Sun™ Netra™ SNMP Management Agent 1.0 Installation and Configuration Guide

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900 U.S.A.
650-960-1300

Part No. 806-5111-10
August 2000, Revision A

Send comments about this document to: docfeedback@sun.com

Please
Recycle

Contents

Tables

Code Examples

Preface

This manual describes the prerequisites and procedures for installing and configuring Sun Netra SNMP Management Agent 1.0 on a Netra server.

How This Book Is Organized

Chapter 1 explains everything you need to know and the preparations you should make before installing Sun Netra SNMP Management Agent 1.0 on a Netra server.

Chapter 2 describes the procedure for installing, validating and running the Sun Netra SNMP Management Agent 1.0 on a Netra server. It also explains how to uninstall the software, should it become necessary.

Chapter 3 provides the information you need in order to configure Sun Netra SNMP Management Agent 1.0 on a Netra server.

Appendix A gives listings of the configuration files supplied.

Related Documentation

TABLE P-1 Related Documentation

Application	Title	Part Number
Using the software	*Sun Netra SNMP Management Agent 1.0 User's Reference Guide*	806-5817-10
Netra t servers	*Sun Netra SNMP Management Agent 1.0 Supplement for Netra t Servers*	806-5818-10
Netra t 1120/1125 servers	*Netra t 1120/1125 Installation and Basic Maintenance Guide*	805-6803-10
Netra t1 Model 100/105 servers	*LOMlite User's Guide*	806-2038-10
Netra t 1400/1405 servers	*Netra t 1400/1405 Installation and User's Guide* *LOMlite User's Guide*	806-0575-10 806-2038-10

Accessing Sun Documentation Online

The `docs.sun.com`[sm] web site enables you to access Sun technical documentation on the Web. You can browse the `docs.sun.com` archive or search for a specific book title or subject at:

`http://docs.sun.com`

Ordering Sun Documentation

Fatbrain.com, an Internet professional bookstore, stocks select product documentation from Sun Microsystems, Inc.

For a list of documents and how to order them, visit the Sun Documentation Center on Fatbrain.com at:

`http://www1.fatbrain.com/documentation/sun`

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Sun at:

`docfeedback@sun.com`

Please include the part number (806-5111-10) of your document in the subject line of your email.

CHAPTER 1

Before You Start

This chapter explains what you need to know before installing Sun Netra SNMP Management Agent 1.0 on your system.

Module Overview

Sun Netra SNMP Management Agent 1.0 comprises the following modules:

- `SUNW1jdrt` – Java DMK runtime. This provides a foundation framework for dynamic Java Management applications. Sun Netra SNMP Management Agent 1.0 makes use of the Java DMK SNMP protocol adapter to provide SNMP protocol connectivity.
- `SUNWsnimo` – Generic agent, platform adaptors and Java runtime. This provides the generic and platform specific components of Sun Netra SNMP Management Agent 1.0, the MIBs, and the Java Runtime Environment (JRE) 1.1.8_10 Localized.
- `SUNWsnimr` – Startup scripts and configuration files. This provides Sun Netra SNMP Management Agent 1.0 components which are invoked on changes to system run levels, and the two agent configuration files `snim.conf` and `snmp.acl`.

The default installation directories are:

- Software – `/opt/SUNWsnim`, `/opt/SUNWjdmk`
- Log files – `/var/opt/SUNWsnim`
- Configuration and Access Control List files – `/etc/opt/SUNWsnim`
- Run control scripts – `/etc/init.d` with links to `/etc/rc0.d`, `/etc/rc1.d`, `/etc/rc2.d`, `/etc/rc3.d` and `/etc/rcS.d`.

The following components are installed:

- Sun Netra SNMP Management Agent 1.0 MIBs
- Sun Netra SNMP Management Agent 1.0 classes
- Native Libraries
- JDMK run time environment (V 4.0)
- Java Runtime Environment (JRE) 1.1.8_10 Localized
- Startup scripts

Supported Platforms

The following platforms are supported:

- Sun Netra t 1120 server
- Sun Netra t 1125 server
- Sun Netra t 1400 server
- Sun Netra t 1405 server
- Sun Netra t 1 Model 100 server
- Sun Netra t 1 Model 105 server

System Requirements

Operating Environment

The following Operating Environments are supported:

- Solaris™ 2.6
- Solaris™ 7 (32-bit and 64-bit versions)
- Solaris™ 8

Disk Space

The Sun Netra SNMP Management Agent 1.0 software packages and operating environment patches require hard disk space as shown in TABLE 1-1:

TABLE 1-1 Disk Space Requirements

Solaris Version	Agent	SunSolve Patch Cluster	Total
2.6	8 Mbytes	91 Mbytes	99 Mbytes
7	8 Mbytes	112 Mbytes	120 Mbytes
8	8 Mbytes	No patches required	8 Mbytes

Patches

The required Solaris operating environment patch clusters can be obtained from `http://sunsolve.sun.com`.

The required / recommended patches are:

TABLE 1-2 Required / Recommended Patches

Patch No.	Required/ Recommended	Description
Solaris 2.6		
106040-13	Required	X Input and Output Method patch
107733-08	Recommended	Linker patch
105181-22	Recommended	Kernel Update (socket close / hang)
105284-37	Recommended	Motif Runtime Library patch
105633-41	Recommended	OpenWindows 3.6: Xsun patch
105568-18	Recommended	Libthread Patch
105210-32	Recommended	LibC Patch
105669-10	Recommended	CDE 1.2: libDTSvc patch (dtmail)
Solaris 7		
107636-05	Required	X Input and Output Method patch
106980-11	Recommended	Libthread patch
107078-18	Recommended	OpenWindows 3.6.1 Xsun patch

TABLE 1-2 Required / Recommended Patches *(Continued)*

Patch No.	Required/ Recommended	Description
107081-21	Recommended	motif runtime patch
Solaris 8		
No patches required		

These are the minimum version levels; use the latest version of each patch, as supplied in the patch clusters.

Netra-Specific Requirements

Checking the Alarms Software Installation (LOM or tsalarms)

The Netra-specific alarms software should be installed to ensure that the complete functionality of the Sun Netra SNMP Management Agent 1.0 is available.

▼ To Check a Netra t 1120/1125

- **As root, type:**

```
# /usr/sbin/modinfo -c | grep tsalarm
```

The result should resemble:

```
82          1 tsalarm                              LOADED/INSTALLED
#
```

The number may vary.

If different text or no text at all is returned, you must re-install the tsalarms software as described in the *Netra t 1120/1125 Installation and Basic Maintenance Guide*.

▼ To Check a Netra t1 or Netra t 1400/1405

- **As root, type:**

```
# /usr/sbin/modinfo -c | grep lom
```

The result should resemble:

```
83          1 lom                                     LOADED/INSTALLED
#
```

The number may vary.

If different text or no text at all is returned, you must re-install the LOM software as described in the *LOMlite User's Guide* or the *Netra t 1400/1405 Installation and User's Guide*.

Checking the OpenBoot PROM

This only applies to Netra t 1120 and Netra t 1125 systems.

Caution – Some Netra t 1120 and Netra t 1125 systems will require an upgrade to the OpenBoot PROM. If the Sun Netra SNMP Management Agent 1.0 is installed on a system which requires such an upgrade, the agent will not start and the error message `unrecognized platform "Sun Ultra 60 UPA/PCI"` will be displayed.

▼ To Check the OpenBoot PROM

- **As root, type:**

```
# eeprom banner-name
```

- If the result is:

```
banner-name=Netra t 1120/1125
```

you need take no further action and can proceed directly to the installation process as described in Chapter 2.

- If the result is:

```
banner-name=<message>
```

  where <*message*> may be anything else, including nothing at all, type:

```
# eeprom banner-name='Netra t 1120/1125'
# reboot
```

  You must restart the system as shown before installing Sun Netra SNMP Management Agent 1.0 as described in Chapter 2.

- If the result is:

```
banner-name: data not available
```

  you must upgrade the PROM. Refer to the documentation accompanying the system for instructions, or contact your local Sun representative.

CHAPTER 2

Installing and Starting the Software

This chapter describes the installation procedure in different Solaris environments.

It also explains how to start and stop the software, and how to uninstall it.

Installing the Software and Patches

The default installation directories are:

- Software – `/opt/SUNWsnim`, `/opt/SUNWjdmk`
- Log files – `/var/opt/SUNWsnim`
- Configuration and Access Control List files – `/etc/opt/SUNWsnim`
- Run control scripts – `/etc/init.d` with links to `/etc/rc0.d`, `/etc/rc1.d`, `/etc/rc2.d`, `/etc/rc3.d` and `/etc/rcS.d`.

▼ To Install the Required Patches

Patches are only required for versions 2.6 and 7 of the Solaris Operating Environment. If you are using the Solaris 8 Operating Environment, proceed directly to “To Install the Sun Netra SNMP Management Agent 1.0 Software” on page 13.

Solaris 2.6 Patches

1. **Log on as root.**
2. **Create a temporary directory into which to download the patch cluster, for instance:**

```
# mkdir /var/tmp/SunNIM
# cd /var/tmp/SunNIM
```

3. **Download the appropriate patch cluster or individual patches from** `http://sunsolve.sun.com` **into the directory you have created.**

TABLE 2-1 Solaris 2.6 Required/Recommended Patches

Patch No.	Required/ Recommended	Description
106040-13	Required	X Input and Output Method patch
107733-08	Recommended	Linker patch
105181-22	Recommended	Kernel Update (socket close/hang)
105284-37	Recommended	Motif Runtime Library patch
105633-41	Recommended	OpenWindows 3.6: Xsun patch
105568-18	Recommended	Libthread Patch
105210-32	Recommended	LibC Patch
105669-10	Recommended	CDE 1.2: libDTSvc patch (dtmail)

These are the minimum version levels required; the cluster may contain later versions of the patches than those shown above.

4. **Uncompress and untar the patches:**

```
# zcat 2.6_Recommended.tar.Z | tar -xvf -
```

or

```
# zcat <patch-id>.tar.Z | tar -xvf -
```

5. **You can install all the patches or select individual patches.**

To install all the patches, type:

```
# cd 2.6_Recommended
# ./install_cluster
```

To install the patches selectively, type:

```
# cd <patch-id>
# ./installpatch
```

Refer to the patch cluster README file and the individual patch README files for more detailed information.

6. **Reboot the system:**

```
# init 6
```

Solaris 7 Patches

1. **Log on as root.**
2. **Create a temporary directory into which to download the patch clusters, for instance:**

```
# mkdir /var/tmp/SunNIM
# cd /var/tmp/SunNIM
```

3. **Download the appropriate patch cluster or individual patches from** `http://sunsolve.sun.com` **into the directory you have created.**

TABLE 2-2 Solaris 7 Required/Recommended Patches

Patch No.	Required/ Recommended	Description
107636-05	Required	X Input and Output Method patch
106980-11	Recommended	Libthread patch
107078-18	Recommended	OpenWindows 3.6.1 Xsun patch
107081-21	Recommended	motif runtime patch[1]

1. This patch may need to be downloaded separately as it may not be incoporated in the patch cluster.

These are the minimum version levels required; the cluster may contain later versions of the patches than those shown above.

4. **You can install all the patches or select individual patches.**

- **To install all the patches, type:**

```
# unzip 7_Recommended.zip
# cd 7_Recommended
# ./install_cluster.
.
. <output truncated>
.
# cd 107081-21
# unzip 107081-21.zip
# patchadd 107081-20
```

- **To install the patches selectively, type:**

```
# patchadd -M <patch-dir> <patch-id> <patch-id>
```

For instance:

```
# patchadd 7_Recommended 107636-04 106980-11 107078-18 107081-20
```

Refer to the `patchadd` manpage, the patch cluster README file and the individual patch README files for more detailed information.

5. **Reboot the system:**

```
# init 6
```

▼ To Install the Sun Netra SNMP Management Agent 1.0 Software

1. **Create a temporary directory into which to download the software, for instance:**

```
# mkdir /var/tmp/SunNIM
# cd /var/tmp/SunNIM
```

2. **Download the Sun Netra SNMP Management Agent 1.0 software from** `http://www.sun.com/download` **into the directory you have created.**

3. **Unzip the file:**

```
# unzip SUNWsnim.1.0.zip
```

4. **To install the software, type:**

```
# pkgadd -d SUNWsnim.1.0
```

You should see the following:

```
The following packages are available:
  1  SUNW1jdrt     Java DMK runtime
                   (all) 4.0
  2  SUNWsnimo     Sun Netra SNMP Management Agent
                   (sparc) 1.0
  3  SUNWsnimr     Sun Netra SNMP Management Agent
                   (sparc) 1.0

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

5. **Press Return to install all the packages.**

6. **Delete the downloaded files and the temporary directory.**

Starting and Stopping the Agent

You must configure the agent before starting it for the first time. Refer to Chapter 3 for more information.

▼ To Start the Agent

- **Start the** `snim` **daemon by typing:**

```
# /etc/init.d/snimd start
```

▼ To Stop the Agent

- **Stop the** `snim` **daemon by typing:**

```
# /etc/init.d/snimd stop
```

Uninstalling the Software

This procedure explains how to uninstall the software, should it become necessary.

▼ To Uninstall the Software

1. **Log on as root.**
2. **Stop the Sun Netra SNMP Management Agent 1.0 daemon:**

```
# /etc/init.d/snimd stop
```

3. **Type**:

```
# pkgrm SUNWsnimo SUNWsnimr SUNW1jdrt
```

CHAPTER 3

Configuration

This chapter describes how to configure Sun Netra SNMP Management Agent 1.0 for use on your system. Refer also to the *Sun Netra SNMP Management Agent 1.0 User's Reference Guide*.

Note – It is necessary to configure the agent before starting it. Any configuration changes you make will not take effect until the agent is stopped and then started again.

Supplied SNMP MIBs

The four MIBs supplied with Sun Netra SNMP Management Agent 1.0 are:

- SNMP-FRAMEWORK-MIB (RFC2571)
- ENTITY-MIB (RFC2737)
- SUN-NET-INFO-MIB
- SUN-NIM-EXT-MIB

These MIBs must be loaded into the SNMP manager that you will use to access the SNMP agent.

The Sun Netra SNMP Management Agent 1.0-specific MIBs, `SUN-NET-INFO-MIB` and `SUN-NIM-EXT-MIB`, currently have OIDs of

`.iso.org.dod.internet.private.enterprises.sun.products.netra.netra-test.sunNimMIB`
and
`.iso.org.dod.internet.private.enterprises.sun.products.netra.netra-test.sunNemMIB`

respectively.

Note – The MIBs are currently in the `netra-test` group, but will be moved to the `netra` group in future releases of the Sun Netra SNMP Management Agent.

The default location for the MIBs is `/opt/SUNWsnim/1.0/mibs`.

Agent Configuration

The configuration of the agent is controlled by the `snim.conf` file, which controls the operation of the agent, and the `snmp.acl` file, which defines access to the agent. Examples of these files are given in Appendix A.

Communicating With the Agent

By default, the SNMP agent is configured to use port 8085. If it is not configured as a subagent you can change the port number by modifying `snim.conf` to set `SNMP_PORT` to the appropriate port number.

CODE EXAMPLE 3-1 Setting the SNMP Port Number in `snim.conf`

```
#
# Default SNMP port
#
SNMP_PORT=8085
```

Access to the agent is controlled by the ACL file, as described in “Access Control Lists (ACLs)” on page 21.

Notification Options

The classes of SNMP trap sent to managers specified in the ACL can be controlled by setting the agent option flags.

Notification options are specified in the `snim.conf` file.

CODE EXAMPLE 3-2 Specifying Notification Options in `snim.conf`

```
#
# Agent option flags
#
# -a    Send attribute change notifications
# -s    Send state change notifications
# -c    Send object creation notifications
# -d    Send object deletion notifications
#
OPTIONS="-ascd"
```

Configuration as a Subagent

The Sun Netra SNMP Management Agent 1.0 is intended to be used as an SNMP subagent in conjunction with a suitable master agent.

In order to use the SNMP agent as a sub-agent in conjunction with a third-party SNMP master agent, the following steps may need to be performed. Note that the master agent must be SNMPv2-compliant. The configuration may differ in detail for each master agent; refer to the documentation provided with your master agent for more details.

This procedure should be used where the master agent dynamically allocates port numbers for communication with its subagent when it is started. If the master agent is only able to connect to a subagent which is already up and running, the Sun Netra SNMP Management Agent 1.0 configuration should be left as it is. The master agent must still be configured to forward SNMP requests (see Step 4).

By default, the SNMP agent is configured to use port 8085.

▼ To Configure as a Subagent

1. **If the agent has already been started, stop it by typing:**

```
# /etc/init.d/snimd stop
```

2. **Modify the** `snim.conf` **file to set** `SUB_AGENT=yes`**.**

```
#
# Sub-agent configuration
#
# Define to “yes” for sub-agent operation in which case agent will only
# start when startup script is passed an SNMP port argument.
#
SUB_AGENT=yes
#
```

   This will prevent the agent being started automatically at startup. It will still be stopped on shutdown in the normal fashion.

3. **Configure the master agent to start the SNMP agent with the following invocation, using an appropriate port number:**

```
/etc/init.d/snimd start <port>
```

   where <*port*> is the SNMP port number to use for communication between the master and subagents.

4. **Configure the master agent to forward requests within the following OID subtrees:**

   `.iso.org.dod.internet.mgmt.mib-2.entityMIB`

   `.iso.org.dod.internet.private.enterprises.sun.products.netra.netra-test.sunNimMIB`

   `.iso.org.dod.internet.private.enterprises.sun.products.netra.netra-test.sunNemMIB`

   or numerically:

   `.1.3.6.1.2.1.47`

   `.1.3.6.1.4.1.42.2.25.99.2`

   `.1.3.6.1.4.1.42.2.25.99.3`

   Note that the SNMP agent will send all SNMP traps to port 162, so these need not be routed via the master agent.

Access Control Lists (ACLs)

Access control is based on the IP address and community of the manager's host machine. Information on the access rights for communities and host machines is stored in an ACL file. A full listing of the ACL file supplied is given in Appendix A.

The ACL file also defines the hosts of managers to which to agent will send traps. When a trap is sent, the agent will send it to all hosts listed in the trap definitions of the ACL file.

To enable access control and traps for the SNMP adaptor, ensure that an ACL file exists when any agents are started. The ACL file is typically called `snmp.acl` and is located in the configuration directory `/etc/opt/SUNWsnim/snmp.acl`.

As the ACL file contains security-related information, it should be given restricted access rights, ideally readable only by `root`.

To use an `snmp.acl` file other than the default, specify an alternative using the `SNMP_ACL` configuration parameter in `snim.conf`.

CODE EXAMPLE 3-3 Specifying an Access Control List in `snim.conf`

```
# The default ACL file may be overridden here
#
# e.g.
# SNMP_ACL=/home/eg/myconfig.acl
#
SNMP_ACL=
```

If an ACL file exists, the access rights it defines apply to all managers or proxy servers that access the agent through its SNMP adapter. If the ACL file does not exist when the agents are started, all managers are granted full access to the agent through the SNMP adapter.

ACL File Format

An ACL file contains an `acl` group defining community and manager access rights and a `trap` group defining the community and hosts for sending traps.

Format of the `acl` Group

The `acl` group contains one or more lists of community configurations:

CODE EXAMPLE 3-4 Setting Community Configurations in the ACL File

```
acl = {
    <list1>
    <list2>
    ...
    <listN>
}
```

Each list has the following format:

CODE EXAMPLE 3-5 Community Configuration List Format

```
{
   communities = <communityList>
   access = <accessRights>
   managers = <hostList>
}
```

The *<communityList>* is a list of SNMP community names to which this access control applies. The community names in this list are separated by commas.

The *<accessRights>* specifies the rights to be granted to all managers running on the machines specified in the managers item. There are two possible values:

- `read-write`
- `read-only`

The <*hostList*> item specifies the host machines of the managers to be granted the access rights. The <*hostList*> is a comma-separated list of hosts, each of which can be expressed as any one of the following:

- A host name
- An IP address
- A subnet mask

Note – To distinguish between IP addresses and subnet masks in an ACL file, each integer in a subnet mask is separated by an exclamation mark (!) instead of a dot.

Format of the `trap` Group

The `trap` group specifies the hosts to which the agent can send traps. This group contains one or more trap community definitions:

CODE EXAMPLE 3-6 Specifying Trap Definitions in the ACL File

```
trap = {
    <community1>
    <community2>
    ...
    <communityN>
}
```

Each defines the association between a set of hosts and the SNMP community string in the traps to be sent to them. Each `trap-community` definition has the following format:

CODE EXAMPLE 3-7 Specifying Trap Community Definitions in the ACL File

```
{
   trap-community = <trapCommunityString>
   hosts = <trapInterestHostList>
}
```

The <*trapCommunityString*> item specifies the SNMP community string. It will be included in the traps sent to the hosts specified in the `hosts` item.

The <*trapInterestHostList*> item specifies a comma-separated list of hosts. Each host must be identified by its name or complete IP address.

CODE EXAMPLE 3-8 Example ACL File

```
acl = {
    {
        communities = public, private
        access = read-only
        managers = rag, tag, bobtail
    }
    {
        communities = tigger
        access = read-write
        managers = brittas
    }
}

trap = {
    {
        trap-community = tigger
        hosts = brittas
    }
}
```

APPENDIX **A**

Configuration Files

This Appendix contains complete listings of the configuration files supplied with Sun Netra SNMP Management Agent 1.0:

snim.conf

CODE EXAMPLE A-1 snim.conf

```
#!/sbin/sh
#
# Copyright (c) 1997 by Sun Microsystems, Inc.
# All rights reserved.
#
#ident“@(#)snim.conf 1.5 00/06/29 SMI”

#
# This file is used to control the configuration of the snimd daemon
#

#
# Sub-agent configuration
#
# Define to “yes” for sub-agent operation in which case agent will only
# start when startup script is passed an SNMP port argument.
#
SUB_AGENT=no

#
# The default log file may be overridden here
#
# e.g.
# LOG_FILE=/var/tmp/snim.log
#
LOG_FILE=

#
# Default SNMP port
#
SNMP_PORT=8085

#
# The default ACL file may be overridden here
#
# e.g.
# SNMP_ACL=/home/eg/myconfig.acl
#
SNMP_ACL=

#
```

CODE EXAMPLE A-1 snim.conf *(Continued)*

```
# Agent option flags
#
# -a    Send attribute change notifications
# -s    Send state change notifications
# -c    Send object creation notifications
# -d    Send object deletion notifications
#
OPTIONS=”-ascd”
```

snmp.acl

CODE EXAMPLE A-2 snmp.acl

```
#
#  @(#)snmp.acl 1.4 00/07/10 SMI
#
# Copyright 2000 Sun Microsystems, Inc. All rights reserved.
# This software is the proprietary information of Sun Microsystems, Inc.
# Use is subject to license terms.
#
# Template ACL file
#
# The SNMP agent provides access control based on the IP address and
# community of the manager's host machine. Information on the access rights
# for communities and host machines is stored in an ACL file.
#
# The ACL file also defines the hosts of managers to which to agent will send
# traps. When a trap is sent, the agent will send it to all hosts listed in
# the trap definitions of the ACL file.
#
# To enable access control and traps for the SNMP adapter, ensure that an ACL
# file exists when the agent is started. The ACL file is, by default,
# located at /etc/opt/SUNWsnim/<version>/snmp.acl. An alternate file may be
# specified by the SNIM_ACL definition in the snim.conf configuration file,
# at /etc/opt/SUNWsnim/<version>/snim.conf.
#
# If the ACL file does not exist when the agent is started, all managers are
# granted full access rights and no traps will be generated.
#


#
# The 'acl' group in this file specifies the access rights for specific
# communities/managers.
#
# It consists of a list of community configurations with the following format:
#   {
#       communities = communityList
#       access = accessRights
#       managers = hostList
#   }
#
# The communityList is a comma-separated list of SNMP community names to which
# this access control applies.
#
```

CODE EXAMPLE A-2 snmp.acl

```
# The accessRights specifies the permissions granted to the managers named
# in the hostList, using a community name from the communityList. It may
# be set to either ‘read-only’ or ‘read-write’.
#
# The hostList is a comma-separated list of hostnames to be granted the
# specified accessRights. Each hostname may be specified as:
#   - hostname: e.g. hubble
#   - ip address: e.g. 123.456.789.12
#   - subnet mask: e.g. 123!255!255!255
#     (This is an IP address where “.” are replaced by “!”)
#
# Example:
#
# acl = {
#     {
#         communities = public, private
#         access = read-only
#         managers = rag, tag, bobtail
#     }
#     {
#         communities = tigger
#         access = read-write
#         managers = brittas
#     }
# }

# The trap group specifies the hosts to which the agent can send traps.
# This group contains one or more trap community definitions.
#
# trap = {
#     community1
#     community2
#     ...
#     communityN
# }
#
# Each defines the association between a set of hosts and the SNMP community
# string in the traps to be sent to them. Each trap definition has the
# following format:
# {
#     trap-community = trapCommunityString
#     hosts = trapInterestHostList
# }
#
# The trapCommunityString item specifies the SNMP community string. It will
# be included in the traps sent to the hosts specified in the hosts item.
#
```

CODE EXAMPLE A-2 snmp.acl

```
# The trapInterestHostList item specifies a comma-separated list of
# hosts. Each host must be identified by its name or complete IP address.
#
# Example:
#
# trap = {
#     {
#         trap-community = tigger
#         hosts = brittas
#     }
# }
```