



オンプレミスの ONTAP データをパブリッククラウドにバックアップす る

Cloud Manager

Tom Onacki
May 05, 2021

目次

オンプレミスの ONTAP データをパブリッククラウドにバックアップする.....	1
クイックスタート	1
要件	2
Cloud Backup を有効にしています	9

オンプレミスの **ONTAP** データをパブリッククラウドにバックアップする

オンプレミスの ONTAP システムからパブリッククラウドの低コストのオブジェクトストレージへのデータのバックアップを開始するには、いくつかの手順を実行します。これには、Amazon S3、Azure Blob、Google Cloud Storage 上でのバックアップファイルの作成が含まれます。

NetApp StorageGRID システムを使用しており、バックアップを作成する場合は、「方法」を参照してください ["オンプレミスの ONTAP データをプライベートクラウドにバックアップ"](#)。

ヒント

ほとんどの場合、Cloud Manager を使用してすべてのバックアップおよびリストア処理を実行します。ただし、ONTAP 9.9.1 以降では、ONTAP System Manager を使用して、オンプレミスの ONTAP クラスターのボリュームバックアップ処理を開始できます。 ["Cloud Backup を使用してボリュームをクラウドにバックアップする方法については、System Manager の説明を参照してください。"](#)

2021 年 1 月にリリースされたベータ版の機能により、バックアップされたボリュームに対して、オンプレミスシステムからコンプライアンススキャンを実行できます。通常、コンプライアンススキャンでは最大 1TB のデータを解放し、サービスのコストは 1TB を超えるデータに対して適用されます。オンプレミスのボリュームにバックアップとコンプライアンスを組み合わせることで、オンプレミスのボリューム上のスキャンコストを抑えることができます。詳細については、こちらをご覧ください ["クラウドコンプライアンス"](#) ビジネスアプリケーションとクラウド環境のプライバシーを確保できます。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

構成がサポートされていることを確認します

- オンプレミスクラスタを検出し、Cloud Manager の作業環境に追加しておきます。を参照してください ["ONTAP クラスタの検出"](#) を参照してください。
 - クラスタで ONTAP 9.7P5 以降が実行されています。
 - クラスタには SnapMirror ライセンスがあり、PREM または Data Protection Bundle に含まれています。
- に登録しておきます ["Azure"](#)、["AWS"](#)または ["Google"](#) Cloud Manager Marketplace のバックアップ製品またはを購入済みである ["アクティブ化されます"](#) NetApp の Cloud Backup BYOL ライセンス。
- バックアップを格納するオブジェクトストレージスペース用の有効なクラウドプロバイダサブスクリプションが必要です。
- AWS と GCP については、ONTAP クラスタがデータをバックアップできるように、アクセスキーと必要な権限を持つアカウントが必要です。

システムで **Cloud Backup** を有効にします

作業環境を選択し、右パネルの [バックアップとコンプライアンス] サービスの横にある [*Enable] をクリックして、セットアップ・ウィザードに従います。



ボタンを示すスクリーンショット。"]

クラウドプロバイダを選択し、プロバイダの詳細を入力します

プロバイダを選択し、プロバイダの詳細を入力します。また、ボリュームが配置されている ONTAP クラスタ内の IPspace を指定する必要があります。

バックアップポリシーを定義

デフォルトポリシーでは、毎日ボリュームがバックアップされ、各ボリュームの最新の 30 個のバックアップコピーが保持されます。日単位、週単位、または月単位のバックアップに変更するか、システム定義のポリシーの中からオプションを追加するものを 1 つ選択します。

バックアップするボリュームを選択します

クラスタからバックアップするボリュームを特定します。

バックアップしたボリュームで **Compliance** スキャンをアクティブ化（オプション）

クラウドにバックアップされているボリュームを Cloud Compliance でスキャンするかどうかを選択します。

必要に応じて、データをリストアします

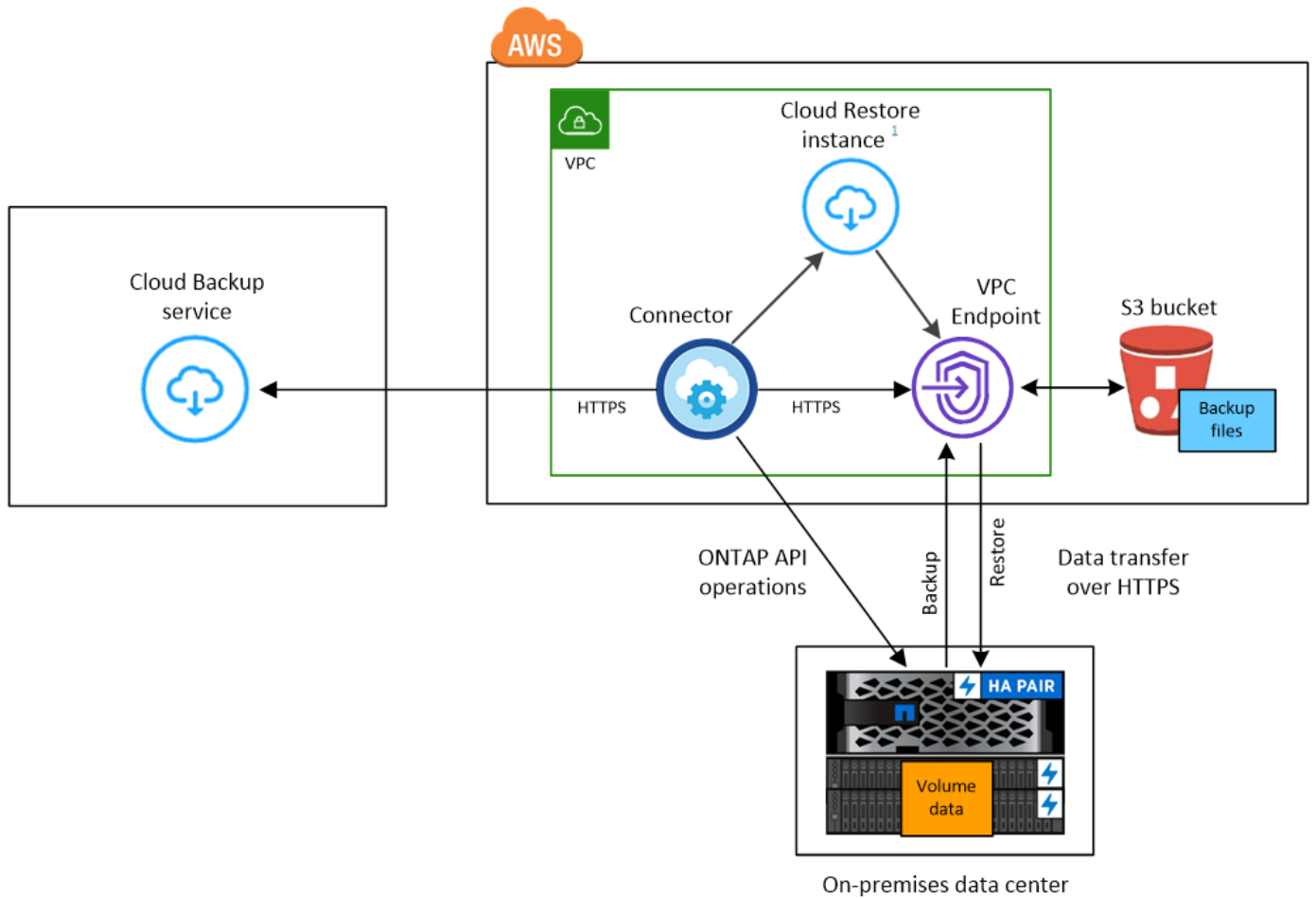
バックアップ全体を新しいボリュームにリストアするか、またはバックアップから既存のボリュームに個々のファイルをリストアするかを選択します。同じクラウドプロバイダを使用している Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムにデータをリストアできます。

を参照してください ["バックアップファイルからのボリュームデータのリストア"](#) を参照してください。

要件

オンプレミスボリュームをオブジェクトストレージにバックアップする前に、次の要件を確認し、サポートされている構成であることを確認してください。

次の図は、オンプレミスの ONTAP システムを Amazon S3 にバックアップする場合と、それらの間の接続を準備する必要がある場合の各コンポーネントを示しています。



¹ Cloud Restore instance is active only during single-file restore operations.

次の図は、オンプレミスの ONTAP システムを Azure Blob にバックアップする場合の各コンポーネントと、その間の準備に必要な接続を示しています。



¹ Cloud Restore instance is active only during single-file restore operations.

次の図は、オンプレミスの ONTAP システムを Google Cloud Storage にバックアップする場合の各コンポーネントと、それらの間の準備に必要な接続を示しています。



ONTAP クラスタの準備

クラウドストレージにデータをバックアップするときは、ONTAP クラスタが次の要件を満たしている必要があります。

ONTAP の要件

- ONTAP 9.7P5 以降
- SnapMirror ライセンス（PREM または Data Protection Bundle に含まれます）。

方法を参照してください ["クラスタライセンスを管理します"](#)。

- 時間とタイムゾーンが正しく設定されている。

方法を参照してください ["クラスタ時間を設定します"](#)。

クラスタネットワークの要件

- ONTAP クラスタが、クラウドオブジェクトストレージへのポート 443 経由の HTTPS 接続を開始します。

ONTAP は、オブジェクトストレージとの間でデータの読み取りと書き込みを行います。オブジェクトストレージが開始されることはなく、応答するだけです。

- コネクタからのインバウンド接続が必要です。この接続は、使用するオブジェクトストレージプロバイダに応じて、AWS VPC、Azure VNet、または Google Cloud Platform VPC に配置できます。
- クラスタ間 LIF は、バックアップ対象のボリュームをホストする各 ONTAP ノードに必要です。LIF は、ONTAP がオブジェクトストレージへの接続に使用する IPspace に関連付けられている必要があります。

ります。 ["IPspace の詳細については、こちらをご覧ください"](#)。

Cloud Backup をセットアップすると、IPspace で使用するように求められます。各 LIF を関連付ける IPspace を選択する必要があります。これは、「デフォルト」の IPspace または作成したカスタム IPspace です。

- ノードとクラスタ間 LIF からインターネットにアクセスできます。
- ボリュームが配置されている Storage VM に DNS サーバが設定されている。

方法を参照してください ["SVM 用に DNS サービスを設定"](#)。

- 必要に応じてファイアウォールルールを更新し、ONTAP からオブジェクトストレージへのポート 443 経由の Cloud Backup Service 接続と、ポート 53 （ TCP / UDP ） 経由での Storage VM から DNS サーバへの名前解決トラフィックを許可します。

ONTAP クラスタを検出しています

ボリュームデータのバックアップを開始する前に、Cloud Manager でオンプレミスの ONTAP クラスタを検出する必要があります。

["クラスタの検出方法について説明します"](#)。

コネクタの作成または切り替え

コネクタは、データをクラウドにバックアップするために必要です。コネクタは、デスティネーションオブジェクトストレージと同じクラウドプロバイダになければなりません。たとえば、AWS S3 にデータをバックアップする場合は、AWS VPC 内のコネクタを使用する必要があります。オンプレミスに導入されているコネクタは使用できません。新しいコネクタを作成するか、現在選択されているコネクタが正しいプロバイダーにあることを確認する必要があります。

- ["コネクタについて説明します"](#)
- ["AWS でコネクタを作成する"](#)
- ["Azure でコネクタを作成する"](#)
- ["GCP でコネクタを作成する"](#)
- ["コネクタ間の切り替え"](#)

コネクタのネットワークを準備しています

コネクタに必要なネットワーク接続があることを確認します。

手順

1. コネクタが取り付けられているネットワークで次の接続が有効になっていることを確認します。
 - Cloud Backup Service へのアウトバウンドインターネット接続 ポート 443 （ HTTPS ）
 - ポート 443 経由でのオブジェクトストレージ（ S3 、 Blob 、 Google ） への HTTPS 接続
 - ONTAP クラスタへのポート 443 経由の HTTPS 接続
2. オブジェクトストレージのエンドポイントを有効にします。

- for AWS : S3 に対して VPC エンドポイントを有効にします。ONTAP クラスタから VPC への Direct Connect または VPN 接続が確立されている環境で、コネクタと S3 の間の通信を AWS 内部ネットワークのままにする場合は、この接続が必要です。
- Azure の場合 : Azure ストレージへの VNet プライベートエンドポイントを有効化これは、ONTAP クラスタから VNet への ExpressRoute または VPN 接続があり、コネクタと BLOB ストレージ間の通信を仮想プライベートネットワークのままにする場合に必要です。
- Google の場合 : サービスコネクタを配置するサブネットに Google プライベートアクセスを有効にします。"プライベート Google アクセス" ONTAP クラスタから VPC への直接接続が確立されており、Connector と Google Cloud Storage 間の通信を仮想プライベートネットワークのままにする場合は、が必要です。

プライベート Google アクセスは、内部（プライベート）IP アドレスのみ（外部 IP アドレスは使用しない）を持つ VM インスタンスで機能します。

サポートされている地域

オンプレミスシステムからパブリックシステムへのバックアップを作成できます。すべての地域でクラウドを利用できます。"Cloud Volumes ONTAP がサポートされている場合"。サービスのセットアップ時にバックアップを保存するリージョンを指定します。

ライセンス要件

Cloud Backup PAYGO ライセンスの場合は、へのサブスクリプションが必要です。"Azure"、"AWS"または"Google" Cloud Backup を有効にする前に、Cloud Manager Marketplace のバックアップサービスを利用できます。Cloud Backup の請求は、このサブスクリプションを通じて行われます。

Cloud Backup BYOL ライセンスを使用するには、ライセンスの期間と容量にサービスを使用できるように、ネットアップから提供されたシリアル番号が必要です。を参照してください "バックアップ BYOL ライセンスを追加および更新する"。

また、バックアップを格納するオブジェクトストレージスペースについて、クラウドプロバイダからのサブスクリプションが必要になります。

バックアップのための Amazon S3 の準備

Amazon S3 を使用している場合は、Cloud Manager が S3 バケットにアクセスするための権限を設定する必要があります。また、オンプレミスの ONTAP クラスタが S3 バケットにアクセスできるように権限を設定する必要があります。

手順

1. 最新のから次の S3 権限を指定します "Cloud Manager ポリシー"）を作成して、Cloud Manager に権限を付与する IAM ロールに付与します。

```
{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
    ],
    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ]
}
```

2. ONTAP クラスタから S3 にデータをバックアップできるように、IAM ユーザに次の権限を付与します。

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetBucketLocation",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject"
```

を参照してください ["AWS ドキュメント：「Creating a Role to Delegate Permissions to an IAM User」](#) を参照してください。

3. アクセスキーを作成または検索します。

Cloud Backup が ONTAP クラスタにアクセスキーを渡します。クレデンシャルは Cloud Backup Service には保存されません。

を参照してください ["AWS ドキュメント：「Managing Access Keys for IAM Users」](#) を参照してください。

Google Cloud Storage でバックアップを準備しています

バックアップを設定するときは、Storage Admin の権限があるサービスアカウントにストレージアクセスキーを指定する必要があります。サービスアカウントを使用すると、Cloud Backup でバックアップの格納に使用する Cloud Storage バケットを認証してアクセスできます。キーは、Google Cloud Storage がリクエストを発行しているユーザーを認識できるようにするために必要です。

手順

1. "事前定義されたストレージ管理者を含むサービスアカウントを作成します ロール"。
2. に進みます "GCP Storage Settings (GCP ストレージ設定)" サービスアカウントのアクセスキーを作成します。
 - a. プロジェクトを選択し、* 互換性 * をクリックします。まだ有効にしていない場合は、[相互運用アクセスを有効にする *] をクリックします。
 - b. [サービスアカウントのアクセスキー *] で、[サービスアカウントのキーの作成 *] をクリックし、作成したサービスアカウントを選択して、[キーの作成 *] をクリックします。

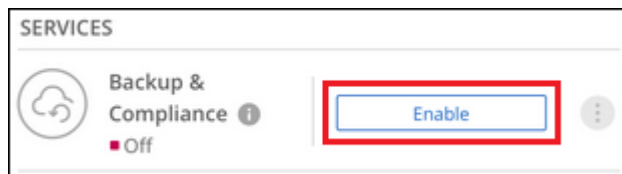
Cloud Backup でキーを入力する必要があるのは、あとでバックアップサービスを設定するときです。

Cloud Backup を有効にしています

Cloud Backup は、オンプレミスの作業環境からいつでも直接有効にできます。

手順

1. キャンバスから作業環境を選択し、右パネルのバックアップとコンプライアンスサービスの横にある * 有効化 * をクリックします。



ボタンを示すスクリーンショット。"]

2. プロバイダを選択し、* 次へ * をクリックして、プロバイダの詳細を入力します。
 - Azure の場合は次のように入力します
 - i. バックアップおよびバックアップを格納する Azure リージョンで使用する Azure サブスクリプション。
 - ii. リソースグループ - 新しいリソースグループを作成することも、を選択して既存のリソースグループを選択することもできます。
 - iii. バックアップするボリュームが配置されている ONTAP クラスタ内の IPspace 。

Provider Settings

Provider Information Azure Subscription <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">Azure_Subscription_1</div> <hr/> Resource Group <input checked="" type="radio"/> Create a new <input type="radio"/> Use an existing Resource Group Name <div style="border: 1px solid #ccc; height: 20px; width: 100%; margin-top: 5px;"></div>	Location & Connectivity Region <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">Default_CM_Region</div> IPspace <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;">IP_Space_1</div>
--	---

- AWS の場合は次のように入力します
 - i. バックアップの格納に使用する AWS アカウント、AWS Access Key、および Secret Key。
 - ii. バックアップを格納する AWS リージョン。
 - iii. バックアップするボリュームが配置されている ONTAP クラスタ内の IPspace。

Provider Settings

Provider Information AWS Account <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">AWS_Account_1</div> AWS Access Key <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">Enter AWS Access Key</div> AWS Secret Key <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;">Enter AWS Secret Key</div>	Location & Connectivity Region <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">us-east-2</div> IPspace i <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;">IP_Space_1</div>
---	--

- Google の場合、次のように入力します
 - i. バックアップ用に Google Cloud Storage バケットを作成する Google Cloud Project。これは、Cloud Manager が配置されているプロジェクトとは異なる場合があります。（プロジェクトには、事前定義された Storage Admin ロールを持つサービスアカウントが必要です）。
 - ii. バックアップの保存に使用する Google Access Key および Secret Key。
 - iii. バックアップが保存される Google リージョン。これは、Cloud Manager が配置されているリージョンとは異なるリージョンにすることもできます。
 - iv. バックアップするボリュームが配置されている ONTAP クラスタ内の IPspace。

Provider Settings

Provider Information	Location & Connectivity
<p>Google Cloud Project</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> Cloud Manager Default Project ▼ </div>	<p>Region</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> Cloud Manager Default Region ▼ </div>
<p>Google Cloud Access Key</p> <div style="border: 1px solid #ccc; padding: 2px; min-height: 20px;"> Enter Google Cloud Access Key </div>	<p>IPspace i</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> IP_Space_1 ▼ </div>
<p>Google Cloud Secret Key</p> <div style="border: 1px solid #ccc; padding: 2px; min-height: 20px;"> Enter Google Cloud Secret Key </div>	

- StorageGRID については、「方法」を参照してください ["オンプレミスの ONTAP データをプライベートクラウドにバックアップ"](#)。

この情報は、サービスの開始後は変更できないことに注意してください。

- プロバイダの詳細を入力したら、「* 次へ *」をクリックします。
- [Define Policy] ページで、既存のバックアップスケジュールと保持期間の値を選択するか、新しいバックアップポリシーを定義して、[* 次へ *]をクリックします。

Define Policy

Policy - Retention & Schedule

☐ Create a New Policy
☒ Select an Existing Policy

Select Policy

Default Policy (30 Daily)
▼

DP Volumes

Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

を参照してください ["既存のポリシーのリスト"](#)。

- バックアップするボリュームを選択します。
 - すべてのボリュームをバックアップするには、タイトル行 (☒ Volume Name)。
 - 個々のボリュームをバックアップするには、各ボリュームのボックス (☒ Volume_1)。

Select Volumes						
57 Volumes						
<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2	RW	SVM_Name_2	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3	RW	SVM_Name_3	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4	DP	SVM_Name_4	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5	RW	SVM_Name_5	0.25 TB	10 TB	Not Active

6. Activate Backup * をクリックすると、ボリュームの初期バックアップの作成が開始されます。

AWS または Azure でバックアップファイルを作成する場合、バックアップされたボリュームで準拠スキャンを実行するかどうかの確認を求められます。Cloud Compliance スキャンは、実行時に無料で実行できます。バックアップされたボリューム（を除く）"[導入された Cloud Compliance インスタンスのコスト](#)"）。

Activate Compliance on your Backed Up Volumes

You have successfully activated Backup to Cloud on 12 Volumes in your working environment "Name 1".

Cloud Compliance

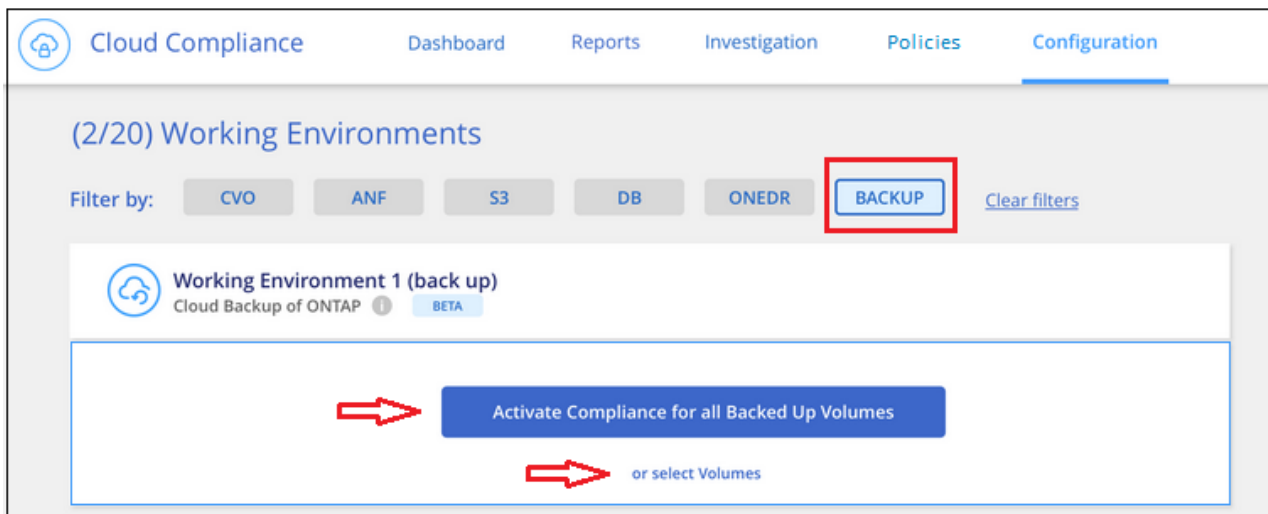
- > Cloud Compliance offer automated controls for data privacy regulations such as the GDPR, CCPA and more.
- > Driven by powerful artificial intelligence algorithms, Cloud Compliance gets your business application data and cloud environments privacy ready.

Go to Compliance

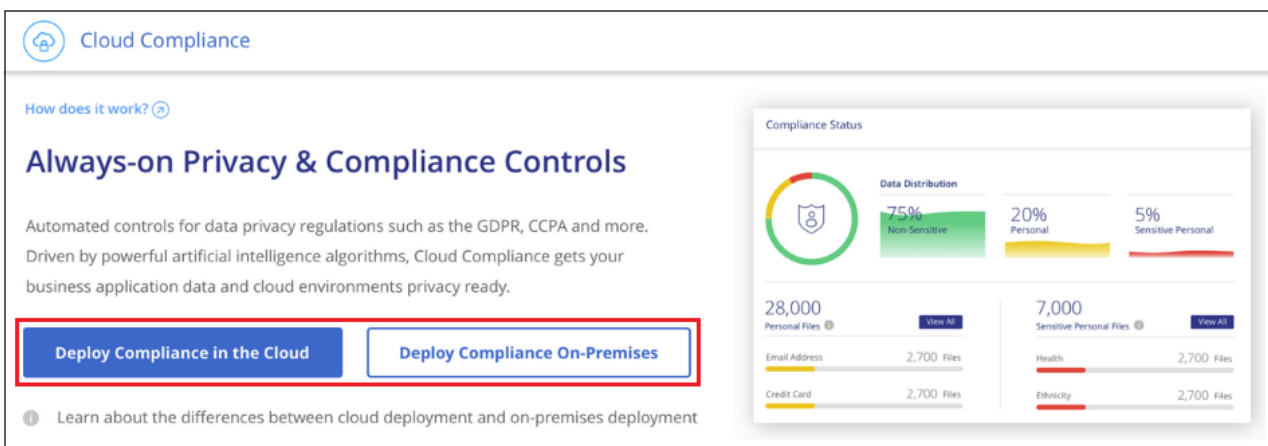
Close

7. コンプライアンスへ移動 * をクリックして、ボリュームのコンプライアンススキャンをアクティブ化します。（バックアップされたボリュームをスキャンせずに * Close * を選択すると、いつでもスキャンできます "[この機能を有効にします](#)" Cloud Compliance を後で参照）。

。Cloud Compliance のインスタンスがすでに環境に導入されている場合は、バックアップがある各オンプレミスの作業環境でスキャンするボリュームを設定ページで選択するように求められます。を参照してください "[ボリュームを選択する方法](#)"。



- 。クラウドコンプライアンスが導入されていない場合は、コンプライアンスページが表示され、クラウドまたは社内にコンプライアンスを導入できます。クラウドに導入することを強く推奨します。実行します ["こちらをご覧ください"](#) を参照してください。



Compliance の導入が完了したら、上記の手順でスキャンするボリュームを選択できます。

Cloud Backup は、オンプレミスの ONTAP システムからボリュームをバックアップします。必要に応じて、Cloud Compliance はバックアップしたボリュームに対してコンプライアンススキャンを実行します。

可能です ["ボリュームのバックアップを開始および停止したり、バックアップを変更したりできます スケジュール"](#) また、次のことも可能です ["ボリューム全体または個々のファイルをバックアップファイルからリストアする"](#)。

また可能です ["コンプライアンススキャンの結果を表示します"](#) また、データコンテキストを理解し、組織内の機密データを識別するのに役立つ、Cloud Compliance のその他の機能についても確認できます。



Cloud Compliance で準拠スキャンを開始するにはバックアップの作成を完了する必要があります。そのため、スキャン結果はすぐには使用できません。

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.