

# System Administration

## Contents

<b>1</b>	<b>Users and account management</b>	<b>4</b>
1.1	User accounts	4
1.2	Service accounts	5
1.3	Roles	5
1.4	Superuser account	5
1.4.1	SUperuser DO: sudo(1m)	6
1.5	Managing accounts	6
1.5.1	useradd	6
1.5.2	userdel	7
1.5.3	usermod	7
1.5.4	groupadd	7
1.5.5	groupdel	7
1.5.6	groupmod	7
1.5.7	roleadd	7
1.5.8	roledel	7
1.5.9	rolemod	7
1.5.10	passwd	7
1.6	Role-Based Access Control (RBAC)	7
1.6.1	What is RBAC	8
1.6.2	How to use RBAC	8
1.7	Active Directory Integration	8
1.7.1	Introduction	8
1.7.2	Native AD integration	9
1.7.3	Kerberos and LDAP	9
1.7.4	winbind	9
<b>2</b>	<b>Management of System Resources</b>	<b>10</b>
2.1	Basic system information	10
2.1.1	System processes	10
2.1.2	Disk usage	10
2.1.3	Largest files in a directory	10
2.1.4	Who is logged on to the system	10
2.1.5	List all software packages installed on the system	10
2.2	System shutdown, reboot, ...	10
<b>3</b>	<b>Service Management Facility</b>	<b>11</b>
3.1	SMF Basic Commands	12

3.1.1	svcs	12
3.1.2	svcadm	14
3.1.3	svccfg	15
3.1.4	svcprop	15
3.1.5	inetadm	15
3.1.6	inetconv	15
3.2	Troubleshooting	15
3.2.1	Basic Strategy	15
3.2.2	Corrupt Service Configuration: Revert to an Old Configuration	17
3.2.3	Boot Failure	17
3.2.4	Maintenance Mode	17
<b>4</b>	<b>Configuring and Tuning</b>	<b>17</b>
4.1	Configuring a UPS	18
4.2	Fault management (FMA)	18
4.3	Virtual Terminals/Consoles (VT)	18
4.4	Service management (SMF)	19
4.5	Systems logging and monitoring	19
<b>5</b>	<b>Illumos boot process</b>	<b>20</b>
<b>6</b>	<b>Security</b>	<b>20</b>
<b>7</b>	<b>Zones</b>	<b>20</b>
7.1	Zone networking model	21
7.2	Quick Setup Example	21
7.3	System repository configuration	23
7.4	Troubleshooting	24
7.4.1	Fixing zone installation issues	24
<b>8</b>	<b>Storage</b>	<b>24</b>
8.1	Mounting file systems	24
8.1.1	Mounting and Unmounting ISO images	25
8.1.2	Mounting NTFS Volumes - 3rd party support	25
8.2	Configuring OpenIndiana as an iSCSI Target Server - (COMSTAR)	26
8.3	System backups	26
8.4	ZFS	26
8.4.1	Importing ZFS disks	26
8.4.2	How does one mirror their root zpool?	27
8.4.3	How does one create additional zpools?	27
8.4.4	Modifying zpool settings and attributes	27
8.4.5	Modifying zfs file system settings and attributes	27
8.4.6	How does one create additional zfs datasets?	27
8.4.7	Configuring system swap	27
<b>9</b>	<b>Virtualization</b>	<b>28</b>
9.1	OpenIndiana as a virtualization host server	28
<b>10</b>	<b>Localization</b>	<b>28</b>
<b>11</b>	<b>Dtrace</b>	<b>28</b>

<b>12 Configuring Networking</b>	<b>28</b>
12.1 Automatic Configuration (NWAM) . . . . .	28
12.2 Changing from NWAM to Manual Configuration . . . . .	29
12.3 More on Automatic Configuration (NWAM) . . . . .	30
12.3.1 Using NWAM configuration tools . . . . .	30
12.3.2 Network automagic online help . . . . .	34
12.3.3 Troubleshooting NWAM . . . . .	34
<b>13 Clustering with Open HA Cluster</b>	<b>34</b>

Once OpenIndiana has been installed, the system will require monitoring to ensure smooth operation. Software will periodically have to be updated, redundant software removed, new users added to the system, etc. All these activities and many more are referred to as system administration.

Basic system administration can be reduced to a number of common tasks:

- Users and account management
- Management of system resources
- Installation and maintenance of software

While it is certainly possible to add more to this list or select alternative items, this small selection is readily absorbed and is convenient to illustrate a number of essential concepts central to OpenIndiana system administration.

① **NOTE:**

Administrative commands are usually expected to be run with elevated privileges - directly from root user, via `sudo(1M)` or `pfexec` (if user was granted privileges via RBAC). In this document commands which require elevated privileges are prefixed with “#”. Commands, which don’t require elevated privileges, are prefixed with “\$”.

## 1 Users and account management

OpenIndiana allows multiple users to work on the same computer at the same time. Only one person can sit in front of the monitor and keyboard. However, many can be remotely logged into machine and work on it. If a user wants to use the system, he needs an account.

There are also special service accounts which are used by system services.

### 1.1 User accounts

User accounts are primarily used for day-to-day tasks. Every user accessing the system should have his own unique account. This allows the administrator of the system to find out who is doing what. This also allows him to set different access rights for each user separately.

When system is installed, usually one user account is created. Additional accounts can be added later.

Every user account has some attributes associated with it.

- **username** - name of the account, which is typed at the login screen. Username format is briefly described in [passwd\(4\)](#)
- **password** - password associated with the account.

△ **CAUTION:**

Accounts without password should not exist on the system as they could put the system at the security risk!

- **UID** (user ID) - unique numerical ID of the account in the system. The maximum value for uid is 2147483647. However, for compatibility reasons one should not use numbers over 65535.
- **GID** (group ID) - unique numerical ID of the account's primary group.
- **comment** (also referred to as gecos) - account description Often this field is set to real user name.
- **home directory** - a path where user will be after he logs into the system.
- **login shell** - user's initial shell program.
- **password last change time** - time when the password was lastly changed.
- password aging information - several [shadow\(4\)](#) fields determining when password should be changed
- **min** - the minimum number of days required between password changes;
- **max** - the maximum number of days the password is valid;
- **warn** - the number of days before password expires that the user is warned.

## 1.2 Service accounts

Service (system) accounts are used by applications, which are running on the system and are providing some services to the network such as DNS, SMTP or WWW. For security reasons these services are ran under non-privileged accounts.

OpenIndiana comes with several service accounts such as `webserverd` for web servers, `pkg5srv` for `pkg(5)` server or `nobody`. `nobody` is a system account for services needing unprivileged user. However, the more services are ran under this account, the more privileged it becomes as it gains access to service processes and files.

## 1.3 Roles

A role is a basic unit of Role-Based access control (RBAC) or set of privileges one can assume. A role can be thought of as a no-login account. It has most of the attributes of normal user account and is identified like normal user, but is not allowed to log into a system directly. One should login using regular account and use [su\(1M\)](#) to assume the role.

## 1.4 Superuser account

Every UNIX-like system has the superuser account, named `root`, used for system administrative tasks. This account has UID 0.

Using this account for everyday usage like web browsing, email reading or movie watching is not recommended as `root` account can operate without any restrictions or limits and could cause serious damage to the system.

If you created user during installation, `root` is created as role (not a regular account). This role is assigned to the user created during the installation. This means that you can't directly log into a system using the `root` account. One has to log in as the created user and switch to `root` role using [su\(1M\)](#).

However, if the user was not created during installation, then the `root` is created as regular account and is able to log in directly. Note, that even when `root` is created as role, one can use this account directly to log into the system when it's booted in single user mode.

### 1.4.1 Superuser DO: sudo(1m)

It is not always feasible for one user to perform all administrative tasks. It would be more flexible if some tasks could be performed by some, say, experienced users. To enable some users to carry out a command with *all* root privileges, or to *do* an administrative command `sudo(1M)` can be used.

The `sudo` command, i.e., superuser do, permits a regular user to execute the specified set of commands with superuser privileges without having to become the superuser.

If user was permitted to use some commands with superuser privileges via `sudo` he/she can execute them with elevated privileges simply starting command with `sudo`.

To permit a user to use `sudo`, the superuser edits `/etc/sudoers`.

This can be done using special `visudo(1M)` tool. `visudo` tool edits `/etc/sudoers` file performing various syntax checks. `sudoers(1)` provides details on the precise means to appropriately grant user elevated privileges via `sudo`.

Example:

To shutdown the system, root privileges are required. If a standard user issues the `shutdown` command, the system will issue a warning. However, if the user has been enabled to use `sudo`, then the user can now shutdown the system:

```
$ sudo shutdown -i5 -g0 -y
```

## 1.5 Managing accounts

There are several tools in OpenIndiana to manage user accounts. They are listed in the table below.

Tool	Description
<a href="#">useradd(1M)</a>	creates new account on the system
<a href="#">userdel(1M)</a>	deletes account from the system
<a href="#">usermod(1M)</a>	modifies account information on the system
<a href="#">groupadd(1M)</a>	creates group on the system
<a href="#">groupdel(1M)</a>	deletes group from the system
<a href="#">groupmod(1M)</a>	modifies group information on the system
<a href="#">roleadd(1M)</a>	creates new role on the system
<a href="#">roledel(1M)</a>	deletes role from the system
<a href="#">rolemod(1M)</a>	modifies role information in the system
<a href="#">passwd(1)</a>	changes login password and password attributes

### 1.5.1 useradd

`useradd` is a program to create user accounts on the system. When creating account one can set some attributes of the newly created account such as comment, group membership, home directory path, UID number of the account or login shell.

### **1.5.2 userdel**

One can use `userdel` to remove the account from the system.

### **1.5.3 usermod**

`usermod` is used to modify properties of existing account.

### **1.5.4 groupadd**

`groupadd` creates a new group definition on the system by adding the appropriate to the `/etc/group` file.

### **1.5.5 groupdel**

`groupdel` deletes a group definition from the system.

### **1.5.6 groupmod**

When one needs to modify group attributes, `groupmod` should be used.

### **1.5.7 roleadd**

`roleadd` is used create roles in the system.

### **1.5.8 roledel**

`roledel` deletes selected role from the system.

### **1.5.9 rolemod**

`rolemod` modifies role's information on the system.

### **1.5.10 passwd**

`passwd` changes password for user accounts. An unprivileged user may only change the password for his/her own account, while the superuser may change the password for any account. Privileged user can also use `passwd` to change login password attributes (such as expiration date) or lock the account.

## **1.6 Role-Based Access Control (RBAC)**

The *all-or-nothing* power assigned to the root user has its obvious limitations. While `sudo` is an improvement by limiting root privileges for only several commands, more granular control is often desired.

An improvement on the above systems would be one in which privileges could be assigned on a more fine-grained and selective basis.

Imagine a user assigned the task of administrating some particular hardware, for example, printers attached to the system. A more desirable system would be one in which this user had the ability to permit users to use a printing device, remove print jobs from the print spool or add new printers to the system. Moreover, it would be advantageous if it were possible to assign privileges to perform only these actions and none other.

RBAC was developed to accomplish this.

### 1.6.1 What is RBAC

### 1.6.2 How to use RBAC

The root user or a user with sudo enabled can shutdown the system. We can use RBAC to enable a user to be able to shutdown the system. However, we can create a role that allows only the privilege to shutdown the system, and no additional privileges. We can then assign this role to one or several users.

- assign a privilege to a role to shutdown the system

```
# roleadd shutdown
```

- Assign a password

```
# passwd shutdown
```

- Assign this role to a user

```
# usermod -R shutdown whoever
```

- Create a SHUTDOWN profile

```
# echo "SHUTDOWN:::profile to shutdown:help=shutdown.html" >>
```

```
↪ /etc/security/prof_attr
```

- Okay, now assign the role profile SHUTDOWN to the role shutdown

```
# rolemod -P SHUTDOWN shutdown
```

- Assign some administrative command to profile

```
# echo "SHUTDOWN:suser:cmd:::/usr/sbin/shutdown:uid=0" >> /etc/security/exec_attr
```

- Use it

```
$ su shutdown
```

```
# shutdown -i5 -g0 -y
```

Now user whoever can shutdown the system.

The `pfexec` command is more flexible in the number of privileges that can be assigned to a user.

## 1.7 Active Directory Integration

### 1.7.1 Introduction

There are at least three different possible approaches for Active Directory authentication and each has its pros and cons.



1. Use the new native AD integration with **idmap**, **nss\_ad** and **kclient**, this will work with CIFS and NFS out of the box.
2. Use Kerberos and LDAP (**kclient**, **ldapclient**, **pam\_krb5** and **nss\_ldap**).
3. Use **windbind** (**pam\_winbind** and **nss\_winbind**).

### 1.7.2 Native AD integration

- Pro: Fully integrated and native tools only
- Cons: Doesn't work for UNIX services other than CIFS and NFS. The ephemeral id mapping strategy supposedly wasn't designed for other UNIX services. As a result several problems arise, one of them is that the mappings aren't constant over the lifetime of UNIX processes which severely breaks UNIX semantics. Depending on your UNIX service you will see unexpected results or even process crashing.

In order to use this approach with any UNIX service (eg **FTP**) you need to enable *directory-based name mapping* and install **IDMU** (Identity Management for UNIX) on the AD server.

Refer to the original documentation from Oracle for getting this working: [nss\\_ad](#), [CIFS](#).

### 1.7.3 Kerberos and LDAP

- Pro: Fully integrated and native tools only
- Cons: Requires installation of additional role services (IDMU, Identity Management for UNIX) on the Active Directory side

#### ① NOTE:

On the Wiki the 'Kerberos and LDAP' page was a separate detailed article on configuration of Windows Server 2008 Active Directory to work with OI. As of 2021, Windows Server 2008 is EoL. This section should not be migrated until it has been checked and updated for recent Windows. Ideally this information should be on a separate page (potentially community contributions) as it's large and contains a lot of Windows information.

### 1.7.4 winbind

- Pro: Easy setup, no AD modification
- Cons: Depends on 3rd party software (Samba), group membership resolution didn't work

#### ① NOTE:

As above note, the 'winbind' page was a separate detailed article which needs to be checked and updated before it's migrated.

## 2 Management of System Resources

### 2.1 Basic system information

#### 2.1.1 System processes

```
$ prstat
```

This command provides a host of information on all processes running on the system. Some of the information provided is as follows:

- percentage of CPU used by each process
- amount of memory consumed by each process
- unique id of each process (which can, for example, be used to stop the process)

#### 2.1.2 Disk usage

```
# df -h
```

Provides information on disk size, amount of space used and available free space for all attached storage devices. The `-h` option reports this information in human readable format.

#### 2.1.3 Largest files in a directory

Go to the directory using the `cd` command and issue the following command:

```
$ du | sort -n
```

This will list the size of each file in the current directory and all sub-directories, starting with the smallest up to the largest files.

#### 2.1.4 Who is logged on to the system

```
$ listusers
```

#### 2.1.5 List all software packages installed on the system

```
$ pkg list
```

### 2.2 System shutdown, reboot, ...

OpenIndiana defines a number of different system states known as run-levels. You can change from one system state to another by using the `shutdown` command and specify the run-level using the `i` option. You can always determine the run-level via `who -r`.

You must be root or have root privileges (e.g., using `sudo`) to send the system into a different state, i.e., turn off, reboot, etc. Shutdown and turn off all hardware (if supported by the hardware) now:

```
# shutdown -i5 -g0 -y
```

Changing the run-level of the system can be disruptive to other users currently using the system. Thus, it is always wise to establish who is currently logged onto the system before changing the run-level.

- `-i [run-level]` is used to specify the run-level. This is either a digit or a single letter. Here are some run-levels available:
- `5` stop all system services, and turns off hardware devices, etc.
- `6` reboot the system.
- `1` single-user mode. Primarily used for system maintenance.
- `s` single-user mode where only a command line terminal is available.
- `-g [seconds]` is used to specify the number of seconds after which to commence shutting down services. `0` immediately initiates shutting down all services.
- `-y` automatically answers all system questions with 'yes'. The shutdown process is not interrupted by system prompts requiring user-interactive intervention.

### 3 Service Management Facility

Services are an extension to processes. The administration of services is carried out on OpenIndiana using *Service Management Facility*, commonly known as *SMF*.

As application become more complex, their demands on system resources and peripheral resource increase. Modern applications often require more resource to provide more services. Resources such as an internet connection, a web server running in the background, a databank up and running in an appropriate state or mode of operation are increasingly found to be the prerequisite of modern applications. Although the application may provide users with a single service, the application might require many processes before it can itself run.

To provide some system functionality, more than one process is required and some of these processes might depend on other processes. A modern application that provides some functionality might require a group of interrelated processes. We would like to start, stop, analyse, diagnose, in other words, manage the group as a single unit. We refer to such a unit as a *service* and the mechanism of providing this on OpenIndiana as *Service Management Facility*.

SMF was originally developed to improve limitations of the old startup mechanism of the Solaris operating system using scripts known as `init.d`.

Service Management Framework on OI	Purpose
<a href="#">smf(7)</a>	Service Management Facility

A service is a definition of how a service should be started while a service instance is a precise configuration. Some services can have multiple instances whereas others are defined to be a singleton.

Each service instance can be identified by a FMRI which uniquely defines each instance, which is why the SMF commands use FMRI to identify services. A SMF FMRI is composed of three sections, the sections are delimited by a colon:

```
service resource:service name:service instance
```

FMRI are found in various areas: software packages, ZFS, etc., and the first part denotes this area or *scheme*. For software packages the scheme is `pkg:`, while for services the scheme is `svc`.

Many commands use the FMRI to identify service instances, but it is not the only way of specifying a service instance to the commands. In this manual, nomenclature is simplified as `[service]` as a unique identification of a service.

- [Opensolaris documentation](#)

### 3.1 SMF Basic Commands

Command	Purpose
<a href="#">svcs(1)</a>	display information about services
<a href="#">svcadm(7)</a>	manage services (enable/disable, ...)
<a href="#">svccfg(8)</a>	configure services
<a href="#">svccprop(1)</a>	display service configuration properties
<a href="#">inetadm(8)</a>	initialise service managed by <code>inetd</code>
<a href="#">inetconv(8)</a>	convert <code>inetd</code> service to smf services

Use of the SMF commands require relevant privileges. The following RBAC profiles can be made available to all a user to become a SMF administrator:

RBAC profile	Purpose
Service Management	manage services. A service manager can manipulate any service in any way
Service Operator	administer services. A service operator can enable or disable any service.

Further details: [smf\\_security\(7\)](#)

#### 3.1.1 svcs

This command is used to display services and their relevant status. It is also used to provide a list of services that depend on a service, and it can also display a list of services that a service requires to operate.

All services generate log files and the location of a log file associated with a service can be obtained using this command. A list of processes required by a service can be displayed using this command.

*Usage:* `svcs [options] [FMRI]`

Option	Information to Display
	enabled services
<code>?</code>	detailed help
<code>a</code>	all services
<code>d [service]</code>	services that this service requires

Option	Information to Display
D [service]	services that require this service
l [service]	verbose information on service
L [service]	log file associated with service
o column,...	various information as defined by <i>columns</i>
p [service]	processes associated with service
x	details on services that are enabled but not running or prevent other services from running
v	more verbose output for some options
z [zone]	services in zone

- **service:** to specify a service use the FMRI, an FRMI instance or a FMRI pattern. Obtain a list of service FMRIs via `-o FMRI`.
  - **column:** comma separated column names
- **desc::** description of service
- **fmri::** Fault Management Resource Identifier
- **inst::** service instance
- **svc::** name of service
- **state::** service state: uninitialised, offline, online, maintenance, disabled, degraded

### 3.1.1.1 Examples List services and their status

```
svcs
svcs -a
svcs -o svc,state,desc
```

#### Get printer information

```
> svcs -o svcs,desc | grep -i print
application/print/service-selector print service selector
application/cups/scheduler CUPS Print Spooler
> svcs -l scheduler
fmri          svc:/system/scheduler:default
name          default scheduling class configuration
enabled       true
state         online
next_state    none
state_time    March 27, 2023 at 08:03:54 AM CEST
logfile       /var/svc/log/system-scheduler:default.log
restarter     svc:/system/svc/restarter:default
dependency    require_all/none svc:/system/filesystem/root (online)

fmri          svc:/application/cups/scheduler:default
name          CUPS Print Spooler
enabled       true
state         online
next_state    none
state_time    March 27, 2023 at 08:03:57 AM CEST
logfile       /var/svc/log/application-cups-scheduler:default.log
```

```

restarter      svc:/system/svc/restarter:default
contract_id    42
dependency     require_all/none file:///localhost/etc/cups/cupsd.conf (online)
dependency     require_all/none svc:/system/filesystem/minimal (online)
dependency     optional_all/error svc:/network/loopback (online)
dependency     optional_all/error svc:/milestone/network (online)

```

### 3.1.2 svcadm

Use this command to change the status of a service: enable, disable, etc.

*Usage:* `svcadm [options] [subcommand] [subcommand options] [service]`

options	purpose
v	verbose
z [zone]	command applies to the zone specified

subcommand	subcommand option	Purpose
enable		enable service to online state
	r	enable service, but also recursively enable its dependencies
	t	enabling a service as persistent, even after rebooting. This option enables the service <i>only temporarily</i> until the next system boot
disable		disable service to offline state
	c	add a comment which can be viewed by <code>svcs</code>
	t	disable service <i>temporarily</i> . The service will be enabled on ensuing boots
restart		restart service
refresh		re-read service configuration, so any configuration changes will take effect after a service restart
clear		for a service in a <i>maintenance</i> state, signal the service as repaired.
		for a service in a <i>degraded</i> state, attempt to bring the service online

#### 3.1.2.1 Examples Restart a service

```

$ date
XXXXX, 2023 at 03:26:50 PM CEST
# svcadm restart application/cups/scheduler
# svcs -l application/cups/scheduler | grep state_time
XXXXX, 2023 at 03:27:02 PM CEST

```

First, we check the system time which is 3:26:30 PM. We then restart the CUPS printer scheduler, then check the status of the service using `-l` and extract the service property `stat_time` to obtain the time at which the service became online.

### 3.1.3 `svccfg`

This command is used to manage service configurations.

*Usage:* `svccfg [options] -s [FMRI]`

### 3.1.4 `svccprop`

This is used to retrieve service instance properties. It is also used to snapshots. It can also be used to validate the existence of a property.

options	purpose
[service]	display all properties of service
v	verbose
z [zone]	command applies to the zone specified

Refer to the manual page for details: [scvprop\(1\)](#)

### 3.1.5 `inetadm`

### 3.1.6 `inetconv`

## 3.2 Troubleshooting

### 3.2.1 Basic Strategy

Here is general methodology intended as an introduction in how to resolve a service that fails.

`svcs -xv`

This command provides the following information: - a possible reason for the failure - location of the log file associated with the service - references for further reading

Analysis during this step will frequently suffice to resolve your issue. However, this is not always the case.

`svcs -d FMRI`

This command provides a list of services that the failed service requires. The failed service might be failing due to a service that it depends on not operating appropriately, although its status is online and it *appears* to function correctly.

`svcs -l FMRI`

While this command provides similar information provided by the first command, this command will also provide information on services that are online and but might exhibit dubious behaviour. This command will provide information similar to the first command.

```
svcs -d FMRI
```

Should analysis of the previous commands not be sufficient to resolve the issue, examination of the processes associated with suspicious service might be necessary. Use this command to list all processes associated with the service. Use the tools from the previous section, System Monitoring, to scrutinise each process listed.

**3.2.1.1 Examples** To illustrate troubleshooting, we manipulate a service by removing a dependency:

- move a dependency file `/etc/cups/cupsd.conf`
- refresh and restart the service
- Use SMF commands in an attempt to reveal the cause of the failure

```
# svcs -l svc:/application/cups/scheduler:default
fmri          svc:/application/cups/scheduler:default
name          CUPS Print Spooler
enabled       true
state         online
next_state    none
state_time    XXXXX XX, 2023 at 09:18:13 AM CEST
logfile       /var/svc/log/application-cups-scheduler:default.log
restarter     svc:/system/svc/restarter:default
contract_id   42
dependency    require_all/none file:///localhost/etc/cups/cupsd.conf (online)
dependency    require_all/none svc:/system/filesystem/minimal (online)
dependency    optional_all/error svc:/network/loopback (online)
dependency    optional_all/error svc:/milestone/network (online)
```

The service is online and is operating satisfactorily.

Rename `/etc/cups/cupsd.conf`, refresh the configuration and restart the service, will cause the service to fail:

```
# mv /etc/cups/cupsd.conf /etc/cups/cupsd.conf.orig
# svcadm refresh svc:/application/cups/scheduler:default
# svcadm restart svc:/application/cups/scheduler:default
```

Obtain a list of failed services:

```
# svcs -xv
svc:/application/cups/scheduler:default (CUPS Print Spooler)
  State: offline since March 29, 2023 at 07:25:48 PM CEST
  Reason: Dependency file:///localhost/etc/cups/cupsd.conf is absent.
    See: http://illumos.org/msg/SMF-8000-E2
    See: man -M /usr/share/man -s 8 cupsd
    See: /var/svc/log/application-cups-scheduler:default.log
  Impact: This service is not running.
```

We always obtain a reason which in our case pinpoints the error precisely. This is not always the case.



### 3.2.2 Corrupt Service Configuration: Revert to an Old Configuration

SMF periodically takes snapshots of the service configuration so that it is always possible to revert to a previous configuration.

```
# List all cups services:
$ svcs | grep -i cups
legacy_run      16:33:35 lrc:/etc/rc3_d/S99cups-browsed
online          14:33:25 svc:/application/cups/scheduler:default
# list snapshots associated with the cups service
$ svccfg -s svc:/application/cups/scheduler:default listsnap
initial
last-import
running
start
# There are four snapshots available one of which is currently running.
# Lets suppose we had a corrupt config and would like to revert to the initial
# cups service configuration:
$ svccfg -s svc:/application/cups/scheduler:default revert initial
# re-read configuration
svcadm refresh svc:/application/cups/scheduler:default
svcadm restart svc:/application/cups/scheduler:default
```

### 3.2.3 Boot Failure

- On the boot menu, select =3= to load boot prompt

3. Escape to loader prompt

- Now boot without services by entering: boot -m milestone=none:

```
OK boot -m milestone=none
```

- Login as root and enable all services:

```
svcadm milestone all
```

- Now the system will boot and fail. So use svcs to determine which services are failing:

```
svcs -a
```

### 3.2.4 Maintenance Mode

## 4 Configuring and Tuning

There are a few tools to configure and tune an OpenIndiana system. One of the tools is sysdng, a tool that is used by the current OpenIndiana installer to setup static IP addresses when NWAM (automatic network configuration) is not used.

For more information on sysdng, see the manpage and example config file :

```
# man sysdng
```

The configuration file is :

```
/etc/sysding.conf
```

There is also a logfile :

```
/var/log/sysding.log
```

For example a simple `/etc/sysding.conf` configuration file for a static IP is :

```
setup_interface e1000g0 v4 10.0.2.16
setup_route default 10.0.2.2
```

This service is meant to be run only once and sets a boolean flag `config/finished`. In case you want to run `sysding` again, you'll have to force the finished flag to false :

```
svccfg -s sysding:system
setprop config/finished = false
refresh
```

## 4.1 Configuring a UPS

- NUT?

## 4.2 Fault management (FMA)

< place holder >

## 4.3 Virtual Terminals/Consoles (VT)

Virtual Terminals/Virtual Consoles (VT) are used to switch between terminals and using system in text mode with `Ctrl+Alt+F1,F2..F8` key combinations.

### ❗ NOTE:

Switching to VTs using `Ctrl+Alt+Fn` during current desktop session (at **VT7**) can result in **X server** and **lightdm** (or **gdm**) restarting and stopping all applications running within it. Currently, there could be problems with getting back to `gdm/Xorg` session if switching to VTs after `gdm` restart. Use `svcadm restart lightdm` (or `svcadm restart gdm`) command again, to have `lightdm/gdm Xorg` session restarted at **VT8** (`Ctrl+Alt+F8`).

At fresh OpenIndiana install, VT/Consoles are **not enabled by default**. One needs to set up `vtdaemon` and `console-login:vt2` (till `:vt6`) and enable **vtdaemon** options/hotkeys property:

```
pfexec svcadm enable vtdaemon
pfexec svcadm enable console-login:vt2
pfexec svcadm enable console-login:vt3
pfexec svcadm enable console-login:vt4
pfexec svcadm enable console-login:vt5
pfexec svcadm enable console-login:vt6
```

Or do that in a one-liner Bash script: `for i in 2 3 4 5 6 ; do pfexec svcadm enable console-login:vt$i; done;`

Then, enable options/hotkeys property (*Ctrl+Alt+Fn*) to switch VTs and refresh and restart **vtdaemon** service:

```
pfexec svccfg -s vtdaemon setprop options/hotkeys=true
pfexec svcadm refresh vtdaemon
pfexec svcadm restart vtdaemon
```

Optionally, you can also disable VT consoles auto screen locking (recommended for personal use, not recommended on server): `pfexec svccfg -s vtdaemon setprop options/secure=false`

The above was inspired by [this blog by Danx on Virtual Consoles](#).

## 4.4 Service management (SMF)

### ① NOTE:

ITEMS TO WRITE ABOUT: provide more detailed explanations.

List services:

```
$ svcs # list (permanently) enabled services
$ svcs -a # list all services
$ svcs -vx # list faulty services
```

Get information about a service:

```
$ svcs <service name> # one-line status
$ svcs -x <service name> # important information
$ svcs -d <service name> # check the service's dependencies
$ svcs -l <service name> # all the available information
```

Start a service:

```
# svcadm enable <service name> # permanently enable/start
# svcadm enable -t <service name> # temporary start (won't survive a reboot)
# svcadm enable -r <service name> # permanently enable/start service along with its
↳ dependencies
```

Restart / reload a service:

```
# svcadm refresh <service name> # reload the service's configuration
# svcadm restart <service name> # restart the service
```

## 4.5 Systems logging and monitoring

### ① NOTE:

ITEMS TO WRITE ABOUT:

- Where to find the logs (`/var/log`, `/var/svc/log`).

## 5 Illumos boot process

< place holder >

## 6 Security

< place holder >

## 7 Zones

### ① NOTE:

#### ITEMS TO WRITE ABOUT:

- Need to mention some of the changes to zone management...e.g..
  - sys-unconfig gone.
  - sysdng replaced syscfg
  - now have to have DNS, root password, etc. all configured inside the zone before being able to logon using `zlogin -C <zonenumber>`, otherwise have to do `zlogin <zonenumber>`.

So a fair amount of stuff has changed there.

Zones are an OpenIndiana feature that provides [operating system-level virtualization](#). Each zone is managed as a completely separate OpenIndiana machine. Zones have very low overhead and are one of the most efficient forms of OS virtualization.

The global zone (GZ) is the operating system itself, which has hardware access. From the global zone, non-global zones (NGZ) are created and booted. Boot time for non-global zones is very fast, often a few seconds. The CPU, network, and memory resources for each zone can be controlled from the global zone, ensuring fair access to system resources. Disk space access is usually controlled by ZFS (with quotas and reservations if needed), as well as mounting of filesystem resources with NFS or lofs. As with other forms of virtualization, each zone is isolated from the other zones – zones cannot see processes or resources used in other zones. The low marginal cost of a zone allows large systems have tens or even hundreds of zones without significant overhead. The theoretical limit to the number of zones on a single platform is 8,192.

Different releases of (Open)Solaris used different packaging distribution method for the global zone. OpenIndiana zones use two basic brands - “ipkg” and “nlipkg”, which are based on IPS Packaging. The brand determines how zone is initialized and how zone’s processes are treated by kernel. Both type of zones represent a PKG image. “ipkg”-branded zones are tightly coupled with GZ. Image pakaging system (IPS) knows about ipkg-branded zones and can perform several actions simultaneously in GZ and NGZ. For example, you can update all your zones and GZ with a single “pkg update -r” command. IPS can ensure some dependencies between packages in GZ and NGZ. To allow this it cheks that NGZ’s publishers are a superset of GZ’s publishers and their properties are the same (for example, stickiness or repository location). As this is not always suitable for development zones, “nlipkg”-branded zones were introduced. “nlipkg”-branded zone behave like completely independent instance and IPS ignores them during operations in GZ.

An easy way to implement zones is to use a separate ZFS file system as the zone root's backing store. File systems are easy to create in ZFS and zones can take advantage of the ZFS snapshot and clone features. Due to the strong isolation between zones, sharing a file system must be done with traditional file sharing methods (eg NFS).

When each zone is created it comes with a minimal set of packages, and from there you can add and use most packages and applications as required.

## 7.1 Zone networking model

OpenIndiana zones can use one of two networking models: a shared IP stack and an exclusive IP stack. There are pros and cons to each of them.

Low-level system networking components, such as the ipfilter firewall and the kernel IP routing tables attach to an "IP stack", and are thus either unique to a zone or shared by all zones with the one shared stack. There are also some other nuances, such as that the zones with the shared stack can communicate over IP directly, regardless of their subnetting and, to some extent, default firewall packet filtering (that has to be specially configured), while exclusive-IP zones with addresses in different subnets have to communicate over external routers and are subject to common firewall filtering.

The global zone defines which physical networks and VLANs the NGZ has access to, and hands down the predefined networking interfaces (the NGZ can not use or create other interfaces). Also, while shared networking allows to configure and attach (or detach) network interfaces from GZ to the NGZ "on the fly", changes in exclusive networking require reboot of the zone to propagate device delegation.

A zone with an exclusive IP stack can have all the benefits of dedicated hardware networking, including a firewall, access to promiscuous sniffing, routing, configuration of its own IP address (including use of DHCP and static network addressing), etc. This requires a fully dedicated NIC. Usually this is a VNICs - a virtual adapter with own MAC address, that operate as if the VNIC was plugged directly into local LAN in a particular (or default) VLAN. Note also that the local zones with an exclusive IP stack are not subject to the host's shared-stack firewall.

### ① NOTE:

Note that if you create zone in VM, the hypervisor can require you to provide some information about its mac addresses. For example, if you configure bridged networking on VirtualBox running on OpenIndiana, you must set secondary-macs property of the VNIC, delegated to VM, to the set of mac addresses of VNICs created inside VMs and enable promiscuous mode on VirtualBox network adapter.

## 7.2 Quick Setup Example

Zone creation consists of two steps - creating zone configuration and zone installation or cloning. Zone configuration determines basic parameters, such as zone's root location and provided resources. Zone configuration is performed using zonecfg tool, zone administration (for example, installation) is performed using zoneadm tool.

For example, we create a simple zone with shared networking model:

```
# zonecfg -z example
example: No such zone configured
Use 'create' to begin configuring a new zone.
zonecfg:example> create
zonecfg:example> add net
zonecfg:example:net> set physical=e1000g0
zonecfg:example:net> set address=192.168.0.10/24
zonecfg:example:net> end
zonecfg:example> set zonepath=/zones/example
zonecfg:example> verify
zonecfg:example> commit
zonecfg:example> exit
```

Here `create` puts you inside the zone configuration program where you can change and update settings particular to the zone specified with `-z`. `zonecfg` break different resource groups of data, you add a new resource with `add`. The next block adds resource “net”, configuring network in default shared ip-type mode. It allows zone to share IP stack with GZ. If you want to get dedicated nic in NGZ, you have to use `set ip-type=exclusive`. In exclusive mode zone has complete control over network interface and you can't assigned address in `zonecfg` prompt. After network configuration `zonepath` is set. It's a location for zone's root file system, which should be a ZFS filesystem. The `verify` command checks that no mistakes were made. Finally changes are committed (saved to zone configuration file).

If you want to use dedicated networking for your zone, you should create VNIC and delegate it to the zone.

```
# dladm create-vnic -l e1000g0 vnic0
```

If you want to specify VLAN id for VNIC, use `-v dladm create-vnic` option:

```
# dladm create-vnic -l e1000g0 -v 123 vnic0
```

Now you can create your zone and delegate VNIC to it (note that we set zone's `ip-type` to `exclusive`):

```
# zonecfg -z example
example: No such zone configured
Use 'create' to begin configuring a new zone.
zonecfg:example> create
zonecfg:example> set ip-type=exclusive
zonecfg:example> add net
zonecfg:example:net> set physical=vnic0
zonecfg:example:net> end
zonecfg:example> set zonepath=/zones/example
zonecfg:example> verify
zonecfg:example> commit
zonecfg:example> exit
```

After configuring a zone you can install it with `zoneadm install` subcommand:

```
# zoneadm -z example install
```

During installation pkg image rooted at `$zonepath/root` is created and minimal set of packages is installed to the image. When installation finishes, zone can be booted with `zoneadm -z`

example boot command. If you want your zone to boot automatically during system startup, you should set autoboot parameter to true during zone configuration:

```
zonecfg:example> set autoboot=true
```

Once zone is booted you can log in locally with `zlogin example`. If you created zone with dedicated network adapter, you should configure it inside zone.

**① NOTE:**

Note, that on first zone boot `sysding(1M)` will set root's password to NP. Before this happened you will not be able to login to zone with `zlogin`, so this command will not work on early startup stage.

## 7.3 System repository configuration

On OpenIndiana it is possible to allow NGZs to access configured publishers via GZ proxy service (so-called zone proxy daemon). This can be useful for sharing pkg cache between zones or to provide network access for performing updates to otherwise restricted zone environment (i.e. to zone without Internet access).

The functionality is provided by series of services in GZ and NGZs. In GZ two services are running: system repository service and zones proxy daemon (see `pkg.sysrepo(1M)`). In NGZ zones proxy client communicates with GZ's zone proxy daemon. System repository service `svc:/application/pkg/system-repository` is responsible for providing access to the package repositories configured in a reference image through a centralized proxy. Zones proxy daemon service `svc:/application/pkg/zones-proxyd` starts on system boot and registers door in each running `ipkg`-branded zone (the door is created at `/var/tmp/zoneproxy_door` path). Later, on zone startup or shutdown `/usr/lib/zones/zoneproxy-adm` is used to notify `zones-proxyd`, so that it could create the door for the zone or to cleanup it. Zones proxy daemon client `svc:/application/pkg/zones-proxy-client:default` runs in NGZ and talks to GZ's `zones-proxyd` via created door.

**① NOTE:**

Note, you can't use system repository with `nlipkg`-branded zones.

IPS determines if it should use zones proxy client in zone based on image's `use-system-repo` property (defaults to False).

To configure your system to use system repository, perform the following actions.

1) In global zone:

```
# pkg install pkg:/package/pkg/system-repository pkg:/package/pkg/zones-proxy
# svcadm enable svc:/application/pkg/system-repository:default
# svcadm enable svc:/application/pkg/zones-proxyd:default
```

2) In non-global zone:

```
# pkg install pkg:/package/pkg/zones-proxy
# svcadm enable svc:/application/pkg/zones-proxy-client:default
# pkg set-property use-system-repo True
```

After this in NGZ's publisher description you'll see system-repository location:

```
# pkg publisher
PUBLISHER          TYPE      STATUS P LOCATION
openindiana.org (non-sticky, syspub) origin   online T <system-repository>
hipster-encumbered (syspub)      origin   online T <system-repository>
```

You can check if your configuration works by issuing `pkg refresh` command in the zone. `pkg(1M)` should contact repository indirectly via `zones-proxy-client`.

To revert your zone to proxy-less configuration, run

```
# pkg set-property use-system-repo False
```

## 7.4 Troubleshooting

Zone configuration and management operations can fail for a number of reasons, sometimes obscure. This section contains information on how to solve different well-known issues.

### 7.4.1 Fixing zone installation issues

Zones on OpenIndiana use ZFS features to manage boot environments. Zone's root and its parent directory should be a ZFS dataset. It's not enough for zone's root (or its parent directory) to be just a directory on ZFS filesystem. If you try to create a zone which root doesn't satisfy this requirement, you can get the following error:

```
# zoneadm -z example install
Sanity Check: Looking for 'entire' incorporation.
ERROR: the zonepath must be a ZFS dataset.
The parent directory of the zonepath must be a ZFS dataset so that the
zonepath ZFS dataset can be created properly.
```

To fix this, you can just uninstall the zone and create its root dataset manually:

```
# zoneadm -z example uninstall
Are you sure you want to uninstall zone example (y/[n])? y
# zfs create rpool/zones/example
# chmod 700 /zones/example
# zoneadm -z example install
```

## 8 Storage

< place holder >

### 8.1 Mounting file systems

#### ① NOTE:

ITEMS TO WRITE ABOUT:

- Need a walkthrough of mounting options for other filesystems...FAT, UFS, etc.



### 8.1.1 Mounting and Unmounting ISO images

One can use [lofiadm\(1M\)](#) to mount ISO images by attaching them to a block device.

```
pfexec lofiadm -a /path/to/foo.iso /dev/lofi/1
```

When the above line is repeated for several ISO images, issue the `lofiadm` command to list which ISO images are attached to which block devices.

```
pfexec lofiadm
Block Device File Options
/dev/lofi/1 /home/scarcry/foo.iso -
/dev/lofi/2 /home/scarcry/bar.iso -
```

Use the [mount\(1M\)](#) command to mount an image:

```
pfexec mount -F hsfs -o ro /dev/lofi/1 /mnt
```

Check the mounted image by issuing `ls` on the mount point.

```
ls /mnt
```

To unmount and detach the image(s):

```
pfexec umount /mnt
pfexec lofiadm -d /dev/lofi/1
```

### 8.1.2 Mounting NTFS Volumes - 3rd party support

#### ① NOTE:

For removable storage devices, first make sure your external disk drive is connected and powered on.

To list attached removable storage devices: `rmformat -l`

Verify the pX partition number that contains the NTFS filesystem, typically “p1”, using `fdisk`. Even though it may seem counterintuitive, include the partition number “p0” as shown by `rmformat` in `fdisk` inquiries.

```
pfexec fdisk /dev/rdisk/c6t0d0p0
```

**8.1.2.1 Additional software installation and configuration** NTFS and FUSE support is provided by Tuxera’s NTFS-3G project that aims at providing a stable NTFS driver for several operating systems.

It is made possible thanks to Jean-Pierre André, on Openindiana page: <http://jp-andre.pageperso-orange.fr/openindiana-ntfs-3g.html> Follow instructions on this page to install. Please install 64-bit package on 64-bit installations.

**8.1.2.2 Mounting the NTFS filesystem** Now mount the NTFS partition using:

```
pfexec ntfs-3g /dev/dsk/c6t0d0p1 /mnt/backup/
```

You can now also add a `vfstab` entry like so:

```
/dev/dsk/c6t0d0p1 /dev/rdisk/c6t0d0p1 /mnt/backup ntfs-3g - no -
```

## 8.2 Configuring OpenIndiana as an iSCSI Target Server - (COMSTAR)

< Place holder for content >

## 8.3 System backups

OpenIndiana offers several backup solutions. Here are just a few of them:

- [Borg Backup](#)
- [Bacula](#)
- Time-Slider
- [rdiff-backup](#)
- Rsync
- [Zetaback](#)
- ZFS exports
- cpio
- tar, zip, etc.

## 8.4 ZFS

### ① NOTE:

ITEMS TO WRITE ABOUT:

Gotcha's such as the following:

<e^ipi> don't suppose there's any solution to this:

<e^ipi> cannot replace 1509280528045021472 with

↪ /dev/dsk/c0t5000C5009204EB9Bd0s0: devices have different sector alignment

<tsoome> that's 512 versus non-512 sector issue

<tsoome> you need to build new pool based on larger sector

<tsoome> if it's mirror, you can attach 512B disk to 4k pool, but not vice

↪ versa...

<e^ipi> well, damn.

<tsoome> that error message is too confusing, should be replaced by more clear

↪ one;)

<e^ipi> I swear this pool is already mix & match, freebsd complained about it

<e^ipi> (but still used it)

<tsoome> there is that thing that ashift is vdev property;

<tsoome> not pool property (one reason why that linux zpool create ashift=

↪ option is bad)

<tsoome> or sort of bad anyhow

### 8.4.1 Importing ZFS disks

#### ① NOTE:

ITEMS TO WRITE ABOUT:

- Talk about the ZFS import command.

#### 8.4.2 How does one mirror their root zpool?

① **NOTE:**

ITEMS TO WRITE ABOUT:

- Adding a 2nd disk to the root pool

#### 8.4.3 How does one create additional zpools?

① **NOTE:**

ITEMS TO WRITE ABOUT:

- zpool create command
  - Mirrors
  - Raidz

#### 8.4.4 Modifying zpool settings and attributes

① **NOTE:**

ITEMS TO WRITE ABOUT:

- zpool get/set commands

#### 8.4.5 Modifying zfs file system settings and attributes

① **NOTE:**

ITEMS TO WRITE ABOUT:

- zfs get/set commands

#### 8.4.6 How does one create additional zfs datasets?

① **NOTE:**

ITEMS TO WRITE ABOUT:

- zfs create command

#### 8.4.7 Configuring system swap

① **NOTE:**

ITEMS TO WRITE ABOUT:

- zfs set command
- swap -l

## 9 Virtualization

< Place holder >

### 9.1 OpenIndiana as a virtualization host server

#### ① NOTE:

ITEMS TO WRITE ABOUT:

- Qemu-KVM (KVM) walkthrough
  - illumos KVM port does not support AMD processors.
  - Intel processors require EPT support.
- Virtualbox walkthrough
  - There is no package for this yet, but folks do have it working, see the wiki for details.

#### ① NOTE:

ITEMS TO WRITE ABOUT:

In a nutshell, most modern Intel processors such as i3, i5, i7, and Xeon provide EPT support. Most older processors such as Core2duo and Core2Quad lack EPT support, and a few of them lack virtualization support at all. You can check your processor for EPT support via the following link: <http://ark.intel.com/Products/VirtualizationTechnology>

## 10 Localization

#### ① NOTE:

ITEMS TO WRITE ABOUT:

Possible resources to help write this section:

- <https://wiki.openindiana.org/oi/4.4+Localization>
- [https://docs.oracle.com/cd/E23824\\_01/html/E26033/glmen.html](https://docs.oracle.com/cd/E23824_01/html/E26033/glmen.html)

## 11 Dtrace

< Place Holder >

## 12 Configuring Networking

### 12.1 Automatic Configuration (NWAM)

During installation of OpenIndiana, there are three options to configure networking : Automatic, Manual (static IP), and None.

Option Automatic enables NWAM and configures all interfaces automatically.

Network Auto-Magic (NWAM) manages network interfaces as they are dynamically added or removed to or from the system, using network profiles, and is able to change network settings on the fly.

NWAM is suitable for servers, laptops, desktops and workstations alike, to automatically configure all wired or wireless network interfaces.

Option Manual disables NWAM and creates a /etc/sysdng.conf file to setup static IP addresses.

Option None can be used to configure networking manually, without NWAM, after installation.

## 12.2 Changing from NWAM to Manual Configuration

If during install you enabled NWAM, and if you want to disable NWAM you can proceed as follows :

```
# svcadm disable physical:nwam
```

Define your IP/hostname in /etc/hosts. For example:

```
192.168.1.22 hostname hostname.local localhost loghost  
# Substittude 192.168.1.22 for YOUR IP
```

Enable the default physical service with svcadm and configure the interface:

```
# svcadm enable physical:default
```

There are multiple ways to configure the interface : using sysdng or directly with ipadm.

For more information on sysdng, see the section on Configuring and Tuning.

To configure an interface with ipadm:

```
# ipadm create-addr -T static -a local=192.168.1.22/24 bge0/v4static
```

or

```
# ipadm create-addr -T dhcp bge0/dhclient
```

The previous example sets up DHCP without using NWAM. NWAM is more than DHCP, because NWAM automatically configures any new interfaces, while the above way to manually setup DHCP is fixed for a specific interface.

If you do not know what the interface name is (bge0 in this case); then type in

```
$ dladm show-link
```

or:

```
$ kstat -c net | grep net
```

```
# look for hme0, bge0, e1000g0 or soemthing that resembles the driver in use.
```

Add gateway

```
# route -p add default 192.168.1.121
```

or

```
# nano /etc/defaultrouter
```

```
# Enter in your gateways IP
```

or use the /etc/sysdng.conf file to configure a default router and DNS servers.

Set DNS server(s)

```
# nano /etc/resolv.conf
```

```
# Enter in the DNS server IP(s)
```

```
nameserver 192.168.1.121
```

or

```
# echo "nameserver 192.168.1.121" >> /etc/resolv.conf
```

Restart

```
# reboot
```

**NOTE:**

IF you cannot ping an external IP (e.g. google.com) run this command and try again.

```
# cp /etc/nsswitch.dns /etc/nsswitch.conf
```

credit for this section of the docs go to [/u/127b](#)

## 12.3 More on Automatic Configuration (NWAM)

The following is a more in depth discussion of NWAM, which normally works without any user interaction, but NWAM can be customized using profiles by the user.

### 12.3.1 Using NWAM configuration tools

Usually NWAM configuration is done via GUI `nwam-manager` applet and `nwam-manager-properties` program.

From CLI all configuration can be done using two tools, `nwamcfg` to configure network profiles and `nwamadm` to manage them.

On its backend, NWAM relies on `nwamd`, the NWAM policy engine daemon and `netcfgd`, the NWAM repository daemon.

Access to the command line and GUI tools is controlled via security profiles 'Network Autoconf Admin' and 'Network Autoconf user'.

To create NWAM profile use `nwamcfg` tool.

```
# nwamcfg
```

```
nwamcfg> create ncp Abroad
```

```
nwamcfg:ncp:Abroad> end
```

Now you can see a new profile in the list of NCPs:

```

nwamcfg> list
NCPs:
Abroad
Automatic
Locations:
Automatic
NoNet
User
nwamcfg>

```

The network interface to be managed under the new profile can be set and configured with `create ncu` command:

```

# nwamcfg
nwamcfg> select ncp Abroad
nwamcfg:ncp:Abroad> create ncu phys e1000g0
Created ncu 'e1000g0'. Walking properties ...
activation-mode (manual) [manual|prioritized]> prioritized
enabled (true) [true|false]>
priority-group> 0
priority-mode [exclusive|shared|all]> exclusive
link-mac-addr>
link-autopush>
link-mtu>
nwamcfg:ncp:Abroad:ncu:e1000g0>

```

Most important here is the `activation-mode`, which states if the profile is to be automatically set based on certain policies or if it is to be manually set using `nwamadm`. The latter should be most likely the case in a server environment. The `priority-group` and `priority-mode` here are set to (0 / exclusive). This says that the profile is for wired access and will always be the only active one at a time.

If after listing the changes you are satisfied with the configuration, permanently store it using `commit` command:

```

nwamcfg:ncp:Abroad:ncu:e1000g0> list
ncu:e1000g0
  type link
  class phys
  parent "Abroad"
  activation-mode prioritized
  enabled true
  priority-group 0
  priority-mode exclusive
nwamcfg:ncp:Abroad:ncu:e1000g0> commit
Committed changes
nwamcfg:ncp:Abroad:ncu:e1000g0> end

```

After an interface has been assigned to the profile, its IP configuration has to be defined:

```

nwamcfg:ncp:Abroad> create ncu ip e1000g0
Created ncu 'e1000g0'. Walking properties ...
enabled (true) [true|false]>

```

```

ip-version (ipv4,ipv6) [ipv4|ipv6]> ipv4
ipv4-addrsrc (dhcp) [dhcp|static]> static
ipv4-addr> 192.168.100.100
ipv4-default-route> 192.168.100.1
nwamcfg:ncp:Abroad:ncu:e1000g0> list
ncu:e1000g0
  type interface
  class ip
  parent "Abroad"
  enabled true
  ip-version ipv4
  ipv4-addrsrc static
  ipv4-addr "192.168.100.100"
  ipv4-default-route "192.168.100.1"
  ipv6-addrsrc dhcp,autoconf
nwamcfg:ncp:Abroad:ncu:e1000g0>

```

As you can see, the profile uses a static IP address and, for simplicity reasons, only provides IPv4 networking. Again, if you're happy with the results, commit them.

```

nwamcfg:ncp:Abroad:ncu:e1000g0> commit
Committed changes
nwamcfg:ncp:Abroad:ncu:e1000g0>

```

As it stands, now you have defined a physical and ip layer attached to a network profile:

```

nwamcfg:ncp:Abroad:ncu:e1000g0> end
nwamcfg:ncp:Abroad> list
NCUs:
  phys e1000g0
  ip e1000g0
nwamcfg:ncp:Abroad>exit

```

To activate the profile, you use `nwamadm`. First of all, check for the current situation:

```

# nwamadm list
TYPE      PROFILE    STATE
ncp       Abroad     disabled
ncp       Automatic  online
ncu:phys  e1000g0    online
ncu:ip    e1000g0    online
loc       Automatic  online
loc       NoNet      offline
loc       User       disabled

```

As you can see, Automatic is the active profile while Abroad is currently disabled. We can change that easily, but be aware that you might lock yourself out if you are connected via SSH when changing the profile!

```

# nwamadm enable -p ncp Abroad
Enabling ncp 'Abroad'

```

To check if the change has worked, you can use `nwam` again, and also `ifconfig` should show that interface is up:



```
# nwamadm list
TYPE PROFILE STATE
ncp Abroad online
ncu:phys e1000g0 online
ncu:ip e1000g0 online
ncp Automatic disabled
loc Automatic online
loc NoNet offline
loc User disabled

# ifconfig e1000g0
e1000g0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 8
inet 192.168.100.100 netmask ffffffff00 broadcast 192.168.100.255
ether 0:c:29:56:46:73
```

If you want to revert to default Automatic ncp, use the following command:

```
# nwamadm enable -p ncp Automatic
```

Although it is possible to directly modify profiles using an editor, it is not advisable and will be hardly necessary, anyway. One of the coolest features of NWAM tools is that they can be completely scripted. All steps above could also be put in one line:

```
# nwamcfg "create ncp Abroad;create ncu phys e1000g0;set activation-mode=manual;set
↪ enabled=true;set priority-group=0;set priority-mode=exclusive;end;create ncu ip
↪ e1000g0;set enabled=true;set ip-version=ipv4;set ipv4-addrsrc=static;set
↪ ipv4-addr=192.168.100.100;set ipv4-default-route=192.168.100.1;commit"
```

Or, more nicely formatted, commented and stored in a file:

```
#
# Profile for use on the road
#
# Created on 13/01/2013 by S. Mueller-Wilken
#
create ncp Abroad

# Create physical interface definition for 1st network card
create ncu phys e1000g0
set activation-mode=manual
set enabled=true
set priority-group=0
set priority-mode=exclusive
end

# Create IP configuration for first network card
create ncu ip e1000g0
set enabled=true
set ip-version=ipv4
set ipv4-addrsrc=static
set ipv4-addr=192.168.100.100
set ipv4-default-route=192.168.100.1
```

```
# Commit the settings
commit
```

This file can then be read by `nwamcfg`:

```
# nwamcfg -f abroad.cfg
Configuration read.
```

While there is no longer a need to fiddle around in `/etc/nwam`, the configuration is still completely there, as can be easily verified:

```
# ls /etc/nwam
loc loc.conf ncp-Abroad.conf ncp-Automatic.conf
```

All configuration is placed in readable ASCII files so that configuration from a global zone is possible:

```
# cat /etc/nwam/ncp-Abroad.conf
link:e1000g0 type=uint64,0;class=uint64,0;parent=string,Abroad;enabled=boolean,true;
↪ e;activation-mode=uint64,4;priority-group=uint64,0;priority-mode=uint64,0;
interface:e1000g0 type=uint64,1;class=uint64,1;parent=string,Abroad;enabled=boolean,true;
↪ n,true;ipv6-addrsrc=uint64,0,1;ip-version=uint64,4;ipv4-addrsrc=uint64,2;ipv4-
↪ default-route=string,192.168.100.1;ipv4-addr=string,192.168.100.100;
```

### 12.3.2 Network automagic online help

Comprehensive and fully illustrated online help for using NWAM is available by right clicking the NWAM tray icon and selecting *Help*. This opens help browser.

### 12.3.3 Troubleshooting NWAM

If NWAM is already configured and fails to connect to a wireless network try restarting the service.

For example:

```
# svcadm restart nwam
```

Sometimes the location gets set to *NoNet* and it's necessary to manually change the location to *Automatic*.

When the location setting is configured to *Switch Locations Automatically*, it's not possible to change the location. This is resolved by reconfiguring the location to allow manual switching. To perform this task, do the following:

Right click the NWAM tray icon and select **Location > Switch Locations Manually**. Right click the NWAM tray icon and select **Location > Automatic**.

## 13 Clustering with Open HA Cluster

ITEMS TO WRITE ABOUT:

See old sun docs

- <http://docs.oracle.com/cd/E19735-01/>

Also see:

- <http://zfs-create.blogspot.nl/>