

Description and guidelines on creating system service agent accounts on Mac OS X (Tiger)

For any system service agent that you want to create in Mac OS X, you would do the following:

```
sudo dscl localhost -create /NetInfo/root/Groups/system_groupname
sudo dscl localhost -create /NetInfo/root/Groups/system_groupname gid group_id
sudo dscl localhost -create /NetInfo/root/Users/system_username
sudo dscl localhost -create /NetInfo/root/Users/system_username uid user_id
sudo dscl localhost -create /NetInfo/root/Users/system_username gid primary_group_id
sudo dscl localhost -create /NetInfo/root/Users/system_username shell user_shell
sudo dscl localhost -create /NetInfo/root/Users/system_username home user_home
sudo dscl localhost -create /NetInfo/root/Users/system_username passwd "*"

```

Where,

system_groupname is a unique group name. By convention on Mac OS X, it is the same name as the username. Examples: tomcat, postfix, amavis, sendmail, etc.

group_id is the unique numeric id for the primary group used by the system service agent. Typically on Mac OS X (probably on other UNIX as well) this is going to be a number below 500. Best practice requires that it be unique, so you have to see what's already been assigned and consult with documentation of the service you're installing. Below is a dump of the groups that come on Mac OS X (Tiger)¹. You can see that there are already pre-existing groups which could be used for many services which aren't included on Mac OS X client.

system_username is a unique name of the system service agent. Examples: tomcat, postfix, amavis, sendmail, etc. Note: some of these names are traditional, like www, tomcat, postfix, etc. Others are up to you to come up with a naming convention. I recommend using the traditional name whenever possible.

user_id is the unique numeric primary number of the user agent under which the service will run. As Tim Parker points out this is a number below 500, but not a number already assigned to

another agent account. Below is a dump of the accounts that come on Mac OS X (Tiger)².

primary_group_id is the primary group which the system agent will belong to. This is the same number which was created in *group_id*.

user_shell is the shell under which the service agent will operate. In most cases this can be set to */usr/bin/false*.

user_home by convention is set to a benign directory. In case the system agent account or its service has a vulnerability you don't want the agent having access to sensitive directories. Typically these are */var/empty*, or */var/service_directory*. Service directory is a directory which you would create for exclusive use by the service.

passwd for system agents this is set to "*", or no password.

1 System groups in Mac OS X (Tiger)

nidump group .

```
nobody:*:-2:
nogroup:*:-1:
wheel:*:0:root
daemon:*:1:root
kmem:*:2:root
sys:*:3:root
tty:*:4:root
operator:*:5:root
mail:*:6:
bin:*:7:
procview:*:8:root
procmmod:*:9:root
staff:*:20:root
lp:*:26:
postfix:*:27:
postdrop:*:28:
certusers:*:29:root,jabber,postfix,cyrusimap
utmp:*:45:
uucp:*:66:
dialer:*:68:
network:*:69:
www:*:70:
mysql:*:74:
sshd:*:75:
qtss:*:76:
mailman:*:78:
appserverusr:*:79:
```

admin:*:80:root,
appserveradm:*:81:
clamav:*:82:
amavisd:*:83:
jabber:*:84:
xgridcontroller:*:85:
xgridagent:*:86:
appowner:*:87:
windowserver:*:88:
accessibility:*:90:
tokend:*:91:
securityagent:*:92:
unknown:*:99:
everyone::12:
authedusers::50:
interactusers::51:
netusers::52:
consoleusers::53:
owner::10:
group::16:
smmsp::25:

2 System users on Mac OS X (Tiger)

nidump passwd .

nobody:*-2:-2::0:0:Unprivileged User:/var/empty:/usr/bin/false
root:*****:0:0:0:0:System Administrator:/var/root:/bin/tcsh
daemon:*:1:1::0:0:0:System Services:/var/root:/usr/bin/false
unknown:*:99:99::0:0:0:Unknown User:/var/empty:/usr/bin/false
lp:*:26:26::0:0:0:Printing Services:/var/spool/cups:/usr/bin/false
uucp:*:4:4::0:0:0:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
postfix:*:27:27::0:0:0:Postfix User:/var/spool/postfix:/usr/bin/false
www:*:70:70::0:0:0:World Wide Web Server:/Library/WebServer:/usr/bin/false
eppc:*:71:71::0:0:0:Apple Events User:/var/empty:/usr/bin/false
mysql:*:74:74::0:0:0:MySQL Server:/var/empty:/usr/bin/false
sshd:*:75:75::0:0:0:sshd Privilege separation:/var/empty:/usr/bin/false
qtss:*:76:76::0:0:0:QuickTime Streaming Server:/var/empty:/usr/bin/false
cyrusimap:*:77:6::0:0:0:Cyrus IMAP User:/var/imap:/usr/bin/false
mailman:*:78:78::0:0:0:Mailman user:/var/empty:/usr/bin/false
appserver:*:79:79::0:0:0:Application Server:/var/empty:/usr/bin/false
clamav:*:82:82::0:0:0:Clamav User:/var/virusmails:/bin/tcsh
amavisd:*:83:83::0:0:0:Amavisd User:/var/virusmails:/bin/tcsh
jabber:*:84:84::0:0:0:Jabber User:/var/empty:/usr/bin/false
xgridcontroller:*:85:85::0:0:0:Xgrid Controller:/var/xgrid/controller:/usr/bin/false
xgridagent:*:86:86::0:0:0:Xgrid Agent:/var/xgrid/agent:/usr/bin/false
appowner:*:87:87::0:0:0:Application Owner:/var/empty:/usr/bin/false

windowserver*:88:88::0:0:WindowServer:/var/empty:/usr/bin/false
tokend*:91:91::0:0:Token Daemon:/var/empty:/usr/bin/false
securityagent*:92:92::0:0:SecurityAgent:/var/empty:/usr/bin/false

Revision #1

Created Wed, Jun 20, 2007 11:04 AM by Garcia, Jose

Updated Wed, Jun 20, 2007 11:04 AM by Garcia, Jose