MIB SNMP

Ce chapitre décrit comment configurer le protocole simple de gestion de réseau (SNMP) pour superviser l'ASA.

À propos de SNMP

SNMP est un protocole de couche d'application qui facilite l'échange d'informations de gestion entre les appareils réseau et fait partie de la suite de protocoles TCP /IP. L'ASA prend en charge la surveillance du réseau à l'aide des versions SNMP 1, 2c et 3 de SNMP, et prend en charge l'utilisation des trois versions simultanément. L'agent SNMP qui s'exécute sur l'interface ASA vous permet de surveiller les périphériques réseau à l'aide de systèmes de gestion par réseau (Network Management Systems ou NMS), comme HP OpenView. L'ASA prend en charge l'accès SNMP en lecture seule par l'émission d'une requête GET. L'accès en écriture SNMP n'est pas autorisé, vous ne pouvez donc pas effectuer de modifications avec SNMP. En outre, la requête SNMP SET n'est pas prise en charge.

Vous pouvez configurer la ASA pour envoyer des déroutements, qui sont des messages non sollicités du périphérique géré vers le poste de gestion pour certains événements (notifications d'événement) à un système de gestion de réseau, ou vous pouvez utiliser le système de gestion de réseau pour parcourir les bases d'information de gestion (MIB) sur le périphériques de sécurité. Les MIB sont un ensemble de définitions, et les ASA gèrent une base de données de valeurs pour chaque définition. Parcourir une MIB signifie émettre une série de demandes GET-NEXT ou GET-BULK de l'arborescence MIB à partir du système NMS pour déterminer les valeurs.

Remarque Avec des charges de travail intensives, le déploiement de plus de 10 NMS peut avoir une incidence sur les performances de l'appareil. Pour assurer la stabilité et la réactivité de l'appareil, nous vous conseillons d'utiliser avec prudence NMS pour effectuer des interrogations SNMP et gérer le trafic d'interruption.

Les ASA possèdent un agent SNMP qui informe les stations de gestion désignées si des événements prédéfinis nécessitent une notification, par exemple, lorsqu'une liaison du réseau monte ou tombe en panne. La notification

qu'il envoie comprend un OID SNMP, qui s'identifie aux stations de gestion. L'agent ASA répond également lorsqu'une station de gestion demande des renseignements.

Terminologie SNMP

Le tableau suivant répertorie les termes couramment utilisés avec SNMP.

Tableau 1 : Terminologie SNMP

Terme	Description
Agent	Le serveur SNMP exécuté sur ASA. L'agent SNMP présente les caractéristiques suivantes : • Répond aux demandes d'informations et d'actions de le poste de gestion de réseau. • Contrôle l'accès à sa base d'information de gestion, l'ensemble d'objets que le gestionnaire SNMP peut afficher ou modifier. • N'autorise pas les opérations SET.
Navigation	Surveille l'intégrité d'un périphérique à partir de le poste de gestion de réseau en interrogeant les informations requises de l'agent SNMP sur le périphérique. Cette activité peut comprendre l'émission d'une série de demandes GET-NEXT ou GET-BULK de l'arborescence MIB à partir de le poste de gestion de réseau afin de déterminer les valeurs.
Bases d'informations de gestion (MIB)	Structures de données normalisées pour la collecte d'informations sur les paquets, les connexions, les tampons, les basculements, etc. Les MIB sont définies par le produit, les protocoles et les normes matérielles utilisés par la plupart des périphériques réseau. Les stations de gestion de réseau SNMP peuvent parcourir les MIB et demander l'envoi de données ou d'événements précis au fur et à mesure qu'ils se produisent.
Postes de gestion de réseau (NSM, Network Management Station)	Les ordinateurs ou postes de travail configurés pour superviser les événements SNMP et gérer les périphériques, tels que l'ASA
Identifiant d'objet (OID)	Le système qui identifie un appareil auprès de son système de gestion système et indique aux utilisateurs la source des renseignements surveillés et affichés.
Trap	Événements prédéfinis qui génèrent un message de l'agent SNMP au système NMS. Les événements comprennent des conditions d'alarme telles qu'un démarrage, un retrait, un démarrage à froid, un démarrage à chaud, une authentification ou des messages syslog.

MIB et déroutements

Les MIB sont standard ou spécifiques à l'entreprise. Les MIB standard sont créées par l'IETF et documentées dans diverses RFC. Un déroutement signale des événements importants se produisant sur un périphérique réseau, le plus souvent des erreurs ou des défaillances. Les déroutements SNMP sont définies dans les MIB standard ou spécifiques à l'entreprise. Les déroutements standard sont créés par l'IETF et documentés dans diverses normes RFC. Les déroutements de SNMP sont compilés dans le logiciel ASA.

Si nécessaire, vous pouvez également télécharger des RFC, des MIB standard et des déroutements standard à partir des emplacements suivants :

http://www.ietf.org/

Parcourez la liste complète des MIB, des déroutements et des OID de Cisco à partir de l'emplacement suivant :

https://github.com/cisco/cisco-mibs/blob/main/supportlists/asa/asa-supportlist.html

Téléchargez également les OID de Cisco par FTP à partir de l'emplacement suivant :

https://github.com/cisco/cisco-mibs/tree/main/oid

Remarque Dans les versions logicielles 7.2(1), 8.0(2) et ultérieures, les renseignements sur l'interface accessibles par SNMP sont actualisés toutes les 5 secondes. Par conséquent, nous vous conseillons d'attendre au moins 5 secondes entre des interrogations consécutives.

Tous les OID des MIB ne sont pas pris en charge. Pour obtenir une liste des MIB et OID SNMP pris en charge pour un ASA en particulier, utilisez la commande suivante :

```
ciscoasa(config)# show snmp-server oidlist
```

Remarque Bien que le mot clé **oidlist** n'apparaisse pas dans la liste d'options de l'aide sur la commande **show snmp-server**, il est disponible. Cependant, cette commande est destinée à l'utilisation de Cisco TAC uniquement. Communiquez avec le centre d'assistance technique (TAC) de Cisco avant d'utiliser cette commande.

Voici un exemple de sortie de la commande **show snmp-server oidlist** :

```
ciscoasa(config)# show snmp-server oidlist
[0]     1.3.6.1.2.1.1.1.        sysDescr
[1]     1.3.6.1.2.1.1.2.        sysObjectID
[2]     1.3.6.1.2.1.1.3.        sysUpTime
[3]     1.3.6.1.2.1.1.4.        sysContact
[4]     1.3.6.1.2.1.1.5.        sysName
[5]     1.3.6.1.2.1.1.6.        sysLocation
[6]     1.3.6.1.2.1.1.7.        sysServices
[7]     1.3.6.1.2.1.2.1.        ifNumber
[8]     1.3.6.1.2.1.2.2.1.1.    ifIndex
[9]     1.3.6.1.2.1.2.2.1.2.    ifDescr
[10]    1.3.6.1.2.1.2.2.1.3.    ifType
[11]    1.3.6.1.2.1.2.2.1.4.    ifMtu
[12]    1.3.6.1.2.1.2.2.1.5.    ifSpeed
[13]    1.3.6.1.2.1.2.2.1.6.    ifPhysAddress
[14]    1.3.6.1.2.1.2.2.1.7.    ifAdminStatus
[15]    1.3.6.1.2.1.2.2.1.8.    ifOperStatus
[16]    1.3.6.1.2.1.2.2.1.9.    ifLastChange
[17]    1.3.6.1.2.1.2.2.1.10.   ifInOctets
[18]    1.3.6.1.2.1.2.2.1.11.   ifInUcastPkts
[19]    1.3.6.1.2.1.2.2.1.12.   ifInNUcastPkts
[20]    1.3.6.1.2.1.2.2.1.13.   ifInDiscards
[21]    1.3.6.1.2.1.2.2.1.14.   ifInErrors
[22]    1.3.6.1.2.1.2.2.1.16.   ifOutOctets
[23]    1.3.6.1.2.1.2.2.1.17.   ifOutUcastPkts
[24]    1.3.6.1.2.1.2.2.1.18.   ifOutNUcastPkts
[25]    1.3.6.1.2.1.2.2.1.19.   ifOutDiscards
```

```
[26]    1.3.6.1.2.1.2.2.1.20.   ifOutErrors
[27]    1.3.6.1.2.1.2.2.1.21.   ifOutQLen
[28]    1.3.6.1.2.1.2.2.1.22.   ifSpecific
[29]    1.3.6.1.2.1.4.1.        ipForwarding
[30]    1.3.6.1.2.1.4.20.1.1.   ipAdEntAddr
[31]    1.3.6.1.2.1.4.20.1.2.   ipAdEntIfIndex
[32]    1.3.6.1.2.1.4.20.1.3.   ipAdEntNetMask
[33]    1.3.6.1.2.1.4.20.1.4.   ipAdEntBcastAddr
[34]    1.3.6.1.2.1.4.20.1.5.   ipAdEntReasmMaxSize
[35]    1.3.6.1.2.1.11.1.       snmpInPkts
[36]    1.3.6.1.2.1.11.2.       snmpOutPkts
[37]    1.3.6.1.2.1.11.3.       snmpInBadVersions
[38]    1.3.6.1.2.1.11.4.       snmpInBadCommunityNames
[39]    1.3.6.1.2.1.11.5.       snmpInBadCommunityUses
[40]    1.3.6.1.2.1.11.6.       snmpInASNParseErrs
[41]    1.3.6.1.2.1.11.8.       snmpInTooBigs
[42]    1.3.6.1.2.1.11.9.       snmpInNoSuchNames
[43]    1.3.6.1.2.1.11.10.      snmpInBadValues
[44]    1.3.6.1.2.1.11.11.      snmpInReadOnlys
[45]    1.3.6.1.2.1.11.12.      snmpInGenErrs
[46]    1.3.6.1.2.1.11.13.      snmpInTotalReqVars
[47]    1.3.6.1.2.1.11.14.      snmpInTotalSetVars
[48]    1.3.6.1.2.1.11.15.      snmpInGetRequests
[49]    1.3.6.1.2.1.11.16.      snmpInGetNexts
[50]    1.3.6.1.2.1.11.17.      snmpInSetRequests
[51]    1.3.6.1.2.1.11.18.      snmpInGetResponses
[52]    1.3.6.1.2.1.11.19.      snmpInTraps
[53]    1.3.6.1.2.1.11.20.      snmpOutTooBigs
[54]    1.3.6.1.2.1.11.21.      snmpOutNoSuchNames
[55]    1.3.6.1.2.1.11.22.      snmpOutBadValues
[56]    1.3.6.1.2.1.11.24.      snmpOutGenErrs
[57]    1.3.6.1.2.1.11.25.      snmpOutGetRequests
[58]    1.3.6.1.2.1.11.26.      snmpOutGetNexts
[59]    1.3.6.1.2.1.11.27.      snmpOutSetRequests
[60]    1.3.6.1.2.1.11.28.      snmpOutGetResponses
[61]    1.3.6.1.2.1.11.29.      snmpOutTraps
[62]    1.3.6.1.2.1.11.30.      snmpEnableAuthenTraps
[63]    1.3.6.1.2.1.11.31.      snmpSilentDrops
[64]    1.3.6.1.2.1.11.32.      snmpProxyDrops
[65]    1.3.6.1.2.1.31.1.1.1.1. ifName
[66]    1.3.6.1.2.1.31.1.1.1.2. ifInMulticastPkts
[67]    1.3.6.1.2.1.31.1.1.1.3. ifInBroadcastPkts
[68]    1.3.6.1.2.1.31.1.1.1.4. ifOutMulticastPkts
[69]    1.3.6.1.2.1.31.1.1.1.5. ifOutBroadcastPkts
[70]    1.3.6.1.2.1.31.1.1.1.6. ifHCInOctets
--More--
```

Identifiants d'objet SNMP

Chaque produit Cisco de niveau système a un identifiant d'objet SNMP (OID) à utiliser comme sysObjectID MIB-II. Les commandes CISCO-PRODUCTS-MIB et CISCO-ENTITY-VENDORTYPE-OID-MIB comprennent les OID qui peuvent être signalés dans l'objet sysObjectID de SNMPv2-MIB, Entity Sensor MIB et Entity Sensor Threshold Ext MIB. Vous pouvez utiliser cette valeur pour identifier le type de modèle. Le tableau suivant répertorie les OID sysObjectID pour les modèles ASA et ISA.

Tableau 2 : Identifiants d'objet SNMP

Identifiant de produit	sysObjectID	Numéro de modèle
ASA virtuel	ciscoASAv (ciscoProducts 1902)	Appareil virtuel de sécurité adaptable Cisco (ASA virtuel)
Contexte système ASA virtuel	ciscoASAvsy (ciscoProducts 1903)	Contexte système de l'appareil virtuel de sécurité adaptable Cisco (ASA virtuel)
Contexte de sécurité ASA virtuel	ciscoASAvsc (ciscoProducts 1904)	Contexte de sécurité de l'appareil virtuel de sécurité adaptable Cisco (ASA virtuel)
Appareil de sécurité industrielle ISA30004C	ciscoProducts 2268	ciscoISA30004C
CISCO ISA30004C avec 4 contextes de sécurité GE en cuivre	ciscoProducts 2139	ciscoISA30004Csc
CISCO ISA30004C avec 4 contextes système GE en cuivre	ciscoProducts 2140	ciscoISA30004Csy
Appareil de sécurité industrielle ISA30002C2F	ciscoProducts 2267	ciscoISA30002C2F
CISCO ISA30002C2F avec 2 ports GE en cuivre + 2 contextes de sécurité GE en fibre	ciscoProducts 2142	ciscoISA30002C2Fsc
CISCO ISA30002C2F avec 2 ports GE en cuivre + 2 contextes système GE en fibre	ciscoProducts 2143	ciscoISA30002C2Fsy
Châssis de l'appareil de sécurité industrielle (ISA) Cisco 30004C	cevChassis 1677	cevChassisISA30004C
Châssis de l'appareil de sécurité industrielle (ISA) Cisco 30002C2F	cevChassis 1678	cevChassisISA30002C2F
Capteur de température de l'unité de traitement Central pour l'UGS ISA30004C en cuivre	cevSensor 187	cevSensorISA30004CCpuTempSensor
Capteur de température de l'unité de traitement Central pour ISA30002C2F en fibre	cevSensor 189	cevSensorISA30002C2FCpuTempSensor
Capteur de température de carte de processeur pour l'UGS ISA30004C en cuivre	cevSensor 192	cevSensorISA30004CPTS
Capteur de température de carte de processeur pour l'UGS ISA30002C2F en fibre	cevSensor 193	cevSensorISA30002C2FPTS

Identifiant de produit	sysObjectID	Numéro de modèle
Capteur de température de carte d'alimentation pour l'UGS ISA30004C en cuivre	cevSensor 197	cevSensorISA30004CPowercardTS
Capteur de température de carte d'alimentation pour l'UGS ISA30002C2F en fibre	cevSensor 198	cevSensorISA30002C2FPowercardTS
Capteur de température de carte de port pour ISA30004C	cevSensor 199	cevSensorISA30004CPortcardTS
Capteur de température de carte de port pour ISA30002C2F	cevSensor 200	cevSensorISA30002C2FPortcardTS
Unité de traitement Central pour l'UGS ISA30004C en cuivre	cevModuleCpuType 329	cevCpuISA30004C
Unité de traitement Central pour l'UGS ISA30002C2F en fibre	cevModuleCpuType 330	cevCpuISA30002C2F
Modules ISA30004C, ISA30002C2F	cevModule 111	cevModuleISA3000Type
Disque SSD pour appareil de sécurité industrielle 30004C	cevModuleISA3000Type 1	cevModuleISA30004CSSD64
Disque SSD pour appareil de sécurité industrielle 30002C2F	cevModuleISA3000Type 2	cevModuleISA30002C2FSSD64
Contournement matériel Cisco ISA30004C/ISA30002C2F	cevModuleISA3000Type 5	cevModuleISA3000HardwareBypass
Appareil de sécurité FirePOWER 4140, 1U avec module de sécurité intégré 36	ciscoFpr4140K9 (ciscoProducts 2293)	FirePOWER 4140
Appareil de sécurité FirePOWER 4120, 1U avec module de sécurité intégré 24	ciscoFpr4120K9 (ciscoProducts 2294)	FirePOWER 4120
Baie de ventilateur FirePOWER 4K	cevContainer 363	cevContainerFPR4KFanBay
Baie d'alimentation FirePOWER 4K	cevContainer 364	cevContainerFPR4KPowerSupplyBay
Cisco Cisco Secure Firewall Threat Defense Virtual , VMWare	cevChassis 1795	cevChassisCiscoFTDVVMW
Cisco Firewall Threat Defense Virtual, AWS	cevChassis 1796	cevChassisCiscoFTDVAWS

Valeurs de type de prestataire physique

Chaque châssis ou système autonome Cisco a un numéro de type unique pour l'utilisation de SNMP. Les OID entPhysicalVendorType sont définis dans CISCO-ENTITY-VENDORTYPE-OID-MIB. Cette valeur est

renvoyée dans l'objet entPhysicalVendorType à partir de l'agent SNMP ASA, ASA virtuel ou ASASM. Vous pouvez utiliser cette valeur pour identifier le type de composant (module, alimentation, ventilateur, capteurs, CPU, etc.). Le tableau suivant répertorie les valeurs de type de prestataire physique pour les modèles ASA.

Tableau 3 : Valeurs de type de prestataire physique

Article	Description de l'OID entPhysicalVendorType
Port Gigabit Ethernet	cevPortGe (cevPort 109)
Appareil virtuel de sécurité adaptable Cisco	cevChassisASAv (cevChassis 1451)

Tableaux et objets pris en charge dans les MIB

Le tableau suivant répertorie les tableaux et les objets pris en charge pour les MIB précisées.

En mode de contexte multiple, ces tableaux et objets fournissent des renseignements sur un contexte unique. Si vous souhaitez des données dans tous les contextes, vous devez les résumer. Par exemple, pour obtenir l'utilisation générale de la mémoire, effectuez la somme des valeurs cempMemPoolHCUsed pour chaque contexte.

Tableau 4 : Tableaux et objets pris en charge dans les MIB

Nom et OID de MIB	Tableaux et objets pris en charge
CISCO-ENHANCED-MEMPOOL-MIB; OID : 1.3.6.1.4.1.9.9.221	cempMemPoolTable, cempMemPoolIndex, cempMemPoolType, cempMemPoolName, cempMemPoolAlternate, cempMemPoolValid. Pour un système de mémoire de 32 bits, interrogez à l'aide des compteurs de mémoire de 32 bits : cempMemPoolUsed, cempMemPoolFree,cempMemPoolUsedOvrflw, cempMemPoolFreeOvrflw, cempMemPoolLargestFree, cempMemPoolLowestFree, cempMemPoolUsedLowWaterMark, cempMemPoolAllocHit, cempMemPoolAllocMiss, cempMemPoolFreeHit, cempMemPoolFreeMiss, cempMemPoolLargestFreeOvrflw, cempMemPoolLowestFreeOvrflw, cempMemPoolUsedLowWaterMarkOvrflw, cempMemPoolSharedOvrflw. Pour un système de mémoire de 64 bits, interrogez à l'aide des compteurs de mémoire de 64 bits : cempMemPoolHCUsed, cempMemPoolHCFree, cempMemPoolHCLargestFree, cempMemPoolHCLowestFree, cempMemPoolHCUsedLowWaterMark, cempMemPoolHCShared
CISCO-REMOTE-ACCESS-MONITOR-MIB; OID : 1.3.6.1.4.1.9.9.392 **Remarque** Ces trois OID de MIB peuvent être utilisés pour déterminer les raisons pour lesquelles les connexions d'accès à distance échouent.	crasNumTotalFailures, crasNumSetupFailInsufResources, crasNumAbortedSessions
CISCO-ENTITY-SENSOR-EXT-MIB; OID : 1.3.6.1.4.1.9.9.745	ceSensorExtThresholdTable

Nom et OID de MIB	Tableaux et objets pris en charge
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB; OID : 1.3.6.1.4.1.9.9.480	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB; OID : 1.3.6.1.4.1.9.9.720 **Remarque** Non pris en charge sur l'ASA virtuel	ctsxSxpGlobalObjects, ctsxSxpConnectionObjects, ctsxSxpSgtObjects
DISMAN-EVENT-MIB; OID : 1.3.6.1.2.1.88	mteTriggerTable, mteTriggerThresholdTable, mteObjectsTable, mteEventTable, mteEventNotificationTable
DISMAN-EXPRESSION-MIB; OID : 1.3.6.1.2.1.90	expExpressionTable, expObjectTable, expValueTable
ENTITY-SENSOR-MIB; OID : 1.3.6.1.2.1.99 **Remarque** Fournit des renseignements sur les capteurs physiques, comme la température du châssis, le régime des ventilateurs, la tension d'alimentation, etc. Non pris en charge sur la plateforme ASA virtuel.	entPhySensorTable
NAT-MIB; OID : 1.3.6.1.2.1.123	natAddrMapTable, natAddrMapIndex, natAddrMapName, natAddrMapGlobalAddrType, natAddrMapGlobalAddrFrom, natAddrMapGlobalAddrTo, natAddrMapGlobalPortFrom, natAddrMapGlobalPortTo, natAddrMapProtocol, natAddrMapAddrUsed, natAddrMapRowStatus
CISCO-PTP-MIB; OID : 1.3.6.1.4.1.9.9.760 **Remarque** Seules les MIB correspondant au mode d'horloge E2E transparent sont prises en charge.	ciscoPtpMIBSystemInfo, cPtpClockDefaultDSTable, cPtpClockTransDefaultDSTable, cPtpClockPortTransDSTable
CISCO-PROCESS-MIB; 1.3.6.1.4.1.9.9.109.1.1.1.1.7.1 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 to 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	cpmCPUTotal1minRev Paramètres associés et valeurs de cPMCPUTotal1minRev Exemples : • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+2) : pourcentage d'utilisation de la CPU agrégé du système (cette valeur est identique à l'utilisation de la CPU du système de la version .3.6.1.4.1.9.9.109.1.1.1.1.7.1 en mode contexte unique). • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+3) : pourcentage d'utilisation moyenne du processeur Snort (valeur agrégée totale de toutes les instances Snort) • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+4) : pourcentage moyen de processus système (moyenne des cœurs « Sysprocess »)

Interruptions prises en charge (notifications)

Le tableau suivant répertorie les interruptions prises en charge (notifications) et les MIB associées.

Tableau 5 : Interruptions prises en charge (notifications)

Nom de l'interruption et de la MIB	Liste des variables	Description
authenticationFailure (SNMPv2-MIB)	—	Pour SNMP version 1 ou 2, l'identifiant de communauté fourni dans la demande SNMP est incorrect. Pour SNMP version 3, une PDU de rapport est générée au lieu d'une interruption si les mots de passe ou les noms d'utilisateur de l'authentification ou du privilège sont incorrects. La commande **snmp-server enable traps snmp authentication** est utilisée pour activer et désactiver la transmission de ces interruptions.
bgpBackwardTransition	bgpPeerLastError, bgpPeerState	La commande **snmp-server enable traps peer-flap** est utilisée pour activer la transmission des interruptions BGP homologues.
ccmCLIRunningConfigChanged (CISCO-CONFIG-MAN-MIB)	ccmHistoryRunningLastChanged, ccmHistoryEventTerminalType	La commande **snmp-server enable traps config** est utilisée pour activer la transmission de cette interruption.
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	La commande **snmp-server enable traps entity fru-insert** est utilisée pour activer cette notification.
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	La commande **snmp-server enable traps entity fru-remove** est utilisée pour activer cette notification.

Nom de l'interruption et de la MIB	Liste des variables	Description
ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB)	entPhysicalName, entPhysicalDescr, entPhySensorValue, entPhySensorType, ceSensorExtThresholdValue	La commande **snmp-server enable traps entity** [**power-supply-failure** | **fan-failure** | **cpu-temperature**] est utilisée pour activer la transmission des notifications de seuil d'entité. Cette notification est envoyée en cas de défaillance de l'alimentation. Les objets envoyés identifient la température du ventilateur et du processeur. La commande **snmp-server enable traps entity fan-failure** est utilisée pour activer la transmission de l'interruption de défaillance du ventilateur.Cette interruption ne s'applique pas à la série Firepower 2100. La commande **snmp-server enable traps entity power-supply-failure** est utilisée pour activer la transmission de l'interruption de défaillance de l'alimentation.Cette interruption ne s'applique pas à la série Firepower 2100. La commande **snmp-server enable Traps entités châssis-ventilateur** est utilisée pour activer la transmission de l'interruption de défaillance du ventilateur du châssis. La commande **snmp-server enable traps entity cpu-temperature** est utilisée pour activer la transmission de l'interruption de température CPU élevée. Cette interruption ne s'applique pas à la série Firepower 2100. La commande **snmp-server enable traps entity power-supply-presence** est utilisée pour activer la transmission de l'interruption de défaillance de la présence de l'alimentation. La commande **snmp-server enable traps entity power-supply-temperature** est utilisée pour activer la transmission de l'interruption de seuil de température de l'alimentation. La commande **snmp-server enable traps entity chassis-temperature** est utilisée pour activer la transmission de l'interruption de la température ambiante du châssis. Cette interruption ne s'applique pas à la série Firepower 2100. La commande **snmp-server enable traps entity accelerator-temperature** est utilisée pour activer la transmission de l'interruption de la température de l'accélérateur du châssis.

Nom de l'interruption et de la MIB	Liste des variables	Description
cikeTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cikePeerLocalAddr, cikePeerRemoteAddr, cikeTunLifeTime	La commande **snmp-server enable traps ikev2 start** est utilisée pour activer la transmission de l'interruption de démarrage ikev2.
cikeTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cikePeerLocalAddr, cikePeerRemoteAddr, cikeTunActiveTime	La commande **snmp-server enable traps ikev2 stop** est utilisée pour activer la transmission de l'interruption d'arrêt ikev2.
cipSecTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunLifeTime, cipSecTunLifeSize	La commande **snmp-server enable traps ipsec start** est utilisée pour activer la transmission de cette interruption.
cipSecTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunActiveTime	La commande **snmp-server enable traps ipsec stop** est utilisée pour activer la transmission de cette interruption.
ciscoConfigManEvent (CISCO-CONFIG-MAN-MIB)	ccmHistoryEventCommandSource, ccmHistoryEventConfigSource, ccmHistoryEventConfigDestination	La commande **snmp-server enable traps config** est utilisée pour activer la transmission de cette interruption.
ciscoRasTooManySessions (CISCO-REMOTE-ACCESS-MONITOR-MIB)	crasNumSessions, crasNumUsers, crasMaxSessionsSupportable, crasMaxUsersSupportable, crasThrMaxSessions	La commande **snmp-server enable traps remote-access session-threshold-exceeded** est utilisée pour activer la transmission de ces interruptions.
ciscoUFwFailoverStateChanged (CISCO-UNIFIED-FIREWALL-MIB)	gid, FOStatus	La commande **snmp-server enable traps failover-state** est utilisée pour activer la transmission de l'interruption d'état du basculement.
clogMessageGenerated (CISCO-SYSLOG-MIB)	clogHistFacility, clogHistSeverity, clogHistMsgName, clogHistMsgText, clogHistTimestamp	Des messages de journal système sont générés. La valeur de l'objet clogMaxSeverity est utilisée pour décider quels messages de journal système sont envoyés en tant qu'interruptions. La commande **snmp-server enable traps syslog** est utilisée pour activer et désactiver la transmission de ces interruptions.
clrResourceLimitReached (CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB)	crlResourceLimitValueType, crlResourceLimitMax, clogOriginIDType, clogOriginID	La commande **snmp-server enable traps connection-limit-reached** est utilisée pour activer la transmission de la notification de limite de connexion atteinte. L'objet clogOriginID comprend le nom du contexte à partir duquel provient l'interruption.

Nom de l'interruption et de la MIB	Liste des variables	Description
coldStart (SNMPv2-MIB)	—	L'interruption coldStart qui se produit lorsque l'agent SNMP démarre après la configuration de SNMP. Cette interruption se produit également lorsque l'agent démarre après un redémarrage du système. **Remarque** Pour les nœuds de grappe et de haute disponibilité, publiez un rechargement, si le temps de redémarrage des interfaces dépasse 5 minutes (seuil de présélection), l'interruption est abandonnée. Lorsque la grappe et les nœuds à haute disponibilité ont redémarré avec succès, toutes les autres interruptions sont envoyées comme prévu. La commande **snmp-server enable traps snmp coldstart** est utilisée pour activer et désactiver la transmission de ces interruptions.
cpmCPURisingThreshold (CISCO-PROCESS-MIB)	cpmCPURisingThresholdValue, cpmCPUTotalMonIntervalValue, cpmCPUInterruptMonIntervalValue, cpmCPURisingThresholdPeriod, cpmProcessTimeCreated, cpmProcExtUtil5SecRev	La commande **snmp-server enable traps cpu threshold rising** est utilisée pour activer la transmission de la notification d'augmentation du seuil de CPU. L'objet cpmCPURisingThresholdPeriod est envoyé avec les autres objets.
cufwClusterStateChanged (CISCO-UNIFIED-FIREWALL-MIB)	status	La commande **snmp-server enable traps cluster-state** est utilisée pour activer la transmission de l'interruption d'état de la grappe.
entConfigChange (ENTITY-MIB)	—	La commande **snmp-server enable traps entity config-change fru-insert fru-remove** est utilisée pour activer cette notification. **Remarque** Cette notification est envoyée uniquement en multimode, lorsqu'un contexte de sécurité est créé ou supprimé.
linkDown (IF-MIB)	ifIndex, ifAdminStatus, ifOperStatus	L'interruption linkdown (perte de liaison) pour les interfaces. La commande **snmp-server enable traps snmp linkdown** est utilisée pour activer et désactiver la transmission de ces interruptions.
linkUp (IF-MIB)	ifIndex, ifAdminStatus, ifOperStatus	L'interruption linkup (établissement de liaison) pour les interfaces. La commande **snmp-server enable traps snmp linkup** est utilisée pour activer et désactiver la transmission de ces interruptions.

Nom de l'interruption et de la MIB	Liste des variables	Description
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, cempMemPoolName, cempMemPoolHCUsed	La commande **snmp-server enable traps memory-threshold** est utilisée pour activer la notification de seuil de mémoire. Le mteHotOID est défini sur cempMemPoolHCUsed. Les objets cempMemPoolName et cempMemPoolHCUsed sont envoyés avec les autres objets.
mteTriggerFired (DISMAN-EVENT-MIB)	mteHotTrigger, mteHotTargetName, mteHotContextName, mteHotOID, mteHotValue, ifHCInOctets, ifHCOutOctets, ifHighSpeed, entPhysicalName	La commande **snmp-server enable traps interface-threshold** est utilisée pour activer la notification de seuil d'interface. Les objets entPhysicalName sont envoyés avec les autres objets.
natPacketDiscard (NAT-MIB)	ifIndex	La commande **snmp-server enable traps nat packet-discard** est utilisée pour activer la notification de suppression de paquet NAT. Cette notification est limitée pendant 5 minutes et est générée lorsque les paquets IP sont rejetés par la NAT en raison de l'espace de mappage non disponible. L'ifIndex donne l'ID de l'interface mappée.
ospfNbrStateChange	ospfRouterId, ospfNbrIpAddr, ospfNbrAddressLessIndex, ospfNbrRtrId, ospfNbrState	La commande **snmp-server enable traps peer-flap** est utilisée pour activer la transmission des pièges OSPF homologues. **Remarque** Pour les modèles ASA5585, le moteur SNMP est modifié pour utiliser la bibliothèque netsnmp version 5.8 et les OID suivants ne sont pas disponibles dans la bibliothèque : • ospfIfStateChange 1.3.6.1.2.1.14.16.2.16 • ospfVirtIfStateChange 1.3.6.1.2.1.14.16.2.1 • ospfVirtNbrStateChange 1.3.6.1.2.1.14.16.2.3
warmStart (SNMPv2-MIB)	—	L'interruption warmStart qui se produit lorsque l'agent SNMP redémarre pour la première fois. Cette interruption se produit également lorsque l'agent redémarre après une modification de configuration SNMP, où toutes les configuration d'hôte SNMP sont supprimées et une nouvelle configuration SNMP est effectuée. La commande **snmp-server enable traps snmp warmstart** est utilisée pour activer et désactiver la transmission de ces interruptions.

Types d'interface et exemples

Voici les types d'interfaces qui produisent les statistiques de trafic SNMP :

- Logique : statistiques recueillies par le pilote logiciel, qui constituent un sous-ensemble de statistiques physiques.
- Physique : statistiques recueillies par le pilote matériel. Chaque interface physique nommée est associée à un ensemble de statistiques logiques et physiques. Chaque interface physique peut être associée à plusieurs interfaces VLAN. Les interfaces VLAN n'ont que des statistiques logiques.

Remarque Pour une interface physique qui est associée à plusieurs interfaces VLAN, sachez que les compteurs SNMP pour les OID ifInOctets et ifOutoctets correspondent aux compteurs de trafic agrégé pour cette interface physique.

- VLAN uniquement : SNMP utilise les statistiques logiques pour ifInOctets et ifOutOctets.

Les exemples du tableau suivant montrent les différences entre les statistiques de trafic SNMP. L'exemple 1 montre la différence entre les statistiques de sortie physiques et logiques des commandes **show interface** et **show traffic**. L'exemple 2 présente les statistiques de sortie d'une interface VLAN uniquement pour les commandes **show interface** et **show traffic**. L'exemple montre que les statistiques sont proches de la sortie qui s'affiche pour la commande **show traffic**.

Tableau 6 : Statistiques de trafic SNMP pour les interfaces physiques et VLAN

Exemple 1

```
ciscoasa# show interface GigabitEthernet3/2
interface GigabitEthernet3/2
description fullt-mgmt
nameif mgmt
security-level 10
ip address 10.7.14.201 255.255.255.0
management-only

ciscoasa# show traffic
(Condensed output)

Physical Statistics
GigabitEthernet3/2:
received (in 121.760 secs)
36 packets       3428 bytes
0 pkts/sec      28 bytes/sec

Logical Statistics
mgmt:
received (in 117.780 secs)
36 packets       2780 bytes
0 pkts/sec      23 bytes/sec
```

Les exemples suivants montrent les statistiques de sortie SNMP pour l'interface de gestion et l'interface physique. La valeur ifInOctets est proche de la sortie des statistiques physiques qui apparaît dans la sortie de la commande **show traffic**, mais pas de la sortie des statistiques logiques.

ifIndex de l'interface de gestion :

```
IF_MIB::ifDescr.6 = Adaptive Security Appliance 'mgmt' interface
```

ifInOctets correspondant aux statistiques de l'interface physique :

```
IF-MIB::ifInOctets.6 = Counter32:3246
```

Exemple 2

```
ciscoasa# show interface GigabitEthernet
interface GigabitEthernet0/0.100
vlan 100
nameif inside
security-level 100
ip address 10.7.1.101 255.255.255.0 stan

ciscoasa# show traffic
inside
received (in 9921.450 secs)
1977 packets       126528 bytes
0 pkts/sec      12 bytes/sec
transmitted (in 9921.450 secs)
1978 packets       126556 bytes
0 pkts/sec      12 bytes/sec
```

ifIndex du VLAN interne :

```
IF-MIB::ifDescr.9 = Adaptive Security Ap
IF-MIB::ifInOctets.9 = Counter32: 126318
```

Présentation du SNMP version 3

SNMP version 3 offre des améliorations de sécurité qui ne sont pas disponibles dans les versions SNMP 1 et 2c. Les versions SNMP 1 et 2c transmettent des données entre le serveur SNMP et l'agent SNMP en texte clair. SNMP version 3 ajoute des options d'authentification et de confidentialité pour sécuriser les opérations du protocole. En outre, cette version contrôle l'accès à l'agent SNMP et aux objets MIB par le biais du modèle de sécurité basé sur l'utilisateur (USM) et du modèle de contrôle d'accès basé sur l'affichage (VACM). L'ASA prend également en charge la création de groupes SNMP et d'utilisateurs, ainsi que d'hôtes, ce qui est nécessaire pour activer l'authentification et le chiffrement du transport pour des communications SNMP sécurisées.

Modèles de sécurité

À des fins de configuration, les options d'authentification et de confidentialité sont regroupées dans des modèles de sécurité. Les modèles de sécurité s'appliquent aux utilisateurs et aux groupes, qui sont répartis dans les trois types suivants :

- NoAuthPriv : pas d'authentification ni de confidentialité, ce qui signifie qu'aucune sécurité n'est appliquée aux messages.
- AuthNoPriv : authentification mais pas de confidentialité, ce qui signifie que les messages sont authentifiés.
- AuthPriv : authentification et confidentialité, ce qui signifie que les messages sont authentifiés et chiffrés.

SNMP Groups (groupes SNMP)

Un groupe SNMP est une stratégie de contrôle d'accès à laquelle des utilisateurs peuvent être ajoutés. Chaque groupe SNMP est configuré avec un modèle de sécurité et est associé à une vue SNMP. Un utilisateur appartenant à un groupe SNMP doit correspondre au modèle de sécurité du groupe SNMP. Ces paramètres spécifient le type d'authentification et de confidentialité utilisé par un utilisateur appartenant à un groupe SNMP. Chaque paire de noms de groupes SNMP et de modèles de sécurité doit être unique.

Utilisateurs SNMP

Les utilisateurs SNMP disposent d'un nom d'utilisateur spécifié, d'un groupe auquel ils appartiennent, d'un mot de passe d'authentification, d'un mot de passe de chiffrement et d'algorithmes d'authentification et de chiffrement à utiliser. Les options d'algorithme d'authentification sont SHA-1, SHA-224, SHA-256 HMAC et SHA-384. Les options d'algorithme de chiffrement sont 3DES et AES (qui sont disponibles en versions 128, 192 et 256). Lorsque vous créez un utilisateur, vous devez l'associer à un groupe SNMP. L'utilisateur hérite ensuite du modèle de sécurité du groupe.

Remarque Lors de la configuration d'un compte d'utilisateur SNMPv3, assurez-vous que la longueur de l'algorithme d'authentification est égale ou supérieure à la longueur de l'algorithme de chiffrement.

Hôtes SNMP

Un hôte SNMP est une adresse IP à laquelle les notifications et les alertes SNMP sont envoyées. Pour configurer les hôtes SNMP version 3, ainsi que l'adresse IP cible, vous devez configurer un nom d'utilisateur, car les alertes ne sont envoyées qu'à un utilisateur configuré. Les adresses IP cibles SNMP et les noms de paramètre cibles doivent être uniques sur l'ASA. Chaque hôte SNMP ne peut être associé qu'à un seul nom d'utilisateur. Pour recevoir des alertes SNMP, après avoir ajouté la commande **snmp-server host**, assurez-vous de configurer les renseignements d'authentification de l'utilisateur sur le NMS pour qu'ils correspondent aux renseignements d'authentification de l'ASA.

Remarque Vous pouvez ajouter jusqu'à 8 192 hôtes. Cependant, seulement 128 de ceux-cis peuvent être utilisés pour les déroutements.

Différences d'implémentation entre les logiciels ASA et Cisco IOS

La mise en œuvre de SNMP version 3 dans l'ASA diffère de la mise en œuvre de SNMP version 3 dans le logiciel Cisco IOS de la manière suivante :

- Les ID du moteur local et du moteur distant ne sont pas configurables. L'ID du moteur local est généré au démarrage de l'ASA ou lors de la création d'un contexte.
- Aucune prise en charge n'existe pour le contrôle d'accès basé sur l'affichage, ce qui entraîne une navigation MIB non limitée.
- La prise en charge est limitée aux MIB suivantes : USM, VACM, FRAMEWORK et TARGET.
- Vous devez créer des utilisateurs et des groupes avec le modèle de sécurité approprié.
- Vous devez supprimer les utilisateurs, les groupes et les hôtes dans le bon ordre.
- L'utilisation de la commande snmp-server host crée une règle ASA pour autoriser le trafic SNMP entrant.

Messagerie du journal système SNMP

SNMP génère des messages de journal système détaillés, numérotés 212*nnn*. Les messages du journal système indiquent l'état des requêtes SNMP, des interruptions SNMP, des canaux SNMP et des réponses SNMP de l'ASA ou de l'ASASM à un hôte spécifié sur une interface spécifiée.

Pour obtenir des renseignements détaillés sur les messages du journal système, consultez le guide des messages de journal système.

Remarque L'interrogation SNMP échoue si les messages de journal système du protocole SNMP dépassent un débit élevé (environ 4 000 par seconde).

Services d'application et outils tiers

Pour en savoir plus sur la prise en charge de SNMP, consultez l'URL suivante :

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

Pour en savoir plus sur l'utilisation d'outils tiers pour parcourir les MIB de la version 3 du SNMP, consultez l'URL suivante :

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

Lignes directrices pour SNMP

Cette section comprend les lignes directrices et les limites que vous devez consulter avant de configurer SNMP.

Lignes directrices en matière de basculement et de mise en grappe

- Lorsque vous utilisez SNMPv3 avec mise en grappe ou basculement, si vous ajoutez une nouvelle unité de grappe après la formation initiale de la grappe ou si vous remplacez une unité de basculement, les

utilisateurs SNMPv3 ne sont pas répliqués sur la nouvelle unité. Vous devez rajouter les utilisateurs SNMPv3 à l'unité de contrôle ou active pour forcer les utilisateurs à être dupliqués sur la nouvelle unité; ou vous pouvez ajouter les utilisateurs directement sur la nouvelle unité (les utilisateurs et les groupes SNMPv3 sont une exception à la règle selon laquelle vous ne pouvez pas saisir de commandes de configuration sur une unité de données en grappe). Reconfigurez chaque utilisateur en saisissant la commande **snmp-server user** *username group-name* **v3** sur l'unité de contrôle/active ou directement sur l'unité de données/secours avec les options *priv-password* et *auth-password* dans leur format non chiffré.

Lignes directrices relatives à IPv6 (tous les modèles ASA)

SNMP peut être configuré sur le transport IPv6 de sorte qu'un hôte IPv6 puisse exécuter des requêtes SNMP et recevoir des notifications SNMP d'un périphérique exécutant le logiciel IPv6. L'agent SNMP et les MIB associées ont été améliorés pour prendre en charge l'adressage IPv6.

Lignes directrices relatives à IPv6 pour Firepower 2100

Firepower 2100 exécute un système d'exploitation sous-jacent appelé FXOS et prend en charge le mode appareil (par défaut) et le mode plateforme; voir Régler le Firepower 2100 en mode appareil ou plateforme.

En mode plateforme, vous devez configurer une adresse IP de gestion IPv6 dans FXOS. Dans l'exemple suivant, une passerelle et une interface de gestion IPv6 sont configurées :

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if
Management IPv6 Interface:
IPv6 Address Prefix IPv6 Gateway
---------------------------------- ---------- ------------
2001::8998 64 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

Directives supplémentaires

- Les interruptions d'alimentation ne sont pas émises pour les systèmes fonctionnant en mode appareil.
- Pour Firepower 2100, en mode plateforme, vous ne pouvez pas interroger les interfaces membres d'un EtherChannel, et les interruptions pour les interfaces membres ne sont pas générées. Cette fonctionnalité est prise en charge si vous activez SNMP directement dans FXOS. Le mode appareil n'est pas affecté.
- Ne prend pas en charge les interruptions ASA pour les membres de ports individuels pour le Firepower 2100 en mode plateforme; consultez le Guide de référence de Cisco Firepower 2100 FXOS MIB.
- Pour Firepower 2100, en mode appareil, vous ne pouvez pas interroger le modèle matériel ni le numéro de série. De plus, dans l'ASA, les interruptions ne sont pas générées pour ces détails. Par conséquent, configurez SNMP sur FXOS ou Chassis Manager pour interroger l'adresse IP de gestion de châssis au lieu des interfaces sur l'instance ASA.
- Vous devez disposer de Cisco Works pour Windows ou d'un autre navigateur conforme à SNMP MIB-II pour recevoir des alertes SNMP ou parcourir une MIB.

- L'accès de gestion sur un tunnel VPN n'est pas pris en charge avec SNMP (la commande **management-access**). Pour SNMP sur VPN, nous vous recommandons d'activer SNMP sur une interface de boucle avec retour. Vous n'avez pas besoin d'activer la fonctionnalité d'accès de gestion pour utiliser SNMP sur l'interface de boucle avec retour. La boucle avec retour fonctionne également pour SSH.
- Ne prend pas en charge le contrôle d'accès basé sur l'affichage, mais il est possible de parcourir la MIB VACM pour déterminer les paramètres d'affichage par défaut.
- ENTITY-MIB n'est pas disponible dans le contexte de non-administration. Utilisez plutôt IF-MIB pour effectuer des requêtes dans le contexte de non-administration.
- ENTITY-MIB n'est pas disponible pour l'Firepower 9300. Utilisez plutôt CISCO-FIREPOWER-EQUIPMENT-MIB et CISCO-FIREPOWER-SM-MIB.
- Sur certains périphériques, il a été observé que l'ordre des interfaces (ifDescr) dans la sortie de **snmpwalk** change après un redémarrage. L'ASA utilise un algorithme pour déterminer le tableau ifIndex que SNMP interroge. Lorsque l'ASA est démarré, les interfaces sont ajoutées au tableau ifIndex dans l'ordre chargé au fur et à mesure que l'ASA lit la configuration. Les nouvelles interfaces ajoutées à l'ASA sont ajoutées à la liste des interfaces dans le tableau ifIndex. Lorsque des interfaces sont ajoutées, supprimées ou renommées, cela peut affecter l'ordre des interfaces lors du redémarrage.
- Lorsque vous fournissez un OID dans la commande **snmpwalk**, l'outil snmpwalk interroge toutes les variables de la sous-arborescence qui se trouve sous l'OID spécifié et affiche leurs valeurs. Ainsi, pour afficher une sortie complète des objets sur le périphérique, assurez-vous de fournir l'OID dans la commande **snmpwalk**.
- Ne prend pas en charge la version 3 du SNMP pour AIP SSM ou AIP SSC.
- Ne prend pas en charge le débogage SNMP.
- Ne prend pas en charge la récupération des renseignements ARP.
- Ne prend pas en charge les commandes SNMP NET.
- Lorsque vous utilisez NET-SNMP version 5.4.2.1, prend uniquement en charge la version de l'algorithme de chiffrement AES128. Ne prend pas en charge les versions des algorithmes de chiffrement AES256 ou AES192.
- Les modifications apportées à la configuration existante sont refusées si le résultat place la fonctionnalité SNMP dans un état incohérent.
- Pour la version 3 de SNMP, la configuration doit avoir lieu dans l'ordre suivant : groupe, utilisateur, hôte.
- Pour Firepower 2100, lorsque SNMPv3 est configuré sur l'interface de gestion des périphériques, tous les utilisateurs de SNMPv3 peuvent interroger le périphérique même lorsqu'ils ne sont pas mappés dans la configuration de l'hôte.
- Pour les modèles Secure Firewall, la commande **snmpwalk** interroge les membres FXOS uniquement à partir du contexte d'administration.
- Avant de supprimer un groupe, vous devez vous assurer que tous les utilisateurs associés à ce groupe sont supprimés.
- Avant de supprimer un utilisateur, vous devez vous assurer qu'aucun hôte associé à ce nom d'utilisateur n'est configuré.

- Si les utilisateurs ont été configurés pour appartenir à un groupe particulier avec un certain modèle de sécurité, et si le niveau de sécurité de ce groupe est modifié, vous devez effectuer les opérations suivantes dans cet ordre :
  - Supprimer les utilisateurs de ce groupe.
  - Modifier le niveau de sécurité du groupe.
  - Ajouter des utilisateurs qui appartiennent au nouveau groupe.
- La création de vues personnalisées pour restreindre l'accès des utilisateurs à un sous-ensemble d'objets MIB n'est pas prise en charge.
- Toutes les requêtes et toutes les interruptions sont disponibles uniquement dans la vue Lecture/Notification par défaut.
- L'interruption de la limite de connexion atteinte est générée dans le contexte d'administration. Pour générer cette interruption, vous devez avoir au moins un hôte de serveur SNMP configuré dans le contexte d'utilisateur dans lequel la limite de connexion a été atteinte.
- Vous pouvez ajouter jusqu'à 4 000 hôtes. Cependant, seulement 128 de ceux-cis peuvent être utilisés pour les déroutements.
- Le nombre total de destinations d'interrogation actives prises en charge est de 128.
- Vous pouvez spécifier un objet réseau pour indiquer les hôtes individuels que vous souhaitez ajouter en tant que groupe d'hôtes.
- Vous pouvez associer plusieurs utilisateurs à un hôte.
- Vous pouvez spécifier des objets réseau qui se chevauchent dans différentes commandes **host-group**. Les valeurs que vous spécifiez pour le dernier groupe d'hôtes s'appliquent à l'ensemble commun d'hôtes dans les différents objets réseau.
- Si vous supprimez un groupe d'hôtes ou des hôtes qui se chevauchent avec d'autres groupes d'hôtes, les hôtes sont reconfigurés en utilisant les valeurs qui ont été spécifiées dans les groupes d'hôtes configurés.
- Les valeurs acquises par les hôtes dépendent de la séquence spécifiée que vous utilisez pour exécuter les commandes.
- La limite de taille des messages que SNMP envoie est de 1 472 octets.
- L'ASA prend en charge un nombre illimité d'hôtes d'interruption de serveur SNMP par contexte. La sortie de la commande **show snmp-server host** affiche uniquement les hôtes actifs qui interrogent l'ASA, ainsi que les hôtes configurés de manière statique.

Astuces de dépannage

- Pour vous assurer que le processus SNMP qui reçoit les paquets entrants du NMS est en cours d'exécution, saisissez la commande suivante :

```
ciscoasa(config)# show process | grep snmp
```

- Pour capturer les messages de journal système provenant du SNMP et les faire apparaître sur la console ASA, saisissez les commandes suivantes :

```
ciscoasa(config)# logging list snmp message 212001-212015
ciscoasa(config)# logging console snmp
```

- Pour vous assurer que le processus SNMP envoie et reçoit des paquets, saisissez les commandes suivantes :

```
ciscoasa(config)# clear snmp-server statistics
ciscoasa(config)# show snmp-server statistics
```

  La sortie est basée sur le groupe SNMP de SNMPv2-MIB.

- Pour vous assurer que les paquets SNMP passent par l'ASA et parviennent au processus SNMP, saisissez les commandes suivantes :

```
ciscoasa(config)# clear asp drop
ciscoasa(config)# show asp drop
```

- Si le NMS ne parvient pas à demander des objets avec succès ou ne traite pas correctement les interruptions entrantes provenant de l'ASA, utilisez une capture de paquets pour isoler le problème en saisissant les commandes suivantes :

```
ciscoasa (config)# access-list snmp permit udp any eq snmptrap any
ciscoasa (config)# access-list snmp permit udp any any eq snmp
ciscoasa (config)# capture snmp type raw-data access-list snmp interface mgmt
ciscoasa (config)# copy /pcap capture:snmp tftp://192.0.2.5/exampledir/snmp.pcap
```

- Si l'ASA ne fonctionne pas comme prévu, obtenez des renseignements sur la topologie du réseau en procédant comme suit :
  - Pour la configuration NMS, obtenez les renseignements suivants :

    Nombre de délais d'expiration

    Nombre de tentatives :

    Mise en mémoire cache de l'ID du moteur

    Nom d'utilisateur et mot de passe utilisés
  - Exécutez les commandes suivantes :

    show block

    show interface

    show process

    show cpu

    show vm

- Si une erreur fatale se produit, pour faciliter la reproduction de l'erreur, envoyez un fichier de recherche de la source et la sortie de la commande **show tech-support** au TAC de Cisco.
- Si le trafic SNMP n'est pas autorisé par les interfaces ASA, vous devrez peut-être également autoriser le trafic ICMP provenant du serveur SNMP distant à l'aide de la commande **icmp permit**.

- Si vous avez configuré le périphérique avec **snmp-server enable oid**, lors des opérations de marche SNMP, l'ASA interrogera les renseignements de mémoire des groupes MEMPOOL_DMA et MEMPOOL_GLOBAL_SHARED. Cela peut entraîner des saturations du CPU liées à SNMP qui peuvent entraîner des abandons de paquet. Pour maîtriser ce problème, évitez d'interroger les OID qui se rapportent au groupe partagé global à l'aide de la commande **no snmp-server enable oid**. Lorsqu'ils sont désactivés, les OID du groupe de mémoire renvoient 0 octet.
- Lorsque vous utilisez SNMPGET avec un grand nombre d'OID dans une seule demande d'interrogation des compteurs d'abandon ASP, une interrogation répétée des compteurs d'abandon ASP se traduit par une utilisation accrue du CPU. Par conséquent, nous vous conseillons de déterminer les compteurs importants à surveiller et à utiliser SNMPGET sur chaque compteur pour obtenir ces valeurs de manière à limiter l'impact sur le CPU.
- Lorsque SNMP est configuré sur plusieurs contextes dans un ASA à contextes multiples, interrogez les contextes de manière séquentielle et utilisez SNMPBULKGET au lieu de snmpwalk pour réduire le nombre de connexions à la plateforme. Cette approche évitera les retards ou les délais d'expiration de SNMP lorsqu'un grand nombre de contextes sont interrogés en même temps.
- L'ASA définit de manière cohérente le bit Don't Fragment (DF) lors de la réponse aux interrogations SNMP avec des messages SNMP get-response, tels que SNMPBULKGET, qui nécessite que l'ensemble du chemin réseau prenne en charge au moins l'unité de transfert maximale (MTU) configurée dans l'ASA. Si une MTU inférieure est configurée sur le chemin réseau, d'autres périphériques peuvent envoyer des paquets ICMP (Internet Control Message Protocol) demandant la fragmentation. Cependant, puisque le bit DF est défini, l'ASA ne répond pas et ne fragmente pas les paquets, ce qui entraîne une perte de réponse de l'ASA.

  Pour résoudre ce problème, vous pouvez modifier la MTU sur l'ASA ou sur l'ensemble du chemin réseau, utiliser plusieurs demandes get au lieu de SNMPBULKGET, ou réduire la taille groupée des demandes SNMPBULKGET.

- Pour en savoir plus sur le dépannage, consultez l'URL suivante : http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/116423-troubleshoot-asa-snmp.html

Configurer SNMP

Cette section décrit comment configurer SNMP.

Procédure

Étape 1 Activez l'agent SNMP et le serveur SNMP.

Étape 2 Configurez les alertes SNMP.

Étape 3 Configurez les paramètres SNMP de version 1 et 2c ou les paramètres SNMP de version 3.

Activer l'agent SNMP et le serveur SNMP

Pour activer l'agent SNMP et le serveur SNMP, procédez comme suit :

Procédure

Activez l'agent SNMP et le serveur SNMP sur l'ASA. Par défaut, le serveur SNMP est activé.

snmp-server enable

Exemple :

```
ciscoasa(config)# snmp-server enable
```

Configurer les déroutements SNMP

Pour désigner les interruptions que l'agent SNMP génère et la manière dont elles sont collectées et envoyées aux NMS, procédez comme suit :

Remarque Lorsque vous activez toutes les alertes de SNMP ou de syslog, il est possible que le processus SNMP consomme les ressources excédentaires de l'agent et du réseau, ce qui entraîne le blocage du système. Si vous remarquez des retards du système, des demandes non terminées ou des échéances de délais d'expiration, vous pouvez activer de manière sélective les déroutements SNMP et syslog. Par exemple, vous pouvez ignorer le niveau de gravité *Informational* (Informationnel) de l'interruption de journal système.

Procédure

Envoyez des interruptions individuelles, des ensembles d'interruptions ou toutes les interruptions au NMS.

snmp-server enable traps [**all** | **syslog** | **snmp** [**authentication** | **linkup** | **linkdown** | **coldstart** | **warmstart**] | **config** | **entity** [**config-change** | **fru-insert** | **fru-remove** | **fan-failure** | **cpu-temperature** | **chassis-fan-failure** | **power-supply**] | **chassis-temperature** | **power-supply-presence** | **power-supply-temperature** **l1-bypass-status**] | **ikev2** [**start** | **stop**] | **cluster-state** | **failover-state** | **peer-flap** | **ipsec** [**start** | **stop**] | **remote-access** [**session-threshold-exceeded**] | **connection-limit-reached** | **cpu threshold rising** | **interface-threshold** | **memory-threshold** | **nat** [**packet-discard**]

Exemple :

```
ciscoasa(config)# snmp-server enable traps snmp authentication
linkup linkdown coldstart warmstart
```

Cette commande permet d'envoyer les messages de journal système en tant qu'interruptions au NMS. Toutes les interruptions standard SNMP sont activées dans la configuration par défaut, comme le montre l'exemple. Pour désactiver ces interruptions, utilisez la commande **no snmp-server enable traps snmp**.

Si vous saisissez cette commande et ne spécifiez pas de type d'interruption, la valeur par défaut est l'interruption **syslog**. Par défaut, l'interruption **syslog** est activée. Les alertes SNMP par défaut continuent d'être activées avec l'interruption **syslog** (journal système).

Vous devez configurer la commande **logging history** (historique de journalisation) et la commande **snmp-server enable traps syslog** pour générer des interruptions à partir de la MIB du journal système.

Pour rétablir l'activation par défaut des alertes SNMP, utilisez la commande **clear configure snmp-server**. Toutes les autres interruptions sont désactivées par défaut.

Interruptions disponibles dans le contexte d'administration uniquement :

- **connection-limit-reached**
- **entity**
- **memory-threshold**

Interruptions générées via le contexte d'administration uniquement pour les interfaces physiquement connectées dans le contexte système :

- **interface-threshold**

Toutes les autres interruptions sont disponibles dans les contextes d'administration et d'utilisateur en mode unique.

L'interruption **config** active les notifications ciscoConfigManEvent et ccmCLIRunningConfigChanged, qui sont générées après avoir quitté le mode de configuration.

Si l'utilisation du CPU est supérieure à la valeur de seuil configurée pour la période de supervision configurée, l'interruption **cpu threshold rising** est générée.

Lorsque la mémoire du contexte système utilisée atteint 80 % de la mémoire totale du système, l'interruption **memory-threshold** est générée à partir du contexte d'administration. Pour tous les autres contextes d'utilisateur, cette interruption est générée lorsque la mémoire utilisée atteint 80 % de la mémoire totale du système dans ce contexte en particulier.

Certains déroutements ne sont pas applicables à certains modèles de matériel. Utilisez ? à la place d'un mot clé d'interruption pour déterminer quelles interruptions sont disponibles pour votre appareil. Par exemple :

- Le Série Firepower 1000 prend uniquement en charge les interruptions d'entité suivantes : **chassis-temperature**, **config-change** et **cpu-temperature**.

Remarque
SNMP ne surveille pas les capteurs de tension.

Configurer un seuil d'utilisation du CPU

Pour configurer un seuil d'utilisation du CPU, procédez comme suit :

Procédure

Configurez la valeur de seuil pour un seuil de CPU élevé et la période de supervision du seuil.

snmp cpu threshold rising *threshold_value monitoring_period*

Exemple :

```
ciscoasa(config)# snmp cpu threshold rising 75% 30 minutes
```

Pour effacer la valeur de seuil et la période de supervision de l'utilisation du CPU, utilisez la forme **no** de cette commande. Si la commande **snmp cpu threshold rising** n'est pas configurée, la valeur par défaut pour le niveau de seuil élevé est supérieure à 70 % et la valeur par défaut pour le niveau de seuil critique est supérieure à 95 %. La période de supervision par défaut est fixée à 1 minute.

Vous ne pouvez pas configurer le niveau de seuil critique du CPU, qui est maintenu à une valeur constante de 95 %. Les valeurs de seuil valides pour un seuil de CPU élevé sont comprises entre 10 et 94 %. Les valeurs valides pour la période de supervision sont comprises entre 1 et 60 minutes.

Configurer un seuil d'interface physique

Pour configurer le seuil d'interface physique, procédez comme suit :

Procédure

Configurez la valeur de seuil pour une interface physique SNMP.

snmp interface threshold *threshold_value*

Exemple :

```
ciscoasa(config)# snmp interface threshold 75%
```

Pour effacer la valeur de seuil d'une interface physique SNMP, utilisez la forme **no** de cette commande. La valeur de seuil est définie en pourcentage d'utilisation de la bande passante de l'interface. Les valeurs de seuil valides sont comprises entre 30 et 99 %. La valeur par défaut est 70 %.

La commande **snmp interface threshold** est disponible uniquement dans le contexte d'administration.

L'utilisation des interfaces physiques est supervisée en mode de contexte unique et multiple, et les interruptions pour les interfaces physiques dans le contexte système sont envoyées par l'entremise du contexte d'administration. Seules les interfaces physiques sont utilisées pour calculer l'utilisation du seuil.

Configurer les paramètres pour la version 1 ou 2c du SNMP

Pour configurer les paramètres pour la version 1 ou 2c du SNMP, procédez comme suit :

Procédure

Étape 1 Spécifiez le destinataire d'une notification SNMP, indiquez l'interface à partir de laquelle les interruptions sont envoyées et identifiez le nom et l'adresse IP du gestionnaire NMS ou SNMP qui peut se connecter à l'ASA.

snmp-server host{*interface hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1 2c**| *username*}] [**udp-port** *port*]

Exemple :

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 2c
ciscoasa(config)# snmp-server host corp 172.18.154.159 community public

ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 2c
```

Le mot clé **trap** limite le NMS à la réception d'interruptions uniquement. Le mot clé **poll** limite le NMS à l'envoi de requêtes (interrogation) uniquement. Par défaut, les alertes SNMP sont activées. Par défaut, le port UDP est 162. L'identifiant de communauté est une clé secrète partagée entre l'ASA et le NMS. La clé est une valeur sensible à la casse pouvant comporter jusqu'à 32 caractères alphanumériques. Les espaces ne sont pas permises. L'identifiant de communauté par défaut est public. L'ASA utilise cette clé pour déterminer si la requête SNMP entrante est valide ou non. Par exemple, vous pouvez désigner un site avec un identifiant de communauté, puis configurer l'ASA et la station de gestion avec le même identifiant. L'ASA utilise l'identifiant spécifié et ne répond pas aux requêtes contenant un identifiant de communauté non valide. Cependant, si la supervision SNMP se fait par l'interface de gestion plutôt que par l'interface de diagnostic, l'interrogation a lieu sans que l'ASA ne valide l'identifiant de communauté. Après avoir utilisé un identifiant de communauté chiffré, seule la forme chiffrée est visible pour tous les systèmes (par exemple, interface de ligne de commande, ASDM, CSM, etc.). Le mot de passe en clair n'est pas visible. L'identifiant de communauté chiffré est toujours généré par l'ASA; vous devez généralement saisir la forme en clair.

Le mot clé **version** spécifie la version du SNMP à utiliser pour les interruptions et les requêtes (interrogation). La communication avec le serveur est autorisée uniquement en utilisant la version sélectionnée.

Pour recevoir des interruptions après avoir ajouté la commande **snmp-server host**, assurez-vous de configurer l'utilisateur sur le NMS avec les mêmes renseignements d'authentification que ceux configurés sur l'ASA.

Étape 2 Définissez l'identifiant de communauté, qui doit être utilisé *uniquement* avec la version 1 ou 2c du SNMP.

snmp-server community *community-string*

Exemple :

```
ciscoasa(config)# snmp-server community onceuponatime
```

Remarque
Vous devez éviter l'utilisation de caractères spéciaux (!, @, #, $, %, ^, &, *, \) dans les identifiants de communauté. En général, l'utilisation de caractères spéciaux réservés aux fonctions utilisées par le système d'exploitation peut entraîner des résultats inattendus. Par exemple, la barre oblique inverse (\) est interprétée comme un caractère d'échappement et ne doit pas être utilisée dans l'identifiant de communauté.

Étape 3 Définissez l'emplacement du serveur SNMP ou ses coordonnées.

snmp-server [**contact** | **location**] *text*

Exemple :

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

L'argument *text* spécifie le nom de la personne-ressource ou de l'administrateur système de l'ASA. Le nom est sensible à la casse et peut comporter jusqu'à 127 caractères. Les espaces sont acceptés, mais plusieurs espaces sont raccourcis en un seul espace.

Étape 4 Définissez le port d'écoute pour les requêtes SNMP.

snmp-server listen-port *lport*

Exemple :

```
ciscoasa(config)# snmp-server lport 192
```

L'argument *lport* est le port sur lequel les requêtes entrantes sont acceptées. Le port d'écoute par défaut est le 161. La commande **snmp-server listen-port** n'est disponible que dans le contexte d'administration et non pas dans le contexte système. Si vous configurez la commande **snmp-server listen-port** sur un port en cours d'utilisation, le message suivant apparaît :

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different port.
```

Le fil SNMP existant continue d'interroger toutes les 60 secondes jusqu'à ce que le port soit disponible et émet le message de journal système %ASA-1-212001 si le port est toujours utilisé.

Configurer les paramètres pour la version 3 du SNMP

Pour configurer les paramètres pour la version 3 du SNMP, procédez comme suit :

Procédure

Étape 1 Spécifiez un nouveau groupe SNMP, qui doit être utilisé *uniquement* avec la version 3 du SNMP.

snmp-server group *group-name* **v3** [**auth** | **noauth** | **priv**]

Exemple :

```
ciscoasa(config)# snmp-server group testgroup1 v3 auth
```

Lorsqu'un identifiant de communauté est configuré, deux groupes supplémentaires dont le nom correspond à l'identifiant de communauté sont automatiquement générés : un pour le modèle de sécurité version 1 et un pour le modèle de sécurité version 2. Le mot clé **auth** active l'authentification des paquets. Le mot clé **noauth** indique qu'aucune authentification ou ni aucun chiffrement de paquet n'est utilisé. Le mot clé **priv** active le chiffrement et l'authentification des paquets. Aucune valeur par défaut n'existe pour les mots clés **auth** ou **priv**.

Étape 2 Configurez un nouvel utilisateur pour un groupe SNMP, qui doit être utilisé uniquement avec la version 3 du SNMP.

snmp-server user *username group_name* **v3** [**engineID** *engineID*] [**encrypted**] [**auth** {**sha** | **sha224** | **sha256** | **sha384**} *auth_password* [**priv** {**3des** | **aes** {**128** | **192** | **256**}} *priv_password*]]

Exemple :

```
ciscoasa(config)# snmp-server user testuser1 testgroup1 v3 auth md5 testpassword
aes 128 mypassword
ciscoasa(config)# snmp-server user testuser1 public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

L'argument username est le nom de l'utilisateur sur l'hôte qui appartient à l'agent SNMP. Saisissez 32 caractères ou moins pour le nom d'utilisateur. Le nom doit commencer par une lettre. Les caractères valides sont les lettres, les chiffres, _ (trait de soulignement) et . (point), @ (at) et - (trait d'union).

L'argument group-name est le nom du groupe auquel appartient l'utilisateur. Le mot clé **v3** spécifie que le modèle de sécurité SNMP version 3 doit être utilisé et permet l'utilisation des mots clés **encrypted**, **priv** et **auth**. Le mot clé **engineID** est facultatif et spécifie l'ID du moteur de l'ASA qui a été utilisé pour localiser les renseignements d'authentification et de chiffrement de l'utilisateur. L'argument engineID doit spécifier un ID de moteur ASA valide.

Le mot clé **encrypted** spécifie le mot de passe au format chiffré. Les mots de passe cryptés doivent répondre aux exigences suivantes :

- Doit être au format hexadécimal.
- Doit contenir un minimum de 8 caractères et un maximum de 80 caractères.
- Doit contenir uniquement des lettres, des chiffres et les caractères suivants : ~`!@#%^&*()_-+{}[]|\:;"'<,>./
- Ne doit pas contenir les symboles suivants : $ (signe de dollar), ? (point d'interrogation) ou = (signe d'égalité).
- Doit contenir au moins cinq caractères différents.
- Ne doit pas contenir trop de chiffres ou de lettres consécutifs croissants ou décroissants. Par exemple, la chaîne « 12345 » comporte quatre caractères de ce type et la chaîne « ZYXW » en comporte trois. Si le nombre total de caractères de ce type dépasse une certaine limite (généralement plus de 4 à 6 occurrences), la vérification de la simplicité échouera.

  Remarque
  Le nombre de caractères consécutifs croissants ou décroissants n'est pas réinitialisé lorsque des caractères non croissants ou non décroissants sont utilisés entre eux. Par exemple, abcd&!21 échouera à la vérification du mot de passe, mais abcd&!25 n'échouera pas.

Le mot clé **auth** spécifie le niveau d'authentification (**sha**, **sha224**, **sha256** ou **sha384**) à utiliser. Le mot clé **priv** spécifie le niveau de chiffrement. Il n'existe aucune valeur par défaut pour les mots clés **auth** ou **priv**, ni aucun mot de passe par défaut.

Pour l'algorithme de chiffrement, vous pouvez spécifier le mot clé **3des** ou **aes**. Vous pouvez également spécifier la version de l'algorithme de chiffrement AES à utiliser : **128**, **192** ou **256**. L'argument auth-password spécifie le mot de passe d'authentification de l'utilisateur. L'argument priv-password spécifie le mot de passe de chiffrement de l'utilisateur.

Si vous ignorez un mot de passe, vous ne pouvez pas le récupérer et vous devez reconfigurer l'utilisateur. Vous pouvez spécifier un mot de passe en texte brut ou un condensé localisé. Le condensé localisé doit correspondre à l'algorithme d'authentification sélectionné pour l'utilisateur, qui peut être SHA, SHA-224, SHA-256, ou SHA-384. Lorsque la configuration de l'utilisateur s'affiche sur la console ou est écrite dans un fichier (par exemple, le fichier de configuration de démarrage), les condensés d'authentification et de confidentialité localisés s'affichent toujours au lieu d'un mot de passe en texte brut (voir le deuxième exemple).

La longueur minimum d'un mot de passe est de 1 caractère alphanumérique; cependant, nous vous conseillonns d'utiliser au moins 8 caractères alphanumériques pour des raisons de sécurité.

Lorsque vous utilisez SNMPv3 avec mise en grappe ou basculement, si vous ajoutez une nouvelle unité de grappe après la formation initiale de la grappe ou si vous remplacez une unité de basculement, les utilisateurs SNMPv3 ne sont pas répliqués sur la nouvelle unité. Vous devez rajouter les utilisateurs SNMPv3 à l'unité de contrôleou active pour forcer les utilisateurs à être dupliqués sur la nouvelle unité; ou vous pouvez ajouter les utilisateurs directement sur la nouvelle unité (les utilisateurs et les groupes SNMPv3 sont une exception à la règle selon laquelle vous ne pouvez pas saisir de commandes de configuration sur une unité de données en grappe). Reconfigurez chaque utilisateur en saisissant la commande **snmp-server user** *username group-name* **v3** sur l'unité de contrôle/active ou directement sur l'unité de données/secours avec les options *priv-password* et *auth-password* dans leur format non chiffré.

Si vous saisissez un utilisateur sur l'unité de contrôle/active avec le mot clé **encrypted**, un message d'erreur s'affiche pour vous informer que les commandes utilisateur SNMPv3 ne seront pas répliquées. Ce comportement signifie également que les commandes d'utilisateur et de groupe SNMPv3 existantes ne sont pas supprimées pendant la réplication.

Par exemple, une unité de contrôle/active utilisant des commandes saisies avec des clés chiffrées :

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a
priv aes 256 cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:
f6:86:cf:18:c0:f0:47:d6:94:e5:da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

Par exemple, une unité de données pendant la réplication de la grappe (apparaît uniquement si des commandes **snmp-server user** existent dans la configuration) :

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

Étape 3 Spécifiez le destinataire d'une notification SNMP. Indiquez l'interface à partir de laquelle les interruptions sont envoyées. Identifiez le nom et l'adresse IP du gestionnaire NMS ou SNMP qui peut se connecter à l'ASA.

snmp-server host *interface* {*hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

Exemple :

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 3 testuser1
ciscoasa(config)# snmp-server host mgmt 10.7.26.5 version 3 testuser2
ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 3 testuser3
```

Le mot clé **trap** limite le NMS à la réception d'interruptions uniquement. Le mot clé **poll** limite le NMS à l'envoi de requêtes (interrogation) uniquement. Par défaut, les alertes SNMP sont activées. Par défaut, le port UDP est 162. L'identifiant de communauté est une clé secrète partagée entre l'ASA et le NMS. La clé est une valeur sensible à la casse pouvant comporter jusqu'à 32 caractères alphanumériques. Les espaces ne sont pas permises. L'identifiant de communauté par défaut est public. L'ASA utilise cette clé pour déterminer si la requête SNMP entrante est valide. Par exemple, vous pouvez désigner un site avec un identifiant de communauté, puis configurer l'ASA et le NMS avec le même identifiant. L'ASA utilise l'identifiant spécifié et ne répond pas aux requêtes contenant un identifiant de communauté non valide. Après avoir utilisé un

identifiant de communauté chiffré, seule la forme chiffrée est visible pour tous les systèmes (par exemple, interface de ligne de commande, ASDM, CSM, etc.). Le mot de passe en clair n'est pas visible. L'identifiant de communauté chiffré est toujours généré par l'ASA; vous devez généralement saisir la forme en clair.

Le mot clé **version** spécifie la version du SNMP à utiliser pour les interruptions et les requêtes (interrogation). La communication avec le serveur est autorisée uniquement en utilisant la version sélectionnée.

Lorsque des hôtes SNMP version 3 sont configurés sur l'ASA, un utilisateur doit être associé à cet hôte.

Pour recevoir des interruptions après avoir ajouté la commande **snmp-server host**, assurez-vous de configurer l'utilisateur sur le NMS avec les mêmes renseignements d'authentification que ceux configurés sur l'ASA.

Étape 4 Définissez l'emplacement du serveur SNMP ou ses coordonnées.

snmp-server [**contact** | **location**] *text*

Exemple :

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

L'argument *text* spécifie le nom de la personne-ressource ou de l'administrateur système de l'ASA. Le nom est sensible à la casse et peut comporter jusqu'à 127 caractères. Les espaces sont acceptés, mais plusieurs espaces sont raccourcis en un seul espace.

Étape 5 Définissez le port d'écoute pour les requêtes SNMP.

snmp-server listen-port *lport*

Exemple :

```
ciscoasa(config)# snmp-server lport 192
```

L'argument *lport* est le port sur lequel les requêtes entrantes sont acceptées. Le port d'écoute par défaut est le 161. La commande **snmp-server listen-port** n'est disponible que dans le contexte d'administration et non pas dans le contexte système. Si vous configurez la commande **snmp-server listen-port** sur un port en cours d'utilisation, le message suivant apparaît :

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different port.
```

Le fil SNMP existant continue d'interroger toutes les 60 secondes jusqu'à ce que le port soit disponible et émet le message de journal système %ASA-1-212001 si le port est toujours utilisé.

Configurer un groupe d'utilisateurs

Pour configurer une liste d'utilisateurs SNMP avec un groupe d'utilisateurs spécifiés, procédez comme suit :

Procédure

Configurez une liste d'utilisateurs SNMP.

snmp-server user-list *list_name* **username** *user_name*

Exemple :

```
ciscoasa(config)# snmp-server user-list engineering username user1
```

L'argument *listname* spécifie le nom de la liste d'utilisateurs, qui peut comporter jusqu'à 33 caractères. La paire mot clé-argument **username** *user_name* spécifie les utilisateurs qui peuvent être configurés dans la liste des utilisateurs. Vous configurez les utilisateurs dans la liste des utilisateurs à l'aide de la commande **snmp-server user** *username*, qui est disponible uniquement si vous utilisez la version 3 de SNMP. La liste d'utilisateurs doit comporter plusieurs utilisateurs et peut être associée à un nom d'hôte ou à une plage d'adresses IP.

Associer les utilisateurs à un objet réseau

Pour associer un seul utilisateur ou un groupe d'utilisateurs d'une liste d'utilisateurs à un objet réseau, procédez comme suit :

Procédure

Associez un seul utilisateur ou un groupe d'utilisateurs dans une liste d'utilisateurs à un objet réseau.

snmp-server host-group *net_obj_name* [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}] [**udp-port** *port*]

Exemple :

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

L'argument *net_obj_name* spécifie le nom de l'objet réseau de l'interface auquel un utilisateur ou un groupe d'utilisateurs est associé.

Le mot clé **trap** spécifie que seules des alertes peuvent être envoyées et que cet hôte n'est pas autorisé à naviguer (interrogation). Les alertes SNMP sont activées par défaut.

Le mot clé **poll** indique que l'hôte est autorisé à naviguer (interrogation), mais qu'aucune interruption ne peut être envoyée.

Le mot clé **community** spécifie qu'une chaîne autre que par défaut est requise pour les demandes du NMS ou lors de la génération des alertes envoyées au NMS. Vous pouvez utiliser ce mot clé uniquement pour la version 1 ou 2c du SNMP. L'argument *community-string* spécifie l'identifiant de communauté de type mot de passe qui est envoyé avec la notification ou dans une demande du NMS. L'identifiant de communauté peut comporter un maximum de 32 caractères.

Le mot clé **version** définit la version de notification SNMP à la version 1, 2c ou 3 à utiliser pour l'envoi d'interruptions et l'acceptation des demandes (interrogation). La version par défaut est 1.

L'argument *username* spécifie le nom de l'utilisateur si vous utilisez la version 3 du SNMP.

La paire mot de passe-argument **user-list** *list_name* spécifie le nom de la liste d'utilisateurs.

La paire mot de passe-argument **udp-port** *port* précise que les alertes SNMP doivent être envoyées à un hôte NMS sur un port autre que par défaut et définit le numéro de port UDP de l'hôte NMS. Le port UDP par défaut est 162.

Supervision SNMP

Consultez les commandes suivantes pour superviser SNMP.

- **show running-config snmp-server** [**default**]

  Cette commande affiche tous les renseignements de configuration du serveur SNMP.

- **show running-config snmp-server group**

  Cette commande affiche les paramètres de configuration du groupe SNMP.

- **show running-config snmp-server host**

  Cette commande affiche les paramètres de configuration utilisés par SNMP pour contrôler les messages et les notifications envoyés aux hôtes distants.

- **show running-config snmp-server host-group**

  Cette commande affiche les configurations du groupe d'hôtes SNMP.

- **show running-config snmp-server user**

  Cette commande affiche les paramètres de configuration SNMP basés sur l'utilisateur.

- **show running-config snmp-server user-list**

  Cette commande affiche les configurations de la liste d'utilisateurs SNMP.

- **show snmp-server engineid**

  Cette commande affiche l'ID du moteur SNMP configuré.

- **show snmp-server group**

  Cette commande affiche les noms des groupes SNMP configurés. Si l'identifiant de communauté a déjà été configuré, deux groupes supplémentaires s'affichent par défaut dans la sortie. Ce comportement est normal.

- **show snmp-server statistics**

  Cette commande affiche les caractéristiques configurées du serveur SNMP. Pour réinitialiser tous les compteurs SNMP à zéro, utilisez la commande **clear snmp-server statistics**.

- **show snmp-server user**

  Cette commande affiche les caractéristiques configurées des utilisateurs.

Exemples

L'exemple suivant montre comment afficher les statistiques du serveur SNMP :

```
ciscoasa(config)# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

L'exemple suivant montre comment afficher la configuration en cours d'exécution du serveur SNMP :

```
ciscoasa(config)# show running-config snmp-server
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

Exemples de SNMP

La section suivante fournit des exemples que vous pouvez utiliser comme référence pour toutes les versions de SNMP.

SNMP versions 1 et 2c

L'exemple suivant montre comment l'ASA peut recevoir des requêtes SNMP de l'hôte 192.0.2.5 sur l'interface interne, mais n'envoie aucune demande de journal système SNMP à aucun hôte :

```
ciscoasa(config)# snmp-server host 192.0.2.5
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
ciscoasa(config)# snmp-server community ohwhatakeyisthee
```

SNMP version 3

L'exemple suivant montre comment l'ASA peut recevoir des requêtes SNMP en utilisant le modèle de sécurité SNMP version 3, qui nécessite que la configuration suive cet ordre précis : groupe, suivi de l'utilisateur, suivi de l'hôte :

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

Historique de SNMP

Tableau 7 : Historique de SNMP

Nom de la caractéristique	Version	Description
SNMP versions 1 et 2c	7.0(1)	Fournit des renseignements sur la supervision du réseau ASA et les événements en transmettant les données entre le serveur SNMP et l'agent SNMP par l'identifiant de communauté en texte clair.
SNMP version 3	8.2(1)	Fournit un chiffrement et une prise en charge 3DES ou AES pour SNMP version 3, la forme la plus sécurisée des modèles de sécurité pris en charge. Cette version vous permet de configurer les utilisateurs, les groupes et les hôtes, ainsi que les caractéristiques d'authentification à l'aide d'USM. En outre, cette version permet le contrôle d'accès à l'agent et aux objets MIB et comprend une prise en charge MIB supplémentaire. Nous avons ajouté ou modifié les commandes suivantes : **show snmp-server engineid**, **show snmp-server group**, **show snmp-server user**, **snmp-server group**, **snmp-server user**, **snmp-server host**.
Chiffrement de mot de passe	8.3(1)	Prend en charge le chiffrement de mot de passe. Nous avons modifié les commandes suivantes : **snmp-server community**, **snmp-server host**.
Alertes SNMP et MIB	v 8.4(1)	Prend en charge les mots clés supplémentaires suivants : **connection-limit-reached**, **cpu threshold rising**, **entity cpu-temperature**, **entity fan-failure**, **entity power-supply**, **ikev2 stop | start**, **interface-threshold**, **memory-threshold**, **nat packet-discard**, **warmstart**. Le tableau entPhysicalTable signale les entrées pour les capteurs, les ventilateurs, les alimentations et les composants connexes. Prend en charge les MIB supplémentaires suivantes : CISCO-ENTITY-SENSOR-EXT-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-PROCESS-MIB, CISCO-ENHANCED-MEMPOOL-MIB, CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB, DISMAN-EVENT-MIB, DISMAN-EXPRESSION-MIB, ENTITY-SENSOR-MIB, NAT-MIB. Prend en charge les interruptions supplémentaires suivantes : ceSensorExtThresholdNotification, clrResourceLimitReached, cpmCPURisingThreshold, mteTriggerFired, natPacketDiscard, warmStart. Nous avons introduit ou modifié les commandes suivantes : **snmp cpu threshold rising**, **snmp interface threshold**, **snmp-server enable traps**.
Prise en charge de l'OID IF-MIB ifAlias	8.2(5)/8.4(2)	L'ASA prend désormais en charge l'OID ifAlias. Lorsque vous parcourez l'IF-MIB, l'OID ifAlias sera défini à la valeur qui a été définie pour la description de l'interface.

Nom de la caractéristique	Version	Description
Module de services ASA (ASASM)	8.5(1)	L'ASASM prend en charge toutes les MIB et interruptions présentes dans 8.4(1), à l'exception des éléments suivants : MIB non prises en charge dans 8.5(1) : • CISCO-ENTITY-SENSOR-EXT-MIB (seuls les objets du groupe entPhySensorTable sont pris en charge). • ENTITY-SENSOR-MIB (seuls les objets du groupe entPhySensorTable sont pris en charge). • DISMAN-EXRPSION-MIB (seuls les objets des groupes expExpressionTable, expObjectTable et expValueTable sont pris en charge). Interruptions non prises en charge dans 8.5(1) : • ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB). Cette interruption est utilisée uniquement pour les défaillances d'alimentation, les défaillances de ventilateur et les événements de température élevée du processeur. • InterfacesBandwidthUtilization.
Interruptions SNMP	8.6(1)	Prend en charge les mots clés supplémentaires suivants pour les modèles ASA 5512-X, 5515-X, 5525-X, 5545-X et 5555-X : **entity power-supply-presence**, **entity power-supply-failure**, **entity chassis-temperature**, **entity chassis-fan-failure, entity power-supply-temperature**. Nous avons modifié la commande suivante : **snmp-server enable traps**.
MIB liées au VPN	9.0(1)	Une version mise à jour de CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB a été implementée pour prendre en charge la fonctionnalité de chiffrement de nouvelle génération. Les MIB suivantes ont été activées pour l'ASASM : • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
MIB TrustSec de Cisco	9.0(1)	La prise en charge de la MIB suivante a été ajoutée : CISCO-TRUSTSEC-SXP-MIB.
OID SNMP	9.1(1)	Cinq nouveaux OID de type prestataire physique SNMP ont été ajoutés pour prendre en charge les appareils ASA 5512-X, 5515-X, 5525-X, 5545-X et 5555-X.

Nom de la caractéristique	Version	Description
MIB NAT	9.1(2)	Ajout des OID cnatAddrBindNumberOfEntries et cnatAddrBindSessionCount pour prendre en charge les entrées xlate_count et max_xlate_count, qui sont équivalents à l'autorisation de l'interrogation à l'aide de la commande **show xlate count**.
Hôtes SNMP, groupes d'hôtes et listes d'utilisateurs	9.1(5)	Vous pouvez maintenant ajouter jusqu'à 4 000 hôtes. Le nombre de destinations d'interrogation actives prises en charge est de 128. Vous pouvez spécifier un objet réseau pour indiquer les hôtes individuels que vous souhaitez ajouter en tant que groupe d'hôtes. Vous pouvez associer plusieurs utilisateurs à un hôte. Nous avons introduit ou modifié les commandes suivantes : **snmp-server host-group**, **snmp-server user-list**, **show running-config snmp-server**, **clear configure snmp-server**.
Taille des messages SNMP	9.2(1)	La limite de taille des messages que SNMP envoie a été augmentée à 1 472 octets.
OID et MIB SNMP	9.2(1)	L'ASA prend désormais en charge l'OID cpmCPUTotal5minRev. L'ASA virtuel a été ajouté en tant que nouveau produit aux OID sysObjectID et entPhysicalVendorType de SNMP. Les fichiers CISCO-PRODUCTS-MIB et CISCO-ENTITY-VENDORTYPE-OID-MIB ont été mis à jour pour prendre en charge la nouvelle plateforme ASA virtuel. Une nouvelle MIB SNMP pour superviser l'utilisation des licences partagées des VPN a été ajoutée.
OID et MIB SNMP	9.3(1)	La prise en charge de CISCO-REMOTE-ACCESS-MONITOR-MIB (OID 1.3.6.1.4.1.9.9.392) a été ajoutée pour l'ASASM.
MIB et alertes SNMP	9.3(2)	Les fichiers CISCO-PRODUCTS-MIB et CISCO-ENTITY-VENDORTYPE-OID-MIB ont été mis à jour pour prendre en charge l'ASA 5506-X. L'ASA 5506-X a été ajouté en tant que nouveau produit aux tableaux d'OID sysObjectID et entPhysicalVendorType de SNMP. L'ASA prend désormais en charge CISCO-CONFIG-MAN-MIB, qui vous permet de faire les opérations suivantes : • Savoir quelles commandes ont été saisies pour une configuration en particulier. • Avertir le NMS lorsqu'une modification s'est produite dans la configuration d'exécution. • Suivez les horodatages associés à la dernière fois que la configuration d'exécution a été modifiée ou enregistrée. • Suivez les autres modifications apportées aux commandes, comme les détails du terminal et les sources de commandes. Nous avons modifié la commande suivante : **snmp-server enable traps**.

Nom de la caractéristique	Version	Description
MIB et alertes SNMP	9.4(1)	Les ASA 5506W-X, ASA 5506H-X, ASA 5508-X et ASA 5516-X ont été ajoutés en tant que nouveaux produits aux tableaux d'OID sysObjectID et entPhysicalVendorType de SNMP.
Hôtes d'interruption de serveur SNMP illimités par contexte	9.4(1)	L'ASA prend en charge un nombre illimité d'hôtes d'interruption de serveur SNMP par contexte. La sortie de la commande **show snmp-server host** affiche uniquement les hôtes actifs qui interrogent l'ASA, ainsi que les hôtes configurés de manière statique. Nous avons modifié la commande suivante : **show snmp-server host**.
Ajout de la prise en charge pour ISA 3000	9.4(1.225)	La gamme de produits ISA 3000 est désormais prise en charge pour SNMP. Nous avons ajouté de nouveaux OID pour cette plateforme. La commande **snmp-server enable traps entity** a été modifiée pour inclure une nouvelle variable *l1-bypass-status*. Cela active le changement d'état du contournement matériel. Nous avons modifié la commande suivante : **snmp-server enable traps entity**.
Prise en charge de cempMemPoolTable dans CISCO-ENHANCED-MEMPOOL-MIB	9.6(1)	Le tableau cempMemPoolTable de CISCO-ENHANCED-MEMPOOL-MIB est maintenant pris en charge. Il s'agit d'un tableau des entrées de surveillance de la réserve de mémoire pour toutes les entités physiques d'un système géré. **Remarque** CISCO-ENHANCED-MEMPOOL-MIB utilise des compteurs de 64 bits et prend en charge les rapports de mémoire sur les plateformes avec plus de 4 Go de RAM.
Prise en charge des MIB en mode d'horloge E2E transparent pour le protocole PTP (Precision Time Protocol)	9.7(1)	Les MIB correspondant au mode d'horloge E2E transparent sont maintenant prises en charge. **Remarque** Seules les opérations SNMP get, bulkget, getnext et walk sont prises en charge.

Nom de la caractéristique	Version	Description
SNMP sur IPv6	9.9(2)	L'ASA prend désormais en charge SNMP sur IPv6, y compris la communication avec des serveurs SNMP sur IPv6, permettant l'exécution de requêtes et d'interruptions sur IPv6 et prenant en charge les adresses IPv6 pour les MIB existantes. Nous avons ajouté les nouveaux objets MIB IPv6 SNMP suivants, comme décrit dans la RFC 8096. • ipv6InterfaceTable (OID : 1.3.6.1.2.1.4.30) : contient des renseignements spécifiques à IPv6 par interface. • ipAddressPrefixTable (OID :1.3.6.1.2.1.4.32) : comprend tous les préfixes appris par cette entité. • ipAddressTable (OID : 1.3.6.1.2.1.4.34) : contient des renseignements d'adressage pertinents pour les interfaces de l'entité. • ipNetToPhysicalTable (OID : 1.3.6.1.2.1.4.35) : contient le mappage des adresses IP aux adresses physiques. Commande nouvelle ou modifiée : **snmp-server host** **Remarque** La commande **snmp-server host-group** ne prend pas en charge IPv6.
Prise en charge de l'activation et de la désactivation des résultats de la mémoire libre et des statistiques de mémoire utilisée lors des opérations de marche SNMP	9.10(1)	Pour éviter la surutilisation des ressources du processeur, vous pouvez activer et désactiver la requête de mémoire libre et les statistiques de mémoire utilisée collectées par les opérations de marche de SNMP. Commande nouvelle ou modifiée : **snmp-server enable oid**
Prise en charge de l'activation et de la désactivation des résultats de la mémoire libre et des statistiques de mémoire utilisée lors des opérations de marche SNMP	9.12(1)	Pour éviter la surutilisation des ressources du processeur, vous pouvez activer et désactiver la requête de mémoire libre et les statistiques de mémoire utilisée collectées par les opérations de marche de SNMP. Nous n'avons pas modifié de commandes.
Authentification SNMPv3	9.14(1)	Vous pouvez maintenant utiliser le code HMAC SHA-256 pour l'authentification de l'utilisateur. Commandes nouvelles ou modifiées : **snmp-server user**
Pour les paires de basculements en version 9.14(1) ou toute version ultérieure, l'ASA ne partage plus les données du moteur client SNMP avec son homologue.	9.14(1)	L'ASA ne partage plus les données du moteur client SNMP avec son homologue.
Interrogation SNMP sur le VPN de site à site	9.14(2)	Pour une interrogation SNMP sécurisée sur un VPN de site à site, incluez l'adresse IP de l'interface externe dans la liste d'accès de la carte cryptographique dans le cadre de la configuration du VPN.

Nom de la caractéristique	Version	Description
La prise en charge des OID CISCO-MEMORY-POOL-MIB est rendue obsolète	9.15(1)	Les OID CISCO-MEMORY-POOL-MIB (ciscoMemoryPoolUsed, ciscoMemoryPoolFree) sont obsolètes pour les systèmes qui utilisent des compteurs de 64 bits. Le tableau cempMemPoolTable de CISCO-ENHANCED-MEMPOOL-MIB fournit des entrées de supervision de la réserve de mémoire pour les systèmes qui utilisent des compteurs de 64 bits.
Authentification SNMPv3	9.16(1)	Vous pouvez maintenant utiliser SHA-224 et SHA-384 pour l'authentification de l'utilisateur. Vous ne pouvez plus utiliser MD5 pour l'authentification de l'utilisateur. Vous ne pouvez plus utiliser DES pour le chiffrement. Commandes nouvelles ou modifiées : **snmp-server user**
SNMP sur IPv6	9.17(1)	La commande **snmp-server host-group** prend désormais en charge les objets d'hôte, de plage et de sous-réseau IPv6.
Prise en charge de l'interface de boucle avec retour pour SNMP	9.18(2)	Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour SNMP. Commandes nouvelles/modifiées : **interface loopback**, **snmp-server host**

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.