



プライベートデータの管理

Cloud Manager

Tom Onacki
May 06, 2021

目次

プライベートデータの管理	1
ポリシーを使用したデータの制御	1
AIP ラベルを使用してデータを分類する	4
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	9
ソースファイルを削除しています	10

プライベートデータの管理

Cloud Compliance では、さまざまな方法でプライベートデータを管理できます。一部の機能では、最も重要なデータを簡単に確認できます。その他の機能を使用すると、データに変更を加えることができます。

- 「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。
- 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 Compliance を使用して AIP ラベルを管理します。
- 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。

ポリシー機能と AIP 機能の両方で提供される機能の詳細については、以下を参照してください。

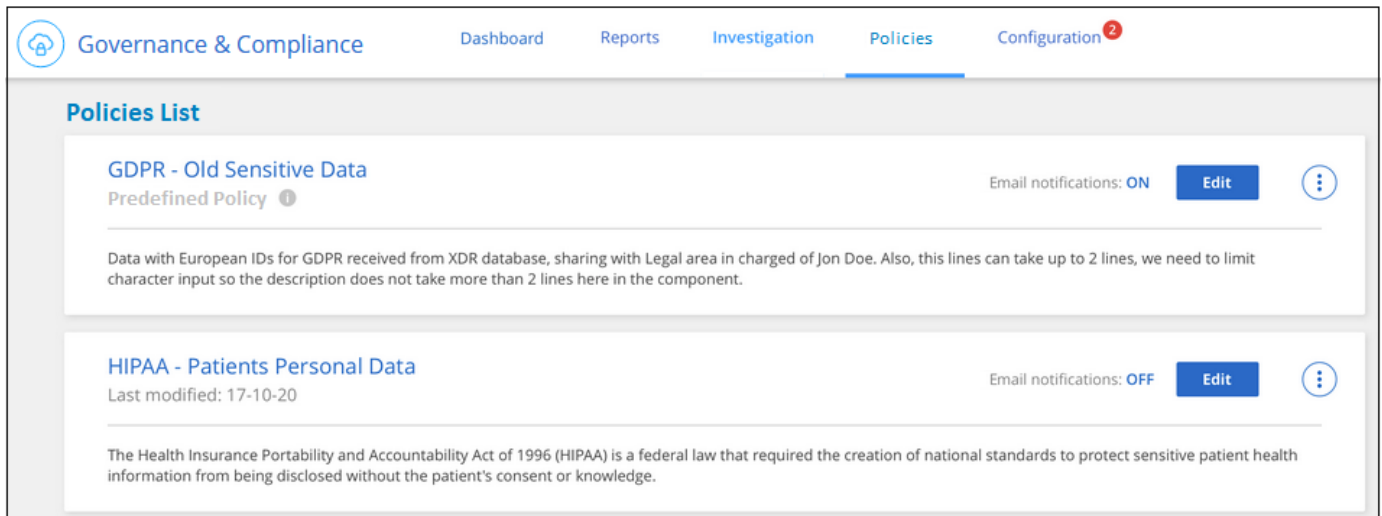
ポリシーを使用したデータの制御

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 Compliance では、お客様からの一般的な要求に基づいて、一連のポリシーが事前定義されています。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

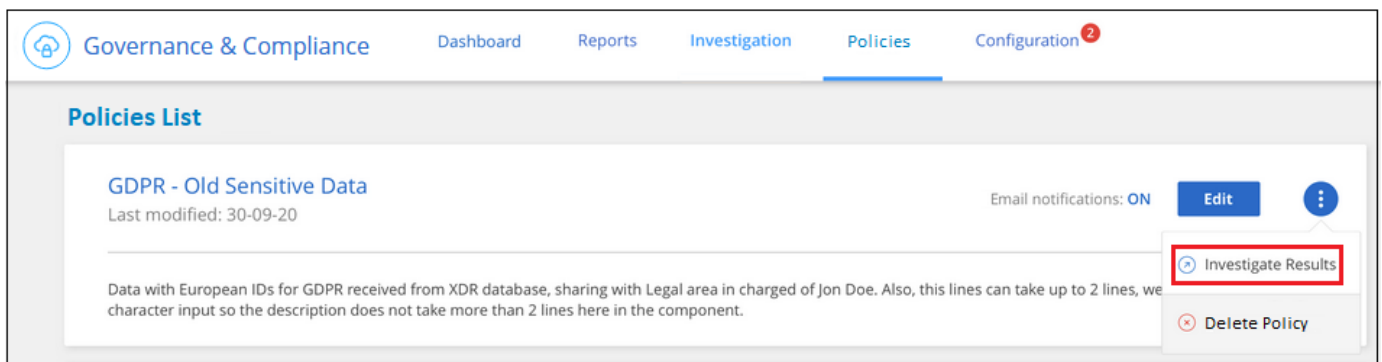
コンプライアンスダッシュボードの * ポリシー * タブには、このクラウドコンプライアンスインスタンスで利用可能なすべての事前定義ポリシーとカスタムポリシーが表示されます。



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。

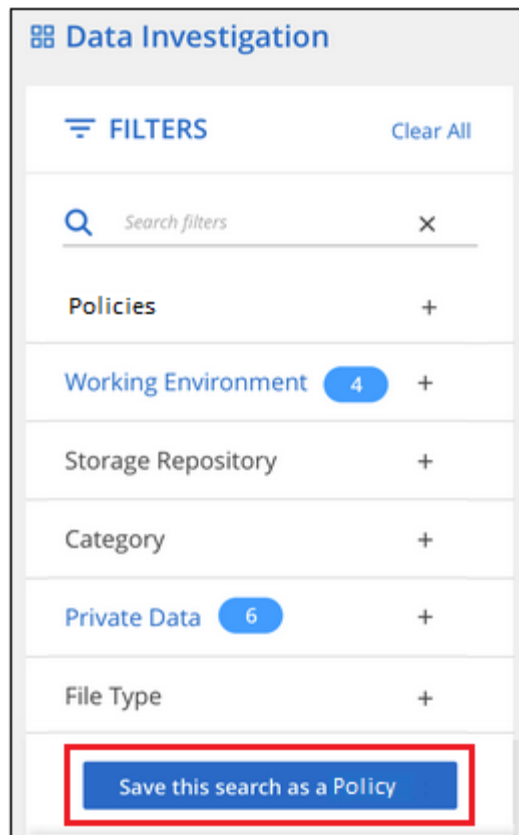


カスタムポリシーを作成しています

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. フィルタの特性をすべて希望どおりに設定したら、[* この検索をポリシーとして保存 *] 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、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。
 - c. 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。の詳細を確認してください [AIP ラベル](#)。
)
 - d. [ポリシーの作成 *] をクリックします。

Create Policy

Saving this filtered view will create a new Policy, you can view/edit it in the "Policy" tab

Name this Policy

HIPAA - Patient Personal Data

Give it a description to quickly identify it

Files containing patient health information that is more than 30 days old

☒ Send email updates about this Policy to Cloud Manager_users on this account every Week

☐ Automatically label matches of this Policy with: select 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。

AIP ラベルを使用してデータを分類する

クラウドファイルで AIP ラベルを管理できます 登録している場合は、コンプライアンスがスキャンされます "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。Cloud Compliance では、すで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、すでにラベルが存在する場合にラベルを変更したりできます。

Cloud Compliance は、.pdf 、 .DOCX 、 .DOC 、 .PPTX 、 .XLS 、 .xlsx の各ファイルタイプで AIP ラベルをサポートします。

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 Compliance はラベルのないファイルと見なします。

ワークスペースへの **AIP** ラベルの統合

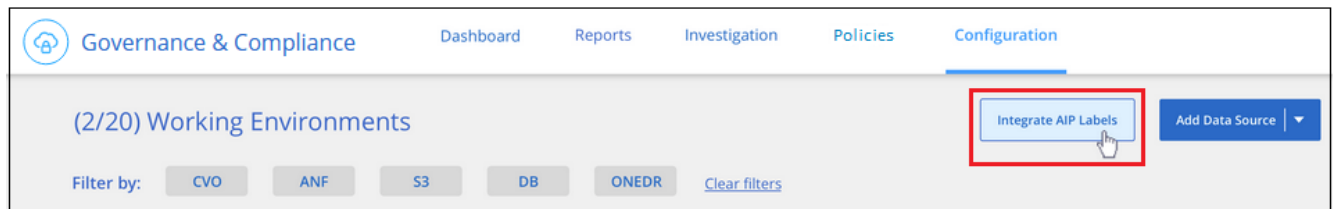
AIP ラベルを管理するには、既存の Azure アカウントにサインインして AIP ラベル機能をクラウド準拠に統合する必要があります。有効にすると、すべてのファイルの AIP ラベルを管理できます "[作業環境とデータソース](#)" をクリックします。

要件

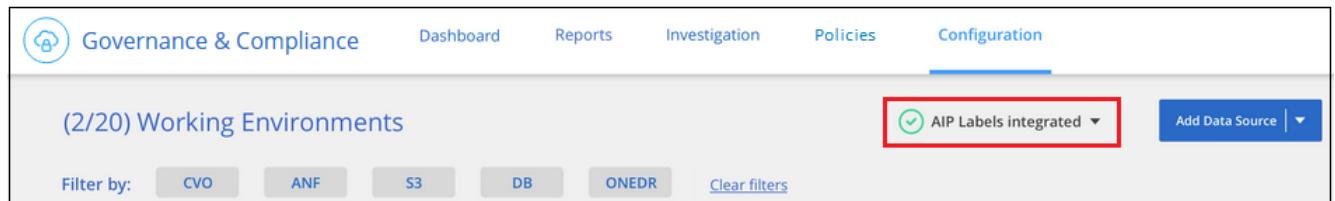
- アカウントと Azure Information Protection のライセンスが必要です。
- Azure アカウントのログインクレデンシャルが必要です。
- Amazon S3 バケット内のファイルのラベルを変更する場合は、権限「 3 : PutObject 」が IAM ロールに含まれていることを確認します。を参照してください "[IAM ロールを設定します](#)"。

手順

1. Cloud Compliance 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 Compliance 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。

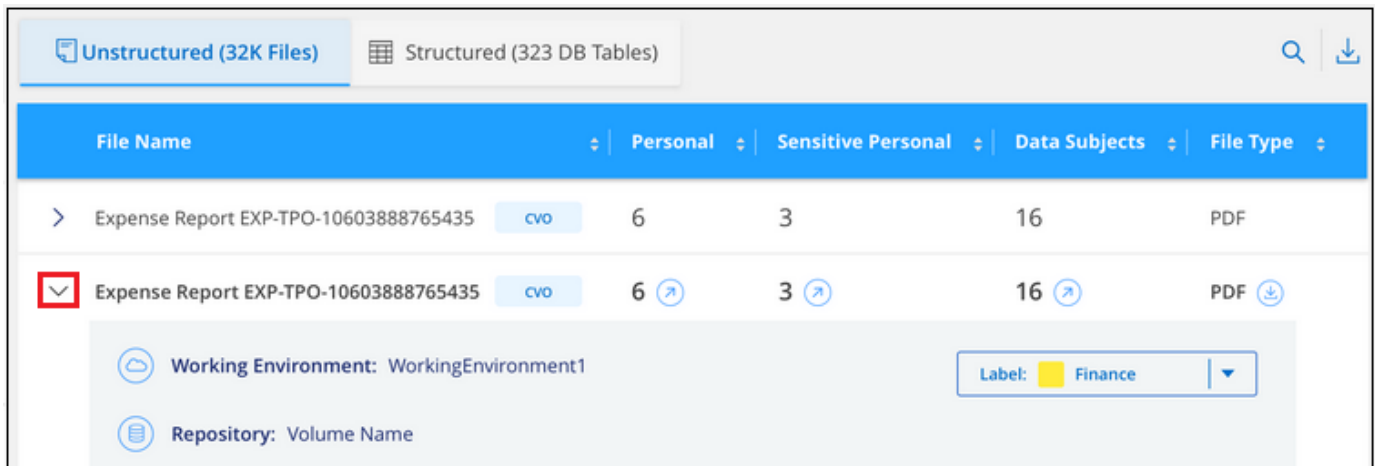


AIP ラベルは、 [調査] ページの結果ペインで表示および割り当てることができます。また、ポリシーを使用して AIP ラベルをファイルに割り当てすることもできます。

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。



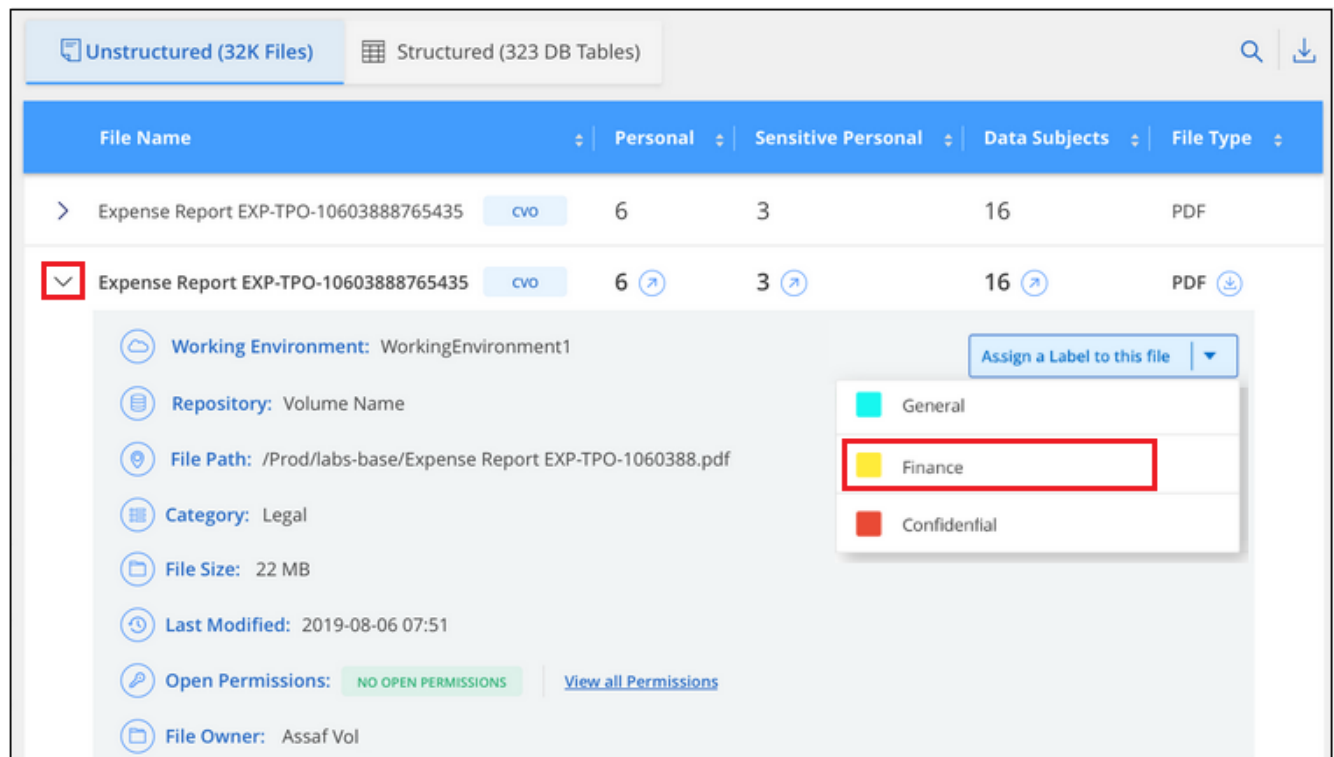
AIP ラベルを手動で割り当てる

Cloud Compliance 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。

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 Compliance 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。

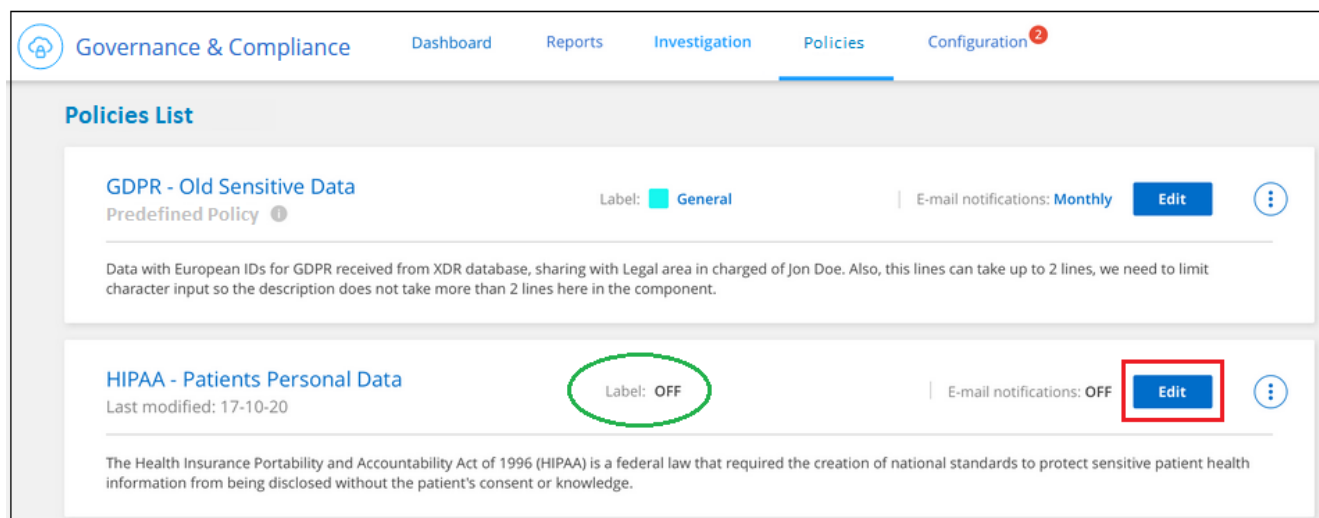
ラベルがすでにファイルに適用されているかどうか、およびラベルの分類レベルによって、ラベルを変更するときに次のアクションが実行されます。

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。

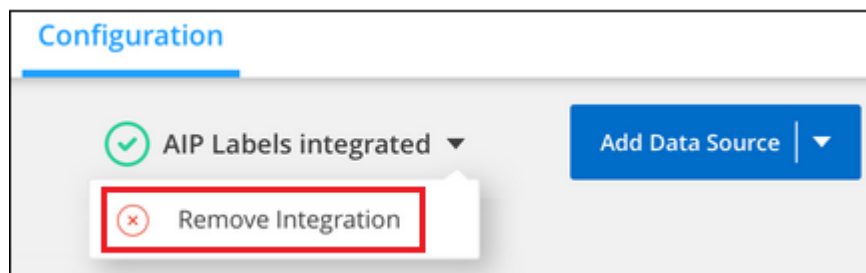
AIP 連動の削除

ファイルの AIP ラベルを管理できないようにするには、クラウドコンプライアンスインターフェイスから AIP アカウントを削除します。

Cloud Compliance で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。

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

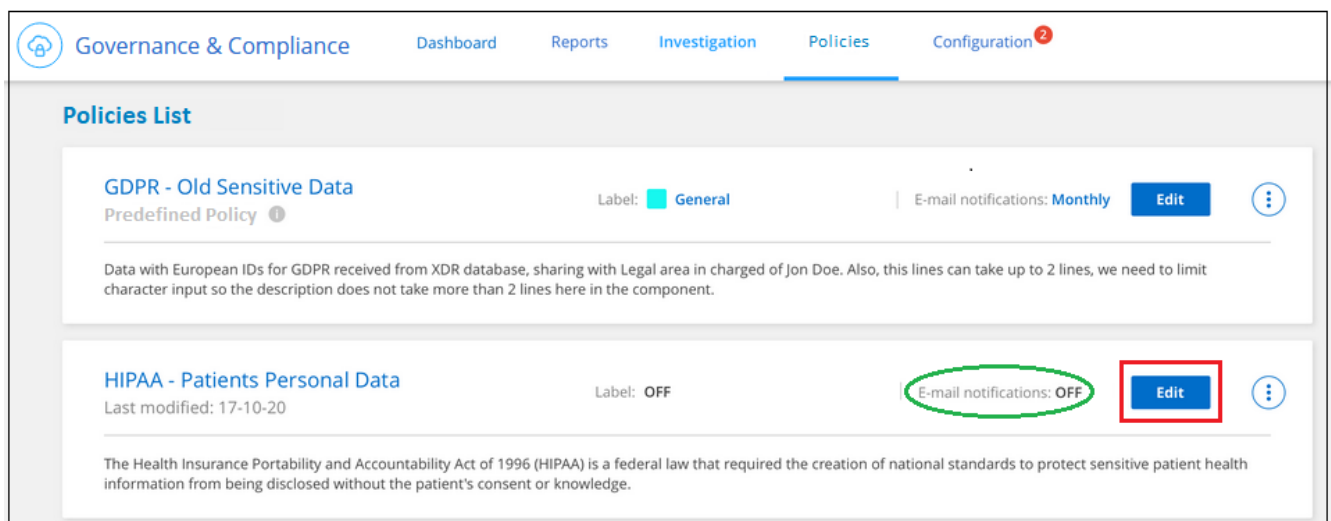
Cloud Compliance は、特定の重要なポリシーの結果が返されたときに Cloud Manager ユーザに E メールアラートを送信して、データを保護する通知を受け取ることができます。E メール通知は、日単位、週単位、または月単位で送信することができます。

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。

Edit Policy


Saving this filtered view will create a new Policy, you can view/edit it in the "Policy" tab

Name this Policy

HIPAA - Patient Personal Data

Give it a description to quickly identify it

Files containing patient health information that is more than 30 days old

☒ Send email updates about this Policy to Cloud Manager_users on this account every Week 

Day

Week

Month

Save Policy Cancel

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は送信されません。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。

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ソースファイルや重複として識別したソースファイルは、安全でないように見えたり危険すぎるソースファイルを完全に削除することができます。このアクションは永続的であり、元に戻すことはできません。




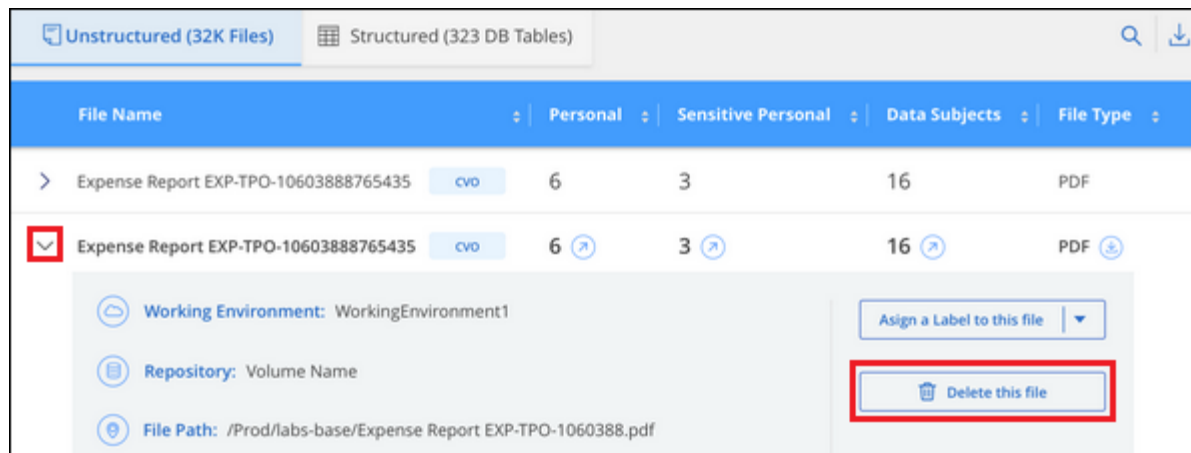
ボリューム・バックアップ内のデータベースまたはファイルに存在するファイルは削除できません。

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」

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。"]

2. [このファイルを削除する *] 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

事前定義されたポリシーのリスト

Cloud Compliance 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) に格納され、個人情報または機密性の高い個人情報を含む)
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 個を超えるファイル、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

Copyright Information

Copyright © 2021 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.