

Resuelva problemas el PGW2200 Softswitch con el SNMP

ID del Documento: 62683

Actualizado: De julio el 23 de 2008



[Descarga PDF](#)



[Imprimir](#)

[Comentarios](#)

Productos Relacionados

- [Cisco SC 2200 Signaling Controller](#)
- [Cisco PGW 2200 Softswitch](#)
- [Signaling System 7 \(SS7\)](#)

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Información de SNMP del Troubleshooting en Cisco PGW2200](#)

[Información Relacionada](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

Introducción

Este documento proporciona la información de Troubleshooting para el Simple Network Management Protocol (SNMP) en el gateway del Public Switched Telephone Network de Cisco PGW2200 (PSTN) (referido como simplemente Cisco PGW2200 en este documento). La información en este documento se aplica específicamente a la solución de gateway PSTN de Cisco para los modos del Control de Llamadas y de la señalización de llamada. Este documento contiene las extremidades y las advertencias en el uso de los componentes SNMP con la solución, así como los pasos de Troubleshooting para solucionar los problemas potenciales.

El agente SNMP proporciona una tarea del Simple Network Management. SNMP intercambia información alrededor el estatus de un dispositivo, en este caso un dispositivo conectado a Cisco PGW2200, dentro del Marco de administración usando las unidades de datos de protocolo (PDU) cifradas en el formato de la Notación de sintaxis abstracta (ASN).

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Plataforma	Nombre de la plataforma	Versión
Nodo de Cisco PGW2200	Controlador de gateway de los medios de Cisco (MGC)	<ul style="list-style-type: none">• 9.3(2) (de la corrección 9.3(2)S20) — Release Note para la versión del Cisco Media Gateway Controller Software 9.3(2)• 9.4(1) (de la corrección 9.4(01)S06) — Release Note para la versión del Cisco Media Gateway Controller Software 9.4(1)• 9.5(2) Integrado — Release Note para la versión del Cisco Media Gateway Controller Software 9.5(2)
Información de los Management Information Base de Cisco PGW2200 (MIB)		Id. de bug Cisco CSCeb37011 (clientes registrados solamente) — Mejora de la Seguridad SNMP

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las [Convenciones](#)

Resuelva problemas la información de SNMP en Cisco PGW2200

La cadena predeterminada de la Seguridad SNMP (comunidad) es pública para los propósitos leída y de la notificación. La cadena de la Seguridad de la escritura (comunidad) se genera aleatoriamente para la función de recuperación de proceso. Las configuraciones SNMP varían; para los defectos específicos, Id. de bug Cisco [CSCeb73838 \(clientes registrados solamente\)](#) del control que se conecta a un **comando config-snmp** de Cisco PGW2200 que necesite ser utilizado para configurar los elementos SNMP en Cisco PGW2200.

El comando config-snmp, situado en el directorio de /opt/CiscoMGC/local, es una herramienta controlada por menú que se puede ejecutar del modo del superusuario de UNIX. Su característica de la migración puede limitar la operación determinada a solamente dos objetos de MIB que habilite o inhabilite la recuperación de proceso. La cadena de seguridad de la operación establecida se genera y se limita aleatoriamente al acceso del host local. **El comando config-snmp** también proporciona al usuario la capacidad para agregar y para borrar la cadena y el destino capturado de la Seguridad (comunidad). Ésta es salida de muestra del **comando config-snmp**:

```
mgcusr@mgc-bru-20% su - root Password: # config-snmp Migrating snmpd.cnf into a more secure
setting... ===== SNMPD Configuration Main Menu ===== 1. View
Configuration Entries 2. Add an SNMP Community 3. Delete an SNMP Community 4. Add a Trap
Destination 5. Delete a Trap Destination 6. Activate the New Settings Enter a selection (1
through 6) or 'q' to quit: 1 ===== Entries Menu ===== 1. sysDescr 2.
sysObjectID 3. sysLocation 4. sysContact 5. sysName 6. snmpEnableAuthenTraps 7. MAX_THREADS 8.
MAX_PDU_TIME 9. MAX_OUTPUT_WAITING 10. MAX_SUBAGENTS 11. subagent 12. snmpCommunityEntry 13.
communityEntry 14. snmpEngineBoots 15. usmUserEntry 16. vacmAccessEntry 17.
vacmSecurityToGroupEntry 18. vacmViewTreeFamilyEntry 19. snmpNotifyEntry 20. snmpTargetAddrEntry
21. snmpTargetParamsEntry 22. snmpNotifyFilterProfileEntry 23. snmpNotifyFilterEntry 24.
httpUserNameEntry Enter a selection (1 through 24) or 'q' to quit to Main Menu:
===== SNMPD Configuration Main Menu ===== 1. View Configuration
Entries 2. Add an SNMP Community 3. Delete an SNMP Community 4. Add a Trap Destination 5. Delete
a Trap Destination 6. Activate the New Settings Enter a selection (1 through 6) or 'q' to quit:
2 ===== Add CommunityString Menu ===== SnmpCommunityName
CommunitySecurityName public ReadAndNotifyToAll -- Where: CommunitySecurityName SecurityModel
Read Write Notification ReadAndNotifyToAll snmpv1 AllMibObjects - AllMibObjects
ReadAndNotifyToAll snmpv2c AllMibObjects - AllMibObjects ReadWriteAll snmpv1 AllMibObjects
AllMibObjects - ReadWriteAll snmpv2c AllMibObjects AllMibObjects - Would you like to proceed
with the Add [n]/[y]? From this level you can change the SnmpCommunityName on the Cisco PGW
2200.
```

Nota: Si el SNMP daemon se inhabilita en Cisco PGW2200, no hay función de recuperación para los procesos de Cisco PGW2200 (véase /opt/CiscoMGC/snmp/critagt.cnf). Los procesos monitoreados por el subagente de la aplicación crítica (critagt) no pueden ser recuperados si este agente se mata involuntariamente. No hay soporte de la recuperación.

Una vez que usted ha fijado toda la información correctamente, usted puede todavía encontrar algunos problemas. Aquí están algunos pasos de Troubleshooting:

1. Asegúrese que el proceso del snmpdm se esté ejecutando en Cisco PGW2200:mgcusr@PGW2200a% **ps -ef | grep snmp** root 931 1 0 Mar 29 ? 3:20 /opt/CiscoMGC/snmp/snmpdm -tcplocal -d root 932 1 0 Mar 29 ? 0:31 /opt/CiscoMGC/snmp/mib2agt -d root 15519 1 0 Jun 29 ? 0:06 /opt/CiscoMGC/snmp/critagt -d root 933 1 0 Mar 29 ? 1:26 /opt/CiscoMGC/snmp/hostagt -d root 934 1 0 Mar 29 ? 0:25 /opt/CiscoMGC/snmp/fsagt -d root 935 1 0 Mar 29 ? 4:34 /opt/CiscoMGC/snmp/brassagt -d

2. Criadgt se supervisa del init. Verifique que usted tenga esta entrada en el directorio de `/etc/inittab:ca:3:respawn:/opt/CiscoMGC/snmp/criadgt -d`
3. Critagt supervisa el snmpdm, el mib2agt, el hostagt, el fsagt, el brassagt, el procM y los agentes LogServeres. Verifique que usted vea estos procesos SNMP el ejecutarse en `/opt/CiscoMGC/snmp/criadgt.cnf:mgcusr@PGW 2200a% ps -ef | grep snmp`

```

root 931 1 0 Mar 29 ? 3:20 /opt/CiscoMGC/snmp/snmpdm -tcplocal -d root 932 1 0 Mar 29 ? 0:31
/opt/CiscoMGC/snmp/mib2agt -d root 15519 1 0 Jun 29 ? 0:06 /opt/CiscoMGC/snmp/criadgt -d
root 933 1 0 Mar 29 ? 1:26 /opt/CiscoMGC/snmp/hostagt -d root 934 1 0 Mar 29 ? 0:25
/opt/CiscoMGC/snmp/fsagt -d root 935 1 0 Mar 29 ? 4:34 /opt/CiscoMGC/snmp/brassagt -d

```
4. Publique el **netstat -a** del comando unix | el **grep 161** y el control que el comando vuelve un estatus **ocioso** para el User Datagram Protocol (UDP) SNMP vira hacia el lado de `babor.mgcusr@PGW 2200a% netstat -a | grep 161`

```

*.161 Idle localhost.7161 *.* 0 0 24576 0
LISTEN 30006f41610 stream-ord 00000000 00000000 ../var/lsd_addr mgcusr@PGW 2200a%netstat -a
| grep 162 *.162 Idle mgcusr@PGW 2200a%

```

Nota: El SNMP estándar envía las respuestas a los pedidos de administración sobre el puerto 161 UDP y a la información de trampa sobre el puerto 162 UDP. **Nota:** Usted puede publicar el comando **snoop** de UNIX de descubrir qué se ha enviado entre Cisco PGW2200 y la estación del sistema de administración de la red (NMS). En la estación NMS, usted puede publicar el comando **snmpwalk** del freeware conjuntamente con el comando **snoop** de UNIX.
5. Publique el comando **snoop -v <IP address NMS>** en Cisco PGW2200 de descubrir qué mensajes se han enviado y a la estación NMS. También lea a los detalles del comando **man snoop**; usted puede querer salvarlos en un archivo. Usted puede también capturar esta información y marcar el contenido usando el analizador [etéreo del Network Protocol](#).
6. Publique el comando **snmpwalk -c public <PGW 2200 IP address>** en su sistema NMS. Interrogaciones de este comando para un árbol de información. La versión del comando **snmpwalk** usado con el propósito de este documento es:

```

% snmpwalk No hostname specified.
USAGE: snmpwalk [OPTIONS] AGENT [OID]
Version: 5.0.9 Web: http://www.net-snmp.org/ Email:
net-snmp-coders@lists.sourceforge.net

```

Ésta es una salida de muestra del comando

```

snmpwalk:SNMPv2-MIB::sysDescr.0 = STRING: SNMPv3 agent from Cisco Systems, Inc.
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.2496.1.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1599337216)
185 days, 2:36:12.16
SNMPv2-MIB::sysContact.0 = STRING: Cisco Systems, Inc. +1 703 484 3000
SNMPv2-MIB::sysName.0 = STRING: NSSU - MGC
SNMPv2-MIB::sysLocation.0 = STRING: Herndon, Virginia
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
IF-MIB::ifNumber.0 = INTEGER: 3
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifDescr.1 = STRING: lo0
IF-MIB::ifDescr.2 = STRING: eri0
IF-MIB::ifDescr.3 = STRING: eri1
IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifMtu.1 = INTEGER: 8232
IF-MIB::ifMtu.2 = INTEGER: 1500
IF-MIB::ifMtu.3 = INTEGER: 1500
RFC1213-MIB::atNetAddress.2.1.50.0.0.1 = Network Address: 32:00:00:01
RFC1213-MIB::atNetAddress.2.1.224.0.0.0 = Network Address: E0:00:00:00
RFC1213-MIB::atNetAddress.3.1.10.48.85.20 = Network Address: 0A:30:55:14
RFC1213-MIB::atNetAddress.3.1.224.0.0.0 = Network Address: E0:00:00:00
IP-MIB::ipForwarding.0 = INTEGER: notForwarding(2)
IP-MIB::ipDefaultTTL.0 = INTEGER: 255

```

```
IP-MIB::ipInReceives.0 = Counter32: 535077888
IP-MIB::ipInHdrErrors.0 = Counter32: 0
IP-MIB::ipInAddrErrors.0 = Counter32: 0
IP-MIB::ipForwDatagrams.0 = Counter32: 0
```

!--- Output suppressed due to the enormity of information, which !--- would require several HTML pages to display.

Usted no puede comenzar el proceso del snmpdm en el directorio de /opt/CiscoMGC/snmp del modo del superusuario de UNIX, usando el apall del argumento "-" como registro todos los mensajes más. Esto no es posible porque el software quita este argumento y lo trae nuevamente dentro del escenario de configuración normal como snmpdm - tcplocal - d, mostrado en esta salida de muestra: Esto da lugar a este mensaje de error:

```
#/etc/init.d/snmpd stop # /opt/CiscoMGC/snmp/snmpdm -tcplocal -d -apall & !--- Start the snmpdm
process with the command snmpd -tcplocal -d -apall &. SNMP Research SNMP Agent Resident Module
Version 15.4.1.16 Copyright 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999,
2000, 2001, 2002, 2003 SNMP Research, Inc. Successfully opened log file /tmp/snmpd.log at line
397 in file mastmain.c Only APERROR and APWARN messages are being printed to the log file
(override with -log_tracefile) at line 421 in file mastmain.c [1] 11204 # init_fnames: searching
for configuration files in /opt/CiscoMGC/snmp from getenv("SR_AGT_CONF_DIR") at line 90 in file
../../../../snmpd/shared/fnames.c AgentSocketCreate: bind failed: Address already in use at line 262
in file tcp.c InitMaster: IPCFP[0].AgentSocketCreate failed at line 735 in file master.c master
agent initialization failed, exiting at line 478 in file mastmain.c # /opt/CiscoMGC/snmp/snmpdm
-h usage: ./snmpdm [options] options: -d execute in the foreground window -trap_send_port PORT
send SNMP trap/inform messages from port PORT -tcp any accept connections from any TCP subagent -
tcplocal accept connections from local TCP subagents -tcpnone disallow connections from TCP
subagents (default) -apnone no log messages -apwarn log warning messages -aperror log error
messages -apconfig log config file i/o messages -appacket log SNMP packet build/parse messages -
aptrap log trap/inform messages -apaccess log agent processing messages -apemanate log
master/subagent messages -aptimer log timer debug messages -apthread log thread debug messages -
apverbose log verbose debug messages -apuser log user messages -hexdump dump packets in hex -
vbdump dump packets as varbinds -aptrace trace packet in application -apaudit audit SET
processing in application -apall log all messages -log_mtos allow sending log messages to
Subagents -log_nomtos disallow sending log messages to Subagents -log_stom allow receiving log
messages from Subagents -log_nostom disallow receiving log messages from Subagents -log_format 0
use traditional log message format -log_format 1 use new log message format -log_stdout allow
log messages to go to standard output -log_nostdout disallow log messages to go to standard
output -log_stderr allow log messages to go to standard error -log_nostderr disallow log
messages to go to standard error -log_file allow log messages to go to snmpd.log -log_nofile
disallow log messages to go to snmpd.log -log_tracefile allow APTRACE messages to go to
snmpd.log -log_notracefile disallow APTRACE messages to go to snmpd.log -log_append append log
messages to snmpd.log -log_noappend discard previous contents of snmpd.log, if any -
large_vl_pdus lift 484 byte restriction for v1/v2c PDUs -help print this usage line -pkt_size
value use supplied value as max packet size mgcusr@PGW 2200a%
```

El archivo critagt.cnf en el directorio de /opt/CiscoMGC/snmp, mostrado aquí, es responsable del mensaje de error antedicho:

```
mgcusr@pw2200a% more critagt.cnf # Entry type: critAppProcEntry # Entry format: integer #
octetString # octetString # octetString # integer # integer # integer # integer # integer #
integer critAppProcEntry 1 snmpdm "/opt/CiscoMGC/snmp/snmpdm -tcplocal -d" - 1 true 0 true true
true
```

Porque el critagt recomienza el SNMP daemon y se comienza una vez, el puerto llega a estar ocupado, usted encuentra el mensaje de error descrito.

Nota: Usted no puede cambiar ninguna entrada en el archivo critagt.cnf, porque después de que usted recomience la aplicación de Cisco PGW2200, restablece automáticamente las configuraciones predeterminadas.

Nota: Para información detallada sobre el archivo de snmpd.log, control bajo directorio de /tmp.

Para los expedientes DDTs conectados a los detalles del snmpd de Cisco PGW2200, refiera al Id. de bug Cisco [CSCef55514](#) ([clientes registrados solamente](#)) — los desvíos genéricos perdidos SNMP para el link abajo y suba.

[Información Relacionada](#)

- [Notas técnicas del Cisco PGW 2200 Softswitch](#)
- [Soporte de tecnología de voz](#)
- [Soporte de Productos de Voice and Unified Communications](#)
- [Troubleshooting de Cisco IP Telephony](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

¿Era este documento útil? [Sí](#) [ningún](#)

Gracias por su feedback.

[Abra un caso de soporte](#) (requiere un [contrato de servicios con Cisco](#).)

Discusiones relacionadas de la comunidad del soporte de Cisco

[La comunidad del soporte de Cisco](#) es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los [convenios de los consejos técnicos de Cisco](#) para la información sobre los convenios usados en este documento.

Actualizado: De julio el 23 de 2008

ID del Documento: 62683