



Cloud Volumes ONTAP、オンプレミス ONTAP、 Azure NetApp Files 向けクラウドデータサービスを最初に導入する 方法

Cloud Manager

Tom Onacki, Ben Cammett
June 06, 2021

This PDF was generated from https://docs.netapp.com/ja-jp/occm/task_getting_started_compliance.html on June 08, 2021. Always check docs.netapp.com for the latest.

目次

Cloud Volumes ONTAP、オンプレミス ONTAP、Azure NetApp Files

向けクラウドデータサービスを最初に導入する方法	1
クイックスタート	1
スキャンするデータソースを検出しています	2
Cloud Data Sense インスタンスの導入	2
作業環境でクラウドデータを有効に活用	2
Cloud Data Sense がボリュームにアクセスできることの確認	3
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	5
オンプレミスの ONTAP システムからバックアップファイルをスキャンする	6
データ保護ボリュームをスキャンしています	7

Cloud Volumes ONTAP、オンプレミス ONTAP、Azure NetApp Files 向けクラウドデータサービスを最初に導入する方法

Cloud Volumes ONTAP、オンプレミス ONTAP システム、Azure NetApp Files 向けクラウドデータセンスの導入を開始するには、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。

目的のデータが含まれているデータソースを検出します をクリックしてください

ボリュームをスキャンする前に、Cloud Manager でシステムを作業環境として追加する必要があります。

- Cloud Volumes ONTAP システムの場合、これらの作業環境はすでに Cloud Manager で使用可能になっている必要があります
- オンプレミスの ONTAP システムでは、["ONTAP クラスタは Cloud Manager で検出する必要があります"](#)
- Azure NetApp Files の場合、["構成を検出するには、Cloud Manager が設定されている必要があります"](#)。

Cloud Data Sense インスタンスを導入する

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

Cloud Data Sense を有効にして、スキャンするボリュームを選択します

コンプライアンス * をクリックし、* 構成 * タブを選択して、特定の作業環境で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 Data Sense 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。

- クラウドデータセンシンスインスタンスには、各 Cloud Volumes ONTAP サブネット、Azure NetApp Files サブネット、またはオンプレミスの ONTAP システムへのネットワーク接続が必要です。
- Cloud Volumes ONTAP のセキュリティグループは、データセンシンス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。
- これらのポートが Data Sense インスタンスに対して開いていることを確認します。
 - NFS –ポート 111 および 2049。
 - CIFS の場合 - ポート 139 および 445
- NFS ボリュームエクスポートポリシーで、データセンシンス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、Active Directory 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 Data Sense でスキャンが開始または停止します。

スキャンするデータソースを検出しています

スキャンするデータソースがまだ Cloud Manager 環境にない場合は、ここでキャンバスに追加できます。

Cloud Volumes ONTAP システムは、Cloud Manager のキャンバスですでに使用できるようになっている必要があります。オンプレミスの ONTAP システムには、が必要です ["これらのクラスタは Cloud Manager で検出されます"](#)。Azure NetApp Files の場合は、["構成を検出するには、Cloud Manager が設定されている必要があります"](#)。

Cloud Data Sense インスタンスの導入

["クラウドデータの導入センス"](#) インスタンスが展開されていない場合。

クラウドデータセンスは、Cloud Volumes ONTAP やオンプレミスの ONTAP システムをスキャンする際に、クラウドやオンプレミスの場所に導入することができます。

Azure NetApp Files ボリュームをスキャンするときは、データセンスをクラウドに導入する必要があります。また、スキャンするボリュームと同じリージョンに導入する必要があります。

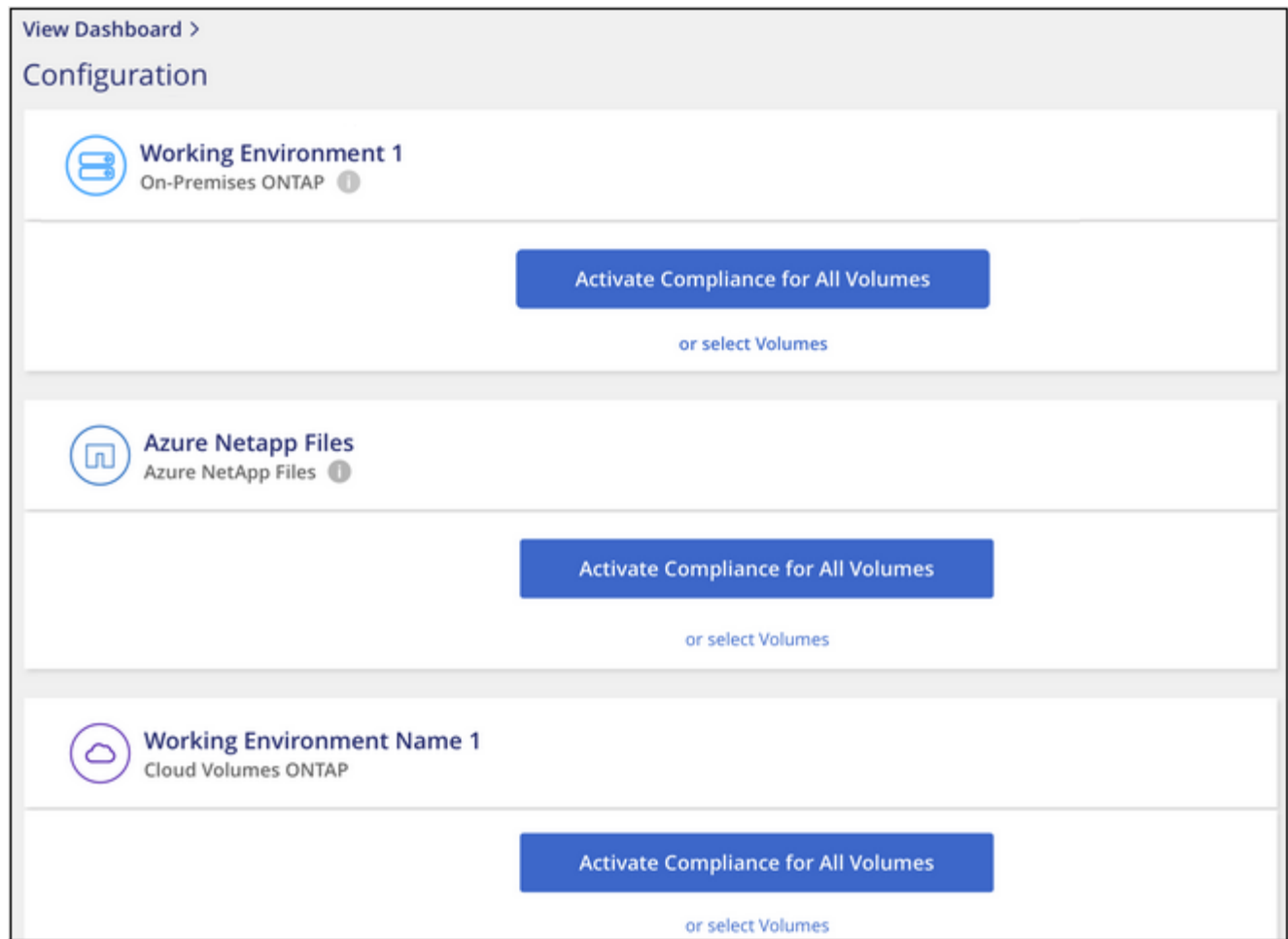
作業環境でクラウドデータを有効に活用

Cloud Volumes ONTAP システム（AWS および Azure）、オンプレミスの ONTAP クラスタ、および Azure NetApp Files でクラウドデータセンスを有効にすることができます。



オンプレミス ONTAP システムで次の手順を実行すると、オンプレミス ONTAP システム上のボリュームが直接スキャンされます。すでにオンプレミスからバックアップファイルを作成している場合 ["クラウドバックアップ"](#)ではなく、クラウド内のバックアップファイルに対してコンプライアンススキャンを実行できます。に進みます [オンプレミスの ONTAP システムからバックアップファイルをスキャンする](#) バックアップファイルをスキャンしてボリュームをスキャンします。

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



タブのスクリーンショット。"]

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 Data Sense により、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 Data Sense が最初のスキャンを完了するとすぐに Compliance ダッシュボードに表示されます。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 Data Sense 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 Data Sense で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、 CIFS クレデンシャルをデータセンスに指定する必要があります。

手順

1. クラウドデータセンスインスタンスと、 Cloud Volumes ONTAP 、 Azure NetApp Files 、 オンプレミスの ONTAP クラスター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確立されていることを確認します。

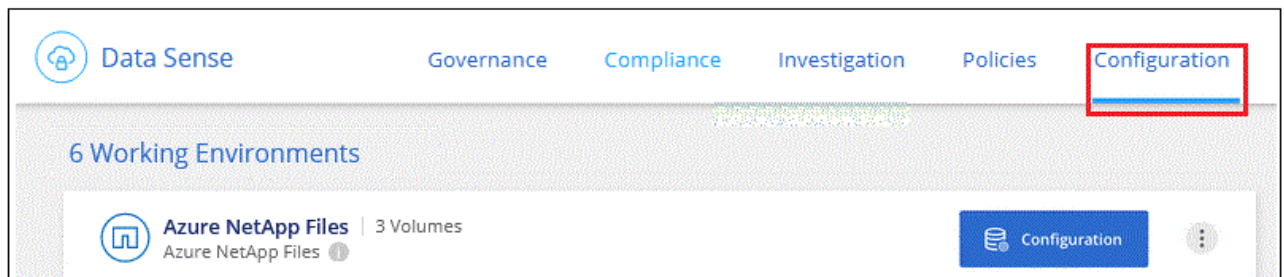


Azure NetApp Files の場合、Cloud Data Sense は Cloud Manager と同じリージョンにあるボリュームのみをスキャンできます。

2. Cloud Volumes ONTAP のセキュリティグループがデータセンシブ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。

データセンシブインスタンスの IP アドレスからのトラフィックのセキュリティグループを開くか、仮想ネットワーク内からのすべてのトラフィックのセキュリティグループを開くことができます。

3. 次のポートがデータセンシブインスタンスに対して開いていることを確認します。
 - NFS –ポート 111 および 2049。
 - CIFS の場合 - ポート 139 および 445
4. NFS ボリュームのエクスポートポリシーに、各ボリュームのデータにアクセスできるように Data sense インスタンスの IP アドレスが含まれていることを確認します。
5. CIFS を使用する場合は、CIFS ボリュームをスキャンできるように、Active Directory クレデンシャルを使用したデータセンスを設定します。
 - a. Cloud Manager の上部で、* Data Sense * をクリックします。
 - b. [* 構成 *] タブをクリックします。

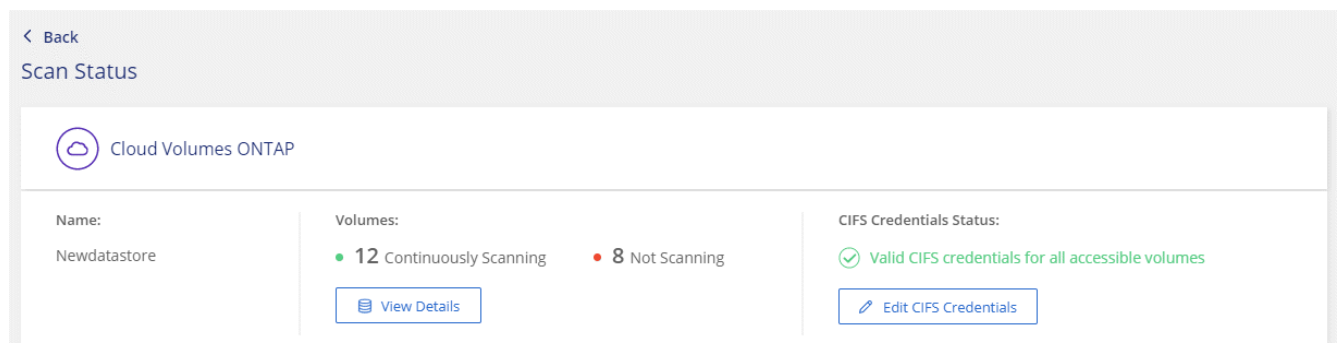


ボタンを示す [遵守] タブのスクリーンショット。"]

- c. 各作業環境について、* CIFS 資格情報の編集 * をクリックし、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、データセンス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 Data Sense 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。



6. 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、データセンシブ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クラウドデータセンシブでスキャンできないボリュームです。

Compliance	Name	Protocol	Status	Required Action
<input checked="" type="checkbox"/>	10.160.7.6/ylval22	NFS	Continuously Scanning	
<input checked="" type="checkbox"/>	10.160.7.6/ylvalnewtarget	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...

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

作業環境内のボリュームのスキャンは、設定ページからいつでも停止または開始できます。すべてのボリュームをスキャンすることを推奨します。

Compliance	Volume Name	Status	Required Action
<input checked="" type="checkbox"/>	VolumeName1	Not Scanning	Add CIFS Credentials
<input checked="" type="checkbox"/>	VolumeName2	Continuously Scanning	
<input type="checkbox"/>	VolumeName3	Not Scanning	
<input checked="" type="checkbox"/>	VolumeName4	Continuously Scanning	
<input checked="" type="checkbox"/>	VolumeName5	Continuously Scanning	

終了：	手順：
ボリュームのスキャンを無効にします	音量スライダを左に動かします
すべてのボリュームのスキャンを無効にします	[すべてのボリュームのコンプライアンスを有効にする *] スライダを左に移動します
ボリュームのスキャンを有効にします	音量スライダを右に動かします
すべてのボリュームのスキャンを有効にします	[すべてのボリュームのコンプライアンスを有効にする *] スライダを右に移動します



作業環境に追加した新しいボリュームは、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 * 設定が有効になっている場合にのみ自動的にスキャンされます。この設定を無効にすると、作業環境で作成する新しいボリュームごとにスキャンを有効にする必要があります。

オンプレミスの ONTAP システムからバックアップファイルをスキャンする

Cloud Data Sense でオンプレミスの ONTAP システム上のボリュームを直接スキャンしない場合は、2021 年 1 月にリリースされる新しいベータ機能によって、オンプレミスの ONTAP ボリュームから作成されたバックアップファイルに対してコンプライアンススキャンを実行できます。を使用してバックアップファイルを既に作成している場合は ["クラウドバックアップ"](#)この新機能を使用して、バックアップファイルに対してコンプライアンススキャンを実行できます。

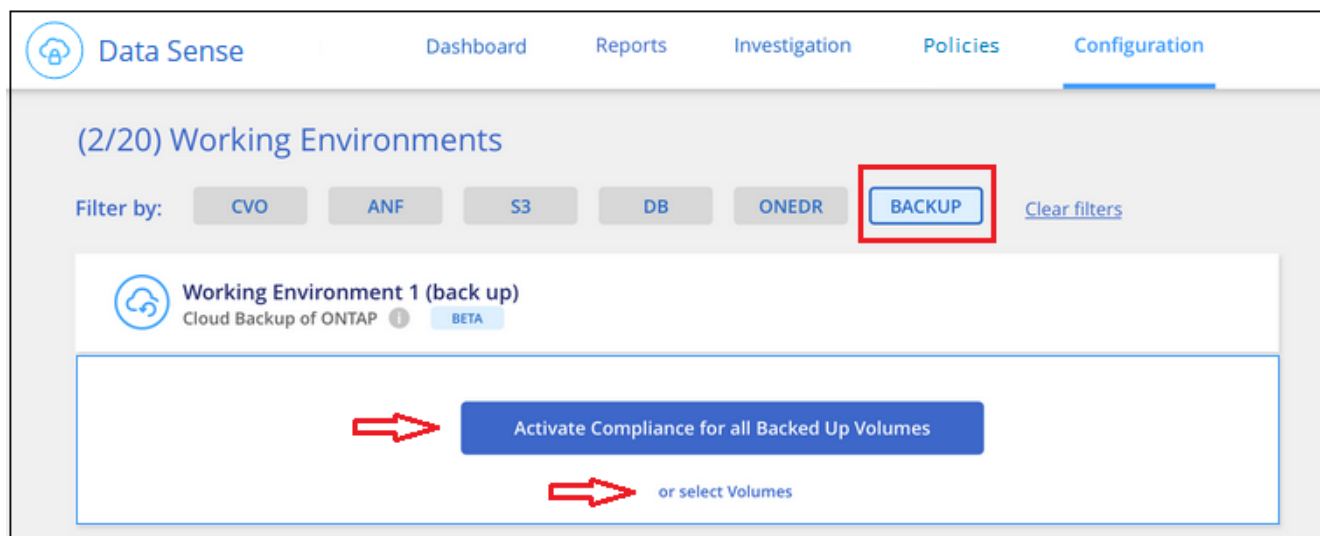
バックアップファイルで実行するコンプライアンススキャンは * 無料 * - Cloud Data Sense サブスクリプションやライセンスは不要です。

- ・注： * データセンスがバックアップファイルをスキャンすると、Cloud Restore インスタンスを通じて付与された権限を使用してバックアップファイルにアクセスします。通常、ファイルをアクティブにリストアしていない場合はリストア・インスタンスの電源がオフになりますが、バックアップ・ファイルのスキャン時はオンのまま * になります。を参照してください ["Restore インスタンスに関する詳細情報"](#)。

オンプレミスの ONTAP システムからバックアップファイルをスキャンする場合は、次の手順を実行します。

1. Cloud Manager の上部で、 * Data Sense * をクリックし、 * Configuration * タブを選択します。
2. 作業環境のリストで、フィルタのリストから * backup * ボタンをクリックします。

バックアップファイルがあるオンプレミスの ONTAP 作業環境がすべて表示されます。オンプレミスシステムのバックアップファイルがない場合、作業環境は表示されません。



3. 作業環境でバックアップされたすべてのボリュームをスキャンするには、 * すべてのバックアップされた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。

作業環境でバックアップされた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、スキャンするバックアップファイル（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。

オンプレミスボリュームをスキャンするか、それらのボリュームのバックアップをスキャンするか

作業環境のリスト全体を表示すると、ファイルをバックアップしている場合は、オンプレミスクラスタごとに 2 つのリストが表示されます。



最初の項目はオンプレミスクラスタと実際のボリュームです。2 番目の項目は、同じオンプレミスクラスタにあるボリュームのバックアップファイルです。

オンプレミスシステム上のボリュームをスキャンする最初のオプションを選択します。2 番目のオプションを選択して、対象のボリュームからバックアップファイルをスキャンします。同じクラスタのオンプレミスボリュームとバックアップファイルの両方をスキャンしないでください。

データ保護ボリュームをスキャンしています

デフォルトでは、データ保護（ DP ）ボリュームは外部から公開されておらず、クラウドデータセンスでアクセスできないため、スキャンされません。オンプレミスの ONTAP システムまたは Cloud Volumes ONTAP システムからの SnapMirror 処理のデスティネーションボリュームです。

最初は、ボリュームリストでこれらのボリュームを *Type* DP ** でスキャンしていないステータス * および必要なアクション *_ * DP* ボリュームへのアクセスを有効にします *。

'Working Environment Name' Configuration

☐ Activate Compliance for all Volumes | 22/28 Volumes selected for compliance scan

[Enable Access to DP Volumes](#)
[Edit CIFS Credentials](#)

Compliance	Volume Name	Type	Status	Required Action
<input type="checkbox"/>	VolumeName1	DP	Not Scanning	Enable access to DP Volumes
<input checked="" type="checkbox"/>	VolumeName2	NFS	Continuously Scanning	
<input type="checkbox"/>	VolumeName3	CIFS	Not Scanning	

これらのデータ保護ボリュームをスキャンする場合は、次の手順を実行します。

1. ページ上部の * DP ボリュームへのアクセスを有効にする * をクリックします。
2. 確認メッセージを確認し、もう一度「 * DP ボリュームへのアクセスを有効にする * 」をクリックします。
 - ソース ONTAP システムで最初に NFS ボリュームとして作成されたボリュームが有効になります。
 - ソース ONTAP システムで最初に CIFS ボリュームとして作成されたボリュームでは、それらの DP ボリュームをスキャンするために CIFS クレデンシャルを入力する必要があります。Cloud Data Sense で CIFS ボリュームをスキャンするためにすでに Active Directory のクレデンシャルを入力している場合は、それらのクレデンシャルを使用できます。また、別の管理クレデンシャルを指定することもできます。

Provide Active Directory Credentials

☒ Use existing CIFS Scanning Credentials (user1@domain2)
 ☐ Use Custom Credentials

Active Directory Domain
 DNS IP Address

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

[Enable Access to DP Volumes](#)
[Cancel](#)

Provide Active Directory Credentials

☐ Use existing CIFS Scanning Credentials (user1@domain2)
 ☒ Use Custom Credentials

Username
 Password

Active Directory Domain
 DNS IP Address

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

[Enable Access to DP Volumes](#)
[Cancel](#)

3. スキャンする各 DP ボリュームをアクティブ化します [他のボリュームも有効にした場合と同じです](#) をクリックするか、すべてのボリュームで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。

有効にすると、スキャン対象としてアクティブ化された各 DP ボリュームから NFS 共有が作成されます。共有エクスポートポリシーでは、データセンスインスタンスからのアクセスのみが許可されます。

- ・注： DP ボリュームへのアクセスを最初に有効にしたときに CIFS データ保護ボリュームがない場合は、あとで追加しても、CIFS DP の有効化ボタン * が設定ページの上部に表示されます。このボタンをクリックして、CIFS DP ボリュームへのアクセスを有効にする CIFS クレデンシャルを追加します。

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.