SNMP pour Firepower 1000/2100

Ce chapitre décrit comment configurer SNMP pour les périphériques Firepower 1000/2100.

- À propos de SNMP pour les périphériques Firepower 1000ou2100, à la page 1
- Activation de SNMP et configuration des propriétés de SNMP pour Firepower 1000/2100, à la page 2
- Création d'un déroutement SNMP pour Firepower 1000/2100, à la page 3
- Création d'un utilisateur SNMP pour Firepower 1000 ou 2100, à la page 4

À propos de SNMP pour les périphériques Firepower 1000ou2100

Le protocole SNMP (Simple Network Management Protocol) est un protocole de couche applicative qui fournit un format de message pour la communication entre les gestionnaires et les agents SNMP. SNMP fournit un cadre normalisé et un langage commun utilisés pour la surveillance et la gestion des périphériques dans un réseau.

Le cadre SNMP comprend trois parties :

- Un SNMP Manager (gestionnaire SNMP) : le système utilisé pour contrôler et surveiller les activités des périphériques réseau à l'aide de SNMP.
- Un agent SNMP : composant logiciel des châssis Firepower 1000ou2100 qui conserve les données pour le châssis Firepower et qui transmet les données, au besoin, au gestionnaire SNMP. Le châssis Firepower comprend l'agent et un ensemble de MIB. Pour activer l'agent SNMP et créer la relation entre le gestionnaire et l'agent, activez et configurez SNMP dans centre de gestion.
- Une base d'information gérée (MIB) : l'ensemble des objets gérés sur l'agent SNMP.

Les châssis Firepower 1000/2100prennent en charge SNMPv1,SNMPv2c et SNMPv3. Les protocoles SNMPv1 et SNMPv2C utilisent tous deux une forme de sécurité basée sur la communauté.

Activation de SNMP et configuration des propriétés de SNMP pour Firepower 1000/2100

Remarque Cette procédure s'applique uniquement aux périphériquesFirepower 1000/2100.

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 Cliquez sur **SNMP**.

Étape 3 Remplissez les champs comme suit :

Nom	Description
Case à cocher **État de l'administrateur**	Si SNMP est activé ou désactivé. Activez ce service uniquement si votre système comprend une intégration avec un serveur SNMP.
Champ **Port**	Port sur lequel le châssis Firepower communique avec l'hôte SNMP. Vous ne pouvez pas modifier le port par défaut.
Champ **Communauté**	Le nom de communauté SNMP v1 ou v2 ou le nom d'utilisateur SNMP v3 par défaut que le châssis Firepower inclut dans tous les messages de déroutement qu'il envoie à l'hôte SNMP. Saisissez une chaîne alphanumérique comprise entre 1 et 32 caractères. N'utilisez pas @ (at), \ (barre oblique inverse), « (guillemets), ? (point d'interrogation) ou un espace vide. La valeur par défaut est **`public`**. Notez que si le champ **Community** (communauté) est déjà défini, le texte à droite du champ vide indique **Set: Yes** (définir : oui). Si le champ **Community** (communauté) ne contient pas encore de valeur, le texte à droite du champ vide indique **Set: No** (Définir : non).
Champ **Nom de l'administrateur du système** :	La personne-ressource responsable de l'implémentation de SNMP. Saisissez une chaîne de 255 caractères maximum, comme une adresse de courriel ou un nom et un nom distinctif.
Champ **Emplacement**	Emplacement de l'hôte sur lequel l'agent SNMP (serveur) est exécuté. Saisissez une chaîne alphanumérique de 510 caractères maximum.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

créer des déroutements et des utilisateurs SNMP;

Création d'un déroutement SNMP pour Firepower 1000/2100

Remarque Cette procédure s'applique uniquement aux périphériquesFirepower 1000/2100.

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 Cliquez sur **SNMP**.

Étape 3 Dans la zone **SNMP Traps Configuration** (configuration des déroutements SNMP), cliquez sur **Add** (Ajouter).

Étape 4 Dans la boîte de dialogue **Configuration des déroutements SNMP**, remplissez les champs suivants :

Nom	Description
Champ**Nom d'hôte**	Le nom d'hôte ou l'adresse IP de l'hôte SNMP auquel le châssis Firepower doit envoyer le déroutement.
Champ **Communauté**	Le nom de communauté SNMP v1 ou v2 ou le nom d'utilisateur SNMPv3 que le châssis Firepower inclut lorsqu'il envoie le déroutement à l'hôte SNMP. Il doit s'agir de la communauté ou du nom d'utilisateur configuré pour le service SNMP. Saisissez une chaîne alphanumérique comprise entre 1 et 32 caractères. N'utilisez pas @ (at), \ (barre oblique inverse), « (guillemets), ? (point d'interrogation) ou un espace vide.
Champ **Port**	Port sur lequel le châssis Firepower communique avec l'hôte SNMP pour le déroutement. Saisissez un entier entre 1 et 65 535.
Champ**Version**	La version et le modèle du SNMP utilisés pour le déroutement. Voici les options offertes : • **V1** • **V2** • **V3**
Champ**Type**	Si vous sélectionnez **V2** ou **V3** pour la version, le type de déroutement à envoyer. Voici les options offertes : • **Trap** • **Information**

Nom	Description
Champ **Privilège**	Si vous sélectionnez **V3** pour la version, le privilège associé au déroutement. Voici les options offertes : • **Auth** : Authentification mais pas de chiffrement • **Noauth** : Pas d'authentification ni de chiffrement • **Priv** : Authentification et chiffrement

Étape 5 Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration du déroutement SNMP**.

Étape 6 Cliquez sur **Save** (enregistrer).

Création d'un utilisateur SNMP pour Firepower 1000 ou 2100

Remarque Cette procédure s'applique uniquement aux périphériquesFirepower 1000/2100.

Procédure

Étape 1 Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

Étape 2 Cliquez sur **SNMP**.

Étape 3 Dans la zone **SNMP Users Configuration** (Configuration des utilisateurs SNMP), cliquez sur **Add** (Ajouter).

Étape 4 Dans la boîte de dialogue **Configuration des utilisateurs SNMP**, remplissez les champs suivants :

Nom	Description
Champ **Nom d'utilisateur**	Le nom d'utilisateur affecté à l'utilisateur SNMP. Saisissez jusqu'à 32 lettres ou chiffres. Le nom doit commencer par une lettre et vous pouvez également spécifier un _ (trait de soulignement), . (point), @ (at) et - (trait d'union).
Champ **Type d'algorithme d'authentification**	Le type d'autorisation : **SHA**.
La case à cocher **Use AES-128 (utiliser AES-128**)	Si cette option est cochée, cet utilisateur utilise le chiffrement AES-128. **Remarque** SNMPv3 ne prend pas en charge DES. Si vous laissez la case AES-128 décochée, aucun chiffrement de confidentialité ne sera effectué et tout mot de passe de confidentialité configuré n'aura aucun effet.
Le champ **Mot de passe d'authentification**	Le mot de passe de l'utilisateur.

Nom	Description
Le champ **Confirmer**	Le mot de passe est répété pour confirmation.
Le champ **Mot de passe de chiffrement**	Le mot de passe de confidentialité de l'utilisateur.
Le champ **Confirmer**	Le mot de passe de confidentialité est à nouveau utilisé à des fins de confirmation.

Étape 5 Cliquez sur **OK** pour fermer la boîte de dialogue **Configuration de l'utilisateur SNMP**.

Étape 6 Cliquez sur **Save** (enregistrer).

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.