クラスタのセキュリティ目標を管理する

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/active-iq-unified-manager-918/health-checker/concept_manage_cluster_security_objectives.html on November 13, 2026. Always check docs.netapp.com for the latest.

目次

クラスタのセキュリティ目標を管理する . . . 1
- Active IQ Unified Manager でクラスターのセキュリティ目標を管理する . . . 1
- 評価されるセキュリティ条件 . . . 1
  - Active IQ Unified Manager がセキュリティ基準を評価する方法を理解する . . . 1
  - Active IQ Unified Manager のクラスターコンプライアンスカテゴリについて . . . 2
  - Active IQ Unified Manager でのストレージ VM コンプライアンスカテゴリについて . . . 5
  - Active IQ Unified Manager のボリュームコンプライアンスカテゴリについて . . . 6
- Active IQ Unified Manager でのクラスターと SVM のコンプライアンスステータスについて . . . 6
- Active IQ Unified Manager でクラスターとストレージ VM のセキュリティステータスを表示する . . . 7
  - [セキュリティ]ページでのオブジェクト レベルのセキュリティ ステータスの表示 . . . 7
  - [クラスタ]ページでのすべてのクラスタのセキュリティの詳細表示 . . . 8
  - [Storage VM]ページでのすべてのクラスタのセキュリティの詳細の表示 . . . 8
- Active IQ Unified Manager でソフトウェアまたはファームウェアのアップデートが必要になる可能性のあるセキュリティイベントを表示する . . . 9
- Active IQ Unified Manager のすべてのクラスターでユーザ認証を管理する方法を確認する . . . 9
- Active IQ Unified Manager ですべてのボリュームの暗号化ステータスを表示する . . . 10
- Active IQ Unified Manager ですべてのボリュームとストレージ VM のランサムウェア対策ステータスを確認する . . . 10
  - ランサムウェア対策検出機能による全ボリュームのセキュリティの詳細表示 . . . 11
  - ランサムウェア対策の検出機能による全Storage VMのセキュリティの詳細表示 . . . 11
- Active IQ Unified Manager ですべてのアクティブなセキュリティイベントを表示する . . . 11
- Active IQ Unified Manager でセキュリティイベントのアラートを追加する . . . 12
- Active IQ Unified Manager で特定のセキュリティイベントを無効にする . . . 12
- Active IQ Unified Manager でセキュリティイベントを表示する . . . 13

クラスタのセキュリティ目標を管理する

Active IQ Unified Manager でクラスターのセキュリティ目標を管理する

Unified Manager は、*NetApp Security Hardening Guide for ONTAP 9* で定義されている推奨事項に基づいて、ONTAP クラスター、Storage Virtual Machine （SVM）、およびボリュームのセキュリティレベルを識別するダッシュボードを提供します。

セキュリティ ダッシュボードの目的は、ONTAPクラスタがNetApp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かぎらないため、変更が不要な場合もあります。

詳細な推奨事項と解決策については、 "NetApp ONTAP 9 セキュリティ強化ガイド"（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。

詳細については、"評価されるセキュリティ条件"を参照してください。

評価されるセキュリティ条件

Active IQ Unified Manager がセキュリティ基準を評価する方法を理解する

一般的に、ONTAPクラスター、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 Security Hardening Guide for ONTAP 9_で定義されている推奨事項に基づいて評価されています。

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"に関するトピックで詳細情報をご確認ください。

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、"クラスタのセキュリティ目標の管理"を参照してください。

Active IQ Unified Manager のクラスターコンプライアンスカテゴリについて

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 パラメーター、NetApp の推奨事項、およびそのパラメーターがクラスターの準拠または非準拠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。

クラスター内に規格に準拠していないSVMが存在すると、クラスターの準拠値に影響します。そのため、場合によっては、クラスターのセキュリティが準拠しているとみなされる前に、SVMのセキュリティ問題を修正する必要があります。

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	クラスター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。	Disabled	はい
安全でない SSH 設定	*cbcで始まる暗号など、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。	×	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

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します
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	クラスターに1つ以上のNTPサーバーが設定されているかどうかを示します。冗長性と最高のサービスのために、NetAppはクラスターに少なくとも3つのNTPサーバーを関連付けることを推奨します。	設定	はい
OCSP	9.14.1から、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）のステータス情報を提供します。これは、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完全性と有効性が保証されることを意味します。	有効	×
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	HTTPSが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使用されるかどうかを示します。	有効	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します
デフォルトの管理ユーザ	デフォルトの管理者ユーザー（組み込み）が有効か無効かを示します。NetApp では、不要な組み込みアカウントはロック（無効化）することを推奨します。	Disabled	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。	×	×
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。	×	×
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。	×	×
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。	×	×
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。	×	×
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。	Disabled	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します
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。	×	はい
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	×

Active IQ Unified Manager でのストレージ **VM** コンプライアンスカテゴリについて

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します
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*`で始まる暗号などです。	×	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になっているか無効になっているかを示します。	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	×
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	×
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	×

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
CHAP 設定	CHAPが有効になっているかどうかを示します。	有効	×
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	×
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。	Disabled	×
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	×
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	×
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	×

Active IQ Unified Manager のボリュームコンプライアンスカテゴリについて

この表は、Unified Manager がボリューム上のデータが不正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について説明しています。

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
ソフトウェアで暗号化	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。
ハードウェアで暗号化	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で暗号化	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。

Active IQ Unified Manager でのクラスターと **SVM** のコンプライアンスステータスについて

クラスターおよびストレージ仮想マシン（SVM）は、*NetApp Security Hardening Guide*

for ONTAP 9 で定義されている推奨事項に対して評価されているセキュリティ基準のいずれかが満たされていない場合、準拠していないとみなされます。さらに、いずれかの SVM が準拠していないとフラグ付けされた場合、そのクラスターは準拠していないとみなされます。

セキュリティ カードの各ステータス アイコンとその意味は次のとおりです。

- - パラメータは推奨どおりに設定されています。
- - パラメータが推奨設定どおりに設定されていません。
- - クラスター上で機能が有効になっていないか、パラメータが推奨どおりに設定されていないが、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寄与しない。

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。

Active IQ Unified Manager でクラスターとストレージ VM のセキュリティステータスを表示する

Active IQ Unified Managerでは、環境内のストレージ オブジェクトのセキュリティ ステータスをインターフェイスのさまざまなポイントで確認できます。定義したパラメータに基づいて情報とレポートを収集および分析し、監視対象のクラスタおよびStorage VMについて、不審な挙動や不正なシステム変更を検出することができます。

セキュリティに関する推奨事項については、以下を参照してください。 "NetApp ONTAP 9 セキュリティ強化ガイド"

[セキュリティ]ページでのオブジェクト レベルのセキュリティ ステータスの表示

システム管理者は、*セキュリティ*ページを使用して、データセンターおよびサイトレベルでのONTAPクラスタとストレージVMのセキュリティ強度を可視化できます。サポートされているオブジェクトは、クラスタ、ストレージVM、およびボリュームです。以下の手順に従ってください：

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. 監視対象のすべてのクラスタのセキュリティステータスを表示するか、単一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、**All Clusters** を選択するか、ドロップダウンメニューから単一のクラスタを選択してください。
3. 「セキュリティ」パネルの右矢印をクリックします。[セキュリティ]ページが表示されます。

棒グラフ、カウント、および `View Reports`リンクをクリックすると、ボリューム、クラスタ、またはStorage VMsページに移動し、必要に応じて対応する詳細を表示したり、レポートを生成したりすることができます。

[セキュリティ]ページには、次のパネルが表示されます。

- クラスタコンプライアンス：データセンター内のすべてのクラスタのセキュリティステータス（準拠しているクラスタ数または準拠していないクラスタ数）

- ストレージ**VM**のコンプライアンス：データセンター内のすべてのストレージVMのセキュリティステータス（準拠しているストレージVMの数、または準拠していないストレージVMの数）
- ボリューム暗号化：環境内のすべてのボリュームの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と暗号化されていないボリュームの数）
- ボリュームのランサムウェア対策ステータス：環境内のすべてのボリュームのセキュリティステータス（ランサムウェア対策が有効または無効になっているボリュームの数）
- クラスタ認証と証明書：SAML、Active Directory、証明書、ローカル認証など、各認証方法を使用しているクラスタの数。このパネルには、証明書の有効期限が切れている、または60日以内に有効期限が切れるクラスタの数も表示されます。

[クラスタ]ページでのすべてのクラスタのセキュリティの詳細表示

「クラスタ／セキュリティ」の詳細ページでは、クラスタレベルでのセキュリティコンプライアンス状況を確認できます。

手順

1. 左側のナビゲーションペインで、*ストレージ > クラスタ*をクリックします。
2. *表示 > セキュリティ > すべてのクラスタ*を選択します。

グローバルFIPS、Telnet、安全でないSSH設定、ログイン バナー、ネットワーク タイム プロトコル、AutoSupport HTTPS転送、クラスタの証明書の有効期限のステータスなど、デフォルトのセキュリティパラメータが表示されます。

「その他のオプション」ボタンをクリックして、Unified Managerの「セキュリティ」ページまたはSystem Managerでセキュリティの詳細を表示するように選択できます。System Managerで詳細を表示するには、有効な認証情報が必要です。

クラスタに期限切れの証明書がある場合は、**Cluster Certificate Validity** の下にある `expired` をクリックして、System Manager（9.10.1以降）から更新できます。System Managerインスタンスのリリースが9.10.1より前の場合、 `expired`をクリックすることはできません。

[Storage VM]ページでのすべてのクラスタのセキュリティの詳細の表示

「ストレージVM / セキュリティ」の詳細ページでは、ストレージVMレベルでのセキュリティコンプライアンス状況を確認できます。

手順

1. 左側のナビゲーションペインで、*ストレージ > ストレージVM*をクリックします。
2. *表示 > セキュリティ > すべてのStorage VM*を選択します。セキュリティパラメータが設定されたクラスタの一覧が表示されます。

Storage VMのセキュリティ コンプライアンスのデフォルトのビューで、Storage VM、クラスタ、ログイン バナー、監査ログ、安全でないSSH設定などのセキュリティ パラメータを確認できます。

「その他のオプション」ボタンをクリックして、Unified Managerの「セキュリティ」ページまたはSystem Managerでセキュリティの詳細を表示するように選択できます。System Managerで詳細を表示するには、有効な認証情報が必要です。

ボリュームおよびストレージVMのランサムウェア対策セキュリティの詳細については、"すべてのボリュームとストレージVMのランサムウェア対策ステータスを表示する"を参照してください。

Active IQ Unified Manager でソフトウェアまたはファームウェアのアップデートが必要になる可能性のあるセキュリティイベントを表示する

影響エリアが「Upgrade」であるセキュリティイベントがいくつかあります。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、解決策として 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の場合）のアップグレードが必要な問題を特定します。

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、通知が不要なアップグレード 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。

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。

   [イベント管理]インベントリ ページには、デフォルトではすべてのアクティブなイベント（新規と確認済みのイベント）が表示されます。

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。

Active IQ Unified Manager のすべてのクラスターでユーザ認証を管理する方法を確認する

[セキュリティ]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タイプと、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数が表示されます。このページを使用して、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. ダッシュボード上部のドロップダウンメニューから「すべてのクラスター」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」カードを表示すると、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ー数を確認できます。
5. 各クラスターでユーザー認証に使用されている認証メカニズムを確認するには、「Cluster Security」カー

ドを参照してください。

安全でない方法、または NetApp が推奨していない方法を使用してシステムにアクセスしているユーザーがいる場合は、その方法を無効にすることができます。

Active IQ Unified Manager ですべてのボリュームの暗号化ステータスを表示する

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。

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。

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、ストレージ ＞ ボリューム をクリックします。
2. 「表示」メニューで、ヘルス > *ボリューム暗号化*を選択します。
3. *健全性：ボリュームの暗号化*ビューで、*暗号化タイプ*フィールドで並べ替えるか、フィルタを使用して、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（暗号化タイプが「None」）を表示します。

Active IQ Unified Manager ですべてのボリュームとストレージ VM のランサムウェア対策ステータスを確認する

すべてのボリュームとStorage VM（SVM）、およびそれらの現在のランサムウェア対策ステータスのリストを表示して、ボリュームおよびSVMのデータがランサムウェア攻撃から適切に保護されているかどうかを確認できます。

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。

さまざまなランサムウェア対策ステータスの詳細については、"ONTAP：ランサムウェア対策を有効にする"を参照してください。

ランサムウェア対策検出機能による全ボリュームのセキュリティの詳細表示

手順

1. 左側のナビゲーションペインで、ストレージ ＞ ボリューム をクリックします。
2. 「表示」メニューで、ヘルス > セキュリティ > *ランサムウェア対策*を選択します。
3. *セキュリティ：ランサムウェア対策*ビューでは、さまざまなフィールドで並べ替えたり、フィルタを使用したりできます。

ランサムウェア対策は、オフライン ボリューム、制限状態のボリューム、SnapLockボリューム、FlexGroupボリューム、FlexCacheボリューム、SANのみのボリューム、停止中のStorage VMのボリューム、Storage VMのルート ボリューム、データ保護ボリュームに対してはサポートされていません。

ランサムウェア対策の検出機能による全**Storage VM**のセキュリティの詳細表示

手順

1. 左側のナビゲーションペインで、*ストレージ > ストレージVM*をクリックします。
2. *表示 > セキュリティ > ランサムウェア対策*を選択します。ランサムウェア対策ステータスを持つSVMのリストが表示されます。

ランサムウェア対策による監視は、NASプロトコルが有効になっていないStorage VMではサポートされていません。

Active IQ Unified Manager ですべてのアクティブなセキュリティイベントを表示する

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。

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。

   [イベント管理]インベントリ ページには、デフォルトでは新規と確認済みのイベントが表示されます。

2. 「表示」メニューから「アクティブな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。

Active IQ Unified Manager で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。または、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。

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。

以下の例は、「`Telnet Protocol Enabled`」セキュリティイベントに対するアラートを作成する方法を示しています。クラスターへのリモート管理アクセスに Telnet アクセスが設定されている場合、アラートが送信されます。この同じ方法を使用して、すべてのセキュリティイベントに対する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、ストレージ管理 > アラート設定 をクリックします。
2. *アラート設定*ページで、*追加*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、アラートの名前と説明を入力します。
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ーを選択します。
5. 「イベント」をクリックし、以下の操作を実行してください：
   a. イベントの重大度リストで、*警告*を選択します。
   b. 一致するイベントの一覧で、*Telnetプロトコルが有効*を選択します。
6. **Actions** をクリックし、**Alert these users** フィールドで、アラート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*をクリックします。

Active IQ Unified Manager で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。

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。

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再開されます。

手順

1. 左側のナビゲーションペインで、ストレージ管理 ＞ イベント設定 をクリックします。
2. 「イベント」設定ページで、以下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
イベントを無効にする	a. **Disable** をクリックします。 b. 「イベントを無効にする」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。 c. [一致イベント]列で無効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[イベントの無効化]列に移します。 d. 「保存して閉じる」をクリックします。 e. 無効にしたイベントが[イベント セットアップ]ページのリスト ビューに表示されていることを確認します。
イベントを有効にする	a. 無効になっているイベントのリストで、再び有効にするイベント（複数可）のチェックボックスをオンにします。 b. * Enable * をクリックします。

Active IQ Unified Manager でセキュリティイベントを表示する

セキュリティイベントは、_NetApp Security Hardening Guide for ONTAP 9_で定義されているパラメータに基づいて、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 タイプ別にまとめられ、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。

著作権に関する情報

Copyright © 2026 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。