



# クラスタのセキュリティ目標の管理

## Active IQ Unified Manager 9.13

NetApp  
December 18, 2023

# 目次

クラスタのセキュリティ目標の管理	1
評価されるセキュリティ条件	1
非準拠の条件	7
クラスタとStorage VMのセキュリティステータスの表示	7
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	9
すべてのクラスタでのユーザ認証の管理状況の表示	10
すべてのボリュームの暗号化ステータスを表示します	10
すべてのボリュームおよびStorage VMのランサムウェア対策ステータスを表示する	11
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	11
セキュリティイベントのアラートを追加する	12
特定のセキュリティイベントを無効にする	13
セキュリティイベント	13

# 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。

詳細については、を参照してください ["評価されるセキュリティ条件"](#)。

## 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。

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
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。
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。

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
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
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

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
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。
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
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。

## 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。

## クラスタと Storage VM のセキュリティステータスの表示

Active IQ Unified Manager を使用すると、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から確認できます。定義され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、疑わしい動作や不正なシステム変更を検出できます。

セキュリティに関する推奨事項については、を参照してください "[ONTAP 9 セキュリティ設定ガイド](#)"

## セキュリティページでオブジェクトレベルのセキュリティステータスを表示します

システム管理者は、セキュリティ\*ページを使用して、データセンターレベルとサイトレベルのONTAP クラスタとStorage VMのセキュリティ強度を可視化できます。サポートされるオブジェクトは、クラスタ、Storage VM、およびボリュームです。次の手順を実行します。

### 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。[セキュリティ]ページが表示されます。

棒グラフ、カウント、およびをクリックします 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 VMのページが表示され、必要に応じて対応する詳細を確認したりレポートを生成したりできます。

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（準拠または非準拠のクラスタ数）
- \* Storage VM Compliance \*：データセンター内のすべてのStorage VMのセキュリティステータス（準拠または非準拠のStorage VM数）
- \* Volume Encryption \*：環境内のすべてのボリュームの暗号化ステータス（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）
- \* Volume Anti-Ransomware Status \*：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）
- クラスタ認証および証明書：SAML、Active Directory、証明書およびローカル認証など、各タイプの認証方法を使用するクラスタの数。このパネルには、証明書の有効期限が切れているか、60日以内に期限切れになる予定のクラスタの数も表示されます。


## クラスタページで、すべてのクラスタのセキュリティの詳細を表示します

[\*クラスタ/セキュリティ\*の詳細]ページでは、セキュリティコンプライアンスのステータスをクラスタレベルで表示できます。

### 手順

1. 左側のナビゲーションペインで、\* Storage > Clusters \*の順にクリックします。
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、セキュアでない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転送プロトコルと、クラスタ証明書の有効期限のステータスが表示されます。

をクリックできます  オプションボタンをクリックし、Unified ManagerまたはSystem Managerの\* Security \* ページでセキュリティの詳細を表示します。System Managerで詳細を表示するには、有効なクレデンシャルが必要です。



クラスタの証明書の有効期限が切れている場合は、をクリックします `expired` 「\*クラスタ証明書の有効性」の下にあるSystem Manager (9.10.1以降) から更新してください。をクリックすることはできません `expired` System Managerインスタンスが9.10.1より前のリリースの場合。


## すべてのクラスタのセキュリティの詳細を**Storage VM**ページで表示する

Storage VMs/Security \*の詳細ページでは、Storage VMレベルでセキュリティ準拠ステータスを確認できます。

### 手順

1. 左側のナビゲーションペインで、\* Storage > Storage VM\*をクリックします。
2. [\*表示]>[セキュリティ]>[すべてのStorage VMs]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リストが表示されます。

Storage VMのセキュリティコンプライアンスのデフォルトビューを使用するには、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します。

をクリックできます  オプションボタンをクリックし、Unified ManagerまたはSystem Managerの\* Security \* ページでセキュリティの詳細を表示します。System Managerで詳細を表示するには、有効なクレデンシャルが必要です。

ボリュームやStorage 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、を参照してください "[すべてのボリュームおよびStorage VMのランサムウェア対策ステータスを表示する](#)"。

## 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。

- 必要なもの \*

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。

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。

- 必要なもの \*

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、\* 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]）。

## すべてのボリュームおよびStorage VMのランサムウェア対策ステータスを表示する

すべてのボリュームとStorage VM（SVM）およびその最新のランサムウェア対策ステータスのリストを表示して、ボリュームやSVM上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。

- 必要なもの \*

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。

ランサムウェア対策のさまざまなステータスの詳細については、を参照してください ["ONTAP：ランサムウェア対策を有効化"](#)。

ランサムウェア対策の検出機能で、すべてのボリュームのセキュリティの詳細を表示できます

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、[\* Health > Security > Anti-Ransomware \*]を選択します
3. セキュリティ：アンチランサムウェア\*表示では、さまざまなフィールドでソートしたり、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、制限付きボリューム、SnapLock ボリューム、FlexGroup ボリューム、FlexCache ボリュームではサポートされていません。SAN専用ボリューム、停止しているStorage VMのボリューム、Storage VMのルートボリューム、またはデータ保護ボリューム。

ランサムウェア対策検出で、すべてのStorage VMのセキュリティの詳細を確認できます

手順

1. 左側のナビゲーションペインで、\* Storage > Storage 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] の順に選択します。ランサムウェア対策のステータスが設定されたSVMのリストが表示されます。



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

## 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。

- 必要なもの \*

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。

- 必要なもの \*

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。

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。

- 必要なもの \*

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	<ol style="list-style-type: none"><li>a. <b>[Disable]</b> をクリックします。</li><li>b. [ 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。</li><li>c. [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。</li><li>d. [ 保存して閉じる ] をクリックします。</li><li>e. 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。</li></ol>
イベントを有効にします	<ol style="list-style-type: none"><li>a. 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。</li><li>b. <b>[Enable]</b> をクリックします。</li></ol>

## 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。



## 著作権に関する情報

Copyright © 2023 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。