Gérer les alertes SNMP

SANtricity 11.7

NetApp
February 12, 2024

Sommaire

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 :

  - Accédez 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 :

  - Accédez 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:

- Accédez 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 baie 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.
   - **Location** — 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.