



データセキュリティ ASA r2

NetApp
September 26, 2024

目次

データセキュリティ	1
ASA R2ストレージシステム上の保存データの暗号化	1
ASA R2ストレージシステムに対するランサムウェア攻撃からデータを保護	2
ASA R2ストレージシステム上のセキュアなNVMe接続	2

データセキュリティ

ASA R2ストレージシステム上の保存データの暗号化

保存データを暗号化すると、ストレージメディアの転用、返却、置き忘れ、盗難に際してデータを読み取ることができません。ONTAP System Managerを使用してデータをハードウェアレベルとソフトウェアレベルで暗号化し、デュアルレイヤ保護を実現できます。

NetAppストレージ暗号化（NSE）は、自己暗号化ドライブ（SED）を使用したハードウェア暗号化をサポートしています。SEDはデータを書き込み時に暗号化します。各SEDには一意の暗号化キーが含まれています。SEDに保存されている暗号化されたデータは、SEDの暗号化キーなしでは読み取ることができません。SEDから読み取るノードは、SEDの暗号化キーにアクセスするために認証される必要があります。ノードの認証では、キー管理ツールから認証キーを取得し、その認証キーをSEDに提供します。認証キーが有効な場合、SEDはノードに格納されたデータにアクセスするための暗号化キーをノードに付与します。

ASA R2のオンボードキーマネージャまたは外部キーマネージャを使用して、ノードに認証キーを提供します。

NSEに加えて、ソフトウェア暗号化を有効にしてデータのセキュリティを強化することもできます。

手順

1. System Managerで、*[クラスタ]>[設定]*を選択します。
2. セクションの[暗号化]で、[設定]*を選択します。
3. キー管理ツールを設定します。

オプション	手順
オンボードキーマネージャの設定	<ol style="list-style-type: none">a. [オンボードキーマネージャ]*を選択してキーサーバを追加します。b. パスフレーズを入力します。
外部キー管理ツールを設定する	<ol style="list-style-type: none">a. [外部キーマネージャ]*を選択してキーサーバを追加します。b. + Add キーサーバを追加する場合に選択します。c. KMIPサーバCA証明書を追加します。d. KMIPクライアント証明書を追加します。

4. [デュアルレイヤ暗号化]*を選択して、ソフトウェア暗号化を有効にします。
5. [保存（Save）]を選択します。

次の手順

保存データの暗号化が完了したので、NVMe/TCPプロトコルを使用している場合は["ネットワーク経由で送信されるすべてのデータを暗号化"](#)、NVMe/TCPホストとASA R2システムの間でデータを暗号化できます。


ASA R2ストレージシステムに対するランサムウェア攻撃からデータを保護

ランサムウェア攻撃に対する保護を強化するには、Snapshotをリモートクラスタにレプリケートし、デスティネーションSnapshotをロックして改ざんを防止します。ロックされたSnapshotは、誤ってまたは悪意を持って削除することはできません。ロックされたSnapshotを使用して、ランサムウェア攻撃によってストレージユニットが侵害された場合にデータをリカバリできます。

SnapLock Complianceクロックの初期化

改ざん防止Snapshotを作成する前に、ローカルクラスタとデスティネーションクラスタでSnapLock Complianceクロックを初期化する必要があります。

手順

1. [*Cluster] > [Overview] を選択します。
2. セクションで、[Initialize SnapLock Compliance Clock]*を選択します。
3. [初期化]*を選択します。
4. コンプライアンスクロックが初期化されていることを確認します。
 - a. [*Cluster] > [Overview] を選択します。
 - b. セクションでを選択し、 SnapLock Compliance Clock *を選択します。

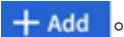

次の手順

ローカルクラスタとデスティネーションクラスタでSnapLock Complianceクロックを初期化したら、を実行できます"[ロックされたSnapshotを使用してレプリケーション関係を作成する](#)"。

ASA R2ストレージシステム上のセキュアなNVMe接続

NVMeプロトコルを使用している場合は、インバンド認証を設定してデータセキュリティを強化できます。インバンド認証を使用すると、NVMeホストとASA R2システムの間でセキュアな双方向認証と一方向認証を確立できます。インバンド認証はすべてのNVMeホストで使用できます。NVMe/TCPプロトコルを使用している場合は、NVMe/TCPホストとASA R2システムの間でネットワーク経由で送信されるすべてのデータを暗号化するようにトランスポートレイヤセキュリティ (TLS) を設定することで、データセキュリティをさらに強化できます。

手順

1. を選択し、[NVMe]*を選択します。
2. を選択します 。
3. ホスト名を入力し、ホストオペレーティングシステムを選択します。
4. ホストの説明を入力し、ホストに接続するStorage VMを選択します。
5.  ホスト名の横にあるを選択します。

6. [インバンド認証]*を選択します。
7. NVMe/TCPプロトコルを使用している場合は、*[Transport Layer Security (TLS) が必要]*を選択します。
8. 「* 追加」を選択します。

結果

インバンド認証やTLSによって、データのセキュリティが強化されます。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。