

Pesquise defeitos o PGW2200 Softswitch com SNMP

ID do Documento: 62683

Atualizado em: julho 23, 2008



[Transferência PDF](#)



[Imprimir](#)

[Feedback](#)

Produtos Relacionados

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

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Pesquise defeitos a informação de SNMP em Cisco PGW2200](#)

[Informações Relacionadas](#)

[Cisco relacionado apoia discussões da comunidade](#)

Introdução

Este documento fornece a informação de Troubleshooting para o Simple Network Management Protocol (SNMP) no gateway da rede telefônica pública comutada de Cisco PGW2200 (PSTN) (referido como simplesmente Cisco PGW2200 neste documento). A informação neste documento aplica-se especificamente à solução de gateway Cisco PSTN para modos do Controle de chamadas e da sinalização de chamada. Este documento contém pontas e avisos no uso dos componentes SNMP com a solução, assim como passos de Troubleshooting para resolver problemas potenciais.

O agente SNMP fornece uma tarefa do Simple Network Management. O SNMP troca informações sobre o estado de um dispositivo, neste caso um dispositivo ligado a Cisco PGW2200, dentro do framework de gerenciamento usando as unidades de dados de protocolo (PDU) codificadas no formato da anotação de sintaxe abstrata (ASN).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

Plataforma	Nome da plataforma	Versão
Nó de Cisco PGW2200	Controlador do gateway do Cisco media (MGC)	<ul style="list-style-type: none">• 9.3(2) (da correção de programa 9.3(2)S20) — Release Note para a liberação de Cisco Media Gateway Controller Software 9.3(2)• 9.4(1) (da correção de programa 9.4(01)S06) — Release Note para a liberação de Cisco Media Gateway Controller Software 9.4(1)• 9.5(2) Integrado — Release Note para a liberação de Cisco Media Gateway Controller Software 9.5(2)
Informação das bases de informação de gerenciamento de Cisco PGW2200 (MIB)		Identificação de bug Cisco CSCeb37011 (clientes registrados somente) — Realce da segurança SNMP

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

[Pesquise defeitos a informação de SNMP em Cisco PGW2200](#)

A corda da segurança SNMP do padrão (a comunidade) é pública para finalidades lida e da notificação. A corda da Segurança da escrita (a comunidade) é gerada aleatoriamente para a função de recuperação do processo. As configurações de SNMP variam; para defeitos específicos, identificação de bug Cisco [CSCeb73838 da verificação \(clientes registrados somente\)](#) que é ligada a um **comando config-snmp de Cisco PGW2200** que precise de ser usado para configurar os itens SNMP em Cisco PGW2200.

O **comando config-snmp**, situado no diretório de /opt/CiscoMGC/local, é uma ferramenta menu-conduzida que possa ser executada do modo do superusuário UNIX. Sua característica da migração pode limitar a operação ajustada a somente dois objetos MIB que permita ou desabilite a recuperação do processo. A série de segurança de operação em conjunto aleatoriamente é gerada e limitada ao acesso do host local. O **comando config-snmp** igualmente fornece o usuário a capacidade de adicionar e suprimir da corda e do destino de armadilha da Segurança (a comunidade). Este é exemplo de saída do **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: Se o daemon de SNMP é desabilitado em Cisco PGW2200, não há nenhum recurso de recuperação para processos de Cisco PGW2200 (veja /opt/CiscoMGC/snmp/critagt.cnf). Os processos monitorados pelo Subagent do aplicativo crítico (critagt) não podem ser recuperados se este agente é matado involuntariamente. Não há nenhum apoio da recuperação.

Uma vez que você ajustou toda a informação corretamente, você pode ainda encontrar algumas edições. Estão aqui alguns passos de Troubleshooting:

1. Assegure-se de que o processo do snmpdm esteja sendo executado em Cisco

```
PGW2200: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/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. Criatgt é supervisionado do init. Verifique que você tem esta entrada no diretório de

```
/etc/inittab:ca:3:respawn:/opt/CiscoMGC/snmp/critagt -d
```

3. Critagt supervisiona o snmpdm, o mib2agt, o hostagt, o fsagt, o brassagt, o procM e os agentes LogServer. Verifique que você vê estes processos SNMP ser executado em

```

/opt/CiscoMGC/snmp/criagt.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/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

```

4. Emita o **netstat -a** do comando unix | o **grep 161** e certifique-se do comando retorne um estado inativo para as portas do User Datagram Protocol (UDP) SNMP.

```
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: O padrão SNMP envia respostas às requisições de gerenciamento sobre a porta 161 UDP e à informação de armadilha sobre a porta 162 UDP. **Nota:** Você pode emitir o comando **snoop** de UNIX encontrar o que foi enviado entre Cisco PGW2200 e a estação do sistema de gerenciamento de rede (NMS). Na estação NMS, você pode emitir o comando **snmpwalk** do freeware em combinação com o comando **snoop** de UNIX.
5. Emita o comando **snoop -v <IP address NMS>** em Cisco PGW2200 encontrar que mensagens foram enviados e à estação NMS. Igualmente leia os detalhes do comando **man snoop**; você pode querer armazená-los em um arquivo. Você pode igualmente capturar esta informação e verificar o índice usando o analisador [etéreo do](#) protocolo de rede.
6. Emita o comando **snmpwalk -c public <PGW 2200 IP address>** em seu sistema de NMS.

Perguntas deste comando para uma árvore de informação. A versão do comando **snmpwalk** usado para fins deste documento é:

```

% 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 Este é um exemplo de saída do 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.

Você não pode começar o processo do snmpdm no diretório de /opt/CiscoMGC/snmp do modo do superusuário UNIX, usando o apall do argumento "-" como o log todas as mensagens anymore. Isto não é possível porque o software remove este argumento e o traz de novo no cenário de inicialização normal como o snmpdm - tcplocal - d, mostrado neste exemplo de saída: Isto conduz a este Mensagem de Erro:

```
#/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
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_v1_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%
```

O arquivo critagt.cnf no diretório de /opt/CiscoMGC/snmp, mostrado aqui, é responsável para o Mensagem de Erro acima:

```
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 o critagt reinicia o daemon de SNMP e é começado uma vez, a porta torna-se ocupada, você encontra o Mensagem de Erro descrito.

Nota: Você não pode mudar nenhuma entrada no arquivo critagt.cnf, porque depois que você reinicia o aplicativo de Cisco PGW2200, restaura automaticamente as configurações padrão.

Nota: Para informações detalhadas sobre do arquivo de snmpd.log, verifique sob o diretório de /tmp.

Para os registros DDTs ligados aos detalhes do snmpd de Cisco PGW2200, refira a identificação de bug Cisco [CSCef55514](#) ([clientes registrados somente](#)) — armadilhas genéricas de falta SNMP para o link para baixo e levante.

Informações Relacionadas

- [Notas Técnica de Softswitch Cisco PGW 2200](#)
- [Suporte à Tecnologia de Voz](#)
- [Suporte ao Produto de Voz e Comunicações Unificadas](#)
- [Troubleshooting da Telefonia IP Cisco](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Era este documento útil? [Sim nenhum](#)

Obrigado para seu feedback.

[Abra um caso de suporte](#) (exige um [contrato de serviço Cisco](#).)

Cisco relacionado apoia discussões da comunidade

[Cisco apoia a comunidade](#) é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira [convenções dos dicas técnicas da Cisco](#) para obter informações sobre das convenções usadas neste documento.

Atualizado em: julho 23, 2008

ID do Documento: 62683