



アラート

SANtricity 11.8

NetApp
December 16, 2024

目次

アラート.....	1
アラートの概要.....	1
概念.....	1
Eメールアラートの管理.....	3
SNMPアラートの管理.....	7
syslogアラートの管理.....	14
FAQ.....	16

アラート

アラートの概要

System Managerでは、ストレージレイのアラートをEメール、SNMPトラップ、およびsyslogメッセージで送信するように設定できます。

アラートとは

_アラート_ストレージレイで発生した重要なイベントについて管理者に通知します。イベントには、バッテリーの障害、最適からオフラインへのコンポーネントの移動、コントローラの冗長性の問題などが含まれます。重大イベントはすべて「アラート対象」とみなされるほか、一部の警告イベントと情報イベントも「アラート対象」とみなされます。

詳細：

- ["アラートの仕組み"](#)
- ["アラートの用語"](#)

アラートの設定方法

アラートは、メッセージとして1つ以上のEメールアドレスに送信するか、SNMPサーバにSNMPトラップとして送信するか、syslogサーバにメッセージとして送信するように設定できます。アラート設定はメニューから選択できます。Settings [Alerts]

詳細：

- ["メールサーバとアラートの受信者の設定"](#)
- ["アラート用のsyslogサーバの設定"](#)
- ["SNMPアラートの設定"](#)

関連情報

アラートに関連する概念の詳細については、以下を参照してください。

- ["イベントログの概要"](#)
- ["一貫性のないタイムスタンプ"](#)

概念

アラートの仕組み

アラートは、ストレージレイで発生した重要なイベントについて管理者に通知します。Eメール、SNMPトラップ、syslogを使用してアラートを送信できます。

アラートプロセスは次のように機能します。

1. 管理者がSystem Managerで、次のうち1つ以上のアラート方法を設定します。
 - 電子メール--電子メールアドレスにメッセージが送信されます。
 - *snmp *-- SNMPトラップがSNMPサーバに送信されます。
 - *syslog *--メッセージがsyslogサーバに送信される。
2. ストレージアレイのイベントモニタが問題を検出すると、その問題に関する情報をイベントログに書き込みます（メニュー：サポート[イベントログ]から選択できます）。これには、バッテリーの障害、最適からオフラインへのコンポーネントの状態の変化、コントローラの冗長性の問題などが含まれます。
3. イベントモニタがイベントが「アラート対象」とであると判断すると、設定されているアラート方法（Eメール、SNMP、syslog）を使用して通知が送信されます。重大イベントはすべて「アラート対象」とみなされるほか、一部の警告イベントと情報イベントも「アラート対象」とみなされます。

アラートの設定

アラートは、初期セットアップウィザード（Eメールアラートのみ）または[アラート]ページから設定できます。現在の設定を確認するには、メニューから「Settings [Alerts]」に移動します。

[アラート]タイルには、次のいずれかのアラート設定が表示されます。

- 未設定
- 設定：少なくとも1つのアラート方法が設定されています。どのアラート方法が設定されているかを確認するには、カーソルでタイルをポイントします。

アラート情報

アラートには次の種類の情報を含めることができます。

- ストレージアレイの名前。
- イベントログエントリに関連するイベントエラータイプ。
- イベントが発生した日時。
- イベントの簡単な説明。



syslogアラートはRFC 5424のメッセージング標準に準拠します。

アラートの用語

ストレージアレイに関連するアラートの用語を次に示します。

コンポーネント	製品説明
イベントモニタ	イベントモニタはストレージアレイに常駐し、バックグラウンドタスクとして実行されます。イベントモニタは、ストレージアレイの異常を検出すると、問題に関する情報をイベントログに書き込みます。これには、バッテリーの障害、最適からオフラインへのコンポーネントの状態の変化、コントローラの冗長性の問題などが含まれます。イベントモニタがイベントが「アラート対象」と判断すると、設定されているアラート方法（Eメール、SNMP、syslog）を使用して通知が送信されます。重大イベントはすべて「アラート対象」とみなされるほか、一部の警告イベントと情報イベントも「アラート対象」とみなされます。
メールサーバ	メールサーバは、Eメールアラートの送受信に使用されます。サーバはSimple Mail Transfer Protocol（SMTP；簡易メール転送プロトコル）を使用します。
SNMP	簡易ネットワーク管理プロトコル（SNMP）は、IPネットワーク上のデバイス間で情報を管理および共有するために使用されるインターネット標準プロトコルです。
SNMPトラップ	SNMPトラップは、SNMPサーバに送信される通知です。トラップには、ストレージアレイの重大な問題に関する情報が含まれています。
SNMPトラップの送信先	SNMPトラップの送信先は、SNMPサービスを実行しているサーバのIPv4またはIPv6アドレスです。
コミュニティ名	コミュニティ名は、SNMP環境でネットワークサーバのパスワードのように機能する文字列です。
MIBファイル	管理情報ベース（MIB）ファイルは、ストレージアレイ内で監視および管理されるデータを定義します。SNMPサービスアプリケーションがインストールされたサーバにコピーしてコンパイルする必要があります。このMIBファイルは、サポートサイトのSystem Managerソフトウェアで入手できます。
MIB変数	管理情報ベース（MIB）変数は、SNMP GetRequestsへの応答として、ストレージアレイ名、アレイの場所、担当者などの値を返すことができます。
syslog	syslogは、ネットワークデバイスがイベントメッセージをロギングサーバに送信するために使用するプロトコルです。
UDP	User Datagram Protocol（UDP；ユーザデータグラムプロトコル）は、パケットヘッダーで送信元と宛先のポート番号を指定するトランスポートレイヤプロトコルです。

Eメールアラートの管理

メールサーバとアラートの受信者の設定

Eメールアラートを設定するには、メールサーバのアドレスとアラート受信者のEメール

アドレスを指定する必要があります。Eメールアドレスは20個まで指定できます。

開始する前に

- メールサーバのアドレスを確認しておく必要があります。アドレスには、IPv4アドレス、IPv6アドレス、または完全修飾ドメイン名を使用できます。



完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバは[ハードウェア]ページで設定できます。

- アラート送信者として使用するEメールアドレスを確認しておく必要があります。これは、アラートメッセージの「送信元」フィールドに表示されるアドレスです。SMTPプロトコルでは送信者アドレスが必要です。ない場合はエラーになります。
- アラート受信者のEメールアドレスを確認しておく必要があります。受信者は、通常、ネットワーク管理者またはストレージ管理者のアドレスです。Eメールアドレスは20個まで入力できます。

タスクの内容

このタスクでは、メールサーバを設定し、送信者と受信者のEメールアドレスを入力し、入力したすべてのEメールアドレスを[アラート]ページからテストする方法について説明します。



Eメールアラートは初期セットアップウィザードで設定することもできます。

手順

1. メニューを選択します。Settings [Alerts] (設定[Alerts])。
2. [Email]タブを選択します。

Eメールサーバがまだ設定されていない場合は、[Email]タブに[Configure Mail Server]と表示されます。

3. [メールサーバーの設定] を選択します。

メールサーバーの設定ダイアログボックスが開きます。

4. メールサーバの情報を入力し、[保存]をクリックします。

- メールサーバーアドレス--メールサーバーの完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを入力します。



完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバは[ハードウェア]ページで設定できます。

- *Email sender address*--電子メールの送信者として使用する有効な電子メールアドレスを入力します。このアドレスは、電子メールメッセージの[送信元]フィールドに表示されます。
- **Encryption**--メッセージを暗号化する場合は、暗号化タイプとして*SMTPS*または*STARTTLS*を選択し、暗号化されたメッセージのポート番号を選択します。それ以外の場合は、*なし*を選択します。
- ユーザー名とパスワード--必要に応じて、送信側とメールサーバーで認証を行うためのユーザー名とパスワードを入力します。
- 電子メールに連絡先情報を含める--送信者の連絡先情報を警告メッセージに含めるには、このオプションを選択し、名前と電話番号を入力します。

[保存]をクリックすると、[アラート]ページの[電子メール]タブに電子メールアドレスが表示されます。

5. [電子メールの追加]を選択します。

[電子メールの追加]ダイアログボックスが開きます。

6. アラート受信者のEメールアドレスを1つ以上入力し、*追加*をクリックします。

EメールアドレスがAlerts（アラート）ページに表示されます。

7. メールアドレスが有効であることを確認するには、「すべてのメールをテスト」をクリックして、テストメッセージを受信者に送信します。

結果

Eメールアラートを設定すると、アラート対象のイベントが発生するたびに、イベントモニタから指定した受信者にEメールメッセージが送信されます。

アラート用のEメールアドレスの編集

Eメールアラートを受信する受信者のEメールアドレスを変更できます。

開始する前に

編集する電子メールアドレスは、[Alerts]ページの[Email]タブで定義する必要があります。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [Email]タブを選択します。
3. [Email Address]テーブルで、変更するアドレスを選択し、右端にある*Edit*（鉛筆）アイコンをクリックします。

行が編集可能なフィールドになります。

4. 新しいアドレスを入力し、保存（チェックマーク）アイコンをクリックします。



変更をキャンセルする場合は、* Cancel * (X) アイコンを選択します。

結果

[Alerts]ページの[Email]タブには、更新された電子メールアドレスが表示されます。

アラート用のEメールアドレスの追加

Eメールアラートには受信者を20人まで追加できます。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. [Email]タブを選択します。
3. [電子メールの追加]を選択します。

[電子メールの追加]ダイアログボックスが開きます。

4. 空のフィールドに、新しいEメールアドレスを入力します。複数のアドレスを追加する場合は、[別の電子メールを追加]を選択して別のフィールドを開きます。
5. [追加]*をクリックします。

結果

[Alerts]ページの[Email]タブに新しい電子メールアドレスが表示されます。

アラート用のメールサーバまたはEメールアドレスの削除

以前に定義したメールサーバを削除してアラートがEメールアドレスに送信されないようにすることも、個々のEメールアドレスを削除することもできます。

手順

1. メニューを選択します。Settings [Alerts] (設定[Alerts])。
2. [Email]タブを選択します。
3. テーブルで、次のいずれかを実行します。
 - メールサーバを削除してアラートがEメールアドレスに送信されないようにするには、メールサーバの行を選択します。
 - Eメールアドレスを削除してこのアドレスにアラートが送信されないようにするには、削除するEメールアドレスの行を選択します。表の右上にある* Delete *ボタンを選択できるようになります。
4. [削除 (Delete)]をクリックし、操作を確定する。

アラート用のメールサーバの編集

Eメールアラートに使用するメールサーバのアドレスやEメール送信者のアドレスを変更することができます。

開始する前に

変更するメールサーバのアドレスを確認しておく必要があります。アドレスには、IPv4アドレス、IPv6アドレス、または完全修飾ドメイン名を使用できます。



完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバは[ハードウェア]ページで設定できます。

手順

1. メニューを選択します。Settings [Alerts] (設定[Alerts])。
2. [Email]タブを選択します。
3. [メールサーバーの設定] を選択します。

メールサーバーの設定ダイアログボックスが開きます。

4. メールサーバのアドレス、送信者情報、および連絡先情報を編集します。

- メールサーバのアドレス--メールサーバの完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを編集します。



完全修飾ドメイン名を使用するには、両方のコントローラにDNSサーバを設定する必要があります。DNSサーバは[ハードウェア]ページで設定できます。

- 電子メール送信者のアドレス--電子メールの送信者として使用される電子メールアドレスを編集します。このアドレスは、電子メールメッセージの[送信元]フィールドに表示されます。
- 電子メールに連絡先情報を含める--送信者の連絡先情報を編集するには、このオプションを選択し、名前と電話番号を編集します。

5. [保存 (Save)] をクリックします。

SNMPアラートの管理

SNMPアラートの設定

簡易ネットワーク管理プロトコル (SNMP) アラートを設定するには、ストレージレイのイベントモニタからSNMPトラップを送信できるサーバを少なくとも1つ指定する必要があります。この設定には、コミュニティ名またはユーザ名、およびサーバのIPアドレスが必要です。

開始する前に

- ネットワークサーバにSNMPサービスアプリケーションが設定されている必要があります。イベントモニタがトラップメッセージをそのアドレスに送信できるようにするには、このサーバのネットワークアドレス (IPv4またはIPv6アドレス) が必要です。複数のサーバを使用できます (最大10台のサーバを使用できます)。
- 管理情報ベース (MIB) ファイルは、SNMPサービスアプリケーションを使用してサーバにコピーおよびコンパイルされています。このMIBファイルは、監視および管理されるデータを定義します。

MIBファイルがない場合は、NetAppサポートサイトから入手できます。

- に進みます ["NetAppのサポート"](#)。
- [*ダウンロード] タブをクリックし、[*ダウンロード] を選択します。
- EシリーズSANtricity OSコントローラソフトウェア* をクリックします。
- [最新リリースのダウンロード] を選択します。
- ログインします。
- 注意事項と使用許諾契約書に同意します。
- コントローラタイプのMIBファイルが表示されるまで下にスクロールし、リンクをクリックしてファイルをダウンロードします。

タスクの内容

このタスクでは、トラップの送信先となるSNMPサーバを指定し、設定をテストする方法について説明します。

手順

1. メニューを選択します。Settings [Alerts] (設定[Alerts])。

2. SNMP *タブを選択します。

初回セットアップ時に、[SNMP]タブに「コミュニティ/ユーザの設定」と表示されます。

3. コミュニティ/ユーザーの設定*を選択します。

[SNMPバージョンの選択]ダイアログボックスが開きます。

4. アラートのSNMPバージョンとして、* SNMPv2c または SNMPv3 *のいずれかを選択します。

選択した内容に応じて、[コミュニティの設定]ダイアログボックスまたは[SNMPv3ユーザの設定]ダイアログボックスが開きます。

5. SNMPv2c (コミュニティ) またはSNMPv3 (ユーザ) に対応する手順に従います。

- **SNMPv2c (communities)**--コミュニティの設定ダイアログで、ネットワークサーバーのコミュニティストリングを1つ以上入力します。コミュニティ名は、既知の管理ステーションのセットを識別する文字列で、通常はネットワーク管理者によって作成されます。印刷可能なASCII文字のみで構成されます。コミュニティは最大256個追加できます。完了したら、*保存*をクリックします。
- **SNMPv3(Users)**-- SNMPv3ユーザーの設定ダイアログで、*Add*をクリックし、次の情報を入力します。
 - ユーザー名--ユーザーを識別するための名前を入力します最大31文字まで入力できます
 - エンジンID *--メッセージの認証キーと暗号化キーを生成するために使用されるエンジンIDを選択します管理ドメイン上で一意である必要がありますほとんどの場合、*ローカル*を選択してください。標準以外の設定を使用している場合は、「*カスタム」を選択します。別のフィールドが表示され、10~32文字の範囲で、正規のエンジンIDを16進数の文字列で入力する必要があります。
 - 認証資格情報--ユーザーの識別を保証する認証プロトコルを選択します次に、認証プロトコルを設定または変更するときに必要な認証パスワードを入力します。パスワードは8~128文字で指定する必要があります。
 - プライバシー資格情報--メッセージの内容を暗号化するために使用するプライバシープロトコルを選択します次に、プライバシープロトコルを設定または変更するときに必要なプライバシーパスワードを入力します。パスワードは8~128文字で指定する必要があります。完了したら、[*追加]をクリックし、[*閉じる]をクリックします。

6. [SNMP]タブが選択されている[Alerts]ページで、[Add Trap Destinations*]をクリックします。

トラップ送信先の追加ダイアログボックスが開きます。

7. 1つ以上のトラップ送信先を入力し、関連付けられているコミュニティ名またはユーザ名を選択して、* Add *をクリックします。

- **Trap Destination**-- SNMPサービスを実行しているサーバーのIPv4またはIPv6アドレスを入力します
- コミュニティ名またはユーザー名--ドロップダウンから、このトラップの送信先のコミュニティ名 (SNMPv2c) またはユーザー名 (SNMPv3) を選択します。(定義した名前が1つだけの場合は、このフィールドにすでに名前が表示されます)。
- 認証失敗トラップを送信--コミュニティ名またはユーザ名が認識されないためにSNMP要求が拒否された場合にトラップの送信先にアラートを送信するには、このオプション (チェックボックス) を選択します。[Add (追加)]をクリックすると、[* Alerts]ページの[* SNMP]タブにトラップの送信先と関連する名前が表示されます。

8. トラップが有効であることを確認するには、テーブルからトラップの送信先を選択し、*トラップの送信先のテスト*をクリックして、設定したアドレスにテストトラップを送信します。

結果

アラート対象のイベントが発生すると、イベントモニタはSNMPトラップをサーバに送信します。

SNMPアラートのトラップ送信先の追加

SNMPトラップを送信するサーバは最大10台まで追加できます。

開始する前に

- 追加するネットワークサーバにSNMPサービスアプリケーションが設定されている必要があります。イベントモニタがトラップメッセージをそのアドレスに送信できるようにするには、このサーバのネットワークアドレス（IPv4またはIPv6アドレス）が必要です。複数のサーバを使用できます（最大10台のサーバを使用できます）。
- 管理情報ベース（MIB）ファイルは、SNMPサービスアプリケーションを使用してサーバにコピーおよびコンパイルされています。このMIBファイルは、監視および管理されるデータを定義します。

MIBファイルがない場合は、NetAppサポートサイトから入手できます。

- に進みます ["NetAppのサポート"](#)。
- [* Downloads（ダウンロード）]をクリックし、[* Downloads（ダウンロード）]を選択します。
- EシリーズSANtricity OSコントローラソフトウェア*をクリックします。
- [最新リリースのダウンロード]を選択します。
- ログインします。
- 注意事項と使用許諾契約書に同意します。
- コントローラタイプのMIBファイルが表示されるまで下にスクロールし、リンクをクリックしてファイルをダウンロードします。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. SNMP *タブを選択します。

現在定義されているトラップ送信先が表に表示されます。

3. 「トラップのディスパクションを追加」*を選択します。

トラップ送信先の追加ダイアログボックスが開きます。

4. 1つ以上のトラップ送信先を入力し、関連付けられているコミュニティ名またはユーザー名を選択して、*Add *をクリックします。
 - **Trap Destination**-- SNMPサービスを実行しているサーバーのIPv4またはIPv6アドレスを入力します
 - コミュニティ名またはユーザー名--ドロップダウンから、このトラップの送信先のコミュニティ名（SNMPv2c）またはユーザー名（SNMPv3）を選択します。（定義した名前が1つだけの場合は、このフィールドにすでに名前が表示されます）。

- 。認証失敗トラップを送信--コミュニティ名またはユーザ名が認識されないためにSNMP要求が拒否された場合にトラップの送信先にアラートを送信するには、このオプション（チェックボックス）を選択します。「*追加」をクリックすると、トラップの送信先と関連するコミュニティ名またはユーザ名が表に表示されます。

5. トラップが有効であることを確認するには、テーブルからトラップの送信先を選択し、*トラップの送信先のテスト*をクリックして、設定したアドレスにテストトラップを送信します。

結果

アラート対象のイベントが発生すると、イベントモニタはSNMPトラップをサーバに送信します。

SNMP MIB変数の設定

SNMPアラートの場合、必要に応じて、SNMPトラップに表示される管理情報ベース（MIB）変数を設定できます。これらの変数は、ストレージアレイ名、アレイの場所、および担当者を返すことができます。

開始する前に

MIBファイルは、SNMPサービスアプリケーションがインストールされたサーバにコピーしてコンパイルする必要があります。

MIBファイルがない場合は、次の方法で入手できます。

- 。に進みます "[NetAppのサポート](#)"。
- 。[* Downloads（ダウンロード）]をクリックし、[* Downloads（ダウンロード）]を選択します。
- 。EシリーズSANtricity OSコントローラソフトウェア*をクリックします。
- 。[最新リリースのダウンロード]を選択します。
- 。ログインします。
- 。注意事項と使用許諾契約書に同意します。
- 。コントローラタイプのMIBファイルが表示されるまで下にスクロールし、リンクをクリックしてファイルをダウンロードします。

タスクの内容

このタスクでは、SNMPトラップのMIB変数を定義する方法について説明します。これらの変数は、SNMP GetRequestsへの応答として次の値を返すことができます。

- 。sysName（ストレージアレイの名前）
- 。sysLocation（ストレージアレイの場所）
- 。sysContact（管理者の名前）

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。
2. SNMP *タブを選択します。
3. [Configure SNMP MIB Variables]を選択します。

SNMP MIB変数の設定ダイアログボックスが開きます。

4. 次の値を1つ以上入力し、*保存*をクリックします。
 - **Name**-- MIB変数の値 `sysName`。たとえば、ストレージアレイの名前を入力します。
 - **Location**-- MIB変数の値 `sysLocation`。たとえば、ストレージアレイの場所を入力します。
 - **Contact**-- MIB変数の値 `sysContact`。たとえば、ストレージアレイを担当する管理者を入力します。

結果

これらの値は、ストレージアレイのアラートのSNMPトラップメッセージに表示されます。

SNMPv2cトラップのコミュニティの編集

SNMPv2cトラップのコミュニティ名を編集できます。

開始する前に

コミュニティ名を作成する必要があります。

手順

1. メニューを選択します：[Alerts]を設定します。
2. SNMP *タブ*を選択します。

トラップの送信先とコミュニティ名が表に表示されます。

3. [コミュニティの設定]を選択します。
4. 新しいコミュニティ名を入力し、* Save *をクリックします。コミュニティ名には印刷可能なASCII文字のみを使用できます。

結果

[アラート]ページの[SNMP]タブに、更新されたコミュニティ名が表示されます。

SNMPv3トラップのユーザ設定の編集

SNMPv3トラップのユーザ定義を編集できます。

開始する前に

SNMPv3トラップ用のユーザを作成する必要があります。

手順

1. メニューを選択します。Settings [Alerts] (設定[Alerts])。
2. SNMP *タブ*を選択します。

トラップの送信先とユーザ名が表に表示されます。

3. ユーザー定義を編集するには、テーブルでユーザーを選択し、*ユーザーの設定*をクリックします。
4. ダイアログで、*表示/設定の編集*をクリックします。

5. 次の情報を編集します。

- ユーザー名--ユーザーを識別する名前を変更します最大31文字まで入力できます
- エンジンID *--メッセージの認証キーと暗号化キーを生成するために使用されるエンジンIDを選択します管理ドメイン上で一意である必要がありますほとんどの場合、*ローカル*を選択してください。標準以外の設定を使用している場合は、「*カスタム」を選択します。別のフィールドが表示され、10～32文字の範囲で、正規のエンジンIDを16進数の文字列で入力する必要があります。
- 認証資格情報--ユーザーの識別を保証する認証プロトコルを選択します次に、認証プロトコルを設定または変更するときに必要な認証パスワードを入力します。パスワードは8~128文字で指定する必要があります。
- プライバシー資格情報--メッセージの内容を暗号化するために使用するプライバシープロトコルを選択します次に、プライバシープロトコルを設定または変更するときに必要なプライバシーパスワードを入力します。パスワードは8~128文字で指定する必要があります。

結果

[アラート]ページの[SNMP]タブに、更新された設定が表示されます。

SNMPv2cトラップのコミュニティの追加

SNMPv2cトラップには、最大256個のコミュニティ名を追加できます。

手順

1. メニューを選択します。Settings [Alerts] (設定[Alerts])。
2. SNMP *タブを選択します。

トラップの送信先とコミュニティ名が表に表示されます。

3. [コミュニティの設定]を選択します。

コミュニティの設定ダイアログボックスが開きます。

4. [別のコミュニティを追加]を選択します。
5. 新しいコミュニティ名を入力し、* Save *をクリックします。

結果

[Alerts]ページの[SNMP]タブに新しいコミュニティ名が表示されます。

SNMPv3トラップのユーザの追加

SNMPv3トラップには最大256人のユーザを追加できます。

手順

1. メニューを選択します。Settings [Alerts] (設定[Alerts])。
2. SNMP *タブを選択します。

トラップの送信先とユーザ名が表に表示されます。

3. [ユーザーの設定]を選択します。

[SNMPv3ユーザの設定]ダイアログボックスが開きます。

4. 「*追加」を選択します。

5. 次の情報を入力し、*追加*をクリックします。

- ユーザー名--ユーザーを識別するための名前を入力します最大31文字まで入力できます
- エンジンID *--メッセージの認証キーと暗号化キーを生成するために使用されるエンジンIDを選択します管理ドメイン上で一意である必要がありますほとんどの場合、*ローカル*を選択してください。標準以外の設定を使用している場合は、「*カスタム」を選択します。別のフィールドが表示され、10~32文字の範囲で、正規のエンジンIDを16進数の文字列で入力する必要があります。
- 認証資格情報--ユーザーの識別を保証する認証プロトコルを選択します次に、認証プロトコルを設定または変更するときに必要な認証パスワードを入力します。パスワードは8~128文字で指定する必要があります。
- プライバシー資格情報--メッセージの内容を暗号化するために使用するプライバシープロトコルを選択します次に、プライバシープロトコルを設定または変更するときに必要なプライバシーパスワードを入力します。パスワードは8~128文字で指定する必要があります。

SNMPv2cトラップのコミュニティを削除します。

SNMPv2cトラップのコミュニティ名を削除できます。

手順

1. メニューを選択します。Settings [Alerts] (設定[Alerts])。

2. SNMP *タブを選択します。

トラップの送信先とコミュニティ名は、[* Alerts]*ページに表示されます。

3. [コミュニティの設定]を選択します。

コミュニティの設定ダイアログボックスが開きます。

4. 削除するコミュニティ名を選択し、右端の*削除* (X) アイコンをクリックします。

このコミュニティ名にトラップ送信先が関連付けられている場合は、Confirm Remove Communityダイアログボックスに、影響を受けるトラップ送信先アドレスが表示されます。

5. 操作を確定し、*削除*をクリックします。

結果

コミュニティ名とそれに関連付けられているトラップ送信先は、[Alerts]ページから削除されます。

SNMPv3トラップのユーザの削除

SNMPv3トラップのユーザを削除できます。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。

2. SNMP *タブを選択します。

トラップの送信先とユーザ名が[アラート]ページに表示されます。

3. [ユーザーの設定]を選択します。

[SNMPv3ユーザの設定]ダイアログボックスが開きます。

4. 削除するユーザー名を選択し、*削除*をクリックします。

5. 操作を確定し、*削除*をクリックします。

結果

ユーザ名と関連付けられているトラップ送信先が[アラート]ページから削除されます。

トラップ送信先の削除

トラップ送信先アドレスを削除して、ストレージレイのイベントモニタからそのアドレスにSNMPトラップが送信されないようにすることができます。

手順

1. メニューを選択します。Settings [Alerts]（設定[Alerts]）。

2. SNMP *タブを選択します。

トラップ送信先のアドレスが表に表示されます。

3. トラップの送信先を選択し、ページ右上の*削除*をクリックします。

4. 操作を確定し、*削除*をクリックします。

宛先アドレスは[Alerts]ページに表示されなくなります。

結果

削除したトラップ送信先にストレージレイのイベントモニタからSNMPトラップが受信されなくなります。

syslogアラートの管理

アラート用のsyslogサーバの設定

syslogアラートを設定するには、syslogサーバのアドレスとUDPポートを入力する必要があります。最大5つのsyslogサーバを指定できます。

開始する前に

- syslogサーバのアドレスを確認しておく必要があります。このアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
- syslogサーバのUDPポート番号を確認しておく必要があります。通常は514です。

タスクの内容

このタスクでは、syslogサーバのアドレスとポートを入力し、入力したアドレスをテストする方法について説明します。

手順

1. メニューを選択します。Settings [Alerts] (設定[Alerts])。
2. *Syslog *タブを選択します。

syslogサーバがまだ定義されていない場合は、[アラート]ページに「syslogサーバの追加」と表示されません。

3. [Add Syslog Servers]をクリックします。

[Add Syslog Server]ダイアログボックスが開きます。

4. 1つ以上のsyslogサーバ (最大5つ) の情報を入力し、* Add *をクリックします。
 - サーバーアドレス--完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを入力します。
 - **UDP**ポート-- syslogのUDPポートは通常514です。設定されているsyslogサーバが表に表示されます。
5. サーバーアドレスにテストアラートを送信するには、*すべてのSyslogサーバをテスト*を選択します。

結果

アラート対象のイベントが発生すると、イベントモニタからsyslogサーバにアラートが送信されます。監査ログのsyslog設定の詳細については、を参照してください "[監査ログ用のsyslogサーバの設定](#)".



複数のsyslogサーバが設定されている場合は、設定されているすべてのsyslogサーバに監査ログが送信されます。

アラート用のsyslogサーバの編集

syslogアラートの受信に使用するサーバアドレスを編集できます。

手順

1. メニューを選択します。Settings [Alerts] (設定[Alerts])。
2. *Syslog *タブを選択します。
3. 表からsyslogサーバのアドレスを選択し、右端の* Edit * (鉛筆) アイコンをクリックします。

行が編集可能なフィールドになります。

4. サーバーアドレスとUDPポート番号を編集し、保存 (チェックマーク) アイコンをクリックします。

結果

更新されたサーバアドレスがテーブルに表示されます。

アラート用のsyslogサーバの追加

syslogアラート用に最大5台のサーバを追加できます。

開始する前に

- syslogサーバのアドレスを確認しておく必要があります。このアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
- syslogサーバのUDPポート番号を確認しておく必要があります。通常は514です。

手順

1. メニューを選択します。Settings [Alerts] (設定[Alerts])。
2. *Syslog *タブを選択します。
3. [Add Syslog Servers]を選択します。

[Add Syslog Server]ダイアログボックスが開きます。

4. [Add another syslog server*]を選択します。
5. syslogサーバの情報を入力し、*Add*をクリックします。

- **Syslog**サーバ・アドレス--完全修飾ドメイン名'IPv4アドレス'またはIPv6アドレスを入力します
- **UDP**ポート-- syslogのUDPポートは通常514です。



最大5台のsyslogサーバを設定できます。

結果

syslogサーバのアドレスが表に表示されます。

アラート用のsyslogサーバの削除

syslogサーバを削除してアラートの受信を中止することができます。

手順

1. メニューを選択します。Settings [Alerts] (設定[Alerts])。
2. *Syslog *タブを選択します。
3. syslogサーバのアドレスを選択し、右上の「* Remove *」をクリックします。

Confirm Delete Syslog Serverダイアログボックスが開きます。

4. 操作を確定し、*削除*をクリックします。

結果

削除したサーバにイベントモニタからアラートが送信されなくなります。

FAQ

アラートが無効になっている場合

ストレージアレイで発生した重要なイベントに関する通知を管理者が受信できるようにするには、アラート方法を設定する必要があります。

SANtricity System Managerで管理されるストレージアレイの場合は、アラートページからアラートを設定します。アラート通知は、Eメール、SNMPトラップ、またはsyslogメッセージを使用して送信できます。また、初期セットアップウィザードでEメールアラートを設定することもできます。

SNMPまたはsyslogアラートを設定するにはどうすればよいですか？

Eメールアラートに加えて、簡易ネットワーク管理プロトコル（SNMP）トラップまたはsyslogメッセージで送信されるようにアラートを設定できます。

SNMPまたはsyslogのアラートを設定するには、メニューの[アラート]に移動します。

アレイとアラートでタイムスタンプが一致しないのはなぜですか？

ストレージアレイは、アラートの送信時に、アラートを受信するターゲットサーバまたはホストのタイムゾーンに合わせて修正しません。代わりに、ローカル時間（GMT）を使用してアラートの記録に使用されるタイムスタンプを作成します。そのため、ストレージアレイのタイムスタンプとアラートを受信するサーバまたはホストのタイムスタンプが一致しないことがあります。

ストレージアレイではアラートの送信時にタイムゾーンが修正されないため、アラートのタイムスタンプはGMT相対であり、タイムゾーンオフセットはゼロです。ローカルタイムゾーンに適したタイムスタンプを計算するには、GMTからの時間オフセットを決定し、タイムスタンプからその値を加算または減算する必要があります。

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。