



評価されるセキュリティ条件 Active IQ Unified Manager

NetApp
October 15, 2025

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のコンプライアンス 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、ストレージ仮想マシン (SVM)、およびボリュームのセキュリティ基準は、『NetApp セキュリティ強化ガイド for ONTAP 9』で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

コンプライアンスカテゴリと ["NetApp ONTAP 9 セキュリティ強化ガイド"](#)詳細情報については、



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、["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

この表では、Unified Manager が評価するクラスタ セキュリティ コンプライアンス パラメータ、NetApp の推奨事項、およびパラメータがクラスタが準拠しているかどうかの全体的な判断に影響するかどうかについて説明します。

クラスタ上に非準拠の SVM があると、クラスタのコンプライアンス値に影響します。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어링」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	クラスターコンプライアンスに影響
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。セキュアなリモートアクセスを確立するために、Secure Shell（SSH）を推奨します。	無効	はい
安全でない SSH 設定	SSH が安全でない暗号（たとえば *cbc で始まる暗号）を使用するかどうかを示します。	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
ネットワーク タイム プロトコル	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。冗長性と最適なサービスを確保するために、NetApp少なくとも3台のNTPサーバをクラスタに関連付けることをお勧めします。	設定	はい

パラメータ	説明	推奨事項	クラスターコンプライアンスに影響
OCSP	9.14.1 以降、Active IQ Unified Manager は、ストレージ仮想マシン (SVM、旧称 Vserver) レベルでオンライン証明書ステータス プロトコル (OCSP) ステータス情報を提供します。つまり、SVM へのすべての SSL/TLS 接続に OCSP 検証が適用され、これらの接続で使用される証明書の整合性と有効性が保証されます。	有効	いいえ
リモート監査ログ	ログ転送 (syslog) が暗号化されるかどうかを示します。	暗号化	はい
AutoSupport HTTPS 転送	AutoSupportメッセージをNetAppサポートに送信するためのデフォルトのトランスポート 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。NetApp、不要な組み込みアカウントをロック (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	クラスターコンプライアンスに影響
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、クラスター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ー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ー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 ユーザがクラスター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	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は無効にしてください。セキュアなリモート アクセスを確立するために、Secure Shell (SSH) が推奨されます。	無効	はい
MD5 の使用	ONTAPユーザ アカウントに安全性が低いMD5ハッシュ関数が使用されているかどうかを示します。MD5ハッシュを使用したユーザ アカウントについては、より安全なSHA-512などの暗号化ハッシュ関数に移行することが推奨されます。	いいえ	はい

パラメータ	説明	推奨事項	クラスターコンプライアンスに影響
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のコンプライアンス 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各条件 (パラメータ)、NetAppの推奨設定、およびSVMが準拠しているかどうかの総合的な判断にその条件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
監査ログ	監査ログが有効になっているかどうかを示します。	有効	はい
安全でない 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*。	いいえ	はい
ログイン バナー	システム上の SVM にアクセスするユーザーに対してログイン バナーが有効か無効かを示します。	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
Kerberos V5	Kerberos V5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

パラメータ	説明	推奨事項	SVMコンプライアンスに影響
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 のステータスがアクティブ	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	SMBの署名と封印が有効になっているかどうかを示します。	はい	いいえ
SMB 署名が有効	SMBの署名が有効になっている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

この表は、Unified Manager がボリューム上のデータが不正なユーザー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するために評価するボリューム暗号化パラメータを示しています。

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
ソフトウェア暗号化	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の暗号化	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せん。

著作権に関する情報

Copyright © 2025 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。