評価されるセキュリティ条件

Active IQ Unified Manager 9.14

NetApp
March 07, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/active-iq-unified-manager/health-checker/reference_cluster_compliance_categories.html on March 07, 2024. Always check docs.netapp.com for the latest.

目次

評価されるセキュリティ条件 1
クラスタコンプライアンスのカテゴリ 1
Storage VM コンプライアンスのカテゴリ 5
ボリュームコンプライアンスのカテゴリ 6

評価されるセキュリティ条件

一般に、 ONTAP クラスタ、 Storage Virtual Machine （ SVM ）、およびボリュームのセキュリティ条件は、『 ONTAP 9_ ネットアップセキュリティ設定ガイド』に定義されている推奨事項に照らして評価されます。

セキュリティチェックには、次のようなものがあります。

- クラスタが SAML などのセキュアな認証方式を使用しているかどうか
- ピアクラスタの通信が暗号化されているかどうか
- Storage VM の監査ログが有効になっているかどうか
- ボリュームでソフトウェアまたはハードウェアの暗号化が有効になっているかどうか

コンプライアンスのカテゴリおよびのトピックを参照してください "『 ONTAP 9 セキュリティ設定ガイド』" を参照してください。

> Active IQ プラットフォームから報告されるアップグレードイベントもセキュリティイベントとみなされます。これらのイベントは、 ONTAP ソフトウェア、ノードファームウェア、またはオペレーティングシステムソフトウェア（セキュリティアドバイザリ用）のアップグレードが必要な問題を示します。これらのイベントは [セキュリティ] パネルには表示されませんが、 [イベント管理] インベントリページから確認できます。

詳細については、を参照してください "クラスタのセキュリティ目標の管理"。

クラスタコンプライアンスのカテゴリ

次の表に、 Unified Manager で評価されるクラスタセキュリティコンプライアンスのパラメータ、ネットアップの推奨事項、およびクラスタが準拠か非準拠かの総合的な判断にパラメータが影響するかどうかを示します。

クラスタに非準拠の SVM があると、クラスタのコンプライアンスに影響します。そのため、クラスタのセキュリティが準拠とみなされるためには、事前に SVM のセキュリティ問題の修正が必要となる場合があります。

以下のパラメータは、すべてのインストール環境で表示されるわけではありません。たとえば、ピアクラスタがない場合やクラスタで AutoSupport を無効にしている場合、「クラスタピアリング」や「 AutoSupport HTTPS 転送」の項目は表示されません。

パラメータ	説明	推奨事項	クラスタコンプライアンスに影響します
グローバル FIPS	グローバル FIPS （連邦情報処理標準） 140-2 準拠モードが有効になっているかどうかを示します。FIPS を有効にすると、 TLSv1 と SSLv3 は無効になり、 TLSv1.1 と TLSv1.2 のみが許可されます。	有効	はい。
Telnet	システムへの Telnet アクセスが有効になっているかどうかを示します。ネットアップでは、セキュアなリモートアクセスのために Secure Shell （ SSH ）を推奨しています。	無効	はい。
セキュアでない SSH 設定	SSH でセキュアでない暗号を使用しているかどうかを示します。たとえば、 CBC で始まる暗号などです。	いいえ	はい。
ログインバナー	システムにアクセスするユーザに対してログインバナーが有効になっているかどうかを示します。	有効	はい。
クラスタピアリング	ピアクラスタ間の通信が暗号化されているかどうかを示します。このパラメータが準拠とみなされるためには、ソースとデスティネーションの両方のクラスタで暗号化が設定されている必要があります。	暗号化	はい。

パラメータ	説明	推奨事項	クラスタコンプライアンスに影響します
Network Time Protocol の略	クラスタに NTP サーバが 1 つ以上設定されているかどうかを示します。ネットアップでは、冗長性と最適なサービスを実現するために最低 3 台の NTP サーバをクラスタに関連付けることを推奨しています。	を設定します	はい。
OCSP	ONTAP に OCSP （ Online Certificate Status Protocol ）が設定されていないアプリケーションがないか、そのため通信が暗号化されていないかどうかを示します。非準拠のアプリケーションが一覧表示されます。	有効	いいえ
リモート監査ログ	ログ転送（ syslog ）が暗号化されているかどうかを示します。	暗号化	はい。
AutoSupport HTTPS 転送	ネットアップサポートに AutoSupport メッセージを送信するためのデフォルトの転送プロトコルとして HTTPS が使用されているかどうかを示します。	有効	はい。
デフォルトの管理ユーザ	デフォルトの管理ユーザ（組み込み）が有効になっているかどうかを示します。ネットアップでは、不要な組み込みアカウントはすべてロック（無効化）することを推奨しています。	無効	はい。
SAML ユーザ	SAML が設定されているかどうかを示します。SAML を使用すると、シングルサインオンのログイン方法として多要素認証（ MFA ）を設定できます。	いいえ	いいえ

パラメータ	説明	推奨事項	クラスタコンプライアンスに影響します
Active Directory ユーザ	Active Directory が設定されているかどうかを示します。Active Directory と LDAP は、クラスタにアクセスするユーザに対して推奨される認証メカニズムです。	いいえ	いいえ
LDAP ユーザ	LDAP が設定されているかどうかを示します。Active Directory と LDAP は、ローカルユーザよりもクラスタを管理するユーザに対して推奨される認証メカニズムです。	いいえ	いいえ
証明書ユーザ	証明書ユーザがクラスタにログインするように設定されているかどうかを示します。	いいえ	いいえ
ローカルユーザ	ローカルユーザがクラスタにログインするように設定されているかどうかを示します。	いいえ	いいえ
リモートシェル（ Remote Shell ）	RSH が有効になっているかどうかを示します。セキュリティ上の理由から、 RSH は無効にする必要があります。セキュアなリモートアクセスを実現するために、 Secure Shell （ SSH ）が推奨されます。	無効	はい。
MD5 使用中です	ONTAP ユーザアカウントでセキュアでない MD5 ハッシュ関数を使用しているかどうかを示します。MD5 ハッシュ化されたユーザアカウントは、SHA-512 などのより安全な暗号化ハッシュ関数への移行が推奨されます。	いいえ	はい。

パラメータ	説明	推奨事項	クラスタコンプライアンスに影響します
証明書発行者タイプ	使用されているデジタル証明書のタイプを示します。	CA 署名	いいえ

Storage VM コンプライアンスのカテゴリ

次の表に、 Unified Manager で評価される Storage Virtual Machine （ SVM ）セキュリティコンプライアンスの条件、ネットアップの推奨事項、および SVM が準拠か非準拠かの総合的な判断にパラメータが影響するかどうかを示します。

パラメータ	説明	推奨事項	**SVM** コンプライアンスに影響します
監査ログ	監査ロギングが有効になっているかどうかを示します。	有効	はい。
セキュアでない SSH 設定	SSH が安全でない暗号を使用しているかどうかを示します。たとえば、「 CBC * 」で始まる暗号などです。	いいえ	はい。
ログインバナー	システムで SVM にアクセスするユーザに対してログインバナーが有効になっているかどうかを示します。	有効	はい。
LDAP 暗号化	LDAP 暗号化が有効になっているかどうかを示します。	有効	いいえ
NTLM 認証	NTLM 認証が有効になっているかどうかを示します。	有効	いいえ
LDAP ペイロードの署名	LDAP ペイロードの署名が有効になっているかどうかを示します。	有効	いいえ
CHAP 設定	CHAP が有効になっているかどうかを示します。	有効	いいえ

パラメータ	説明	推奨事項	**SVM** コンプライアンスに影響します
Kerberos V5	Kerberos v5 認証が有効か無効かを示します。	有効	いいえ
NIS 認証	NIS 認証の使用が設定されているかどうかを示します。	無効	いいえ
FPolicy ステータスがアクティブです	FPolicy が作成されているかどうかを示します。	はい。	いいえ
SMB 暗号化が有効です	SMB 署名と封印が有効になっていないかどうかを示します。	はい。	いいえ
SMB 署名が有効になりました	SMB 署名が有効になっていないかどうかを示します。	はい。	いいえ

ボリュームコンプライアンスのカテゴリ

Unified Manager は、次の表に示すボリューム暗号化パラメータを評価して、ボリューム上のデータが権限のないユーザによるアクセスから適切に保護されているかどうかを判断します。

ボリューム暗号化パラメータは、クラスタまたは Storage VM が準拠しているとみなされるかどうかには影響しません。

パラメータ	説明
暗号化されたソフトウェア	NetApp Volume Encryption （ NVE ）または NetApp Aggregate Encryption （ NAE ）ソフトウェア暗号化ソリューションを使用して保護されているボリュームの数が表示されます。
ハードウェア暗号化	NetApp Storage Encryption （ NSE ）ハードウェア暗号化を使用して保護されているボリュームの数が表示されます。
ソフトウェアとハードウェアを暗号化	ソフトウェア暗号化とハードウェア暗号化の両方で保護されているボリュームの数が表示されます。
暗号化なし	暗号化されていないボリュームの数が表示されます。

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権を有し、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権については、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。