



転送中のデータ暗号化を使用した NFS データの同期 Cloud Manager

Ben Cammett
April 24, 2021

目次

転送中のデータ暗号化を使用した NFS データの同期	1
データインフラライト暗号化の仕組み	1
サポートされている NFS のバージョン	2
プロキシサーバの制限事項	2
作業を開始するために必要なもの	2
転送中のデータ暗号化を使用した NFS データの同期	2

転送中のデータ暗号化を使用した **NFS** データの同期

厳格なセキュリティポリシーを適用している場合は、転送中データの暗号化を使用して NFS データを同期できます。この機能は、NFS サーバから別の NFS サーバ、および Azure NetApp Files から Azure NetApp Files へサポートされます。

たとえば、異なるネットワークにある 2 つの NFS サーバ間でデータを同期できます。また、サブネットやリジョン間で Azure NetApp Files 上のデータをセキュアに転送しなければならない場合もあります。

データインフラライト暗号化の仕組み

データ転送中の暗号化では、2 つのデータブローカー間でネットワークを介して送信される NFS データが暗号化されます。次の図は、2 つの NFS サーバと 2 つのデータブローカーの関係を示しています。



1 つのデータブローカーは、*initiator* として機能します。データを同期するときは、接続要求をもう 1 つのデータブローカー（つまり *listener*）に送信します。そのデータブローカーは、ポート 443 で要求をリスンします。必要に応じて別のポートを使用できますが、そのポートが別のサービスで使用されていないことを確認してください。

たとえば、オンプレミスの NFS サーバからクラウドベースの NFS サーバにデータを同期する場合、接続要求を受信するデータブローカーと送信するデータブローカーを選択できます。

転送中の暗号化の仕組みは次のとおりです。

1. 同期関係を作成すると、イニシエータは他のデータブローカーとの暗号化された接続を開始します。
2. ソースデータブローカーは、TLS 1.3 を使用してソースのデータを暗号化します。
3. 次に、ネットワーク経由でデータをターゲットデータブローカーに送信します。
4. ターゲットのデータブローカーは、ターゲットに送信する前にデータを復号化します。
5. 最初のコピーの後、変更されたデータは 24 時間ごとに同期されます。同期するデータがある場合は、イニシエータが他のデータブローカーとの暗号化された接続を開いてプロセスが開始されます。

データをより頻繁に同期する場合は、["スケジュールは関係の作成後に変更することができます"](#)。

サポートされている NFS のバージョン

- NFS サーバでは、データ転送時の暗号化が NFS バージョン 3、4.0、4.1、4.2 でサポートされています。
- Azure NetApp Files では、NFS バージョン 3 および 4.1 でデータ転送時の暗号化がサポートされます。

プロキシサーバの制限事項

暗号化された同期関係を作成すると、暗号化されたデータは HTTPS 経由で送信され、プロキシサーバ経由でルーティングすることはできません。

作業を開始するために必要なもの

次のものを用意してください。

- に対応した 2 台の NFS サーバ ["移行元と移行先の要件"](#) または、2 つのサブネットまたはリージョンの Azure NetApp Files。
- サーバの IP アドレスまたは完全修飾ドメイン名。
- 2 つのデータブローカーのネットワークロケーション。

既存のデータブローカーを選択できますが、イニシエータとして機能する必要があります。リスナーデータブローカーは、_NET_DATA ブローカーである必要があります。

データブローカーをまだ導入していない場合は、データブローカーの要件を確認します。厳格なセキュリティポリシーがあるため、ポート 443 およびからの発信トラフィックを含むネットワーク要件を確認してください ["インターネットエンドポイント"](#) データブローカーの連絡先。

- ["AWS のインストールを確認します"](#)
- ["Azure のインストールを確認します"](#)
- ["GCP のインストールを確認します"](#)
- ["Linux ホストのインストールを確認します"](#)

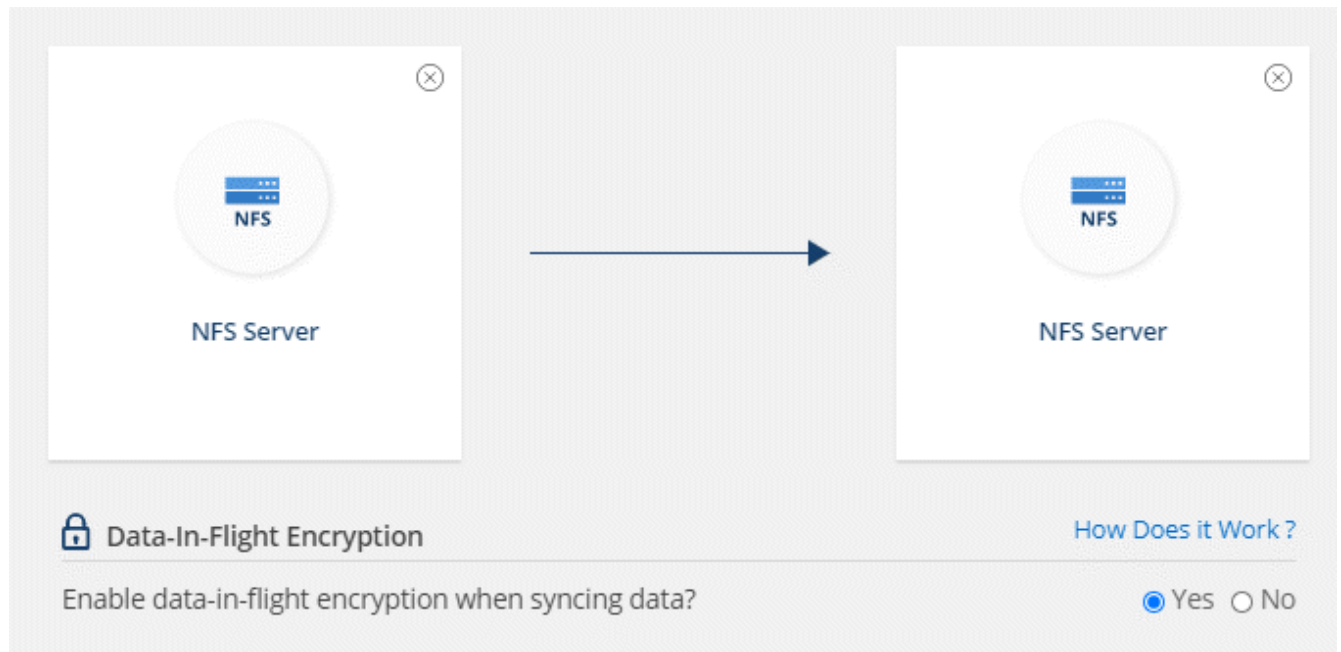
転送中のデータ暗号化を使用した NFS データの同期

2 つの NFS サーバ間または Azure NetApp Files 間で新しい同期関係を作成し、転送中の暗号化オプションを有効にして、画面の指示に従います。

手順

1. [新しい同期の作成 *] をクリックします。
2. NFS サーバ * をソースとターゲットの場所にドラッグアンドドロップするか、* Azure NetApp Files * をソースとターゲットの場所にドラッグアンドドロップして、* はい * を選択して転送中のデータ暗号化を有効にします。

次の図は、2 つの NFS サーバ間でデータを同期する際に選択する内容を示しています。



次の図は、Azure NetApp Files 間でデータを同期する際に選択する内容を示しています。



3. プロンプトに従って関係を作成します。

- a. * NFS サーバ * / * Azure NetApp Files * : NFS のバージョンを選択し、新しい NFS ソースを指定するか、既存のサーバを選択します。
- b. * データブローカー機能の定義 * : ポート上での接続要求に対して ' どのデータ・ブローカ・リスナー ' がどのデータ・ブローカ・リスナー を実行するか ' およびどのデータ・ブローカが接続を開始するかを定義しますネットワークング要件に基づいて選択してください。
- c. * データブローカー * : 新しいソースデータブローカーを追加するか、既存のデータブローカーを選択するよう求められます。

ソースデータブローカーがリスナーとして機能する場合は、新しいデータブローカーである必要があ

ります。

新しいデータブローカーが必要な場合は、インストール手順が表示されます。クラウドにデータブローカーを導入したり、独自の Linux ホスト用のインストールスクリプトをダウンロードしたりできます。



- d. * ディレクトリ *: すべてのディレクトリを選択するか、ドリルダウンしてサブディレクトリを選択して、同期するディレクトリを選択します。

「* ソースオブジェクトのフィルター *」をクリックして、ソースファイルとフォルダーの同期方法とターゲットの場所での維持方法を定義する設定を変更します。




オプションを選択するオプションを示すスクリーンショット。"]

- e. * ターゲット NFS サーバー */ * ターゲット Azure NetApp Files * : NFS バージョンを選択し、新しい NFS ターゲットを入力するか、既存のサーバーを選択します。
- f. * ターゲットデータブローカー * : 新しいソースデータブローカーを追加するか、既存のデータブローカーを選択するよう求められます。


ターゲットデータブローカーがリスナーとして機能する場合は、新しいデータブローカーである必要があります。

ターゲットのデータブローカーがリスナーとして機能する場合のプロンプトの例を次に示します。ポートを指定するオプションに注目してください。


Select a Provider




Microsoft Azure



Amazon Web Services



Google Cloud Platform



On-Prem Data Broker

Data Broker Name

Port

- a. * ターゲットディレクトリ * : トップレベルのディレクトリを選択するか、ドリルダウンして既存のサブディレクトリを選択するか、エクスポート内に新しいフォルダを作成します。
- b. * 設定 * : ソースファイルとフォルダをターゲットの場所で同期および維持する方法を定義します。
- c. * 確認 * : 同期関係の詳細を確認し、* 関係の作成 * をクリックします。



Cloud Sync が新しい同期関係の作成を開始します。完了したら、[ダッシュボードで表示] をクリックして、新しい関係の詳細を表示します。

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.