



オンプレミスの ONTAP データをクラウドコンプライアンスでスキャン Cloud Manager

Tom Onacki, Ben Cammett
May 06, 2021

目次

| | |
|--|---|
| オンプレミスの ONTAP データをクラウドコンプライアンスでスキャン | 1 |
| オンプレミスの ONTAP 作業環境内のデータをスキャンする | 1 |
| Cloud Compliance がボリュームにアクセスできることの確認 | 2 |
| SnapMirror を使用してオンプレミスの ONTAP データをスキャンする | 4 |

オンプレミスの **ONTAP** データをクラウドコンプライアンスでスキャン

オンプレミスの ONTAP システム上のデータは、Cloud Compliance を使用して直接スキャンできます。オンプレミスの NFS または CIFS データを Cloud Volumes ONTAP 作業環境にレプリケートして、それらのデータ保護ボリュームの準拠を有効にすることもできます。最適な方法をお選びください。

オンプレミスの **ONTAP** 作業環境内のデータをスキャンする

ある場合 ["ONTAP クラスタが検出されました"](#) 作成したボリュームを Cloud Manager の作業環境に追加すると、オンプレミスクラスタから直接ボリュームデータをスキャンできます。

オンプレミスの ONTAP クラスタ向けの Cloud Compliance で作業を開始するには、いくつかの手順を実行します。

クイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

Cloud Compliance インスタンスを導入します

["Cloud Manager に Cloud Compliance を導入"](#) インスタンスが展開されていない場合。

オンプレミスの作業環境で **Cloud Compliance** を有効にし、を選択します スキャンするボリューム

コンプライアンス * をクリックし、* 構成 * タブを選択して、すべてのボリュームまたは特定のボリュームのコンプライアンススキャンを有効にします。

ボリュームへのアクセスを確認

Cloud Compliance が有効になったので、すべてのボリュームにアクセスできることを確認します。

- クラウドコンプライアンスインスタンスには、それぞれのオンプレミス ONTAP システムへのネットワーク接続が必要です。
- セキュリティグループが、Cloud Compliance インスタンスからのインバウンド接続を許可する必要があります。
- NFS ボリュームのエクスポートポリシーで、Cloud Compliance インスタンスからのアクセスを許可する必要があります。
- CIFS ボリュームをスキャンするには、Cloud Compliance で Active Directory のクレデンシャルが必要です。

コンプライアンス * > * 構成 * > * CIFS クレデンシャルの編集 * をクリックし、クレデンシャルを入力します。

スキャンするボリュームを管理します

スキャンするボリュームを選択または選択解除すると、Cloud Compliance によるスキャンが開始または停止します。

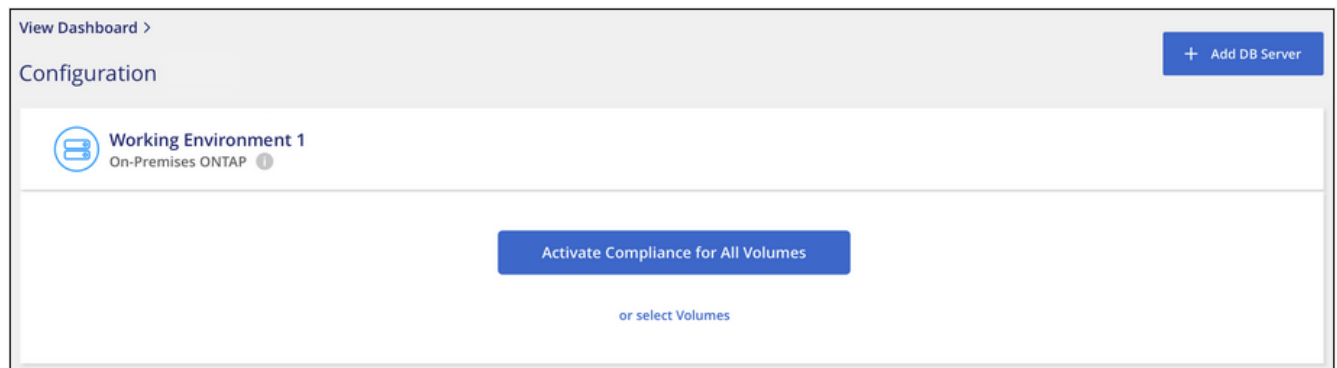
Cloud Compliance インスタンスの導入

"Cloud Compliance の導入" インスタンスが展開されていない場合。

Cloud Compliance は、オンプレミスの ONTAP クラスタをスキャンする際に、クラウドまたはオンプレミスの場所に導入できます。

作業環境での Cloud Compliance の有効化

1. Cloud Manager の上部で、* Compliance * をクリックし、* Configuration * タブを選択します。



2. 作業環境内のすべてのボリュームをスキャンするには、* すべてのボリュームのコンプライアンスをアクティブ化 * をクリックします。

作業環境内の特定のボリュームのみをスキャンするには、* をクリックするか、Volumes（ボリューム）* を選択して、スキャンするボリュームを選択します。

を参照してください ["ボリュームのコンプライアンススキャンの有効化と無効化"](#) を参照してください。

Cloud Compliance によって、作業環境で選択したボリュームのスキャンが開始されます。結果は、Cloud Compliance ダッシュボードで最初のスキャンが完了するとすぐに表示されます。所要時間はデータ量によって異なります。数分から数時間かかる場合もあります。

Cloud Compliance がボリュームにアクセスできることの確認

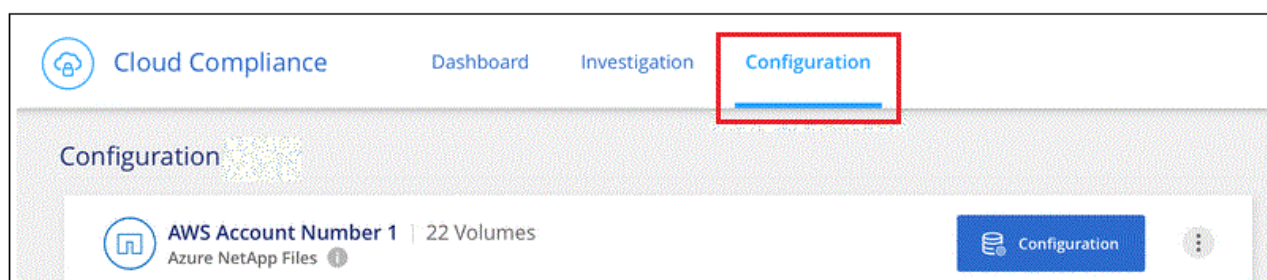
ネットワーク、セキュリティグループ、およびエクスポートポリシーを確認して、Cloud Compliance がボリュームにアクセスできることを確認します。CIFS ボリュームにアクセスできるようにするには、Cloud Compliance に CIFS クレデンシャルを指定する必要があります。

手順

1. クラウドコンプライアンスインスタンスと、オンプレミス ONTAP システムのボリュームを含む各ネットワークとの間にネットワーク接続があることを確認します。
2. オンプレミス ONTAP システムのセキュリティグループが、クラウドコンプライアンスインスタンスからのインバウンドトラフィックを許可していることを確認します。

そのためには、Cloud Compliance インスタンスの IP アドレスからトラフィックのセキュリティグループを開きます。

3. NFS ボリュームのエクスポートポリシーに Cloud Compliance インスタンスの IP アドレスが含まれていて、各ボリュームのデータにアクセスできることを確認します。
4. CIFS を使用する場合は、Active Directory クレデンシャルを使用して Cloud Compliance を提供し、CIFS ボリュームをスキャンできるようにします。
 - a. Cloud Manager の上部で、* Compliance * をクリックします。
 - b. [* 構成 *] タブをクリックします。

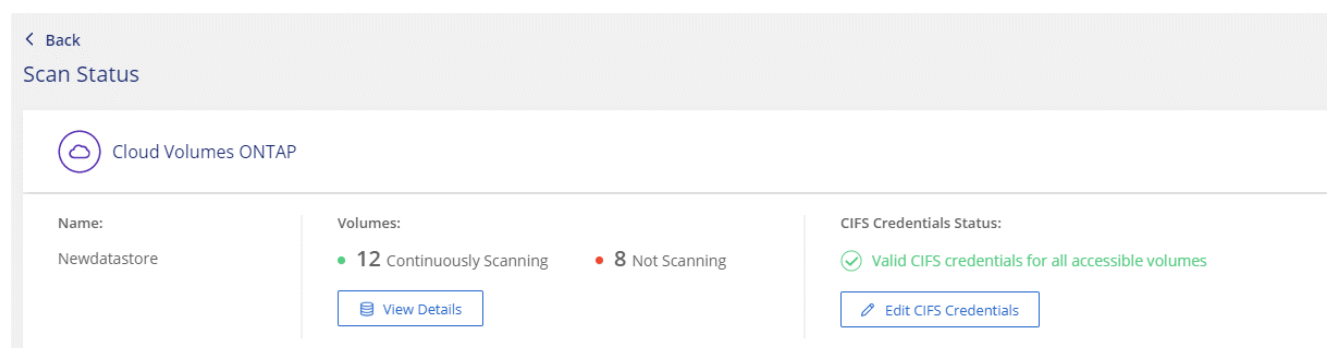


ボタンを示す [遵守] タブのスクリーンショット。"]

- c. 各作業環境について、* CIFS 資格情報の編集 * をクリックし、クラウド・コンプライアンスがシステム上の CIFS ボリュームにアクセスするために必要なユーザー名とパスワードを入力します。

クレデンシャルは読み取り専用ですが、管理者のクレデンシャルを指定することで、Cloud Compliance は昇格された権限が必要なデータを読み取ることができます。クレデンシャルは Cloud Compliance インスタンスに保存されます。

クレデンシャルを入力すると、すべての CIFS ボリュームが認証されたことを示すメッセージが表示されます。



5. _Configuration_page で、*View Details * をクリックして、各 CIFS および NFS ボリュームのステータスを確認し、エラーを修正します。

たとえば、次の図は 3 つのボリュームを示しています。1 つは Cloud Compliance インスタンスとボリュームの間のネットワーク接続の問題が原因で Cloud Compliance がスキャンできないボリュームです。

< Back

Newdatastore Configuration

☒ Activate Compliance for all Volumes
 | 28/28 Volumes selected for compliance scan

 🔍 [Edit CIFS Credentials](#)

| Compliance | Name ↑↑ | Protocol ↑↑ | Status ↑↑ | Required Action ↑↑ |
|-------------------------------------|---------------------------|-------------|-------------------------|--|
| <input checked="" type="checkbox"/> | 10.160.7.6/yuval22 | NFS | ● Continuously Scanning | |
| <input checked="" type="checkbox"/> | 10.160.7.6/yuvalnewtarget | NFS | ● Continuously Scanning | |
| <input checked="" type="checkbox"/> | \\10.160.7.6\Danny_share | CIFS | ● No Access | The CIFS credentials that you provided have expired. Edit the CIFS credential... |

SnapMirror を使用してオンプレミスの **ONTAP** データをスキャンする

オンプレミスの NFS または CIFS データを Cloud Volumes ONTAP 作業環境にレプリケートし、それらのデータ保護ボリュームのコンプライアンスを有効にすることで、オンプレミスの ONTAP データをクラウドコンプライアンスでスキャンできます。

ヒント

でオンプレミスの ONTAP システムを検出することを推奨します Cloud Manager を使用して、作成したものを作業環境に追加します 可能です ["Cloud Compliance からシステム上のデータを直接スキャンできます"](#)。

が必要です ["Cloud Manager に Cloud Compliance のインスタンスを導入済みである"](#)。

手順

- Cloud Manager で、オンプレミスの ONTAP クラスタと Cloud Volumes ONTAP の間に SnapMirror 関係を作成します。
 - ["Cloud Manager でオンプレミスクラスタを検出"](#)。
 - ["オンプレミスの ONTAP クラスタとの間に、SnapMirror レプリケーションを作成 Cloud Manager から Cloud Volumes ONTAP にアクセスします"](#)。
- Cloud Manager から、SnapMirror データが格納されている Cloud Volumes ONTAP 作業環境で Cloud Compliance をアクティブ化します。
 - [「* キャンバス *」](#) をクリックします。
 - SnapMirror データを含む作業環境を選択し、[* コンプライアンスを有効にする *](#) をクリックします。

["Cloud Compliance の有効化に関するサポートが必要な場合は、ここをクリックしてください Cloud Volumes ONTAP システム"](#)。

- [_Configuration_page](#) の上部にある [* DP ボリュームへのアクセスを有効にする *](#) ボタンをクリックして、Cloud Compliance が DP ボリュームにアクセスできるようにします。

NFS ボリュームが有効になっているが、CIFS ボリュームには Active Directory 管理者クレデンシャルの入力が必要である。

- スキャンする各 DP ボリュームをアクティブ化するか、[* すべてのボリュームのコンプライアンスのアクティブ化 *](#) コントロールを使用して、すべての DP ボリュームを含むすべてのボリュームを有効にします。

を参照してください ["データ保護ボリュームをスキャンしています"](#) を参照してください。

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.