Alertes

SANtricity 11.8

NetApp
December 16, 2024

Sommaire

Alertes

Présentation des alertes

Vous pouvez configurer System Manager pour envoyer des alertes de baie de stockage par e-mail, des interruptions SNMP et des messages syslog.

Que sont les alertes ?

Alerts signale aux administrateurs les événements importants qui se produisent sur la baie de stockage. Les événements peuvent inclure des problèmes, par exemple une panne de batterie, le déplacement d'un composant de optimal à hors ligne ou les erreurs de redondance dans le contrôleur. Tous les événements critiques sont considérés comme « alertables », ainsi que quelques événements Avertissement et informationnel.

En savoir plus :

- "Fonctionnement des alertes"
- "Terminologie des alertes"

Comment configurer les alertes ?

Vous pouvez configurer les alertes pour qu'elles soient envoyées sous forme de message à une ou plusieurs adresses e-mail, sous forme de trap SNMP vers un serveur SNMP ou sous forme de message vers un serveur syslog. La configuration des alertes est disponible dans le **Paramètres › alertes**.

En savoir plus :

- "Configurer le serveur de messagerie et les destinataires pour les alertes"
- "Configurer le serveur syslog pour les alertes"
- "Configurez les alertes SNMP"

Informations associées

En savoir plus sur les concepts liés aux alertes :

- "Présentation du journal des événements"
- "Horodatage incohérent"

Concepts

Fonctionnement des alertes

Les alertes signalent aux administrateurs les événements importants survenant sur la baie de stockage. Les alertes peuvent être envoyées par e-mail, des traps SNMP et des syslog.

La procédure d'alertes fonctionne comme suit :

1. Un administrateur configure une ou plusieurs des méthodes d'alerte suivantes dans System Manager :
   - **Email** — les messages sont envoyés à des adresses électroniques.
   - **SNMP** — les interruptions SNMP sont envoyées à un serveur SNMP.
   - **Syslog** — les messages sont envoyés à un serveur syslog.
2. Lorsque le moniteur d'événements de la matrice de stockage détecte un problème, il écrit les informations relatives à ce problème dans le journal des événements (disponible à partir du **support › Journal des événements**). Par exemple, des problèmes peuvent inclure des événements, tels qu'une panne de batterie, le déplacement d'un composant d'optimal vers hors ligne ou les erreurs de redondance dans le contrôleur.
3. Si le moniteur d'événements détermine que l'événement est « alertable », il envoie ensuite une notification en utilisant les méthodes d'alerte configurées (messagerie électronique, SNMP et/ou syslog). Tous les événements critiques sont considérés comme « alertables », ainsi que quelques événements Avertissement et informationnel.

Configuration des alertes

Vous pouvez configurer les alertes à partir de l'assistant de configuration initiale (pour les alertes par e-mail uniquement) ou de la page alertes. Pour vérifier la configuration actuelle, accédez au **Paramètres › alertes**.

La mosaïque alertes affiche la configuration des alertes, qui peut être l'une des suivantes :

- Non configuré.
- Configuré ; au moins une méthode d'alerte est configurée. Pour déterminer quelles méthodes d'alerte sont configurées, pointez le curseur sur la mosaïque.

Informations sur les alertes

Les alertes peuvent inclure les types d'informations suivants :

- Nom de la matrice de stockage.
- Type d'erreur d'événement lié à une entrée du journal des événements.
- Date et heure auxquelles l'événement s'est produit.
- Brève description de l'événement.

Les alertes syslog suivent la norme de messagerie RFC 5424.

Terminologie des alertes

Découvrez comment les conditions d'alerte s'appliquent à votre baie de stockage.

Composant	Description
Contrôle des événements	Le moniteur d'événements se trouve sur la matrice de stockage et s'exécute en arrière-plan. Lorsque le contrôle des événements détecte des anomalies sur la baie de stockage, il écrit les informations relatives aux problèmes dans le journal des événements. Les problèmes peuvent inclure des événements, tels qu'une panne de batterie, le passage d'un composant optimal à hors ligne ou les erreurs de redondance dans le contrôleur. Si le moniteur d'événements détermine que l'événement est « alertable », il envoie ensuite une notification en utilisant les méthodes d'alerte configurées (messagerie électronique, SNMP et/ou syslog). Tous les événements critiques sont considérés comme « alertables », ainsi que quelques événements Avertissement et informationnel.
Serveur de messagerie	Le serveur de messagerie est utilisé pour envoyer et recevoir des alertes par e-mail. Le serveur utilise le protocole SMTP (simple Mail Transfer Protocol).
SNMP	Le protocole SNMP (simple Network Management Protocol) est un protocole standard Internet utilisé pour gérer et partager des informations entre des périphériques sur des réseaux IP.
Interruption SNMP	Une interruption SNMP est une notification envoyée à un serveur SNMP. Le trap contient des informations sur des problèmes majeurs avec la matrice de stockage.
Destination du trap SNMP	Une destination d'interruption SNMP est une adresse IPv4 ou IPv6 du serveur exécutant un service SNMP.
Nom de communauté	Un nom de communauté est une chaîne qui agit comme un mot de passe pour le ou les serveurs réseau dans un environnement SNMP.
Fichier MIB	Le fichier MIB (Management information base) définit les données en cours de contrôle et de gestion dans la baie de stockage. Il doit être copié et compilé sur le serveur avec l'application de service SNMP. Ce fichier MIB est disponible avec le logiciel System Manager sur le site de support.
Variables MIB	Les variables de la base d'informations de gestion (MIB) peuvent renvoyer des valeurs telles que le nom de la matrice de stockage, l'emplacement de la matrice et une personne de contact en réponse à SNMP GetRequests.
Syslog	Syslog est un protocole utilisé par les périphériques réseau pour envoyer des messages d'événement à un serveur de consignation.
UDP	User Datagram Protocol (UDP) est un protocole de couche transport qui spécifie un numéro de port source et de destination dans leurs en-têtes de paquets.

Gérer les alertes par e-mail

Configurer le serveur de messagerie et les destinataires pour les alertes

Pour configurer les alertes par e-mail, vous devez spécifier une adresse de serveur de messagerie et les adresses e-mail des destinataires de l'alerte. Jusqu'à 20 adresses e-mail sont autorisées.

Avant de commencer

- L'adresse du serveur de messagerie doit être disponible. L'adresse peut être une adresse IPv4 ou IPv6 ou un nom de domaine complet.

> Pour utiliser un nom de domaine complet, vous devez configurer un serveur DNS sur les deux contrôleurs. Vous pouvez configurer un serveur DNS à partir de la page matériel.

- L'adresse e-mail à utiliser comme expéditeur de l'alerte doit être disponible. Il s'agit de l'adresse qui apparaît dans le champ « de » du message d'alerte. Une adresse d'expéditeur est requise dans le protocole SMTP ; sans cette adresse, une erreur se produit.
- L'adresse e-mail du ou des destinataires de l'alerte doit être disponible. Le destinataire est généralement une adresse pour un administrateur réseau ou un administrateur de stockage. Vous pouvez entrer jusqu'à 20 adresses électroniques.

Description de la tâche

Cette tâche décrit comment configurer le serveur de messagerie, saisir les adresses e-mail de l'expéditeur et des destinataires, et tester toutes les adresses e-mail saisies à partir de la page alertes.

> Les alertes par e-mail peuvent également être configurées à partir de l'assistant de configuration initiale.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.

   Si un serveur de messagerie n'est pas encore configuré, l'onglet E-mail affiche « configurer le serveur de messagerie ».

3. Sélectionnez **configurer le serveur de messagerie**.

   La boîte de dialogue configurer le serveur de messagerie s'ouvre.

4. Entrez les informations du serveur de messagerie, puis cliquez sur **Enregistrer**.
   - **Adresse du serveur de messagerie** — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6 du serveur de messagerie.

     > Pour utiliser un nom de domaine complet, vous devez configurer un serveur DNS sur les deux contrôleurs. Vous pouvez configurer un serveur DNS à partir de la page matériel.

   - **Adresse de l'expéditeur de l'e-mail** — Entrez une adresse e-mail valide à utiliser comme expéditeur de l'e-mail. Cette adresse apparaît dans le champ « de » du message électronique.
   - **Cryptage** — si vous souhaitez crypter des messages, sélectionnez **SMTPS** ou **STARTTLS** pour le type de cryptage, puis sélectionnez le numéro de port pour les messages cryptés. Sinon, sélectionnez **aucun**.

- **Nom d'utilisateur et mot de passe** — si nécessaire, entrez un nom d'utilisateur et un mot de passe pour l'authentification avec l'expéditeur sortant et le serveur de messagerie.
- **Inclure les informations de contact dans l'e-mail** — pour inclure les coordonnées de l'expéditeur avec le message d'alerte, sélectionnez cette option, puis entrez un nom et un numéro de téléphone.

  Après avoir cliqué sur **Enregistrer**, les adresses e-mail apparaissent dans l'onglet E-mail de la page alertes.

5. Sélectionnez **Ajouter des e-mails**.

   La boîte de dialogue Ajouter des e-mails s'ouvre.

6. Entrez une ou plusieurs adresses e-mail pour les destinataires de l'alerte, puis cliquez sur **Ajouter**.

   Les adresses e-mail s'affichent sur la page alertes.

7. Si vous voulez vous assurer que les adresses électroniques sont valides, cliquez sur **Tester tous les e-mails** pour envoyer des messages de test aux destinataires.

Résultats

Une fois que vous avez configuré des alertes par e-mail, le moniteur d'événements envoie des e-mails aux destinataires spécifiés lorsqu'un événement alertable se produit.

Modifiez les adresses e-mail des alertes

Vous pouvez modifier les adresses e-mail des destinataires qui reçoivent des alertes par e-mail.

Avant de commencer

L'adresse e-mail que vous souhaitez modifier doit être définie dans l'onglet E-mail de la page alertes.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.
3. Dans le tableau **Email Address**, sélectionnez l'adresse à modifier, puis cliquez sur l'icône **Edit** (crayon) à l'extrême droite.

   La ligne devient un champ modifiable.

4. Entrez une nouvelle adresse, puis cliquez sur l'icône **Enregistrer** (coche).

   Pour annuler les modifications, sélectionnez l'icône **Annuler** (X).

Résultats

L'onglet E-mail de la page alertes affiche les adresses e-mail mises à jour.

Ajoutez des adresses e-mail pour les alertes

Vous pouvez ajouter jusqu'à 20 destinataires pour les alertes par e-mail.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.
3. Sélectionnez **Ajouter des e-mails**.

   La boîte de dialogue Ajouter des e-mails s'ouvre.

4. Dans le champ vide, saisissez une nouvelle adresse e-mail. Si vous souhaitez ajouter plusieurs adresses, sélectionnez **Ajouter un autre e-mail** pour ouvrir un autre champ.
5. Cliquez sur **Ajouter**.

Résultats

L'onglet E-mail de la page alertes affiche les nouvelles adresses e-mail.

Supprimez le serveur de messagerie ou les adresses e-mail pour les alertes

Vous pouvez supprimer le serveur de messagerie précédemment défini afin que les alertes ne soient plus envoyées aux adresses électroniques, ou vous pouvez supprimer des adresses électroniques individuelles.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.
3. Dans le tableau, effectuez l'une des opérations suivantes :
   - Pour supprimer un serveur de messagerie afin que les alertes ne soient plus envoyées aux adresses e-mail, sélectionnez la ligne du serveur de messagerie.
   - Pour supprimer une adresse e-mail afin que les alertes ne soient plus envoyées à cette adresse, sélectionnez la ligne de l'adresse e-mail que vous souhaitez supprimer. Le bouton **Supprimer** dans le coin supérieur droit de la table devient disponible pour la sélection.
4. Cliquez sur **Supprimer** et confirmez l'opération.

Modifiez le serveur de messagerie pour les alertes

Vous pouvez modifier l'adresse du serveur de messagerie et l'adresse de l'expéditeur utilisée pour les alertes par e-mail.

Avant de commencer

L'adresse du serveur de messagerie que vous modifiez doit être disponible. L'adresse peut être une adresse IPv4 ou IPv6 ou un nom de domaine complet.

Pour utiliser un nom de domaine complet, vous devez configurer un serveur DNS sur les deux contrôleurs. Vous pouvez configurer un serveur DNS à partir de la page matériel.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **E-mail**.
3. Sélectionnez **configurer le serveur de messagerie**.

La boîte de dialogue configurer le serveur de messagerie s'ouvre.

4. Modifiez l'adresse du serveur de messagerie, les informations d'expéditeur et les informations de contact.
   - **Adresse du serveur de messagerie** — modifiez le nom de domaine complet, l'adresse IPv4 ou l'adresse IPv6 du serveur de messagerie.

     Pour utiliser un nom de domaine complet, vous devez configurer un serveur DNS sur les deux contrôleurs. Vous pouvez configurer un serveur DNS à partir de la page matériel.

   - **Adresse de l'expéditeur de l'e-mail** — modifiez l'adresse e-mail à utiliser comme expéditeur de l'e-mail. Cette adresse apparaît dans le champ « de » du message électronique.
   - **Inclure les informations de contact dans l'e-mail** — pour modifier les coordonnées de l'expéditeur, sélectionnez cette option, puis modifiez le nom et le numéro de téléphone.
5. Cliquez sur **Enregistrer**.

Gérer les alertes SNMP

Configurez les alertes SNMP

Pour configurer les alertes SNMP (simple Network Management Protocol), vous devez identifier au moins un serveur sur lequel le moniteur d'événements de la baie de stockage peut envoyer des traps SNMP. La configuration requiert un nom de communauté ou d'utilisateur et une adresse IP pour le serveur.

Avant de commencer

- Un serveur réseau doit être configuré avec une application de service SNMP. Vous avez besoin de l'adresse réseau de ce serveur (soit une adresse IPv4, soit une adresse IPv6), de sorte que le moniteur d'événements puisse envoyer des messages d'interruption à cette adresse. Vous pouvez utiliser plusieurs serveurs (jusqu'à 10 serveurs sont autorisés).
- Le fichier MIB (Management information base) a été copié et compilé sur le serveur avec l'application de service SNMP. Ce fichier MIB définit les données en cours de contrôle et de gestion.

  Si vous ne possédez pas le fichier MIB, vous pouvez l'obtenir sur le site de support NetApp :

  - Allez à "Support NetApp".
  - Cliquez sur l'onglet **Téléchargements**, puis sélectionnez **Téléchargements**.
  - Cliquez sur **logiciel de contrôleur de système d'exploitation SANtricity E-Series**.
  - Sélectionnez **Télécharger la dernière version**.
  - Connectez-vous.
  - Acceptez la déclaration de mise en garde et le contrat de licence.
  - Faites défiler vers le bas jusqu'à ce que le fichier MIB de votre type de contrôleur, puis cliquez sur le lien pour télécharger le fichier.

Description de la tâche

Cette tâche décrit comment identifier le serveur SNMP pour les destinations de déroutement, puis tester votre configuration.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Lors de la configuration initiale, l'onglet SNMP affiche « configurer les communautés/utilisateurs ».

3. Sélectionnez **configurer les communautés/utilisateurs**.

   La boîte de dialogue Sélectionner une version SNMP s'ouvre.

4. Sélectionnez la version SNMP pour les alertes, soit **SNMPv2c**, soit **SNMPv3**.

   Selon votre sélection, la boîte de dialogue configurer les communautés ou configurer les utilisateurs SNMPv3 s'ouvre.

5. Suivez les instructions appropriées pour SNMPv2c (communautés) ou SNMPv3 (utilisateurs) :
   - **SNMPv2c (communautés)** — dans la boîte de dialogue configurer les communautés, entrez une ou plusieurs chaînes de communauté pour les serveurs réseau. Un nom de communauté est une chaîne qui identifie un ensemble connu de stations de gestion et qui est généralement créé par un administrateur réseau. Il se compose uniquement de caractères ASCII imprimables. Vous pouvez ajouter jusqu'à 256 communautés. Lorsque vous avez terminé, cliquez sur **Enregistrer**.
   - **SNMPv3 (utilisateurs)** — dans la boîte de dialogue configurer les utilisateurs SNMPv3, cliquez sur **Ajouter**, puis entrez les informations suivantes :
     - **Nom d'utilisateur** — Entrez un nom pour identifier l'utilisateur, qui peut comporter jusqu'à 31 caractères.
     - **ID moteur** — sélectionnez l'ID moteur, qui est utilisé pour générer des clés d'authentification et de cryptage pour les messages, et doit être unique dans le domaine administratif. Dans la plupart des cas, vous devez sélectionner **local**. Si vous avez une configuration non standard, sélectionnez **Custom** ; un autre champ apparaît où vous devez entrer l'ID de moteur faisant autorité en tant que chaîne hexadécimale, avec un nombre pair de caractères compris entre 10 et 32 caractères.
     - **Authentification d'authentification** — sélectionnez un protocole d'authentification qui garantit l'identité des utilisateurs. Ensuite, entrez un mot de passe d'authentification requis lorsque le protocole d'authentification est défini ou modifié. Le mot de passe doit comporter entre 8 et 128 caractères.
     - **Données d'identification** — sélectionnez un protocole de confidentialité utilisé pour crypter le contenu des messages. Ensuite, entrez un mot de passe de confidentialité, requis lorsque le protocole de confidentialité est défini ou modifié. Le mot de passe doit comporter entre 8 et 128 caractères. Lorsque vous avez terminé, cliquez sur **Ajouter**, puis sur **Fermer**.
6. Dans la page alertes avec l'onglet SNMP sélectionné, cliquez sur **Ajouter des destinations de déroutement**.

   La boîte de dialogue Ajouter des destinations de recouvrement s'ouvre.

7. Entrez une ou plusieurs destinations d'interruption, sélectionnez leurs noms de communauté ou d'utilisateur associés, puis cliquez sur **Ajouter**.
   - **Trap destination** — Entrez une adresse IPv4 ou IPv6 du serveur exécutant un service SNMP.
   - **Nom de communauté ou Nom d'utilisateur** — dans le menu déroulant, sélectionnez le nom de communauté (SNMPv2c) ou le nom d'utilisateur (SNMPv3) pour cette destination de déroutement. (Si vous en avez défini un seul, le nom apparaît déjà dans ce champ.)

- **Send Authentication Failure Trap** — sélectionnez cette option (la case à cocher) si vous souhaitez alerter la destination de l'interruption lorsqu'une requête SNMP est rejetée en raison d'un nom de communauté ou d'utilisateur non reconnu. Après avoir cliqué sur **Ajouter**, les destinations de déroutement et les noms associés apparaissent dans l'onglet **SNMP** de la page **alertes**.

8. Pour vous assurer qu'une interruption est valide, sélectionnez une destination d'interruption dans le tableau, puis cliquez sur **Test Trap destination** pour envoyer une interruption de test à l'adresse configurée.

Résultats

Le moniteur d'événements envoie des interruptions SNMP au(x) serveur(s) chaque fois qu'un événement alertable se produit.

Ajoutez des destinations d'interruption pour les alertes SNMP

Vous pouvez ajouter jusqu'à 10 serveurs pour envoyer des interruptions SNMP.

Avant de commencer

- Le serveur réseau que vous souhaitez ajouter doit être configuré avec une application de service SNMP. Vous avez besoin de l'adresse réseau de ce serveur (soit une adresse IPv4, soit une adresse IPv6), de sorte que le moniteur d'événements puisse envoyer des messages d'interruption à cette adresse. Vous pouvez utiliser plusieurs serveurs (jusqu'à 10 serveurs sont autorisés).
- Le fichier MIB (Management information base) a été copié et compilé sur le serveur avec l'application de service SNMP. Ce fichier MIB définit les données en cours de contrôle et de gestion.

  Si vous ne possédez pas le fichier MIB, vous pouvez l'obtenir sur le site de support NetApp :

  - Allez à "Support NetApp".
  - Cliquez sur **Téléchargements**, puis sélectionnez **Téléchargements**.
  - Cliquez sur **logiciel de contrôleur de système d'exploitation SANtricity E-Series**.
  - Sélectionnez **Télécharger la dernière version**.
  - Connectez-vous.
  - Acceptez la déclaration de mise en garde et le contrat de licence.
  - Faites défiler vers le bas jusqu'à ce que le fichier MIB de votre type de contrôleur, puis cliquez sur le lien pour télécharger le fichier.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations d'interruption actuellement définies apparaissent dans le tableau.

3. Sélectionnez **Ajouter des déations de recouvrement**.

   La boîte de dialogue Ajouter des destinations de recouvrement s'ouvre.

4. Entrez une ou plusieurs destinations d'interruption, sélectionnez leurs noms de communauté ou d'utilisateur associés, puis cliquez sur **Ajouter**.
   - **Trap destination** — Entrez une adresse IPv4 ou IPv6 du serveur exécutant un service SNMP.

- **Nom de communauté ou Nom d'utilisateur** — dans le menu déroulant, sélectionnez le nom de communauté (SNMPv2c) ou le nom d'utilisateur (SNMPv3) pour cette destination de déroutement. (Si vous en avez défini un seul, le nom apparaît déjà dans ce champ.)
- **Send Authentication Failure Trap** — sélectionnez cette option (la case à cocher) si vous souhaitez alerter la destination de l'interruption lorsqu'une requête SNMP est rejetée en raison d'un nom de communauté ou d'utilisateur non reconnu. Après avoir cliqué sur **Ajouter**, les destinations de déroutement et les noms de communauté ou d'utilisateur associés apparaissent dans le tableau.

5. Pour vous assurer qu'une interruption est valide, sélectionnez une destination d'interruption dans le tableau, puis cliquez sur **Test Trap destination** pour envoyer une interruption de test à l'adresse configurée.

Résultats

Le moniteur d'événements envoie des interruptions SNMP au(x) serveur(s) chaque fois qu'un événement alertable se produit.

Configurer les variables MIB SNMP

Pour les alertes SNMP, vous pouvez éventuellement configurer les variables MIB (Management information base) qui apparaissent dans les traps SNMP. Ces variables peuvent renvoyer le nom de la matrice de stockage, l'emplacement de la matrice et une personne à contacter.

Avant de commencer

Le fichier MIB doit être copié et compilé sur le serveur avec l'application de service SNMP.

Si vous n'avez pas de fichier MIB, vous pouvez l'obtenir comme suit:

- Allez à "Support NetApp".
- Cliquez sur **Téléchargements**, puis sélectionnez **Téléchargements**.
- Cliquez sur **logiciel de contrôleur de système d'exploitation SANtricity E-Series**.
- Sélectionnez **Télécharger la dernière version**.
- Connectez-vous.
- Acceptez la déclaration de mise en garde et le contrat de licence.
- Faites défiler vers le bas jusqu'à ce que le fichier MIB de votre type de contrôleur, puis cliquez sur le lien pour télécharger le fichier.

Description de la tâche

Cette tâche décrit comment définir des variables MIB pour les interruptions SNMP. Ces variables peuvent renvoyer les valeurs suivantes en réponse à SNMP GetRequests :

- `sysName` (nom de la matrice de stockage)
- `sysLocation` (emplacement de la matrice de stockage)
- `sysContact` (nom d'un administrateur)

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

3. Sélectionnez **configurer les variables MIB SNMP**.

   La boîte de dialogue configurer les variables MIB SNMP s'ouvre.

4. Entrez une ou plusieurs des valeurs suivantes, puis cliquez sur **Enregistrer**.
   - **Nom** — la valeur de la variable MIB `sysName` . Par exemple, entrez un nom pour la matrice de stockage.
   - **Emplacement** — la valeur de la variable MIB `sysLocation` . Par exemple, entrez un emplacement de la matrice de stockage.
   - **Contact** — la valeur de la variable MIB `sysContact` . Par exemple, entrez un administrateur responsable de la matrice de stockage.

Résultats

Ces valeurs apparaissent dans les messages d'interruption SNMP relatifs aux alertes de la baie de stockage.

Modifier des communautés pour les déroutements SNMPv2c

Vous pouvez modifier les noms de communauté pour les déroutements SNMPv2c.

Avant de commencer

Un nom de communauté doit être créé.

Étapes

1. Sélectionnez **Réglage › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations d'interruption et les noms de communauté apparaissent dans le tableau.

3. Sélectionnez **configurer les communautés**.
4. Entrez le nouveau nom de communauté, puis cliquez sur **Enregistrer**. Les noms de communauté ne peuvent contenir que des caractères ASCII imprimables.

Résultats

L'onglet SNMP de la page alertes affiche le nom de communauté mis à jour.

Modifier les paramètres utilisateur pour les recouvrements SNMPv3

Vous pouvez modifier les définitions d'utilisateur pour les recouvrements SNMPv3.

Avant de commencer

Un utilisateur doit être créé pour le trap SNMPv3.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations d'interruption et les noms d'utilisateur apparaissent dans le tableau.

3. Pour modifier une définition d'utilisateur, sélectionnez-la dans le tableau, puis cliquez sur **configurer les**

utilisateurs.

4. Dans la boîte de dialogue, cliquez sur **Afficher/Modifier les paramètres**.
5. Modifiez les informations suivantes :
   - **Nom d'utilisateur** — modifiez le nom qui identifie l'utilisateur, qui peut comporter jusqu'à 31 caractères.
   - **ID moteur** — sélectionnez l'ID moteur, qui est utilisé pour générer des clés d'authentification et de cryptage pour les messages, et doit être unique dans le domaine administratif. Dans la plupart des cas, vous devez sélectionner **local**. Si vous avez une configuration non standard, sélectionnez **Custom** ; un autre champ apparaît où vous devez entrer l'ID de moteur faisant autorité en tant que chaîne hexadécimale, avec un nombre pair de caractères compris entre 10 et 32 caractères.
   - **Authentification d'authentification** — sélectionnez un protocole d'authentification qui garantit l'identité des utilisateurs. Ensuite, entrez un mot de passe d'authentification requis lorsque le protocole d'authentification est défini ou modifié. Le mot de passe doit comporter entre 8 et 128 caractères.
   - **Données d'identification** — sélectionnez un protocole de confidentialité utilisé pour crypter le contenu des messages. Ensuite, entrez un mot de passe de confidentialité, requis lorsque le protocole de confidentialité est défini ou modifié. Le mot de passe doit comporter entre 8 et 128 caractères.

Résultats

L'onglet SNMP de la page alertes affiche les paramètres mis à jour.

Ajouter des communautés pour les déroutements SNMPv2c

Vous pouvez ajouter jusqu'à 256 noms de communauté pour les déroutements SNMPv2c.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations d'interruption et les noms de communauté apparaissent dans le tableau.

3. Sélectionnez **configurer les communautés**.

   La boîte de dialogue configurer les communautés s'ouvre.

4. Sélectionnez **Ajouter une autre communauté**.
5. Entrez le nouveau nom de communauté, puis cliquez sur **Enregistrer**.

Résultats

Le nouveau nom de communauté apparaît dans l'onglet SNMP de la page alertes.

Ajouter des utilisateurs pour les interruptions SNMPv3

Vous pouvez ajouter jusqu'à 256 utilisateurs pour les interruptions SNMPv3.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

Les destinations d'interruption et les noms d'utilisateur apparaissent dans le tableau.

3. Sélectionnez **configurer les utilisateurs**.

   La boîte de dialogue configurer les utilisateurs SNMPv3 s'ouvre.

4. Sélectionnez **Ajouter**.
5. Entrez les informations suivantes, puis cliquez sur **Ajouter**.
   - **Nom d'utilisateur** — Entrez un nom pour identifier l'utilisateur, qui peut comporter jusqu'à 31 caractères.
   - **ID moteur** — sélectionnez l'ID moteur, qui est utilisé pour générer des clés d'authentification et de cryptage pour les messages, et doit être unique dans le domaine administratif. Dans la plupart des cas, vous devez sélectionner **local**. Si vous avez une configuration non standard, sélectionnez **Custom** ; un autre champ apparaît où vous devez entrer l'ID de moteur faisant autorité en tant que chaîne hexadécimale, avec un nombre pair de caractères compris entre 10 et 32 caractères.
   - **Authentification d'authentification** — sélectionnez un protocole d'authentification qui garantit l'identité des utilisateurs. Ensuite, entrez un mot de passe d'authentification requis lorsque le protocole d'authentification est défini ou modifié. Le mot de passe doit comporter entre 8 et 128 caractères.
   - **Données d'identification** — sélectionnez un protocole de confidentialité utilisé pour crypter le contenu des messages. Ensuite, entrez un mot de passe de confidentialité, requis lorsque le protocole de confidentialité est défini ou modifié. Le mot de passe doit comporter entre 8 et 128 caractères.

Supprimer des communautés pour les déroutements SNMPv2c

Vous pouvez supprimer un nom de communauté pour les déroutements SNMPv2c.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations de déroutement et les noms de communauté apparaissent sur la page **alertes**.

3. Sélectionnez **configurer les communautés**.

   La boîte de dialogue configurer les communautés s'ouvre.

4. Sélectionnez le nom de communauté à supprimer, puis cliquez sur l'icône **Supprimer** (X) à l'extrême droite.

   Si les destinations d'interruption sont associées à ce nom de communauté, la boîte de dialogue confirmer la suppression de la communauté affiche les adresses de destination d'interruption affectées.

5. Confirmez l'opération, puis cliquez sur **Supprimer**.

Résultats

Le nom de communauté et sa destination de déroutement associée sont supprimés de la page alertes.

Supprimer les utilisateurs pour les interruptions SNMPv3

Vous pouvez supprimer un utilisateur pour les interruptions SNMPv3.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les destinations des interruptions et les noms d'utilisateur apparaissent sur la page alertes.

3. Sélectionnez **configurer les utilisateurs**.

   La boîte de dialogue configurer les utilisateurs SNMPv3 s'ouvre.

4. Sélectionnez le nom d'utilisateur à supprimer, puis cliquez sur **Supprimer**.
5. Confirmez l'opération, puis cliquez sur **Supprimer**.

Résultats

Le nom d'utilisateur et sa destination de déroutement associée sont supprimés de la page alertes.

Supprimer les destinations d'interruption

Vous pouvez supprimer une adresse de destination d'interruption afin que le moniteur d'événements de la matrice de stockage n'envoie plus d'interruptions SNMP à cette adresse.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **SNMP**.

   Les adresses de destination des interruptions apparaissent dans le tableau.

3. Sélectionnez une destination d'interruption, puis cliquez sur **Supprimer** dans le coin supérieur droit de la page.
4. Confirmez l'opération, puis cliquez sur **Supprimer**.

   L'adresse de destination n'apparaît plus sur la page alertes.

Résultats

La destination de trap supprimée ne reçoit plus d'interruptions SNMP du moniteur d'événements de la matrice de stockage.

Gérer les alertes syslog

Configurer le serveur syslog pour les alertes

Pour configurer les alertes syslog, vous devez entrer une adresse de serveur syslog et un port UDP. Jusqu'à cinq serveurs syslog sont autorisés.

Avant de commencer

- L'adresse du serveur syslog doit être disponible. Cette adresse peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.

- Le numéro de port UDP du serveur syslog doit être disponible. Ce port est généralement 514.

Description de la tâche

Cette tâche décrit comment saisir l'adresse et le port du serveur syslog, puis tester l'adresse que vous avez saisie.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **Syslog**.

   Si un serveur syslog n'est pas encore défini, la page alertes affiche « Ajouter des serveurs Syslog ».

3. Cliquez sur **Ajouter des serveurs Syslog**.

   La boîte de dialogue Ajouter un serveur Syslog s'ouvre.

4. Entrez des informations pour un ou plusieurs serveurs syslog (maximum de cinq), puis cliquez sur **Ajouter**.
   - **Adresse du serveur** — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
   - **Port UDP** — généralement, le port UDP pour syslog est 514. Le tableau affiche les serveurs syslog configurés.
5. Pour envoyer une alerte de test aux adresses du serveur, sélectionnez **Tester tous les serveurs Syslog**.

Résultats

Le moniteur d'événements envoie des alertes au serveur syslog lorsqu'un événement alertable se produit. Pour configurer davantage les paramètres syslog des journaux d'audit, reportez-vousà la section "Configuration du serveur syslog pour les journaux d'audit".

> Si plusieurs serveurs syslog sont configurés, tous les serveurs syslog configurés recevront un journal d'audit.

Modifier les serveurs syslog pour les alertes

Vous pouvez modifier l'adresse du serveur utilisée pour la réception d'alertes syslog.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **Syslog**.
3. Dans le tableau, sélectionnez une adresse de serveur syslog, puis cliquez sur l'icône **Edit** (crayon) à l'extrême droite.

   La ligne devient un champ modifiable.

4. Modifiez l'adresse du serveur et le numéro de port UDP, puis cliquez sur l'icône **Enregistrer** (coche).

Résultats

L'adresse du serveur mise à jour apparaît dans le tableau.

Ajouter des serveurs syslog pour les alertes

Vous pouvez ajouter au maximum cinq serveurs pour les alertes syslog.

Avant de commencer

- L'adresse du serveur syslog doit être disponible. Cette adresse peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Le numéro de port UDP du serveur syslog doit être disponible. Ce port est généralement 514.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **Syslog**.
3. Sélectionnez **Ajouter des serveurs Syslog**.

   La boîte de dialogue Ajouter un serveur Syslog s'ouvre.

4. Sélectionnez **Ajouter un autre serveur syslog**.
5. Entrez les informations relatives au serveur syslog, puis cliquez sur **Ajouter**.

   - **Adresse du serveur Syslog** — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
   - **Port UDP** — généralement, le port UDP pour syslog est 514.

   Vous pouvez configurer jusqu'à cinq serveurs syslog.

Résultats

Les adresses des serveurs syslog apparaissent dans le tableau.

Supprimez les serveurs syslog pour les alertes

Vous pouvez supprimer un serveur syslog afin qu'il ne reçoive plus d'alertes.

Étapes

1. Sélectionnez **Paramètres › alertes**.
2. Sélectionnez l'onglet **Syslog**.
3. Sélectionnez une adresse de serveur syslog, puis cliquez sur **Supprimer** dans le coin supérieur droit.

   La boîte de dialogue confirmer la suppression du serveur Syslog s'ouvre.

4. Confirmez l'opération, puis cliquez sur **Supprimer**.

Résultats

Le serveur que vous avez supprimé ne reçoit plus d'alertes du moniteur d'événements.

FAQ

Que se passe-t-il si les alertes sont désactivées ?

Si vous souhaitez que les administrateurs reçoivent des notifications concernant les événements importants qui se produisent dans la matrice de stockage, vous devez configurer une méthode d'alerte.

Pour les baies de stockage gérées avec SANtricity System Manager, vous configurez les alertes à partir de la page alertes. Des notifications d'alerte peuvent être envoyées par e-mail, des traps SNMP ou des messages syslog. En outre, les alertes par e-mail peuvent être configurées à partir de l'assistant d'installation initiale.

Comment configurer les alertes SNMP ou syslog ?

En plus des alertes par e-mail, vous pouvez configurer les alertes pour qu'elles soient envoyées par des traps SNMP (simple Network Management Protocol) ou par des messages syslog.

Pour configurer des alertes SNMP ou syslog, accédez au **Paramètres › alertes**.

Pourquoi les horodatages sont-ils incohérents entre la baie et les alertes ?

Lorsque la matrice de stockage envoie des alertes, elle ne corrige pas le fuseau horaire du serveur ou de l'hôte cible qui reçoit les alertes. À la place, la matrice de stockage utilise l'heure locale (GMT) pour créer l'horodatage utilisé pour l'enregistrement d'alerte. Par conséquent, vous pouvez constater des incohérences entre les horodatages de la baie de stockage et le serveur ou l'hôte recevant une alerte.

Comme la matrice de stockage ne corrige pas le fuseau horaire lors de l'envoi d'alertes, l'horodatage des alertes est fonction du GMT-relatif, avec un décalage de fuseau horaire de zéro. Pour calculer un horodatage approprié à votre fuseau horaire local, vous devez déterminer votre décalage horaire par rapport à GMT, puis ajouter ou soustraire cette valeur de l'horodatage.