Configuration et dépannage du protocole SNMP dans SWA

Table des matières

Introduction

Ce document décrit les étapes de dépannage du protocole SNMP (Simple Network Monitoring Protocol) dans l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Accès à l'interface de ligne de commande (CLI) de SWA
- Accès administratif au SWA.

- Connaissances de base du protocole SNMP.

Composants utilisés

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

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

Fonctionnement de SNMP

SNMP est un protocole de communication de couche application qui permet aux périphériques réseau d'échanger des informations de gestion entre ces systèmes et avec d'autres périphériques extérieurs au réseau.

Grâce au protocole SNMP, les administrateurs réseau peuvent gérer les performances du réseau, détecter et résoudre les problèmes réseau et planifier la croissance du réseau.

Le protocole SNMP rend la surveillance du réseau plus rentable et permet à votre réseau d'être plus fiable. (Pour plus d'informations sur SNMP, consultez les documents RFC 1065, 1066 et 1067.)

Un réseau géré par SNMP se compose d'un gestionnaire, d'agents et de périphériques gérés.

- Le gestionnaire fournit l’interface entre le gestionnaire de réseau humain et le système de gestion.
- L'agent fournit l'interface entre le gestionnaire et le périphérique géré
- Les systèmes de gestion exécutent la plupart des processus de gestion et fournissent la majeure partie des ressources mémoire utilisées pour la gestion du réseau.

Un agent résidant sur chaque périphérique géré traduit les données d'informations de gestion locales (telles que les informations de performances ou les informations d'événements et d'erreurs) interceptées dans des déroutements logiciels, sous une forme lisible pour le système de gestion.

L'agent SNMP capture les données de la base MIB (Management Information Base) (référentiels de paramètres de périphérique et de données réseau) ou des déroutements d'erreurs ou de modifications.

MIB

La MIB est une structure de données qui décrit les éléments de réseau SNMP comme une liste d'objets de données. Le gestionnaire SNMP doit compiler le fichier MIB pour chaque type d'équipement du réseau afin de surveiller les périphériques SNMP.

Le gestionnaire et l'agent utilisent une MIB et un ensemble relativement petit de commandes pour échanger des informations. La MIB est organisée en une structure arborescente avec des

variables individuelles représentées sous forme de feuilles sur les branches.

Une longue balise numérique ou un identifiant d'objet (OID) permet de distinguer chaque variable de manière unique dans la base de données MIB et dans les messages SNMP. La MIB associe chaque OID à une étiquette lisible et à divers autres paramètres liés à l'objet.

La MIB sert ensuite de dictionnaire de données ou de livre de codes utilisé pour assembler et interpréter les messages SNMP.

Lorsque le gestionnaire SNMP souhaite connaître la valeur d'un objet, comme l'état d'un point d'alarme, le nom du système ou le temps de disponibilité de l'élément, il assemble un paquet GET qui inclut l'OID pour chaque objet d'intérêt.

L'élément reçoit la demande et recherche chaque OID dans son carnet de codes (MIB). Si l'OID est trouvé (l'objet est géré par l'élément), un paquet de réponse est assemblé et envoyé avec la valeur actuelle de l'objet inclus.

Si l'OID est introuvable, une réponse d'erreur spéciale est envoyée pour identifier l'objet non géré

Déroutement SNMP

Les déroutements SNMP permettent à un agent d'avertir la station de gestion des événements importants par le biais d'un message SNMP non sollicité.

SNMPv1 et SNMPv2c, ainsi que la MIB associée, encouragent la notification dirigée vers les déroutements.

L'idée derrière la notification dirigée par piège est que si un gestionnaire est responsable d'un grand nombre de périphériques, et que chaque périphérique a un grand nombre d'objets, il est peu pratique pour le gestionnaire d'interroger ou de demander des informations à chaque objet sur chaque périphérique.

La solution consiste à ce que chaque agent sur le périphérique géré informe le gestionnaire sans sollicitation. Pour ce faire, il envoie un message appelé « Trap of the event ».

Une fois l'événement reçu par le gestionnaire, ce dernier l'affiche et peut choisir d'effectuer une action en fonction de l'événement. Par exemple, le gestionnaire peut interroger directement l'agent ou interroger d'autres agents de périphérique associés pour mieux comprendre l'événement.

La notification dirigée par déroutement peut entraîner des économies substantielles en ressources réseau et d'agent en éliminant le besoin de requêtes SNMP frivoles. Cependant, il n'est pas possible d'éliminer totalement les interrogations SNMP.

Les requêtes SNMP sont requises pour la découverte et les modifications de topologie. En outre, un agent de périphérique géré ne peut pas envoyer de déroutement si le périphérique a subi une panne catastrophique.

Les déroutements SNMPv1 sont définis dans la RFC 1157, avec les champs suivants :

- Entreprise : identifie le type d'objet géré qui génère le déroutement.
- Agent address : fournit l'adresse de l'objet géré qui génère le déroutement.
- Type de déroutement générique : indique l'un des types de déroutement génériques.
- Specific trap code : indique l’un des codes d’interruption spécifiques.
- Time stamper : indique le temps écoulé entre la dernière réinitialisation du réseau et la génération du déroutement.
- Liaisons de variables : champ de données du déroutement qui contient l'unité de données de protocole. Chaque liaison de variable associe une instance d'objet MIB particulière à sa valeur actuelle.

SNMPv3

SNMPv3 prend en charge l'identificateur SNMP « Engine ID », identifiant de manière unique chaque entité SNMP. Des conflits peuvent se produire si deux entités SNMP ont des ID de moteur dupliqués.

EngineID est utilisé pour générer la clé des messages authentifiés. (Pour plus d'informations sur SNMPv3, consultez les documents RFC 2571-2575.)

De nombreux produits SNMP restent fondamentalement identiques sous SNMPv3, mais sont améliorés par ces nouvelles fonctionnalités :

Sécurité

- Authentification
- Confidentialité

Gestion

- Autorisation et contrôle d'accès
- Contextes logiques
- Nom des entités, identités et informations
- Personnes et politiques
- Gestion des noms d'utilisateur et des clés
- Destinations de notification et relations proxy
- Configuration à distance via des opérations SNMP

Les modèles de sécurité SNMPv3 se présentent principalement sous deux formes : authentification et chiffrement.

L'authentification permet de s'assurer que seul le destinataire visé lit les déroutements. Au fur et à mesure de leur création, les messages reçoivent une clé spéciale basée sur l'ID du moteur d'entité. La clé est partagée avec le destinataire prévu et utilisée pour recevoir le message. Encryption, privacy crypte la charge utile du message SNMP pour s'assurer que les utilisateurs

non autorisés ne peuvent pas le lire. Tout piège intercepté rempli de caractères confus et illisible. La confidentialité est particulièrement utile dans les applications où les messages SNMP doivent être routés sur Internet.
Il existe trois niveaux de sécurité dans un groupe SNMP :

noAuthnoPriv - Communication sans authentification ni confidentialité.
authNoPriv - Communication avec authentification et sans confidentialité. Les protocoles utilisés pour l'authentification sont l'algorithme Message-Digest 5 (MD5) et l'algorithme de hachage sécurisé (SHA).
authPriv - Communication avec authentification et confidentialité. Les protocoles utilisés pour l'authentification sont MD5 et SHA, et pour la confidentialité, les protocoles DES (Data Encryption Standard) et AES (Advanced Encryption Standard) peuvent être utilisés.

SNMP dans SWA

Le système d'exploitation AsyncOS prend en charge la surveillance de l'état du système via SNMP.

Remarque :

- SNMPisoff par défaut.
- Les opérations SNMPSET (configuration) ne sont pas implémentées.
- AsyncOS prend en charge SNMPv1, v2 et v3.
- L'authentification et le chiffrement des messages sont obligatoires lors de l'activation de SNMPv3. Les phrases de passe d'authentification et de chiffrement doivent être différentes.
- L'algorithme de chiffrement peut être AES (recommandé) ou DES.
- L'algorithme d'authentification peut être SHA-1 (recommandé) ou MD5.
- La commande nmpconfig « mémorise » vos phrases de passe lors de la prochaine exécution de la commande.
- Pour les versions d'AsyncOS antérieures à la version 15.0, le nom d'utilisateur SNMPv3 est : v3get.
- Pour AsyncOS version 15.0 et ultérieure, le nom d'utilisateur SNMPv3 par défaut est : v3get. En tant qu'administrateur, vous pouvez choisir n'importe quel autre nom d'utilisateur.
- Si vous utilisez uniquementSNMPv1 ouSNMPv2, vous devez définir une chaîne de communauté. La chaîne de communauté n'est pas publique par défaut.
- PourSNMPv1 etSNMPv2, vous devez spécifier un réseau à partir duquel les requêtes SNMP GET sont acceptées.
- Pour utiliser des déroutements, un gestionnaire SNMP (non inclus dans AsyncOS) doit être

en cours d'exécution et son adresse IP doit être entrée comme cible de déroutement. (Vous pouvez utiliser un nom d'hôte, mais si vous le faites, les déroutements ne fonctionnent que si le DNS fonctionne.)

Configuration de SNMPMonitor

Pour configurer le protocole SNMP afin de collecter des informations sur l'état du système pour l'appliance, utilisez la commande snmpconfig dans l'interface de ligne de commande. Après avoir choisi et configuré les valeurs d'une interface, l'appliance répond aux requêtes GET SNMPv3.

Lorsque vous utilisez SNMP, tenez compte des points suivants :

- Dans SNMP version 3, les requêtes doivent inclure une phrase de passe correspondante.
- Par défaut, les demandes des versions 1 et 2 sont rejetées.
- Si cette option est activée, les demandes des versions 1 et 2 doivent avoir une chaîne de communauté correspondante.

```
SWA_CLI> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP

Do you want to enable SNMP? [Y]> Y

Please choose an IP interface for SNMP requests.
1. Management (10.48.48.184/24 on Management: wsa125to15-man.amojarra.calo)
2. P1 (192.168.13.184/24 on P1: wsa1255p1.amojarra.calo)
3. P2 (192.168.133.184/24 on P2: wsa1255p2.amojarra.calo)
[1]> 1

Which port shall the SNMP daemon listen on?
[161]> 161

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2

Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2

Enter the SNMPv3 username or press return to leave it unchanged.
[w3get]> SNMPMUser

Enter the SNMPv3 authentication passphrase.
[]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[]>
```

```
Enter the SNMPv3 privacy passphrase.
[]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[]>
Service SNMP V1/V2c requests? [N]> N

Enter the Trap target as a host name, IP address or list of IP addresses
separated by commas (IP address preferred). Enter "None" to disable traps.
[10.48.48.192]>

Enter the Trap Community string.
[ironport]> swa_community

Enterprise Trap Status
1. CPUUtilizationExceeded       Enabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. connectivityFailure          Disabled
7. keyExpiration                Enabled
8. linkUpDown                   Enabled
9. memoryUtilizationExceeded    Enabled
10. updateFailure               Enabled
11. upstreamProxyFailure        Enabled
Do you want to change any of these settings? [N]> Y

Do you want to disable any of these traps? [Y]> N

Do you want to enable any of these traps? [Y]> Y

Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 6

Please enter the URL to check for connectivity failure, followed by the
checking interval in seconds, separated by a comma:
[http://downloads.ironport.com,5]>

Enterprise Trap Status
1. CPUUtilizationExceeded       Enabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. connectivityFailure          Enabled
7. keyExpiration                Enabled
8. linkUpDown                   Enabled
9. memoryUtilizationExceeded    Enabled
10. updateFailure               Enabled
11. upstreamProxyFailure        Enabled
Do you want to change any of these settings? [N]>

Enter the System Location string.
[location]>

Enter the System Contact string.
[snmp@localhost]>

Current SNMP settings:
Listening on interface "Management" 10.48.48.184/24 port 161.
```

```
SNMP v3: Enabled.
SNMP v3 UserName: SNMPMUser
SNMP v3 Authentication type: SHA
SNMP v3 Privacy protocol: AES
SNMP v1/v2: Disabled.
Trap target: 10.48.48.192
Location: location
System Contact: snmp@localhost

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>

SWA_CLI> commit
```

Fichiers MIB SWA

Les fichiers MIB sont disponibles à l'adresse URL suivante : https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html

Utilisez la dernière version de chaque fichier MIB.

Il existe plusieurs fichiers MIB :

- asyncoswebsecurityappliance-mib.txt est une description compatible SNMPv2 de la base de données MIB d'entreprise pour les appliances Web sécurisées.
- ASYNCOS-MAIL-MIB.txt est une description compatible SNMPv2 de la base MIB d'entreprise pour les appliances de sécurité de la messagerie.
- IRONPORT-SMI.txt Ce fichier « Structure of Management Information » définit le rôle de asyncoswebsecurityappliance-mib.

Cette version implémente un sous-ensemble en lecture seule de MIB-II tel que défini dans les RFC 1213 et 1907.

Seehttps://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.html pour en savoir plus sur la surveillance de l'utilisation du processeur sur le périphérique avec SNMP.

DÉROUTEMENT SNMP SWA

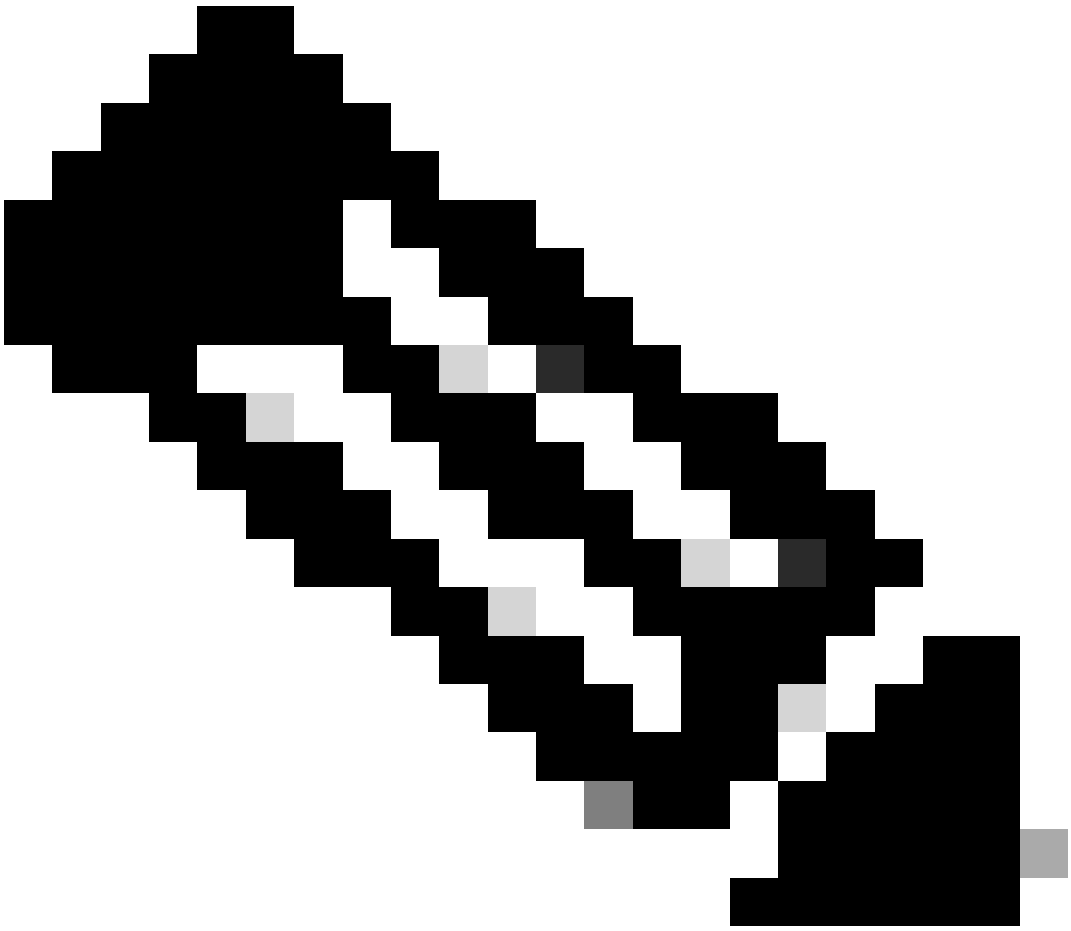
Le protocole SNMP permet d'envoyer des déroutements, ou notifications, pour informer une application d'administration lorsqu'une ou plusieurs conditions sont remplies.

Les déroutements sont des paquets réseau qui contiennent des données relatives à un composant du système qui envoie le déroutement.

Des déroutements sont générés lorsqu'une condition est remplie sur l'agent SNMP (dans ce cas, l'appliance Web CiscoSecure).

Une fois la condition remplie, l'agentSNMP forme alors un paquetSNMP et l'envoie à l'hôte exécutant le logiciel de console de gestionSNMP.

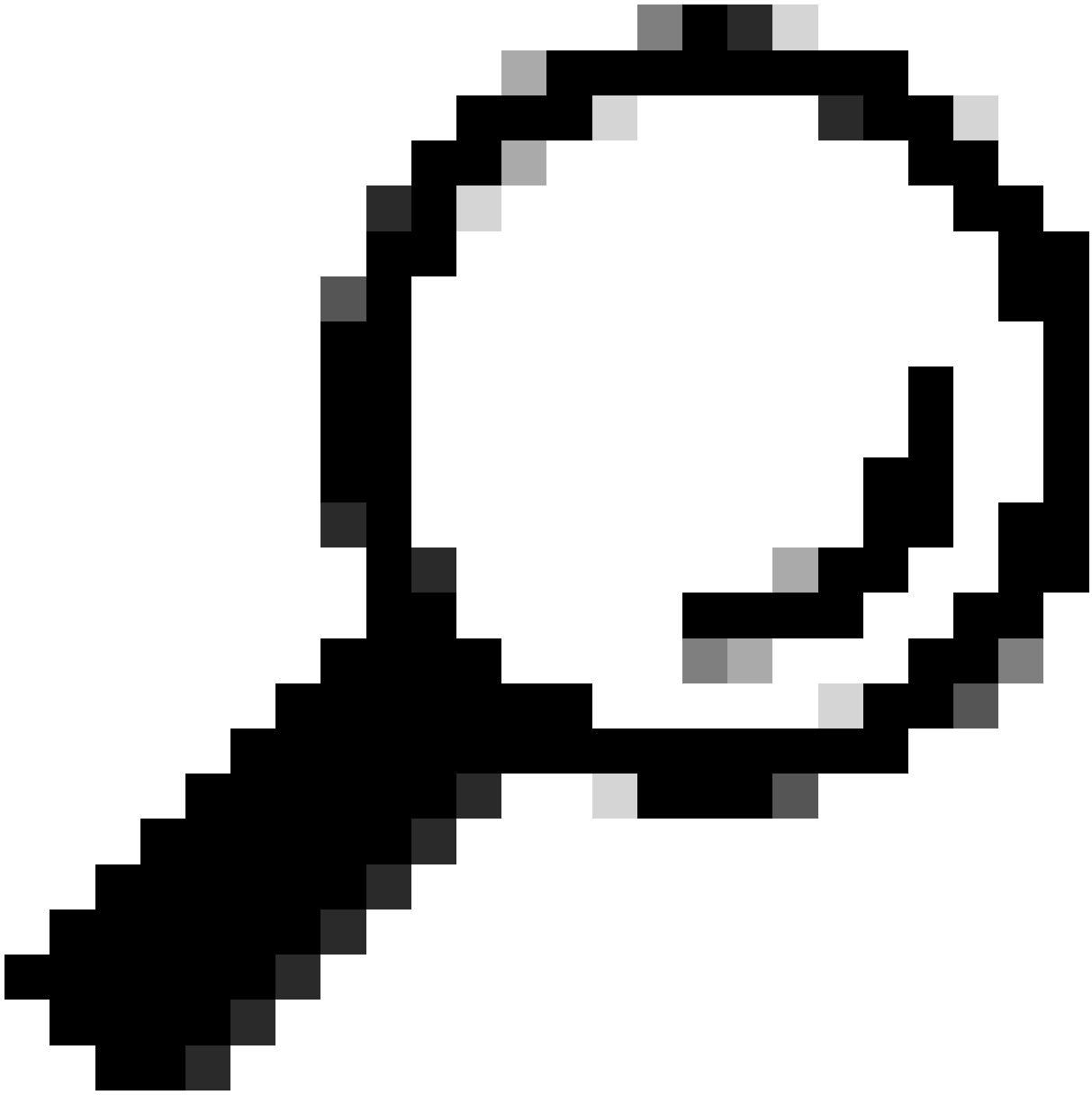
Vous pouvez configurer SNMPtraps (activer ou désactiver des déroutements spécifiques) lorsque vous activez SNMP pour une interface.



> Remarque : pour spécifier plusieurs cibles de déroutement : lorsque vous êtes invité à indiquer la cible de déroutement, vous pouvez saisir jusqu'à 10 adresses IP séparées par des virgules.

Le déroutement de défaillance de connectivité est destiné à surveiller la connexion de votre appliance à Internet. Pour ce faire, il tente de se connecter et d'envoyer une requête HTTP GET à un serveur externe unique toutes les 5 à 7 secondes. Par défaut, l'URL surveillée est downloads.ironport.com sur le port 80.

Pour modifier l'URL ou le port surveillé, exécutez la commande snmpconfig et activez l'interruption connectivityFailure, même si elle est déjà activée. Vous pouvez voir une invite pour modifier l'URL.



Conseil : pour simuler la connectivitéLes déroutements en cas d'échec, vous pouvez utiliser la commande CLI dnsconfig pour entrer un serveur DNS hors service. La recherche de downloads.ironport.com échoue et des déroutements sont envoyés toutes les 5 à 7 secondes. Veillez à remplacer le serveur DNS par un serveur opérationnel une fois le test terminé.

OID de surveillance recommandés

Il s'agit d'une liste des MIB recommandées à surveiller et non d'une liste exhaustive :

OID matériel	Nom
1.3.6.1.4.1.15497.1.1.1.18.1.3	IDraid
1.3.6.1.4.1.15497.1.1.1.18.1.2	ÉtatRaid

1.3.6.1.4.1.15497.1.1.1.18.1.4	raidLastError
1.3.6.1.4.1.15497.1.1.1.10	fanTable
1.3.6.1.4.1.15497.1.1.1.9.1.2	degrés Celsius

Il s'agit d'OID mappés directement à la sortie de la commandeCLI status detail :

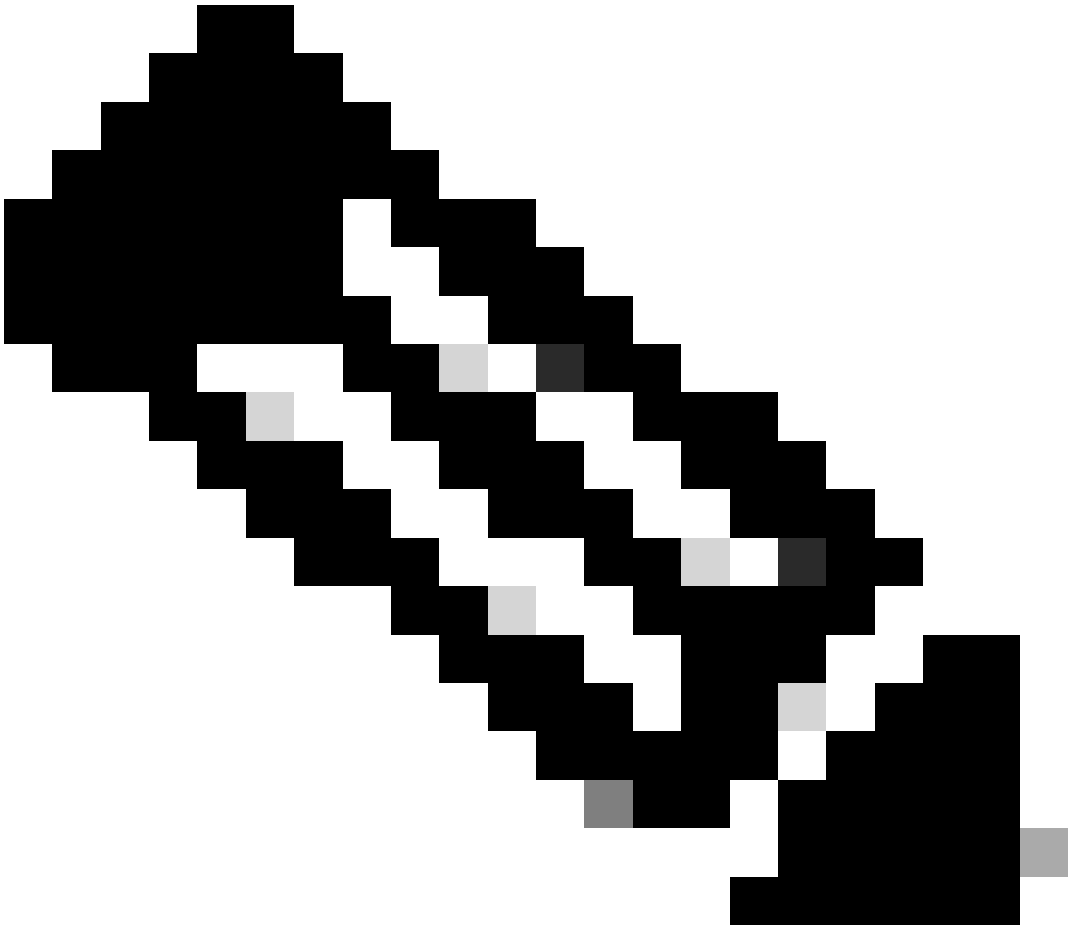
OID	Nom	Champ Détails du statut
Ressources système		
1.3.6.1.4.1.15497.1.1.1.2.0	PourcentageUtilisationUC	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	PourcentageUtilisationMémoire	BÉLIER
Transactions par seconde		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheDébitMaintenant	Nombre moyen de transactions par seconde au cours de la dernière minute.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheDébit1hPic	Nombre maximal de transactions par seconde au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheDébit1hMoyenne	Nombre moyen de transactions par seconde au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheDuréeDébitMaximale	Nombre maximal de transactions par seconde depuis le redémarrage du proxy.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheMoyenneDuréeDébit	Nombre moyen de transactions par seconde depuis le redémarrage du proxy.
Bande passante		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBwidthTotalMaintenant	Bande passante moyenne de la dernière minute.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hPic	Bande passante maximale au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hMoyenne	Bande passante moyenne au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBasseDuréeTotalePic	Bande passante maximale

		depuis le redémarrage du proxy.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBasseMoyenneDuréeTotale	Bande passante moyenne depuis le redémarrage du proxy.
Temps de réponse		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheHitsNow	Taux moyen d'accès au cache au cours de la dernière minute.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	Taux d'accès maximal au cache au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMean	Taux moyen d'accès au cache au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheNombreAtteintesMaximumVie	Taux de succès maximal du cache depuis le redémarrage du proxy.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheMoyenneDuréeRésultats	Taux moyen d'accès au cache depuis le redémarrage du proxy.
Taux de succès du cache		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheHitsNow	Taux moyen d'accès au cache au cours de la dernière minute.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	Taux d'accès maximal au cache au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMean	Taux moyen d'accès au cache au cours de la dernière heure.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheNombreAtteintesMaximumVie	Taux de succès maximal du cache depuis le redémarrage du proxy.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheMoyenneDuréeRésultats	Taux moyen d'accès au cache depuis le redémarrage du proxy.
Connexions		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientInactivitéConnexions	Connexions client inactives.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServeurConnexionsInactives	Connexions serveur inactives.

1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClientTotalConnexions	Nombre total de connexions client.
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheTotalConnexionsServeur	Nombre total de connexions serveur.

Dépannage du protocole SNMP

Pour afficher la connectivité entre SWA et votre gestionnaire SNMP, il est préférable de capturer les paquets, vous pouvez placer le filtre de capture de paquets sur : (port 161 ou port 162)



> Remarque : ce filtre est dû aux ports SNMP par défaut. Si vous avez modifié les ports, insérez les numéros de port configurés dans le filtre de capture de paquets.

Étapes de capture des paquets à partir de SWA :

Étape 1 : connexion à l'interface utilisateur graphique

Étape 2. en haut à droite, sélectionnez Assistance et aide

Étape 3 : sélectionnez Packet Capture

Étape 4. Sélectionnez Modifier les paramètres

Étape 5. Assurez-vous que l'interface sélectionnée est correcte

Étape 6. Saisissez les conditions du filtre.

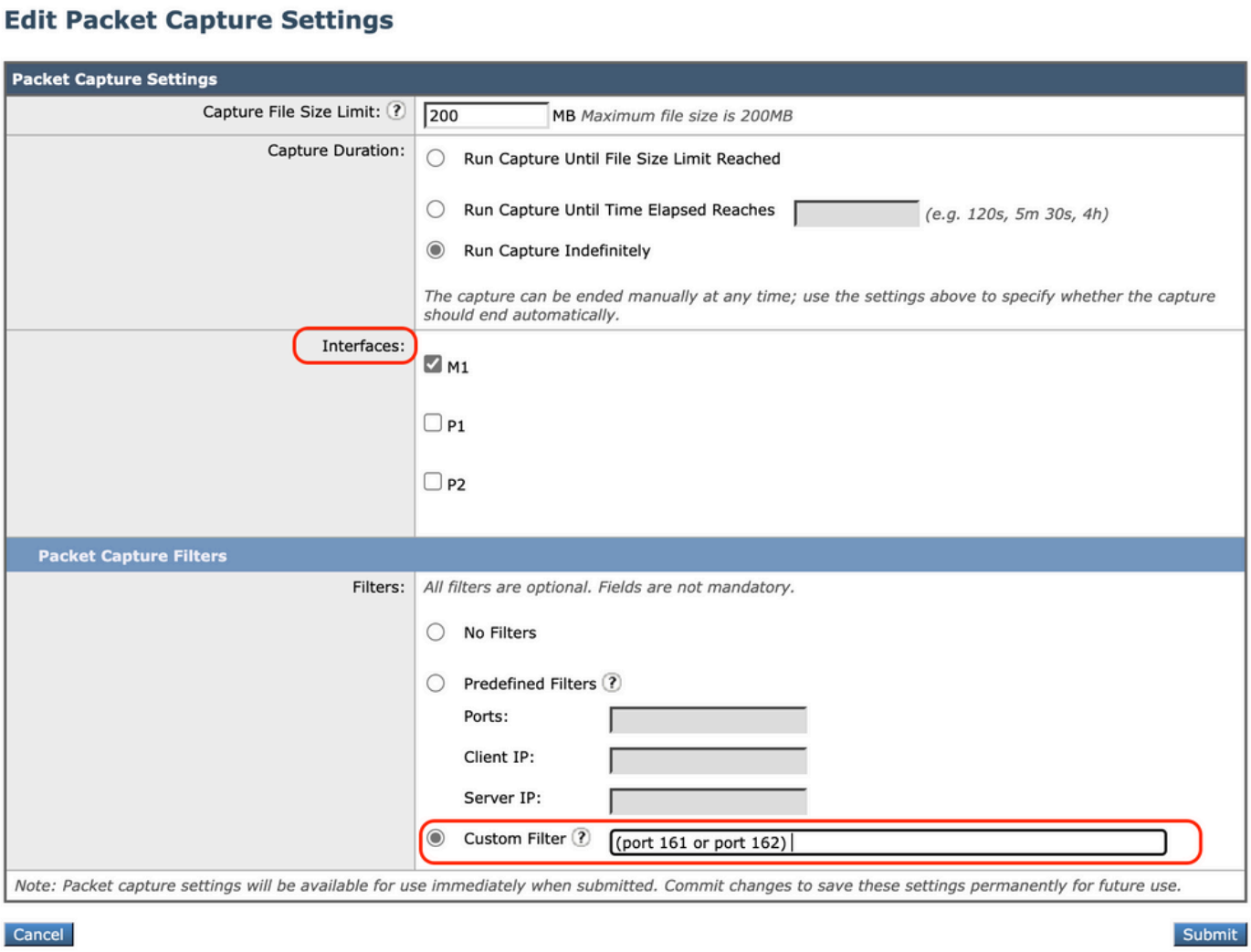
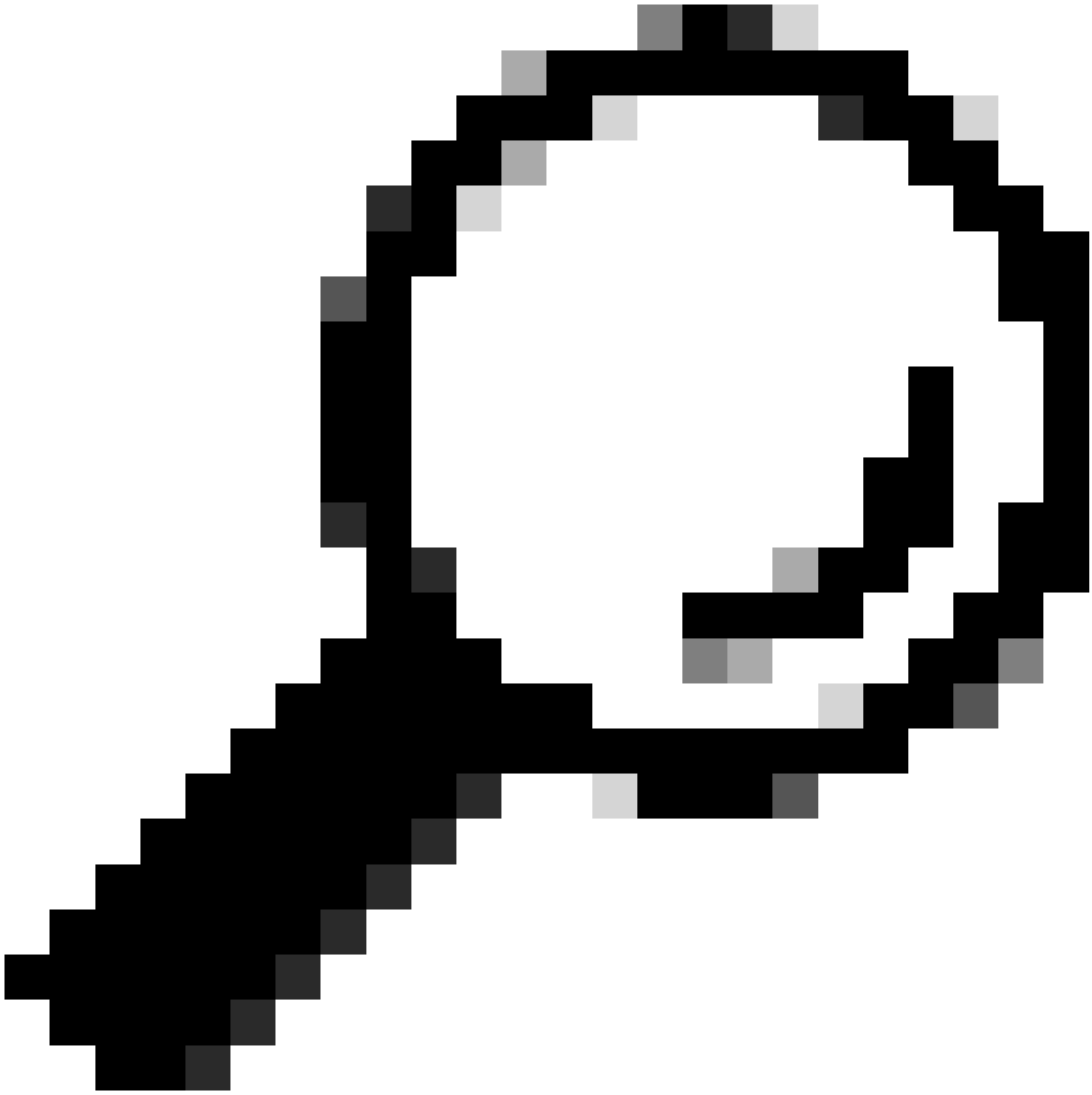


Image : configuration des filtres de capture de paquets

Étape 7. Cliquez sur Soumettre

Étape 8. Sélectionnez Démarrer la capture.



Conseil : vous pouvez déchiffrer les captures de paquets SNMPv3 avec Wireshark. Pour plus d'informations, consultez le lien suivant : [How-to-decrypt-snmpv3-packets-using-wireshark]

MARCHE RAPIDE

snmpwalk est le nom donné à une application SNMP qui exécute automatiquement plusieurs requêtes GET-NEXT. La requête SNMP GET-NEXT est utilisée pour interroger un périphérique activé et récupérer des données SNMP à partir d'un périphérique. La commande snmpwalk est utilisée parce qu'elle permet à l'utilisateur d'enchaîner des requêtes GET-NEXT sans avoir à entrer des commandes uniques pour chaque OID ou noeud dans une sous-arborescence

Installer SNMPWALK sur les systèmes d'exploitation Windows

Pour les utilisateurs de Microsoft Windows, vous devez d'abord télécharger l'outil.

Installer SNMPWALK sur le noyau Linux

```
#For Redhat, Fedora, CentOs:
yum install net-snmp-utils

#For Ubuntu:
apt-get install snmp
```

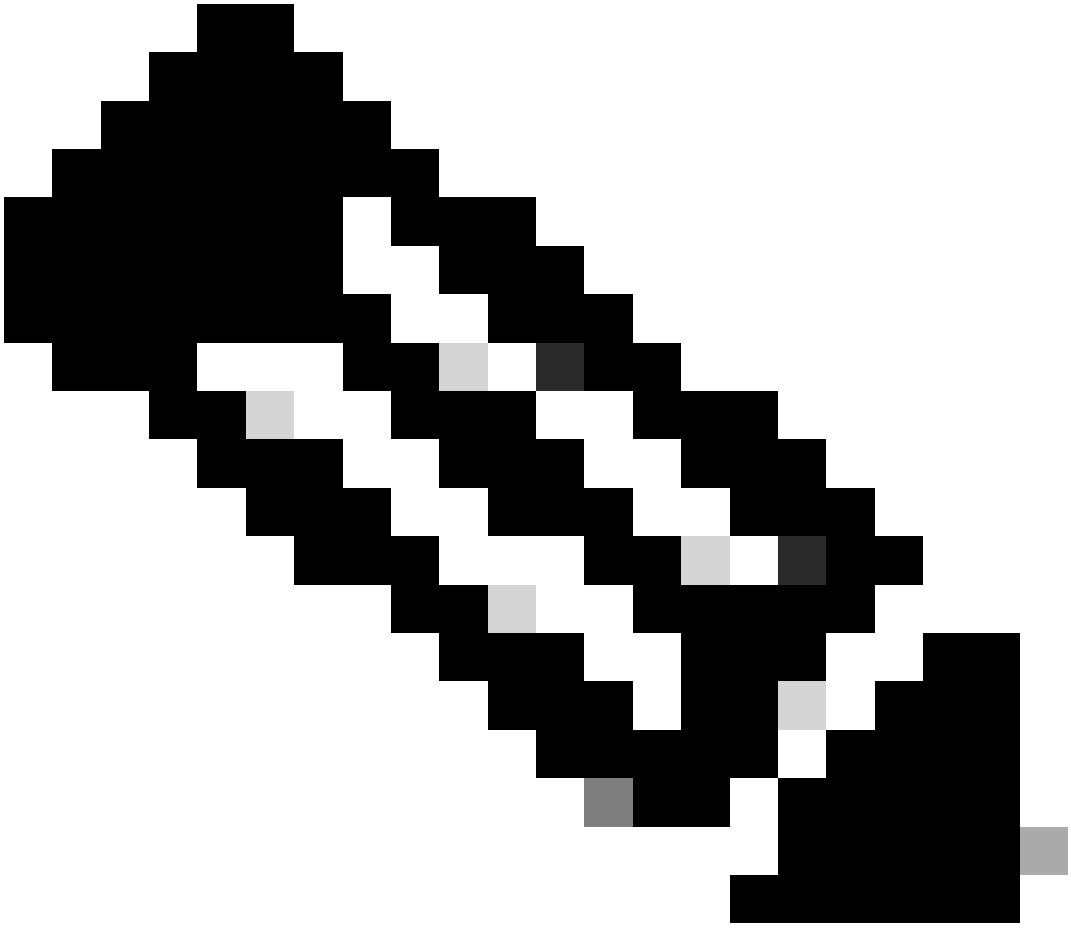
Installer SNMPWALK sur MacOS

Par défaut, snmpwalk est installé sur MacOS

Pour générer une requête GET SNMP, vous pouvez utiliser la commande snmpwalk à partir d'un autre ordinateur de votre réseau qui a une connectivité à SWA, voici quelques exemples de la commande snmpwalk :

```
snmpwalk -v2c -c <Community Name>  <SWA IP Address>

snmpwalk -v3 -l authPriv  -u v3get  -a SHA -A <Password>  -x AES -X <Password>  <SWA IP Address>
```



Remarque : vous pouvez définir le niveau de sécurité sur noAuthNoPriv ou authNoPriv ou authPriv en fonction de vos configurations SWA.

SNMPTRAP

snmptrap est une commande CLI masquée qui nécessitait l'activation de SNMP sur le SWA. Vous pouvez générer un déroutement SNMP en sélectionnant l'objet, et déroutement, voici un exemple :

```
SWA_CLI>nmptrap

1. CPUUtilizationExceeded
2. FIPSModeDisableFailure
3. FIPSModeEnableFailure
4. FailoverHealthy
5. FailoverUnhealthy
6. connectivityFailure
7. keyExpiration
```

```
8. linkUpDown
9. memoryUtilizationExceeded
10. updateFailure
11. upstreamProxyFailure
Enter the number of the trap you would like to send.
[]> 8

1. CPUUtilization
2. FIPSApplicationName
3. FailoverApplicationName
4. RAIDEvents
5. RAIDID
6. connectionURL
7. ifIndex
8. ip
9. keyDescription
10. memoryUtilization
11. raidStatus
12. updateServiceName
Enter the number of the object you would like to send.
[]> 8

Enter the trap value.
[]> 10.20.3.15

Enter the user name
[admin]> SNMPuser

Please select Trap Protocol version:
1. 2c
2. 3
[1]> 2
```

Journaux SNMP dans SWA

SWA a deux journaux associés à SNMP, Certains types de journaux associés au composant proxy Web ne sont pas activés. vous pouvez les activer à partir de :

- Dans l'interface GUI : Administration système > Inscriptions au journal
- Dans CLI : logconfig > new

Type de fichier journal	Description	Prend en charge Syslog Push ?	Activé par défaut ?
Journaux SNMP	Enregistre les messages de débogage relatifs au moteur de gestion de réseau SNMP.	Oui	Oui
Journaux du module SNMP	Enregistre les messages du proxy Web relatifs à l'interaction avec le système de surveillance	Non	Non

	SNMP.		

Problèmes courants avec SNMP

Certains OIDS échouent (aucune valeur ou valeur incorrecte).

Ce problème est lié à l'extraction SNMP. Voici deux exemples de sortie attendue et de sortie avec erreur :

```
Sample Output without Error:
$ snmpwalk -O a -v 3 -M "/var/lib/mibs/" -m "ALL" -l authPriv -a MD5 -x DES -u v3get -A xxx -X xxx prox
iso.3.6.1.4.1.15497.1.1.1.9.1.1.1 = INTEGER: 1
iso.3.6.1.4.1.15497.1.1.1.9.1.2.1 = INTEGER: 22
iso.3.6.1.4.1.15497.1.1.1.9.1.3.1 = STRING: "Ambient"

Sample Output with Error:
$ snmpwalk -O a -v 3 -M "/var/lib/mibs/" -m "ALL" -l authPriv -a MD5 -x DES -u v3get -A xxx -X xxx prox
iso.3.6.1.4.1.15497.1.1.1.9 = No Such Instance currently exists at this OID
```

Vous pouvez rechercher "Application Faults" dans snmp_logs

Vous pouvez vérifier snmp_logs à partir de CLI > grep > choisissez le numéro associé à snmp_logs :

```
SWA_CLI> grep

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "adc_logs" Type: "ADC Engine Logs" Retrieval: FTP Poll
...
37. "snmp_logs" Type: "SNMP Logs" Retrieval: FTP Poll
...
Enter the number of the log you wish to grep.
[]> 37

Enter the regular expression to grep.
[]>

Do you want this search to be case insensitive? [Y]>

Do you want to search for non-matching lines? [N]>

Do you want to tail the logs? [N]> y

Do you want to paginate the output? [N]>
```

Référence

Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance - LD (Limited Deployment) - Troubleshooting [Cisco Secure Web Appliance] - Cisco

Calcul de l'utilisation du CPU proxy sur le WSA à l'aide de SNMP - Cisco

snmpcmd(1) (freebsd)

snmptrap (freebsd)

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

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