Surveillance du WLC AireOS via SNMP avec OID

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Configuration des paramètres SNMP sur WLC
- Noms et ID d'objet (OID)
  - Que sont les noms d'objet et les OID
  - MIB et liste de tous les noms et ID d'objet sur les WLC Cisco
- Utilisation d'OID pour surveiller l'état du WLC
  - Surveillance via SNMPwalk
  - Surveillance via Python 3 et pysmnpLibrary
  - Intégration à des logiciels tiers (Grafana/PRTG Network Monitor/SolarWinds)
- Tableau des OID les plus fréquemment surveillés

Introduction

Ce document décrit comment configurer et surveiller SNMP sur le contrôleur LAN sans fil Cisco (WLC).

Conditions préalables

Exigences

Cisco vous recommande d'installer un outil SNMP (Simple Network Management Protocol) par défaut sur votre système d'exploitation ou sur votre base de connaissances.

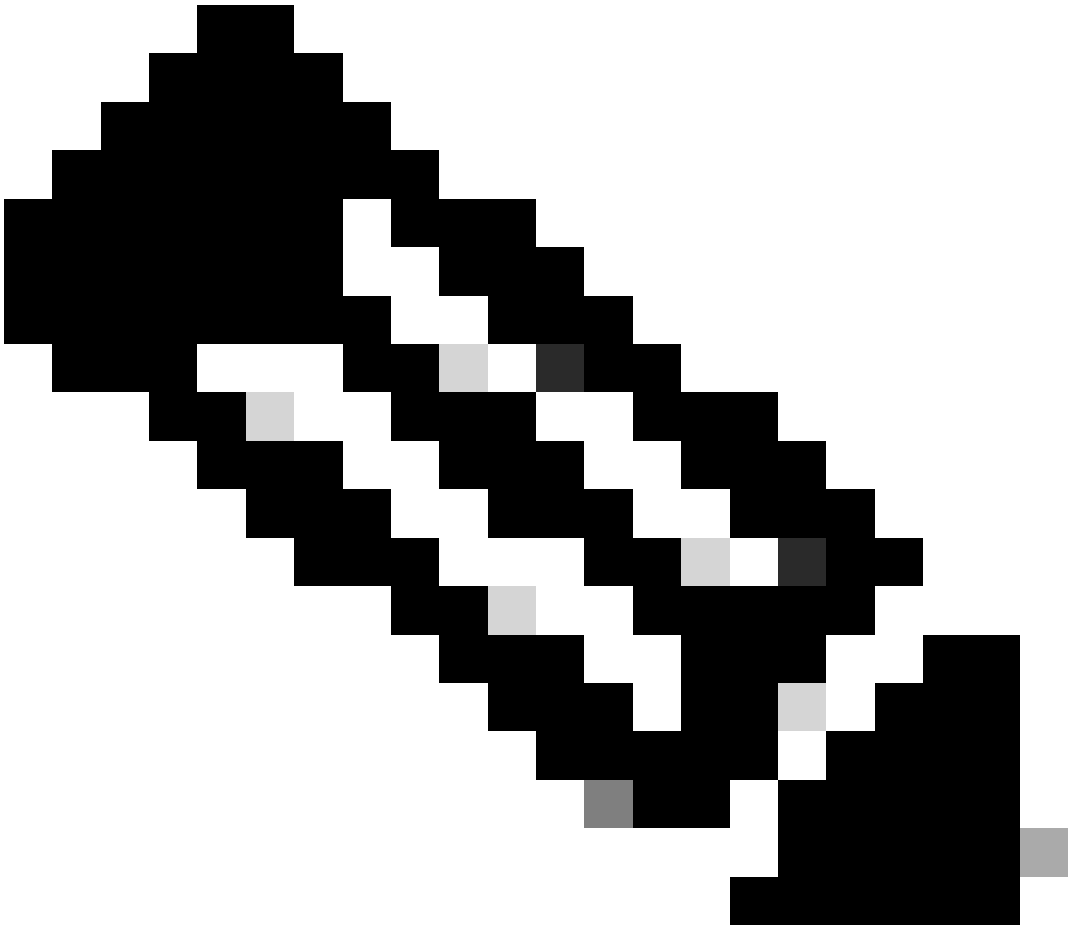
Composants utilisés

Ce document n'est pas limité à des versions logicielles et matérielles spécifiques. Tous les tests ont été effectués sur un WLC 3504 exécutant la version d'image 8.9 et MacOS 10.14. Les OID dans cet article sont également valides sur les versions antérieures d'AireOS et d'autres contrôleurs sans fil basés sur AireOS (8540/5508/5520/2504).

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.

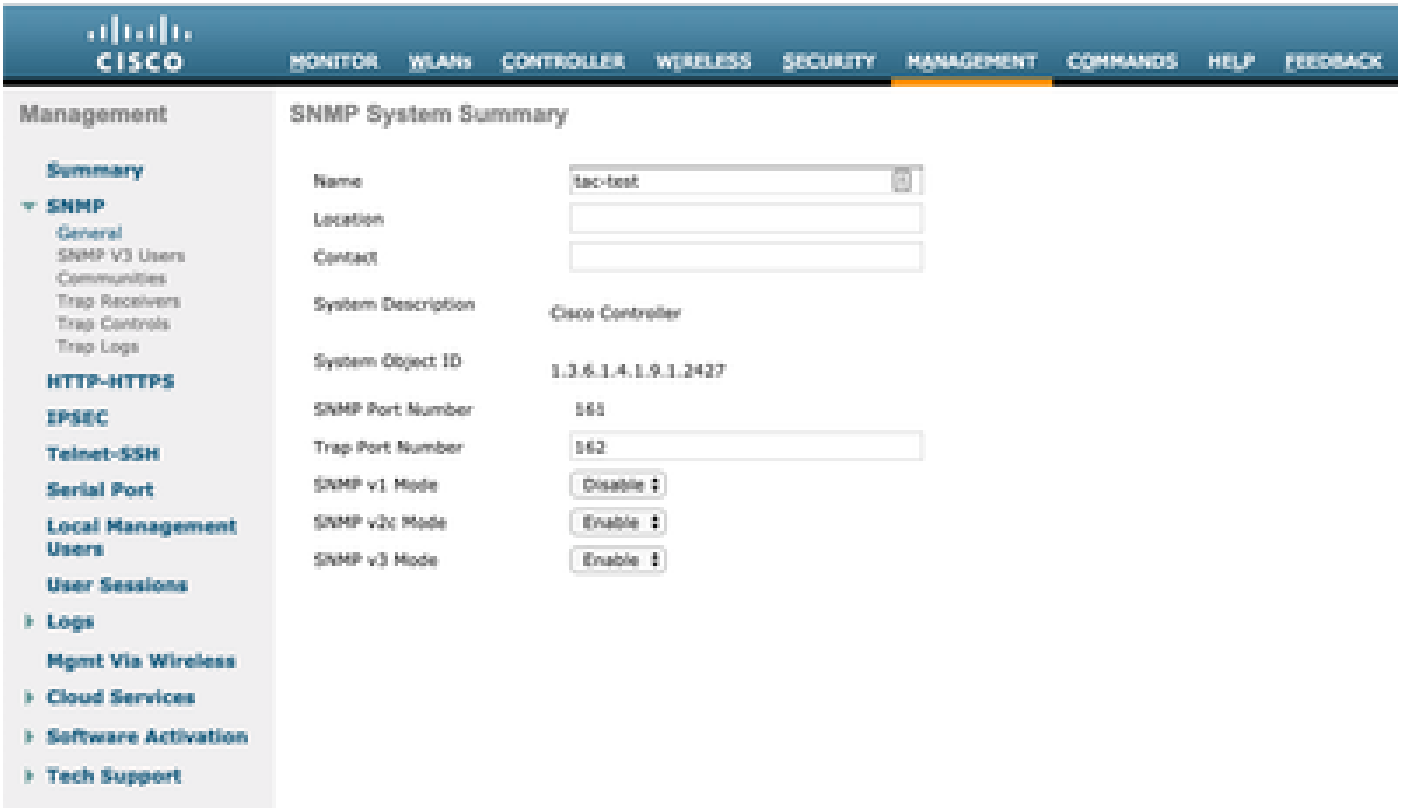
Configuration des paramètres SNMP sur WLC

SNMPv2c est une version communautaire de SNMP et toutes les communications entre les périphériques sont en texte clair. SNMPv3 est la version la plus sécurisée qui offre des contrôles d'intégrité des messages, l'authentification et le chiffrement des paquets. SNMPv1 est extrêmement obsolète, mais il existe toujours pour assurer la compatibilité des anciens logiciels.



> Remarque : Le protocole SNMPv2c est activé par défaut avec des privilèges de lecture et d'écriture pour la communauté privée et des privilèges de lecture seule pour la communauté publique. Il est recommandé de les supprimer et de créer une nouvelle communauté avec un nom différent.

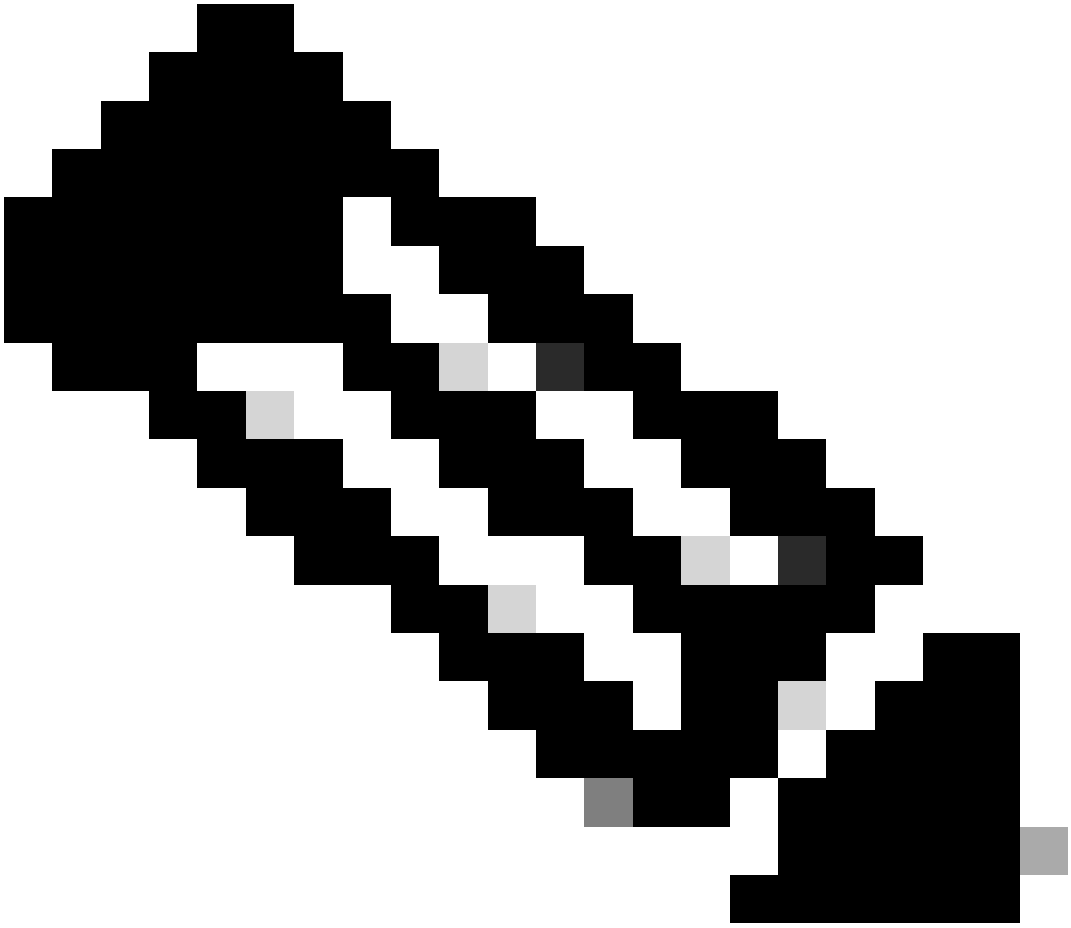
Dans cet article, seuls SNMPv2c et SNMPv3 sont utilisés. Connectez-vous à l'interface Web du contrôleur. Sous`Management > SNMP > General`ensure, activez la version souhaitée du protocole.



Dans le menu des communautés, toutes les communautés actuellement créées s'affichent.

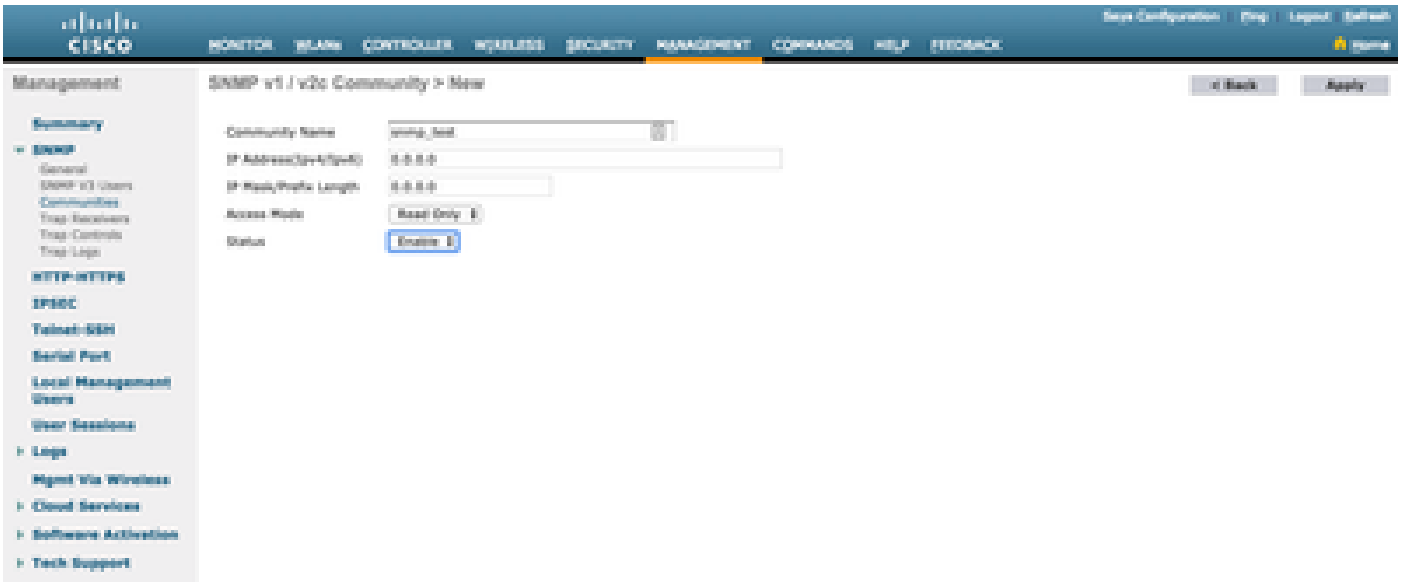


Il est recommandé de supprimer les communautés préconfigurées par défaut et d'en créer une nouvelle. L’adresse IP et le masque de réseau se comportent comme une liste d’accès. Par défaut, les deux sont définis sur 0.0.0.0, ce qui signifie que toutes les adresses IP sont autorisées à effectuer des requêtes SNMP pour cette communauté. Le champ de mode d'accès est laissé en lecture seule, car cette communauté doit être utilisée uniquement pour surveiller, et non pour la configuration du WLC.

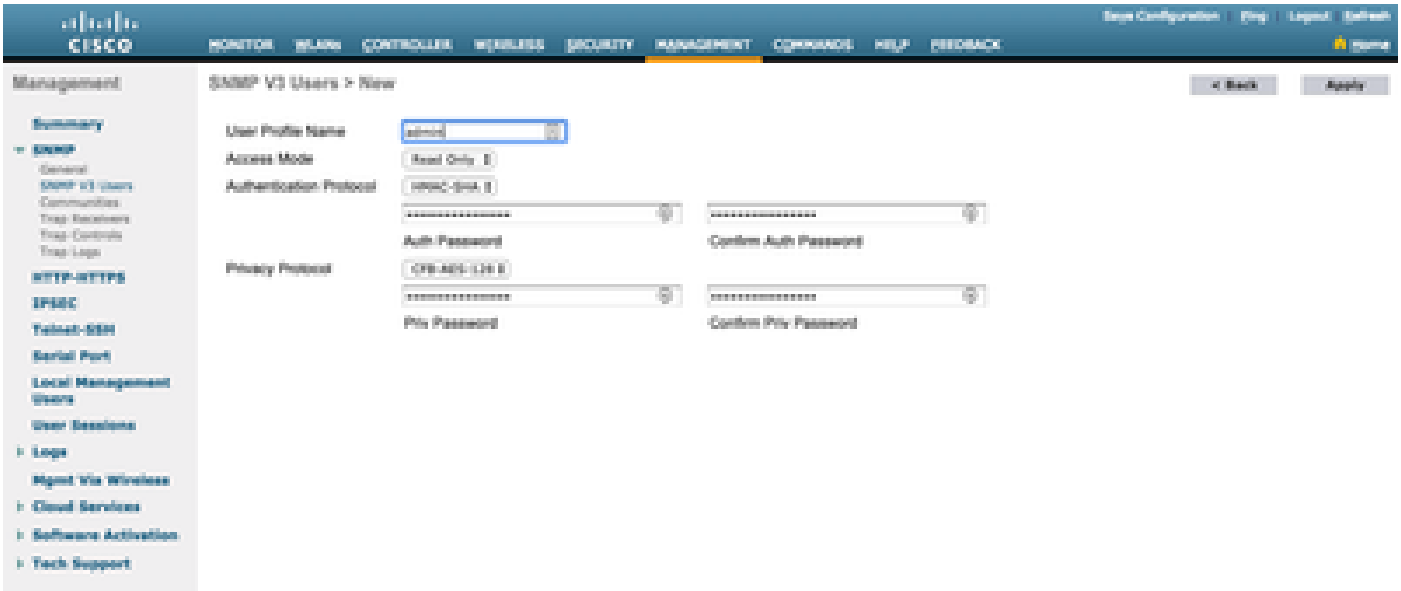


Remarque : Toutes les versions antérieures à 8.7.1.135 sont affectées par un ID de bogue Cisco CSCvg61933 où le masque de réseau ne peut pas être défini sur 255.255.255.255. Mettez à niveau le contrôleur vers la dernière version recommandée postérieure à 8.7.1.135 ou utilisez cette commande dans l'interface de ligne de commande pour créer une nouvelle communautéconfig snmp community ipaddr

.



Dans le menu SNMP V3 Users, vous pouvez voir tous les utilisateurs configurés, leurs privilèges et les protocoles utilisés pour l'authentification et le chiffrement. Le bouton Nouveau permet de créer un nouvel utilisateur. Il est recommandé de choisir HMAC-SHA comme protocole d'authentification et CFB-AES-128 comme protocole de confidentialité. Créez un utilisateur nommé admin avec le mot de passe d'authentification et de confidentialité défini surCisco123Cisco123.



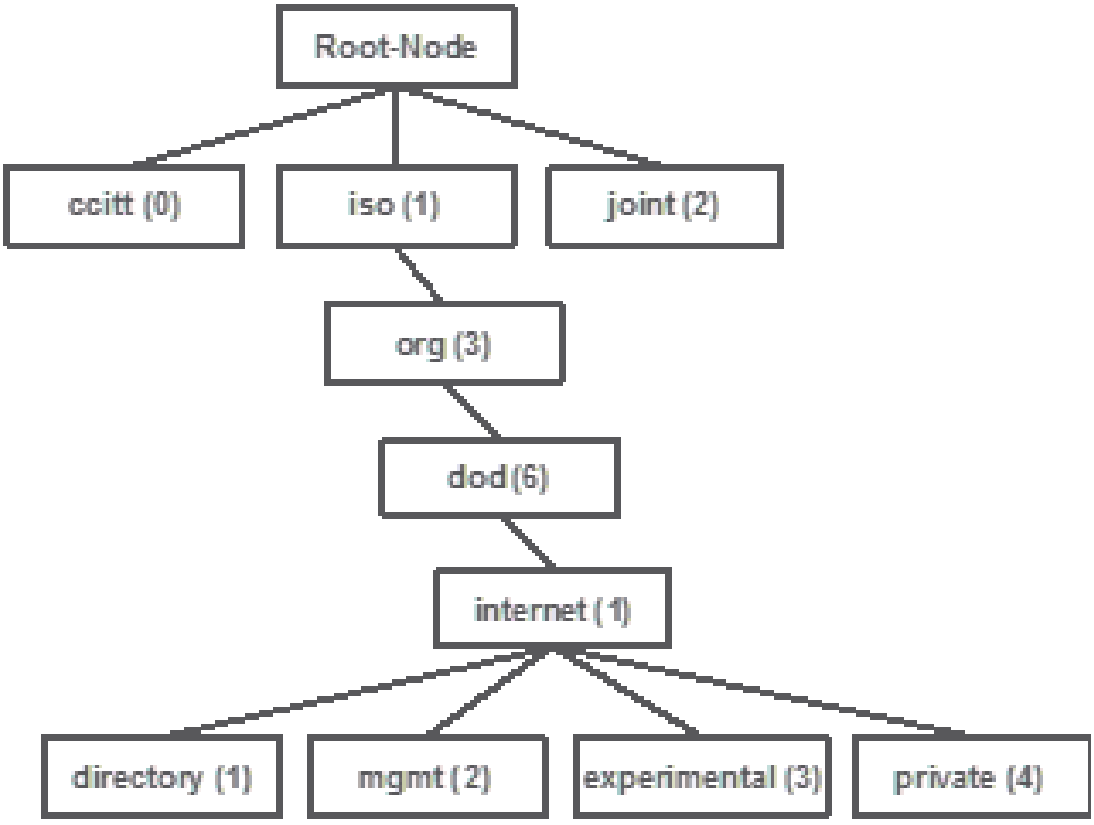
Noms et ID d'objet (OID)

Que sont les noms d'objet et les OID

Les OID sont des identificateurs uniques qui représentent une certaine variable ou un certain objet. Par exemple, l'utilisation actuelle du CPU est considérée comme une variable dont les valeurs peuvent être récupérées lorsque vous appelez leur ID d'objet. Chaque OID est unique et il ne doit pas y en avoir deux identiques dans le monde entier, tout à fait similaires à une adresse MAC. Ces identificateurs se trouvent dans une hiérarchie arborescente et chaque OID peut être retracé jusqu'à sa racine. Chaque fournisseur a sa propre branche après une racine commune.

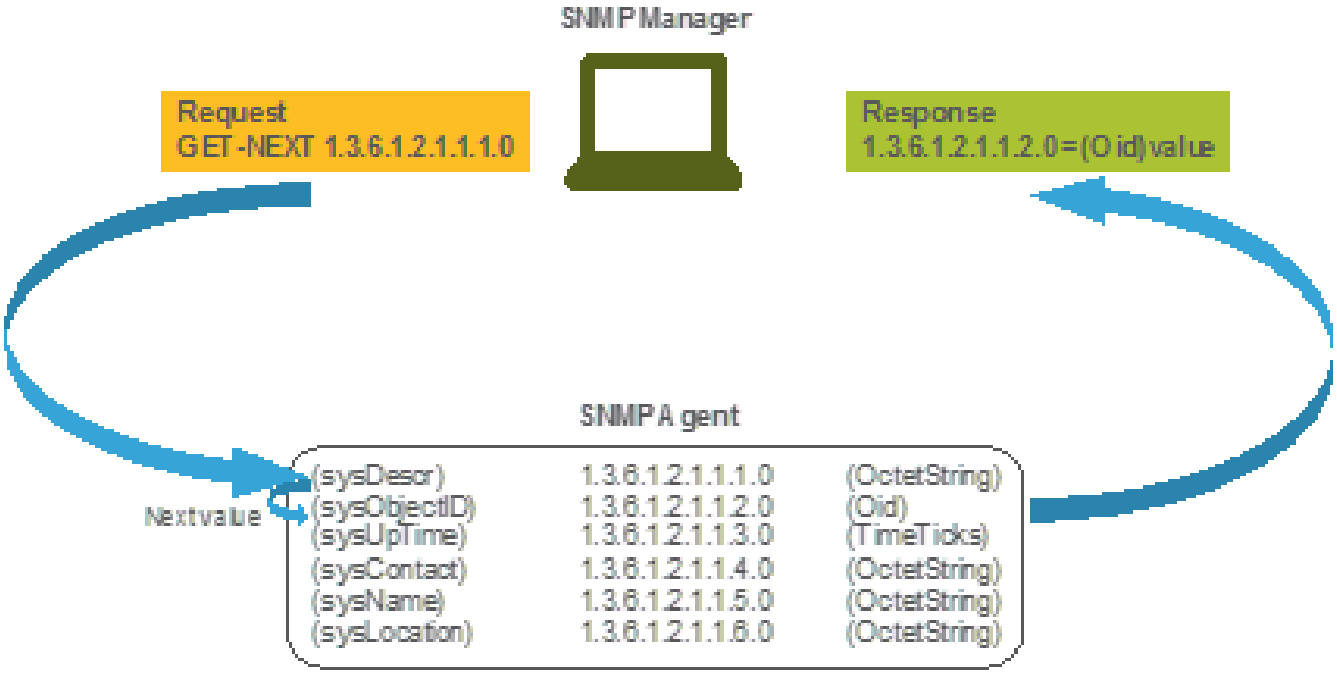
Une analogie peut être une adresse personnelle, où la racine est le pays ou l'état, puis un code postal de la ville, la rue et enfin le numéro de la maison.

Les nombres suivis d'un point représentent chaque étape nécessaire pour atteindre un certain point dans l'arbre ou la branche.



Toutes ces valeurs sont stockées dans une base d'informations de gestion (MIB) dans chaque périphérique réseau. Chaque identificateur possède un nom et une définition (plage de valeurs possibles, types, etc.).

Vous n'avez pas besoin de charger des MIB sur votre outil SNMP pour utiliser SNMP et interroger un périphérique, tant qu'un OID valide est connu. Le périphérique répond avec la valeur stockée dans la variable que l'OID représente. Par exemple, dans l'image affichée, le gestionnaire SNMP interroge l'agent SNMP d'un périphérique pour obtenir sa description système à l'aide de l'OID 1.3.6.1.2.1.1.1.0.



Si vous chargez la MIB dans votre outil de requête, vous pouvez l'utiliser pour traduire les numéros OID en noms et découvrir leurs définitions.

MIB et liste de tous les noms et ID d'objet sur les WLC Cisco

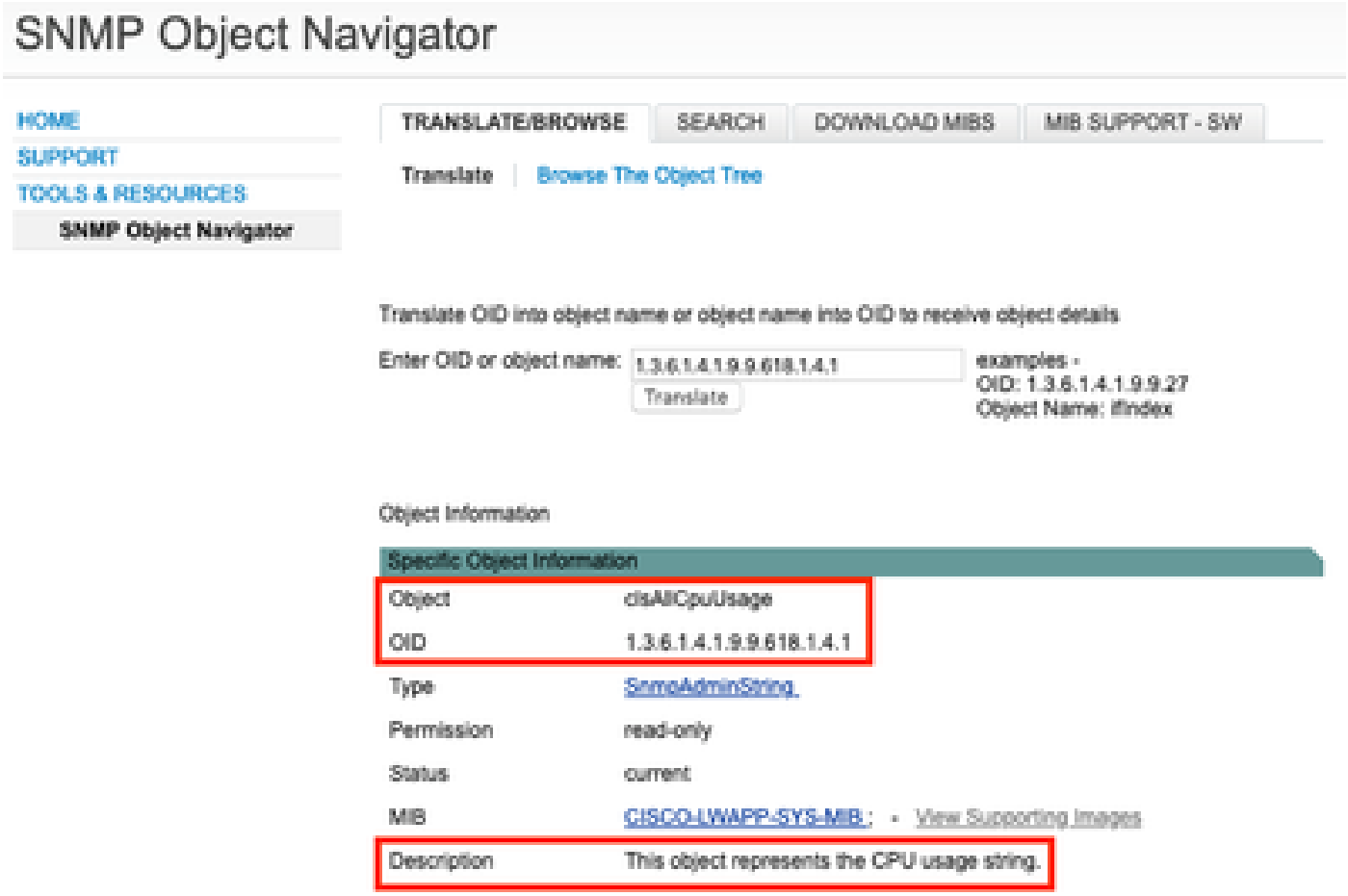
En mai 2019, il n'existe plus de tableau simple et convivial contenant chaque nom d'objet disponible et leurs OID respectifs pour les contrôleurs LAN sans fil. Cisco propose également la base MIB (Management Information Base), qui ne peut pas être facilement lisible, mais qui contient tous les noms d'objets disponibles et leur description. La base MIB WLC Cisco 3504 peut être téléchargée ici.

Le fichier d'archive téléchargé contient plusieurs fichiers texte .my qui peuvent être importés dans n'importe quel serveur de surveillance SNMP tiers ou simplement ouverts avec un éditeur de texte standard. Afin de trouver l'OID d'un nom d'objet spécifique, vous devez d'abord localiser le fichier exact qui le contient.

Par exemple, tous les objets liés à la surveillance de l'état physique du périphérique (comme la température et la vitesse du ventilateur) sont situés à l'intérieur d'une MIB appelée CISCO-ENVMON-MIB.my. Ici, ciscoEnvMonFanState est le nom d'objet qui est utilisé pour fournir l'état du ventilateur WLC. La syntaxe des fichiers MIB est indiquée. Les informations sur l'objet d'état de ventilateur sont les suivantes :

```
ciscoEnvMonFanState OBJECT-TYPE
        SYNTAX     CiscoEnvMonState
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The current state of the fan being instrumented."
        ::= { ciscoEnvMonFanStatusEntry 3 }
```

La plupart des logiciels de surveillance tiers reposent sur des OID et non sur des noms d'objet. La traduction entre le nom d'objet et l'ID d'objet peut être effectuée à l'aide de l'outil Cisco SNMP Object Navigator. Entrez le nom de l'objet dans la barre de recherche. Le résultat fournit l'OID et une brève description. En outre, le même outil peut être utilisé pour rechercher le nom d'objet correspondant de l'OID.



Utilisation d'OID pour surveiller l'état du WLC

Une fois que vous avez acquis l'OID de l'objet qui doit être surveillé, la première requête SNMP peut être exécutée. Ces exemples montrent comment acquérir une utilisation de CPU WLC par coeur (OID = 1.3.6.1.4.1.9.9.618.1.4.1) pour la communauté SNMPv2 et l'utilisateur SNMPv3, `snmp_test` avec le mot de passe d'authentification SHA et le mot de passe de confidentialité AES, `admin` avec le mot de passe d'authentification SHA, `Cisco123Cisco123` défini sur `Cisco123Cisco123` . L'interface de gestion du contrôleur se trouve sur 10.48.39.164.

Surveillance via SNMPwalk

SNMPwalk est une application SNMP qui utilise des requêtes SNMP GETNEXT pour interroger une entité réseau à la recherche d'une arborescence d'informations. Il est présent par défaut sur MacOS et la plupart des distributions Linux. Pour SNMPv2c, la commande présente la syntaxe suivante :

```
snmpwalk -v2c -c <community_name> <WLC_management_interface_ip> <OID>
```

Exemple :

```
VAPEROVI-M-H1YM:~ vaperovi$ snmpwalk -v2c -c snmp_test 10.48.39.164 1.3.6.1.4.1.9.9.618.1.4.1

SNMPv2-SMI::enterprises.9.9.618.1.4.1.0 = STRING: "0%/1%, 0%/1%, 0%/1%, 0%/1%"
```

Si SNMPv3 est utilisé, la commande a la syntaxe suivante :

```
snmpwalk -v3  -l authPriv -u <username> -a [MD5|SHA] -A <auth_password> -x [AES|DES] -X <priv_password>
```

Choisissez MD5/SHA et AES/DES en fonction de la façon dont vous avez créé l'utilisateur SNMPv3 sur le contrôleur.

Exemple :

```
VAPEROVI-M-H1YM:~ vaperovi$ snmpwalk -v3  -l authPriv -u admin -a SHA -A Cisco123Cisco123 -x AES -X Cis

SNMPv2-SMI::enterprises.9.9.618.1.4.1.0 = STRING: "0%/1%, 0%/1%, 0%/0%, 0%/1%"
```

Surveillance via Python 3 et la bibliothèque pysmnp

Ces extraits de code sont écrits en Python 3.7 et utilisent le `pysnmp` module (`pip install pysnmp`) pour faire des requêtes SNMP pour l'utilisation CPU du WLC Cisco 3504. Ces exemples utilisent la communauté SNMPv2 et l'utilisateur SNMPv3 créés dans l'un des chapitres précédents. Remplacez simplement les valeurs des variables et intégrez le code à vos propres scripts personnalisés.

Exemple SNMPv2c :

```
from pysnmp.hlapi import *

communityName = 'snmp_test'
ipAddress = '10.48.39.164'
OID = '1.3.6.1.4.1.14179.2.3.1.13.0'

errorIndication, errorStatus, errorIndex, varBinds = next(
    getCmd(SnmpEngine(),
           CommunityData(communityName),
```

```
           UdpTransportTarget((ipAddress, 161)),
           ContextData(),
           ObjectType(ObjectIdentity(OID)))
)

if errorIndication:
    print(errorIndication)
elif errorStatus:
    print('%s at %s' % (errorStatus.prettyPrint(),
                        errorIndex and varBinds[int(errorIndex) - 1][0] or '?'))
else:
    for varBind in varBinds:
        print(' = '.join([x.prettyPrint() for x in varBind]))
```

Sortie :

```
SNMPv2-SMI::enterprises.14179.2.3.1.13.0 = 73
```

Exemple SNMPv3 :

```
from pysnmp.hlapi import *

username = 'admin'
ipAddress = '10.48.39.164'
OID = '1.3.6.1.4.1.14179.2.3.1.13.0'
authKey = 'Cisco123Cisco123'
privKey = 'Cisco123Cisco123'

errorIndication, errorStatus, errorIndex, varBinds = next(
    getCmd(SnmpEngine(),
           UsmUserData(username, authKey, privKey,
                       authProtocol=usmHMACSHAAuthProtocol,
                       privProtocol=usmAesCfb128Protocol),
           UdpTransportTarget((ipAddress, 161)),
           ContextData(),
           ObjectType(ObjectIdentity(OID)))
)

if errorIndication:
    print(errorIndication)
elif errorStatus:
    print('%s at %s' % (errorStatus.prettyPrint(),
                        errorIndex and varBinds[int(errorIndex) - 1][0] or '?'))
else:
    for varBind in varBinds:
        print(' = '.join([x.prettyPrint() for x in varBind]))
```

Intégration à des logiciels tiers (Grafana/PRTG Network Monitor/SolarWinds)

L'infrastructure Cisco Prime permet de surveiller et de configurer facilement plusieurs

périphériques réseau, notamment des contrôleurs sans fil. Prime Infrastructure est livré préchargé avec tous les OID et l'intégration avec WLC consiste simplement en l'ajout des identifiants WLC à Prime. Après la synchronisation, il est possible de définir des alarmes et d'envoyer simultanément des modèles de configuration pour plusieurs contrôleurs sans fil.

D'autre part, Cisco WLC peut également être intégré à plusieurs solutions de surveillance tierces, à condition que les OID soient connus. Des programmes tels que Grafana, PRTG Network Monitor et le serveur SolarWinds permettent d'importer les MIB ou les OID et d'afficher les valeurs dans un graphique convivial.

Il peut être nécessaire de modifier les serveurs de surveillance pour prendre en charge cette intégration. Dans l'exemple représenté sur l'image, le serveur de surveillance PRTG est fourni avec l'OID d'utilisation de CPU par coeur qui renvoie la chaîne `0%/1%, 1%/1%, 0%/1%, 0%/1%`. PRTG attend une valeur entière et génère une erreur.

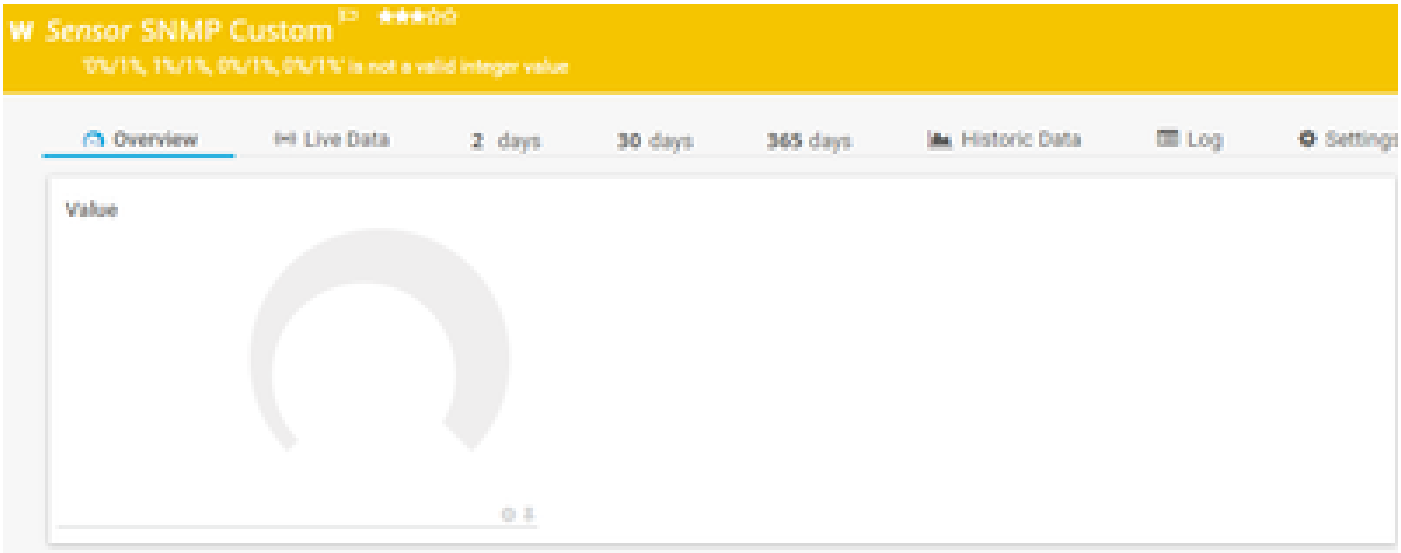


Tableau des OID les plus fréquemment surveillés

Si vous considérez que les MIB présentent les données dans une syntaxe non conviviale, ce tableau inclut certains des noms d'objet les plus courants et leurs OID que les clients Cisco utilisent.

Description	Nom d'objet	OID	Réponse attendue
Utilisation totale de l'UC en %	agentCPUUtilisationActuelle	1.3.6.1.4.1.14179.1.1.5.1.0	NOMBRE ENTIER : 0
Utilisation du processeur par coeur	clsAllCpuUsage	1.3.6.1.4.1.9.9.618.1.4.1.0	CHAÎNE : 0 %/1 %, 0 %/1 %, 0

			%/1 %, 0 %/1 %
Utilisation de la mémoire vive en %	clsSysCurrentMemoryUsage	1.3.6.1.4.1.9.9.618.1.8.6.0	Indicateur32 : 33
Température du processeur en °C	BsnSensorTemperature	1.3.6.1.4.1.14179.2.3.1.13.0	NOMBRE ENTIER : 76
Nombre de points d'accès joints	clsSysApConnectCount	1.3.6.1.4.1.9.9.618.1.8.4.0	Indicateur32 : 2
Nombre de clients	clsMaxClientsCount	1.3.6.1.4.1.9.9.618.1.8.12.0	Indicateur32 : 0
Nombre de clients par WLAN	bsnDot11EssNombreStationsMobiles	1.3.6.1.4.1.14179.2.1.1.1.38.0	Compteur32 : 3 Compteur32 : 2

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.