを NFS 共有にコピーしています"](#) を参照してください。
- ファイルを削除できます。を参照してください ["ソースファイルを削除しています"](#) を参照してください。
- ファイルに特定のステータスを割り当てることができます。を参照してください ["タグの適用"](#) を参照してください。
- ファイルに対して実行する必要があるフォローアップアクションを担当するファイルを Cloud Manager ユーザに割り当てることができます。を参照してください ["ファイルへのユーザの割り当て"](#) を参照してください。
- AIP ラベルを Cloud Data Sense と統合している場合は、このファイルにラベルを割り当てるか、すでに存在する場合は別のラベルに変更できます。を参照してください ["AIP ラベルを手動で割り当てる"](#) を参照してください。

ファイルの権限を表示しています

ファイルへのアクセス権を持つすべてのユーザーまたはグループのリストと、そのファイルに含まれるアクセス権の種類を表示するには、* すべてのアクセス権を表示 * をクリックします。このボタンは、CIFS 共有、SharePoint、OneDrive 内のファイルに対してのみ使用できます。

The screenshot shows a file management interface. On the left, file details for 'Expense Report TPO-1060.pdf' are listed: Working Environment: WorkingEnvironment1, Repository: Volume Name, File Path: /Prod/labs-base/Expense Report TPO-1060.pdf, Category: Legal, File Size: 22 MB, Last Modified: 2019-08-06 07:51, Open Permissions: NO OPEN PERMISSIONS, and File Owner: Avy. A red box highlights the 'View all Permissions' button. On the right, a pop-up window titled 'Permissions list for "Expense Report TPO-1060.pdf"' displays a table of permissions.

| User / Group | Name | Department | Role | Read | Write |
|--------------|------------|------------|------|------|-------|
| | User Name | Department | Role | ✓ | ✓ |
| | Group Name | | | ✓ | ✓ |
| | User Name | Department | Role | ✓ | |
| | Group Name | | | ✓ | ✓ |

ユーザまたはグループの名前をクリックすると、[調査] ページにそのユーザまたはグループの名前が [ユーザ / グループの権限] フィルタに表示され、そのユーザまたはグループがアクセスできるすべてのファイルが表示されます。

ユーザ名とグループ名ではなく SID（セキュリティ識別子）が表示される場合は、Active Directory をデータセンサに統合する必要があります。["詳細については、「方法」を参照してください。"](#)

ストレージシステム内に重複ファイルがないかどうかを確認しています

重複ファイルがストレージシステムに保存されているかどうかを確認できます。これは、ストレージスペースを節約できる領域を特定する場合に便利です。また、特定の権限や機密情報を持つファイルが、ストレージシステム内で不必要に重複しないようにすることもできます。

重複ファイルのリストをダウンロードし、ストレージ管理者に送信して、削除可能なファイルをユーザが判別できるようにします。または ["ファイルを削除します"](#) 特定のバージョンのファイルが不要であることが確信できる場合は、自分自身で実行します。

重複するすべてのファイルを表示します

スキャンする作業環境およびデータソースで複製されているすべてのファイルのリストが必要な場合は、[データの調査] ページで、[重複] > [重複しているもの] というフィルタを使用できます。

すべてのファイルタイプ（データベースを除く）から重複しているすべてのファイルが 50 MB 以上のサイズで、個人情報または機密情報を含むすべてのファイルが結果ページに表示されます。

特定のファイルが複製されているかどうかを表示します

1 つのファイルに重複があるかどうかを確認するには、[データ調査結果] ペインでをクリックします を

クリックすると、単一のファイルについてファイルのメタデータが表示されます。特定のファイルが重複している場合、この情報は _Duplicats_field の横に表示されます。

重複したファイルとその場所のリストを表示するには、[* 詳細の表示 *] をクリックします。次のページで、[重複の表示 *] をクリックして、[調査] ページでファイルを表示します。

File Metadata:

- Last Modified: 2019-08-06 07:51
- Open Permissions: NO OPEN PERMISSIONS
- File Owner: Asaf Ley
- Duplicates: 3

Duplicates of File 'Name 1':

- Duplicates: 3
- Total Size of all Duplicates: 1GB
- File Hash: xxxxxx

| File Name | Personal | Sensitive Personal | Data Subjects | File Type |
|-------------------------------------|----------|--------------------|---------------|-----------|
| Expense Report EXP-TPO-106038887654 | 6 | 3 | 16 | PDF |
| Expense Report EXP-TPO-106038887654 | 6 | 3 | 16 | PDF |
| Expense Report EXP-TPO-106038887654 | 6 | 3 | 16 | PDF |



このページで指定されている「ファイルハッシュ」値を使用して、[調査] ページに直接入力すると、いつでも特定の重複ファイルを検索したり、ポリシーで 사용할 ことができます。

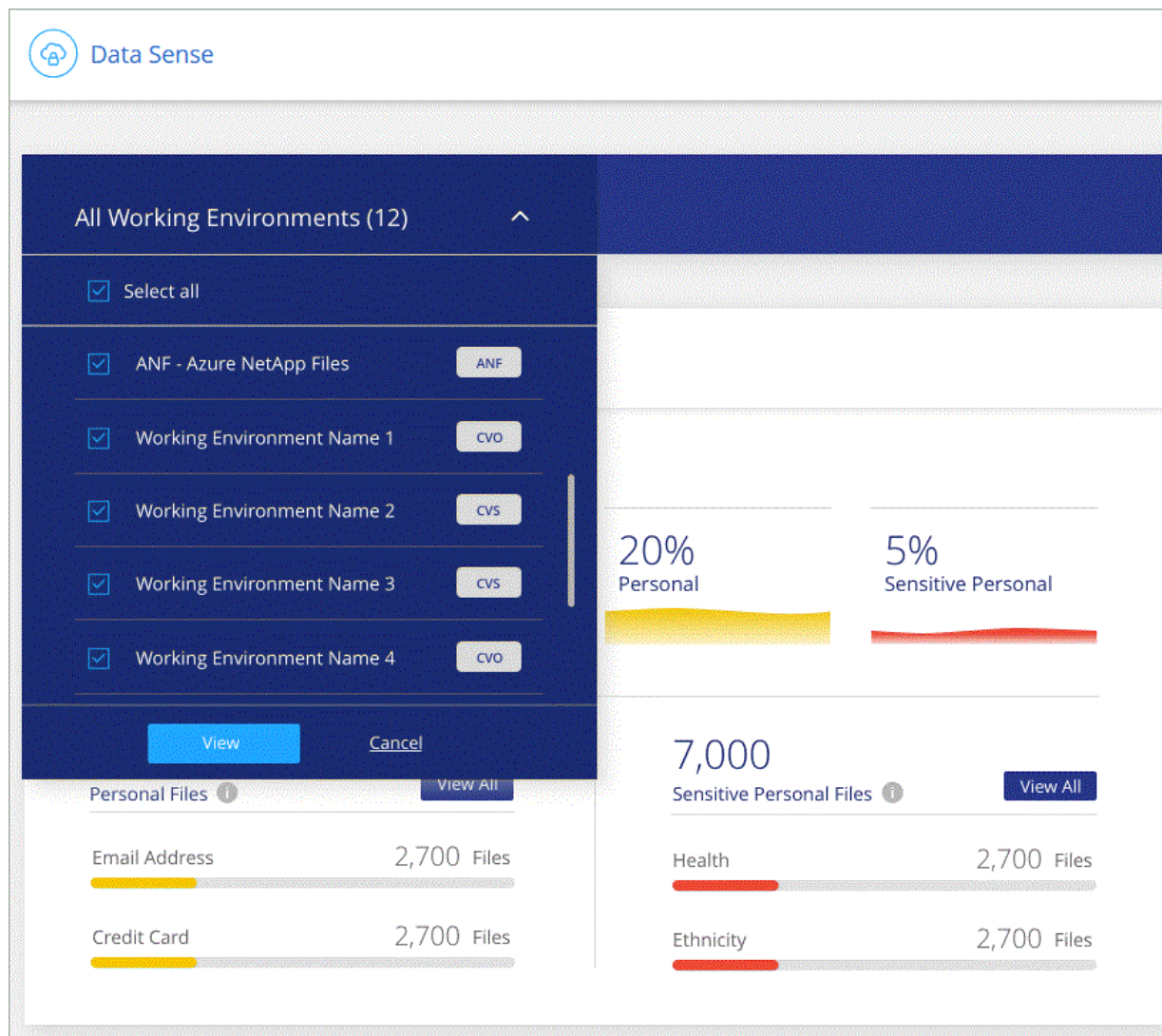
特定の作業環境のダッシュボードデータの表示

Cloud Data Sense ダッシュボードの内容をフィルタリングして、すべての作業環境とデータベース、または特定の作業環境のコンプライアンスデータを表示できます。


ダッシュボードをフィルタすると、Data Sense によって、選択した作業環境だけにコンプライアンスデータとレポートがスコープされます。

手順

1. フィルタドロップダウンをクリックし、データを表示する作業環境を選択して、* 表示 * をクリックします。



【データ調査】ページでデータをフィルタリングします

調査ページの内容をフィルタリングして、表示する結果のみを表示できます。CSV バージョンのコンテンツをリファインした後でレポートとして保存する場合は、をクリックします  ボタン] ボタンを押します。

| | | | | | | |
|--|---|--|--------------------------------------|--|--|--|
| Data Investigation | | Unstructured (252K Files) | Structured (0 Tables) | Search by File or DB Table name or location | | ↓ |
| FILTERS: Clear All | | 252K items | | | | |
| | | Tags | Assign to | Label | Move | Copy |
| | | Delete | | | | |
| Policies + Open Permissions + File Owner + Label + Working Environment Type 2 + Working Environment + Storage Repository 2 + | <input type="checkbox"/> File Name <input type="checkbox"/> cgdpr_yes_adam.txt <input type="checkbox"/> cgdpr_yes_adam.txt <input type="checkbox"/> true positive.txt <input type="checkbox"/> cgdpr_yes_adam.txt <input type="checkbox"/> true positive.txt <input type="checkbox"/> true positive.txt <input type="checkbox"/> cgdpr_yes_adam.txt <input type="checkbox"/> cgdpr_yes_adam.txt | ANF ANF ANF ANF ANF ANF ANF ANF | 0 0 0 0 0 0 0 0 | 797 797 611 611 611 611 611 611 | 111 111 111 111 111 111 111 111 | TXT TXT TXT TXT TXT TXT TXT TXT |

- トップレベルのタブでは、ファイル（非構造化データ）またはデータベース（構造化データ）のデータを表示できます。
- 各列の上部にあるコントロールを使用して、結果を数値またはアルファベット順にソートできます。
- 左側のペインフィルタを使用すると、次の属性を選択して結果を絞り込むことができます。

| フィルタ | 詳細 |
|-------------------------------------|--|
| ポリシー | ポリシーを選択します。実行します "こちらをご覧ください" をクリックして、既存のポリシーのリストを表示し、独自のポリシーを作成します。 |
| [アクセス許可] を開きます | 権限のタイプを選択します |
| ユーザ / グループの権限 | ユーザ名、グループ名、または名前の一部を入力します |
| ファイルの所有者 | ファイル所有者名を入力します |
| ラベル | AIP ラベルを選択します |
| 作業環境タイプ（ Working Environment Type ） | 作業環境のタイプを選択します。OneDrive と SharePoint は、「クラウドアプリ」に分類されています。 |
| 作業環境名 | 特定の作業環境を選択します |
| ストレージリポジトリ | ボリュームやスキーマなどのストレージリポジトリを選択します |
| ファイルパス | 部分パスまたは完全パスを入力してください |
| カテゴリ | を選択します "カテゴリのタイプ" |
| 感度レベル | 感度レベルを選択します |
| 個人データ | を選択します "個人データの種類" |
| 機密性の高い個人データ | を選択します "機密性の高い個人データのタイプ" |
| データの件名 | データ主体のフルネームまたは既知の識別子を入力します |
| ファイルタイプ | を選択します "ファイルのタイプ" |

| フィルタ | 詳細 |
|----------------------|---|
| ファイルサイズ | ファイルサイズの範囲を選択します |
| 作成時刻（ Created Time ） | ファイルを作成したときの範囲を選択します |
| 検出時刻 | データ検出でファイルが検出されたときの範囲を選択します |
| 最終更新日 | ファイルが最後に変更されたときの範囲を選択します |
| 最後にアクセスした | ファイルが最後にアクセスされたときの範囲を選択します。データがスキャンするファイルのタイプの場合、これは最後にデータ検出がファイルをスキャンしたときです。 |
| 重複 | リポジトリ内でファイルを複製するかどうかを選択します |
| ファイル・ハッシュ | ファイルのハッシュを入力し、名前が異なる場合でも特定のファイルを検索します |
| タグ | タグを選択します |
| 割り当て先 | ファイルが割り当てられているユーザーの名前を選択します |

- ・ [フィルタ] ペインの上部にある _Policies_filter には、保存されたデータベースクエリや [お気に入り] リストなど、よく要求されるフィルタの組み合わせを提供するカスタムフィルタがリストされます。実行します ["こちらをご覧ください"](#) 事前定義されたポリシーのリストを表示し、独自のカスタムポリシーを作成する方法を確認できます。

各ファイルリストレポート（ CSV ファイル）に含まれる内容

各 [調査] ページで、をクリックできます [\[ダウンロード \]](#) ボタンをクリックして、特定されたファイルの詳細を含むファイルリスト（ CSV 形式）をダウンロードします。データ検出で、構造化データ（データベーステーブル）と非構造化データ（ファイル）の両方がスキャンされている場合は、ダウンロードした ZIP ファイルに 2 つのレポートが含まれています。

10、000 件を超える結果がある場合は、上位 10、000 件のみがリストに表示されます。

非構造化データ・レポート * には、次の情報が含まれています。

- ・ ファイル名
- ・ 場所のタイプ
- ・ 作業環境の名前
- ・ ストレージリポジトリ（ボリューム、バケット、共有など）
- ・ 作業環境のタイプ
- ・ ファイルパス
- ・ ファイルタイプ
- ・ ファイルサイズ
- ・ 時刻を作成しました
- ・ 最終更新日
- ・ 最後にアクセスした

- ファイルの所有者
- カテゴリ
- 個人情報
- 機密性の高い個人情報
- 削除の検出日

削除の検出日は、ファイルが削除または移動された日付を示します。これにより、機密ファイルがいつ移動されたかを識別できます。削除されたファイルは、ダッシュボードまたは[調査]ページに表示されるファイル番号カウントの一部ではありません。ファイルは CSV レポートにのみ表示されます。

構造化データレポート * には、次の情報が含まれています。

- DB テーブル名
- 場所のタイプ
- 作業環境の名前
- ストレージリポジトリ（スキーマなど）
- 列数
- 行数
- 個人情報
- 機密性の高い個人情報

プライベートデータを整理する

Cloud Data Sense は、プライベートデータを管理、整理するためのさまざまな方法を提供します。これにより、最も重要なデータを簡単に確認できます。

- に登録している場合は "Azure 情報保護 (AIP)" ファイルを分類して保護するには、Cloud Data Sense を使用して AIP ラベルを管理します。
- 組織または特定の種類のフォローアップのためにマークするファイルにタグを追加できます。
- Cloud Manager ユーザを特定のファイルまたは複数のファイルに割り当てて、ユーザがファイルの管理を担当できるようにすることができます。
- 「ポリシー」機能を使用すると、1 つのボタンをクリックして簡単に結果を表示できるように、独自のカスタム検索クエリを作成できます。
- 特定の重要なポリシーが結果を返すと、Cloud Manager ユーザに E メールアラートを送信できます。



このセクションで説明する機能は、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。

タグまたはラベルを使用する必要がありますか？

以下は、データセンスタグと Azure Information Protection ラベルの比較です。

| タグ | ラベル |
|---|---|
| ファイルタグは、データセンスの統合部分です。 | Azure Information Protection （AIP）に加入している必要があります。 |
| タグはデータセンスデータベースにのみ保存され、ファイルには書き込まれません。ファイル、アクセス日時または変更日時は変更されません。 | ラベルはファイルの一部であり、ラベルが変更されるとファイルが変更されます。この変更によって、アクセス日時や変更日時も変更されます。 |
| 1つのファイルに複数のタグを設定できます。 | 1つのファイルに1つのラベルを付けることができます。 |
| タグは、コピー、移動、削除、ポリシーの実行など、内部データセンスアクションに使用できます。 など | ファイルを読み取ることができる他のシステムでは、ラベルを確認できます。このラベルは、自動化のために使用できます。 |
| ファイルにタグが設定されているかどうかを確認するために使用される API 呼び出しは 1 つだけです。 | |

AIP ラベルを使用してデータを分類する

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）"](#)。AIP を使用すると、コンテンツにラベルを適用することで、ドキュメントやファイルを分類して保護できます。データセンスを使用すると、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、ラベルが既に存在する場合にラベルを変更したりできます。

クラウドデータセンスは、.DOC、.DOCX、.pdf、.PPTX、.XLS、.xlsx。



- 現在、30MB を超えるファイルのラベルは変更できません。OneDrive アカウントと SharePoint アカウントの場合、最大ファイルサイズは 4MB です。
- AIP に存在しないラベルがファイルにある場合、Cloud Data Sense はラベルのないファイルと見なします。
- 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（ダークサイトとも呼ばれます）にデータセンスインスタンスを配置した場合、AIP ラベル機能は使用できません。

ワークスペースへの AIP ラベルの統合

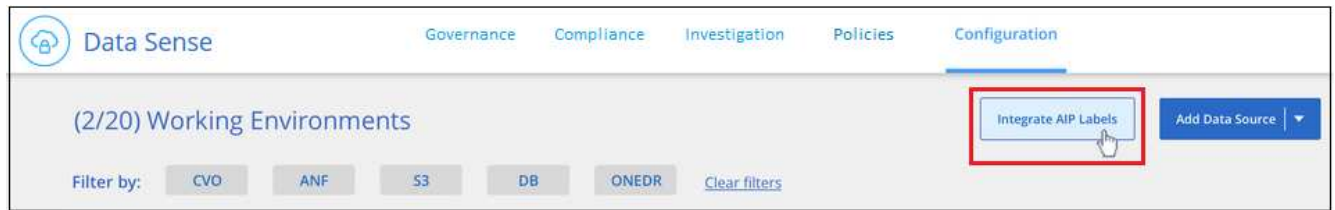
AIP ラベルを管理するには、既存の Azure アカウントにサインインして AIP ラベル機能をクラウドデータセン스에統合する必要があります。有効にすると、すべてのファイルの AIP ラベルを管理できます ["作業環境とデータソース"](#) をクリックします。

要件

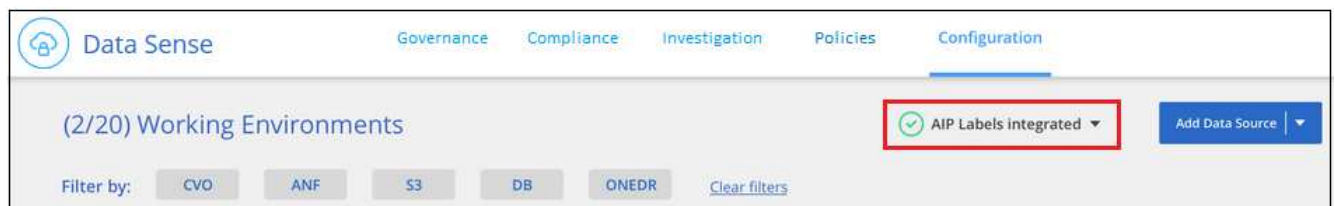
- アカウントと Azure Information Protection のライセンスが必要です。
- Azure アカウントのログインクレデンシャルが必要です。
- Amazon S3 バケット内のファイルのラベルを変更する場合は、権限「3：PutObject」が IAM ロールに含まれていることを確認します。を参照してください ["IAM ロールを設定します"](#)。

手順

1. Cloud Data Sense Configuration ページで、**Integrate AIP Labels** をクリックします。



2. [Integrate AIP Labels (AIP ラベルの統合)] ダイアログで、[* Sign in to Azure* (Azure にサインイン)]
3. 表示される Microsoft ページで、アカウントを選択し、必要なクレデンシャルを入力します。
4. Cloud Data Sense タブに戻り、「AIP Labels were successfully integrated with the account <account_name>」というメッセージが表示されます。
5. [* 閉じる] をクリックすると、ページの上部に「AIP ラベル integrated_」というテキストが表示されます。



AIP ラベルは、[調査] ページの結果ペインで表示および割り当てることができます。また、ポリシーを使用して AIP ラベルをファイルに割り当てることができます。

ファイルで **AIP** ラベルを表示する

ファイルに割り当てられている現在の AIP ラベルを表示できます。

[データ調査結果] ペインで、をクリックします ▼ をクリックします。



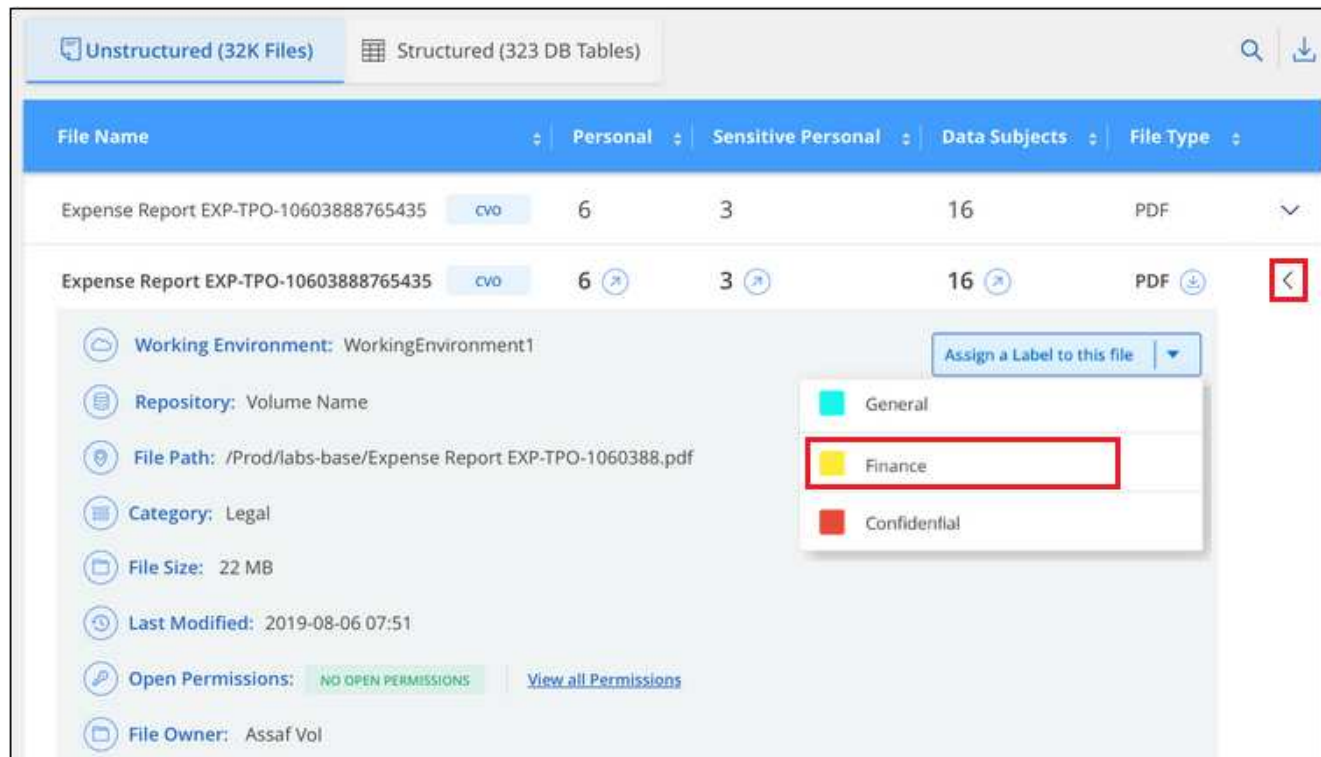
AIP ラベルを手動で割り当てる

Cloud Data Sense を使用して、ファイルに AIP ラベルを追加、変更、および削除できます。

AIP ラベルを 1 つのファイルに割り当てる手順は、次のとおりです。

手順

1. [データ調査結果] ペインで、をクリックします  をクリックします。



ページのファイルのメタデータの詳細を示すスクリーンショット。"]

2. [* このファイルにラベルを割り当て *] をクリックして、ラベルを選択します。

ラベルがファイルメタデータに表示されます。



AIP ラベルを複数のファイルに割り当てるには、次の手順を実行します。

手順

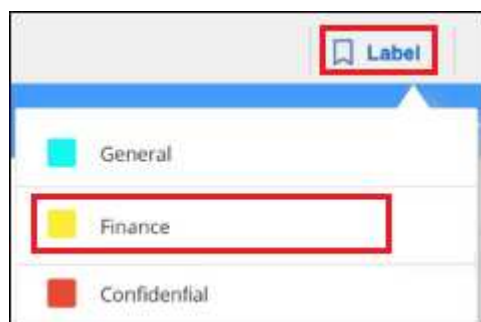
1. [データ調査結果] ペインで、ラベル付けするファイルを選択します。



ページの [ラベル] ボタン。"]

- 個々のファイルを選択するには、各ファイル ( Volume_1)。
- 現在のページのすべてのファイルを選択するには、タイトル行 ( File Name)。

2. ボタンバーの *Label* をクリックし、AIP ラベルを選択します。



AIP ラベルが、選択したすべてのファイルのメタデータに追加されます。

ポリシーを使用して **AIP** ラベルを自動的に割り当てます

AIP ラベルは、ポリシーの条件を満たすすべてのファイルに割り当てることができます。ポリシーの作成時に AIP ラベルを指定することも、ポリシーの編集時にラベルを追加することもできます。

Cloud Data Sense がファイルをスキャンすると、ファイルにラベルが追加または更新されます。

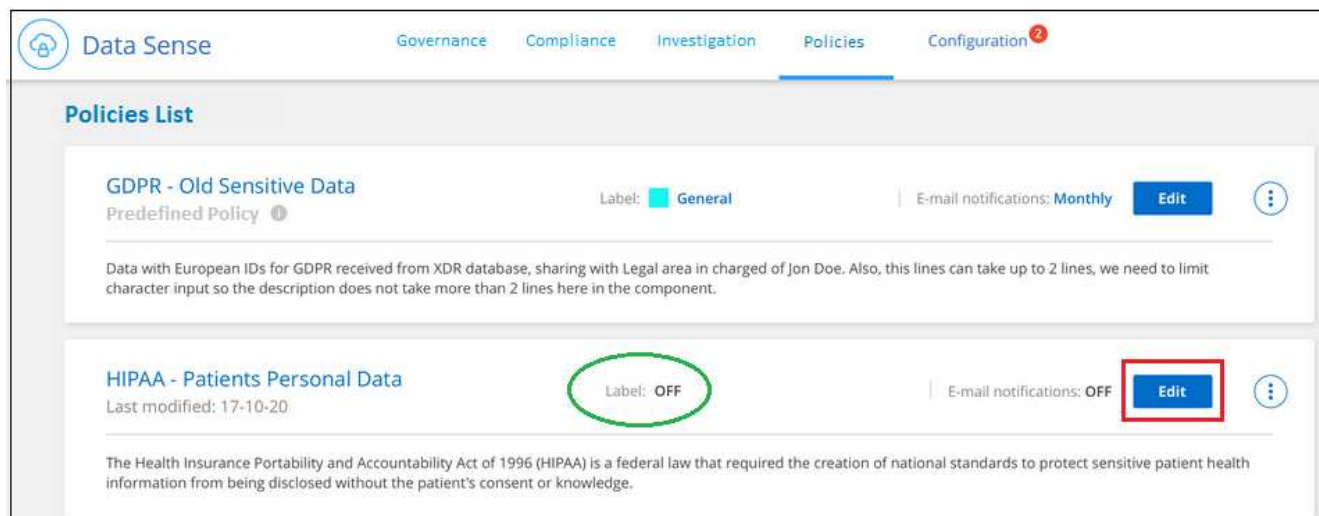
ラベルがすでにファイルに適用されているかどうか、およびラベルの分類レベルによって、ラベルを変更するときに次のアクションが実行されます。

| ファイルの内容 | 作業 |
|----------------------------------|------------------|
| にはラベルがありません | ラベルが追加されます |
| 下位レベルの分類の既存のラベルがあります | 上位レベルのラベルが追加されます |
| より高いレベルの分類の既存のラベルがあります | 上位レベルのラベルが保持されます |
| 手動とポリシーの両方でラベルが割り当てられます | 上位レベルのラベルが追加されます |
| 2 つのポリシーによって 2 つの異なるラベルが割り当てられます | 上位レベルのラベルが追加されます |

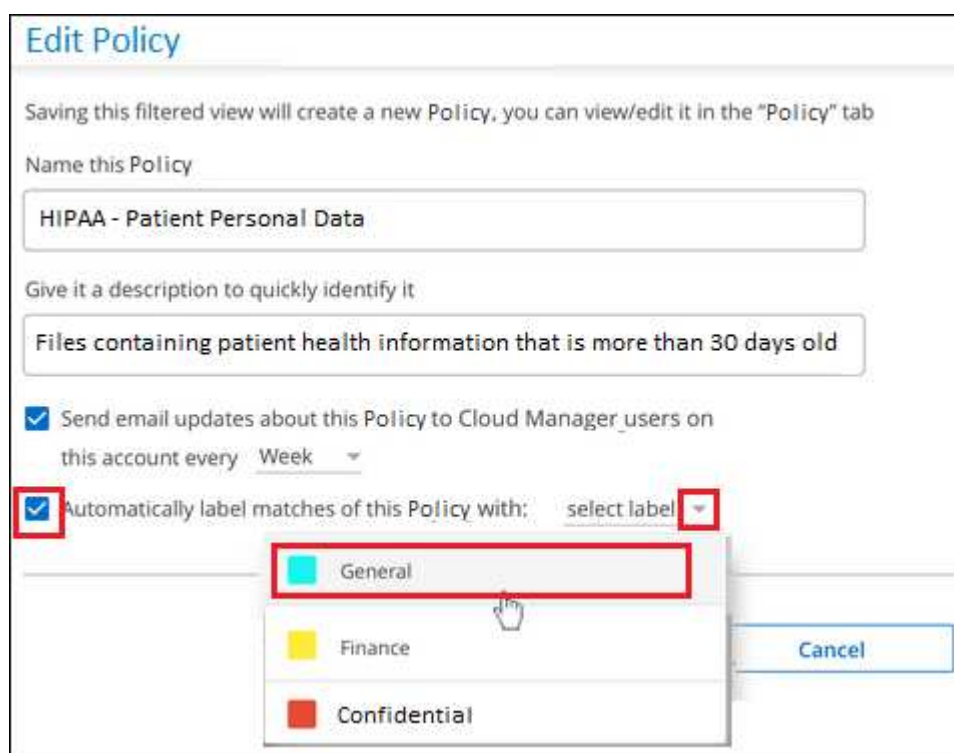
AIP ラベルを既存のポリシーに追加する手順は、次のとおりです。

手順

1. [ポリシーリスト] ページで、AIP ラベルを追加（または変更）するポリシーの **Edit** をクリックします。



2. [ポリシーの編集] ページで、[ポリシー] パラメータに一致するファイルの自動ラベルを有効にするチェックボックスをオンにして、ラベル（**General** など）を選択します。



3. [ポリシーの保存 *] をクリックすると、[ポリシー概要] にラベルが表示されます。



ポリシーにラベルが設定されていても、ラベルが AIP から削除されている場合、ラベル名はオフになり、ラベルは割り当てられなくなります。

AIP 連動の削除

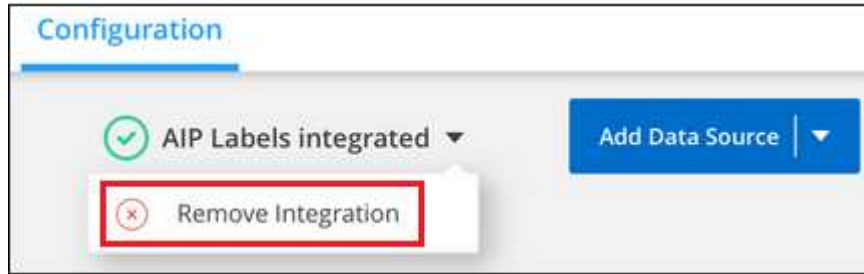
ファイル内の AIP ラベルを管理する機能が不要になった場合は、クラウドデータセンスインターフェイスから AIP アカウントを削除できます。

データセンスを使用して追加したラベルは変更されません。ファイルに存在するラベルは、現在存在している

ラベルのままになります。

手順

1. _Configuration_page で、 *AIP ラベル統合 > 統合の削除 * をクリックします。



2. 確認ダイアログで、[統合の削除 (Remove Integration)] をクリックします。

タグを適用してスキャンしたファイルを管理します

特定の種類のフォローアップでマークするファイルにタグを追加できます。たとえば、重複するファイルがいくつか見つかった場合に、それらのファイルを 1 つ削除する必要がありますが、削除するファイルを確認する必要があります。このファイルに「削除するチェック」というタグを追加すると、このファイルに何らかの調査と将来のアクションが必要であることがわかります。

データセンスを使用すると、ファイルに割り当てられているタグを表示したり、ファイルのタグを追加または削除したり、名前を変更したり、既存のタグを削除したりできます。

AIP ラベルがファイルメタデータの一部であるのと同じ方法で、タグがファイルに追加されないことに注意してください。このタグは、Cloud Manager ユーザが Cloud Data Sense を使用して確認するだけで表示されるので、ファイルを削除する必要があるか、特定の種類のフォローアップを確認する必要があるかを確認できます。

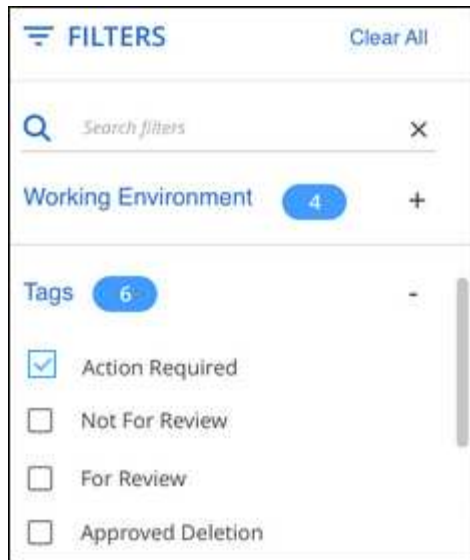


Cloud Data Sense でファイルに割り当てられているタグは、ボリュームや仮想マシンのインスタンスなど、リソースに追加できるタグには関連していません。データセンスタグは、ファイルレベルで適用されます。

特定のタグが適用されているファイルを表示しています

特定のタグが割り当てられているすべてのファイルを表示できます。

1. Cloud Data Sense の [* Investigation* (調査*)] タブをクリックします。
2. [データ調査] ページで、[フィルタ] ペインの [* タグ] をクリックし、必要なタグを選択します。



ペインからタグを選択する方法を示すスクリーンショット。"]

[調査結果] ペインには、これらのタグが割り当てられているすべてのファイルが表示されます。

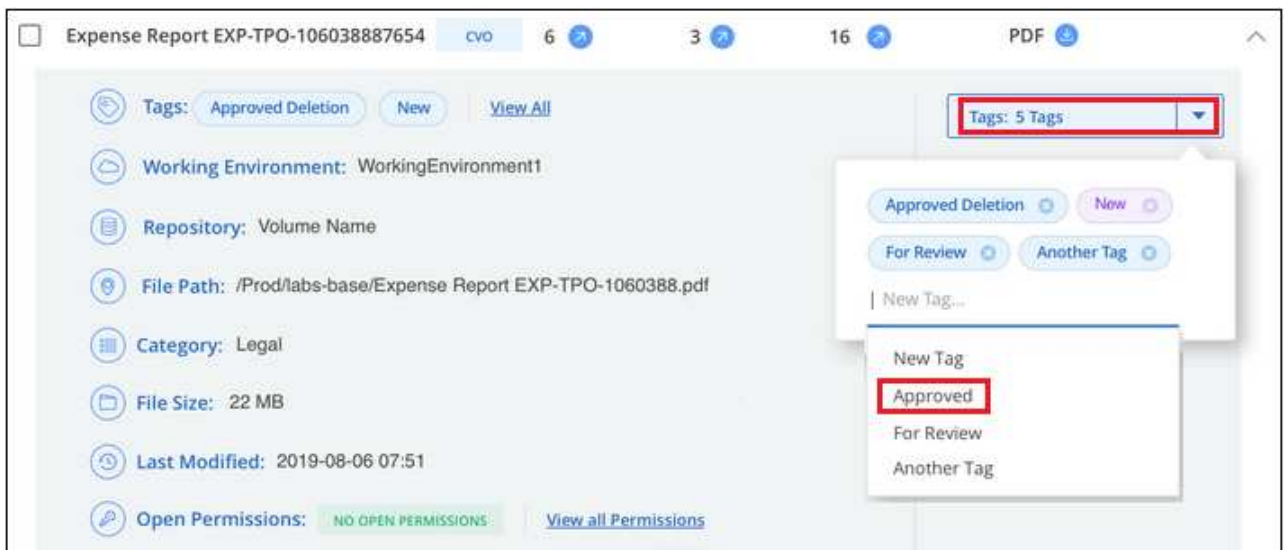
ファイルにタグを割り当てます

タグは、単一のファイルまたはファイルのグループに追加できます。

タグを 1 つのファイルに追加するには：

手順

1. [データ調査結果] ペインで、をクリックします ▼ をクリックします。
2. [* タグ * (* Tags *)] フィールドをクリックすると、現在割り当てられているタグが表示されます。
3. タグを追加します。
 - 既存のタグを割り当てるには、「 * 新しいタグ ... 」フィールドをクリックして、タグの名前を入力します。探しているタグが表示されたら、そのタグを選択して * Enter * を押します。
 - 新しいタグを作成してファイルに割り当てるには、[新しいタグ ...] * フィールドをクリックし、新しいタグの名前を入力して、 **Enter** キーを押します。



ページでファイルにタグを割り当てる方法を示すスクリーンショット。"]

タグがファイルメタデータに表示されます。

複数のファイルにタグを追加するには：

手順

1. [データ調査結果] ペインで、タグを付けるファイルを選択します。

2345 items

Tags

Assign to

Label

Copy

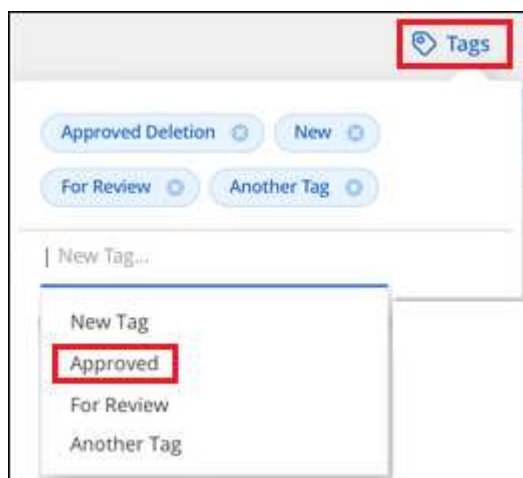
Move

Delete

| <input type="checkbox"/> | File Name | | Personal | Sensitive Personal | Data Subjects | File Type | |
|-------------------------------------|-------------------------------------|-----|----------|--------------------|---------------|-----------|---|
| <input checked="" type="checkbox"/> | Expense Report EXP-TPO-106038887654 | cvo | 6 | 3 | 16 | PDF | ▼ |
| <input checked="" type="checkbox"/> | Expense Report EXP-TPO-106038887654 | cvo | 6 | 3 | 6 | PDF | ▼ |
| <input type="checkbox"/> | Expense Report EXP-TPO-106038887654 | cvo | 6 | 3 | 6 | PDF | ▼ |
| <input type="checkbox"/> | Expense Report EXP-TPO-106038887654 | cvo | 6 | 3 | 6 | PDF | ▼ |

ページから、タグを付けるファイルの選択方法と [タグ] ボタンを示すスクリーンショット。"]

- 個々のファイルを選択するには、各ファイル (☒ Volume_1) 。
 - 現在のページのすべてのファイルを選択するには、タイトル行 (☒ File Name) 。
2. ボタンバーで * タグ * をクリックすると、現在割り当てられているタグが表示されます。
 3. タグを追加します。
 - 既存のタグを割り当てるには、「 * 新しいタグ ... 」フィールドをクリックして、タグの名前を入力します。探しているタグが表示されたら、そのタグを選択して * Enter * を押します。
 - 新しいタグを作成してファイルに割り当てるには、[新しいタグ ...] * フィールドをクリックし、新しいタグの名前を入力して、 **Enter** キーを押します。



ページで複数のファイルにタグを割り当てる方法を示すスクリーンショット。"]

4. 確認ダイアログでタグの追加を承認し、選択したすべてのファイルのメタデータにタグを追加します。

ファイルからタグを削除しています

不要になったタグは削除できます。

既存のタグの *x* をクリックするだけです。



複数のファイルを選択した場合、タグはすべてのファイルから削除されます。

特定のファイルを管理するためのユーザの割り当て

Cloud Manager ユーザには特定のファイルまたは複数のファイルを割り当てることができます。これにより、ファイルに対して実行する必要があるフォローアップアクションをユーザが実行できるようになります。この機能は、多くの場合、カスタムステータスタグをファイルに追加する機能で使用されます。

たとえば、特定の個人データを含むファイルで、読み取りおよび書き込みアクセス（オープン権限）を大量に許可する場合などです。したがって、Status タグ「Change permissions」を割り当て、このファイルをユーザー「Joan Smith」に割り当てて、問題の修正方法を決定することができます。問題を修正すると、Status タグが「Completed」に変更されることがあります。

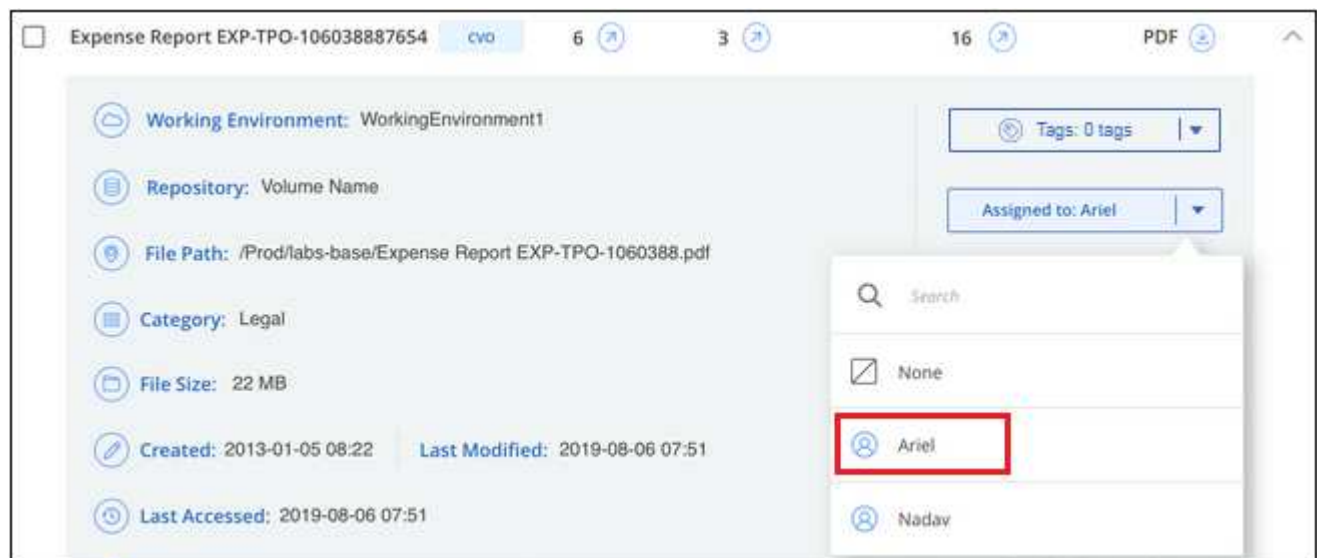
ユーザ名はファイルメタデータの一部としてファイルに追加されません。Cloud Data Sense を使用している場合、Cloud Manager ユーザから確認できます。

[調査] ページの新しいフィルタを使用すると、[割り当て先] フィールドに同じユーザーを持つすべてのファイルを簡単に表示できます。

ユーザーを 1 つのファイルに割り当てするには、次の手順を実行します。

手順

1. [データ調査結果] ペインで、をクリックします ▼ をクリックします。
2. **[Assigned To]** フィールドをクリックして、ユーザ名を選択します。



ページでファイルにユーザーを割り当てする方法を示すスクリーンショット。"]

ユーザ名がファイルメタデータに表示されます。

ユーザーを複数のファイルに割り当てるには：

手順

1. [データ調査結果] ペインで、ユーザーに割り当てるファイルを選択します。

2345 items

Tags

Assign to

Label

Copy

Move

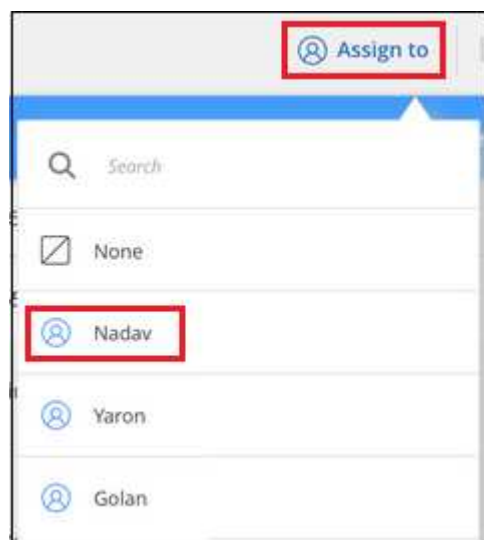
Delete

| <input type="checkbox"/> | File Name | | Personal | Sensitive Personal | Data Subjects | File Type | |
|-------------------------------------|-------------------------------------|-----|----------|--------------------|---------------|-----------|---|
| <input checked="" type="checkbox"/> | Expense Report EXP-TPO-106038887654 | cvo | 6 | 3 | 16 | PDF | ▼ |
| <input checked="" type="checkbox"/> | Expense Report EXP-TPO-106038887654 | cvo | 6 | 3 | 6 | PDF | ▼ |
| <input type="checkbox"/> | Expense Report EXP-TPO-106038887654 | cvo | 6 | 3 | 6 | PDF | ▼ |
| <input type="checkbox"/> | Expense Report EXP-TPO-106038887654 | cvo | 6 | 3 | 6 | PDF | ▼ |

ページから、ユーザーに割り当てるファイルの選択方法と [割り当て先] ボタンを示すスクリーンショット。"]

- 個々のファイルを選択するには、各ファイル（☒ Volume_1）。
- 現在のページのすべてのファイルを選択するには、タイトル行（☒ File Name）。

2. ボタンバーで * Assign to * をクリックし、ユーザー名を選択します。



ページでユーザーを複数のファイルに割り当てる方法を示すスクリーンショット。"]

選択したすべてのファイルのメタデータにユーザが追加されます。

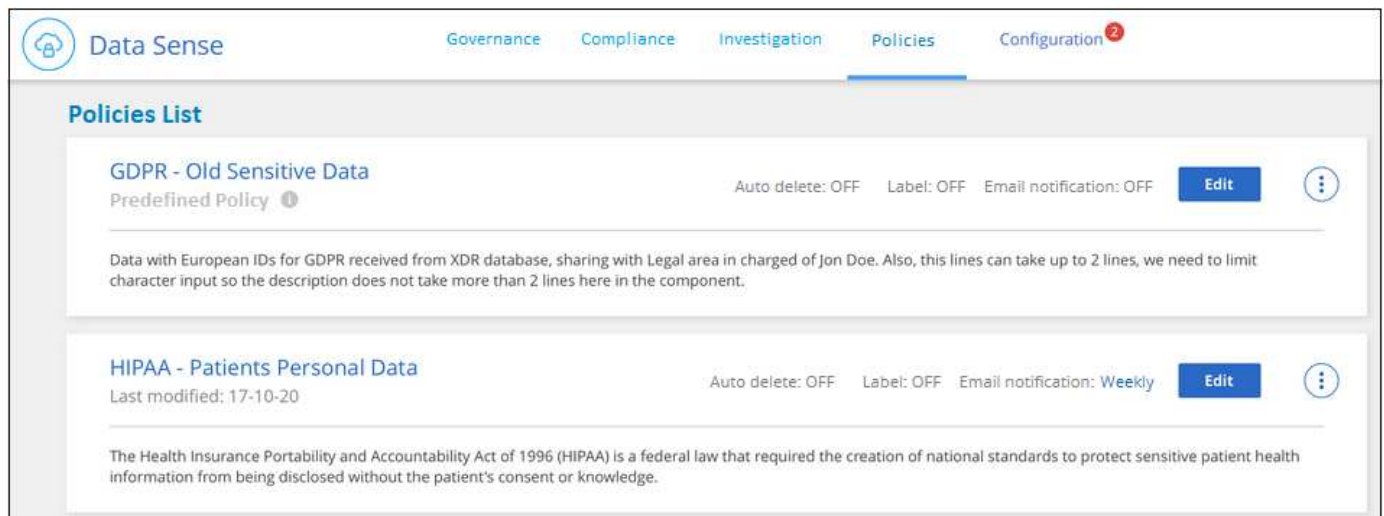
ポリシーを使用したデータの制御

ポリシーは、よく要求されるコンプライアンスクエリーの [調査] ページで検索結果を表示するカスタムフィルタのお気に入りリストのようなものです。Cloud Data Sense は、お客様からの一般的なリクエストに基づいて、一連の事前定義されたポリシーを提供します。組織固有の検索結果を提供するカスタムポリシーを作成できます。

ポリシーには次の機能があります。

- 事前定義されたポリシー ユーザの要求に基づいて作成されます
- 独自のカスタムポリシーを作成できます
- ポリシーの結果を含む [調査] ページを起動します ワンクリックで
- Cloud Manager ユーザに特定の重大度の E メールアラートを送信する ポリシーによって結果が返されるので、通知を取得して保護することができます データを
- AIP の割り当て（ Azure 情報保護） 定義された条件に一致するすべてのファイルに自動的にラベルを付けます ポリシー内
- 特定のポリシーで結果が返されたときにファイルを自動的に削除して（ 1 日に 1 回）、データを自動的に保護できます

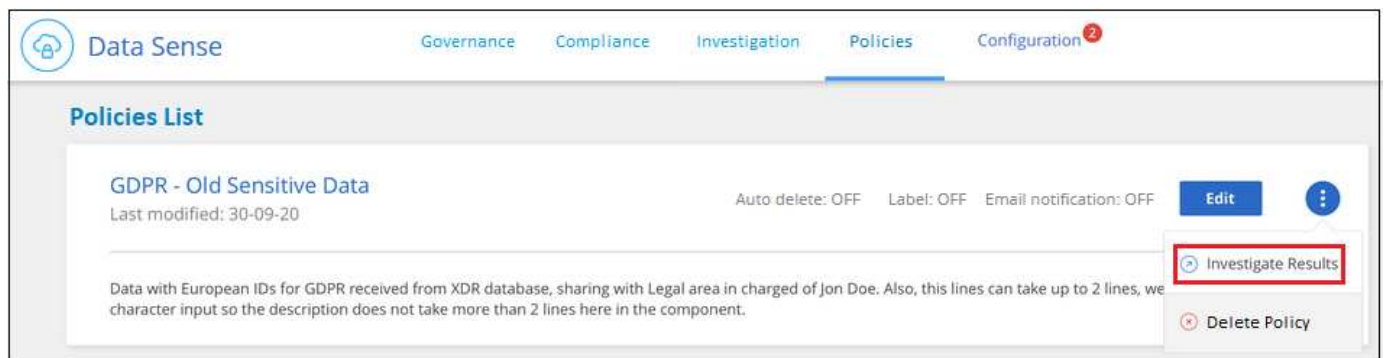
順守ダッシュボードの * ポリシー * タブには、クラウドデータセンスのこのインスタンスで使用可能なすべての定義済みおよびカスタムポリシーが一覧表示されます。



さらに、[調査] ページの [フィルタ] リストにポリシーが表示されます。

[調査] ページでポリシーの結果を表示します

[調査] ページでポリシーの結果を表示するには、をクリックします [ボタン] ボタンをクリックして特定のポリシーを選択し、 * 調査結果 * を選択します。

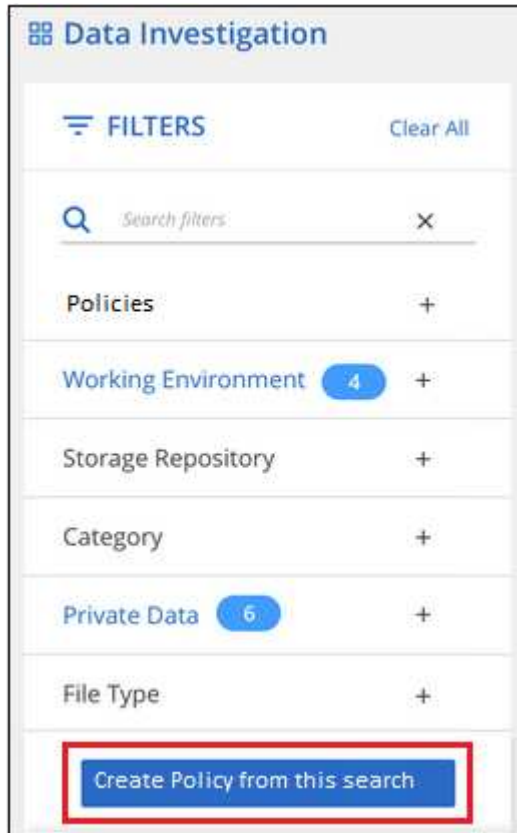


カスタムポリシーを作成しています

組織固有の検索結果を提供する独自のカスタムポリシーを作成できます。

手順

1. [データ調査] ページで、使用するすべてのフィルタを選択して検索を定義します。を参照してください "[データ調査] ページでデータをフィルタリングします" を参照してください。
2. 必要な方法でフィルタ特性をすべて設定したら、[この検索からポリシーを作成する *] をクリックします。



3. ポリシーに名前を付け、そのポリシーで実行できるその他のアクションを選択します。
 - a. 一意の名前と説明を入力します。
 - b. 必要に応じて、このチェックボックスをオンにすると、ポリシーのパラメータに一致するファイルが自動的に削除されます。の詳細を確認してください "ポリシーを使用してソースファイルを削除しています"。
 - c. 必要に応じて、Cloud Manager ユーザに通知 E メールを送信する場合はチェックボックスをオンにし、Eメールの送信間隔を選択します。の詳細を確認してください "ポリシーの結果に基づいて E メールアラートを送信する"。
 - d. 必要に応じて、このチェックボックスをオンにすると、ポリシーパラメータに一致するファイルに AIP ラベルが自動的に割り当てられ、ラベルが選択されます。（AIP ラベルがすでに統合されている場合のみ。の詳細を確認してください "AIP ラベル".）
 - e. [ポリシーの作成 *] をクリックします。

Create Policy

This will create a new Policy according to the current selected filters and search term. You can view or delete this later from the "Policies" tab.

Note it may take up to 15 minutes for results to be displayed for a new Policy.

Name this Policy

New Policy to view all files that were created over 60 days ago

Give it a detailed description that explains what it searches for

See if any files greater than 60 days old should be deleted from the system

☐ Automatically delete files that match this policy (Every Day)

☒ Send email updates about this Policy to Cloud Manager users on this account every Day

☐ Automatically label this Policy's matches with: Select a label

Create Policy Cancel

[ポリシー] タブに新しいポリシーが表示されます。

準拠していないデータが見つかった場合に E メールアラートを送信する

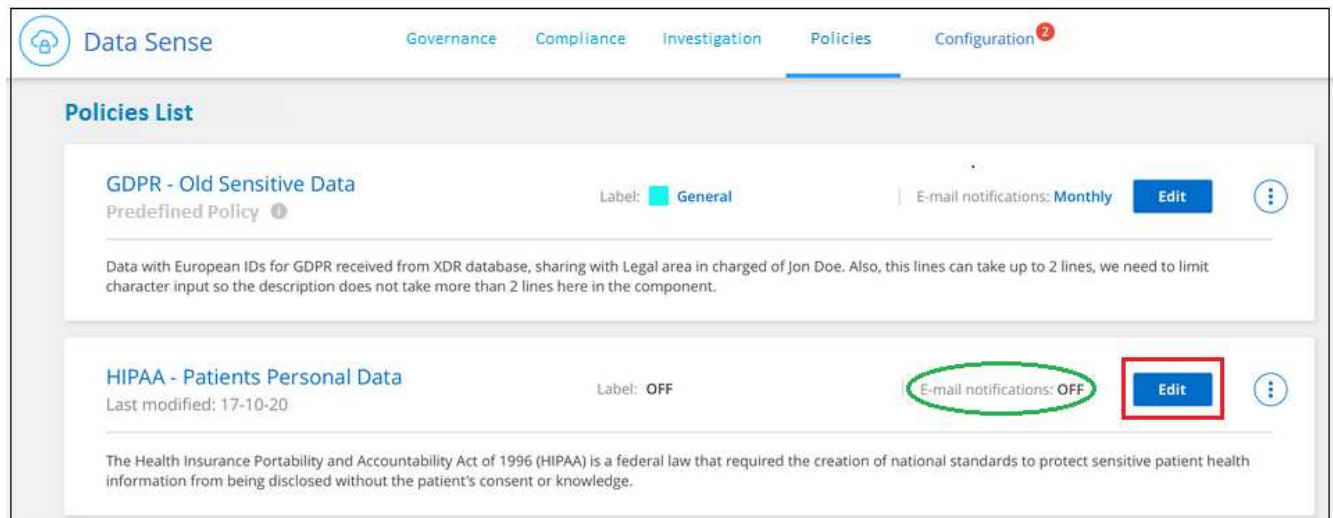
Cloud Data Sense は、特定の重要なポリシーの結果が返されたときに Cloud Manager ユーザに E メールアラートを送信して、データを保護する通知を受け取ることができます。E メール通知は、日単位、週単位、または月単位で送信することができます。

この設定は、ポリシーの作成時または任意のポリシーの編集時に設定できます。

既存のポリシーにメールの更新を追加するには、次の手順を実行します。

手順

1. [ポリシーリスト] ページで、電子メール設定を追加（または変更）するポリシーの [編集 *] をクリックします。



2. ポリシーの編集ページで、Cloud Manager ユーザに通知 E メールを送信する場合はチェックボックスをオンにし、Eメールの送信間隔（毎週 * Week * など）を選択します。

3. [* ポリシーの保存 *] をクリックすると、電子メールの送信間隔が [ポリシー概要] に表示されます。

最初の電子メールは、ポリシーからの結果がある場合に送信されます。ただし、ポリシーの条件を満たすファイルがある場合に限りです。通知メールに個人情報送信されません。Eメールには、ポリシーの条件に一致するファイルがあり、ポリシーの結果へのリンクが記載されています。

ポリシーの編集

ポリシーのタイプに応じて、ポリシーの特定の部分を変更できます。

- カスタムポリシー - _ 名前 _、_ 概要 _、電子メール通知の送信の有無、および ラベルの追加の有無を変更できます。

- 定義済みポリシー - 電子メール通知が送信されるかどうか、および AIP ラベルが追加されるかどうかだけを変更できます。



カスタムポリシーのフィルタパラメータを変更する必要がある場合は、必要なパラメータを含む新しいポリシーを作成してから、古いポリシーを削除する必要があります。

ポリシーを変更するには、[編集 *] ボタンをクリックし、_Edit Policy_page に変更を入力して、[ポリシーの保存 *] をクリックします。

ポリシーの削除

作成したカスタムポリシーが不要になった場合は削除できます。事前定義されたポリシーは削除できません。

ポリシーを削除するには、をクリックします ボタン"] ボタンをクリックして特定のポリシーを削除し、確認ダイアログでもう一度 [* ポリシーの削除 *] をクリックします。

事前定義されたポリシーのリスト

Cloud Data Sense で提供されるシステム定義のポリシーは次のとおりです。

| 名前 | 説明 | ロジック |
|---------------------------|---|---|
| S3 公開プライベートデータ | 個人または機密性の高い個人情報を含む S3 オブジェクト。オープンなパブリック読み取りアクセスが許可されます。 | S3 Public となり、個人情報または機密情報が含まれます |
| PCI DSS : 30 日以上古いデータ | クレジットカード情報を含むファイル。最終更新日は 30 日前です。 | クレジットカードと最終変更日が 30 日以上含まれます |
| HIPAA : 30 日以上データを停滞させます | ヘルス情報が含まれるファイル。最終更新日は 30 日前です。 | 健康データを含む (HIPAA レポートと同様に定義されている) そして、最終変更日は 30 日です |
| プライベートデータ-7 年以上前から停滞しています | 個人情報または機密性の高い個人情報を含むファイル。最終更新日は 7 年前に変更されました。 | 個人情報または機密性の高い個人情報を含むファイル。最終更新日は 7 年前に変更されました |
| GDPR - 欧州市民 | EU 加盟国の市民の 5 つ以上の ID を含むファイル、または EU 加盟国の市民の ID を含む DB テーブル。 | (1 つの) EU 市民または DB テーブルの 5 つ以上の識別子を含むファイル。列の 15% 以上の行と、1 つの国の EU 識別子が含まれています。(欧州諸国のいずれかの国の識別子。ブラジル、カリフォルニア、米国 SSN、イスラエル、南アフリカを含まない) |
| CCPA - カリフォルニア州在住 | この識別子を持つ 10 を超えるカリフォルニアドライバのライセンス ID または DB テーブルを含むファイル。 | 10 を超える California Driver のライセンス ID または DB を含むファイル カリフォルニアドライバのライセンスを含むテーブル |
| データ主体名-高リスク | 50 を超えるデータ主体名を持つファイル。 | 50 を超えるデータ主体名を持つファイル |

| 名前 | 説明 | ロジック |
|----------------------|--|---|
| E メールアドレス–リスクが高くなります | E メールアドレスが 50 を超えるファイル、または E メールアドレスを含む行の 50% を超える DB 列 | E メールアドレスが 50 を超えるファイル、または E メールアドレスを含む行の 50% を超える DB 列 |
| 個人データ–高いリスク | 個人データ識別子が 20 を超えるファイル、または個人データ識別子を含む行の 50% を超える DB 列。 | 20 以上の個人用のファイル、または個人を含む行の 50% を超える DB 列を持つファイル |
| 機密性の高い個人データ–高いリスク | 機密性の高い個人データ識別子が 20 を超えるファイル、または機密性の高い個人データを含む行の 50% を超える DB 列。 | 機密性の高い個人用のファイル、または機密性の高い個人を含む行の 50% 以上を含む DB 列 |

プライベートデータの管理

Cloud Data Sense は、プライベートデータを管理するためのさまざまな方法を提供します。一部の機能を使用すると、データの移行準備が簡単になります。また、他の機能を使用してデータを変更することもできます。

- 特定のデータのコピーを作成して別の NFS の場所に移動する場合は、デスティネーションの NFS 共有にファイルをコピーできます。
- ONTAP ボリュームを新しいボリュームにクローニングしたり、選択したファイルだけをソースボリュームから新しいクローンボリュームに含めたりできます。これは、データを移行しているときに、元のボリュームから特定のファイルを除外する場合に便利です。
- ソースリポジトリから特定の保存先にあるディレクトリにファイルをコピーして同期できます。これは、ソースファイルに最終的なアクティビティが残っている間に、あるソースシステムから別のソースシステムにデータを移行する場合に便利です。
- データがスキャンしているソースファイルを任意の NFS 共有に移動できます。
- 安全でないようであるか危険すぎると思われるファイルを削除して、ストレージシステムに残すことも、重複として識別したファイルを削除することもできます。



このセクションで説明する機能は、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。

ソースファイルをコピーしています

データがスキャンしているすべてのソースファイルをコピーできます。実行しようとしている処理に応じて、次の 3 種類のコピー処理があります。

- * 同一または異なるボリュームまたはデータソースからデスティネーション NFS 共有にファイル * をコピーします。

これは、特定のデータのコピーを作成して別の NFS の場所に移動する場合に便利です。

- * ONTAP ボリュームのクローンを同じアグリゲート内の新しいボリュームに作成します。新しいクローンボリュームには、ソースボリュームから選択されたファイルのみを含めます。

これは、データを移行する際に元のボリュームから特定のファイルを除外する場合に便利です。このアクションではを使用します **"NetApp FlexClone"** ボリュームをすばやく複製し、* 選択しなかったファイルを削除する機能。

- * 単一のソースリポジトリ（ONTAP ボリューム、S3 バケット、NFS 共有など）から特定のデスティネーション（ターゲット）にあるディレクトリにファイルをコピーして同期します。

これは、あるソースシステムから別のシステムにデータを移行する場合に便利です。最初のコピーの後、設定したスケジュールに基づいて変更されたデータが同期されます。このアクションではを使用します **"NetApp Cloud Sync の略"** データをソースからターゲットにコピーおよび同期する機能。

ソースファイルを **NFS** 共有にコピーしています

データがスキャンしているソースファイルを任意の NFS 共有にコピーできます。NFS 共有をデータセンスト統合する必要はありません。選択したすべてのファイルが「<host_name> : /<share_path>」の形式でコピーされる NFS 共有の名前を知っておく必要があります。



データベースに存在するファイルはコピーできません。

要件

- ファイルをコピーするには、アカウント管理者またはワークスペース管理者の役割が必要です。
- ファイルをコピーするには、デスティネーションの NFS 共有でデータセンスインスタンスからのアクセスが許可されている必要があります。
- 一度にコピーできるファイルの最大数は 100、000 です。

手順

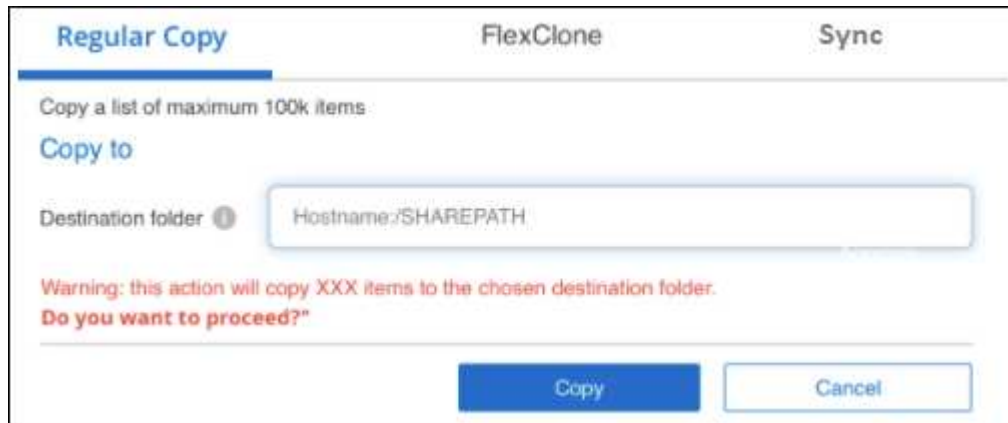
1. [データ調査結果] ペインで、コピーするファイルを選択し、[* コピー] をクリックします。



ページからコピーするファイルを選択する方法と、[コピー] ボタンを示すスクリーンショット。"]

- 個々のファイルを選択するには、各ファイル（☒ Volume_1）。
- 現在のページのすべてのファイルを選択するには、タイトル行（☒ File Name）。
- すべてのページのすべてのファイルを選択するには、タイトル行（☒ File Name）をクリックし、ポップアップメッセージにと入力します **All 20 Items on this page selected Select all Items in list (63K Items)** をクリックし、リスト（xxx 項目）のすべての項目を選択 * をクリックします。

2. _ ファイルのコピー _ ダイアログで * 標準コピー * タブを選択します。



3. 選択したすべてのファイルをコピーする NFS 共有の名前を「<host_name> : /<share_path>`」の形式で入力し、「* Copy *」をクリックします。

コピー処理のステータスを示すダイアログが表示されます。

コピー処理の進捗状況は確認できます [アクションステータス (Actions Status)] パネル。

ファイルのメタデータの詳細を表示するときに、個々のファイルをコピーすることもできます。[ファイルのコピー]をクリックします。



ページのファイルのメタデータ詳細から [ファイルのコピー] ボタンを選択したことを示すスクリーンショット。"]

新しいボリュームへのボリュームデータのクローニング

NetApp_FlexClone_functionality を使用すると、データセンスでスキャンしている既存の ONTAP ボリュームをクローニングできます。これにより、選択したファイルのみを含めて、ボリュームをすばやく複製できます。この機能は、データを移行する際に元のボリュームから特定のファイルを除外する場合や、テスト用にボリュームのコピーを作成する場合に便利です。

新しいボリュームは、ソースボリュームと同じアグリゲート内に作成されます。このタスクを開始する前に、アグリゲート内にこの新しいボリューム用の十分なスペースがあることを確認してください。必要に応じて、ストレージ管理者にお問い合わせください。

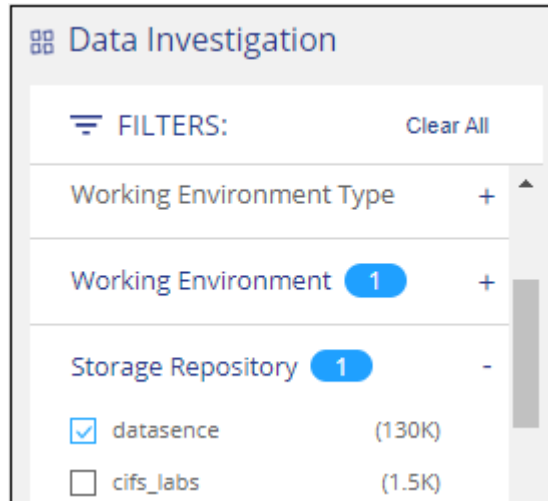
- 注： * FlexGroup ボリュームは FlexClone でサポートされていないため、クローンを作成できません。

要件

- ファイルをコピーするには、アカウント管理者またはワークスペース管理者の役割が必要です。
- 選択したファイルはすべて同じボリュームにあり、ボリュームがオンラインである必要があります。
- ボリュームは、Cloud Volumes ONTAP またはオンプレミスの ONTAP システムから選択する必要があります。他のデータソースは現在サポートされていません。
- クラスタに FlexClone ライセンスがインストールされている必要があります。このライセンスは、Cloud Volumes ONTAP システムにデフォルトでインストールされます。

手順

1. [データ調査] ペインで、1つの * 作業環境 * と1つの * ストレージリポジトリ * を選択してフィルタを作成し、すべてのファイルが同じ ONTAP ボリュームにあることを確認します。



新しいボリュームにクローニングするファイルだけが表示されるように、他のフィルタを適用します。

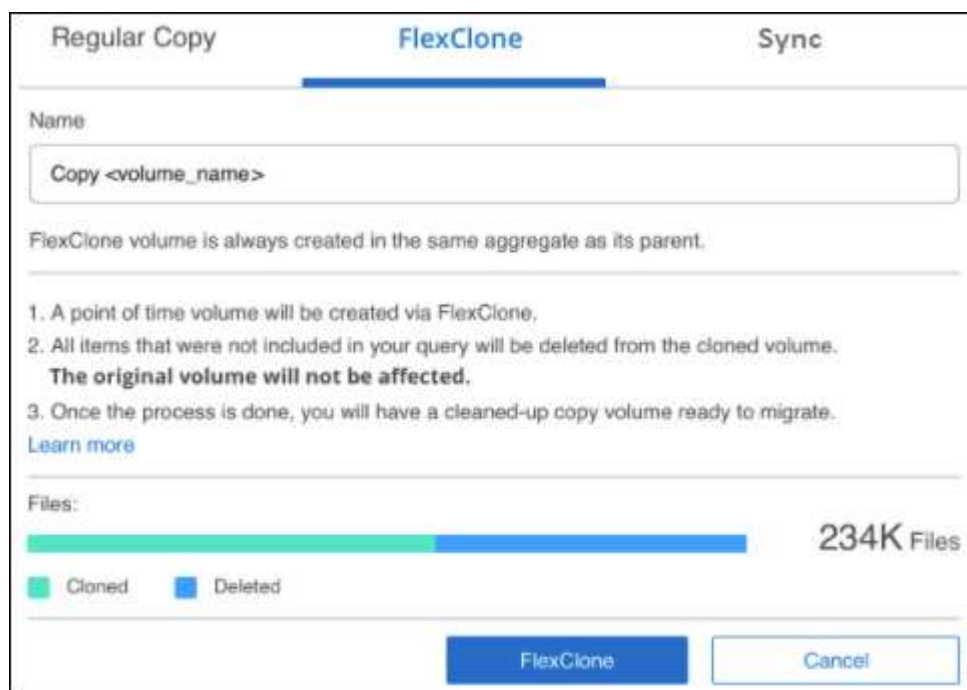
2. [調査結果] ペインで、複製するファイルを選択し、[* コピー *] をクリックします。



ページからコピーするファイルを選択する方法と、[コピー] ボタンを示すスクリーンショット。"]

- 個々のファイルを選択するには、各ファイル (☒ Volume_1)。
- 現在のページのすべてのファイルを選択するには、タイトル行 (☒ File Name)。
- すべてのページのすべてのファイルを選択するには、タイトル行 (☒ File Name) をクリックし、ポップアップメッセージにと入力します [All 20 Items on this page selected](#) [Select all Items in list \(63K Items\)](#) をクリックし、リスト (xxx 項目) のすべての項目を選択 * をクリックします。

3. 「ファイルのコピー」ダイアログで * FlexClone * タブを選択します。このページには、ボリュームからクローニングされるファイル（選択したファイル）の総数と、クローンボリュームに含まれている / 削除されていないファイル（選択しなかったファイル）の数が表示されます。



4. 新しいボリュームの名前を入力し、* FlexClone * をクリックします。

クローン処理のステータスを示すダイアログが表示されます。

新しいクローンボリュームは、ソースボリュームと同じアグリゲート内に作成されます。

クローニング処理の進捗状況は確認できます [[アクションステータス \(Actions Status\)](#)] パネル。

ソースボリュームが存在する作業環境で Data Sense を有効にしたときに、最初に「すべてのボリュームをマップ」または「すべてのボリュームをマップして分類」を選択した場合は、新しいクローンボリュームが自動的にスキャンされます。最初にこれらのいずれかを使用しなかった場合は、この新しいボリュームをスキャンする必要があります ["ボリュームのスキャンを手動で有効にします"](#)。

ソース・ファイルをターゲット・システムにコピーして同期する

データがスキャンしているソースファイルを、サポートされていない非構造化データソースから特定のターゲットの場所にあるディレクトリにコピーできます ("[Cloud Sync でサポートされるターゲットの場所](#)")。最初のコピー後、ファイル内で変更されたデータは、設定したスケジュールに基づいて同期されます。

これは、あるソースシステムから別のシステムにデータを移行する場合に便利です。このアクションではを使用します ["NetApp Cloud Sync の略"](#) データをソースからターゲットにコピーおよび同期する機能。



データベース、OneDrive アカウント、SharePoint アカウントにあるファイルはコピーおよび同期できません。

要件

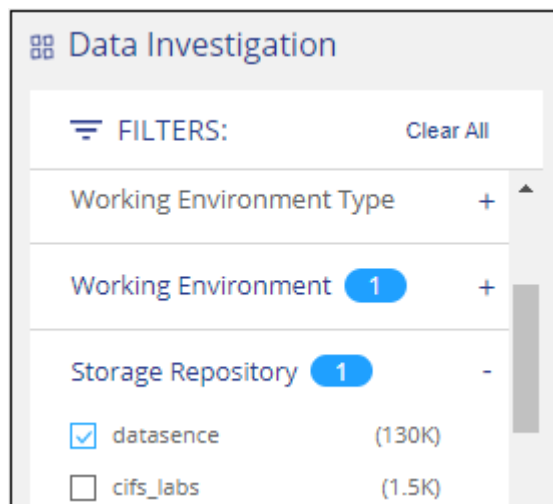
- ファイルをコピーして同期するには、アカウント管理者またはワークスペース管理者の役割が必要です。

- 選択したファイルはすべて、同じソースリポジトリ（ONTAP ボリューム、S3 バケット、NFS 共有、CIFS 共有など）にある必要があります。
- 一度にコピーできるファイルの最大数は 20、000 です。
- Cloud Sync サービスをアクティブ化し、少なくとも 1 つのデータブローカーを構成して、ソースシステムとターゲットシステム間でファイルを転送できるようにする必要があります。から、Cloud Sync の要件を確認します ["Quick Start 概要 の略"](#)。

Cloud Sync サービスでは同期関係のサービス料金が別途請求されるため、データブローカーをクラウドに導入するとリソース料金が発生することに注意してください。

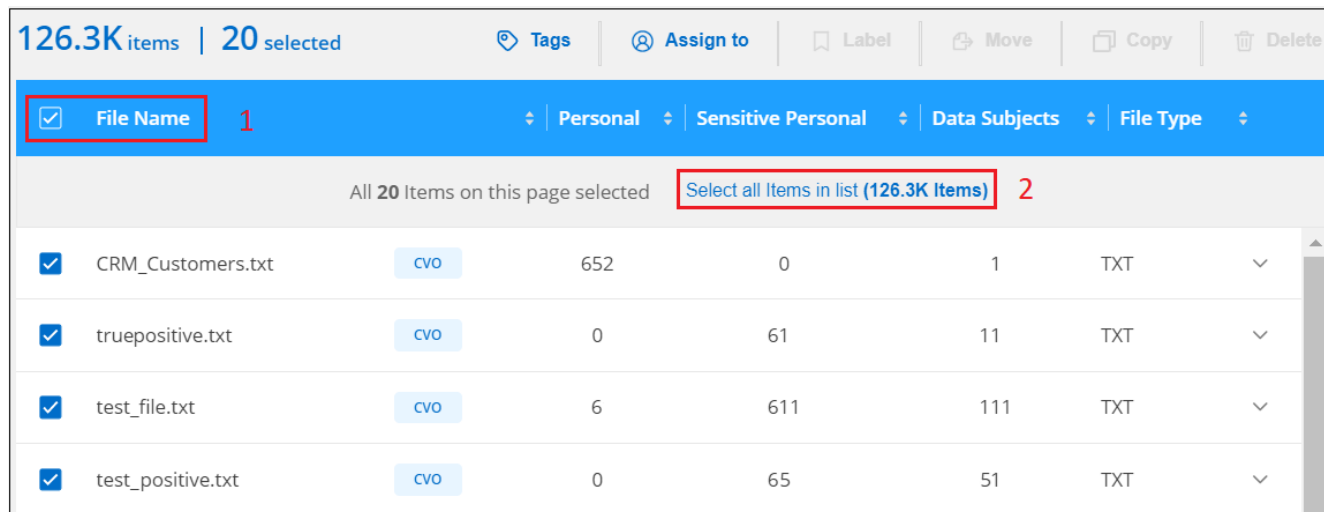
手順

1. [データの調査] ペインで、1 つの * 作業環境 * と 1 つの * ストレージリポジトリ * を選択してフィルタを作成し、すべてのファイルが同じリポジトリにあることを確認します。



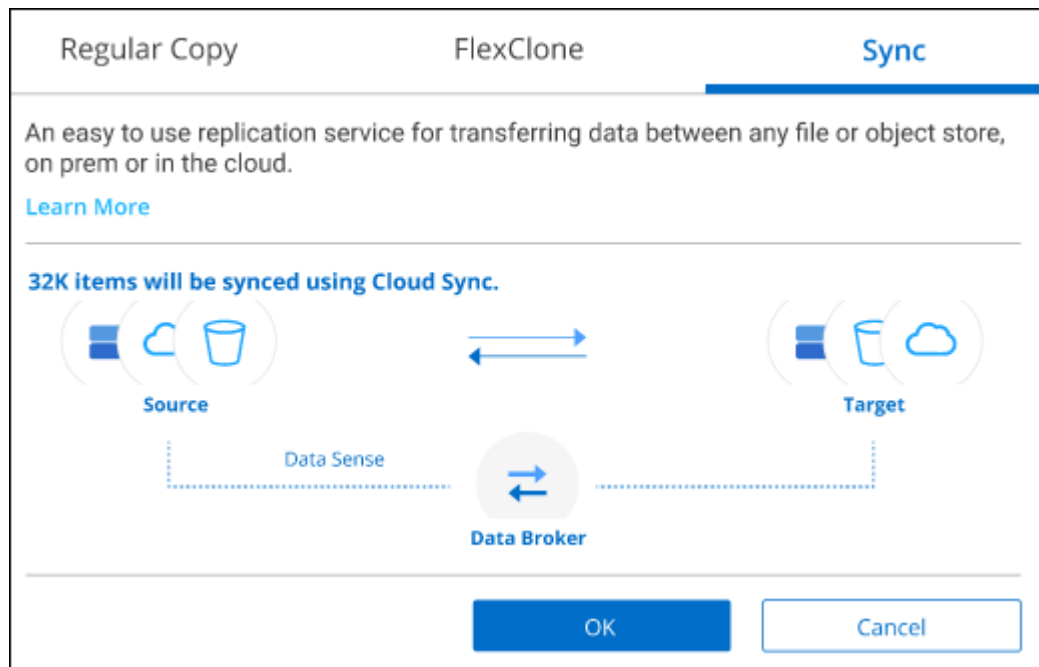
他のフィルタを適用して、コピー先システムに同期するファイルだけが表示されるようにします。

2. [調査結果] ウィンドウ枠で、タイトル行のボックスをオンにして、すべてのページのすべてのファイルを選択します（☒ **File Name**）をクリックし、ポップアップメッセージに入力します
All 20 Items on this page selected [Select all Items in list \(63K Items\)](#) [リスト内のすべての項目を選択（* xxx 項目）]
をクリックし、[* コピー *] をクリックします。



ページからコピーするファイルを選択する方法と、[コピー]ボタンを示すスクリーンショット。"]

3. _ファイルのコピー_ ダイアログで * 同期 * タブを選択します。



ダイアログを示すス

クリーンショットで、[同期]オプションを選択できます。"]

4. 選択したファイルを保存先に同期してもよい場合は、「* OK *」をクリックします。

Cloud Sync UI が Cloud Manager で開きます。

同期関係を定義するよう求められます。ソースシステムは、データセンスで選択したリポジトリとファイルに基づいてあらかじめ設定されています。

5. ターゲットシステムを選択し、使用するデータブローカーを選択（または作成）する必要があります。から、Cloud Sync の要件を確認します "[Quick Start 概要の略](#)"。

ファイルはターゲットシステムにコピーされ、定義したスケジュールに基づいて同期されます。1 回限りの同期を選択した場合、ファイルは 1 回だけコピーされ、同期されます。定期的な同期を選択した場合は、スケジュールに基づいてファイルが同期されます。フィルタを使用して作成したクエリに一致する新しいファイルがソースシステムによって追加されると、これらの _new_files がコピー先にコピーされ、後で同期されることに注意してください。

通常の Cloud Sync 操作の一部は、Data Sense から呼び出されたときに無効になっている点に注意してください。

- ・「ソース上のファイルを削除」または「ターゲット上のファイルを削除」ボタンは使用できません。
- ・レポートの実行が無効になっています。

ソースファイルを **NFS** 共有に移動しています

データがスキャンしているソースファイルを任意の NFS 共有に移動できます。NFS 共有をデータセンスと統合する必要はありません（を参照） "[ファイル共有をスキャンしています](#)"）。



データベースに存在するファイルは移動できません。

ファイルを移動するには、アカウント管理者またはワークスペース管理者の役割が必要です。

ファイルを移動するには、NFS 共有でデータセンシブインスタンスからのアクセスが許可されている必要があります。

手順

1. [データ調査結果] ペインで、移動するファイルを選択します。

2345 items

 Tags

 Assign to

 Label

 Copy

 Move

 Delete

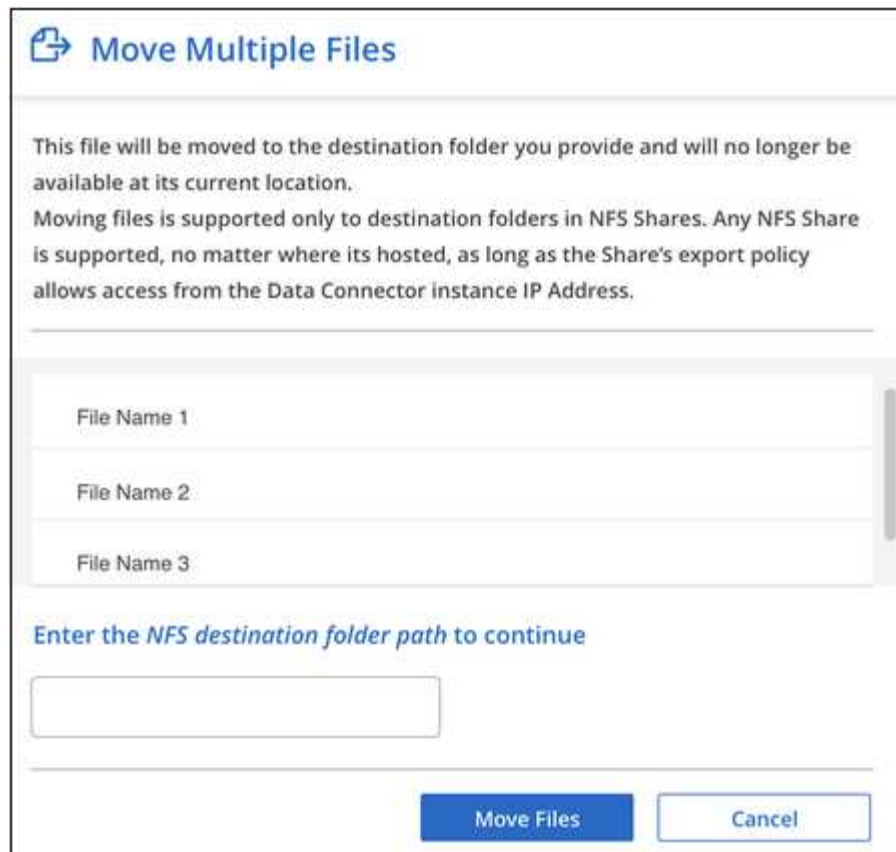
| <input type="checkbox"/> | File Name | Personal | Sensitive Personal | Data Subjects | File Type | |
|-------------------------------------|-------------------------------------|----------|--------------------|---------------|-----------|-----|
| <input checked="" type="checkbox"/> | Expense Report EXP-TPO-106038887654 | cvo | 6 | 3 | 16 | PDF |
| <input checked="" type="checkbox"/> | Expense Report EXP-TPO-106038887654 | cvo | 6 | 3 | 6 | PDF |
| <input type="checkbox"/> | Expense Report EXP-TPO-106038887654 | cvo | 6 | 3 | 6 | PDF |
| <input type="checkbox"/> | Expense Report EXP-TPO-106038887654 | cvo | 6 | 3 | 6 | PDF |

ページから [移動] ボタンをクリックします。"]

。個々のファイルを選択するには、各ファイル (☒ Volume_1) 。

。現在のページのすべてのファイルを選択するには、タイトル行 (☒ File Name) 。

2. ボタンバーで、 * 移動 * をクリックします。



Move Multiple Files

This file will be moved to the destination folder you provide and will no longer be available at its current location.

Moving files is supported only to destination folders in NFS Shares. Any NFS Share is supported, no matter where its hosted, as long as the Share's export policy allows access from the Data Connector instance IP Address.

File Name 1

File Name 2

File Name 3

Enter the NFS destination folder path to continue

Move Files Cancel

3. 「ファイルの移動」ダイアログで「選択したすべてのファイルを移動する NFS 共有の名前を '< ホスト名>:/<share_path>' の形式で入力し「* ファイルの移動 *」をクリックします

ファイルのメタデータの詳細を表示するときに、個々のファイルを移動することもできます。「* ファイルを移動 *」をクリックします。



Unstructured (32K Files) | Structured (323 DB Tables)

| File Name | Personal | Sensitive Personal | Data Subjects | File Type |
|---|----------|--------------------|---------------|-----------|
| <input type="checkbox"/> Expense Report EXP-TPO-1060388765435 | 6 | 3 | 16 | PDF |
| <input type="checkbox"/> Expense Report EXP-TPO-1060388765435 | 6 | 3 | 16 | PDF |

Working Environment: WorkingEnvironment1

Repository: Volume Name

File Path: /Prod/labs-base/Expense Report EXP-TPO-1060388.pdf

Assign a Label to this file

Move File

Copy File

ページのファイルのメタデータ詳細から「ファイルの移動」ボタンを選択したことを示すスクリーンショット。"]

ソースファイルを削除しています

ストレージ・システムに残すのに安全でない、またはリスクが高すぎるソース・ファイルを完全に削除したり、重複として識別したソース・ファイルを削除したりすることができますこの操作は永続的であり、元に戻すことも復元することもできません。

「調査」ペインから手動でファイルを削除することも、「ポリシー」を使用して自動的にファイルを削除

することもできます



データベースに存在するファイルは削除できません。

ファイルを削除するには、次の権限が必要です。

- NFS データ-書き込み権限でエクスポートポリシーを定義する必要があります。
- CIFS データ-CIFS クレデンシャルには書き込み権限が必要です。
- S3 データの場合 - IAM ロールに次の権限を含める必要があります。「3 : DeleteObject」

ソースファイルを手動で削除しています

要件

- ファイルを削除するには、アカウント管理者またはワークスペース管理者の役割が必要です。
- 一度に削除できるファイルの最大数は 100、000 です。

手順

1. [データ調査結果] ペインで、削除するファイルを選択します。



ページの [削除] ボタン。"]

- 個々のファイルを選択するには、各ファイル (☒ Volume_1) 。
- 現在のページのすべてのファイルを選択するには、タイトル行 (☒ File Name) 。
- すべてのページのすべてのファイルを選択するには、タイトル行 (☒ File Name) をクリックし、ポップアップメッセージにと入力します **All 20 Items on this page selected** **Select all Items in list (63K Items)** をクリックし、リスト (xxx 項目) のすべての項目を選択 * をクリックします。

2. ボタンバーで、* 削除 * をクリックします。

3. 削除操作は永続的であるため、後続の _Delete File_Dialog に「* permanently delete *」と入力し、* ファイルの削除 * をクリックする必要があります

削除処理の進捗状況は確認できます [[アクションステータス \(Actions Status \)](#)] パネル。

ファイルのメタデータの詳細を表示するときに、個々のファイルを削除することもできます。[ファイルの削除] をクリックします。



ページのファイルのメタデータ詳細から [ファイルの削除] ボタンを選択したことを示すスクリーンショット。"]

ポリシーを使用してソースファイルを自動的に削除します

カスタムポリシーを作成して、ポリシーに一致するファイルを削除できます。たとえば、過去 30 日間にデータセンサで検出された機密情報を含むファイルを削除できます。

ファイルを自動的に削除するポリシーを作成できるのはアカウント管理者だけです。



ポリシーに一致するすべてのファイルは、1 日に 1 回完全に削除されます。

手順

1. [データ調査] ページで、使用するすべてのフィルタを選択して検索を定義します。を参照してください "[[データ調査](#) ページでデータをフィルタリングします"] を参照してください。
2. 必要な方法でフィルタ特性をすべて設定したら、[この検索からポリシーを作成する *] をクリックします。
3. ポリシーに名前を付け、そのポリシーで実行できるその他のアクションを選択します。
 - a. 一意の名前と説明を入力します。
 - b. このポリシーに一致するファイルを自動的に削除する] チェックボックスをオンにし、「* permanently delete *」と入力して、このポリシーによってファイルが完全に削除されることを確認します。
 - c. [ポリシーの作成 *] をクリックします。

Create Policy

This will create a new Policy according to the current selected filters and search term.
You can view or delete this later from the "Policies" tab.

Note it may take up to 15 minutes for results to be displayed for a new Policy.

Name this Policy

Delete files with sensitive data

Give it a detailed description that explains what it searches for

Delete files that contain sensitive information and that were discovered in the past 30 days

☒ Automatically delete files that match this policy (Every Day)

Type "permanently delete" to continue with the deletion.

permanently delete

☐ Send email updates about this Policy to Cloud Manager users on this account every Day

☐ Automatically label this Policy's matches with: Select a label

Create Policy Cancel

[ポリシー] タブに新しいポリシーが表示されます。ポリシーに一致するファイルは、ポリシーの実行時に 1 日に 1 回削除されます。

で削除されたファイルのリストを確認できます [[アクションステータス \(Actions Status \)](#)] パネル。

コンプライアンスアクションのステータスを表示します

たとえば、100 個のファイルを削除するなど、多くのファイルで [調査結果] ペインからアクションを実行すると、プロセスに時間がかかることがあります。これらの非同期アクションのステータスは、_Action Status_Pane で監視できるので、すべてのファイルにいつ適用されたかを知ることができます。これにより、正常に完了した操作、現在実行中の操作、および失敗した操作を確認できるため、問題を診断して修正できます。

ステータスは次のいずれかになります。

- 完了しました
- 実行中です
- キューに登録され
- キャンセルされました

- 失敗しました

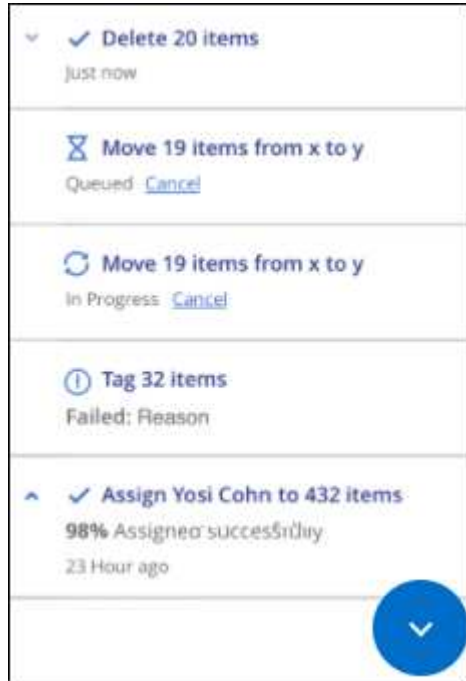
ステータスが「Queued」または「In Progress」のアクションはすべてキャンセルできます。

手順

1.

データセンス UI の右下には、* アクションステータス * ボタンが表示されます .

2. このボタンをクリックすると、最新の 20 件のアクションが表示されます。



アクションの名前をクリックすると、その操作に対応する詳細を表示できます。

Data Fusion を使用して個人データ識別子を追加する

Data Fusion では ' 企業のデータをスキャンして ' データベースから一意の識別子がファイルまたはその他のデータベースで見つかったかどうかを確認できます基本的には ' クラウドデータ検出スキャンで識別される個人データの一覧を作成しますこれにより、機密データが存在する可能性のある場所に関する全体像が _all_your ファイルに表示されます。

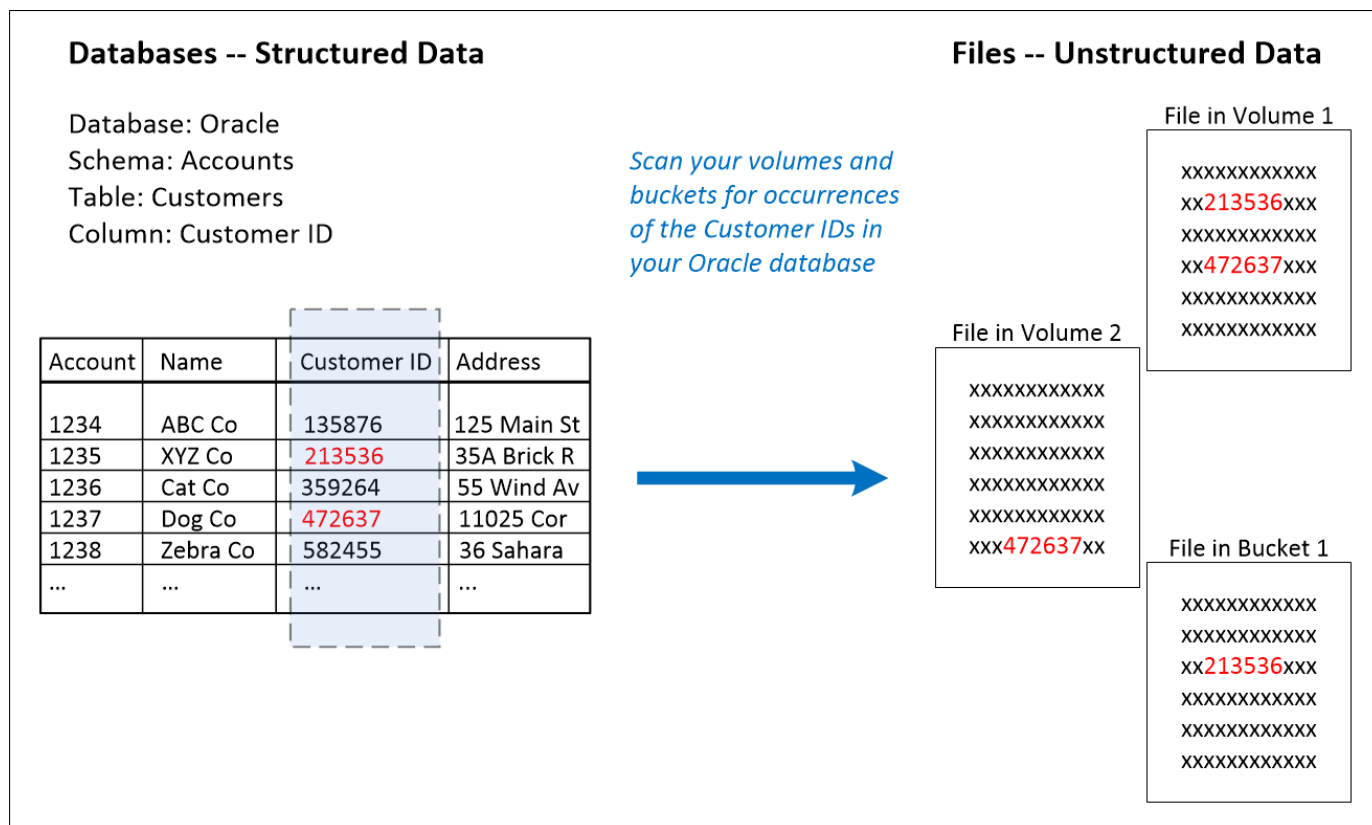
独自のデータベースをスキャンするので、データが保存されている言語に関係なく、将来の Cloud Data Sense スキャンでデータを識別するために使用されます。



このセクションで説明する機能は、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。

データベースからカスタムの個人データ識別子を作成する

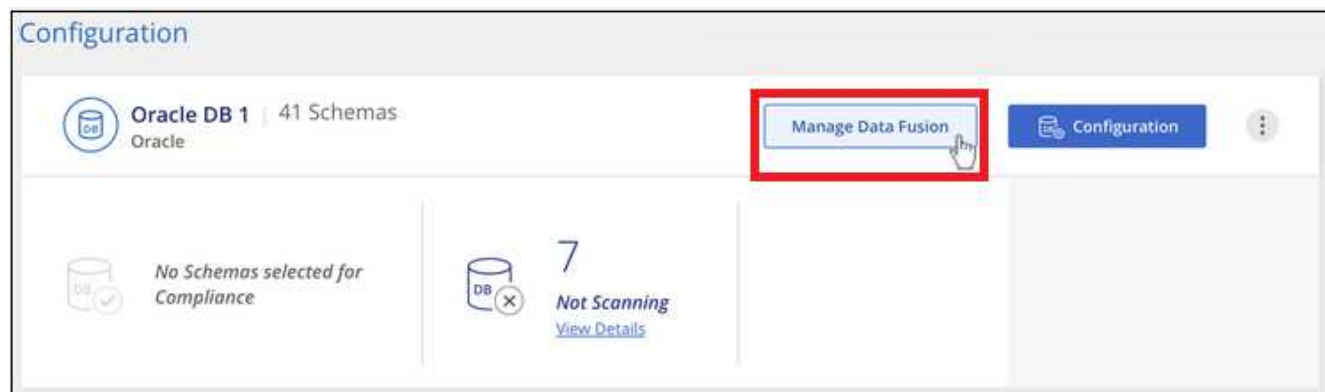
データベーステーブルで特定の列を選択することにより、クラウドデータセンスがスキャンで検索する追加の識別子を選択できます。たとえば、次の図は、データ Fusion を使用してボリューム、バケット、およびデータベースをスキャンし、Oracle データベースからすべての顧客 ID が出現する状況を示しています。



このように、2つのボリュームと1つのS3バケットにそれぞれ一意の顧客IDが見つかりました。データベーステーブル内の一致も識別されます。

が必要です "データベースサーバを少なくとも1つ追加しました" データ Fusion ソースを追加する前にクラウドデータを検出

1. [構成] ページで、ソースデータが存在するデータベースの [データ Fusion の管理] 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。"]

2. 次のページで [Add Data Fusion source*] をクリックします。

3. [Add Data Fusion Source_] ページで、次の手順を実行します。
- a. ドロップダウンメニューからデータベーススキーマを選択します。
 - b. そのスキーマにテーブル名を入力します。
 - c. 使用する一意の識別子を含む列を入力します。

複数の列を追加する場合は、各列名またはテーブルビュー名を別々の行に入力します。

Add Data Fusion Source

To add a Data Fusion source reference, specify one or more columns which contain your organization's unique identifiers, such as a column used to store customer IDs. Note that adding a Data Fusion Source will initiate an additional scan of your data stores

Database Schema: Oracle1,Accounts Table: Customers

Columns Containing Identifiers: Customer ID

Add Data Fusion Source Cancel

4. [Add Data Fusion Source*] をクリックします。

Data Fusion インベントリページには、クラウドデータセンスでスキャンするように設定したデータベースソース列が表示されます。

| Database Schema | Table | Data Fusion Source Columns |
|-----------------|---------|---------------------------------|
| SchemaName1 | Table 1 | Column 12, Column 14, Column 18 |
| SchemaName2 | Table 2 | Column 12, Column 14, Column 18 |

次のスキャンの後、この新しい情報は、[個人] 結果セクションの [ダッシュボード]、[個人データ] フィルタの [調査] ページに表示されます。追加した各ソース・カラムは 'フィルタ・リストに "Table.column" として表示されますたとえば 'Customers .Customer ID' のように表示されます

Data Fusion ソースの削除

特定の Data Fusion ソースを使用してファイルをスキャンしない場合は、Data Fusion インベントリページからソース行を選択し、[* データ Fusion ソースの削除 *] をクリックします。



コンプライアンスレポートの表示

Cloud Data Sense は、組織のデータプライバシープログラムの状況をよりよく把握するために使用できるレポートを提供します。

デフォルトでは、Cloud Data Sense ダッシュボードには、すべての作業環境およびデータベースのコンプライアンスデータとガバナンスデータが表示されます。一部の作業環境のデータのみを含むレポートを表示する場合は、[それらの作業環境を選択します](#)。



このセクションで説明するレポートは、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピング専用スキャンを実行したデータソースでは、データマッピングレポートのみが生成されます。



ネットアップでは、Cloud Data Sense が特定した個人データと機密性の高い個人データの正確性を 100% 保証することはできません。必ずデータを確認して情報を検証してください。

プライバシーリスク評価レポート

プライバシーリスクアセスメントレポートには、GDPR や CCPA などのプライバシー規制に必要な、組織のプライバシーリスクステータスの概要が記載されています。このレポートには次の情報が含まれます。

準拠ステータス

A [重要度スコア](#) 機密性、個人、機密性の高い個人のいずれであっても、データの配信は可能です。

評価の概要

検出された個人データの種類とデータのカテゴリの内訳。

この評価のデータ主体

国 ID が見つかった場所別の人の数。

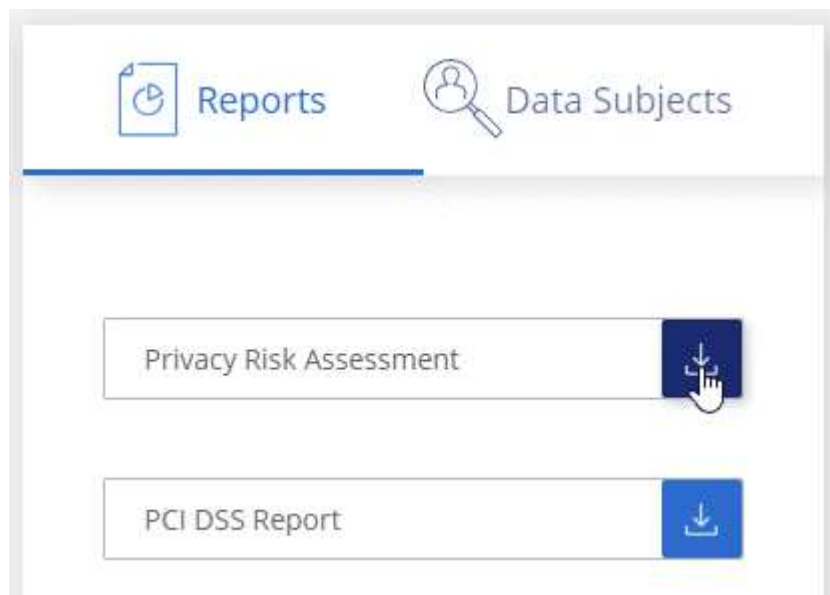
プライバシーリスク評価レポートの生成

[データセンス] タブに移動してレポートを生成します。

手順

1. Cloud Manager の上部で、* Data Sense * をクリックします。
2. [Compliance] をクリックし、[*Reports] の下にある [*Privacy Risk Assessment] の横にあるダウングレード

ードアイコンをクリックします。



Cloud Data Sense は、必要に応じて他のグループにレビューして送信できる PDF レポートを生成します。

重要度スコア

Cloud Data Sense は、プライバシーリスク評価レポートの重要度スコアを次の 3 つの変数に基づいて計算します。

- すべてのデータの個人データの割合。
- すべてのデータの機密性の高い個人データの割合。
- データ主体を含むファイルの割合。国 ID、社会保障番号、税務 ID 番号などの国 ID によって決定されます。

スコアの決定に使用されるロジックは次のとおりです。

| 重要度スコア | ロジック |
|--------|----------------------|
| 0 | 3 つの変数はすべて 0% です |
| 1. | 変数の 1 つが 0% を超えています |
| 2. | 変数の 1 つが 3% を超えています |
| 3. | 2 つの変数が 3% を超えています |
| 4. | 3 つの変数が 3% を超えています |
| 5. | 変数の 1 つが 6% を超えています |
| 6. | 2 つの変数が 6% を超えています |
| 7. | 3 つの変数が 6% を超えています |
| 8. | 変数の 1 つが 15% を超えています |
| 9. | 2 つの変数が 15% を超えています |

| | |
|--------|---------------------|
| 重要度スコア | ロジック |
| 10. | 3 つの変数が 15% を超えています |

PCI DSS レポート

Payment Card Industry Data Security Standard（PCI DSS）Report は、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。このレポートには次の情報が含まれます。

概要

クレジットカード情報を含むファイル数と、作業環境。

暗号化

暗号化された作業環境または暗号化されていない作業環境にあるクレジットカード情報を含むファイルの割合。この情報は Cloud Volumes ONTAP に固有のものです。

ランサムウェアからの保護

ランサムウェアからの保護が有効になっている、または有効になっていない作業環境でのクレジットカード情報を含むファイルの割合。この情報は Cloud Volumes ONTAP に固有のものです。

保持

ファイルが最後に変更された期間。これは、クレジットカード情報を処理するよりも長く保持する必要があるために役立ちます。

クレジットカード情報の配布

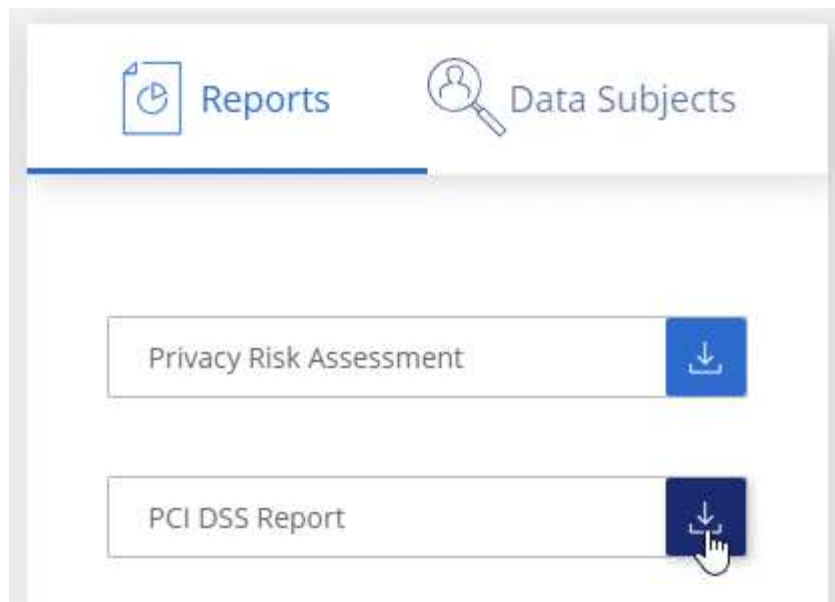
クレジットカード情報が見つかった作業環境、および暗号化とランサムウェアによる保護が有効になっているかどうか。

PCI DSS レポートの生成

[データセンス] タブに移動してレポートを生成します。

手順

1. Cloud Manager の上部で、* Data Sense * をクリックします。
2. [* コンプライアンス *] をクリックし、[レポート] の下の [* PCI DSS レポート *] の横にあるダウンロード・アイコンをクリックします。



Cloud Data Sense は、必要に応じて他のグループにレビューして送信できる PDF レポートを生成します。

HIPAA レポート

Health Insurance Portability and Accountability Act（HIPAA：医療保険の携行性と責任に関する法律）レポートは、健康に関する情報を含むファイルを特定するのに役立ちます。このポリシーは、HIPAA データプライバシー法に準拠するという組織の要件を支援するように設計されています。Cloud Data Sense が探している情報には、次のものがあります。

- ヘルス参照パターン
- ICD-10-CM 医療コード
- ICD-9-CM 医療コード
- HR –健全性カテゴリ
- ヘルスアプリケーションデータカテゴリ

このレポートには次の情報が含まれます。

概要

ヘルス情報が含まれているファイルの数と、作業環境。

暗号化

暗号化された作業環境または暗号化されていない作業環境にあるヘルス情報を含むファイルの割合。この情報は Cloud Volumes ONTAP に固有のものです。

ランサムウェアからの保護

ランサムウェアからの保護が有効になっている、または有効になっていない作業環境でのヘルス情報を含むファイルの割合。この情報は Cloud Volumes ONTAP に固有のものです。

保持

ファイルが最後に変更された期間。健全性の情報は、処理するまでに時間がかかることがないため、この方法が便利です。

健康情報の配布

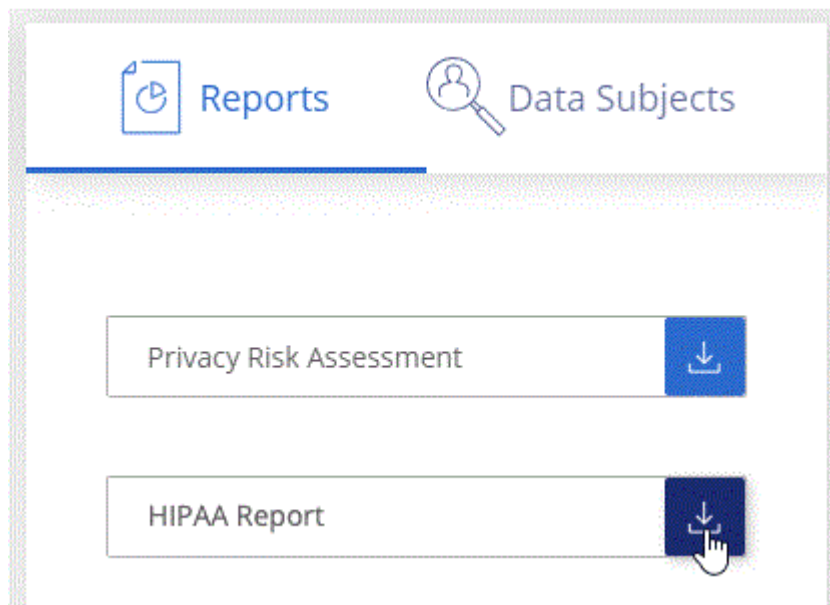
健全性の情報が見つかった作業環境、および暗号化とランサムウェアによる保護が有効になっているかどうか。

HIPAA レポートの生成

[データセンス] タブに移動してレポートを生成します。

手順

1. Cloud Manager の上部で、 * Data Sense * をクリックします。
2. **[Compliance]** をクリックし、 **[*Reports]** の下にある **[HIPAA Report]** の横にあるダウンロードアイコンをクリックします。



Cloud Data Sense は、必要に応じて他のグループにレビューして送信できる PDF レポートを生成します。

データマッピングレポート

データマッピングレポートには、企業データソースに保存されているデータの概要が表示され、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の決定に役立ちます。最初に、すべての作業環境とデータソースをまとめた概要レポートが表示され、それぞれの作業環境の内訳が表示されます。

このレポートには次の情報が含まれます。

使用容量

すべての作業環境：各作業環境のファイル数と使用済み容量が表示されます。単一の作業環境の場合：容量が最も多いファイルが表示されます。

データの経過時間

ファイルが作成されたとき、最終変更されたとき、または最後にアクセスされたときのグラフとグラフが 3 つ表示されます。特定の日付範囲に基づいて、ファイル数とその使用済み容量が表示されます。

データのサイズ

作業環境の特定のサイズ範囲内に存在するファイルの数を示します。

ファイルの種類

作業環境に保存されているファイルタイプごとのファイルの総数と使用容量が表示されます。

データマッピングレポートの生成

[データセンス] タブに移動してレポートを生成します。

手順

1. Cloud Manager の上部で、* Data Sense * をクリックします。
2. [* Governance (ガバナンス)] をクリックし、[Governance Dashboard] から [* Full Data Mapping Overview Report] ボタンをクリックします。



Cloud Data Sense は、必要に応じて他のグループにレビューして送信できる PDF レポートを生成します。

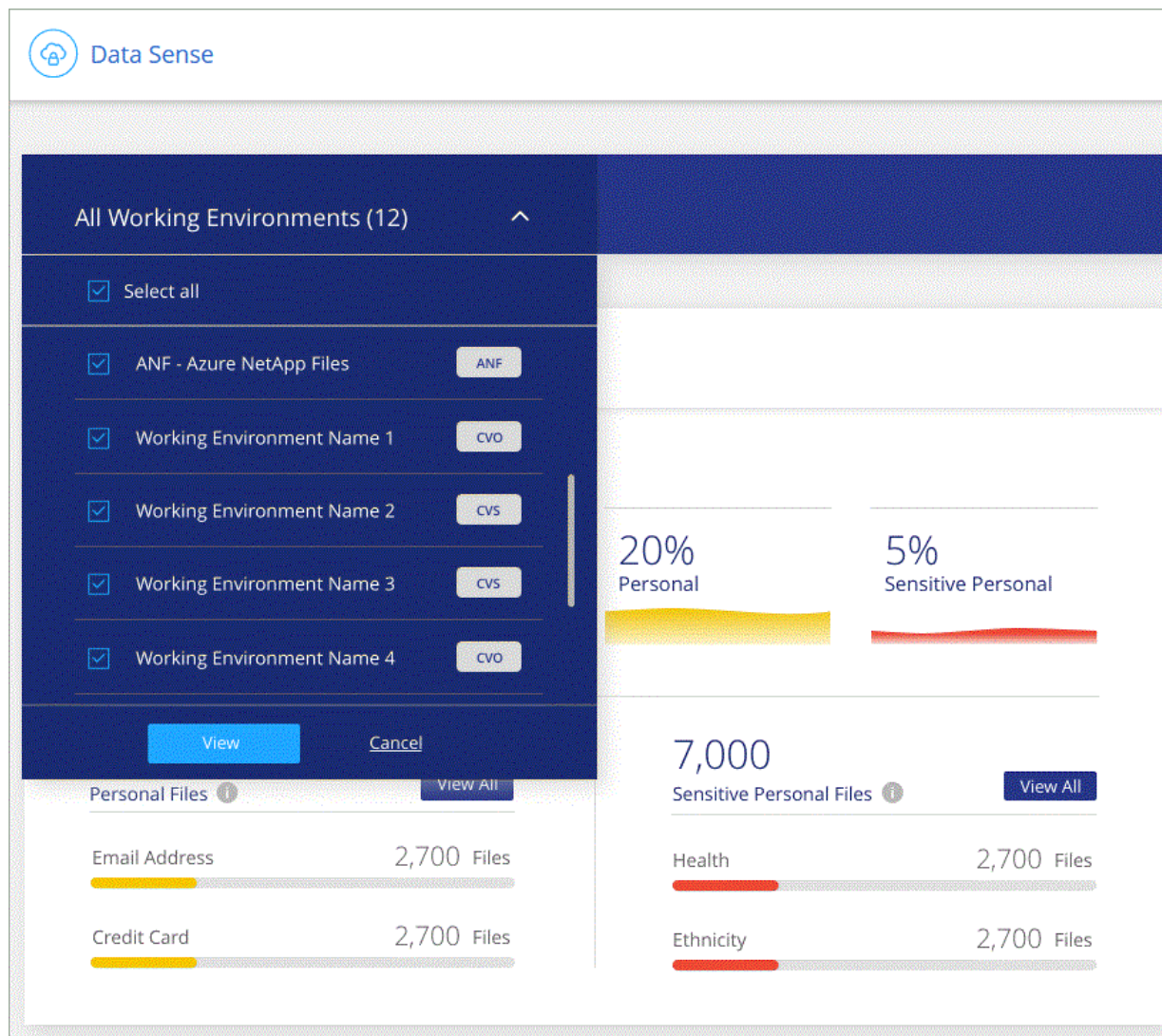
レポートの作業環境を選択する

Cloud Data Sense Compliance ダッシュボードの内容をフィルタリングして、すべての作業環境とデータベース、または特定の作業環境のコンプライアンスデータを表示できます。

ダッシュボードをフィルタすると、Data Sense によって、選択した作業環境だけにコンプライアンスデータとレポートがスコープされます。

手順

1. フィルタドロップダウンをクリックし、データを表示する作業環境を選択して、* 表示 * をクリックします。



データ主体アクセス要求に応答します

データ主体アクセス要求（dsar）に応答するには、件名のフルネームまたは既知の識別子（電子メールアドレスなど）を検索し、レポートをダウンロードします。このレポートは、企業が GDPR や同様のデータプライバシー法を遵守する必要がある場合に役立つように作成されています。



dsar 機能は、データソースで完全な分類スキャンを実行するように選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。



ネットアップでは、Cloud Data Sense が特定した個人データと機密性の高い個人データの正確性を 100% 保証することはできません。必ずデータを確認して情報を検証してください。

データ主体アクセス要求とは

欧州 GDPR などのプライバシー規制により、データ主体（お客様や従業員など）は個人データにアクセスする権利が付与されます。データ主体がこの情報を要求すると、これは dsar（データ主体アクセス要求）と呼ば

れます組織は、これらの要求に「期日前に」、受領後 1 か月以内に対応する必要があります。

クラウドデータの意味は、どのようにして **dsar** に対応するのに役立ちますか？

データ主体検索を実行すると、そのユーザの名前または ID が含まれているすべてのファイル、バケット、OneDrive、SharePoint アカウントが検出されます。データセンスは、最新のインデックス付きデータの名前または識別子をチェックします。新しいスキャンは開始されません。

検索が完了したら、Data Subject Access Request レポートのファイルリストをダウンロードできます。このレポートでは、データから得た情報を集約して、利用者に返すことができる法的条件にします。



現時点では、データベース内でのデータの件名検索はサポートされていません。

データ主体の検索とレポートのダウンロード

データ主体のフルネームまたは既知の識別子を検索し、ファイルリストレポートまたは dsar レポートをダウンロードします。で検索できます ["個人情報の種類"](#)。

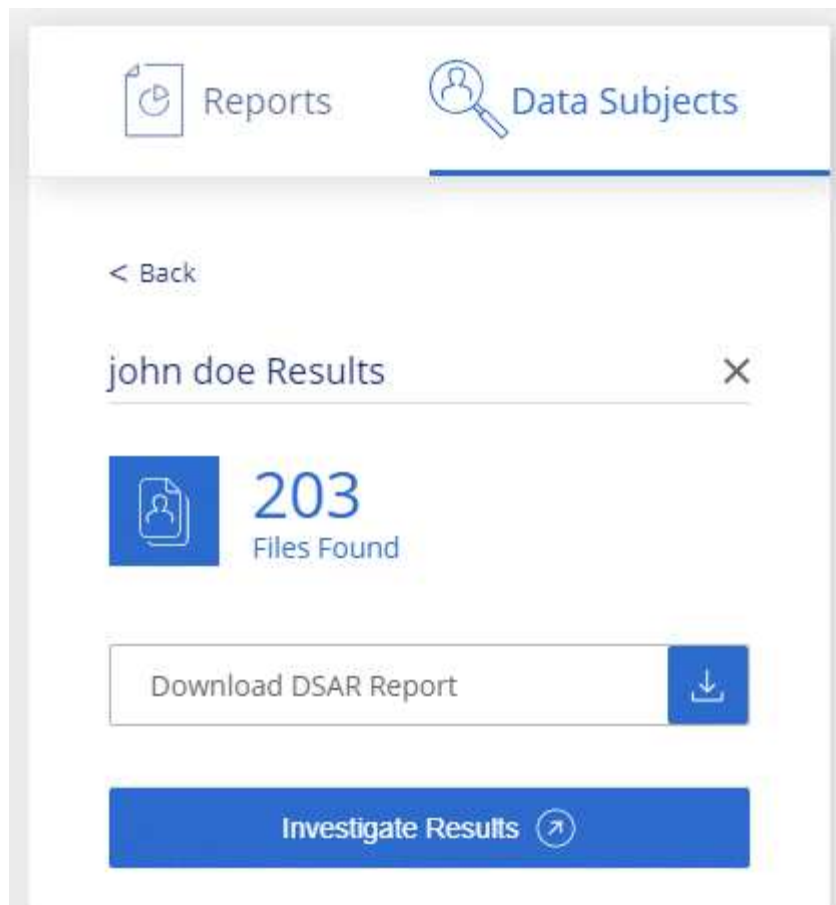


英語、ドイツ語、スペイン語は、データ主体の名前を検索する場合にサポートされています。言語のサポートは、あとで追加されます。

手順

1. Cloud Manager の上部で、* Data Sense * をクリックします。
2. [* データ主体 *] をクリックします。
3. データ主体のフルネームまたは既知の識別子を検索します

次の例では、name *John doe*: を検索しています。



4. 次のいずれかのオプションを選択します。

- **Download dsar Report:** アクセス要求に対する正式な応答で、データ主体に送信できます。このレポートには、クラウドデータが対象とするデータに基づいて自動的に生成された情報が含まれており、テンプレートとして使用するよう設計されています。データ主体に送信する前に、フォームに必要事項を記入して内部で確認してください。
- * 調査結果 * : 特定のファイルの検索、ソート、詳細の展開、およびファイルリストのダウンロードによってデータを調査できるページ。



10、000 件を超える結果がある場合は、ファイルリストに上位 10、000 件のみが表示されます。

プライベートデータのカテゴリ

Cloud Data Sense がボリューム、Amazon S3 バケット、データベース、OneDrive フォルダ、SharePoint アカウントで識別できるプライベートデータには、さまざまな種類があります。以下のカテゴリを参照してください。



その他の国の ID 番号や医療機関の ID など、プライベートデータの種類を識別するためにクラウドデータセンスが必要な場合は、ng-contact-data-sense@netapp.com にリクエストを送信してください。

個人データの種類

ファイルに含まれる個人データは、一般的な個人データまたは国 ID です。3 番目の列は、Cloud Data Sense で使用されているかどうかを示します ["近接性検証"](#) 識別子の調査結果を検証します。

このカテゴリの項目は、どの言語でも認識できます。

データベースサーバーをスキャンする場合は、ファイル内にある個人データのリストに追加できます。Data Fusion 機能を使用すると、データベーステーブルの列を選択して、クラウドデータ検出でスキャンで検索する追加の識別子を選択できます。を参照してください ["Data Fusion を使用して個人データ識別子を追加する"](#) を参照してください。

| を入力します | 識別子 | 近接性検証： |
|--------|-------------------|--------|
| 全般 | E メールアドレス | いいえ |
| | クレジットカード番号 | いいえ |
| | IBAN 番号（国際銀行口座番号） | いいえ |
| | IP アドレス | いいえ |
| | パスワード | はい。 |

| | | |
|--------|-----|--------|
| を入力します | 識別子 | 近接性検証： |
| 国家識別番号 | | |
| | | |

| | | |
|--------|---|--------|
| | ルクセンブルク ID | はい。 |
| | マルタ ID | はい。 |
| を入力します | 識別番号 National Health Service （ NHS ） 番号 | 接続性検証： |
| | ポーランド ID （ PESEL ） | はい。 |
| | ポルトガル語税識別番号 （ NIF ） | はい。 |
| | ルーマニア語 ID （ CNP ） | はい。 |
| | スロベニア語 ID （ EMSO ） | はい。 |
| | 南アフリカ ID | はい。 |
| | スペイン語税識別番号 | はい。 |
| | スウェーデン語 ID | はい。 |
| | 英国ID （ ニーノ ） | はい。 |
| | 米国社会保障番号 （ SSN ） | はい。 |

機密性の高い個人データのタイプ

Cloud Data Sense がファイル内で検出できる機密性の高い個人データには、次のリストが含まれています。このカテゴリの項目は、現時点では英語でのみ認識されます。

刑事手続きの参照

天然人の犯罪に関するデータ。

『民族リファレンス』を参照してください

自然な人の人種または民族の起源に関するデータ。

健全性リファレンス

自然な人の健康に関するデータ。

ICD-9-CM Medical Codes

医療および医療業界で使用されるコード。

ICD-10-CM Medical Codes

医療および医療業界で使用されるコード。

哲学の信仰の参照

自然な人の哲学的信念に関するデータ。

政治的見解参照

自然な人の政治的意見に関するデータ。

宗教的信条参照

自然な人の宗教的信条に関するデータ。

性別生命または方向の参照

自然人の性生活や性的指向に関するデータ。

カテゴリのタイプ

Cloud Data Sense は、次のようにデータを分類します。これらのカテゴリのほとんどは、英語、ドイツ語、スペイン語で認識されます。

| カテゴリ | を入力します | 英語 | ドイツ語 | スペイン語 |
|---------|----------------|----|------|-------|
| 財務 | 貸借対照表 | ✓ | ✓ | ✓ |
| | 注文書 | ✓ | ✓ | ✓ |
| | 請求書 | ✓ | ✓ | ✓ |
| | 四半期ごとのレポート | ✓ | ✓ | ✓ |
| 時間 | バックグラウンドチェック | ✓ | | ✓ |
| | 報酬プラン | ✓ | ✓ | ✓ |
| | 従業員の契約 | ✓ | | ✓ |
| | 従業員レビュー | ✓ | | ✓ |
| | 健全性 | ✓ | | ✓ |
| | 再開します | ✓ | ✓ | ✓ |
| 法律 | NDAS | ✓ | ✓ | ✓ |
| | ベンダー - お客様との契約 | ✓ | ✓ | ✓ |
| マーケティング | キャンペーン | ✓ | ✓ | ✓ |
| | 会議 | ✓ | ✓ | ✓ |
| 処理 | 監査レポート | ✓ | ✓ | ✓ |
| 営業 | SO 番号 | ✓ | ✓ | |
| サービス | RFI (RFI) | ✓ | | ✓ |
| | RFP | ✓ | | ✓ |
| | SOW の作成 | ✓ | ✓ | ✓ |
| | トレーニング | ✓ | ✓ | ✓ |
| サポート | 苦情やチケット | ✓ | ✓ | ✓ |

次のメタデータも分類され、同じサポート対象言語で識別されます。

- アプリケーションデータ
- アーカイブファイル
- 音声
- ビジネスアプリケーションデータ
- CAD ファイル
- コード
- 壊れています

- データベースおよびインデックス・ファイル
- デザインファイル（Design Files）
- E メールアプリケーションデータ
- 暗号化
- 実行可能ファイル
- 財務アプリケーションデータ
- ヘルスアプリケーションデータ
- イメージ
- ログ
- その他の文書
- その他のプレゼンテーション
- その他のスプレッドシート
- その他 " 不明 "
- 構造化データ
- ビデオ
- 0 バイトのファイル

ファイルのタイプ

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。

しかし、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、.

見つかった情報の正確性

ネットアップでは、Cloud Data Sense が特定した個人データと機密性の高い個人データの正確性を 100% 保証することはできません。必ずデータを確認して情報を検証してください。

以下の表は、テストに基づいて、データ検出によって検出された情報の正確さを示しています。精度 _ と _ リコール _ で分解します。

精度（Precision）

検出されたデータが正しく識別された確率。たとえば、個人データの正確な割合が 90% の場合、個人情報を含むと識別された 10 個中 9 個のファイルに個人情報が実際に含まれていることを意味します。10 個のファイルのうち 1 個はフォールスポジティブです。

取り消し

データが持つべきものを見つける確率。たとえば、個人データのリコール率が 70% の場合、データセンス

は、実際に個人情報を含む 10 個のファイルのうち 7 個を識別できます。データセンシブは、データの 30% を見逃すことになり、ダッシュボードには表示されません。

私たちは、常に結果の正確さを改善しています。これらの改善は、今後の Data Sense リリースで自動的に利用できるようになる予定です。


| を入力します | 精度（ Precision ） | 取り消し |
|--------------|-----------------|-----------|
| 個人データ - 一般 | 90% ～ 95% | 60% ～ 80% |
| 個人データ - 国 ID | 30% ～ 60% | 40% ～ 60% |
| 機密性の高い個人データ | 80% ～ 95% | 20% ～ 30% |
| カテゴリ | 90% ～ 97% | 60% ～ 80% |

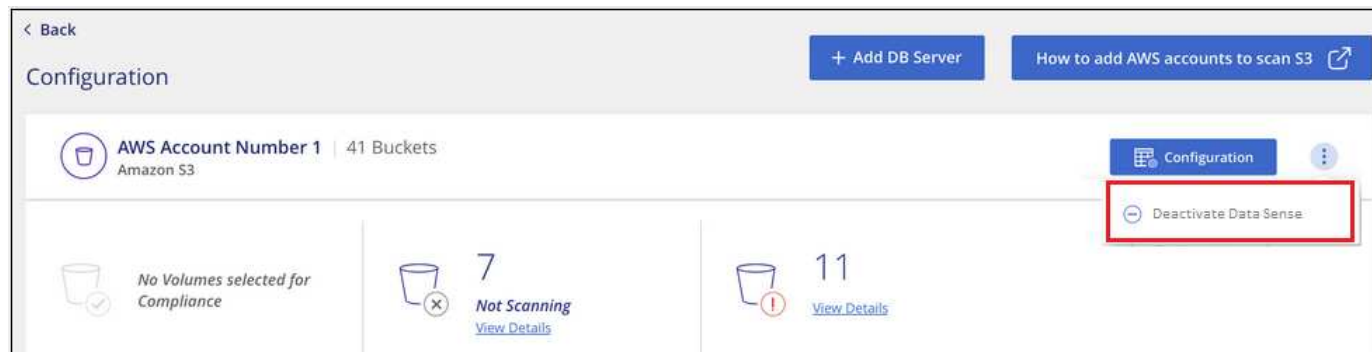
Cloud Data Sense からのデータソースの削除

必要に応じて、Cloud Data Sense を停止することで、1 つ以上の作業環境、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ます。作業環境でデータセンスを使用する必要がなくなった場合は、Cloud Data Sense インスタンスを削除することもできます。

作業環境のコンプライアンススキャンを非アクティブにします

スキャンを非アクティブ化すると、Cloud Data Sense は作業環境上のデータをスキャンなくなり、データセンシブインスタンスからインデックス付きのコンプライアンスインサイトを削除します（作業環境自体のデータは削除されません）。

1. [Configuration] ページで、をクリックします  ボタンをクリックして作業環境を選択し、[* データセンスを非活動化 *（Deactivate Data Sense *）] をクリックします。



作業環境を選択するときに、サービスパネルから作業環境のコンプライアンススキャンを無効にすることもできます。

Cloud Data Sense からのデータベースの削除

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、Cloud Data Sense インターフェイスからそのデータベースを削除して、すべてのスキャンを停止できます。

1. [Configuration] ページで、をクリックします [: ボタン] ボタンをクリックし、 * DB サーバの削除 * をクリックします。



Cloud Data Sense から OneDrive または SharePoint アカウントを削除する

特定の OneDrive アカウントまたは特定の SharePoint アカウント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、クラウドデータセンスインターフェイスからアカウントを削除して、すべてのスキャンを停止できます。

手順

1. [Configuration] ページで、をクリックします [: ボタン] OneDrive または SharePoint アカウントの行にあるボタンをクリックし、 [* OneDrive アカウントの削除 *] または [* SharePoint アカウントの削除 *] をクリックします。



ページから [OneDrive を削除] ボタンのスクリーンショット。"]

2. 確認ダイアログで * アカウントの削除 * をクリックします。

Cloud Data Sense からのファイル共有のグループの削除

ファイル共有グループからユーザファイルをスキャンする必要がなくなった場合は、Cloud Data Sense インターフェイスからファイル共有グループを削除して、すべてのスキャンを停止できます。

手順

1. [Configuration] ページで、をクリックします [: ボタン] [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. 確認ダイアログで * 共有のグループを削除 * をクリックします。

データセンススキャンの速度を下げる

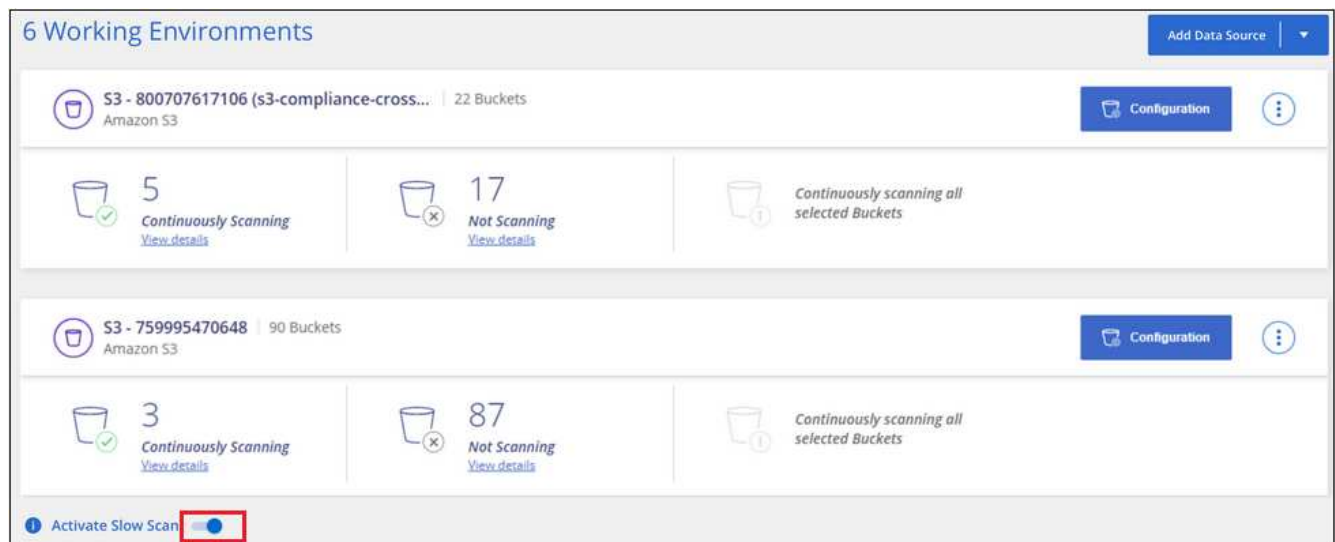
データスキャンは、ストレージシステムとデータにほとんど影響を与えません。ただし、影響が非常に小さい場合でも、低速スキャンを実行するようにデータセンスを設定できます。有効にすると、すべてのデータソースで低速スキャンが使用されます。1つの作業環境またはデータソースで低速スキャンを設定することはできません。



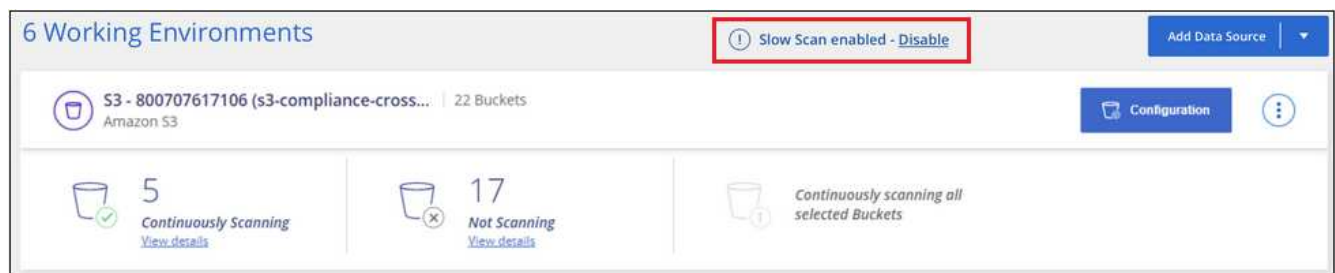
データベースのスキャン中は、スキャン速度を下げることはできません。

手順

1. _Configuration_page の下部から、スライダを右に動かして低速スキャンを有効にします。



設定ページの上部には、低速スキャンが有効になっていることが示されます。



2. このメッセージの * 無効 * をクリックすると、低速スキャンを無効にできます。

クラウドデータセンスインスタンスを削除しています

データセンスを使用する必要がなくなった場合は、Cloud Data Sense インスタンスを削除できます。インスタンスを削除すると、インデックス付きデータが存在する関連ディスクも削除されます。

1. クラウドプロバイダのコンソールに移動して、Cloud Data Sense インスタンスを削除します。

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*

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.