Configuration des déroutements SNMP IOS pris en charge

Table des matières

Introduction

Ce document décrit comment configurer les déroutements SNMP Cisco pris en charge.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

Il n'est pas souhaitable de configurer un appareil Cisco pour qu'il envoie toutes les alertes Trap possibles du protocole SNMP. Par exemple, si vous activez toutes les alertes Trap d'un serveur d'accès à distance comprenant 64 lignes d'accès, vous recevrez une alerte Trap pour chaque utilisateur qui se connecte et se déconnecte du serveur. Le nombre d'alertes s'accumulera rapidement. Le logiciel Cisco IOS® définit des groupes de déroutements que vous pouvez activer ou désactiver. Deux commandes de configuration générale permettent de configurer les alertes

Trap du protocole SNMP sur un appareil utilisant le logiciel Cisco IOS :

- **snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [notification-type]**
  Lancez snmp-server host global configuration pour spécifier le destinataire d'une opération de notification SNMP. Lancez **no** de cette commande pour supprimer l'hôte spécifié.

- **snmp-server enable traps [notification-type] [notification-option]**
  Lancez **snmp-server enable traps global configuration**pour permettre au routeur d'envoyer des déroutements SNMP. Lancez **no** de cette commande afin de désactiver les notifications SNMP.

Les types d'alertes Trap peuvent être définis dans les deux commandes. Vous devez émettre le **snmp-server host< /strong>** afin de définir les systèmes de gestion du réseau où les déroutements doivent être envoyés. Afin de limiter le nombre d'envois, vous devez préciser les types d'alertes que vous souhaitez recevoir. Émettre plusieurs **snmp-server enable traps** , une pour chaque type de déroutement que vous avez utilisé dans la **snmp host** erasecat4000_flash:.

> **Remarque** : pas tous [*notification-type*] sont prises en charge sur ces deux commandes. Exemple : [*notification-type*] x25 et teletype (tty) ne sont pas utilisés pour **snmp-server enable trap** x25 et les alertes tty sont activées par défaut.

Par exemple, émettez ces commandes pour qu'un périphérique du logiciel Cisco IOS signale uniquement la configuration, le protocole BGP (Border Gateway Protocol) et les déroutements tty au système de gestion de réseau 10.10.10.10 :

```
snmp-server host 10.10.10.10 public config bgp tty
snmp-server enable traps config
snmp-server enable traps bgp
```

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Informations générales

> **Remarque** : la version 12.1(3)T du logiciel Cisco IOS a été utilisée pour préparer ce document. Quand vous utilisez une version antérieure du logiciel Cisco IOS, toutes les options ne sont pas prises en charge. Lorsque vous utilisez une version logicielle de Cisco

IOS ultérieure à 12.1(3)T, des options supplémentaires [type de notification] peuvent être prises en charge. Vous pouvez trouver une liste à jour de tous les identifiants d'objet de déroutement (OID) pris en charge par le protocole de gestion de réseau simple (SNMP) du logiciel Cisco IOS dans ce document.

Les périphériques Cisco qui exécutent le logiciel Cisco IOS standard (routeurs, commutateurs ATM (Asynchronous Transfer Mode) et serveurs d'accès à distance) peuvent générer de nombreuses interruptions SNMP.

Commandes

Les snmp-server host Commande

Lancez **snmp-server host global configuration** pour spécifier le destinataire d'une opération de notification SNMP. Lancez **no** de cette commande pour supprimer l'hôte spécifié.

```
snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}]
community-string [udp-port port] [notification-type] no snmp-server host host [traps | informs]
```

Description de la syntaxe

host-addr	Le nom ou l'adresse Internet de l'hôte (le destinataire ciblé).
traps	(Facultatif) Envoie des alertes Trap du protocole SNMP à cet hôte. Il s'agit de la configura par défaut.
informs	(Facultatif) Envoie des alertes Inform du protocole SNMP à cet hôte.
version	(Facultatif) La version du protocole SNMP utilisée pour envoyer les alertes Trap. La versi est le modèle le plus sécurisé, car il permet le cryptage des paquets avec le **priv** mot clé. vous utilisez ce mot-clé, vous devez choisir l'une des options suivantes : • 1 — SNMPv1. Cette option n'est pas disponible avec les alertes Inform. • 2c — SNMPv2C • 3 — SNMPv3. Ces trois mots-clés facultatifs peuvent être placés après le mot-clé ve 3 : **auth**(Facultatif) Active l'authentification des paquets MD5 (Message Digest 5) et S (Secure Hash Algorithm).**noauth** (Par défaut) Niveau de sécurité noAuthNoPriv. Il s'ag la valeur par défaut lorsque le choix de mot-clé [auth | noauth | priv] n'est pas spécifi (Facultatif) Active le cryptage des paquets DES (Data Encryption Standard) (égalem appelé « confidentialité »).
community-string	Semblable au mot de passe, l'identifiant de communauté est transmis lors de la notificati Bien que vous puissiez définir cette chaîne avec la **snmp-server host** seule, Cisco vous recommande de définir cette chaîne avec la commande **snmp-server community** avant d'exéc la commande **snmp-server host** erasecat4000_flash:.
udp-port*port*	Le port du protocole UDP de l'hôte à utiliser. Il est défini par défaut à 162.
notification-type	(Facultatif) Le type de notification à envoyer à l'hôte. Si aucun type n'est spécifié, toutes notifications seront envoyées. Le type de notification peut correspondre à l'un ou à plusie des mots-clés suivants : • **aaa-server** : envoie des notifications AAA. • **bgp** — Envoie des notifications de changement d'état du protocole BGP (Border Gate Protocol). • **bstun**: envoie des notifications BSTUN (Block Serial Tunneling). • **calltracker**: envoie des notifications CallTracker.

- **config**: envoie des notifications de configuration.
- **dlsw**: envoie des notifications de commutation de liaison de données (DLSw).
- **ds0-busyout**: envoie des notifications ds0-busyout.
- **ds1-loopback**: envoie des notifications ds1-loopback.
- **dspu**: envoie des notifications DSPU (unité physique en aval).
- **dsp**: envoie des notifications de traitement numérique du signal (DSP).
- **entity**: envoie des notifications de modification de la base MIB (Entity Management Information Base).
- **envmon**: envoie des notifications de surveillance de l'environnement spécifiques à l'entreprise Cisco lorsqu'un seuil environnemental est dépassé.
- **frame-relay**: envoie des notifications Frame Relay.
- **hsrp**: envoie des notifications HSRP (Hot Standby Router Protocol).
- **isdn**: envoie des notifications RNIS (Réseau Numérique à Intégration de Services).
- **msdp**: envoie des notifications MSDP (Multicast Source Discovery Protocol).
- **llc2**: envoie des notifications LLC2 (Logical Link Control, type 2).
- **repeater**: envoie des notifications de répéteur standard (concentrateur).
- **rsrb**: envoie des notifications RSRB (Source-Route Bridging) à distance.
- **rsvp**: envoie des notifications RSVP (Resource Reservation Protocol).
- **rtr**: envoie des notifications RTR (SA Agent).
- **sdlc**: envoie des notifications SDLC (Synchronous Data Link Control).
- **snmp**: envoie des notifications SNMP (Simple Network Management Protocol) (comm défini dans la RFC 1157).
- **stun**: envoie des notifications STUN (Serial Tunnel).
- **syslog**: envoie des notifications de message d'erreur (MIB Cisco Syslog). Spécifiez le niveau des messages à envoyer avec le**logging history level**erasecat4000_flash:.
- **tty**: envoie des notifications spécifiques à l'entreprise Cisco lorsqu'une connexion TC (Transmission Control Protocol) se ferme.
- **voice**: envoie des notifications vocales.
- **x25**: envoie des notifications d'événements X.25.
- **xgcp**: envoie des notifications XGCP (External Media Gateway Control Protocol).

Valeurs par défaut

Les **snmp-server host** est désactivée par défaut. Aucune notification n’est envoyée.

Si vous entrez cette commande sans mot-clé, la valeur par défaut fera en sorte d’envoyer tous les types d’alertes Trap à l’hôte.

Aucune alerte Inform n’est envoyée à cet hôte. Si non **version** est présent, la valeur par défaut est la version 1. Les **no snmp-server host** sans mot-clé désactive les déroutements, mais pas les informations, vers l’hôte. Lancez **no snmp-server host informs** pour désactiver les informations.

> **Remarque** : si le *community-string* n'est pas défini avec la **snmp-server community** avant d'utiliser cette commande, la forme par défaut du **snmp-server community** est automatiquement insérée dans la configuration. Le mot de passe (*community-string*) utilisé pour cette configuration automatique du **snmp-server community** est identique à celui spécifié dans la **snmp-server host** erasecat4000_flash:. Voici le fonctionnement par défaut du logiciel Cisco IOS, version 12.0(3) et versions ultérieures.

Modes de commande

Configuration générale – historique de commande

Modification de la version du logiciel Cisco IOS	–
10.0	Commande ajoutée.
12.0(3)T	Ces mots-clés ont été ajoutés : • **version 3 [auth | noauth | priv]** • **hsrp**

Directives d’utilisation

Les notifications SNMP peuvent être envoyées sous forme d’alertes « Trap » ou « Inform ». Les alertes Trap sont moins fiables, car le récepteur n’envoie pas de message de confirmation lorsqu’il reçoit cette alerte. L’émetteur ne peut pas savoir si les alertes Trap ont bien été reçues. Par contre, une entité SNMP qui reçoit une alerte Inform confirme la réception du message en envoyant une réponse SNMP comprenant l’unité de données de protocole (PDU). Si l’émetteur ne reçoit aucune réponse, l’alerte Inform peut être envoyée de nouveau. C’est pourquoi les alertes Inform sont plus susceptibles d’atteindre leurs cibles.

Cependant, ce type d’alerte demande plus de ressources dans l’agent et dans le réseau. Contrairement à une alerte Trap, laquelle est supprimée après son envoi, une alerte Inform est enregistrée en mémoire jusqu’au retour d’une réponse ou jusqu’à ce que la demande expire. Les alertes Trap sont envoyées une seule fois, tandis que les alertes Inform peuvent être envoyées à plusieurs reprises. Les nouvelles tentatives augmentent le trafic et contribuent à un temps système plus élevé sur le réseau.

Si vous ne saisissez pas de **snmp-server host** , aucune notification n'est envoyée. Afin de configurer le routeur pour envoyer des notifications SNMP, vous devez entrer au moins une **snmp-server host** erasecat4000_flash:. Si vous entrez la commande sans mot-clé, tous les types d’alertes Trap seront activés pour l’hôte.

Afin d'activer plusieurs hôtes, vous devez émettre un **snmp-server host** pour chaque hôte. Vous pouvez préciser plusieurs types de notification dans la commande pour chaque hôte.

Lorsque plusieurs **snmp-server host** sont fournies pour le même hôte et le même type de notification (trap ou inform), chaque commande remplace la commande précédente. Seulement le dernier **snmp-server host** est prise en compte. Par exemple, si vous saisissez un snmp-server host inform pour un hôte, puis entrez une autre commande **snmp-server host inform** pour le même hôte, la deuxième commande remplace la première.

Les **snmp-server host** est utilisée conjointement avec la commande **snmp-server enable** erasecat4000_flash:. Lancez **snmp-server enable** afin de spécifier quelles notifications SNMP sont envoyées globalement. Pour qu'un hôte reçoive la plupart des notifications, au moins une **snmp-server enable** et la commande **snmp-server host** pour cet hôte doit être activée.

Toutefois, certains types de notification ne peuvent pas être contrôlés avec l' **snmp-server enable** erasecat4000_flash:. Par exemple, certains types de notification sont activés en tout temps. D’autres types de notification sont activés par une autre commande. Par exemple, le `linkUpDown` les notifications sont contrôlées par le **snmp trap link-status** erasecat4000_flash:. Ces types de notification ne nécessitent pas de **snmp-server enable** erasecat4000_flash:.

Les types de notification disponibles varient selon le type de routeur et selon les fonctionnalités du logiciel Cisco IOS que ce dernier prend en charge. Par exemple, le **envmon** notification-type n'est disponible que si le moniteur d'environnement fait partie du système.

Configurer les informations

Suivez les étapes ci-dessous pour autoriser l’envoi d’alertes Inform :

1. Configurez un identifiant d’appareil à distance.
2. Configurez un utilisateur distant.
3. Configurez un groupe sur un appareil à distance.
4. Activez les alertes Trap sur l’appareil à distance.
5. Activez le gestionnaire SNMP.

Exemples

Si vous voulez configurer un identifiant de communauté SNMP unique pour l’envoi d’alertes Trap, mais que vous souhaitez empêcher l’accès par interrogation SNMP pour cet identifiant, la configuration doit comporter une liste d’accès. Dans cet exemple, l’identifiant de communauté se nomme « comaccess » et la liste d’accès indique le nombre 10 :

```
snmp-server community comaccess ro 10
snmp-server host 172.20.2.160 comaccess
access-list 10 deny any
```

Dans cet exemple, les alertes Trap sont envoyées à l’hôte nommé myhost.cisco.com. L’identifiant de communauté est défini comme « comaccess » :

```
snmp-server enable traps
snmp-server host myhost.cisco.com comaccess snmp
```

Dans cet exemple, les alertes Trap relatives au protocole SNMP et à la surveillance des environnements Cisco pour entreprises sont envoyées à l’adresse 172.30.2.160 :

```
snmp-server enable traps
snmp-server host 172.30.2.160 public snmp envmon
```

Dans cet exemple, le routeur envoie toutes les alertes Trap à l’hôte myhost.cisco.com et l’identifiant de communauté est public :

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

Dans cet exemple, aucune alerte Trap n’est envoyée à aucun hôte. Les alertes Trap BGP sont activées pour tous les hôtes, mais seules les alertes Trap ISDN sont activées pour l’envoi à un hôte.

```
snmp-server enable traps bgp
snmp-server host bob public isdn
```

Cet exemple permet au routeur d'envoyer toutes les requêtes d'information à l'hôte myhost.cisco.com avec la chaîne de communauté public :

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version
```

Dans cet exemple, les alertes HSRP SNMPv2c sont envoyées à l'hôte nommé myhost.cisco.com. L'identifiant de communauté est public.

```
snmp-server enable traps
snmp-server host myhost.cisco.com traps version 2c public hsrp
```

Les snmp-server enable traps Commande

Utilisez **snmp-server enable traps** commande de configuration globale pour permettre au routeur d'envoyer des déroutements SNMP. Utilisez **no** de cette commande pour désactiver les notifications SNMP.

```
snmp-server enable traps [notification-type] [notification-option]

no snmp-server enable traps [notification-type] [notification-option]
```

Description de la syntaxe

notification-type	(Facultatif) Le type de notification à activer. Si aucun type n'est spécifié, toutes les notifications sont envoyées (y compris les **envmon** et **repeater** notifications). Le type de notification peut correspondre à l'un des mots-clés suivants : • **aaa-server**: envoie des notifications au serveur AAA. Ce mot-clé a été ajouté dans la version 12.1(3)T du logiciel Cisco IOS pour les plateformes Cisco AS5300 et AS58 seulement. Ceci provient de la base de données MIB CISCO-AAA-SERVER et les notifications sont les suivantes : entreprise 1.3.6.1.4.1.9.10.56.2 1 casServerStateChange • **bgp** — Envoie des notifications de changement d'état du protocole BGP (Border Gateway Protocol). Ceci provient de la MIB-BGP4 et les notifications sont : entrepr 1.3.6.1.2.1.15.7 1 bgpEstablished 2 bgpBackwardTransition • **calltracker** — Envoie une notification chaque fois qu'une nouvelle entrée d'appel acti créée dans cctActiveTable ou qu'une nouvelle entrée d'appel d'historique est créée dans cctHistoryTable. Il s'agit de la MIB CISCO-CALL-TRACKER et les notification sont : enterprise 1.3.6.1.4.1.9.9.163.2 1 cctCallSetupNotification 2 cctCallTerminateNotification • **config** : envoie des notifications de configuration. Ceci provient de la base de donné MIB CISCO-CONFIG-MAN et les notifications sont : enterprise 1.3.6.1.4.1.9.9.43.2 ciscoConfigManEvent • **dial** : envoie une notification chaque fois qu'un appel réussi est supprimé, qu'une

tentative d'appel ayant échoué est considérée comme ayant échoué, ou qu'un mes
d'établissement d'appel est reçu ou envoyé. Ceci provient de la MIB DIAL-CONTR
les notifications sont : enterprise 1.3.6.1.2.1.10.21.2 1 dialCtlPeerCallInformation 2
dialCtlPeerCallSetup

- **dlsw** : envoie des notifications à partir des agents DLSw lorsque le **dlsw** est utilisé, vo
pouvez spécifier *anotification*-optionvalue. Ceci provient de la base de données MI
CISCO-DLSW et les notifications sont les suivantes : entreprise 1.3.6.1.4.1.9.10.9.
ciscoDlswTrapTConnPartnerReject 2 ciscoDlswTrapTConnProtViolation 3
ciscoDlswTrapTConnUp 4 ciscoDlswTrapTConnDown 5 ciscoDlswTrapCircuitUp 6
ciscoDlswTrap CircuitDown
- **ds0-busyout**: envoie une notification chaque fois que l'état de la ligne occupée d'une
interface DS0 change. Ce mot-clé a été ajouté dans la version 12.1(3)T du logiciel
Cisco IOS pour la plateforme Cisco AS5300 seulement. Ceci provient de la base d
données MIB CISCO-POP-MGMT et la notification est : enterprise 1.3.6.1.4.1.9.10
1 cpmDS0BusyoutNotification
- **ds1-loopback**: envoie une notification chaque fois que l'interface DS1 passe en mode
bouclé. Ce mot-clé a été ajouté dans la version 12.1(3)T du logiciel Cisco IOS pou
plateforme Cisco AS5300 seulement. Ceci provient de la base de données MIB CI
POP-MGMT et la notification est : enterprise 1.3.6.1.4.1.9.10.19.2 2
cpmDS1LoopbackNotification
- **dspu**: envoie une notification chaque fois que l'état de fonctionnement de l'unité phy
(PU) ou de l'unité logique (LU) change ou qu'un échec d'activation est détecté. Ce
provient de la base de données MIB CISCO-DSPU et les notifications sont les suiv
: entreprise 1.3.6.1.4.1.9.9.24.1.4.4 1newdspuPuStateChangeTrap 2
newdspuPuActivationFailureTrap entreprise 1.3.6.1.4.1.9.9.24.1.5.3 1
newdspuLuStateChangeTrap 2 dspuLuActivationFailureTrap
- **dsp**: envoie une notification chaque fois que la carte DSP est activée ou désactivée
Ceci provient de la base de données MIB CISCO-DSP-MGMT et la notification est
enterprise 1.3.6.1.4.1.9.9.86.2.1 cdspMIBCardStateNotification
- **entity**: envoie des notifications de modification de MIB d'entité. Ceci provient de la M
ENTITY, et les notifications sont : enterprise 1.3.6.1.2.1.47.2.1 entConfigChange
- **envmon**: envoie des notifications de surveillance environnementale spécifiques à
l'entreprise Cisco lorsqu'un seuil environnemental est dépassé. Quand le**envmon**est
utilisé, vous pouvez spécifier *anotification*-optionvalue. Ces notifications proviennen
la base MIB CISCO-ENVMON et sont les suivantes : entreprise 1.3.6.1.4.1.9.9.13.
ciscoEnvMonShutdownNotification 2 ciscoEnvMonVoltageNotification 3
ciscoEnvMonTemperatureNotification 4 ciscoEnvMonFanNotification 5
ciscoEnvMonRedundantSupplyNotification
- **frame-relay**: envoie des notifications Frame Relay. Il provient de la base de données
RFC1315-MIB et les notifications sont les suivantes : enterprise 1.3.6.1.2.1.10.32.1
frDLCIStatusChange
- **hsrp**: envoie des notifications HSRP (Hot Standby Router Protocol). Cette fonctionn
est offerte dans la version 12.0(3)T du logiciel Cisco IOS et dans les versions
ultérieures. Ceci provient de la MIB CISCO-HSRP, et les notifications sont : enterp
1.3.6.1.4.1.9.9.106.2.1 cHsrpStateChange
- **isdn**: envoie des notifications RNIS. Quand le**isdn**est utilisé, vous pouvez spécifier
anotification-optionvalue. Ces notifications proviennent de la base de données MIB

CISCO-ISDN et sont les suivantes : enterprise 1.3.6.1.4.1.9.9.26.2 1 demandNbrCallInformation 2 demandNbrCallDetails 3 demandNbrLayer2Change [en charge depuis la version du logiciel Cisco IOS 12.1(1)T] 4 demandNbrCNANotification [prise en charge depuis la version du logiciel Cisco IO 12.1(5)T]. Elles proviennent de la base de données MIB CISCO-ISDNU-IF et sont suivantes : enterprise 1.3.6.1.1. 2.1.9.9.18.2.1 ciuIfLoopStatusNotification

- **msdp**: envoie des notifications MSDP (Multicast Source Discovery Protocol). Ceci provient de la base de données MIB MSDP et les notifications sont les suivantes : entreprise 1.3.6.1.3.92.1.1.7 1 msdpEstablished 2 msdpBackwardTransition
- **repeater**: envoie un concentrateur Ethernet**repeater**notifications. Lorsque le mot clé repeater est sélectionné, vous pouvez spécifier un *notification-option* valeur. Ceci provi de la base de données MIB CISCO-REPEATER et les notifications sont les suivan enterprise 1.3.6.1.4.1.9.9.22.3 1 ciscoRptrIllegalSrcAddrTrap
- **rsvp**: envoie des notifications RSVP (Resource Reservation Protocol). Cette fonctionnalité est offerte depuis la version 12.0(2)T du logiciel Cisco IOS. Ceci prov de la base MIB RSVP et les notifications sont : enterprise 1.3.6.1.3.71.2 1 newFlow lostFlow
- **rtr**: envoie des notifications RTR (Service Assurance Agent). Il provient de la base données MIB CISCO-RTMON et les notifications sont les suivantes : entreprise 1.3.6.1.4.1.9.9.42.2 1 rttMonConnectionChangeNotification 2 rttMonTimeoutNotific 3 rttMonThresholdNotification 4 rttMonVerifyErrorNotification
- **snmp**: envoie des notifications SNMP (Simple Network Management Protocol). Qua le**snmp**est utilisé, vous pouvez spécifier une valeur notification-option. Ceci provient CISCO-GENERAL-TRAPS et les notifications sont les suivantes : entreprise 1.3.6.1.2.1.11 0 coldStart 2 linkDown 3 linkUp 4 authenticationFailure 5 egpNeighborLoss entreprise 1.3.6.1.4.1.9 0 reload **Remarque** : ce déroutement est contrôlé par le type de notification « tty » : 1 tcpConnectionClose
- **syslog**: envoie des notifications de message d'erreur (MIB Cisco Syslog). Spécifiez niveau des messages à envoyer avec le**logging history level**erasecat4000_flash:. Ceci provient de la base de données MIB CISCO-SYSLOG et les notifications sont les suivantes : enterprise 1.3.6.1.4.1.9.9.41.2.1 clogMessageGenerated
- **voice**: envoie des notifications vocales de mauvaise qualité. Ceci provient de CISC VOICE-DIAL-CONTROL-MIBSMI et les notifications sont les suivantes : enterprise 1.3.6.1.4.1.9.9.63.2 1 cvdcPoorQoVNotification
- **xgcp**: envoie des notifications XGCP (External Media Gateway Control Protocol). C provient de XGCP-MOB et les notifications sont : enterprise 1.3.6.1.3.90.2 1 xgcpUpDownNotification

notification-option (Facultatif)

- **dlsw [circuit | tconn]**—Quand le**dlsw**est utilisé, vous pouvez spécifier le type de notifica spécifique que vous souhaitez activer ou désactiver. Si aucun mot-clé n'est utilisé, les types de notification DLSw seront activés. L'option peut correspondre à un ou à plusieurs des mots-clés suivants : **circuit**: active les déroutements de circuit DLSw.**t** active les déroutements de connexion de transport homologue DLSw.
- **envmon [voltage | shutdown | supply | fan | temperature]**—Quand le**envmon**est utilisé, vous pou activer un type de notification d'environnement spécifique ou accepter tous les type notification du système de surveillance de l'environnement. Si aucune option n'est spécifiée, toutes les notifications relatives à l'environnement seront activées. L'opti peut correspondre à un ou à plusieurs des mots-clés

suivants :**voltage**,**shutdown**,**supply**,**fan**,et**temperature**.

- **isdn [call-information | isdn u-interface | chan-not-avail | layer2]**—Quand le**isdn**est utilisé, vous pouvez spécifier le mot-clé**call-information**pour activer une notification d'informations d'appel RNIS SNMP pour le sous-système MIB RNIS, ou vous pouvez spécifier le**i interface**pour activer une notification d'interface SNMP RNIS U pour le sous-système d'interface RNIS U.
- **repeater [health | reset]**—Quand le **repeater** est utilisé, vous pouvez spécifier l'option de répéteur. Si aucune option n'est spécifiée, toutes les notifications relatives au répé seront activées. L'option peut contenir un ou plusieurs des mots clés suivants : health—Enables Internet Engineering Task Force (IETF) Repeater Hub MIB (RFC health notification. reset—Enables IETF Repeater Hub MIB (RFC 1516) reset notification. **health**— Active la notification d'état de fonctionnement de la base MIB d répéteur IETF (Internet Engineering Task Force) (RFC 1516).**reset**: active la notifica de réinitialisation du MIB du répéteur-concentrateur IETF (RFC 1516).
- **snmp [authentication | linkup | linkdown | coldstart]**mots-clés **linkup | linkdown | coldstart** ajouté d la version du logiciel Cisco IOS 12.1(3)T. — Lorsque le **snmp** est utilisé, vous pouve spécifier le type de notification spécifique que vous souhaitez activer ou désactiver aucun mot-clé n'est utilisé, tous les types de notification SNMP seront activés (ou désactivés, si la version « no » est utilisée). Les types de notification possibles son suivants : **authentication**: contrôle la distribution des notifications d'échec d'authentific SNMP. Une alerte Trap « authenticationFailure(4) » signifie que l'entité du protocol d'envoi est le destinataire d'un message du protocole, lequel n'est pas authentifié correctement.**linkup**: contrôle l'envoi des notifications de liaison SNMP. Une alerte T « linkUp(3) » signifie que l'entité du protocole d'envoi détecte que l'un des liens de communication se trouvant dans la configuration de l'agent a établi une liaison ave succès.**linkdown**: contrôle le mode d'envoi des notifications de liaison SNMP. Une al Trap « linkDown(2) » signifie que l'entité du protocole d'envoi détecte que l'un des de communication se trouvant dans la configuration de l'agent n'a pas pu établir la liaison.**coldstart**: contrôle l'envoi des notifications SNMP de démarrage à froid. Une interruption coldStart(0) signifie que l'entité de protocole émettrice est réinitialisée sorte que la configuration de l'agent ou l'implémentation de l'entité de protocole pe être modifiée.

Valeurs par défaut

Les notifications SNMP sont désactivées.

Si vous entrez cette commande sans mot-clé « notification-type », la valeur par défaut fera en sorte d'activer tous les types de notifications contrôlés par cette commande.

Modes de commande

Configuration générale – historique de commande

Modification de la version du logiciel Cisco IOS	–
11.1	La commande suivante a été ajoutée.

12.0(2)T	Les**rsvp**a été ajouté.
12.0(3)T	Les **hsrp** a été ajouté.
12.1(3)T	Ces mots-clés ont été ajoutés à la **snmp-server enable traps snmp** forme de ce commande : • **linkup** • **linkdown** • **coldstart** Ces mots-clés relatifs au type de notification ont été ajoutés pour la plateforme Cisco AS5300 seulement : • **ds0-busyout** • **isdn chan-not-avail** • **modem-health** • **ds1-loopback** Ce mot-clé relatif au type de notification a été ajouté pour les plateforme Cisco AS5300 et AS5800 seulement : • **aaa-server**

Directives d'utilisation

Les **snmp-server enable traps snmp [linkup] [linkdown]** de cette commande remplace la commande **snmp trap link-status interface** commande du mode de configuration.

Les **no** forme de la **snmp-server enable traps** est utile pour désactiver les notifications qui génèrent une grande quantité de bruit inutile sur votre réseau.

Les notifications SNMP peuvent être envoyées sous forme d'alertes « Trap » ou « Inform ». Cette commande active à la fois les alertes Trap et Inform pour les types de notifications indiqués.

Si vous ne saisissez pas de **snmp-server enable traps** , aucune notification contrôlée par cette commande n'est envoyée. Afin de configurer le routeur pour envoyer ces notifications SNMP, vous devez entrer au moins une **snmp-server enable traps** erasecat4000_flash:. Si vous entrez la commande sans mot-clé, tous les types de notification seront activés. Si vous entrez la commande avec un mot-clé, seul le type de notification associé à ce mot-clé est activé. Afin d'activer plusieurs types de notifications, vous devez émettre un **snmp-server enable traps** pour chaque type de notification et chaque option de notification.

Les **snmp-server enable traps** est utilisée conjointement avec la commande **snmp-server host** erasecat4000_flash:. Lancez **snmp-server host** pour spécifier le ou les hôtes qui reçoivent des notifications SNMP. Pour envoyer des notifications, vous devez configurer au moins un **snmp-server host** erasecat4000_flash:.

Pour qu'un hôte reçoive une notification contrôlée par cette commande, les deux **snmp-server enable traps** et la commande **snmp-server host** pour cet hôte doit être activée. Si le type de notification n'est pas contrôlé par cette commande, seule la **snmp-server host** doit être activée.

Les types de notification utilisés dans cette commande sont tous associés à un objet MIB qui permet leur activation ou leur désactivation (par exemple, les alertes Trap « HSRP » sont définies par le MIB HSRP, les alertes Trap « repeater » sont définies par le MIB du répéteur [concentrateur] et ainsi de suite). Tous les types de notification disponibles dans le **snmp-server host** ont des objets **notificationEnable MIB**, de sorte que certains d'entre eux ne peuvent pas être contrôlés avec la commande **snmp-server enable** erasecat4000_flash:.

Informations connexes

- Assistance technique et téléchargements Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.