

Monitorar AireOS WLC via SNMP com OIDs

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar as definições de SNMP no WLC](#)

[Nomes de objetos e IDs de objetos \(OIDs\)](#)

[O que são nomes de objetos e OIDs](#)

[MIBs e lista de todos os nomes de objetos e IDs em Cisco WLCs](#)

[Uso de OIDs para monitorar o estado da WLC](#)

[Monitor via SNMPwalk](#)

[Monitoramento via Python 3 e pysmnpLibrary](#)

[Integração com software de terceiros \(Grafana/PRTG Network Monitor/SolarWinds\)](#)

[Tabela dos OIDs mais comumente monitorados](#)

Introdução

Este documento descreve como configurar e monitorar o SNMP no Cisco Wireless LAN Controller (WLC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha uma ferramenta SNMP (Simple Network Management Protocol) padrão em seu sistema operacional ou conhecimento para instalar uma.

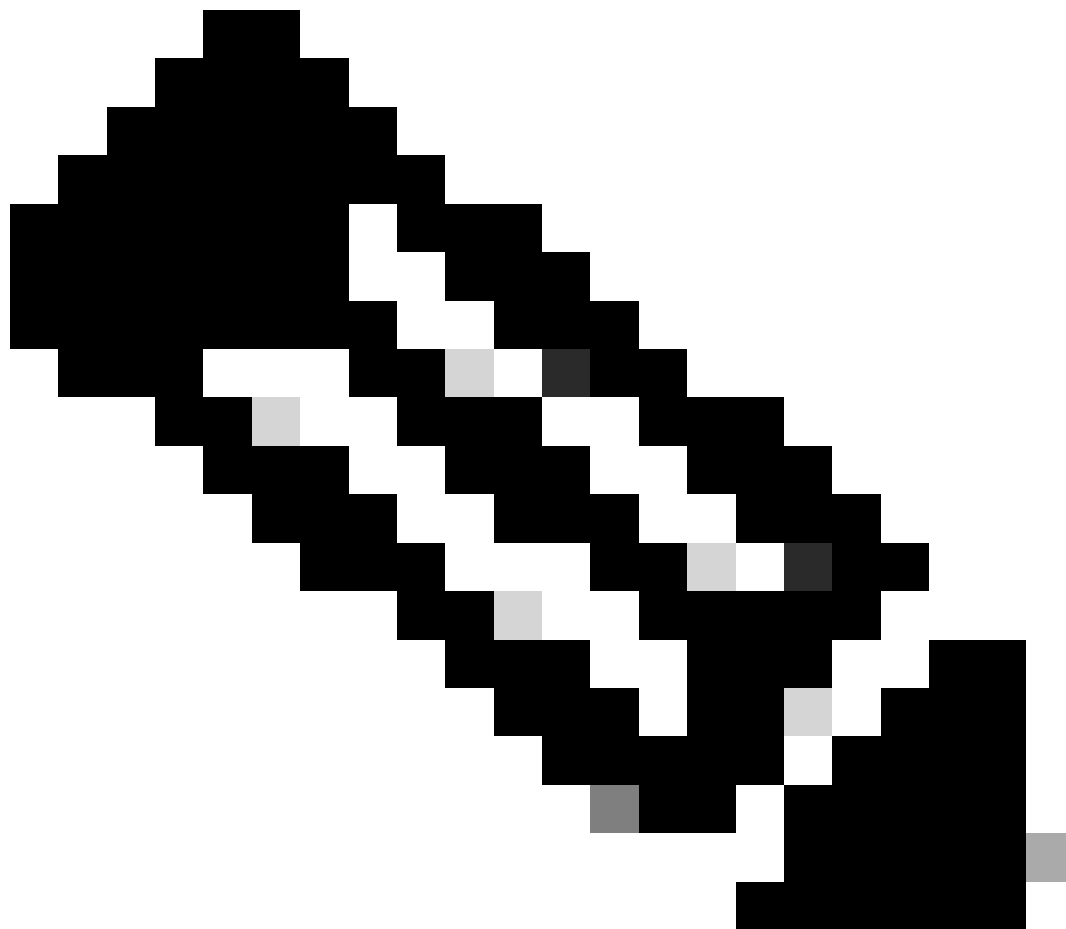
Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas. Todos os testes foram realizados em uma WLC 3504 executando a versão 8.9 e MacOS 10.14 da imagem. Os OIDs neste artigo também são válidos em versões anteriores do AireOS e outros controladores sem fio baseados no AireOS (8540/5508/5520/2504).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar as definições de SNMP no WLC

O SNMPv2c é uma versão baseada em comunidade do SNMP e toda a comunicação entre os dispositivos está em texto claro. O SNMPv3 é a versão mais segura que oferece verificações de integridade de mensagem, autenticação e criptografia dos pacotes. O SNMPv1 está extremamente desatualizado, mas ainda existe para fornecer compatibilidade de software herdado.



Observação: o SNMPv2c é habilitado por padrão com o privado da comunidade que tem privilégios de leitura e gravação, e o público da comunidade que tem privilégios somente leitura. É recomendável removê-los e criar uma nova comunidade com um nome diferente.

Neste artigo, somente SNMPv2c e SNMPv3 são usados. Efetue login na interface da Web do controlador. Em `Management > SNMP > General`, certifique-se de ativar a versão desejada do protocolo.

Management

- Summary
- SNMP
 - General
 - SNMP v3 Users
 - Communities
 - Trap Receivers
 - Trap Controls
 - Trap Logs
- HTTP-HTTPS
- IPSEC
- Telnet-SSH
- Serial Port
- Local Management Users
- User Sessions
- Logs
- Mgmt Via Wireless
- Cloud Services
- Software Activation
- Tech Support

SNMP System Summary

Name: tac-test

Location:

Contact:

System Description: Cisco Controller

System Object ID: 1.3.6.1.4.1.9.1.2437

SNMP Port Number: 161

Trap Port Number: 162

SNMP v1 Mode: Disable

SNMP v2c Mode: Enable

SNMP v3 Mode: Enable

No menu Comunidades, todas as comunidades criadas atualmente são exibidas.

Management

- Summary
- SNMP
 - General
 - SNMP v3 Users
 - Communities
 - Trap Receivers
 - Trap Controls
 - Trap Logs
- HTTP-HTTPS
- IPSEC
- Telnet-SSH
- Serial Port
- Local Management Users
- User Sessions
- Logs
- Mgmt Via Wireless
- Cloud Services
- Software Activation
- Tech Support

SNMP v1 / v2c Community

Apply Save...

Community Name	IP Address (ipv4/ipv6)	IP Mask/Prefix Length	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read-Only	Enable
private	0.0.0.0	0.0.0.0	Read-Write	Enable

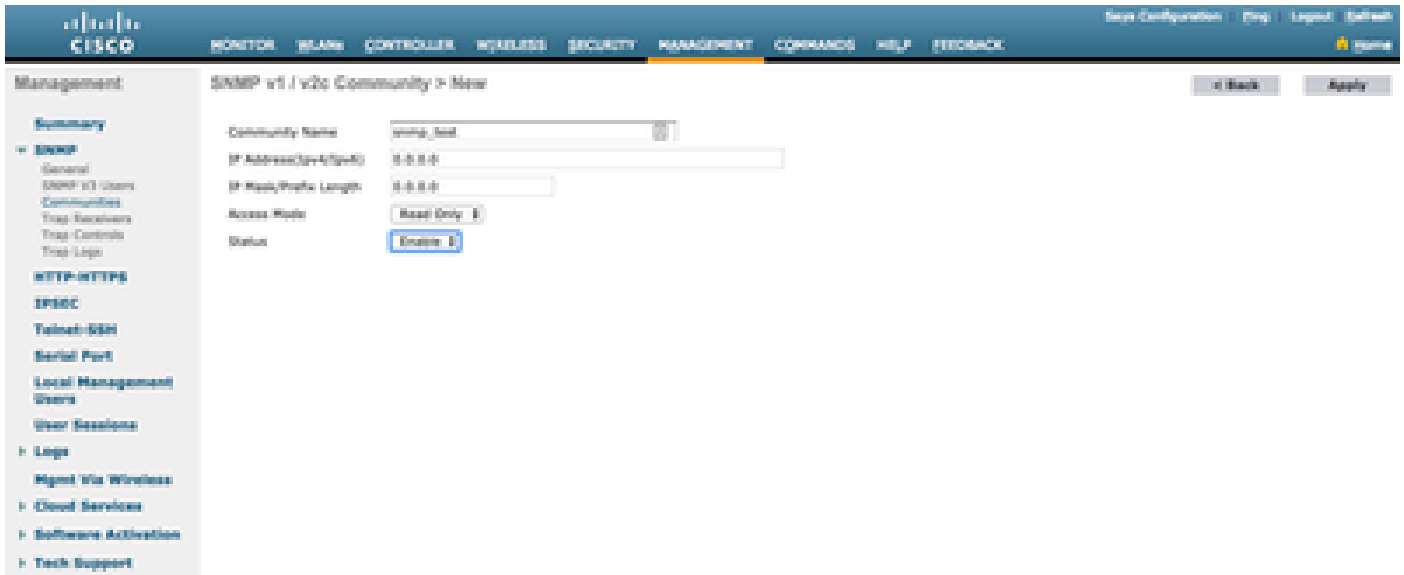
IPsec Parameters

IPsec: ○

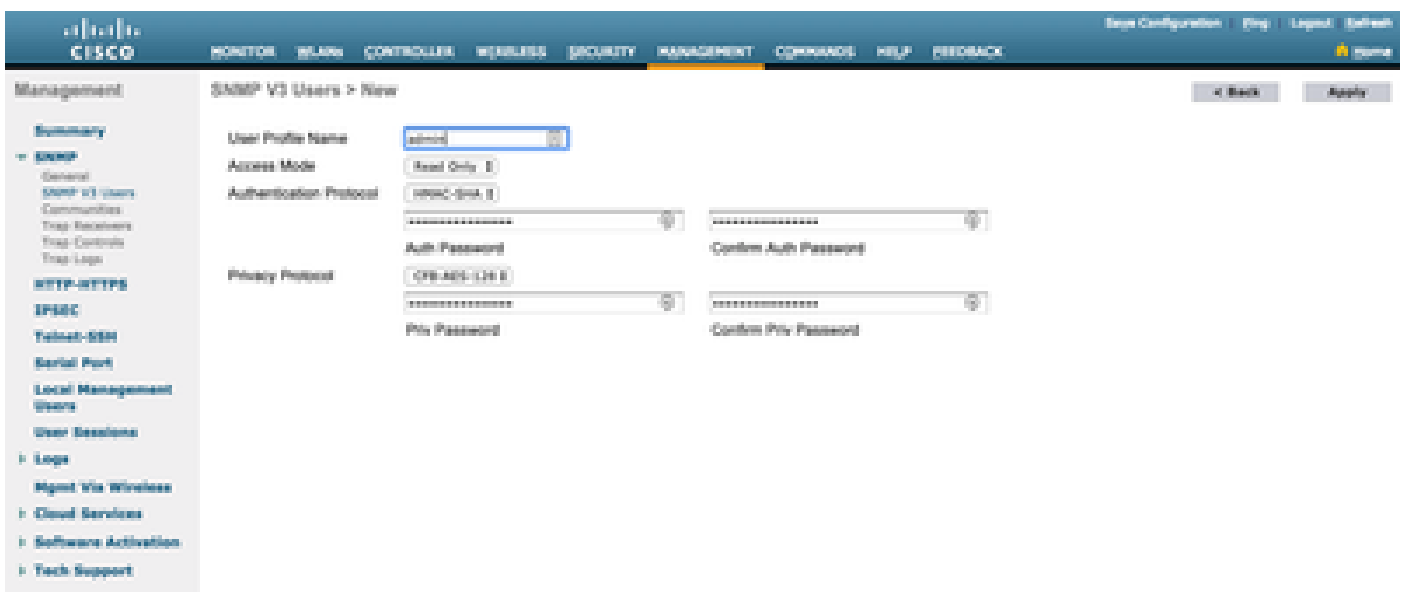
É uma prática recomendada remover comunidades pré-configuradas padrão e criar uma nova. O endereço IP e a máscara de rede comportam-se como uma lista de acesso. Por padrão, ambos são definidos como 0.0.0.0, o que significa que todos os endereços IP têm permissão para fazer consultas SNMP para essa comunidade. O campo do modo de acesso é deixado como somente leitura, pois essa comunidade deve ser usada somente para monitorar e não para a configuração da WLC.



Observação: todas as versões anteriores a 8.7.1.135 são afetadas por um bug da Cisco ID [CSCvg61933](#) onde a máscara de rede não pode ser definida como 255.255.255.255. Atualize o controlador para a versão recomendada mais recente, posterior à 8.7.1.135, ou use este comando na CLI para criar uma nova comunidade config snmp community ipaddr <ip_address> <netmask> <community_name>.



No menu SNMP V3 Users (Usuários do SNMP V3), você pode ver todos os usuários configurados, seus privilégios e protocolos usados para autenticação e criptografia. O botão Novo permite a criação de um novo usuário. É recomendável escolher o HMAC-SHA como protocolo de autenticação e o CFB-AES-128 como protocolo de privacidade. Crie um usuário chamado **admin** com a senha de autenticação e privacidade definida como Cisco123Cisco123.



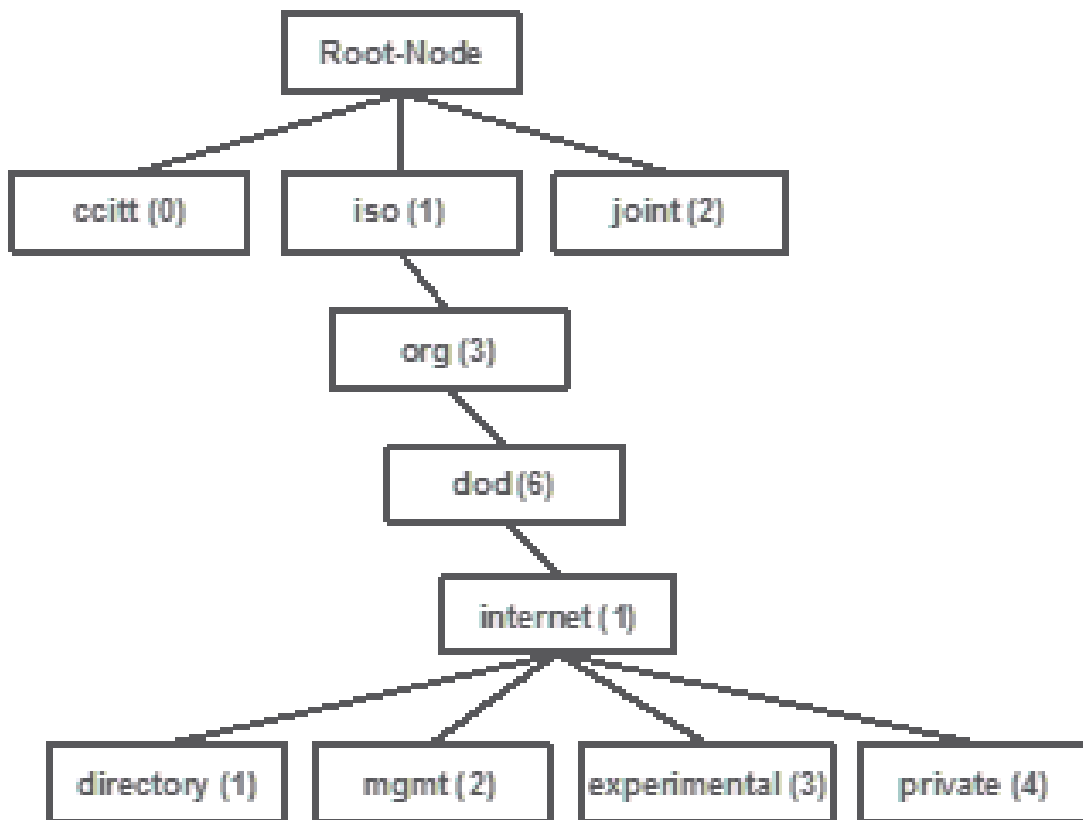
Nomes de objetos e IDs de objetos (OIDs)

O que são nomes de objetos e OIDs

OIDs são identificadores exclusivos que representam uma determinada variável ou objeto. Por exemplo, o uso atual da CPU é considerado uma variável cujos valores podem ser recuperados quando você chama seu ID de objeto. Cada OID é exclusivo e não deve haver dois iguais em todo o mundo, muito semelhante a um endereço MAC. Esses identificadores estão em uma hierarquia de árvore e cada OID pode ser rastreado até sua raiz. Cada fornecedor tem sua própria filial após uma raiz comum.

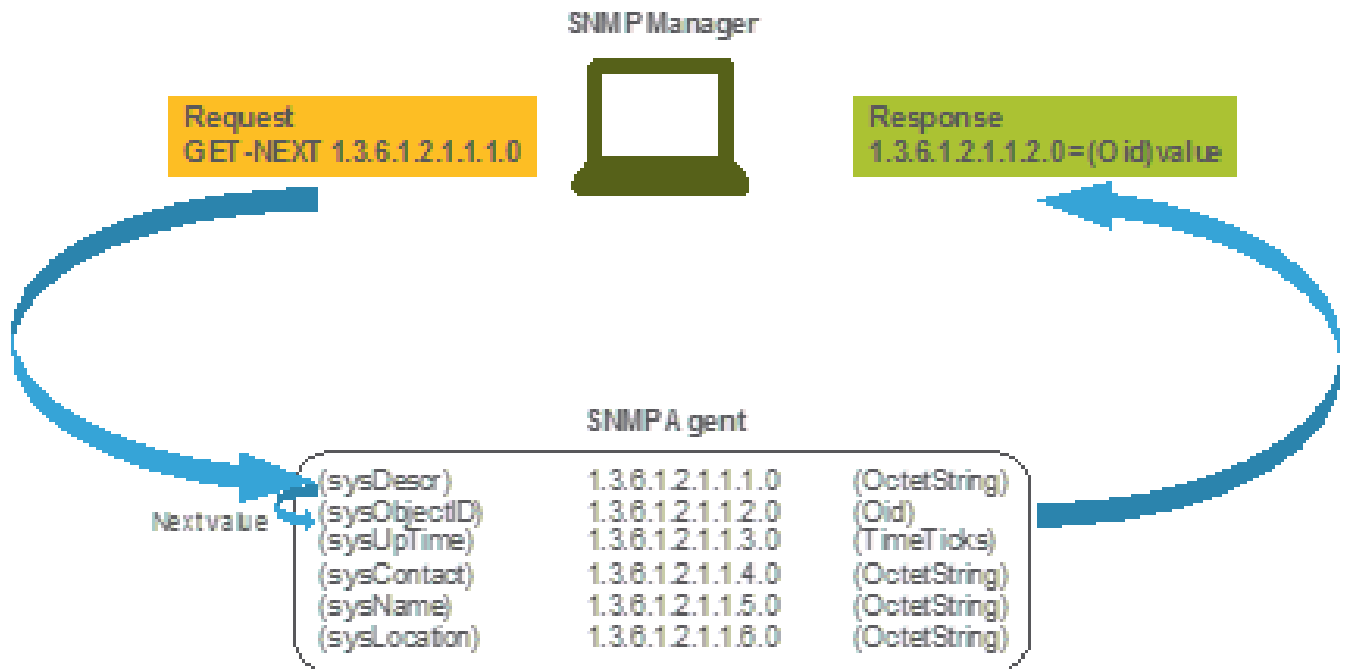
Uma analogia pode ser um endereço residencial, onde a raiz é o país ou o estado, depois um CEP da cidade, a rua e, finalmente, o número residencial.

Os números seguidos de um ponto representam cada etapa necessária para chegar a um certo ponto nessa árvore ou ramificação.



Todos esses valores são armazenados em uma base de informações de gerenciamento (MIB) em cada dispositivo de rede. Cada identificador tem um nome e uma definição (intervalo de valores possíveis, tipos e assim por diante).

Não é necessário carregar MIBs na ferramenta SNMP para usar o SNMP e consultar um dispositivo, desde que um OID válido seja conhecido. O dispositivo responde com o valor armazenado na variável que o OID representa. Por exemplo, na imagem mostrada, o gerenciador SNMP consulta o agente SNMP de um dispositivo para obter sua descrição do sistema com o uso do OID 1.3.6.1.2.1.1.1.0.



Se você carregar o MIB em sua ferramenta de consulta, poderá usá-lo para converter números OID em nomes e descobrir suas definições.

MIBs e lista de todos os nomes de objetos e IDs em Cisco WLCs

A partir de maio de 2019, não existe uma tabela simples e de fácil utilização que contenha cada nome de objeto disponível e seus respectivos OIDs para controladores de LAN sem fio. Como alternativa, a Cisco oferece a Base de Informações de Gerenciamento (MIB - Management Information Base), que não pode ser facilmente lida, mas contém todos os nomes de objetos disponíveis e suas descrições. O MIB do Cisco 3504 WLC pode ser baixado [aqui](#).

O arquivo morto baixado contém vários arquivos de texto .my que podem ser importados para qualquer servidor de monitoramento SNMP de terceiros ou simplesmente abertos com um editor de texto regular. Para localizar o OID de um nome de objeto específico, primeiro é necessário localizar o arquivo exato que o contém.

Por exemplo, todos os objetos relacionados à monitoração do estado físico do dispositivo (como temperatura e velocidade do ventilador) estão localizados dentro de uma MIB chamada CISCO-ENVMON-MIB.my. Aqui ciscoEnvMonFanState está o nome do objeto que é usado para fornecer o estado do ventilador da WLC. Os arquivos MIB têm a sintaxe mostrada. As informações sobre o objeto de estado do ventilador são semelhantes a:

ciscoEnvMonFanState OBJECT-TYPE SYNTAX CiscoEnvMonState MAX-ACCESS read-only STATUS current DESCRIPTION "The current state of th

A maioria dos softwares de monitoramento de terceiros depende de OIDs, e não de nomes de objetos. A conversão entre o nome do objeto e a ID do objeto pode ser feita com o uso da [ferramenta Cisco SNMP Object Navigator](#). Digite o nome do objeto na barra de pesquisa. A saída fornece o OID e uma breve descrição. Além disso, a mesma ferramenta pode ser usada para localizar o nome de objeto correspondente do OID.

SNMP Object Navigator

[HOME](#)

[SUPPORT](#)

[TOOLS & RESOURCES](#)

SNMP Object Navigator

[TRANSLATE/BROWSE](#)

[SEARCH](#)

[DOWNLOAD MIBS](#)

[MIB SUPPORT - SW](#)

[Translate](#) | [Browse The Object Tree](#)

Translate OID into object name or object name into OID to receive object details

Enter OID or object name:

examples -
OID: 1.3.6.1.4.1.9.9.27
Object Name: ifIndex

Object Information

Specific Object Information

Object	disAllCpuUsage
OID	1.3.6.1.4.1.9.9.618.1.4.1
Type	SomeAdminString
Permission	read-only
Status	current
MIB	GISCO-LWAPP-SYS-MIB : - View Supporting Images
Description	This object represents the CPU usage string.

Uso de OIDs para monitorar o estado da WLC

Depois que você adquire o OID do objeto que precisa ser monitorado, a primeira consulta SNMP pode ser executada. Estes exemplos mostram como adquirir um uso de CPU de WLC por núcleo (OID = 1.3.6.1.4.1.9.9.618.1.4.1) para a comunidade SNMPv2 `snmp_test` e o usuário SNMPv3 `admin` com a senha SHA Auth `Cisco123Cisco123` e a senha AES Privacy definidas como `Cisco123Cisco123`. A interface de gerenciamento do controlador está localizada em `10.48.39.164`.

Monitor via SNMPwalk

SNMPwalk é uma aplicação SNMP que usa solicitações SNMP GETNEXT para consultar uma entidade de rede em busca de uma árvore de informações. Ele está presente por padrão no MacOS e na maioria das distribuições Linux. Para o SNMPv2c, o comando tem a sintaxe:

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

Por exemplo:

```
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 = STRI
```


Se o SNMPv3 for usado, o comando terá a sintaxe:

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

Escolha MD5/SHA e AES/DES com base em como você criou o usuário SNMPv3 no controlador.

Por exemplo:

```
VAPEROVI-M-H1YM:~ vaperovi$ snmpwalk -v3 -l authPriv -u admin -a SHA -A Cisco123Cisco123 -x AES -X Cisco123Cisco123 10.48.39.164 1.3.6.1.4.1.14179.2.3.1.13.0
```

Monitoramento através da biblioteca Python 3 e pysnmp

Esses trechos de código são escritos em Python 3.7 e utilizam o pysnmp módulo (pip install pysnmp) para fazer consultas SNMP para utilização da CPU do Cisco 3504 WLC. Esses exemplos usam a mesma comunidade SNMPv2 e o usuário SNMPv3 criados em um dos capítulos anteriores. Simplesmente substitua os valores de variáveis e integre o código com seus próprios scripts personalizados.

Exemplo de 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, 162)), 0, 0, 0))
```

Saída:

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

Exemplo de 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'
```

Integração com software de terceiros (Grafana/PRTG Network Monitor/SolarWinds)

O Cisco Prime Infrastructure oferece a capacidade de monitorar e configurar facilmente vários dispositivos de rede, que incluem controladores

sem fio. A Prime Infrastructure vem pré-carregada com todos os OIDs e a integração com a WLC consiste simplesmente na adição das credenciais da WLC ao Prime. Após a sincronização, é possível definir alarmes e enviar modelos de configuração para vários controladores sem fio de uma só vez.

Por outro lado, o Cisco WLC também pode ser integrado a várias soluções de monitoramento de terceiros, desde que os OIDs sejam conhecidos. Programas como o Grafana, o PRTG Network Monitor e o servidor SolarWinds permitem que as MIBs ou OIDs sejam importadas e que os valores sejam exibidos em um gráfico de fácil utilização.

Os servidores de monitoramento podem precisar ser ajustados para acomodar essa integração. No exemplo mostrado na imagem, o servidor de monitoramento PRTG é fornecido com o OID de utilização de CPU por núcleo que retorna a string 0%/1%, 1%/1%, 0%/1%, 0%/1%. PRTG espera um valor inteiro e gera um erro.

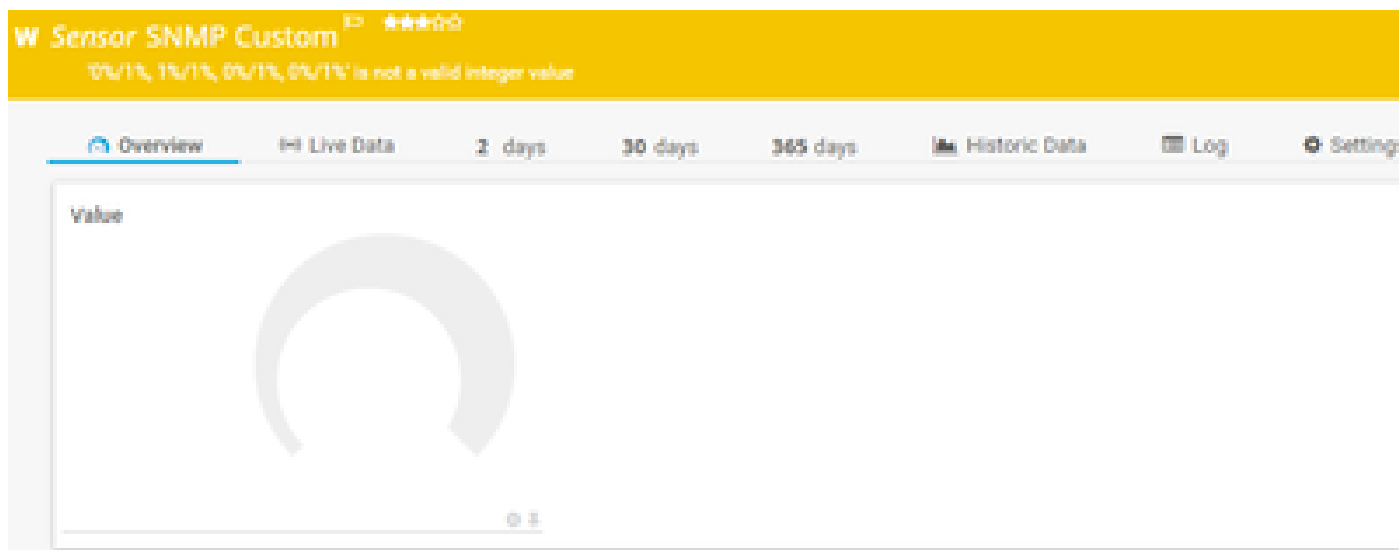


Tabela dos OIDs mais comumente monitorados

Se você considerar que as MIBs apresentam os dados em sintaxe não amigável, esta tabela inclui alguns dos nomes de objetos mais comuns e seus OIDs que os clientes da Cisco usam.

Descrição	Nome do objeto	OID	Resposta esperada
Uso geral de CPU em %	utilizaçãoAtualCPUdoagente	1.3.6.1.4.1.14179.1.1.5.1.0	INTEIRO: 0
Uso da CPU por núcleo	clsAllCpuUsage	1.3.6.1.4.1.9.9.618.1.4.1.0	CADEIA DE CARACTERES: 0%/1%, 0%/1%, 0%/1%, 0%/1%
Uso de RAM	clsSysCurrentMemoryUsage	1.3.6.1.4.1.9.9.618.1.8.6.0	Medidor32: 33

em %			
Temperatura da CPU em °C	bsnSensorTemperature	1.3.6.1.4.1.14179.2.3.1.13.0	INTEIRO: 76
Número de APs associados	clsSysApConnectCount	1.3.6.1.4.1.9.9.618.1.8.4.0	Medidor32: 2
Número de clientes	clsMaxClientsCount	1.3.6.1.4.1.9.9.618.1.8.12.0	Medidor32: 0
Número de clientes por WLAN	bsnDot11EssNúmeroDeEstaçõesMóveis	1.3.6.1.4.1.14179.2.1.1.1.38.0	Contador32: 3 Contador32: 2

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.