クラスタのセキュリティ目標の管理

Active IQ Unified Manager 9.9

NetApp
December 15, 2023

目次

クラスタのセキュリティ目標の管理

Unified Manager には、『 ONTAP 9_ NetApp Security Hardening Guide for ONTAP 』に定義されている推奨事項を基に、 クラスタ、 Storage Virtual Machine （ SVM ）、およびボリュームがどの程度セキュアであるかを示すダッシュボードが用意されています。

セキュリティダッシュボードの目的は、 ONTAP クラスタがネットアップ推奨のガイドラインに従っていない領域を提示して、潜在的な問題を修正できるようにすることです。ほとんどの場合、問題は ONTAP System Manager または ONTAP CLI を使用して解決します。組織がすべての推奨事項に従うとは限らないため、場合によっては変更を加える必要がありません。

を参照してください "ONTAP 9 セキュリティ設定ガイド" 詳細な推奨事項と解決策については、 TR-4569 を参照してください。

Unified Manager は、セキュリティステータスを報告するだけでなく、セキュリティ違反があるクラスタまたは SVM に対してセキュリティイベントを生成します。これらの問題はイベント管理インベントリページで追跡できます。また、イベントにアラートを設定して、新たなセキュリティイベントが発生したときにストレージ管理者が通知を受け取るようにすることができます。

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。

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（で始まる暗号など）を使用しているかどうかを示します `*cbc`。	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。	推奨事項なし	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。	推奨事項なし	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。	推奨事項なし	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。	推奨事項なし	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。	推奨事項なし	いいえ

SVM 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でセキュアでない暗号（で始まる暗号など）を使用しているかどうかを示します `cbc*`。	いいえ	はい。

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
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
Kerberos V5	Kerberos v5 認証が有効か無効かを示します。	有効	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。

パラメータ	説明
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。

非準拠の条件

『 ONTAP 9_ 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るセキュリティ条件が 1 つでも満たされていない場合、クラスタと Storage Virtual Machine （ SVM ）は非準拠とみなされます。また、非準拠と判断された SVM が 1 つでもある場合も、クラスタは非準拠とみなされます。

セキュリティカード内の各ステータスアイコンとその意味は次のとおりです。

- - パラメータは推奨事項に従って設定されています。
- - パラメータは推奨事項に従って設定されていません。
- - クラスタで機能が有効になっていないか、パラメータが推奨事項に従って設定されていませんが、このパラメータはオブジェクトのコンプライアンスには影響しません。

ボリューム暗号化ステータスは、クラスタまたは SVM が準拠とみなされるかどうかには影響しません。

クラスタのセキュリティステータスの概要の表示

Unified Manager のダッシュボードのセキュリティパネルには、現在のビューに応じて、すべてのクラスタまたは単一のクラスタのセキュリティステータスの概要が表示されます。

手順

1. 左側のナビゲーションペインで、 * ダッシュボード * をクリックします。
2. すべての監視対象クラスタのセキュリティステータスを表示するか、 1 つのクラスタのセキュリティステータスを表示するかに応じて、 * すべてのクラスタ * を選択するか、ドロップダウンメニューから 1 つのクラスタを選択します。
3. 全体的なステータスを確認するには、 * セキュリティ * パネルを表示します。

   このパネルには次の情報が表示

   - 過去 24 時間に受信したセキュリティイベントのリスト
   - 各イベントから Event Details ページへのリンク
   - イベント管理インベントリページで、アクティブなすべてのセキュリティイベントを表示するためのリンク

- クラスタのセキュリティステータス（準拠または非準拠のクラスタ数）
- SVM のセキュリティステータス（準拠または非準拠の SVM 数）
- ボリューム暗号化ステータス（暗号化されているボリュームまたは暗号化されていないボリュームの数）

4. パネル上部の右矢印をクリックすると、セキュリティの詳細が * セキュリティ * ページに表示されます。

クラスタと SVM の詳細なセキュリティステータスの表示

Security ページには、すべてのクラスタのセキュリティステータスの概要と、個々のクラスタの詳細なセキュリティステータスが表示されます。詳細なクラスタステータスには、クラスタコンプライアンス、 SVM コンプライアンス、ボリューム暗号化コンプライアンスが含まれます。

手順

1. 左側のナビゲーションペインで、 * ダッシュボード * をクリックします。
2. すべての監視対象クラスタのセキュリティステータスを表示するか、 1 つのクラスタのセキュリティステータスを表示するかに応じて、 * すべてのクラスタ * を選択するか、ドロップダウンメニューから 1 つのクラスタを選択します。
3. セキュリティ * パネルの右矢印をクリックします。

   Security ページには、次の情報が表示されます。

   - クラスタのセキュリティステータス（準拠または非準拠のクラスタ数）
   - SVM のセキュリティステータス（準拠または非準拠の SVM 数）
   - ボリューム暗号化ステータス（暗号化されているボリュームまたは暗号化されていないボリュームの数）
   - 各クラスタで使用されているクラスタ認証方式
4. を参照してください "ONTAP 9 セキュリティ設定ガイド" すべてのクラスタ、 SVM 、およびボリュームを、ネットアップのセキュリティに関する推奨事項に準拠させていただく方法については、を参照してください。

ソフトウェアまたはファームウェアの更新が必要なセキュリティイベントの表示

「アップグレード」の影響領域を持つセキュリティイベントがあります。これらのイベントは Active IQ プラットフォームから報告され、 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特定します。

作業を開始する前に

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

このタスクについて

これらの問題については、すぐに対処が必要なものもあれば、スケジュールされた次回のメンテナンスまで待てるものもあります。これらのイベントをすべて表示し、問題を解決できるユーザに割り当てることができます。また、通知が不要なセキュリティアップグレードイベントがある場合は、このリストを利用して無効にするイベントを特定できます。

手順

1. 左側のナビゲーションペインで、 * イベント管理 * をクリックします。

   デフォルトでは、すべてのアクティブな（新規および確認済みの）イベントがイベント管理インベントリページに表示されます。

2. ［ 表示 ］ メニューから ［ * アップグレードイベント * ］ を選択します。

   アクティブなすべてのアップグレードセキュリティイベントが表示されます。

すべてのクラスタでのユーザ認証の管理状況の表示

Security ページには、各クラスタでユーザの認証に使用されている認証の種類と、各タイプを使用してクラスタにアクセスしているユーザの数が表示されます。これにより、ユーザ認証が組織の定義に従って安全に実行されていることを確認できます。

手順

1. 左側のナビゲーションペインで、 * ダッシュボード * をクリックします。
2. ダッシュボードの上部で、ドロップダウンメニューから「 * すべてのクラスタ * 」を選択します。
3. セキュリティ * パネルの右矢印をクリックすると、セキュリティ * ページが表示されます。
4. クラスタ認証 * カードを表示して、各認証タイプを使用してシステムにアクセスしているユーザの数を確認します。
5. クラスタセキュリティ * カードを表示して、各クラスタのユーザ認証に使用される認証メカニズムを確認します。

結果

安全でない方法またはネットアップが推奨していない方法でシステムにアクセスしているユーザがいる場合は、その方法を無効にできます。

すべてのボリュームの暗号化ステータスを表示します

すべてのボリュームとその現在の暗号化ステータスのリストを表示して、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確認できます。

作業を開始する前に

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

このタスクについて

ボリュームに適用できる暗号化のタイプは次のとおりです。

- 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。
- ハードウェア - 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。
- ソフトウェアとハードウェア - 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。
- なし - 暗号化されていないボリューム。

手順

1. 左側のナビゲーションペインで、 * Storage * > * Volumes * をクリックします。
2. [表示]メニューで、[正常性>*ボリューム暗号化*]を選択します
3. [**Health:Volumes Encryption**]ビューで、[**Encryption Type**]フィールドをソートするか、[Filter]を使用して、特定の暗号化タイプを持つボリューム、または暗号化されていないボリュームを表示します（[Encryption Type]は[None]）。

アクティブなすべてのセキュリティイベントを表示します

アクティブなセキュリティイベントをすべて表示し、問題を解決できるユーザに各イベントを割り当てることができます。また、受信不要なセキュリティイベントがある場合は、このリストを利用して無効にするイベントを特定できます。

作業を開始する前に

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、 * イベント管理 * をクリックします。

   デフォルトでは、新規と確認済みのイベントがイベント管理のインベントリページに表示されます。

2. [表示] メニューから、 [アクティブセキュリティイベント *] を選択します。

   このページには、過去 7 日間に生成された「新規」と「確認済み」のすべてのセキュリティイベントが表示されます。

セキュリティイベントのアラートを追加する

セキュリティイベントのアラートは、 Unified Manager で受信する他のイベントと同様に、イベントごとに個別に設定することができます。また、すべてのセキュリティイベントを同じように扱い、同じユーザに E メールを送信する場合は、セキュリティイベントがトリガーされたときに通知する共通のアラートを作成することもできます。

作業を開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

このタスクについて

次に 'Telnet Protocol enabled' セキュリティ・イベントのアラートを作成する例を示しますクラスタへのリモート管理アクセス用に Telnet アクセスが設定されると、アラートが送信されます。同じ方法で、すべてのセキュリティイベントに対してアラートを作成できます。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Alert Setup * をクリックします。
2. [* Alert Setup*] ページで、 [* Add] をクリックします。
3. [* アラートの追加 *] ダイアログボックスで、 [* 名前 *] をクリックし、アラートの名前と概要を入力します。
4. リソースをクリックし、このアラートを有効にするクラスタを選択します。
5. [* Events （イベント）] をクリックして、次の操作を実行します。
   a. イベントの重大度リストで、 * 警告 * を選択します。
   b. [Matching Events] リストで、 [Telnet Protocol Enabled*] を選択します。
6. [* アクション *] をクリックし、 [これらのユーザーに警告] フィールドで警告メールを受信するユーザーの名前を選択します。
7. 通知頻度、 SNMP トラップの発行、スクリプトの実行など、このページの他のオプションを設定します。
8. [保存（ Save ）] をクリックします。

特定のセキュリティイベントを無効にする

デフォルトでは、すべてのイベントが有効になっています。環境で重要でないイベントは、無効にして通知が生成されないようにすることができます。無効にしたイベントの通知を再開するには、該当するイベントを有効にします。

作業を開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

このタスクについて

イベントを無効にすると、システムで以前に生成されたイベントは「廃止」とマークされ、それらのイベントに設定されたアラートはトリガーされなくなります。無効にしたイベントを有効にすると、それらのイベントの通知の生成が次の監視サイクルから開始されます。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Event Setup * をクリックします。
2. イベント設定 * ページで、次のいずれかのオプションを選択してイベントを無効または有効にします。

状況	操作
イベントを無効にします	1. [**Disable**] をクリックします。 2. [イベントの無効化] ダイアログボックスで、 [警告] の重大度を選択します。これは、すべてのセキュリティイベントのカテゴリです。 3. [Matching Events] カラムで、ディセーブルにするセキュリティイベントを選択し、右矢印をクリックして [Disable Events] カラムに移動します。 4. [保存して閉じる] をクリックします。 5. 無効にしたイベントが Event Setup ページのリストビューに表示されることを確認します。
イベントを有効にします	1. 無効になっているイベントのリストから、再度有効にするイベントのチェックボックスを選択します。 2. [**Enable**] をクリックします。

セキュリティイベント

セキュリティイベントは、『 ONTAP 9_ NetApp Security Hardening Guide 』に定義されているパラメータに基づいて、 ONTAP クラスタ、 Storage Virtual Machine （ SVM ）、およびボリュームのセキュリティステータスに関する情報を提供します。これらのイベントは潜在的な問題を通知するもので、問題の重大度を評価し、必要に応じて問題を修正することができます。

セキュリティイベントはソースタイプ別にグループ化され、イベント名とトラップ名、影響レベル、および重大度が表示されます。これらのイベントは、クラスタおよび Storage VM のイベントカテゴリに表示されます。