Cloud Compliance の詳細をご確認ください

Cloud Manager

Tom Onacki
April 24, 2021

目次

Cloud Compliance の詳細をご確認ください

Cloud Compliance は、 Cloud Manager 向けのデータプライバシーとコンプライアンスのサービスで、ボリューム、 Amazon S3 バケット、データベース、 OneDrive アカウントなどのデータソースをスキャンして、これらのファイルに存在する個人データや機密データを特定します。人工知能（ AI ）ベースのテクノロジを使用したクラウドコンプライアンスは、データの状況を把握し、機密データを特定するのに役立ちます。

"Cloud Compliance のユースケースを紹介します"。

の機能

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

- 個人識別情報（ PII ）の識別
- GDPR 、 CCPA 、 PCI 、 HIPAA の各プライバシー規制の要件に応じて、さまざまな機密情報の範囲を特定します
- データサブジェクトアクセス要求への応答（ dsar ）
- ファイルに特定のが含まれている場合は、 Cloud Manager ユーザに E メールで通知します PII （この基準は、を使用して定義します "ポリシー"）
- 表示と変更 "Azure Information Protection （ AIP ）ラベル" ファイルに保存できます
- 個々のファイルを削除します

Cloud Compliance には、ガバナンスの取り組みに役立つツールも用意されています。Cloud Compliance を使用すると、次のことができます。

- システム内の古いデータ、ビジネス以外のデータ、重複ファイル、大容量ファイルを特定します。

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

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

  これは、オンプレミスの場所からクラウドにデータを移行する場合に便利です。

サポートされている作業環境とデータソース

Cloud Compliance では、次の種類の作業環境とデータソースからデータをスキャンできます。

- AWS の Cloud Volumes ONTAP
- Azure の Cloud Volumes ONTAP
- オンプレミスの ONTAP クラスタ
- Azure NetApp Files の特長

- Amazon S3
- ネットアップ以外のファイル共有
- オブジェクトストレージ（ S3 プロトコルを使用）
- データベース
- OneDrive アカウント

2021 年 1 月にリリースされたベータ版の機能により、次のことが可能になります 作成したバックアップファイルに対して Compliance Scans _ for free_on を実行します を使用して作成したオンプレミスの ONTAP ボリュームから "クラウドバックアップ"）。これにより、オンプレミスの ONTAP ボリュームを Cloud Compliance で直接スキャンするか、またはボリュームから作成されたバックアップファイルをスキャンするかを選択できます。

コスト

- Cloud Compliance の使用コストは、スキャンするデータの量によって異なります。Cloud Compliance が Cloud Manager ワークスペースでスキャンする最初の 1TB のデータは無料です。これには、すべての作業環境とデータソースのすべてのデータが含まれます。その後もデータのスキャンを続行するには、AWS または Azure Marketplace へのサブスクリプションが必要です。を参照してください "価格設定" を参照してください。

  "登録方法については、こちらをご覧ください"。

- 注：このサブスクリプションは、オンプレミスの ONTAP システムから作成されたバックアップファイルのスキャンには必要ありません。
- クラウドに Cloud Compliance をインストールするにはクラウドインスタンスを導入する必要があるため、導入先のクラウドプロバイダから料金が発生します。を参照してください 各クラウドに導入されるインスタンスのタイプ プロバイダ。Cloud Compliance をオンプレミスシステムにインストールすれば、コストは発生しません。
- Cloud Compliance では、コネクタを導入しておく必要があります。多くの場合、 Cloud Manager で他のストレージとサービスを使用しているため、すでにコネクタが用意されています。Connector インスタンスを使用すると、導入先のクラウドプロバイダから料金が発生します。を参照してください "クラウドプロバイダごとに導入されるインスタンスのタイプ"。

データ転送コスト

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

- "AWS ： Amazon EC2 価格設定"
- "Microsoft Azure ： Bandwidth Pricing Details 』"

Cloud Compliance の仕組み

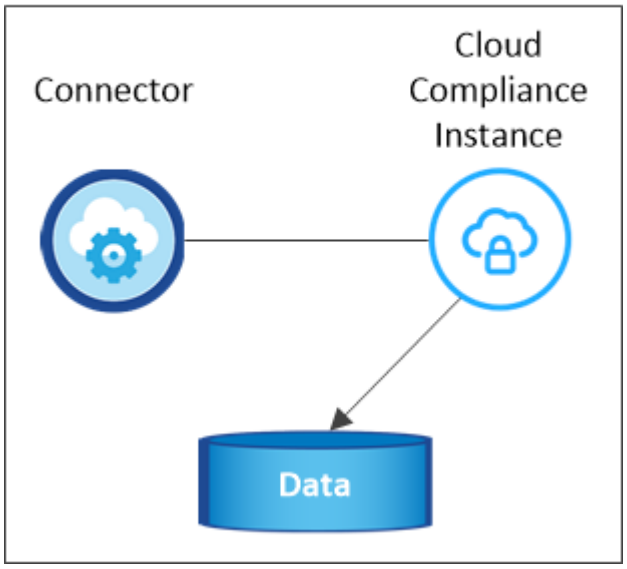
Cloud Compliance の仕組みは次のとおりです。

1. Cloud Manager に Cloud Compliance のインスタンスを導入します。
2. 1 つ以上の作業環境またはデータソースで有効にします。
3. Cloud Compliance は、 AI のラーニングプロセスを使用してデータをスキャンします。
4. [* コンプライアンス] をクリックし、表示されたダッシュボードとレポートツールを使用して、コンプライアンスの取り組みを支援します。

Cloud Compliance インスタンス

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

コネクタがオンプレミスにインストールされている場合は、要求内の最初の Cloud Volumes ONTAP システムと同じ VPC または VNet にクラウド準拠インスタンスを導入します。



インスタンスについては、次の点に注意してください。

- Azure では、 Cloud Compliance はで実行されます "Standard_D16s_v3 VM" 512 GB ディスク
- AWS では、 Cloud Compliance はで実行されます "m5.mc2[インスタンス" 500 GB の gp2 ディスクです。

  m5.mcd を使用できない地域では、代わりに m4.mcd インスタンスに対して Cloud Compliance を実行します。

  インスタンス / VM タイプの変更やサイズ変更はサポートされていません。表示されるサイズを使用する必要があります。

- インスタンスの名前は *CloudCompliancy_with* で、生成されたハッシュ（ *UUID* ）を連結しています。例： *_CloudCompliion-16bb6564-38ad-40802-9a92-36f5fd2f71c7*
- 1 つのコネクタに導入される Cloud Compliance インスタンスは 1 つだけです。

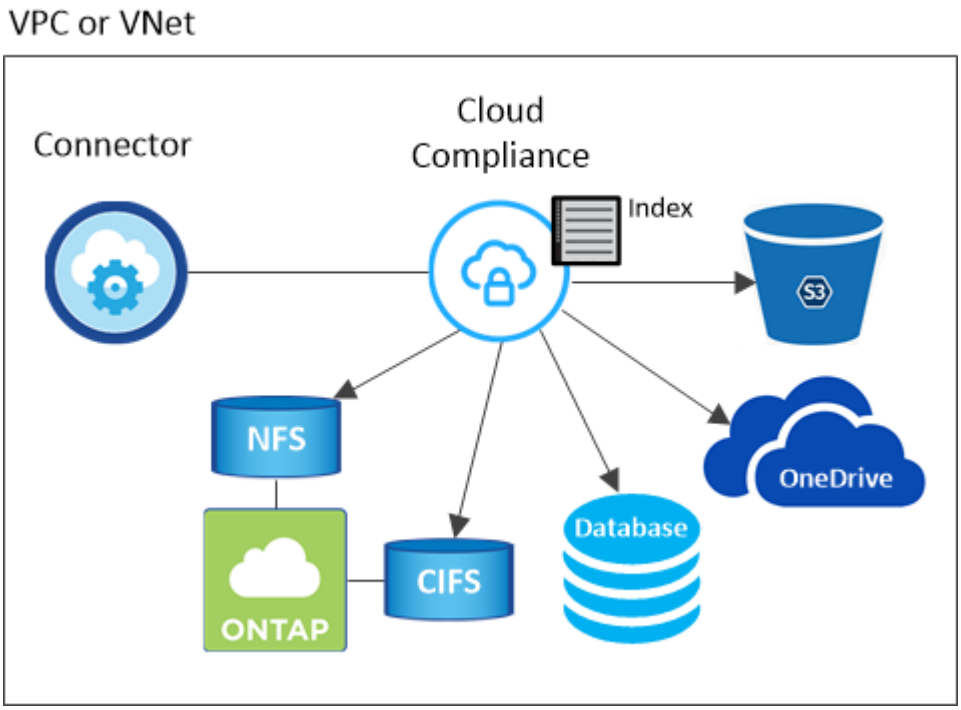
- Cloud Compliance ソフトウェアのアップグレードは自動化されているため、心配する必要はありません。

Cloud Compliance はデータを継続的にスキャンするため、インスタンスは常に実行されている状態にしておく必要があります。

スキャンの動作

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

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



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

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

Cloud Compliance がインデックス化する情報

Cloud Compliance は、データ（ファイル）に対してカテゴリを収集してインデックスを作成し、割り当てます。Cloud Compliance インデックスに含まれるデータは次のとおりです。

標準メタデータ

Cloud Compliance は、ファイルタイプ、サイズ、作成日、変更日など、ファイルに関する標準のメタデータを収集します。

個人データ

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

機密性の高い個人データ

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

カテゴリ

Cloud Compliance 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類します。カテゴリは、各ファイルのコンテンツとメタデータの AI 分析に基づくトピックです。 "カテゴリの詳細については、こちらをご覧ください"。

タイプ（ **Types** ）

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

名前エンティティ認識

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

ネットワークの概要

Cloud Manager によって、コネクタインスタンスからのインバウンド HTTP 接続を有効にするセキュリティグループとともに Cloud Compliance インスタンスが導入されます。

Cloud Manager を SaaS モードで使用する場合、 Cloud Manager への接続には HTTPS が使用され、ブラウザと Cloud Compliance インスタンスの間で送信されるプライベートデータはエンドツーエンドの暗号化によって保護されるため、ネットアップとサードパーティが読み取ることはできません。

何らかの理由で SaaS ユーザインターフェイスの代わりにローカルユーザインターフェイスを使用する必要がある場合でも、ローカルユーザインターフェイスを使用できます "ローカル UI にアクセスします"。

アウトバウンドルールは完全にオープンです。Cloud Compliance ソフトウェアのインストールとアップグレード、および使用状況の指標の送信には、インターネットアクセスが必要です。

ネットワーク要件が厳しい場合は、 "Cloud Compliance が連絡するエンドポイントについて説明します"。

コンプライアンス情報へのユーザアクセス

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

- * アカウント管理者 * は、コンプライアンス設定を管理し、すべての作業環境のコンプライアンス情報を表示できます。
- * ワークスペース管理者 * は、アクセス権を持つシステムについてのみ、コンプライアンス設定を管理

し、コンプライアンス情報を表示できます。ワークスペース管理者が　Cloud　Manager　の作業環境にアクセスできない場合、作業環境のコンプライアンス情報は [コンプライアンス] タブに表示されません。

- コンプライアンスビューア * の役割を持つユーザーは、アクセス権を持つシステムのコンプライアンス情報を表示し、レポートを生成することのみができます。これらのユーザは、ボリューム、バケット、またはデータベーススキーマのスキャンを有効または無効にすることはできません。

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