

**KERNEL  
TECHNOLOGIES**  
(Skilled with Excellence)

# **IBM AIX7.1**

## **Lab Manual**

**Cum**

## **Reference Book**

Student Name: \_\_\_\_\_

Faculty Name: Vinod Kumar (Rahul), IT Architect

Batch: \_\_\_\_\_

Branch: Ameerpet

## Words To The Students

Though we have taken utmost efforts to present you this book error free, but still it may contain some errors or mistakes. Students are encouraged to bring, if there are any mistakes or errors in this document to our notice. So that it may be corrected in the next edition of this document.

This document provides the brief information on every topic and lab practices. The students are advised to make full use of the lab sessions, taking help of the Lab Assistants available. Please, feel free to ask your doubts to our faculties.

“Suppressing your doubts is Hindering your growth”.

You and your suggestions are valuable to us. In case of any suggestions, grievance, or complaints, please feel free to see the Manager Jyoti Singh, or the Head Faculty Vinod Kumar (Rahul) Certified Advance Technical Expert(**CATE**). You can also mail us your queries on the following:

- ↳ [Jyoti@kerneltech.com](mailto:Jyoti@kerneltech.com)
- ↳ [Vinod@kerrneltech.com](mailto:Vinod@kerrneltech.com)
- ↳ [musab@kerrneltech.com](mailto:musab@kerrneltech.com)
- ↳ [sairam.pochampalli@kerneltech.com](mailto:sairam.pochampalli@kerneltech.com)

“We Wish All the Best to our students for their future”

### Acknowledgment:

*Kernel Technologies like to take this opportunity to thank, Mr. Musabuddin Syed, for his contribution in preparation of this Document.*

Mgmt

## **Contents:**

1. Devices.....	4
2. Logical Volume Manager(LVM).....	11
3. Disk Management Procedures .....	24
4. Export and Import of VG .....	33
5. Aix Encrypted Filesystem (EFS).....	35
6. Paging Spaces.....	42
7. System Dumps.....	47
8. Scheduling and Job Automation.....	50
9. User Administration.....	54
10. Problem Determination & Error Reporting.....	62
11. TCP/IP & Networking.....	77
12. Network File System (NFS).....	105
13. Virtual Lan (VLAN).....	119
14. Samba Server .....	126
15. Booting Procedure .....	132
16. Software Installation.....	135
17. Installation of JAVA Version 6 in Aix6.1.....	144
18. Real Time 3rd Party tools Installation.....	149
19. Enhanced user security with SUDO.....	152
20. Ssh on AIX.....	159
21. Role Based Access Control.....	167
22. Backup and Restore.....	175
23. Multibos .....	184
24. Performance Tuning.....	191
25. NIM Configuration: Basic Client Installation.....	197
26. Printers in AIX.....	207
27. Ticket Raising through OTRS.....	210
28. Oracle 11gR2 Database Installation on AIX6.1.....	215
29. Miscellaneous commands in AIX.....	236
30. Smitty Fast Paths.....	240

# DEVICES

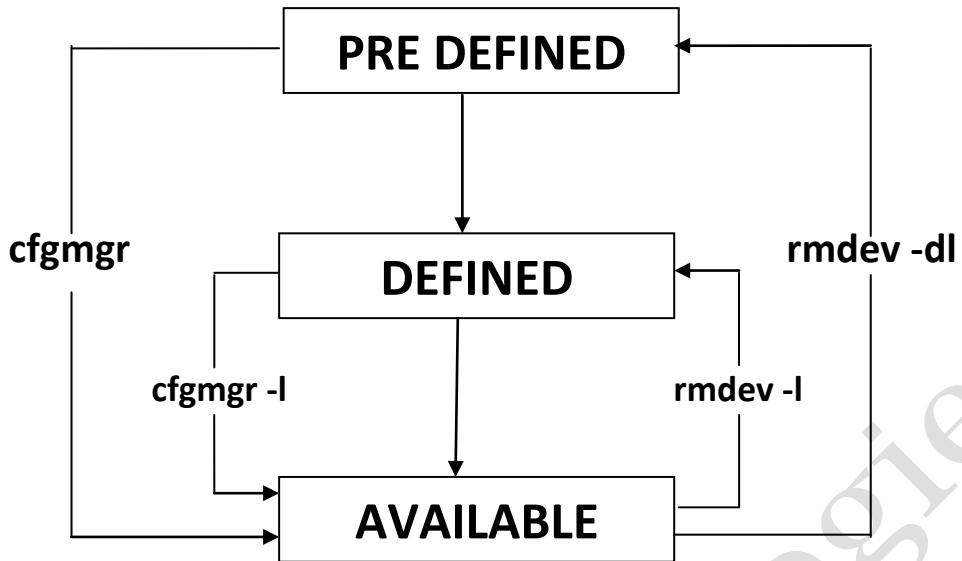
## Terminology of Devices:

- ↳ Actual Device
- ↳ Ports
- ↳ Device Driver
- ↳ Logical Name
- ↳ /dev Directory

- ↳ **Actual Device** may be any device e.g. USB, CD Drive, Tape Drive, etc which is connected to the system in some way.
- ↳ **Ports** are the physical connectors or Adapters through which the Actual devices are connected to the system. The ports will be having some software in it, which allows devices to connect to the system.
- ↳ **Device Driver** is software which is required by the kernel to make device ready to use in the OS. A driver acts like a translator between the device and programs that use the device. Each device has its own set of specialized commands that only its driver knows.
- ↳ **Logical Name** is the name given by the OS (AIX) to a device whenever a new device is attached to the system and its driver is installed properly. The logical name is used by End user.
- ↳ **/dev Directory** is a repository of ODM where all the logical devices (or logical names given to actual devices), which can be directly accessed by the user will be stored.

## States of the Devices

- ↳ **Predefined**
- ↳ **Defined**
- ↳ **Available**



- ↳ **Predefined** is a state where the device is actually not connected to the system, but still its support is available in the system repository. In other words predefined devices are the supported or compatible devices with OS platform
- ↳ **Defined** state means that the devices was once connected and configured on the system but currently not connected to the system or it is not powered on. Whenever a device is in defined state it cannot be used by the user.
- ↳ **Available** state is the state where a device is connected, powered on and configured to the system. A device in available state is ready for use and can be used by the user.

### Object Data Manager (ODM):

- ↳ The **Object Data Manager (ODM)** is a database intended for storing system information.
- ↳ Physical and logical device information is stored and maintained as objects with associated characteristics.

### Repositories of ODM

To support diskless, dataless and other workstations, the ODM object classes are held in three repositories:

- ↳ **/etc/objrepos:**  
Contains the customized devices object classes. It contains the part of the product that cannot be shared among machines.
- ↳ **/usr/lib/objrepos:**  
Contains the predefined devices object classes, the object classes in this repository can be shared across the network by /usr clients, dataless and diskless workstations. Software installed in the /usr-part can be shared among several machines with compatible hardware architectures.

↳ **/usr/share/lib/objrepos:**

The /usr/share part of a software product contains files that are not hardware dependent. They can be shared among several machines, even if the machines have different hardware architecture.

**LAB ACTIVITIES:-**

1. Find out the logical & physical address of hdisk4.

↳ #lsdev -Cc disk |grep hdisk4 → to see logical address

```
# lsdev -Cc disk |grep hdisk4
hdisk4 Available 10-68-00-3,0 Other SCSI Disk Drive
```

↳ #lscfg -vl hdisk4 → to see the physical address.

```
# lscfg -vl hdisk4
hdisk4 P1-I3/Z1-A3 Other SCSI Disk Drive

Manufacturer.....SEAGATE
Machine Type and Model....ST39173W SUN9.0G
Part Number.....0 Seagate A1
ROS Level and ID.....34333135
Serial Number.....9845A635
EC Level.....1 rights r
Device Specific.(20).....000002028B00013E
Device Specific.(21).....93
Device Specific.(22).....opyr
Device Specific.(23).....ight
Device Specific.(24).....c) 1
Device Specific.(25).....90
```

2. Remove hdisk10 & configure back, check if disk name is same?

↳ # rmdev -l hdisk10 to remove a disk

```
# rmdev -l hdisk10
hdisk10 Defined
# lsdev -Cc disk|grep -i hdisk10
hdisk10 Defined 10-68-00-11,0 Other SCSI Disk Drive
```

↳ #cfgmgr -l hdisk10

```
# cfgmgr -l hdisk10
# lsdev -Cc disk|grep -i hdisk10
hdisk10 Available 10-68-00-11,0 Other SCSI Disk Drive
```

3. Check what type of cd-rom is connected, note down Physical address

↳ #lsdev -Cc cdrom to see which type of cd-rom is connected

```
# lsdev -Cc cdrom
cd0 Available 10-60-00-1,0 16 Bit SCSI Multimedia CD-ROM Drive
```

↳ #lscfg -vl cd0 (cd0 is the logical name u can see from above command)

```
# lscfg -vl cd0
cd0          P1/Z1-A1 16 Bit SCSI Multimedia CD-ROM Drive (650 MB)

        Manufacturer.....IBM
        Machine Type and Model....CDRM00203
        ROS Level and ID.....1_06
        Device Specific.(Z0).....058002028F000038
        Part Number.....04N2964
        EC Level.....F73113
        FRU Number.....97H7796
```

4. Find out what target SCSI2 is connected

↳ #lsdev -Cc adapter |grep -i scsi2

```
# lsdev -Cc adapter |grep -i scsi2
scsi2  Available 10-68      Wide/Fast-20 SCSI I/O Controller
```

5. List syntax to see all available disk

↳ #lspv

```
# lspv
hdisk0      0009502c89314046      rootvg      active
hdisk1      0009506cc7f467cc      None
hdisk2      0009502ca98208ad      None
hdisk3      0009506cf79b9925      None
hdisk4      0009506c4d9b619b      None
hdisk5      0009502cbf53bfda      None
hdisk6      0009502cf55f6b69      None
hdisk7      0009502c999cd121      None
hdisk8      0009502c5c611104      None
hdisk9      0009502cbd4308bc      None
hdisk10     0009502c99a07e18      None
hdisk11     0009502c252573e8      None
hdisk12     0009502cb0c92f1f      None
```

↳ # lsdev -Cc disk

```
# lsdev -Cc disk
hdisk0 Available 10-60-00-0,0 Other SCSI Disk Drive
hdisk1 Available 10-68-00-0,0 Other SCSI Disk Drive
hdisk2 Available 10-68-00-1,0 Other SCSI Disk Drive
hdisk3 Available 10-68-00-2,0 Other SCSI Disk Drive
hdisk4 Available 10-68-00-3,0 Other SCSI Disk Drive
hdisk5 Available 10-68-00-4,0 Other SCSI Disk Drive
hdisk6 Available 10-68-00-5,0 Other SCSI Disk Drive
hdisk7 Available 10-68-00-8,0 Other SCSI Disk Drive
hdisk8 Available 10-68-00-9,0 Other SCSI Disk Drive
hdisk9 Available 10-68-00-10,0 Other SCSI Disk Drive
hdisk10 Available 10-68-00-11,0 Other SCSI Disk Drive
hdisk11 Available 10-68-00-12,0 Other SCSI Disk Drive
hdisk12 Available 10-68-00-13,0 Other SCSI Disk Drive
```

6. List syntax for configuring defined & available

↳ #cfgmgr

7. What is difference between defined and available

↳ **Define** is the state where a device might have been connected to the system sometime or it is connected while the server is up and running and it is yet to be configured, hence it cannot be used presently.

**Available** is the state where a device is presently connected to the system and it is ready to be used.

8. Find out serial number of server

↳ #prtconf |more

```
System Model: IBM,7044-170
Machine Serial Number: 109502C
Processor Type: PowerPC_POWER3
Number Of Processors: 1
Processor Clock Speed: 400 MHz
CPU Type: 64-bit
Kernel Type: 64-bit
LPAR Info: -1 NULL
Memory Size: 1024 MB
Good Memory Size: 1024 MB
Platform Firmware level: Not Available
Firmware Version: IBM,SPH02066
Console Login: enable
Auto Restart: true
Full Core: false
```

9. How many SCSI, IDE, PCI adapters are there

↳ # lsdev -Cc adapter (check how many **pci**, **scsi**, **ide** is listed)

```
# lsdev -Cc adapter
ent0 Available 10-70 IBM 10/100 Mbps Ethernet PCI Adapter (23100020)
ent1 Available 10-80 IBM 10/100 Mbps Ethernet PCI Adapter (23100020)
fda0 Available 01-D1 Standard I/O Diskette Adapter
moj10 Available 20-58 GXT4500P Graphics Adapter
paud0 Available 01-Q2 Ultimedia Integrated Audio
ppa0 Available 01-R1 CHRP IEEE1284 (ECP) Parallel Port Adapter
sa0 Available 01-S1 Standard I/O Serial Port
sa1 Available 01-S2 Standard I/O Serial Port
scsi0 Available 10-60 Wide/Ultra-2 SCSI I/O Controller
scsi1 Available 10-61 Wide/Ultra-2 SCSI I/O Controller
scsi2 Available 10-68 Wide/Fast-20 SCSI I/O Controller
sioka0 Available 01-K1-00 Keyboard Adapter
siokma0 Available 01-K1 Keyboard/Mouse Adapter
sioma0 Available 01-K1-01 Mouse Adapter
siota0 Available 01-Q1 Tablet Adapter
```

10. List Physical address off ent1

↳ #lscfg -l ent1

```
# lscfg -l ent1
ent1 P1/E1 IBM 10/100 Mbps Ethernet PCI Adapter (23100020)
```

11. Is there any tape drive is connected to server, if yes address Pls

↳ #lsdev -Cc tape

12. Find out Physical address of processor

↳ In order to know the physical address of processor we should know the Logical name of the processor

↳ #lsdev -Cc processor → (it is **proc0** as shown below)

```
# lsdev -Cc processor
proc0 Available 00-00 Processor
```

↳ #lscfg -vl proc0 → (this will show the physical address of the processor)

```
# lscfg -vl proc0
proc0 P1-C1 Processor

Device Specific. (YL) ..... P1-C1
```

13. To what logical address the graphics adapter (GXT – 4500) is attached, also find out Physical address.

↳ #lsdev -Cc adapter (it will show some logical add and logical name For GXT -4500 as moj10)

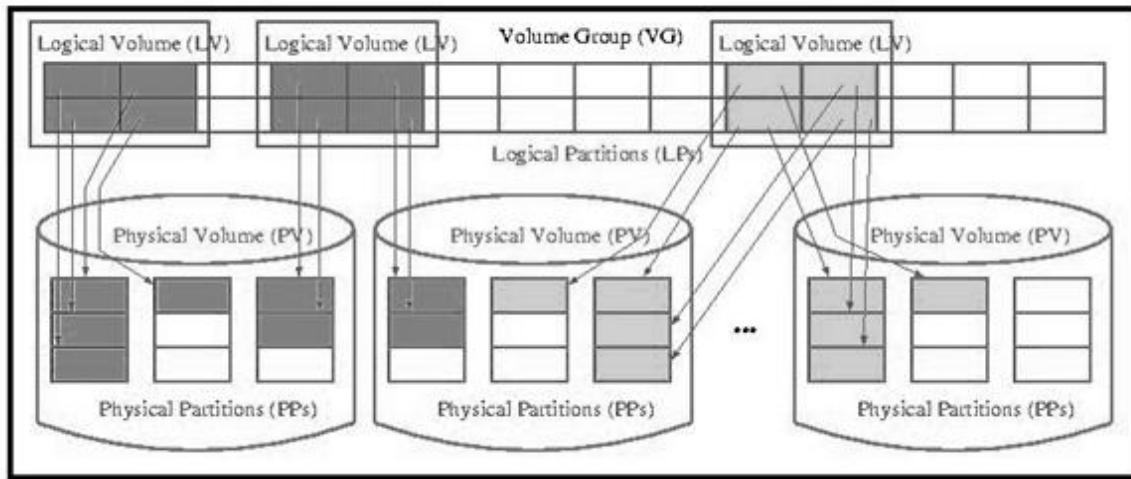
```
# lsdev -Cc adapter
ent0    Available 10-70    IBM 10/100 Mbps Ethernet PCI Adapter (23100020)
ent1    Available 10-80    IBM 10/100 Mbps Ethernet PCI Adapter (23100020)
fda0    Available 01-D1    Standard I/O Diskette Adapter
moj10   Available 20-58    GXT4500P Graphics Adapter
paud0   Available 01-Q2    Ultimedia Integrated Audio
ppa0    Available 01-R1    CHRP IEEE1284 (ECP) Parallel Port Adapter
sa0     Available 01-S1    Standard I/O Serial Port
sa1     Available 01-S2    Standard I/O Serial Port
scsi0   Available 10-60    Wide/Ultra-2 SCSI I/O Controller
scsi1   Available 10-61    Wide/Ultra-2 SCSI I/O Controller
scsi2   Available 10-68    Wide/Fast-20 SCSI I/O Controller
sioka0  Available 01-K1-00 Keyboard Adapter
siokma0 Available 01-K1    Keyboard/Mouse Adapter
sioma0  Available 01-K1-01 Mouse Adapter
siota0  Available 01-Q1    Tablet Adapter
```

↳ #lscfg -vl moj10 - to see the physical address

```
# lscfg -vl moj10
moj10          P1-I1/G1  GXT4500P Graphics Adapter
                           Device Specific. (YL) ..... P1-I1/G1
```

# LOGICAL VOLUME MAGAGER (LVM)

## Components of LVM:



- ↳ Volume Group (VG)
- ↳ Physical Volume(PV)
- ↳ Physical Partition(PP)
- ↳ Logical Volume (LV)
- ↳ Logical Partition(LP)

## Volume Group (VG)

- ↳ Volume group is a collection of disk or physical volumes. **Volume group** consists of one or more **physical volumes** that are divided into **physical partitions**. When a volume group is created, a physical partition size has to be specified. This partition size can range from 1 MB to 1024 MB. This physical partition size is the smallest allocation unit for the LVM. It is not specified, the system will select the minimum size to create 1016 partitions.

## Physical Volume (PV)

- ↳ A physical Volume is an actual physical disk attached to the system, whether internally or externally. The data in VG is actually stored in the PVs.

## Physical Partitions (PP)

- ↳ The smallest allocation unit in LVM is called Physical Partition (PP). All of the physical volumes in a volume group are divided into physical partitions (PPs).All the physical partitions within a volume group are the same size, although different Volume groups can have different PP sizes.

### Logical Volume (LV)

- Physical volumes and volume groups are normally not addressed directly by users and applications to access data, and they cannot be manipulated to provide disk space for use by users and applications. However, logical volumes provide the mechanism to make disk space available for use, giving users and applications the ability to access data stored on them.

### Logical Partitions (LP)

- Each logical volume consists of one or more logical partitions (LPs). Logical partitions are the same size as the physical partitions within a volume group. Each logical partition is mapped to at least one physical partition. Although the logical partitions are numbered consecutively, the underlying physical partitions are not necessarily consecutive or contiguous.

### Types of Volume Group:

- ORIGINAL
- BIG
- SCALABLE

Volume Group Type	Max PVs	Max LVs	Max PPs per VG	Max PP Size
Normal	32	256	32512 (1016 * 32)	1 GB
Big	128	512	130048 (1016 * 128)	1 GB
Scalable	1024	4096	2097152	128 GB

### Volume Group Descriptor Area (VGDA):

- The Volume Group Descriptor Area (VGDA) is an area of disk, at least one per PV, containing information for the entire VG. It contains administrative information about the volume group (for example, a list of all logical volume entries, a list of all the physical volume entries and so forth). There is usually one VGDA per physical volume.

### Quorum:

- The quorum is one of the mechanisms that the LVM uses to ensure that a volume group is ready to use and contains the most up-to-date data. A quorum is a vote of the number of Volume Group Descriptor Areas and Volume Group Status Areas (VGDA) that are active. A quorum ensures data integrity of the VGDA areas in the event of a disk failure.

## File System:

↳ A file system is a directory hierarchy for storing files. It has a root directory and subdirectories. In an AIX system, the various file systems are joined together so that they appear as a single file tree with one root. Many file systems of each type can be created.

↳ The supported file systems in AIX are:

### **Journaled File System**

The Journaled File System is native to AIX. This File System retains a journal for every I/O transaction on a physical Volume. One Logical Volume can contain only one Journaled File System. In order to use the File System, the Operating System has to mount it. The File Systems which are critical to the booting and operation of the Operating System, are mounted during boot time operation.

↳ The Journaled File Systems are of two types: **JFS** and **JFS2**. AIX 5.3 onwards **JFS2** is the default File System. Earlier it used to be JFS. JFS2 has some enhancements over JFS.

### **Network File System**

The NFS is used to allow the users to access the files and directories over the network. NFS has been in use since the very beginning for almost all kind of \*nix Operating Systems. Almost every \*nix OS supports NFS. NFS is a distributed File System and provides seamless access to the files from the server side.

### **CD-ROM File System**

The CDRFS is the one typical to CDs.

## LAB ACTIVITIES:-

1. Have you checked VGDA, create VG with 1 disk, then add 2<sup>nd</sup> disk, 3<sup>rd</sup> disk and 4<sup>th</sup> disk, notice VGDA and quorum status. Remove 1st disk when your VG is with 4 disks, keep removing one disk till your VG is deleted and notice VGDA

↳ To create a vg with one disk through command line

```
# mkvg -y sapvg -s 64 hdisk1
```

↳ To create a vg with 1 disk through smitty

**Step1:** #smitty mkvg

↳ Select the type of vg (ex: Original, Big & Scalable)

**Step2 :** Type or select values in entry fields.

```
Add an Original Volume Group

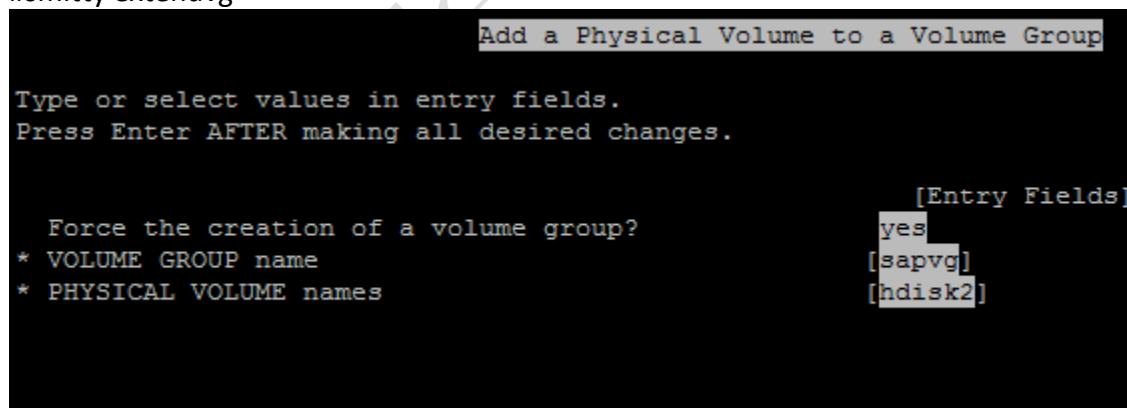
Type or select values in entry fields.
Press Enter AFTER making all desired changes.

VOLUME GROUP name [sapvg]
Physical partition SIZE in megabytes [64]
* PHYSICAL VOLUME names [hdisk1]
Force the creation of a volume group? [yes]
Activate volume group AUTOMATICALLY at system restart? [yes]
Volume Group MAJOR NUMBER []
Create VG Concurrent Capable? [no]
```

- ↳ To see the **vgda** of currently created vg  
`#lsvg sapvg`

```
# lsvg sapvg
VOLUME GROUP:      sapvg          VG IDENTIFIER: 0009502c00004c000000012ebd68d4cf
VG STATE:          active         PP SIZE:       64 megabyte(s)
VG PERMISSION:    read/write    TOTAL PPs:    134 (8576 megabytes)
MAX LVs:           256           FREE PPs:    134 (8576 megabytes)
LVs:                0           USED PPs:   0 (0 megabytes)
OPEN LVs:          0           QUORUM:      2
TOTAL PVs:         1           VG DESCRIPTORS: 2
STALE PVs:        0           STALE PPs:   0
ACTIVE PVs:        1           AUTO ON:     yes
MAX PPs per VG: 32512         MAX PVs:     32
MAX PPs per PV: 1016          AUTO SYNC:  no
LTG size (Dynamic): 256 kilobyte(s) BB POLICY: relocatable
HOT SPARE:        no
#
#
```

- ↳ To add a disk to already created vg through command line  
`#extendvg -f sapvg hdisk2`
- ↳ To do the above task with smitty  
`#smitty extendvg`



- ↳ To remove a disk through command line  
`#reducevg -df sapvg hdisk2`
- ↳ To remove the same through smitty  
`# smitty reducevg`  
 select **Remove a Physical Volume from a Volume Group**  
 select your **Vg**

```

Remove a Physical Volume from a Volume Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
* VOLUME GROUP name sapvg
* PHYSICAL VOLUME names [hdisk2] +
FORCE deallocation of all partitions on
this physical volume? yes +

```

2. Have you created LV, what are the properties have you set, write down and make sure you know all the options.

- ↳ To make an lv with 10 lp's through command line  
#mklv -y saplv -t jfs2 sapvg 10
- ↳ To make an lv through smitty  
# smitty mklv  
Select vg under which you want to make an lv

```

Add a Logical Volume

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]
Logical volume NAME [saplv]
* VOLUME GROUP name sapvg
* Number of LOGICAL PARTITIONS [10]
  PHYSICAL VOLUME names []
  Logical volume TYPE [jfs2]
  POSITION on physical volume middle
  RANGE of physical volumes minimum
  MAXIMUM NUMBER of PHYSICAL VOLUMES []
    to use for allocation []

```

3. Create LV with 3 mirror copies, run **lslv -m lvname** to see mapping, create file system on top of it. Copy data in this new file system like cp -R /etc/\* /sap1 i.e. your new mount point.

- ↳ making lv with 3 mirror copy through command line  
#mklv -y saplv -t jfs2 -c 3 sapvg 10  
Before going for mirroring make sure that your vg is having enough pvs (for 3 mirror copies 3 pv's are required)

- making the above lv through smitty  
 #smitty mklv  
 Select your vg

```
Add a Logical Volume

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP] [Entry Fields]
Logical volume NAME [saplv]
* VOLUME GROUP name sapvg
* Number of LOGICAL PARTITIONS [10]
  PHYSICAL VOLUME names []
  Logical volume TYPE [jfs2]
  POSITION on physical volume middle
  RANGE of physical volumes minimum
  MAXIMUM NUMBER of PHYSICAL VOLUMES []
    to use for allocation []
  Number of COPIES of each logical partition [3]
    partition
  Mirror Write Consistency? active
  Allocate each logical partition copy yes
```

# lsblk -m saplv → and you can see the mapping from lp to pp

- Creating a filesystem through command line  
 #crfs -v jfs2 -d saplv -m /sap -A yes
- Creating the fs with smitty  
 #smitty crfs  
 Select **Add Enhanced Journaled File System**  
 Select **Add Enhanced Journaled File System on previously defined LV**

```
Add an Enhanced Journaled File System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

* LOGICAL VOLUME name [saplv]
* MOUNT POINT [/sap]
  Mount AUTOMATICALLY at system restart? yes
  PERMISSIONS read/write
  Mount OPTIONS []
  Block Size (bytes) [4096]
  Logical Volume for Log []
  Inline Log size (MBytes) []
  Extended Attribute Format Version 1
  ENABLE Quota Management? no
```

Mount your mount point (i.e. /sap)  
#mount /sap  
Go to your mount point (cd /sap) and add some data.

4. Remove 1 copy from your mirrored LV see **lsvg -l vgname** and try to see LP to PP ratio.

↳ Removing a copy of lv through command line

```
#rmlvcopy saplv 2
```

Doing the same with smitty

```
#smitty rmlvcopy
```

Select your lv

Give the new no. copy as 2 (as shown below)

```
Remove Copies from a Logical Volume

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
* LOGICAL VOLUME name          saplv
* NEW maximum number of logical partition
    copies                      2
PHYSICAL VOLUME names          []
```

Now see the mapping by running  
#lslv -m saplv

5. How many disks you can have in a scalable VG, can we convert from BIG VG to SCALABLE VG, try converting? Can we do it online or do we need downtime.

↳ In scalable VG we can have max of 1024 disk.

↳ Yes, we can change a BIG VG TO SCALABLE but we require some downtime as it requires the volume group to be in inactive state i.e. varyoff state.

↳ Converting a big vg to scalable vg format

```
#varyoffvg sapvg
```

```
#smitty chvg
```

#select your vg which is sapvg and do the following changes

```

Change a Volume Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
* VOLUME GROUP name           sapvg
* Activate volume group AUTOMATICALLY
  at system restart?          yes
* A QUORUM of disks required to keep the volume group on-line ?      yes
  Convert this VG to Concurrent Capable?        no
  Change to big VG format?            no
  Change to scalable VG format?       yes
  LTG Size in kbytes             128
  Set hotspare characteristics    n
  Set synchronization characteristics of stale partitions      n
  Max PPs per VG in kilobytes     32
  Max Logical Volumes            256

```

6. Check PP size in your VG, how many PP required for LV of 2.9GB. Calculate and create it.

↳ #lsvg sapvg to check the pp size of sapvg (sapvg's PP size is 64mb)  
Convert 2.9GB to MB (2.9x 1024=2969.7 or 2970)  
2970/64 =46, therefore we require 46 IP's to create an lv of 2.9GB  
#mklv -y saplv2 -t jfs2 sapvg 46, Thus lv is created.

7. Create file system on above LV, give mount point name, copy data into filesystem, unmount this filesystem then go to **#cd /mount point** you gave see if data is there.

↳ Creating a file system through command line  
#crfs -v jfs2 -d saplv2 -m /sap2  
#mount /sap2 to mount the mount point.

↳ creating the above through smitty as shown in Q.3  
#cd /sap2 to enter in the mount point and add some data(ex: touch 1 2 )  
#umount /sap2 to unmount the mount point, enter again in your mount Point i.e. /sap2 and run #ls command and see whether data is there  
(\*Data will not be there)

8. Mount previous filesystem into new mount point manually and see if data is there.

↳ **step1:** Changing the mount point

**Note:** Before changing the mount point, unmount the current mount point

#umount /sap2

#smitty chfs and select the following

```
Change / Show Characteristics of an Enhanced Journaled File System
```

Now select your mount point i.e. **/sap2** and perform following changes

```
Change / Show Characteristics of an Enhanced Journaled File System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
File system name          /sap2
NEW mount point           [/sap2b]
SIZE of file system
    Unit Size             512bytes
    Number of units       [6029312]
Mount GROUP                []
Mount AUTOMATICALLY at system restart?   no
PERMISSIONS                 read/write
Mount OPTIONS                []
Start Disk Accounting?      no
Block Size (bytes)         4096
Inline Log?                 no
Inline Log size (MBytes)   [0]
Extended Attribute Format  [v1]
ENABLE Quota Management?   no
Allow Small Inode Extents? no
```

Now mount the new mount point i.e. **/sap2b** and go to the mount point and see if data is present or not.

9. Does manual mounting update **/etc/filesystems** with your new mount point.

↳ No, manual mounting does not update **/etc/filesystems**

After completing Q.no 8 check **/etc/filesystems** you can find the answer.

10. Create new LVs and filesystems for the following in your VG only.

- /usr/sap
- /usr/sap/trans
- /usr/sap/trans/data1
- /usr/sap/trans/data2
- /usr/sap/trans/data/sap

↳ Step1: Create an lv(say saplv) either through command line or smit.

Step2: Create a fs on top that lv (saplv) with mount point **/usr/sap** and mount it.

Step3: Repeat Step2 and create fs on 2<sup>nd</sup> lv(say saplv2) and give mount point as **/usr/sap/trans** and mount it.

Step4: Again create an lv and fs on 3<sup>rd</sup> lv(say saplv3) and give mount point as **/usr/sap/trans/data1** & mount it, repeat the same step for **/usr/sap/trans/data2** and **/usr/sap/trans/data/sap**

11. How will you see mounted filesystem space usage, try kilo, mega and giga options.  
Check du option.

- ↳ To see the space usage of mounted file system
  - #df -k (k is used for viewing size in KB)
  - #df -m (m for viewing size in MB)
  - #df -g (g for viewing size in GB)
- ↳ The du command displays the number of blocks used for files.  
#du with -a, -s, -k, -m, -g or see man pages for more option

12. Which command will give you what type of file system is mounted?

- ↳ #mount

13. Have you checked what size of loglv in your VG is, try to increase loglv size.

- ↳ #lsvg -l sapvg → will show the size of loglv (which will be 1 LP)  
Now increase the size of loglv (which is loglv00 in sapvg)  
#extendlv loglv00 1 → this will increase its size by 1LP.  
The same can be done by smit using  
#smitty extendlv and selecting loglv

14. Create jfs and jfs2 filesystem in same VG and see how many loglv you have.

- ↳ Create a jfs and jfs2 file system as shown in Q.NO 3  
In case of jfs first create an lv with jfs type and use create a file system with  
#crfs -v jfs##### or #smitty crfs (use add journaled filesystem)  
Now run #lsvg -l vgname (say sapvg) and check how many log file is there.  
(\*There will be two log file ex : loglv00 for jfs2 and loglv01 for jfs )

15. Note down your command to extend and reduce VG as well as LV, may be an interview question.

- ↳ See Q.NO 1 for extend vg and reduce vg command and Q.No 13 for LV

16. What is default max LP in LV, try increasing it in multiples of 2, find out how can you do through command line, I am sure that you have done it through smitty .

- ↳ The default max LP in LV is 512 (can be checked by #lslv lvname)  
The max LP can be changed by using  
#smitty chlv -> change lv -> lv name -> change max lp to 1024.  
#chlv -x 1024 lvname is the command used for increasing the same through command line

17. Hey did you face this, "A device is already mounted or cannot be unmounted, ask your friends did he face this situation or when did this situation occurred, how will you get rid of this.

↳ If you are still in the same directory which is the mount point you are trying to Unmount, will show the above error, or else try #umount -f command.

18. Filesystem is mounted, you need to unmount it, how will you do it forcefully.

**Hint:** fuser (try man fuser)

↳ #fuser -kxuc mount point (say /sap)

19. Add 1 disk in your VG, try making it hot spare... are you able to do this if not what error you are getting.

20. Migrate 1 LV from 1 PV to another PV within the VG.

↳ #migratepv -l lvname hdisk1 hdisk2

Through smitty

#smitty migratepv

Select device in which you want to migrate data and change the following

```
Move Contents of a Physical Volume

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
* SOURCE physical volume name          hdisk2
* DESTINATION physical volumes         [hdisk1]
Move only data belonging to this      [saplv]
LOGICAL VOLUME?
```

21. Try removing mounted file system.

↳ A file system can only be removed when it is unmounted, try yourself and check.

22. Did you increase size of file system on the fly i.e. using chfs; this is what you will do it in real time. Do it and verify the new size, write down result.

↳ #chfs -a size=+1G /sap (where G is for gigabyte and /sap is the mount point)  
For kilobyte use K and M for megabytes, and so forth

- ↳ Through smitty  
 #smit chfs -> select Change Enhanced Journal Filesystem -> select your filesystem and Change the following options

```
Change / Show Characteristics of an Enhanced Journaled File System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]

File system name          /sap
NEW mount point           [/sap]
SIZE of file system
  Unit Size
    Number of units        Gigabytes
  Mount GROUP             [+1]
  Mount AUTOMATICALLY at system restart?   []
  PERMISSIONS             yes
  Mount OPTIONS            read/write
  Start Disk Accounting?   []
  Block Size (bytes)       4096
  Inline Log?              no
  Inline Log size (MBytes) [0]
  Extended Attribute Format [v1]
  ENABLE Quota Management? no
  Allow Small Inode Extents? no
```

23. Export your VG and see if there is lsvg and import it back.

- ↳ #exportvg vgname to export the VG, Make sure your vg is varied off before exporting.

```
#importvg -y vgname diskname  (at least one disk name is required which was part of
The exported vg)
#smit exportvg (to export vg through smit)
#smit importvg ( to import vg through smit)
```

24. I am sure you know major number and minor number, search where they can be located and what command will show us available major number.

Hint: starts with lvlist

- ↳ #lvlistmajor is the command to see the available major number

#ls -l /dev/vgname will show what major number a vg is assigned to.

#ls -l /dev will show all the major and minor number.

25. There is no space in VG to extend File System , Raise a ticket using OTRS and transfer it to KTS\_SAN\_SUPP Team to assign a LUN of 10 GB , once lun assigned, run cfgmgr add disk space and close disk.

26. In practical session we will run scripts to fill filesystem or cross usage to more than 90% to generate alert and show how to resolve this issue.

To see what has caused to fill space Run

First go to directory where FS mounted. Then run following command

```
#ls -lR | sort -nr -k5
```

See if any log files you can compressed or delete any files, else we may have to increase the filesystem size. Don't delete the files which are not owned by root

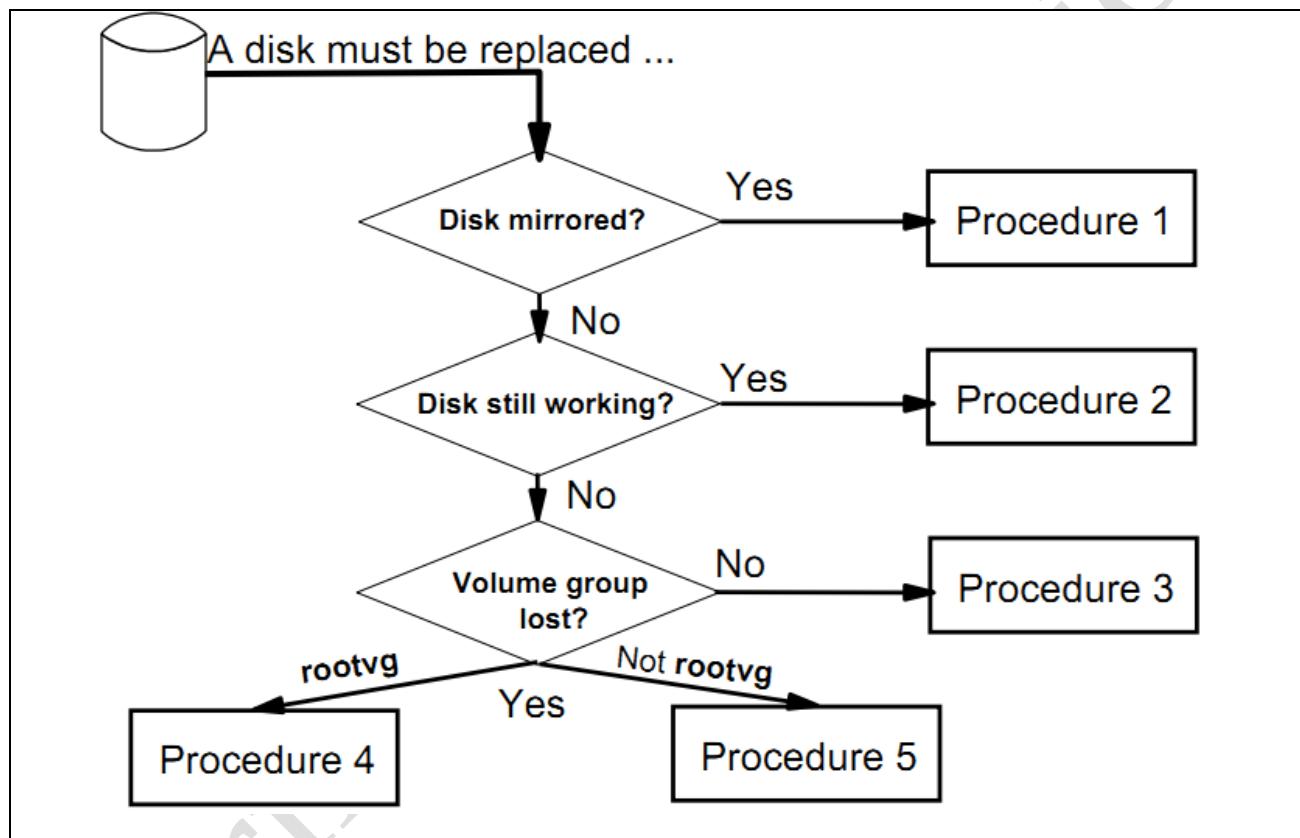
transfer the ticket to respective team.

# Disk management procedures

This unit describes different disk management procedures:

- Disk replacement procedures
- Procedures to solve problems caused by an incorrect disk replacement
- Managing situations where duplicate file systems or logical volumes complicate the import of a volume group.

## Disk replacement techniques:



## Reasons to replace a disk:

Many reasons might require the replacement of a disk, for example:

- Disk too small
- Disk too slow
- Disk produces many DISK\_ERR4 log entries

## **Flowchart:**

Before starting the disk replacement, always follow the flowchart that is shown in the visual. This will help you whenever you have to replace a disk.

1. If the disk that must be replaced is completely mirrored onto another disk, follow procedure 1.
2. If a disk is not mirrored, but still works, follow procedure 2.
3. If you are absolutely sure that a disk failed and you are not able to repair the disk, do the following:
  - ❖ If the volume group can be varied on (normal or forced), use procedure 3.
  - ❖ If the volume group is totally lost after the disk failure, which means the volume group could not be varied on (either normal or forced).
    - If the volume group is rootvg, follow procedure 4.
    - If the volume group is not rootvg follow procedure 5.

## **Procedure 1: Disk mirrored**

1. Remove all copies from disk:  
`# unmirrorvg vg_name hdiskX`
2. Remove disk from volume group:  
`# reducevg vg_name hdiskX`
3. Remove disk from ODM:  
`# rmdev -l hdiskX -d`
4. Connect new disk to system  
May have to shut down if not hot-pluggable
5. Add new disk to volume group:  
`# extendvg vg_name hdiskY`
6. Create new copies:  
`# mirrorvg vg_name hdiskY`  
`# syncvg vg_name`

## **When to use this procedure:**

Use procedure 1 when the disk that must be replaced is mirrored.

## **Disk state:**

This procedure requires that the disk state of the failed disk be either missing or removed. Use lsvg hdiskX to check the state of your physical volume. If the disk is still in the active state, you cannot remove any copies or logical volumes from the failing disk. In this case, one way to bring the disk into a removed or missing state is to run the reducevg -d command or to do a varyoffvg and a varyonvg on the volume group by rebooting the system.

Disable the quorum check if you have only two disks in your volume group.

## **How to do it:**

The goal of each disk replacement is to remove all logical volumes from a disk.

1. Start removing all logical volume copies from the disk. Use either the SMIT fastpath smit unmirrorvg or the unmirrorvg command as shown in the visual. This will unmirror each logical volume that is mirrored on the disk.  
If you have additional unmirrored logical volumes on the disk, you have to either move them to another disk (migratepv), or remove them if the disk cannot be accessed (rmlv).
2. If the disk is completely empty, remove the disk from the volume group. Use SMIT fastpath smit reducevg or the reducevg command.
3. After the disk has been removed from the volume group, you can remove it from the ODM. Use the rmdev command as shown in the visual.  
If the disk must be removed from the system, shut down the machine and then remove it, if the disk is not hot-pluggable.
4. Connect the new disk to the system and reboot your system. The cfgmgr will configure the new disk. If using hot-pluggable disks, a reboot is not necessary.
5. Add the new disk to the volume group. Use either the SMIT fastpath smit extendvg or the extendvg command.
6. Finally, create new copies for each logical volume on the new disk. Use either the SMIT fastpath smit mirrorvg or the mirrorvg command. Synchronize the volume group (or each logical volume) afterwards, using the syncvg command.

## **Procedure 2: Disk still working**

1. Connect new disk to system.
2. Add new disk to volume group:  
`# extendvg vg_name hdiskY`
3. Migrate old disk to new disk: (\*)  
`# migratepv hdiskX hdiskY`
4. Remove old disk from volume group:  
`# reducevg vg_name hdiskX`
5. Remove old disk from ODM:  
`# rmdev -l hdiskX -d`

### **When to use this procedure:**

Procedure 2 applies to a disk replacement where the disk is unmirrored but could be accessed. If the disk that must be replaced is in rootvg, follow the instructions on the next visual.

### **How to do it:**

The goal is the same as always. Before we can replace a disk, we must remove everything from the disk.

1. Shut down your system if you need to physically attach a new disk to the system. Boot the system so that cfgmgr will configure the new disk.
2. Add the new disk to the volume group. Use either the SMIT fastpath smit extendvg or the extendvg command.
3. Before executing the next step, it is necessary to distinguish between the rootvg and a non-rootvg volume group.
  - ❖ If the disk that is replaced is in rootvg, execute the steps that are shown on the visual Procedure 2: Special Steps for rootvg.
  - ❖ If the disk that is replaced is not in the rootvg, use the migratepv command:  
`# migratepv hdisk_old hdisk_new`This command moves all logical volumes from one disk to another. You can do this during normal system activity. The command migratepv requires that the disks are in the same volume group.
4. If the old disk has been completely migrated, remove it from the volume group. Use either the SMIT fastpath smit reducevg or the reducevg command.
5. If you need to remove the disk from the system, remove it from the ODM using the rmdev command as shown. Finally, remove the physical disk from the system.

## Procedure 2: Special steps for rootvg

1. Connect new disk to system.
2. Add new disk to volume group:  
`# extendvg vg_name hdiskY`
3. Disk contains hd5?  
`# migratepv -l hd5 hdiskX hdiskY`  
`# bosboot -ad /dev/hdiskY`  
`# chpv -c hdiskX`  
`# bootlist -m normal hdiskY`
- Migrate old disk to new disk:  
`# migratepv hdiskX hdiskY`
4. Remove old disk from volume group:  
`# reducevg vg_name hdiskX`
5. Remove old disk from ODM:  
`# rmdev -l hdiskX -d`

(Special steps for rootvg)

## Additional steps for rootvg:

Procedure 2 requires some additional steps if the disk that must be replaced is in rootvg.

1. Connect the new disk to the system as described in procedure 2.
2. Add the new disk to the volume group. Use smit extendvg or the extendvg command.
3. This step requires special considerations for rootvg:
  - ❖ Check whether your disk contains the boot logical volume. The default location for the boot logical volume is /dev/hd5.
  - ❖ Use the command lsvg -l to check the logical volumes on the disk that must be replaced.
  - ❖ If the disk contains the boot logical volume, migrate the logical volume to the new disk and update the boot logical volume on the new disk. To avoid a potential boot from the old disk, clear the old boot record by using the chpv -c command. Then, change your bootlist:  
`# migratepv -l hd5 hdiskX hdiskY`  
`# bosboot -ad /dev/hdiskY`  
`# chpv -c hdiskX`  
`# bootlist -m normal hdiskY`
  - ❖ If the disk contains the primary dump device, you must deactivate the dump before migrating the corresponding logical volume:  
`# sysdumpdev -p /dev/sysdumpnull`
  - ❖ Migrate the complete old disk to the new one:  
`# migratepv hdiskX hdiskY`

- ❖ If the primary dump device has been deactivated, you have to activate it again:  
`# sysdumpdev -p /dev/hdX`
4. After the disk has been migrated, remove it from the root volume group.  
`# reducevg rootvg hdiskX`
  5. If the disk must be removed from the system, remove it from the ODM (use the rmdev command), shut down your AIX, and remove the disk from the system afterwards.  
`# rmdev -l hdiskX -d`

### **Procedure 3: Disk in missing or removed state**

1. Identify all LVs and file systems on failing disk:  
`# lspv -l hdiskY`
2. Unmount all file systems on failing disk:  
`# umount /dev/lv_name`
3. Remove all file systems and LVs from failing disk:  
`# smit rmfs # rmlv lv_name`
4. Remove disk from volume group:  
`# reducevg vg_name hdiskY`
5. Remove disk from system:  
`# rmdev -l hdiskY -d`
6. Add new disk to volume group:  
`# extendvg vg_name hdiskZ`
7. Recreate all LVs and file systems on new disk:  
`# mklv -y lv_name # smit crfs`
8. Restore file systems from backup:  
`# restore -rvf /dev/rmt0`

### **When to use this procedure:**

Procedure 3 applies to a disk replacement where a disk could not be accessed but the volume group is intact. The failing disk is either in a state (not device state) of missing (normal varyonvg worked) or removed (forced varyonvg was necessary to bring the volume group online).

If the failing disk is in an active state (this is not a device state), this procedure will not work. In this case, one way to bring the disk into a removed or missing state is to run the reducevg -d command or to do a varyoffvg and a varyonvg on the volume group by rebooting the system. The reboot is necessary because you cannot vary off a volume group with open logical volumes. Because the failing disk is active, there is no way to unmount file systems.

## **How to do it:**

If the failing disk is in a missing or removed state, start the procedure:

1. Identify all logical volumes and file systems on the failing disk. Use commands like lspv, lslv or lsfs to provide this information. These commands will work on a failing disk.
2. If you have mounted file systems on logical volumes on the failing disk, you must unmount them. Use the umount command.
3. Remove all file systems from the failing disk using smit rmfs or the rmfs command. If you remove a file system, the corresponding logical volume and stanza in /etc/filesystems is removed as well.
4. Remove the remaining logical volumes (those not associated with a file system) from the failing disk using smit rmlv or the rmlv command.
5. Remove the disk from the volume group, using the SMIT fastpath smit reducevg or the reducevg command.
6. Remove the disk from the ODM and from the system using the rmdev command.
7. Add the new disk to the system and extend your volume group. Use the SMIT fastpath smit extendvg or the extendvg command.
8. Recreate all logical volumes and file systems that have been removed due to the disk failure. Use smit mklv, smit crfs or the commands directly.
9. Due to the total disk failure, you lost all data on the disk. This data has to be restored, either by the restore command or any other tool you use to restore data (for example, Tivoli Storage Manager) from a previous backup.

## **Procedure 4: Total rootvg failure**

1. Replace bad disk
2. Boot in maintenance mode
3. Restore from a mksysb tape
4. Import each volume group into the new ODM (importvg) if needed

## **When to use this procedure:**

Procedure 4 applies to a total rootvg failure. This situation might come up when your rootvg consists of one disk that fails. Or, your rootvg is installed on two disks and the disk fails that contains operating system logical volumes (for example, /dev/hd4).

## **How to do it:**

Follow these steps:

1. Replace the bad disk and boot your system in maintenance mode.
2. Restore your system from a mksysb tape.
  - ❖ If any rootvg file systems were not mounted when the mksysb was made, those file systems are not included on the backup image. You will need to create and restore those as a separate step.
  - ❖ If your mksysb tape does not contain user volume group definitions (for example, you created a volume group after saving your rootvg), you have to import the user volume group after restoring the mksysb tape. For example:  
`# importvg -y datavg hdisk9`

Only one disk from the volume group (in our example hdisk9), needs to be selected.

## **Procedure 5: Total non-rootvg failure**

1. Export the volume group from the system:  
`# exportvg vg_name`
2. Check /etc/filesystems.
3. Remove bad disk from ODM and the system:  
`# rmdev -l hdiskX -d`
4. Connect the new disk.
5. If volume group backup is available (savevg):  
`# restvg -f /dev/rmt0 hdiskY`
6. If no volume group backup is available: Recreate ...
  - Volume group (mkvg)
  - Logical volumes and file systems (mklv, crfs)Restore data from a backup:  
`# restore -rqvf /dev/rmt0`

## **When to use this procedure:**

Procedure 5 applies to a total failure of a non-rootvg volume group. This situation might come up if your volume group consists of only one disk that fails. Before starting this procedure, make sure this is not just a temporary disk failure (for example, a power failure).

## **How to do it:**

Follow these steps:

1. To fix this problem, export the volume group from the system. Use the command `exportvg` as shown. During the export of the volume group, all ODM objects that are related to the volume group will be deleted.
2. Check your `/etc/filesystems`. There should be no references to logical volumes or file systems from the exported volume group.
3. Remove the bad disk from the ODM (use `rmdev` as shown). Shut down your system and remove the physical disk from the system.
4. Connect the new drive and boot the system. The `cfdmgr` will configure the new disk.
5. If you have a volume group backup available (created by the `savevg` command), you can restore the complete volume group with the `restvg` command (or the SMIT fastpath `smit restvg`). All logical volumes and file systems are recovered.  
If you have more than one disk that should be used during `restvg`, you must specify these disks:  
`# restvg -f /dev/rmt0 hdiskY hdiskZ`
6. If you have no volume group backup available, you have to recreate everything that was part of the volume group.  
Recreate the volume group (`mkvg` or `smit mkvg`), all logical volumes (`mklv` or `smit mklv`) and all file systems (`crfs` or `smit crfs`).  
Finally, restore the lost data from backups, for example with the `restore` command or any other tool you use to restore data in your environment.

# **Export and import**

## **Exporting a volume group:**

1. Unmount all file systems from the volume group:  
# umount /dev/lv10  
# umount /dev/lv11
2. Vary off the volume group:  
# varyoffvg myvg
3. Export volume group: Before exporting notedown disk name belongs to VG.  
# exportvg myvg

The complete volume group is removed from the ODM.

## **The scenario**

The exportvg and importvg commands can be used to fix ODM problems. These commands also provide a way to transfer data between different AIX systems. This is an example of how to export a volume group. This disk belongs to the myvg volume group. This volume group needs to be transferred to another system.

## **Procedure to export a volume group:**

Execute the following steps to export the volume group:

- 1.Unmount all file systems from the volume group. In the example, there are three logical volumes in myvg; lv10, lv11, and loglv01. The loglv01 logical volume is the JFS log device for the file systems in myvg, which is closed when all file systems are unmounted.
- 2.When all logical volumes are closed, use the varyoffvg command to vary off the volume group.
- 3.Finally, export the volume group, using the exportvg command. After this point, the complete volume group (including all file systems and logical volumes) is removed from the ODM.
- 4.After exporting the volume group, the disks in the volume group can be transferred to another system.

### **Importing a volume group:**

1. Configure the disks.
2. Import the volume group:  
`# importvg -y myvg hdisk3`
3. Mount the file systems:  
`# mount /dev/lv10`  
`# mount /dev/lv11`
4. The complete volume group is added to the ODM.

### **Procedure to import a volume group:**

To import a volume group into a system, execute the following steps:

1. Connect all disks (in our example we have only one disk) and reboot the system so that cfgmgr will configure the added disks.
2. You only have to specify one disk (using either hdisk# or the PVID) in the importvg command. Because all disks contain the same VGDA information, the system can determine this information by querying any VGDA from any disk in the volume group. If you do not specify the option -y, the command will generate a new volume group name. The importvg command generates completely new ODM entries. In AIX V4.3 and subsequent releases, the volume group is automatically varied on.
3. Finally, mount the file systems.

## **AIX ENCRYPTED FILESYSTEM (EFS)**

- EFS on AIX was designed so that each file is encrypted with a unique key. The cryptographic information is kept in file-extended attributes. EFS uses Extended Attributes (EA) Version 2.
- EFS is built into the enhanced journaled file system (JFS2) — it is not a new file system. You can create EFS on a new file system or enable it on a new file system. EFS is only meant for the encryption of data file systems, not for system-based file systems (such as /var and /opt).
- You can perform encryption on the entire file system by switching on Inheritance, or by doing it per file.
- A key store is used to access data with password protection. This password can be the login password or a different password that root cannot access.

### **Keystores**

- Each user on the system will have its own keystore where its public and private keys are stored. This keystore can be protected by a separate password or can be synchronized such that it's protected by the normal login password. I believe this is a system-wide setting, and the default is to synchronize the passwords. User keystores are located in /var/efs/users/<username>
- If a user is explicitly granted access to act as a specific group in relation to EFS (in addition to being assigned to that group at the OS level), the group's private and public keys will also be copied into the user's keystore.
- Groups also have their own keystores, located in /var/efs/groups/<groupname>

### **File encryption**

- Each file is encrypted with a unique, symmetric (AES) key. For each user or group that is authorized to view the encrypted file, the symmetric key is then itself encrypted with the user/group's public key from its keystore, and that user-specific encrypted version of the key is stored in the file's extended attributes (EAs). That is, there will be one EA for each user and group that has access to the file in question.

### **Requirements & Constraints**

- AIX 6.1
- CryptoLite in C (CliC) cryptographic library needs to be installed.

- Enable Role Based Access Control (RBAC)
- Explicitly enable the system to use EFS. (**efsenable** command)
- **Restriction:** You cannot export the EFS through NFS.

#### **Tips & Specific Commands:**

- The **efsmgr** command manages encryption of a file or directory. **efskeymgr** manages keystores, including loading them into memory or removing them from memory.

To determine whether a particular file or directory is encrypted, issue the following command:

```
#ls -U filename
```

Encrypted files/directories will have an extra "e" at the end of their access attributes:

```
drwxr-x---e    5 user    group          256 Nov 23 20:44 directory
```

To determine which keys are loaded into your current session, issue the following command:

```
efskeymgr -v
```

- Your personal user key and any group keys to which you have access will be listed. The listed keys will determine which encrypted files or directories you can access. Compare the user and group keys listed against the AIX file/directory ownership and permissions.

To add a group's key to a user's keystore, the following command must be executed by a user who has the Admin key loaded:

```
efskeymgr -k group/<group> -s user/<user>
```

- Note that if the user hasn't yet logged into the system (after EFS was enabled), the keystore won't exist, and this command will fail.
- Note also that the user still has to be added to the group via the normal OS mechanism (/etc/group).

#### **Synchronized passwords:**

- If you wish to de-synchronize your keystore password from your login password, or simply to change your keystore password, run the following command:

```
efskeymgr -n
```

- Even with keystore passwords synchronized to user login passwords, your shell session does not automatically "load" your user's keys unless you've actually entered that password. In particular, if you authenticate via SSH keys, you'll have to explicitly load a

new shell in a manner which forces you to enter your password. One way to do this, using the EFS commands, is:

```
efskeymgr -o ksh
```

- You'll be prompted for the user's "EFS password", which in this case is simply the login password.
- In the same manner, if you use "sudo su -" to switch to another user, you will not load that user's keys. But if you use "su -", where you are forced to provide the user's password, you will load its keys. That is, you have to know a user's password if you want to act as that user and have access to its EFS files/directories. In particular, if you want to start a process which runs as that user and needs access to encrypted locations.

#### Prerequisites:

- The CryptoLite in C (CliC) cryptographic library needs to be installed at level 430. You can verify that CliC is installed by using the AIX lsLpp command. If it is installed, you will see information similar to that

```
# lsLpp -l | grep -i clic
clic.rte.kernext          4.7.0.0 COMMITTED CryptoLite for C Kernel
clic.rte.lib               4.7.0.0 COMMITTED CryptoLite for C Library
clic.rte.kernext          4.7.0.0 COMMITTED CryptoLite for C Kernel
```

- Role-based access control (RBAC has to be enabled). You can verify its installation by using the lsattr command

```
# lsattr -El sys0 -a enhanced_RBAC
enhanced_RBAC true Enhanced RBAC Mode True
```

#### Enabling EFS:

- After the prerequisites are in place, you can enable EFS by running the AIX efsenable -a command

```
# efsenable -a
Enter password to protect your initial keystore:
Enter the same password again:
```

- The efsenable command activates the EFS capability on a system. It creates the EFS-administration keystore, the user keystore and the security-group keystore. (Note: The keystore file is a key database file that contains both public keys and private keys.)
- efsenable command creates the /var/efs directory and updates /etc/security/user and /etc/security/group with the EFS attributes.

- After EFS is enabled, you can create a new file system either by using the AIX smitty or crfs command.

### Creating an EFS-enabled data-file system with smitty

```
# smitty jfs2
```

Add an Enhanced Jounaled File System

rootvg

Add an Enhanced Jounaled File System

Type or select values in entry fields.  
Press Enter AFTER making all desired changes.

[Entry Fields]	
Volume group name	rootvg
<b>SIZE of file system</b>	<input type="button" value=""/>
Unit Size	Megabytes
*     Number of units	[512]
* MOUNT POINT	/secure
Mount AUTOMATICALLY at system restart?	yes
PERMISSIONS	read/write
Mount OPTIONS	[ ]
Block Size (bytes)	4096
Logical Volume for Log	[ ]
Inline Log size (MBytes)	
Extended Attribute Format	[ ]
Enable Quota Management?	no
Enable EFS?	yes
Allow internal snapshots?	no
Mount GROUP	[ ]

```
# mount /secure
```

```
# lsfs -q /secure
Name      Nodename  Mount Pt          VFS  Size   Options  Auto Accounting
/dev/fslv00  --       /secure        jfs2  1048576  rw      yes  no
(lv size: 1048576, fs size: 1048576, block size: 4096, sparse files: yes, inline log: no,
inline log size: 0, EAformat: v2, Quota: no, DMAPI: no, VIX: yes, EFS: yes, ISNAPSHOT: no,
MAXEXT: 0)
```

### Setting Inheritance in EFS

- Encryption Inheritance indicates whether a file or directory inherits both the property of being encrypted and the encryption parameters from its parent directory.

- Encryption inheritance is not turned on initially when a file system is created; you must turn it on explicitly by using the AIX efsmgr command. You can set encryption inheritance at a file or directory level.
- If you need to create all the files in the EFS, you can switch on inheritance at the file-system level, which encrypts all files as they are created. The format of the efsmgr command for doing this is as follows:

```
# efsmgr -s -E /secure
```

- shows the error that is displayed if the Korn shell where you want to switch on inheritance is not authenticated

```
# cat > /secure/file1
No attribute found
ksh: /secure/file1: cannot create
```

- Error that is displayed if the Korn shell is not authenticated
- This error is caused because AIX cannot find the requested security attribute. To acquire a security attribute, run the AIX efskeymgr -o ksh command

```
# ps
 PID      TTY      TIME CMD
 2031670  pts/2    0:00 ps
 7012540  pts/2    0:00 -ksh
```

```
# efskeymgr -o ksh
root's EFS password:
```

- Notice that the efskeymgr command prompts for the user's EFS password. After you enter the password, the command takes you back to the Korn shell (ksh) that has permission to read and write to the EFS.
- The AIX ps command shows you another ksh that is running.
- Now, you can use this alternate ksh to create files that are automatically encrypted when they are written to the EFS partition.

```
# ps
 PID      TTY      TIME CMD
 6750208  pts/2    0:00 ksh
 7012540  pts/2    0:00 -ksh
 7667786  pts/2    0:00 ps
```

```
# cat > /secure/file1
hello kernel
#
```

- To determine whether a particular file or directory is encrypted, issue the following command:

```
# ls -U /secure/file1
-rw-r--r--e 1 root system 13 Apr 16 11:10 /secure/file1
```

- Assigning full permissions to '/secure' directory, so that any user can get into the directory and can create their own encrypted files.

```
# chmod 777 /secure
```

- Creating a new user 'ktuser' so that he can log into the system and create some files in /secure directory.

```
# mkuser ktuser
# passwd ktuser
Changing password for "ktuser"
ktuser's New password:
Re-enter ktuser's new password:
```

- Logging in with the new user 'ktuser' on the same server where the '/secure' filesystem has been created.

```
AIX Version 6
Copyright IBM Corporation, 1982, 2010.
login: ktuser
ktuser's Password:
[compat]: You are required to change your password. Please choose a new one.

ktuser's New password:
Re-enter ktuser's new password:
*****
*
*
* Welcome to AIX Version 6.1!
*
*
*
* Please see the README file in /usr/lpp/bos for information pertinent to
* this release of the AIX Operating System.
*
*
*****
$

*
```

- In EFS, keystore passwords are automatically synchronized to user login passwords.
- Similarly for ktuser, when the user logs in, the user keystore password has been already activated.

```
$ cd /secure
$ cat > file2
this is kernel technologies
$
$ ls -U
total 32
-rw-r--r--e 1 root      system          13 Apr 16 11:10 file1
-rw-r--r--e 1 ktuser    staff           28 Apr 17 11:16 file2
drwxr-xr-x- 2 root      system          256 Apr 16 10:48 lost+found
```

- So when ktuser gets into '/secure' directory and creates a file it doesn't ask for any 'efs password' because the keystore password has already been synchronized with his login password.

```
# su - ktuser
$ cd /secure
$ cat file2
cat: cannot open file2
```

- But here comes the speciality for EFS filesystem:
- When root does su to ktuser and try to read the file 'file2' which was created by the actual 'ktuser', it gets denied because root user doesn't have access to ktuser keystore password.
- so to read the file 'file2', the root user need to load the ktuser keystore password by giving the command:

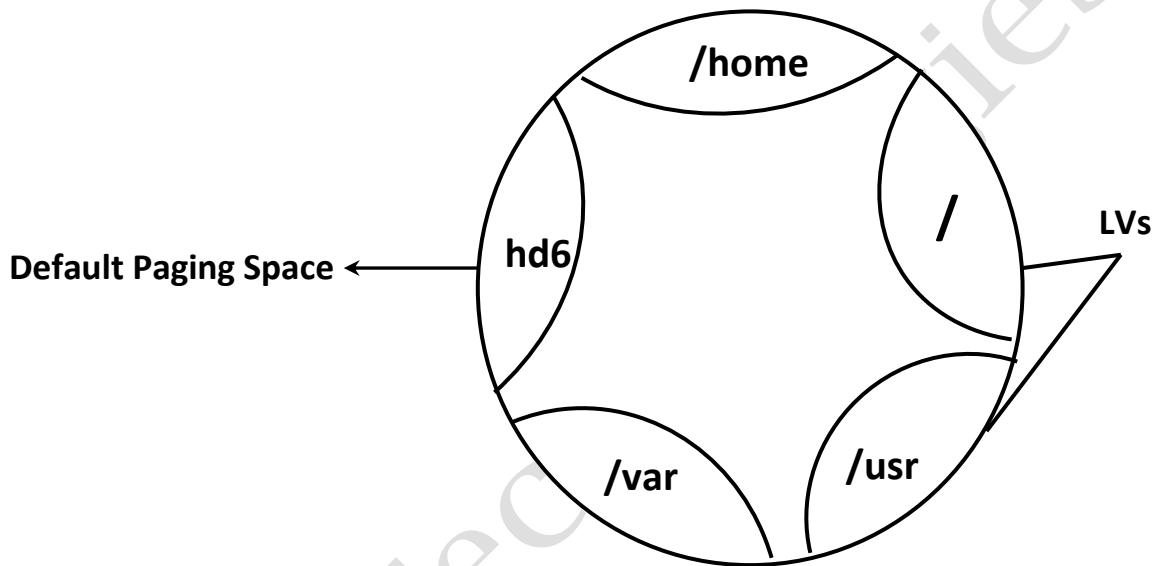
```
#efskeymgr -o ksh
```

```
$ efskeymgr -o ksh
ktuser's EFS password:
```

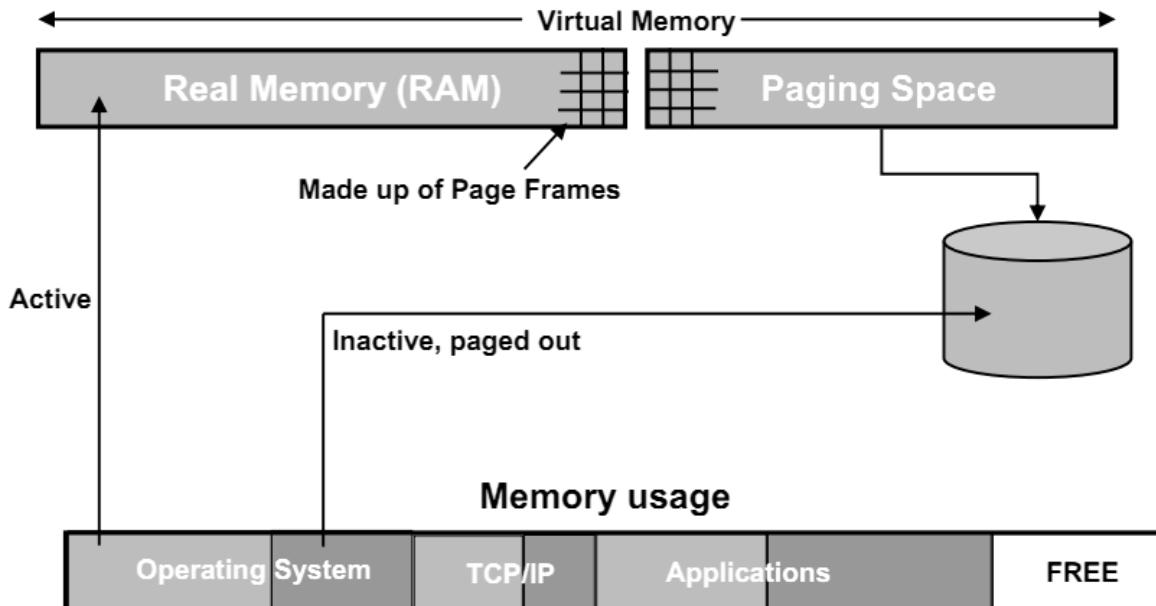
- After the ktuser keystore password is entered, the root user now can read the encrypted file i.e 'file2'

```
$ cat file2
this is kernel technologies
```

## PAGING SPACE



- ◀ For a process to be actively running, it must be loaded into memory. When it is loaded into memory, it is assigned a number of 4 KB areas called page frames. As more processes are loaded into memory, memory may become full. Not everything that resides in memory is active. When memory is full, memory is scanned to locate those page frames that are least-recently used. When one is located (and the data it contains cannot be moved to a “permanent home” in file system space), a 4 KB block or page of disk space is allocated and the data from the page frame is moved to a special area on disk. This area on disk is called paging space.
- ◀ The paging space is a reserved area on disk that can contain information that resided in memory but was inactive and was moved to make room for information that is currently being used. If paged-out information is needed in memory again, the page is retrieved and brought back into memory or paged-in.



- ☞ Whenever a process is shifted to paging area from RAM, it is termed as page out (PO).
- ☞ When a process enters back into RAM from paging space/area, it is termed as page in (PI)
- ☞ Lots of PI and PO activities are not good for the health of System.
- ☞ Paging spaces are just to store processes for temporary periods, it is not at all substitute to RAM.
- ☞ If there are always more PIs and POs in the system, then it is preferable to upgrade the RAM size.
- ☞ The standard size for the paging space would be double the size of RAM, but if the RAM size is more than 4GB, then it is recommended to have paging area not more than 4GB.
- ☞ As paging spaces are not substitute to RAM, it is not recommended to waste more disk space for paging spaces.

Rahul sir will run a video for swap for 18 minutes Very important to understand paging space.

## **LAB ACTIVITIES:-**

1. List all the paging spaces.

↳ #lsp -a or smitty lvm -> paging space -> list all paging space

#	lsp -a	Page Space	Physical Volume	Volume Group	Size	%Used	Active	Auto	Type
		hd6	hdisk0	rootvg	512MB	1	yes	yes	lv

#lsp -s (this will display only the usage of paging space).

#	lsp -s	Total Paging Space	Percent Used
		512MB	1%

2. Add another paging space.

↳ Through command line:-

#mkps -s 6 -n -a rootvg (always use rootvg to create paging space)

# mkps -s 6 -n -a rootvg  
paging00

a new paging space “paging00” will be created.

Through smitty:-

#smitty mkps select rootvg and change the following attributes.

Add Another Paging Space

Type or select values in entry fields.  
Press Enter AFTER making all desired changes.

Volume group name	[Entry Fields]	rootvg
SIZE of paging space (in logical partitions)	[6]	
PHYSICAL VOLUME name		
Start using this paging space NOW?		yes
Use this paging space each time the system is RESTARTED?		yes

3. Increase the size of above created paging space (paging00) with 4 LP.

↳ Through command line:-

#chps -s 4 paging00

Through smitty:-

#smitty chps and make the following changes

```
Change / Show Characteristics of a Paging Space

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
Paging space name          paging00
Volume group name           rootvg
Physical volume name        hdisk0
NUMBER of additional logical partitions [4]
Or NUMBER of logical partitions to remove []
Use this paging space each time the system is      yes
RESTARTED?
```

4. Reduce the size of a paging space with 4 LP

◀ Through command Line:-

#chps -d 4 paging00 (check the output by #lsp -a)

Through Smitty

#smitty chps and change the following attributes.

```
Change / Show Characteristics of a Paging Space

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
Paging space name          paging00
Volume group name           rootvg
Physical volume name        hdisk0
NUMBER of additional logical partitions []
Or NUMBER of logical partitions to remove [4]
Use this paging space each time the system is      yes
RESTARTED?
```

5. Deactivate and activate the paging space

◀ Deactivation of paging space through command Line:-

#swapoff /dev/paging00

```
# swapoff /dev/paging00
# lsp -a
Page Space      Physical Volume   Volume Group    Size %Used Active Auto Type
paging00        hdisk0            rootvg         768MB   0 no   yes   lv
hd6             hdisk0            rootvg         512MB   1 yes  yes   lv
```

Deactivation of paging space through smitty:-

#smitty swapoff and select the paging space name i.e. paging00 and hit enter.

Activation of paging space through Command Line:-

```
#swapon /dev/paging00
# swapon /dev/paging00
# lsns -a
Page Space      Physical Volume   Volume Group    Size %Used Active Auto Type
paging00        hdisk0           rootvg          768MB   1 yes   yes   lv
hd6             hdisk0           rootvg          512MB   1 yes   yes   lv
```

Doing the same through smitty:-

#smitty swapon and select the name of paging space and press enter key.

6. Remove the paging space you have created (i.e paging00)

- ↳ Through command line: - (First deactivate the paging space you are going to remove by using swapoff command.

```
#rmps paging00
# rmps paging00
rmlv: Logical volume paging00 is removed.
```

Removing paging space through smitty:-

#smitty rmps and select the name of the paging space you want to delete.

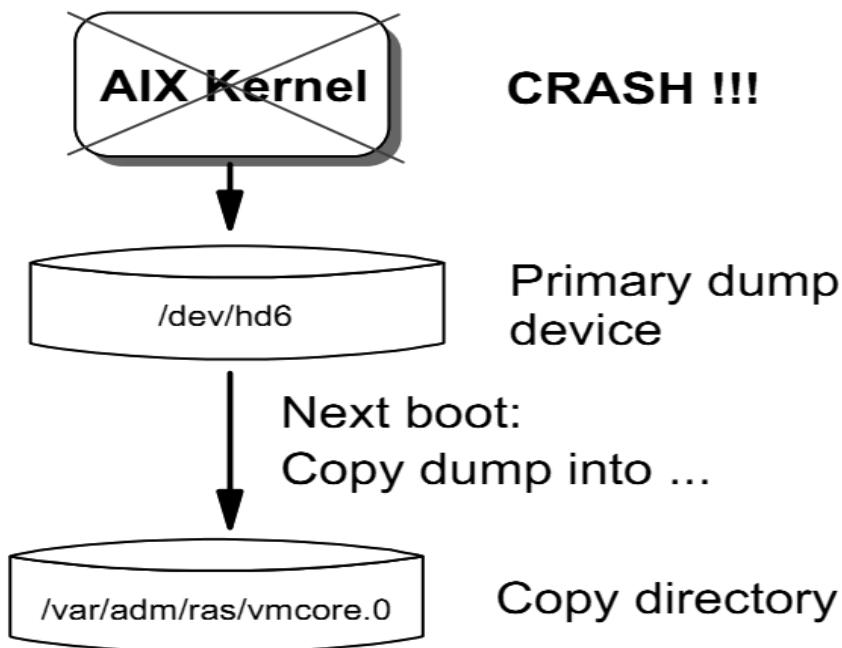
NOTE: In real time L1/L2 admin don't take decision to expand paging space . It will be recommended by IBM or SME. Sometimes increase paging space might affect performance. So, don't take nasty decision by your own.

TASK: You might have learned to Raise and Close ticket. If you haven't Please ask LAB faculty to demonstrate you.

## SYSTEM DUMP

- ↳ If an AIX kernel (the major component of your operating system) crashes, a dump is created. This dump can be used to analyze the cause of the system crash. As administrator you have to know what a dump is, how the AIX dump facility is maintained, and how a dump can be started.
- ↳ Before sending a dump to IBM, use the snap command to package the dump.

### When Dump Occurs



- ↳ If the AIX kernel crashes (system-initiated or user-initiated) kernel data is written to the primary dump device, which is by default /dev/hd6, the paging device. After a kernel crash AIX must be rebooted.
- ↳ During the next boot, the dump is copied into a dump directory, the default is /var/adm/ras. The dump file name is vmcore.x, where x indicates the number of the dump (for example 0 indicates the first dump).
- ↳ In order to send the dump information to IBM, after the rebooting the system run `# snap -ac`, then a snap will be collected in **snap.pax.z** format.
- ↳ Later by logging a call to IBM an PMR NO can be obtained.
- ↳ Rename your **snap.pax.z** fie with adding PMR NO before **snap.pax.z** (e.g 4346b422.snap.pax.z) and send it to IBM as prescribe by IBM executive.

## **LAB ACTIVITIES:-**

1. Check dumpsize.

↳ #sysdumpdev –e

2. Check the status of previous dump.

↳ #sysdumpdev –L

3. Create a LV with type “sysdump” & set as primary dump device.

↳ #Creating an LV

```
#mklv –y lvname –t sysdump rootvg 10 (*10 = No of LP, LV should only be created on  
rootvg)
```

```
#smmit mklv
```

#select a vgnane (say rootvg) and change the following

The screenshot shows a terminal window titled "Add a Logical Volume". It displays a configuration form with several fields:

[Entry Fields]	
Logical volume NAME	[dumplv]
* VOLUME GROUP name	rootvg
* Number of LOGICAL PARTITIONS	[10]
PHYSICAL VOLUME names	[]
Logical volume TYPE	[sysdump]
POSITION on physical volume	middle
RANGE of physical volumes	minimum
MAXIMUM NUMBER of PHYSICAL VOLUMES to use for allocation	[]
Number of COPIES of each logical	1

Changing primary dump device through command line

```
#sysdumpdev –P –p /dev/dumplv (dumplv is the lv created above)
```

Changing primary device through smitty

```
#smmit dump
```

The screenshot shows a terminal window titled "System Dump". It displays a menu with various options:

- Move cursor to desired item and press Enter.
- Show Current Dump Devices
- Show Information About the Previous System Dump
- Show Estimated Dump Size
- Change the Primary Dump Device** (highlighted with a green box)
- Change the Secondary Dump Device
- Change the Directory to which Dump is Copied on Boot
- Start a Dump to the Primary Dump Device
- Start a Dump to the Secondary Dump Device
- Copy a System Dump from a Dump Device to a File
- Always ALLOW System Dump
- System Dump Compression
- Check Dump Resources Utility

Enter new primary device name (i.e. /dev/dumplv)

```
Change Primary Dump Device

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
* Primary dump device [/dev/dumplv]
```

After changing the primary dump device, run **snap** command to collect system information along with the dump information into a file named **snap.pax.Z**.

4. #snap –ac

After this, you can find a file named “**snap.pax.Z**” file in a directory **/tmp/ibmsupt**  
This is the file which we need to send it to IBM for analysis.

5. Set dump device back to null

↳ #sysdumpdev –p /dev/sysdumpnull

6. How to remove previous dump

↳ #snap –r

NOTE: TO log call with IBM you need customer no. and serial no. of your server.

We need to ftp snap.pax.z to IBM support directory to analysis.

In Realtime we prepare Root cause analysis for customer, once IBM and send us feedback.

## SCHEDULING AND JOB AUTOMATION

- ↳ Programming a job to be run at a particular time without the interference of the user, even in the absence of the user is known as scheduling or job automation.
- ↳ In AIX job automation can be done using :

↳ CRON

↳ AT

↳ BATCH

### CRON:

- ↳ **Cron** is a time-based job scheduler in AIX computing system. Cron enables users to schedule jobs (commands or shell scripts) to run periodically at certain times or dates. It is commonly used to automate system maintenance or administration.
- ↳ Cron is driven by a *crontab* (cron table) file, a configuration file that specifies shell commands to run periodically on a given schedule. The crontab files are stored where the lists of jobs and other instructions to the cron daemon are kept. Users can have their own individual crontab files and often there is a system wide crontab file (usually in /etc or a subdirectory of /etc) which only system administrators can edit.

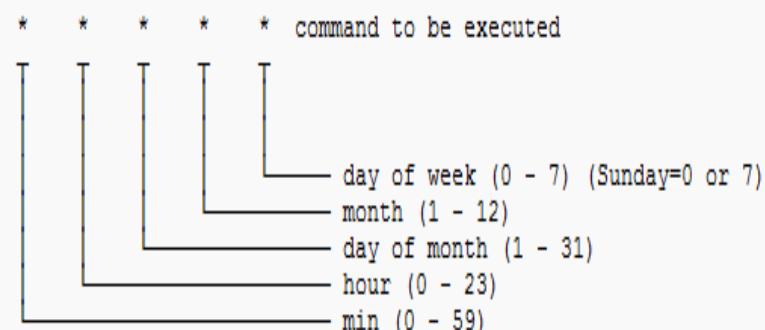
### Crontab files:

- ↳ **Schedule is defined in:**  
**/var/spool/cron/crontabs/\$USER**
- ↳ **Files to control crontab privileges of users:**
  - **/var/adm/cron/cron.deny** lists users who cannot use **crontab**
  - **/var/adm/cron/cron.allow** lists users who can use **crontab**
- ↳ An empty **cron.deny** exists by default
- ↳ If both **cron.allow** and **cron.deny** exist, then **cron.allow** is the file that is used. If neither **cron.allow** nor **cron.deny** exists, then only root can use cron.
- ↳ Please note that if neither of these files exists, then depending on site-dependent configuration parameters, only the super user (root) will be allowed to use cron jobs

### Examples of Cronjobs:

↳ #crontab -l

```
#0 3 * * * /usr/sbin/skulker
#45 2 * * 0 /usr/lib/spell/compress
#45 23 * * * ulimit 5000; /usr/lib/smmon.demon.cleanu > /dev/null
0 11 * * * /usr/bin/errclear -d S,O 30
0 12 * * * /usr/bin/errclear -d H 90
0 15 * * * /usr/lib/ras/dumpcheck >/dev/null 2>&1
```



Entry	Description	Equivalent To
@yearly (or @annually)	Run once a year, midnight, Jan. 1	0 0 1 1 *
@monthly	Run once a month, midnight, first of month	0 0 1 * *
@weekly	Run once a week, midnight on Sun	0 0 * * 0
@daily	Run once a day, midnight	0 0 * * *
@hourly	Run once an hour, beginning of hour	0 * * * *
@reboot	Run at startup	

## **AT & BATCH:**

The **at** and **batch** facilities are used to submit a job for one-time execution

- ◀ The **at** command submits a uniquely occurring job to be run by **cron** at a specified time:

```
# at now + 2 mins
banner Kernel Tech >/dev/pts/0
<ctrl+d>
Job root.1307170859.a will be run at Sat Jun  4 13:00:59 PAKDT 2011.

#      #
#      #####  #####  #      #  #####  #
#      #      #      #  ##  #      #      #
###      #####  #      #  ##  #      #####  #
#      #      #####  #      #  ##  #      #
#      #      #      #  ##  #      #      #
#      #      #####  #      #  ##  #      #####  #####
#####      #
#      #####  #####  #      #
#      #      #      #  ##  #
#      #####  #      #      #####
#      #      #      #  ##  #
#      #      #      #  ##  #
#      #####  #####  #      #
```

```
# batch
banner Kernel Tech > /dev/pts/0
<ctrl+d>
Job root.1307171229.b will be run at Sat Jun  4 13:07:09 PAKDT 2011.

#      #
#      #####  #####  #      #  #####  #
#      #      #      #  ##  #      #      #
###      #####  #      #  ##  #      #####  #
#      #      #      #####  #      #      #
#      #      #      #  ##  #      #
#      #      #####  #      #  ##  #      #####  #####
#####      #
#      #####  #####  #      #
#      #      #      #  ##  #
#      #####  #      #      #####
#      #      #      #  ##  #
#      #      #      #  ##  #
#      #####  #####  #      #
```

### **Controlling use of at**

- ◀ The **at** command can only be used by root unless one of the following files exists:
  - **/var/adm/cron/at.deny**

- ↳ If this file exists, anybody can use at except those listed in it. An empty **at.deny** file exists by default. Therefore, all users can use at by default.  
- **/var/adm/cron/at.allow**
- ↳ If this file exists, only users listed in it can use at jobs (including root).

### **LAB ACTIVITIES:-**

1. Check directory structure of cron.

```
#cd /var/adm/cron  
#cd /var/spool/cron/crontabs
```

2. Create a user and check if he is allowed to use cron jobs.
3. Deny above user & check if he is able to use cron job.

Go to #cd /var/adm/cron

```
#ls  
#vi cron.deny
```

Here add the user name (say “ktuser”) & save it.

Now login as user (ktuser) try to create cron job.

4. Create a “cron.allow” file & put the above user in the file, now check if he can do the cron job & also at the same time check if root can use cron job.

Go to #cd /var/adm/cron

```
#vi cron.allow
```

Here just type the user name (say “ktuser”) in cron.allow & save it.

Now login as user (“ktuser”) try to create cron job.

Now come back to root user and check whether root can create a cron job.

5. Submit one cron job for that user (e.g.: creating a file or directory) & see if the job completes & also check status in “log file”.
6. Now give an entry in the “cron table” to reboot the server after 5min & see if it works.
7. kill “cron daemon” & see if it starts automatically.
8. How many max jobs a cron can take. ( hint: “queuedfs” file)

NOTE:In class Rahul sir will give Realtime note on this problem. This is important chapter for Interview and easy to score in interview.

## USER ADMINISTRATION

- ◀ Users are the primary agents on the system. Each user is required to log in to the system. The user supplies the user name of an account and a password if the account has one (on a secure system, all accounts either have passwords or are invalidated). If the password is correct, the user is logged in to that account; the user acquires the access rights and privileges of the account. The /etc/passwd and /etc/security/passwd files maintain user passwords.

### User accounts:

- ◀ Each user has a unique name, numeric ID, and password
- ◀ File ownership is determined by a numeric user ID
- ◀ The owner is usually the user who created the file, but ownership can be transferred by **root**

### Default users:

- ◀ **Root** Superuser
- ◀ **adm, sys, bin**, ... IDs that own system files but cannot be used for login

### Groups:

- ◀ Groups are collections of users who can share access permissions for protected resources. A group has an ID, and a group is composed of members and administrators. The creator of the group is usually the first administrator. There are three types of groups:
- ◀ **User group:** User groups should be made for people who need to share files on the system, such as people who work in the same department or people who are working on the same project. In general, create as few user groups as possible.
- ◀ **System administrator groups:** System administrator groups correspond to the SYSTEM group. SYSTEM group membership allows an administrator to perform some system maintenance tasks without having to operate with root authority.
- ◀ **System-defined groups:** There are several system-defined groups. The STAFF group is the default group for all non administrative users created in the system. You can change the default group by using the **chsec** command to edit the /usr/lib/security/mkuser.default file. The SECURITY group is a system-defined group having limited privileges for performing security

## **User administration related files**

**The following files are referenced while doing user administration:**

- |                                    |   |
|------------------------------------|---|
| ↳ /etc/security/environ            | Contains the environment attributes for users.                                |
| ↳ /etc/security/lastlog            | Contains the last login attributes for users.                                 |
| ↳ /etc/security/limits             | Contains process resource limits for users.                                   |
| ↳ /etc/security/user               | Contains extended attributes for users.                                       |
| ↳ /usr/lib/security/mkuser.default | Contains the default attributes for new users.                                |
| ↳ /usr/lib/security/mkuser.sys     | Customizes new user accounts.   |
| ↳ /etc/passwd                      | Contains the basic attributes of users.                                       |
| ↳ /etc/security/passwd             | Contains password information.  |
| ↳ /etc/security/login.cfg          | Contains configuration information for login and user authentication.         |
| ↳ /etc/utmp                        | Contains the record of users logged into the system.                          |
| ↳ /var/adm/wtmp                    | Contains connect time accounting records.                                     |
| ↳ /etc/security/failedlogin        | Records all failed login attempts.  |
| ↳ /etc/motd                        | Contains the message to be displayed every time a user logs in to the system. |
| ↳ /etc/environment                 | Specifies the basic environment for all processes.                            |
| ↳ /etc/profile                     | Specifies additional environment settings for all users.                      |
| ↳ \$HOME/.profile                  | Specifies environment settings for specific user needs.                       |
| ↳ /etc/group                       | Contains the basic attributes of groups.                                      |
| ↳ /etc/security/group              | Contains the extended attributes of groups.                                   |

**NOTE:**For L1/L2 engineers user administrator is important topic. As we do must of task in user administration. Learn process of ticketing.

## **LAB ACTIVITIES:-**

1. Create a user by command “#mkuser username” & do “#lsuser username” & see what the default group is & also check the properties of the user?

↳ Creating a user

#mkuser ktuser

# lsuser ktuser

The default group is staff and check other properties also.

Creating a user using smitty

#smitt mkuser

The screenshot shows the 'Add a User' menu from the smitty interface. The menu title is 'Add a User'. It displays a list of configuration fields:

[Entry Fields]	
* User NAME	[ktuser]
User ID	[]
ADMINISTRATIVE USER?	false
Primary GROUP	[]
Group SET	[]
ADMINISTRATIVE GROUPS	[]
ROLES	[]
Another user can SU TO USER?	true
SU GROUPS	[ALL]
HOME directory	[]
Initial PROGRAM	[]
User INFORMATION	[]
EXPIRATION date (MMDDhhmmyy)	[0]

2. Browse through “/etc/security/user & /etc/security /limits” file notice the default values. Is this the default values we have got in ‘#lsuser username’ compare it?

↳ # pg /etc/security/user

```
default:
    admin = false
    login = true
    su = true
    daemon = true
    rlogin = true
    sugroups = ALL
    admgroups =
    ttys = ALL
    auth1 = SYSTEM
    auth2 = NONE
    tpath = nosak
    umask = 022
    expires = 0
    SYSTEM = "compat"
    logintimes =
    pwdwarntime = 0
    account_locked = false
    loginretries = 0
    histexpire = 0
    histsize = 0
    minage = 0
    maxage = 0
    maxexpired = -1
    minalpha = 0
    minother = 0
    minlen = 0
    mindiff = 0
    maxrepeats = 8
    dictionlist =
    pwdchecks =
```

```
#pg /etc/security/limits
```

```
* NOTE: A value of -1 implies "unlimited"
*
default:
    fsize = -1
    core = 2097151
    cpu = -1
    data = 262144
    rss = 65536
    stack = 65536
    nofiles = 2000
```

3. Also check “**failedlogin**, **login.cfg**, **lastlog**” in ‘/etc/security/’.

↳ go to **/etc/security** folder

```
#pg failedlogin
#pg login.cfg
#pg lastlog
```

4. Create a group (give your own name) & check in “/etc/group” file. Add a user to this group, create another group & modify the previous user to include in this group also.

↳ Creating a group through command:

```
#mkgroup group name (say ktgroup)
```

Creating a group through smitty:

```
#smitty mkgroup, then make the following changes
```

Add a Group

Type or select values in entry fields.  
Press Enter AFTER making all desired changes.

* Group NAME ADMINISTRATIVE group? Group ID USER list ADMINISTRATOR list Projects	[Entry Fields] [ktgroup] false [] [] [] []
--	--

Adding user to the group:

```
#smitty chgroup, and add user as below
```

Change Group Attributes

Type or select values in entry fields.  
Press Enter AFTER making all desired changes.

Group NAME Group ID ADMINISTRATIVE group? USER list ADMINISTRATOR list Projects	[Entry Fields] [ktgroup] [203] false [ktuser] [root] []
--	---

5. Lock the previous user & try to login now.

↳ #smit lockuser

Type user name (say ktuser), and make following changes and try logging in now.

Lock / Unlock a User's Account

Type or select values in entry fields.  
Press Enter AFTER making all desired changes.

* User NAME Is this user ACCOUNT LOCKED?	[Entry Fields] ktuser true
---	----------------------------------

6. Change the users “no of failed login attempt to 4” & now try to login with wrong password 4 times & see what happens? To solve this problem “Reset User's Failed Login Count”.

 Changing user's “no of failed login attempts”

#smit chuser, select user (say ktuser) and change following attributes

```
Change / Show Characteristics of a User

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP] [Entry Fields]
User NAME ktuser
User ID [210]
ADMINISTRATIVE USER? false
Primary GROUP [staff]
Group SET [staff]
ADMINISTRATIVE GROUPS []
ROLES []
Another user can SU TO USER? true
SU GROUPS [ALL]
HOME directory [/home/ktuser]
Initial PROGRAM [/usr/bin/ksh]
User INFORMATION []
EXPIRATION date (MMDDhhmmYY) [0]
Is this user ACCOUNT LOCKED? false
User can LOGIN? true
User can LOGIN REMOTELY(rsh,tn,rlogin)? true
Allowed LOGIN TIMES []
Number of FAILED LOGINS before user account is locked [4]
```

Now, open another session and login with wrong passwd for 4 times and see (\*the user account will get locked)

Reset User's failed login counts:

#smit user, select the following and then select the user to whom you want change the Login count.

```
Users

Move cursor to desired item and press Enter.

Add a User
Change a User's Password
Change / Show Characteristics of a User
Lock / Unlock a User's Account
Reset User's Failed Login Count
Remove a User
List All Users
```

7. Remove a user through “rmuser” command without ‘-p’ flag & now remove another user using ‘-p’ flag. Find out what is the difference?

↳ #rmuser user name (say ktuser)  
#rmuser -p user name (say ktuser2)  
\*check /etc/security/passwd file and /home dir of the user

8. Observe difference between “/etc/passwd” & “/etc/security/passwd” permissions.

9. Change one of the user file size limit to be unlimited.

↳ #smmit chuser select user and change the following attribute

```
Change / Show Characteristics of a User

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[MORE...28] [Entry Fields]
Password MIN. AGE [0] #
Password MIN. LENGTH [0] #
Password MIN. ALPHA characters [0] #
Password MIN. OTHER characters [0] #
Password MAX. REPEATED characters [8] #
Password MIN. DIFFERENT characters [0] #
Password REGISTRY [files] #
Soft FILE size [-1] #
Soft CPU time [-1] #
Soft DATA segment [262144] #
Soft STACK size [65536] #
Soft CORE file size [2097151] #
Hard FILE size [] #

[MORE...10]
```

### User Admin Commands:

1. To change the attributes stored in the security configuration stanza files as default.

↳ # vi /etc/security/limits.

2. To change the CPU time limit of a particular user.

↳ #chsec -f /etc/security/limits -s KTUser -a cpu=3600

3. To change the soft file size limit in blocks of a particular user.

↳ #chsec -f /etc/security/limits -s KTUser -a fsize=-1.(-1 is for unlimited you can use your required value in block size)

4. To change the soft data segment size in blocks for a particular user.  
↳ `#chsec -f /etc/security/limits -s KTUser -a data=43786 (or whatever your requirement is).`
5. To change soft stack segment size in blocks for a particular user.  
↳ `#chsec -f /etc/security/limits -s KTUser -a stack=43786 (or your desired value)`
6. To change real memory usage in blocks for particular user.  
↳ `#chsec -f /etc/security/limits -s KTUser -a rss=75536 (or your desired value)`
7. To reset the unsuccessful login counts of a particular value  
↳ `#chsec -f /etc/security/lastlog -s KTUser -a unsuccessful_login_count=0`
8. To change the login times a user can login to the server.  
↳ `#chsec -f /etc/security/user -s KTUser -a logintimes=mon-fri:0800-1700 (to enable user login till 8AM to 5PM from Monday to Friday)`
9. To change the password validy of the user in weeks.  
↳ `#chsec -f /etc/security/user -s KTUser -a maxage=10 (default is 0 and Range is 0-52)`
10. To change the maximum no. of weeks after maxage of the passwd.

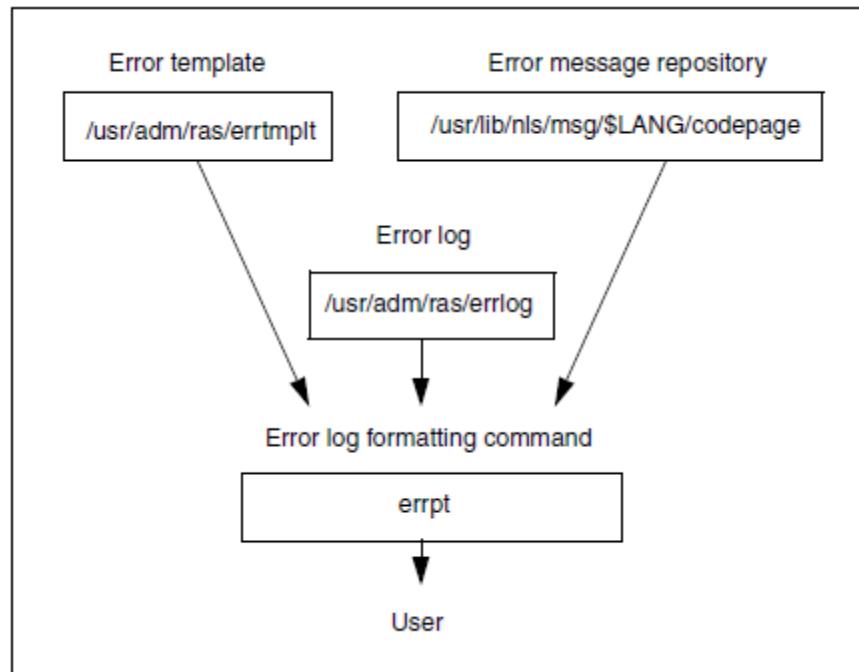
- ↳ **Note:-** The number of weeks after the user's password expires (reaches its maximum age) during which the user can still change the password.If this time period passes without a password change, the user account no longer allows logins until an administrator resets the password. The value is a decimal integer string.If 0 is specified, logins will be prevented at the time the password expires. If -1 is specified, this feature is disabled. If Password MAX. AGE is 0, any value entered here is ignored

`#chsec -f /etc/security/user -s KTUser -a maxexpired=value (ex 1,2 or any desired)`

11. To change users can switch to particular user account.  
↳ `#chsec -f /etc/security/user -s KTUser -a su=true (possible values true or false)`
12. To change the /dev/tty0 port to automatically lock if 5 unsuccessful login attempts occur within 60 seconds  
↳ `#chsec -f /etc/security/login.cfg -s /dev/tty0 -a logindisable=5 -a logininterval=60`
13. To unlock the /dev/tty0 port after it has been locked by system  
↳ `#chsec -f /etc/security/portlog -s /dev/tty0 -a locktime=0`
14. To allow logins from 8:00 AM until 5:00 PM for all users  
↳ `#chsec -f /etc/security/user -s default -a logintimes=mon-fri:0800-1800`

## PROBLEM DETERMINATION AND ERROR REPORTING

- The first step in problem resolution is to define the problem. It is important that the person trying to solve the problem understands exactly what the users of the system perceive the problem to be. A clear definition of the problem is useful in two ways. First of all, it can give you a hint as to the cause of the problem. Secondly, it is much easier to demonstrate to the users that the problem has been solved if you know how the problem is seen from their point of view.



- The error logging process begins when an operating system module detects an error. The error detecting segment of code then sends error information to either the **errsave()** kernel service or the **errlog()** application subroutine, where the information is in turn written to the **/dev/error** special file. This process then adds a timestamp to the collected data. The **errdemon** daemon constantly checks the **/dev/error** file for new entries, and when new data is written, the daemon conducts a series of operations.
- Before an entry is written to the error log, the **errdemon** daemon compares the label sent by the kernel or the application code to the contents of the Error Record Template Repository. If the label matches an item in the repository, the daemon collects additional data from other parts of the system.

<b>Type of Report</b>	Summary, intermediate and detailed reports are available. Detailed reports give comprehensive information. Intermediate reports display most of the error information. Summary reports contain concise descriptions of errors.
<b>Error CLASSES</b>	Values are H (hardware), S (software) and O (operator messages created with <b>errlogger</b> ). You can specify more than one error class.
<b>Resource CLASSES</b>	Means device class for hardware errors (for example, disk).
<b>Error TYPES</b>	
 <b>PEND</b>	The loss of availability of a device or component is imminent
 <b>PERF</b>	The performance of the device or component has degraded to below an acceptable level
 <b>TEMP</b>	Recovered from condition after several attempts
 <b>PERM</b>	Unable to recover from error condition. Error types with this value are usually most severe error and imply that you have a hardware or software defect. Error types other than PERM usually do not indicate a defect, but they are recorded so that they can be analyzed by the diagnostic programs
 <b>UNKN</b>	Severity of the error cannot be determined.
 <b>INFO</b>	The error type is used to record informational entries

## Diagnostics:

- ◀ The lifetime of hardware is limited. Broken hardware leads to hardware errors in the error log, to systems that will not boot or to very strange system behavior. The **diagnostic** package helps you to analyze your system and discover hardware that is broken. Additionally the **diagnostic** package provides information to service representatives that allow fast error analysis.
- ◀ Whenever you detect a hardware problem, for example, a communication adapter error in the error log, use the **diag** command to diagnose the hardware.
- ◀ The **diag** command allows testing of a device if the device is not busy. If any AIX process uses a device, the diagnostic programs cannot test it; they must have exclusive use of the device to be tested.
- ◀ The **diag** command analyses the error log to fully diagnose a problem if run in the correct mode. It provides information that is very useful for the service representative, for example **SRNs** (Service Request Numbers) or probable causes. There is a cross link between the AIX error log and diagnostics. When the **er rpt** command is used to display an error log entry, diagnostic results related to that entry are also displayed.

## **LAB ACTIVITIES:-**

1. check “error” file in /dev.

```
↳ #cd /dev  
#ls
```

2. Check if “errdemon” is running, Kill it.

```
↳ #ps -ef |grep errdemon → will show if the errdemon is running  
#kill -9 pid → of errdemon
```

3. Start errdemon again, use “errstop” to stop it again, start again.

```
↳ #/usr/lib/errdemon → is the command to start errdemon  
#/usr/lib/errstop → will stop errdemon (check by ps -ef)
```

4. Run “errpt” to see latest error.

```
↳ #errpt
```

```
# errpt  
IDENTIFIER TIMESTAMP T C RESOURCE_NAME DESCRIPTION  
9DBCFDEE 0318162311 T O errdemon ERROR LOGGING TURNED ON  
192AC071 0318162211 T O errdemon ERROR LOGGING TURNED OFF  
9DBCFDEE 0318162111 T O errdemon ERROR LOGGING TURNED ON  
192AC071 0318162111 T O errdemon ERROR LOGGING TURNED OFF  
9DBCFDEE 0318162011 T O errdemon ERROR LOGGING TURNED ON  
192AC071 0318161911 T O errdemon ERROR LOGGING TURNED OFF  
0BA49C99 0318153911 T H scsi2 SCSI BUS ERROR  
0BA49C99 0318143311 T H scsi2 SCSI BUS ERROR
```

5. See the details for particular error.

```
↳ #errpt -a -j errorid
```

6. I want to see only ‘Hardware error’. ( Hint: use ‘smitty errpt’ to filter)

```
↳ #smitty errpt -> select “Filename (default to stdouts) -> no and select following
```

```

Generate an Error Report

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
CONCURRENT error reporting? yes
Type of Report summary
Error CLASSES (default is all) [H]
Error TYPES (default is all) []
Error LABELS (default is all) []
Error ID's (default is all) []
Resource CLASSES (default is all) []
Resource TYPES (default is all) []
Resource NAMES (default is all) []

```

Through command line:

#errpt -d H

7. List only hardware errors which are permanent.

↳ #smitty errpt (same as above and change only the following)

```

Generate an Error Report

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
CONCURRENT error reporting? yes
Type of Report summary
Error CLASSES (default is all) [H]
Error TYPES (default is all) [PERM]
Error LABELS (default is all) []
Error ID's (default is all) []
Resource CLASSES (default is all) []
Resource TYPES (default is all) []
Resource NAMES (default is all) []

```

8. Run “diag” on a particular device.

↳ # diag, and select the following

9. Raise a ticket for disk issues and update ticket and collect emcgrab & transfer ticket to SAN team.
10. Raise a Ticket for fibre card replacement , update steps you have taken to replace and close the ticket.

NOTE: You can run diagnostics using diag CD mostly IBM CE use. Diag CD is RED and BLUE in colour available for power server.

### Step 1:

#### FUNCTION SELECTION

Move cursor to selection, then press Enter.

##### Diagnostic Routines

This selection will test the machine hardware. Wrap plugs and other advanced functions will not be used.

##### Advanced Diagnostics Routines

This selection will test the machine hardware. Wrap plugs and other advanced functions will be used.

##### Task Selection (Diagnostics, Advanced Diagnostics, Service Aids, etc.)

This selection will list the tasks supported by these procedures.

Once a task is selected, a resource menu may be presented showing all resources supported by the task.

##### Resource Selection

This selection will list the resources in the system that are supported by these procedures. Once a resource is selected, a task menu will be presented showing all tasks that can be run on the resource(s).

### Step2:

#### TASKS SELECTION LIST

From the list below, select a task by moving the cursor to the task and pressing 'Enter'.

To list the resources for the task highlighted, press 'List'.

[TOP]

##### Run Diagnostics

Run Error Log Analysis

Run Exercisers

Display or Change Diagnostic Run Time Options

Kern  
el

### Step3:

```
RESOURCE SELECTION LIST

From the list below, select any number of resources by moving
the cursor to the resource and pressing 'Enter'.
To cancel the selection, press 'Enter' again.
To list the supported tasks for the resource highlighted, press 'List'.

Once all selections have been made, press 'Commit'.
To avoid selecting a resource, press 'Previous Menu'.

[MORE...10]
  cd0          P1/Z1-A1      16 Bit SCSI Multimedia CD-ROM Drive (650
                           MB)
  scsi1        P1/Z2          Wide/Ultra-2 SCSI I/O Controller
  scsi2        P1-I3/Z1      Wide/Fast-20 SCSI I/O Controller
  hdisk1       P1-I3/Z1-A0    Other SCSI Disk Drive
  hdisk2       P1-I3/Z1-A1    Other SCSI Disk Drive
  hdisk3       P1-I3/Z1-A2    Other SCSI Disk Drive
```

11. Run diag on the whole system

↳ Run #diag and repeat above **step 2** and select the following

```
RESOURCE SELECTION LIST

From the list below, select any number of resources by moving
the cursor to the resource and pressing 'Enter'.
To cancel the selection, press 'Enter' again.
To list the supported tasks for the resource highlighted, press 'List'.

Once all selections have been made, press 'Commit'.
To avoid selecting a resource, press 'Previous Menu'.

[TOP]
  All Resources
    This selection will select all resources that can be tested.
```

12. Make one disk out of VG & run diag on it.

↳ #reducevg vgname diskname  
#diag and repeat steps of Q.no 8

13. Check any error during booting using “alog” command.

↳ #alog -o -t boot |more

14. Find out how to clear error records.

↳ #errclear 0

## Tcp/IP:

### List System Configuration Information

```
# lscfg
INSTALLED RESOURCE LIST

The following resources are installed on the machine.
+/- = Added or deleted from Resource List.
*   = Diagnostic support not available.

Model Architecture: chrp
Model Implementation: Multiple Processor, PCI bus

+ sys0
+ sysplanar0
* vio0
```

### List Device Information

```
# lsdev -Cc if
en0 Available Standard Ethernet Network Interface
en1 Available Standard Ethernet Network Interface
et0 Defined IEEE 802.3 Ethernet Network Interface
et1 Defined IEEE 802.3 Ethernet Network Interface
lo0 Available Loopback Network Interface
vi0 Available Virtual IP Address Network Interface
#
# lsdev -Cc adapter
ent0 Available Virtual I/O Ethernet Adapter (l-lan)
ent1 Available Virtual I/O Ethernet Adapter (l-lan)
vsa0 Available LPAR Virtual Serial Adapter
vscsi0 Available Virtual SCSI Client Adapter
```

- ◀ These two displays simply show how you can use the lsdev command to list out the interfaces and adapters configured on your system. Our interest in these displays is With the network interfaces and adapters.

## List Device Attributes

attribute	value	description	user_settable
alias4		IPv4 Alias including Subnet Mask	True
alias6		IPv6 Alias including Prefix Length	True
arp	on	Address Resolution Protocol (ARP)	True
authority		Authorized Users	True
broadcast		Broadcast Address	True
mtu	1500	Maximum IP Packet Size for This Device	True
netaddr	192.168.1.5	Internet Address	True
netaddr6		IPv6 Internet Address	True
netmask	255.255.255.0	Subnet Mask	True
prefixlen		Prefix Length for IPv6 Internet Address	True
remmtu	576	Maximum IP Packet Size for REMOTE Networks	True
rfc1323		Enable/Disable TCP RFC 1323 Window Scaling	True
security	none	Security Level	True
state	up	Current Interface Status	True

- ☞ The lsattr command displays information about the attributes of a given device or kind of device, as well as some of the possible values for a device on the system.

## Network Interface Parameters Display

```
# ifconfig lo0
lo0: flags=e08084b, c0<UP,BROADCAST,LOOPBACK,RUNNING,SIMPLEX,MULTICAST, GROUPRT, 64
BIT,LARGESEND,CHAIN>
        inet 127.0.0.1 netmask 0xff000000 broadcast 127.255.255.255
        inet6 ::1%1/0
                tcp sendspace 131072 tcp recvspace 131072 rfc1323 1
```

## The Snap Command:

- ☞ Gathers system configuration information
- ☞ Compresses information into pax file
- ☞ Requires root authority to use
- ☞ **#snap -c -l -n -t -o /dev/rmt0** (where rmt0 is a tape drive)
- ☞ What above command capture?
  - ☞ Device VDP information
  - ☞ All NFS information
  - ☞ All TCP/IP information
  - ☞ And compress the output to tape device rmt0

## Display Network Options

```
# no -a
```

```
# no -a
        arpqsiz = 12
        arpt_killc = 20
        arptab_bsiz = 7
        arptab_nb = 149
        bcastping = 0
        clean_partial_conns = 0
        delayack = 0
        delayackports = {}
        dgd_packets_lost = 3
        dgd_ping_time = 5
        dgd_retry_time = 5
        directed_broadcast = 0
        fasttimo = 200
        icmp6_errmsg_rate = 10
        icmpaddressmask = 0
        ie5_old_multicast_mapping = 0
        ifsize = 256
        ip6_defttl = 64
        ip6_prune = 1
        ip6forwarding = 0
        ip6srcrouteforward = 1
        ip_ifdelete_notify = 0
        ip_nfrag = 200
```

- ◀ The **no** command sets or displays current network options in the kernel depending on the option used. When making changes, this command only operates on the current running system and must be run again after each startup or after the network has been configured.

## Test Network Connectivity

```
# ping -c 3 ktaix33 (or IP add can also be used)
```

```
# ping -c 3 ktaix31
PING ktaix31 (192.168.10.31): 56 data bytes
64 bytes from 192.168.10.31: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 192.168.10.31: icmp_seq=1 ttl=255 time=0 ms
64 bytes from 192.168.10.31: icmp_seq=2 ttl=255 time=0 ms

--- ktaix31 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
#
```

Where *c* stands for count

- ◀ The **ping** command sends one datagram per second and prints one line of output for every response received. It calculates round trip times and packet loss statistics, and displays a brief summary upon completion

### Test Network Performance:

- ◀ **spray ktaix -c 5000 -l 1500 -d 1**

```
sending 5000 packets of length 1502 to  
ktaix31 ...
```

```
159 packets (3.180%) dropped by ktaix31  
754 packets/second, 1133741 bytes/second
```

- ◀ Spray sends a specified number of packets to a host and reports performance statistics. The spray command uses the Remote Procedure Call (RPC) protocol to send a one-way stream of packets to the host you specify. As RPC is at a higher level than ICMP it provides a more accurate picture of overhead than using ping. This command reports how many packets were received and at what transfer rate. The Host parameter can be either a name or an Internet address. The host only responds if the sprayd daemon is running.

### Check Address Resolution

```
# arp -a
```

```
? (192.168.10.2) at 0:10:18:33:d5:22 [ethernet] stored in bucket 5
? (192.168.10.6) at 54:52:0:15:9f:51 [ethernet] stored in bucket 9
? (192.168.10.167) at 0:e0:c5:44:9:5a [ethernet] stored in bucket 21
? (192.168.10.25) at e4:1f:13:4e:63:d4 [ethernet] stored in bucket 28
ktaix31 (192.168.10.31) at a2:4b:dd:28:a3:3 [ethernet] stored in bucket 34
? (192.168.10.81) at 0:24:1d:f9:d5:d9 [ethernet] stored in bucket 84
? (192.168.10.84) at bc:ae:c5:35:31:ad [ethernet] stored in bucket 87
```

```
◀ ktaix31 (192.168.10.31) at a2:4b:dd:28:a3:3 (published)
```

```
◀ ? (192.168.10.81) at 0:24:1d:f9:d5:d9 (incomplete)
```

## Display Network Memory Usage

```
# netstat -m
```

Kernel malloc statistics:							
By size	inuse	calls	failed	delayed	free	hiwat	freed
64	150	6618	0	2	106	5240	0
128	1102	6351	0	33	50	2620	0
256	3338	32643	0	205	70	5240	0
512	3987	96276	0	492	101	6550	0
1024	219	1816	0	54	21	2620	0
2048	1078	8296	0	521	20	3930	0
4096	136	152	0	5	1	1310	0
8192	6	28	0	3	15	327	0
16384	256	256	0	33	0	163	0
32768	48	48	0	12	0	81	0
65536	117	117	0	59	0	81	0
131072	4	4	0	0	102	204	0

## Display Transport UDP Statistics

```
# netstat -p udp
udp:
    12336 datagrams received
    0 incomplete headers
    0 bad data length fields
    0 bad checksums
    6962 dropped due to no socket
    3508 broadcast/multicast datagrams dropped due to no socket
    0 socket buffer overflows
    1866 delivered
    1993 datagrams output
```

- ◀ The value for packets dropped due to no socket indicates that a node sent data to a socket on the receiving node that was never opened. Or, this value could indicate that another node sent a packet but the process was killed, which also closes the socket. If this value is high, investigate the way the application is handling sockets.

## Display Transport TCP Statistics

```
# netstat -p tcp
```

```
tcp:
```

```
    25182 packets sent
        12294 data packets (898219 bytes)
        0 data packets (0 bytes) retransmitted
        6545 ack-only packets (318 delayed)
        0 URG only packets
        0 window probe packets
        1532 window update packets
        9766 control packets
        0 large sends
        0 bytes sent using largesend
        0 bytes is the biggest largesend
    29517 packets received
        16865 acks (for 902859 bytes)
        1528 duplicate acks
        0 acks for unsent data
        13142 packets (103923 bytes) received in-sequence
        1 completely duplicate packet (1 byte)
        0 old duplicate packets
        0 packets with some dup. data (0 bytes duped)
        1591 out-of-order packets (138 bytes)
        0 packets (0 bytes) of data after window
```

- For the TCP statistics, compare the number of packets sent to the number of data packets retransmitted. If the number of packets retransmitted is over 10-15% of the total packets sent, TCP is timing out indicating that network traffic may be too high for acknowledgements (ACKs) to return before a time-out. A bottleneck on the receiving node or general network problems can also cause TCP retransmissions. TCP retransmissions increase network traffic, further adding to any network performance problems.

## Monitor State of an Interface

```
# netstat -I trl 2
```

input (en0)			output			input (Total)			output			
packets	errs	packets	errs	colls	packets	errs	packets	errs	colls	packets	errs	colls
1136342	0	1709	0	0	1156559	0	472268	0	0	0	0	0
9	0	1	0	0	16	0	1	0	0	0	0	0
6	0	1	0	0	11	0	1	0	0	0	0	0
5	0	1	0	0	9	0	1	0	0	0	0	0
6	0	1	0	0	10	0	2	0	0	0	0	0
4	0	1	0	0	7	0	1	0	0	0	0	0
4	0	2	0	0	6	0	2	0	0	0	0	0
2	0	2	0	0	2	0	2	0	0	0	0	0
1	0	1	0	0	1	0	1	0	0	0	0	0

- ☞ The netstat -l <network interface> <interval> displays the state of the configured interface as it is being monitored for traffic across that interface. The interval variable displays how frequently to display the information. It shows both input and output traffic along with errors and collisions.

## Display Device Driver Statistics

#netstat -v

```
ETHERNET STATISTICS (ent1) :
Device Type: IBM 10/100 Mbps Ethernet PCI Adapter (23100020)
Hardware Address: 00:06:29:84:f7:58
Elapsed Time: 0 days 9 hours 7 minutes 9 seconds

Transmit Statistics:
-----
Packets: 469077
Bytes: 32073302
Interrupts: 35
Transmit Errors: 0
Packets Dropped: 1

Receive Statistics:
-----
Packets: 32008
Bytes: 2406189
Interrupts: 30358
Receive Errors: 0
Packets Dropped: 1
Bad Packets: 0

Max Packets on S/W Transmit Queue: 23
S/W Transmit Queue Overflow: 0
Current S/W+H/W Transmit Queue Length: 0
```

- ☞ The output from **netstat -v** shows the statistics about each device driver being used. The important information that can be obtained from this command is if there is any value in the S/W Transmit Queue Overflow which would indicate a need for a larger transmit queue size. To increase the transmit queue use SMIT on the **chdev** command. Before making the change be sure to bring down the interface. This can be done with the **ifconfig <interface> down** command. Once the change has been made, bring it back up

## Display Dropped Packets

# netstat -D

Source	Ipkts	Opkts	Idrops	Odrops
ent_dev1	32536	469160	0	0
ent_dev0	1140894	2010	0	0
Devices Total	1173430	471170	0	0
ent_dd1	32536	469161	1	1
ent_dd0	1140894	2011	0	1
Drivers Total	1173430	471172	1	2

- ☞ The **-D** option of **netstat** displays the number of packets received (Ipkts), transmitted (Opkts) and dropped (Idrops, Odrops) in the communications subsystem.

## Trace Packets with the iptrace Daemon

- ☞ Records Internet packets received from configured interfaces
- ☞ Can be started as a command or under control of SRC
- ☞ Can be stopped either with the **kill** or **stopsrc** command
- ☞ Binary output sent to logfile specified at startup
- ☞ **ipreport** command used to format the trace file for viewing

### Examples of iptrace:

```
# iptrace -b -d ktaix16 -s ktaix15 /tmp/telnet.trace
# startsrc -s iptrace -a "-i en0 /home/ktuser1/iptrace.log"
# iptrace -e /tmp/iptrace.log
```

- ☞ The trace facility can be started by either executing **iptrace** as a command or by starting the daemon using **startsrc -s iptrace**. In order to stop **iptrace**, if it was started as a command then use the **kill** command. If it was started as a daemon use **stopsrc -s iptrace**.
- ☞ The first example starts **iptrace** as a command and says to trace all activity destined to interface **ktaix16** from interface **ktaix15** in both directions and put the output in **/tmp/telnet.trace**. The second example says to trace all activity on the en0 interface placing the output in **/home/ktuser/iptrace.log**.
- ☞ The third example starts **iptrace** in promiscuous mode. This allows the **iptrace** daemon to record all packets on the attached network. The **-d** option records packets headed for the destination host; **-s** records packets coming from the source network interface; and the **-b** indicates to record traffic in both directions, coming and going.

### Other options which can be used with iptrace:

- ☞ **A** do not include ARP packets
- ☞ **i** specifies an interface
- ☞ **P** specifies a protocol like TCP or IP
- ☞ **p** specifies a port like telnet or ftp (or a port number can be used)
- ☞ **e** specifies to trace packets in promiscuous mode (all traffic on the network the interface can see)

## View a Trace Report

```
↳ ipreport -n -s /tmp/telnet.trace > /tmp/report1
↳ pg /tmp/report1
```

```
# pg /tmp/report1
IPTRACE version: 2.0

Packet Number 1
ETH: ====( 60 bytes received on interface en0 )==== 21:56:03.895344392
ETH:      [ bc:ae:c5:53:8a:46 -> 00:20:35:b5:2b:c1 ]  type 806  (ARP)
ARP: hardware address format = 1 (ethernet)
ARP: protocol address format = 800 (IP)
ARP: address lengths ; hardware = 6, protocol = 4
ARP: arp operation = 1 (request)
ARP: source addresses: hw [bc:ae:c5:53:8a:46]
ARP:                  protocol [192.168.10.82]
ARP: target addresses: hw [00:20:35:b5:2b:c1]
ARP:                  protocol [192.168.10.15] (ktaix15)

Packet Number 2
ETH: ====( 60 bytes transmitted on interface en0 )==== 21:56:03.895352711
ETH:      [ 00:20:35:b5:2b:c1 -> bc:ae:c5:53:8a:46 ]  type 806  (ARP)
ARP: hardware address format = 1 (ethernet)
ARP: protocol address format = 800 (IP)
ARP: address lengths ; hardware = 6, protocol = 4
ARP: arp operation = 2 (reply)
ARP: source addresses: hw [00:20:35:b5:2b:c1]
ARP:                  protocol [192.168.10.15] (ktaix15)
```

## TCP/IP & Networking

### Special Internet Addresses:-

Class	Private start address	Private finish address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

- ↳ Several special addresses reserved by IANA:
- ↳ Loopback: 127.0.0.1
- ↳ Local network: host part all zeros (e.g. 129.33.151.0/24)
- ↳ Local broadcast: host part all ones (e.g. 129.33.151.255/24)
- ↳ Reserved for intranets not directly connected to the internet:
  - 10.0.0.0/8
  - 172.16..0.0/12
  - 192.168.0.0/16
- ↳ Multicast addresses: 224.0.0.1 and up

The IANA has reserved several addresses and address ranges for special purposes. The most important ones are listed here:

- ↳ The IP address **127.0.0.1** (in fact, the whole 127.0.0.0/8 network) is reserved for the loopback address.  
This loopback address is assigned to a virtual adapter which should be present in each and every TCP/IP host. It can be used, for instance, for TCP/IP client/server communication where both the client program and the server program reside on the same physical system, and that physical system does not have any real, physical adapters configured with a TCP/IP address. The loopback address is not routable over any TCP/IP network.
- ↳ Any IP address with the hostname part all zeros, such as 129.33.151.0/24, is reserved as identification for the network itself. It is not a valid IP address to be assigned to a host.
- ↳ Any IP address with the hostname part all ones, such as 129.33.151.255/24, is reserved as the local broadcast address. Data sent to this address is delivered to all systems on the local network.
- ↳ Addresses 224.0.0.1 and up are reserved for multicasts. A multicast address is a special address which is assigned on a per-application basis. All hosts that run a such an application configure themselves to listen to that specific address.

## Ports and Sockets:

- ↳ A **port** identifies the application on the host
- ↳ Server side ports are well-known and fixed
  - Stored in /etc/services
  - For example, telnet is 23, http is 80, ssh is 22.
- ↳ Client side ports are dynamic, > 1023
  - Every client connection uses a new port
- ↳ A **socket** is a combination of IP address, protocol and port and identifies an application uniquely on the network

## What does /etc/services contains?

### ↳ pg /etc/services

```
# Network services, Internet style
#
#                                0/tcp          # Reserved
#                                0/udp          # Reserved
tcpmux                         1/tcp          # TCP Port Service Multiplex
tcpmux                         1/udp          # TCP Port Service Multiplex
compressnet                     2/tcp          # Management Utility
compressnet                     2/udp          # Management Utility
compressnet                     3/tcp          # Compression Process
compressnet                     3/udp          # Compression Process
#
#                                4/tcp          # Unassigned
#                                4/udp          # Unassigned
rje                            5/tcp          # Remote Job Entry
rje                            5/udp          # Remote Job Entry
#
#                                6/tcp          # Unassigned
#                                6/udp          # Unassigned
echo                           7/tcp          # Echo
echo                           7/udp          # Echo
#
#                                8/tcp          # Unassigned
#                                8/udp          # Unassigned
discard                        9/tcp          # Discard
discard                        9/udp          # Discard
#
#                                10/tcp         # Unassigned
#                                10/udp         # Unassigned
systat                         11/tcp         # Active Users
systat                         11/udp         # Active Users
#
#                                12/tcp         # Unassigned
#                                12/udp         # Unassigned
daytime                        13/tcp         # Daytime (RFC 867)
daytime                        13/udp         # Daytime (RFC 867)
```

- ↳ The file /etc/services assigns common names to port numbers, and also functions as the list of “reserved” ports. In normal operations, a “server” (a program that is ready to receive connections) should be listening on the port that was assigned to it, as listed in

the /etc/services file. A “client” (a program that initiates a connection to a server) should contact the server on that port.

- For example, the telnet server (we'll talk about telnet and the telnet server further in unit 3) should start to listen to port 23, because that is the port that has been assigned to it through the /etc/services file. The telnet client on another host has access to the same /etc/services file, so it knows that the telnet server should be listening on port 23.

### Network Interfaces:

Adapter Prefix	Interface Prefix	Description
ent1	en	Ethernet
tok	et	IEEE 802.3
fddi	tr fi	Token – Ring Floppy disk drive (FDDI)

When each adapter or port is added, a logical device is created in the ODM such as:

- Ethernet adapters are ent0, ent1 and so forth
- Token-Ring adapters are tok0, tok1, and so forth

### Ethernet Network Interface:-

#### Standard Ethernet Version 2 (en0)



SA=Source Address

DA=Destination Address

TYPE=TCP/IP, DECnet, XNS

#### IEEE 802.3 (et0)



**To recognize interface card AIX uses three notations:**

- ↳ ent, en and et.

All are different and are described below and the sake of completeness I am using 0 at the end:

**ent0:**

- ↳ The notation ent0 is used to specify the hardware adapter. It has nothing to do with the TCP/IP address. The parameters associated with ent0 can be seen as below:
  - ↳ # lsattr -El ent0
  - ↳ It will show parameters related to card.
  - ↳ It shows adapter\_names, alt\_addr, auto\_recovery, backup\_adapter, hash\_mode, mode, netaddr, noloss\_failover, num\_retries, retry\_time, use\_alt\_addr, use\_jumbo\_frame.

**en0:**

- ↳ en0 represents the interface associated with hardware adapter ent0. The notation en0 is used for Standard Ethernet/inet). The TCP/IP address is associated with this interface.
- ↳ The parameters associated with en0 can be seen as below:
  - ↳ #lsattr -El en0
  - ↳ It'll shows all the parameters related with the interface en0 of the adapter ent0.
  - ↳ It shows alias4, alias6, arp, authority, broadcast=1500, mtu, netaddr, netaddr6, netmask, prefixlen, remmtu, rfc1323, security, state, tcp\_mssdfilt, tcp\_nodelay, tcp\_recvspace, tcp\_sendspace.
  - ↳ Rest everything is same except mtu(Maximum Transfer Unit) value. Which is 1500 as per the standard ethernet protocol.

**et0:**

- ↳ et0 represents the interface associated with hardware adapter ent0. The notation et0 is used for IEEE 802.3 Ethernet/inet). If you are using standard ethernet protocol then it will not have TCP/IP address.
- ↳ The parameters associated with et0 can be seen as below:
  - ↳ #lsattr -El et0
  - ↳ It'll shows all the parameters related with the interface et0 of the adapter ent0.
  - ↳ It shows alias4, alias6, arp, authority, broadcast, mtu=1492, netaddr, netaddr6, netmask, prefixlen, remmtu, rfc1323, security, state, tcp\_mssdfilt, tcp\_nodelay, tcp\_recvspace, tcp\_sendspace.
  - ↳ Note here as well that the MTU shown will be 1492 as per IEEE 802.3 standard. Rest all parameters will be same. Also, netaddr, netmask fields will be empty fr et0.

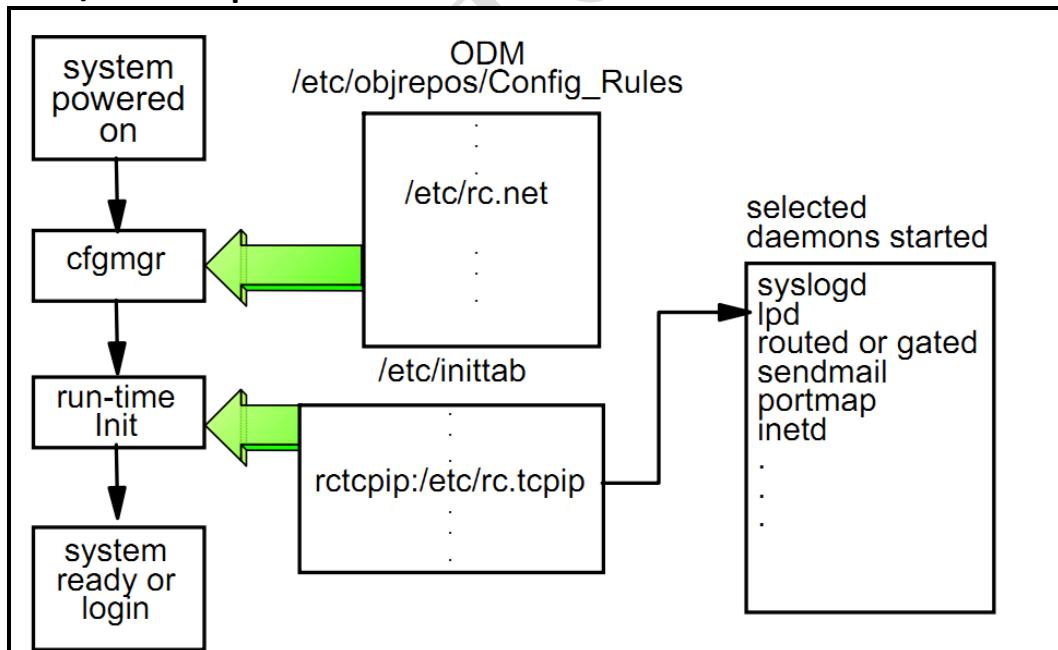
## Starting Daemons:

- ↳ The `/etc/rc.tcpip` file run at system startup can start the following TCP/IP daemons:

↳ <code>syslogd</code>	Logs error messages
↳ <code>portmap</code>	Port lookup facility
↳ <code>inetd</code>	Super daemon
↳ <code>named</code>	Domain nameserver
↳ <code>lpd</code>	Print server
↳ <code>routed</code> or <code>gated</code>	Dynamic routing
↳ <code>sendmail</code>	Mail
↳ <code>timed</code> , <code>xntpd</code>	Time daemons
↳ <code>rwhod</code>	Remote uptime and users
↳ <code>snmpd</code> , <code>dpid2</code>	SNMP daemons
↳ <code>dhcpcd</code> , <code>dhcprd</code> , <code>dhcpsd</code>	DHCP daemons
↳ <code>autoconf6</code> , <code>ndpd-host</code>	IPv6 daemons
↳ <code>mroute</code>	Multicast routing

- ↳ `/etc/rc.tcpip` assumes interfaces are brought up by `/etc/rc.net`. This shell script starts the TCP/IP daemons
- ↳ All these daemons can be started or stopped using the subsystem commands of the system resource controller. They are `stopsrc`, `startsrc` or `refresh`.

## TCP/IP Startup Flow:-



- When the system starts up, it reads out of the ODM whether to use **rc.net** (AIX default network configuration file) to initialize the network interfaces and set up routing.
- An entry in the **/etc/inittab** file is made at installation time to execute the **/etc/rc.tcpip** shellscript at system startup. The various uncommented daemons are started. The system is now ready to accept communication requests from various applications.

### Verifying Network Interfaces:

- The network interfaces can be verify by using the following commands
- #netstat -i and #ifconfig -a.

```
# netstat -i
Name    Mtu   Network      Address          Ipkts  Ierrs     Opkts  Oerrs   Coll
eno     1500  link#2      0.20.35.b5.2b.c1  3685    0        2540    0        0
eno     1500  192.168.10   ktaix15        3685    0        2540    0        0
lo0    16896  link#1      0.0.0.0          410     0        417     0        0
lo0    16896  127         loopback        410     0        417     0        0
lo0    16896  ::1          0.0.0.0          410     0        417     0        0
```

- The netstat command is used to display active sockets for each protocol, routing table information, or contents of a network data structure.
- The -i option shows the state of configured interfaces. This display format provides a table of cumulative statistics for: errors, collisions, and packets transferred. It provides the interface name, number, and address as well as the maximum transmission units (MTUs).
- The address field of the first entry for each interface provides the hardware address of the adapter.

```
# ifconfig -a
en0: flags=4e080863,80<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST,GROUPRT,64BIT,PSEG,CHAIN>
      inet 192.168.10.15 netmask 0xffffffff broadcast 192.168.10.255
lo0: flags=e08084b<UP,BROADCAST,LOOPBACK,RUNNING,SIMPLEX,MULTICAST,GROUPRT,64BIT>
      inet 127.0.0.1 netmask 0xffffffff broadcast 127.255.255.255
      inet6 ::1/0
          tcp_sendspace 131072 tcp_recvspace 131072 rfc1323 1
```

- #ifconfig -a displays interface attributes (for example, Up or Down), the network mask in Hex and the broadcast address for the network

## Verifying Address Resolution:

- ↳ To display and modify address resolution
- ↳ #arp -a

```
# arp -a
? (192.168.10.151) at 0:e0:c5:44:2:b6 [ethernet] stored in bucket 5

? (192.168.10.160) at 0:e0:c5:44:9:58 [ethernet] stored in bucket 14

? (192.168.10.161) at 0:e0:c5:44:9:d [ethernet] stored in bucket 15

ktaix16 (192.168.10.16) at 0:20:35:b5:6b:cd [ethernet] stored in bucket 19

? (192.168.10.167) at 0:e0:c5:44:9:5a [ethernet] stored in bucket 21

? (192.168.10.168) at 0:e0:c5:44:9:72 [ethernet] stored in bucket 22

? (192.168.10.82) at bc:ae:c5:53:8a:46 [ethernet] stored in bucket 85

bucket: 0 contains: 0 entries
bucket: 1 contains: 0 entries
bucket: 2 contains: 0 entries
bucket: 3 contains: 0 entries
bucket: 4 contains: 0 entries
bucket: 5 contains: 1 entries
```

## Verifying Open Ports:

- ↳ To display Open TCP/IP Application Ports
- ↳ #netstat -a -f inet

```
# netstat -a -f inet
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4      0      0  *.daytime             *.*                  LISTEN
tcp       0      0  *.ftp                 *.*                  LISTEN
tcp       0      0  *.telnet              *.*                  LISTEN
tcp4      0      0  *.smtp               *.*                  LISTEN
tcp4      0      0  *.time                *.*                  LISTEN
tcp4      0      0  *.sunrpc              *.*                  LISTEN
tcp4      0      0  *.smux                *.*                  LISTEN
tcp4      0     652  ktaix15.telnet       192.168.10.82.49171 ESTABLISHED
```

- ↳ The netstat -a -f inet command lists all open UDP and TCP ports, both the server ports (which are in the LISTEN state), and any client connections to or from any port (which are in the ESTABLISHED state).

## The **inetd** Daemon(Super Daemon):

Daemon used for low-usage applications such as:

- ↳ telnet
  - ↳ ftp
  - ↳ rexec
  - ↳ rsh
  - ↳ rcp
- 
- ↳ Opens ports on behalf of all these server programs and listens
  - ↳ If traffic arrives, starts the corresponding daemon
    - So the daemon is only running when needed, not 24/7
    - Saves CPU, memory, system startup time
    - But there is a startup delay for each connection
  - ↳ Configured with the /etc/inetd.conf file

### #/etc/inetd.conf

The **/etc/inetd.conf** file controls the behavior of the **inetd** daemon. It consists of seven columns:

```
##          Internet server configuration database
## service  socket  protocol  wait/   user      server      server program
## name     type        nowait    root      /usr/sbin/ftpd      ftpd
##                                     program    arguments
##
ftp      stream  tcp6      nowait   root      /usr/sbin/ftpd      ftpd
telnet   stream  tcp6      nowait   root      /usr/sbin/telnetd    telnetd -a
shell    stream  tcp6      nowait   root      /usr/sbin/rshd      rshd
#kshell  stream  tcp      nowait   root      /usr/sbin/krshd    krshd
login    stream  tcp6      nowait   root      /usr/sbin/rlogind   rlogind
#klogin  stream  tcp      nowait   root      /usr/sbin/krlogind krlogind
exec    stream  tcp6      nowait   root      /usr/sbin/rexecd   rexecd
#comsat dgram  udp       wait     root      /usr/sbin/comsat  comsat
```

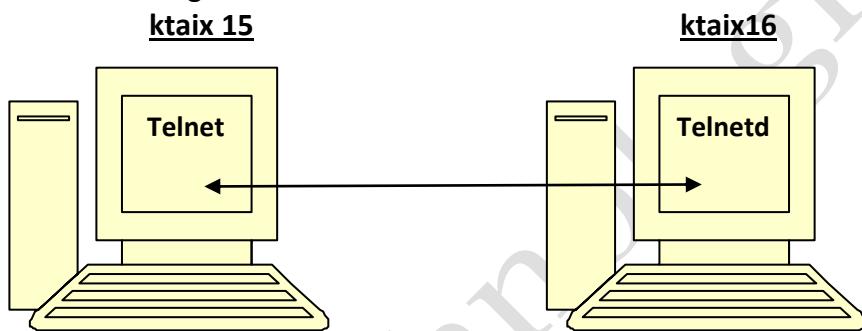
- ↳ The first column identifies the port number or port name that **inetd** should listen on. In most cases a port name is used, which is translated into a port number via the **etc/services** file
- ↳ Columns two through four identify the protocol to be used: TCP or UDP. Initially there were more protocols that were supported which would use a different combination of parameters. Today, TCP always needs “stream” and “nowait”.
- ↳ The **/usr/sbin/inetd** daemon provides Internet service management for a network.

This daemon reduces system load by invoking other daemons only when they are needed and by providing several simple Internet services internally without invoking other daemons.

- ↳ The **inetd** daemon is also known as the super daemon.
- ↳ It reads a file, **/etc/inetd.conf**, for the list of ports it needs to open. It opens these TCP and/or UDP ports and then sits idle waiting for traffic to arrive on any of these ports. When traffic arrives, it looks again at the **/etc/inetd.conf** file to see which daemon should be started. It then starts the daemon and lets the daemon handle the traffic.

### Telnet Command:-

- ↳ TELNET allows you to communicate to an Ethernet attached host from an Ethernet attached machine running TELNET.



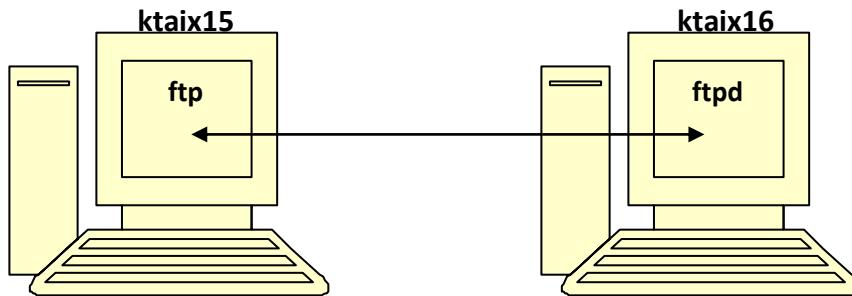
- ↳ Attempting to telnet from ktaix15 to ktaix16:
- ↳ Login into ktaix1 sys and type
- ↳ #telnet ktaix2 or ip address of ktaix2 (e.g. 192.168.10.16)

```
# telnet ktaix16
telnet (ktaix16)

AIX Version 5
(c) Copyrights by IBM and by others 1982, 2005.
login: kernel
kernel's Password:
/dev/pts/1: 3004-031 Password read timed out -- possible noise on po
Connection closed.
#
```

- ↳ The telnet command uses the TELNET protocol which allows remote login to other hosts. The server host must have the telnetd available.
- ↳ The syntax is telnet <hostname> [protocol].
- ↳ There is no automatic login capability with this command on AIX.
- ↳ The tn command performs the same function as the telnet command.
- ↳ The default escape sequence to go into telnet sub command mode on a session started using the tn command is <ctrl-t>.

## The ftp command:



- ↳ Attempting to ftp from ktaix15 to ktaix16
- ↳ Login into ktaix15 and
- ↳ # ftp ktaix16 or Ip address of ktaix16 (e.g. 192.168.10.16)

```
# ftp ktaix16
Connected to ktaix16.
220 ktaix16 FTP server (Version 4.2 Fri Oct 7 19:22:01 CDT 2005) ready.
Name (ktaix16:root): root
331 Password required for root.
Password:
230-Last unsuccessful login: Wed May 25 11:49:56 CDT 2011 on /dev/pts/1 fro
.168.10.168
230-Last login: Wed May 25 12:50:16 CDT 2011 on ftp from ::ffff:192.168.10.
230 User root logged in.
ftp> put KernelTech
200 PORT command successful.
150 Opening data connection for KernelTech.
226 Transfer complete.
24 bytes sent in 0.001807 seconds (12.97 Kbytes/s)
local: KernelTech remote: KernelTech
ftp> get KernelTech
200 PORT command successful.
150 Opening data connection for KernelTech (23 bytes).
226 Transfer complete.
24 bytes received in 0.001394 seconds (16.81 Kbytes/s)
local: KernelTech remote: KernelTech
ftp> 
ftp> bye
221 Goodbye.
#
```

- ↳ The above screen shows how to share a file between two servers through ftp

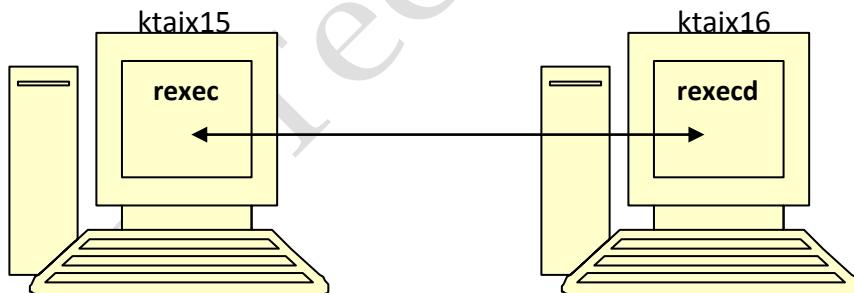
## The **/etc/ftpusers** File:

- File created by root on the server (remote) machine that denies access to certain users from other hosts from using ftp

<b>Ktaix15(Server)</b>  # pg /etc/passwd kernel:!:202:1::/home/kernel:/usr/bin/ksh  # cat /etc/ftpusers kernel	<b>ktaix16(Client)</b> \$ whoami kernel  \$ ftp ktaix15 530 User kernel access denied. Login failed.
--	--

- User names listed in the **/etc/ftpusers** file on the server must also appear in the server's **/etc/passwd** file.
- /etc/ftpusers** is a list of client users who do not have permission to **ftp** into the server's system. The **ftpd** daemon on the server does not allow access to the users names listed in this file.
- /etc/ftpusers** can be built with **vi**, through **smit ftpusers** or by using the **ruser** command.

## The rexec Command:



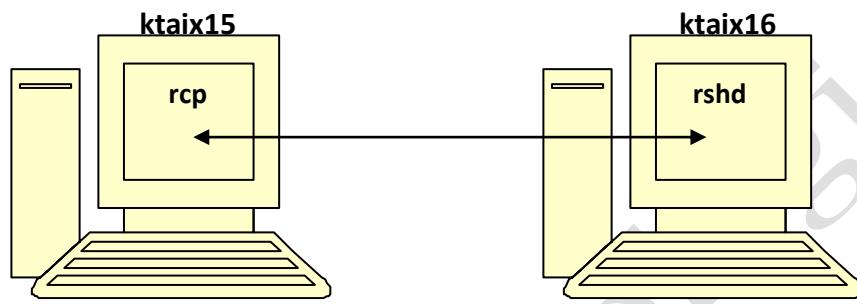
```
# rexec ktaix16 date
Name (ktaix16:root): kernel
Password (ktaix16:kernel):
Wed May 25 13:46:06 CDT 2011
```

Along with **date** command, try some other command like **hostname**, **lspv**, etc and see the output.

- The **reexec** command executes a command on the specified server machine. The host parameter specifies the name of the host where the command is to be executed. The command parameter specifies the command, including any flags or parameters, to be executed on the server host (ktaix15).
- The **reexec** command provides an automatic login feature by checking for a **\$HOME/.netrc** file that contains the user name and password to use at the server host. If such an entry is not found, **reexec** prompts for a valid user name and password for the server host.

- ☞ The **rexec** command does not recognize a macdef entry in the **.netrc** file. If a macdef entry exists, the **rexec** command does not fail, but the user gets an error message about unknown options. **rexec** cannot handle commands that use a full screen such as **vi** or graphical applications. **rexec** command does support interactive command processing.

### **The **rcp** command:**



#### **Copying a file using **rcp****

- ☞ Before doing rcp check whether .rhosts file under / (root) exists or not. If not create a new .rhosts file using vi editor and enter the name of remote hosts which will be connecting to this server to copy a file.
- ☞ Change the permission of .rhosts file to 700 using #chmod 700 .rhosts
- ☞ Create a file in 1<sup>st</sup> server i.e. ktaix15 say ktfile
- ☞ Copy the above created file using rcp with the following commands  
**#rcp ktfile ktaix16:/ktfile1** (where ktfile1 is the new name of the ktfile1)

**#rcp ktfile user@ktaix16:/ktfile1** (use this option to copy a file as a user)

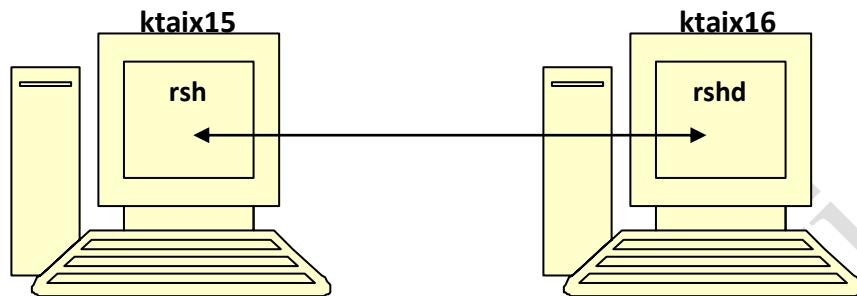
#### **To copy a directory from one server to other**

**#rcp -pr ktaix15:/ktdir ktaix16/ktdir1**

- ☞ The **rcp** command is used to copy one or more files between a client host and a server host.
- ☞ When copying files to or from a server host, any server file or directory name must be prefixed by the server host name and a colon. Client file and directory names do not need to have a host specified.
- ☞ **-p** preserves the modification times and modes of the source file.
- ☞ **-r** recursively copies, for directories only, each file and subdirectory in the source directory into the destination directory.

- If the user name where the file is to be copied to or from is different from the user name issuing the command, the server user name precedes the server host name and is separated from it by an @ sign.

### The rsh Command:

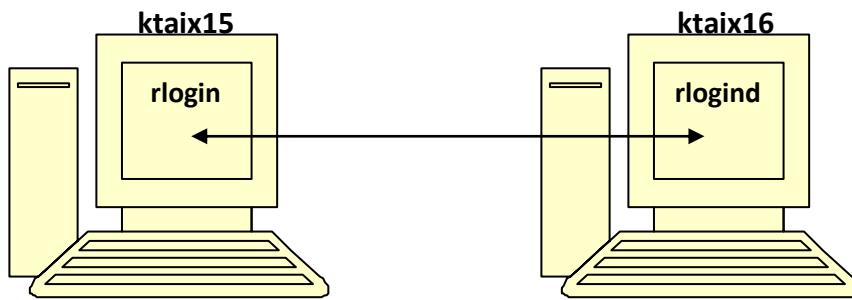


```
# rsh ktaix16 date
Wed May 25 15:58:28 CDT 2011
# rsh ktaix16 hostname
ktaix16
# rsh ktaix16 cal
      May 2011
Sun Mon Tue Wed Thu Fri Sat
  1   2   3   4   5   6   7
  8   9   10  11  12  13  14
 15  16  17  18  19  20  21
 22  23  24  25  26  27  28
 29  30  31
```

- rsh command executes the specified command on the server host.
- If you do not want to execute a command on the server as your logged in client user name, the -l is used followed by another user name.
- rsh executed without a command argument acts as an rlogin and logs the user in. rcmd is a user attribute to control the r- command execution. It accepts the following values:

allow	Allows users to execute r- command
deny	Denies user to execute r- commands. This is the same as "tty=ALL, !RSH".
hostlogincontrol	Specifies that the ability of remote command execute is under control of the hotsallowedlogin and hostdeniedlogin attributes. These attributes control the user login.

## The rlogin Command:



### Logging as root user through rlogin

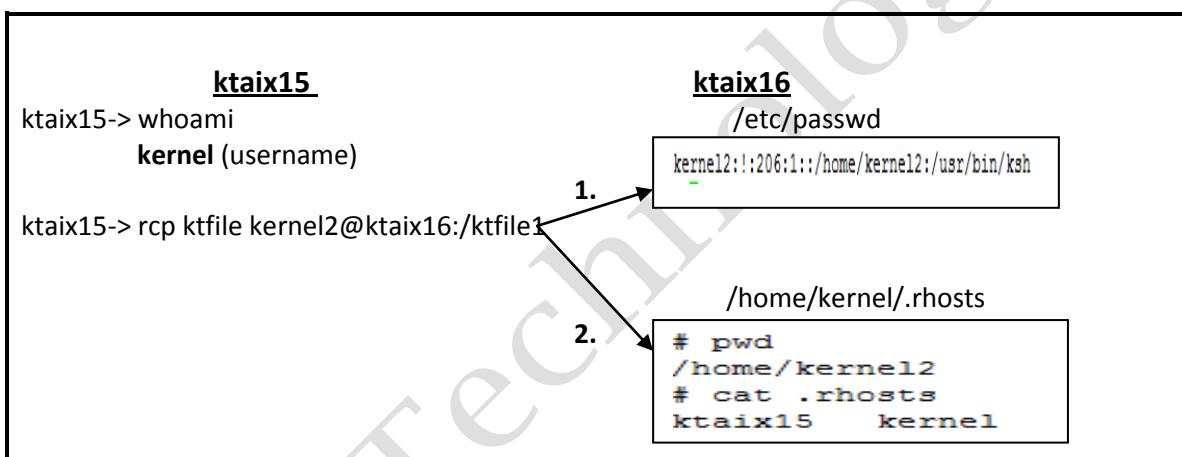
```
# whoami
root
# rlogin ktaix16
*****
*                                                 *
*                                                 *
*   Welcome to AIX Version 5.3!
*                                                 *
*                                                 *
*   Please see the README file in /usr/lpp/bos for information pertinent to
*   this release of the AIX Operating System.
*                                                 *
*                                                 *
*****Last unsuccessful login: Wed May 25 14:20:33 CDT 2011 on /dev/pts/1 from 192.168
.10.161
Last login: Wed May 25 16:22:35 CDT 2011 on /dev/pts/3
#
#
```

### Logging as kernel user using rlogin.

```
# rlogin ktaix16 -l kernel
kernel's Password:
*****
*                                                 *
*                                                 *
*   Welcome to AIX Version 5.3!
*                                                 *
*                                                 *
*   Please see the README file in /usr/lpp/bos for information pertinent to
*   this release of the AIX Operating System.
*                                                 *
*                                                 *
*****1 unsuccessful login attempt since last login.
Last unsuccessful login: Wed May 25 16:26:01 CDT 2011 on /dev/pts/3
Last login: Wed May 25 16:22:16 CDT 2011 on /dev/pts/3
#
$
```

- The **rlogin** command is served by the **rlogind** daemon on the server. The **rlogin** command performs a remote login on behalf of the user. If the user wants to log in using a user name other than the one he/she is currently logged in as, the **-l** option is used along with the new user name.
- A client user name that is not properly authorized is prompted for a login and password. Therefore, if a user does have a valid user name and password in the server's **/etc/passwd** file, they are able to log in when prompted. Authorization consists of several system administration tasks, like port checking and daily usage allowances.
- To close the **rlogin** session, type **logout** or **exit**.

## The \$HOME/.rhosts

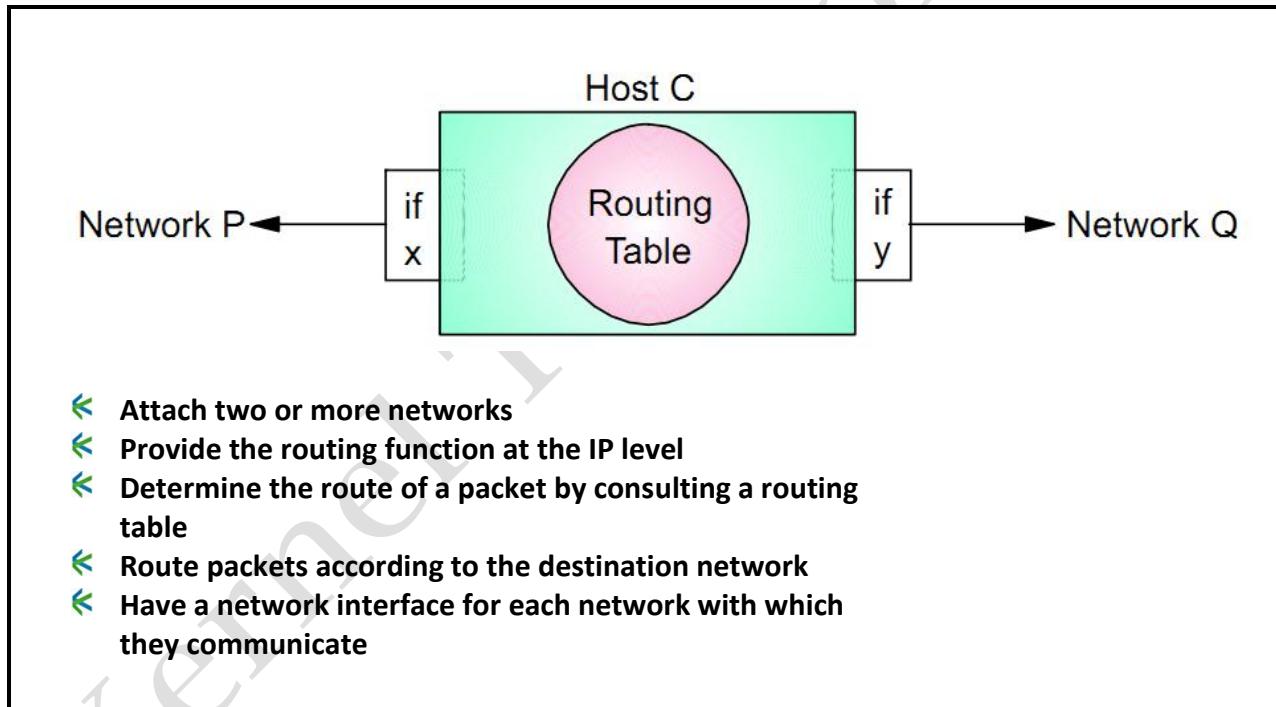


- Defines a list of client users who are not required to supply a login password when they execute **rcp**, **rlogin** and **rsh** using a server user account
- If an **/etc/hosts.equiv** file does not exist on ktaix16, or does exist but does not authorize the user on the remote system, then the **\$HOME/.rhosts** file is looked at for user authentication. In particular, ktaix16 looks at the **.rhosts** file in the home directory of the user under whom the command is to run.
- In the above example, **kernel** wants to remote copy **ktfile** to **kernel2**'s home directory on ktaix16 and rename it **ktfile1**. The user name **kernel2** is checked. Even though **kernel2** has an entry in **/etc/passwd**, the command is not authorized since the entry for **ktaix15** in **/etc/hosts.equiv** authorized users on **ktaix15** only to run as the same ID on ktaix16. Instead, the **rshd** on ktaix16 looks for an entry in the **.rhosts** in **kernel2**'s home directory. **Kernel2** has given **kernel1** on **ktaix15** permission to perform remote copies to its directory.
- The **\$HOME/.rhosts** is a hidden file in a server host user's directory.

## ROUTING

- ↳ A route defines a path for sending packets through the Internet to an address on another network. A route does not define the complete path, only the path from a host to a gateway (router) that can then forward packets on to either the destination or to another gateway.
- ↳ The term routing refers to the process of choosing a path over which to send packets, and router refers to any computer making such a choice.
- ↳ Routing is performed by the IP layer. IP routers are used to connect different networks. No daemons are necessary to make routing occur on a host.

### Routers for TCP/IP



- ↳ Routers connect two or more networks and provide routing functions. The term gateway in this context is used interchangeably with router.
- ↳ Some routers route at the network interface level or the physical level.
- ↳ Gateways route at the network level. Gateways receive IP datagrams from other gateways for delivery to hosts on the local network and route IP datagrams from one network to another. Gateways periodically verify their network connections through interface status messages.
- ↳ Gateways route packets according to the destination network. The destination network then takes care of sending the packet to the destination host.

## Viewing the Routing Table: netstat -rn

```
# netstat -rn
Routing tables
Destination      Gateway          Flags   Refs   Use     If     Exp Groups
Route Tree for Protocol Family 2 (Internet):
127.0.0.1        127.0.0.1       U        4      162  lo0      -      -      -
192.168.10.0     192.168.10.15  UHSb     0      0  en0      -      -      -      =>
192.168.10.15    192.168.10.15  U        1      56  en0      -      -      -
192.168.10.15    127.0.0.1       UGHS     7      126  lo0      -      -      -
192.168.10.255   192.168.10.15  UHSb     0      4  en0      -      -      -
Route Tree for Protocol Family 24 (Internet v6):
::1              ::1             UH      0      0  lo0      -      -      -
```

- ↳ The routing table format indicates:

- ↳ **Destination**

Address of destination (host or network). If the destination is a network, the subnet mask is indicated by “/XX”, where XX is the number of bits in the network portion of the address.

- ↳ **Gateway**

Address of the next hop gateway.

- ↳ **Flags**

**U**=up

**H**=route is to a host

**G**=route is to a gateway

(See the man page for complete list of flags.)

- ↳ **Refs**

The current number of active users for the route.

- ↳ **Use**

A count of the number of packets sent using that route

- ↳ **If**

The network interface used for the route.

- ↳ **PMTU**

Gives the Path Maximum Transmission Unit for the route. Prior to AIX 5L V5.3, PMTU values are kept in the routing table. Starting in AIX 5L V5.3, PMTU values are kept in a separate PMTU table and are not displayed with netstat -r.

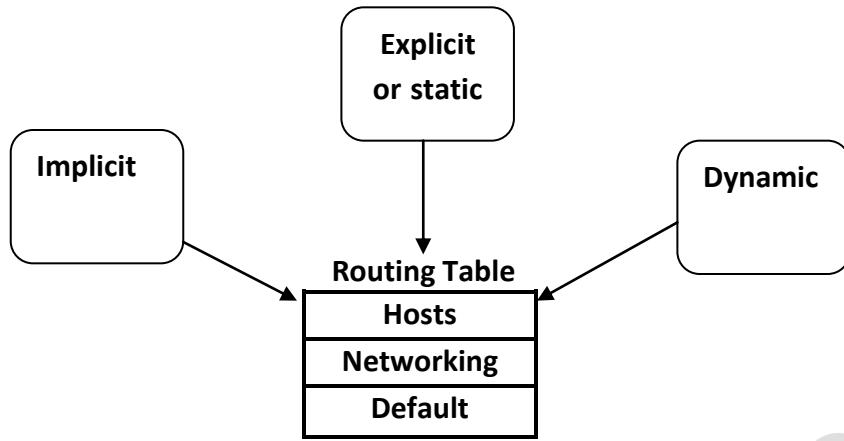
- ↳ **Exp**

Displays the time (in minutes) remaining before the route expires (for cloned routes and ICMP redirect routes).

- ↳ **groups**

Provides a list of group IDs associated with that route.

## Establishing Routes



## Kernel routing table

- Routes are defined in the kernel routing table, which can hold up to 32 route definitions. These route definitions include information on networks reachable from the local host, gateways that can be used to reach remote networks, and the hop count (or distance metric) to those networks.

### Implicit routes

- The implicit method is performed when you configure an interface.

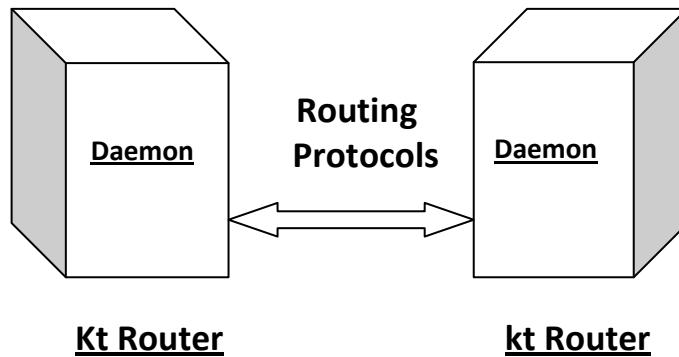
### Explicit routes

- Explicit routes are added by the network administrator.

### Dynamic routes

- Dynamic routes are created by ICMP redirect messages in a static routing environment. ICMP sends redirect messages when a better route to a host is noted. ICMP redirects are only generated by routers and are intended only for use by hosts.
- Additional dynamic routes are established when a new Path Maximum Transmission Unit (PMTU) is discovered. These are called cloned routes. The purpose of cloned routes is to provide a way to identify a maximum transmission unit for a specific route or path (path MTU).

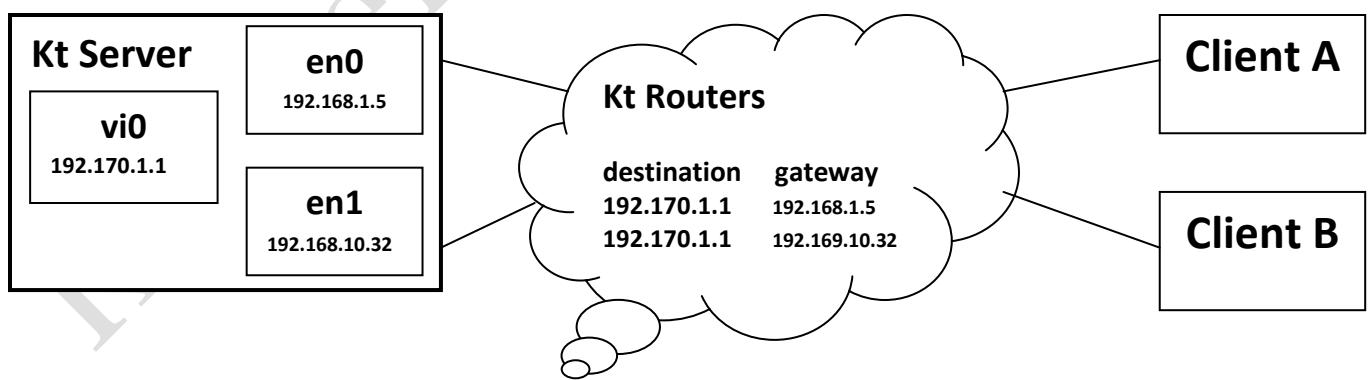
## Dynamic Routing



- ☞ With Dynamic Routing, the routers talk to each other to exchange routing information
- ☞ This should configure all routing tables properly, automatically
- ☞ Implemented through "ICMP Redirects" and formal "routing protocols"

## Virtual IP Address (VIPA)

- ☞ AIX offers Virtual IP Addresses to overcome application availability problems. When a network becomes inaccessible or the network interface fails, a different network interface can be used by modifying the routing table. If the rerouting occurs fast enough, then the TCP/IP sessions are not lost.



- ☞ Outgoing packets are routed via physical interfaces (en0 & en1) based on the destination and the routing table in the server
- ☞ Source address will be set to the VIPA address (vi0: 192.170.1.1)
- ☞ Replies will be directed to the VIPA address
- ☞ Clients and any routers must be configured with routes to the VIPA address

### Advantages of VIPA:

- ↳ Application will be available all the time
- ↳ If one physical interface or network path fails, traffic is routed to the other physical interface
- ↳ VIPA interface can be brought up or down without affecting physical interfaces

### Creating a Virtual IP Address:

#smi mkinetvi

```
Add a Virtual IP Address Interface

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
* INTERNET ADDRESS (dotted decimal) [192.170.1.1]
  Network MASK (hexadecimal or dotted decimal) [255.255.255.0]
* Network Interface [vi0]
* ACTIVATE the Interface after Creating it? yes
  Network Interface(s) using this VIPA [en0,en1]
```

### Using ifconfig

- ↳ ifconfig only changes the current interface device in memory. If you want to make the change permanent (update the ODM), you must use SMIT or mkdev.
- ↳ The ifconfig command can be invoked in one of the following ways using these options:
  - ↳ To configure a list of interfaces to use a particular VIPA:  
# ifconfig vi0 192.170.1.1 vipa\_iflist en0,en1
  - ↳ To remove a list of interfaces that are configured to use VIPA:  
# ifconfig vi0 192.170.1.1 -vipa\_iflist en0,en1
- ↳ Running the ifconfig vi0 command produces the following status:  
[# ifconfig vi0](#)

### The no Command:

- ↳ The **no** command is used to set or display network tuning parameters (tunables) for the current value or reboot value.
- ↳ Check man pages for more no options (man no)

Syntax:

```
# no
Usage:  no -h [tunable] | {[-F] -L [tunable]} | {[-F] -x [tunable]}
        no [-p|-r] (-a [-F] | {-o tunable})
        no [-p|-r] [-y] (-D | ({-d tunable} {-o tunable=value}))
```

<b>Flag</b>	<b>Description</b>
<b>-p</b>	Permanent: makes the change to both current and reboot value
<b>-r</b>	Reboot: makes the change on the next reboot
<b>-o</b>	Displays or sets individual parameters. Without -p or -r, only current value is shown or changed
<b>-d</b>	Resets individual tunable to default value
<b>-D</b>	Resets all tunables to default values
<b>-a</b>	Displays all parameters
<b>-h</b>	Displays help information for a tunable
<b>-L</b>	Lists attributes of one or all tunables; includes: current value, default value, value to be set at next reboot, minimum possible value, maximum possible value, unit, type, and dependencies

## **Managing the Tunables:**

- ↳ **Syntax for tuning commands**
  - ↳ no (network tuning)
  - ↳ vmo (memory tuning)
  - ↳ schedo (CPU tuning)
  - ↳ ioo (I/O tuning)
  - ↳ nfso (NFS tuning)
- ↳ **/etc/tunables contains two stanza files and a log file**
  - ↳ nextboot
  - ↳ lastboot
  - ↳ lastboot.log
- ↳ **File control commands for tunables**
  - ↳ tuncheck
  - ↳ tunrestore
  - ↳ tunsave
  - ↳ tundefault
- ↳ **/etc/tunables**

This directory three files that are used with the tunable commands:

- ↳ **/etc/tunables/nextboot**
- When you change a tunable value for the next boot, an entry is made in this file. At boot time, tunrestore -R is run from /etc/inittab. All tunables that are not already set to the value defined in the nextboot file are modified. Tunables not listed in the nextboot file are forced to their default value. All actions, warnings and errors are logged into /etc/tunables/lastboot.log.

#### **/etc/tunables/lastboot**

This file contains a record of the tunables that were set during the last boot. It lists all the tunables with numerical values. The values representing default values are marked with the comment DEFAULT VALUE.

#### **/etc/tunables/lastboot.log**

This file contains a record of all actions taken by **tunrestore -R** at boot time.

## **File control commands**

There are four commands to manage the files associated with the tunable commands:

#### **tuncheck**

The tuncheck command validates a tunable file. All tunables listed in the specified file are checked for range and dependencies. If a problem is detected, a warning is issued.

#### **tunrestore**

The tunrestore command restores all tunable parameters values stored in a file. **tunrestore -R** can only be called from inittab

#### **tunsave**

The tunsave command saves the current state of tunable parameters (in memory) to a file.

#### **tunsave**

The tunsave command saves the current state of tunable parameters (in memory) to a file.

**Note:** There are some flags to use above commands Pl refer man pages for the usage of flags with the commands.

## **Managing Tunables**

### **Syntax for tuning commands**

-  **no** (network tuning)
-  **vmo** (memory tuning)
-  **schedo** (CPU tuning)
-  **ioo** (I/O tuning) **nfs0** (NFS tuning)

**/etc/tunables** contains two stanza files and a log file

```
# cd /etc/tunables
# ls
lastboot      lastboot.log   nextboot
```

## File control commands for tunables

- ↳ tuncheck
- ↳ tunrestore
- ↳ tunsave
- ↳ tundefault

## /etc/tunables

In this directory there are three files which are used by the tunables commands

### ↳ /etc/tunables/nextboot

When you change a tunable value for the next boot, an entry is made in this file. At boot time, tunrestore -R is run from /etc/inittab. All tunables that are not already set to the value defined in the nextboot file are modified. Tunables not listed in the nextboot file are forced to their default value. All actions, warnings and errors are logged into /etc/tunables/lastboot.log.

### ↳ /etc/tunables/lastboot

This file contains a record of the tunables that were set during the last boot. It lists all the tunables with numerical values. The values representing default values are marked with the comment DEFAULT VALUE.

### ↳ /etc/tunables/lastboot.log

This file contains a record of all actions taken by tunrestore -R at boot time.

## Lab Activities:

### 1. Raise a ticket to Assign IP address and subnet mask on a card and close ticket.

- ↳ #smitty mktcpip → select interface (say en0 or en1) and change the following

```
Minimum Configuration & Startup

To Delete existing configuration data, please use Further Configuration menus

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
[kt2a]
[192.168.10.15]
[255.255.255.0]
en1

* HOSTNAME
* Internet ADDRESS (dotted decimal)
Network MASK (dotted decimal)
* Network INTERFACE
NAMESERVER
    Internet ADDRESS (dotted decimal)
    DOMAIN Name
Default Gateway
    Address (dotted decimal or symbolic name)
    Cost
    Do Active Dead Gateway Detection?
Your CABLE Type
START Now
```

⚡ Raise a ticket to Change IP address and subnet mask and close ticket.  
#smitty chinet, select the interface and change the following

```
Change / Show a Standard Ethernet Interface

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
Network Interface Name          en0
INTERNET ADDRESS (dotted decimal) [192.168.10.18]
Network MASK (hexadecimal or dotted decimal) [255.255.255.0]
Current STATE                   up
Use Address Resolution Protocol (ARP)? yes
```

1. Configure gateway.

⚡ #route add -net 10.1.1.0 192.168.10.1

2. Remove gateway

⚡ #route delete -net 10.1.1.0 192.168.10.1

3. Check Routing Table.

⚡ #netstat -nr

```
# netstat -nr
Routing tables
Destination      Gateway          Flags   Refs      Use     If     Exp Groups
Destination      Gateway          Flags   Refs      Use     If     Exp Groups

Route Tree for Protocol Family 2 (Internet):
127/8           127.0.0.1        U        1       164    lo0      -      -      -
192.168.10.0    192.168.10.15   UHSb     0        0    en0      -      -      -=>
192.168.10/24   192.168.10.15   U        5    2236755  en0      -      -      -
192.168.10.15   127.0.0.1        UGHS     9       134    lo0      -      -      -
192.168.10.255  192.168.10.15   UHSb     0        4    en0      -      -      -

Route Tree for Protocol Family 24 (Internet v6):
::1            ::1              UH      0        0    lo0      -      -      -
```

#### Other routing commands:

#route add -net → to add a network route to the routing table with subnetmask

#route delete → to delete the route set earlier as mention above in Q.no 4

#route -f → to clear the routing table of all routes except those created implicitly. Also **route flush** does the same thing (Be careful while using this option it can harm your routing configuration)

4. Update “/etc/hosts” file.

```
↳ #vi /etc/hosts  
192.168.10.30 ktaix30  
  
192.168.10.31 ktaix31
```

Now save and quit from the file.

5. Configure DNS client.

```
↳ Here we need to give DNS server details in “/etc/resolv.conf” file as given below  
#vi /etc/resolv.conf  
domain kts.com  
Nameserver 192.168.10.5
```

Now save and quit from the file.

6. Configure Ether Channel (Link aggregation & NIB)

↳ **Link Aggregation.**

```
#smitty etherchannel
```

```
EtherChannel / IEEE 802.3ad Link Aggregation  
  
Move cursor to desired item and press Enter.  
  
List All EtherChannels / Link Aggregations  
Add An EtherChannel / Link Aggregation  
Change / Show Characteristics of an EtherChannel / Link Aggregation  
Remove An EtherChannel / Link Aggregation  
Force A Failover In An EtherChannel / Link Aggregation
```

Select **ent2** and **ent3** adapters & press enter. Now logical adapter **ent4** adapter will be created.

Then assign IP for logical adapter **ent4**. (Refer to question no.1)

7. Remove Ether Channel.

```
↳ Before removing an etherchannel, first down and detach the logical interface en4 then delete the adapter ent4.  
#ifconfig en4 down detach
```

```
#rmdev -dl ent4.
```

8. Now configure NIB(Network Interface Backup)

```
#smitty etherchannel
```

```
EtherChannel / IEEE 802.3ad Link Aggregation

Move cursor to desired item and press Enter.

List All EtherChannels / Link Aggregations
Add An EtherChannel / Link Aggregation
Change / Show Characteristics of an EtherChannel / Link Aggregation
Remove An EtherChannel / Link Aggregation
Force A Failover In An EtherChannel / Link Aggregation
```

Now select one adapter which is free (say **ent1**), after selecting **ent1** press enter, now again select **ent2** as a **backup adapter** as shown below.

```
Add An EtherChannel / Link Aggregation

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
EtherChannel / Link Aggregation Adapters          ent1
Enable Alternate Address                         no
Alternate Address                                []
Enable Gigabit Ethernet Jumbo Frames            no
Mode                                              standard
Hash Mode                                         default
Backup Adapter                                 ent2
    Automatically Recover to Main Channel        yes
    Perform Lossless Failover After Ping Failure yes
Internet Address to Ping                        []
Number of Retries                             []
Retry Timeout (sec)                            []
```

Now press enter a logical adapter **ent3** will be created.

That's it now Assing IP to adapter **ent3** (Refer to question no.1)

9. Do failover in Ether Channel.

```
#smitty etherchannel.
```

```
EtherChannel / IEEE 802.3ad Link Aggregation

Move cursor to desired item and press Enter.

List All EtherChannels / Link Aggregations
Add An EtherChannel / Link Aggregation
Change / Show Characteristics of an EtherChannel / Link Aggregation
Remove An EtherChannel / Link Aggregation
Force A Failover In An EtherChannel / Link Aggregation
```

After doing a fail over, to check which adapter is active, type:

```
#entstat -d ent3 | grep -i active
```

```
#lsattr -El ent3 → to check attributes of etherchannel i.e. ent3
```

10. How to force a failover of an EtherChannel ?

```
↳ # /usr/lib/methods/ethchan_config -f Etherchannel_Device
```

11. How to add a backup adapter to an existing etherchannel device ?

```
↳ # /usr/lib/methods/ethchan_config -a -b Etherchannel_Device Ethernet_Adapter
```

12. How to change the address to ping attribute of an EtherChannel ?

```
↳ # /usr/lib/methods/ethchan_config -c Etherchannel_Device netaddr  
New_Ping_IP_Addr
```

13. Raise a ticket to open port services in server and do the job and close ticket.

↳ **To check port services go to**

```
#pg /etc/services
```

**To check port listening,**

```
#netstat -Aan | grep -i 23 (23 is the port no for telnet)
```

```
# netstat -Aan | grep -i 23  
f100020000b8d398 tcp      0      0  *.23          *.*          LISTEN  
f100020000b82398 tcp4     0      0  *.199         *.*          LISTEN  
f100020000dd0398 tcp4     0      2  192.168.10.15.23  192.168.10.81.5158 ESTABLISHED  
f100020000d54b98 tcp4     0      0  192.168.10.15.23  192.168.10.165.550 ESTABLISHED  
f100020000d3b398 tcp4     0      0  192.168.10.15.23  192.168.10.167.485 ESTABLISHED
```

**To check link status,**

```
#entstat -d ent0 |grep -i link
```

```
#netstat -v ent0 | grep -i link
```

14. Start SRC.

↳ ex: #startsrc -g nfs (g stands for group, s stands for subsystem)

```
#startsrc -s qdaemon
```

```
#startsrc -s tcPIP
```

```
#startsrc -s inetd
```

15. How to start and stop the services.

- ↳ ex: #startsrc -g nfs  
#stopsrc -g nfs

16. Modify “inetd.conf”.

- ↳ #vi /etc/inetd.conf  
If you want to stop a service, comment a service i.e (just put '#' at begining of the line) which is shown below.

```
## service socket protocol wait/ user      server      server program
## name      type           nowait      program      arguments
##
ftp      stream  tcp6    nowait   root     /usr/sbin/ftpd      ftpd
#telnet   stream  tcp6    nowait   root     /usr/sbin/telnetd    telnetd -a
shell    stream  tcp6    nowait   root     /usr/sbin/rshd      rshd
#kshell   stream  tcp     nowait   root     /usr/sbin/krshd    krshd
login    stream  tcp6    nowait   root     /usr/sbin/rlogind   rlogind
#klogin   stream  tcp     nowait   root     /usr/sbin/krlogind krlogind
exec     stream  tcp6    nowait   root     /usr/sbin/rexecd   rexecd
#comsat   dgram   udp     wait     root     /usr/sbin/comsat   comsat
#uucp    stream  tcp     nowait   root     /usr/sbin/uucpd    uucpd
#bootps  dgram   udp     wait     root     /usr/sbin/bootpd   bootpd /etc/bootptab
```

Then refresh the service to take effect

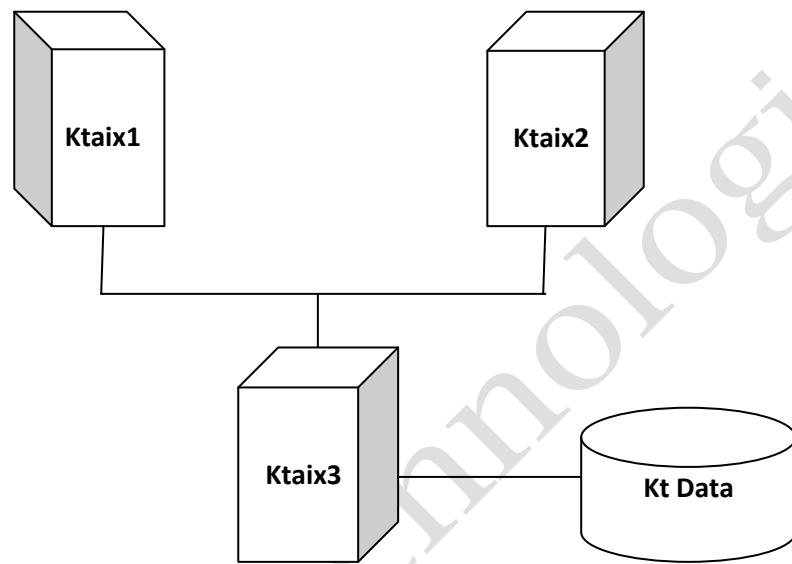
```
#refresh -s inetd
```

17. Enable ftp & other services.

- ↳ Here /etc/inetd.conf file contains the entire ftp and other services.  
#startsrc -s inetd  
  
#refresh -s inetd  
  
#stopsrc -s inetd

## NETWORK FILE SYSTEM (NFS)

### Sharing Data on a Network



On a TCP/IP network, data can be shared as follows:

- ↳ Log in remotely with **rlogin**, **telnet** and **rsh**
- ↳ Transfer files with **ftp** and **rcp**
- ↳ Remote execution with **rexec** and **rsh**

### Network File Systems (NFS)

- ↳ Network File System (NFS) is a facility for sharing files in a heterogeneous environment of machines, operating systems, and networks.
- ↳ NFS is supported over TCP/IP on Local Area Networks. Although NFS functions over any TCP/IP network, it requires the speed of local area networks to perform file sharing with acceptable performance.
- ↳ Sharing is accomplished by building a view of a remote file system, then reading or writing across the network to the files. Only one copy of a file exists on the NFS network, thus maximizing file storage availability.

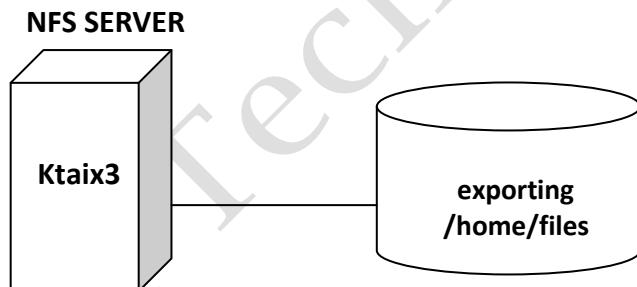
- ↳ The NFS function is built into the kernel of the operating system so it is transparent to applications and users.
- ↳ NFS provides a Client/Server relationship where the server stores files and provides administration services and the client requests these services.
- ↳ AIX supports NFS Version 4 as well as NFS Version 2 and 3 protocols.
- ↳ One or more systems can be configured to provide a range of server functions for a range of client systems. A system can play both the client and server role with other systems, providing some services and requesting others.

### **Stateless:**

The NFS protocol is stateless:

- ↳ Server does not remember anything about transactions
- ↳ Client is not notified when server is down
- ↳ No system recovery procedures

NFS Version 4 is stateful



Exporting = Lists the directories on the NFS server that clients can access.

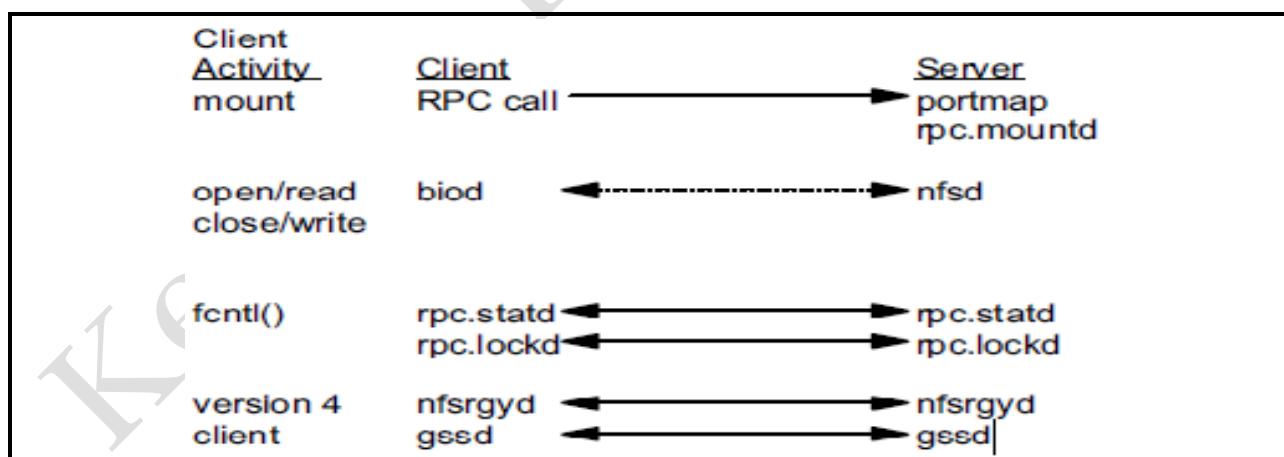
- ↳ NFS servers export file systems or directories to NFS clients. Thus, the server can control which areas of its disks are accessible to clients. Exporting a directory makes the directory available for use by other NFS client hosts on the network.

## Mount Table

#	mount node	mounted	mounted over	vfs	date	options
	/dev/hd4		/	jfs2	May 31 20:41	rw,log=/dev/hd8
	/dev/hd2		/usr	jfs2	May 31 20:41	rw,log=/dev/hd8
	/dev/hd9var		/var	jfs2	May 31 20:42	rw,log=/dev/hd8
	/dev/hd3		/tmp	jfs2	May 31 20:42	rw,log=/dev/hd8
	/dev/hd1		/home	jfs2	May 31 20:42	rw,log=/dev/hd8
	/proc		/proc	procfs	May 31 20:42	rw
	/dev/hd10opt		/opt	jfs2	May 31 20:42	rw,log=/dev/hd8
	/dev/fslv00		/share	jfs2	May 31 20:42	rw,log=/dev/hd8
	ktaix3	/home/files	/home/mntpt	nfs3	Jun 01 00:39	rw

- ☞ The host name in the **node** column is the name of the server.
- ☞ **mounted** is the server's exported directory where the data physically resides.
- ☞ **mounted over** is the client's local mount point to which the server's exported directory gets mounted to allow users to access the remote data.
- ☞ **vfs** states that the virtual file system type for the remote mount is nfs rather than jfs.  
**date** is the date mounted.
- ☞ **options** are the attributes with which the file system was mounted.

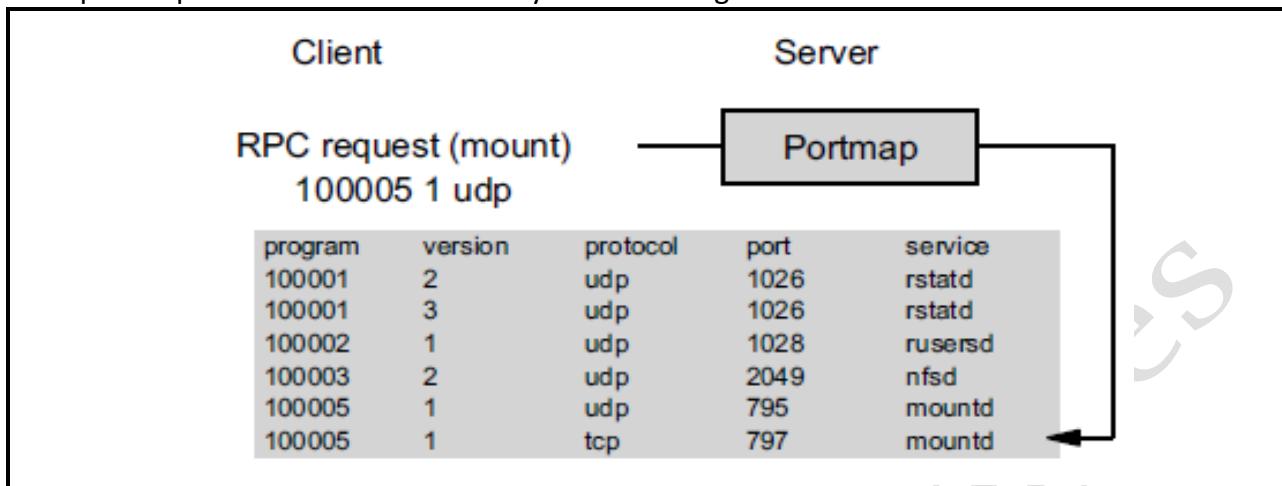
## NFS Daemon



- ☞ NFS client daemons consist of **biod**, **rpc.statd**, and **rpc.lockd**.
- ☞ NFS server daemons consist of **rpc.mountd**, **nfsd**, **rpc.statd**, and **rpc.lockd**.

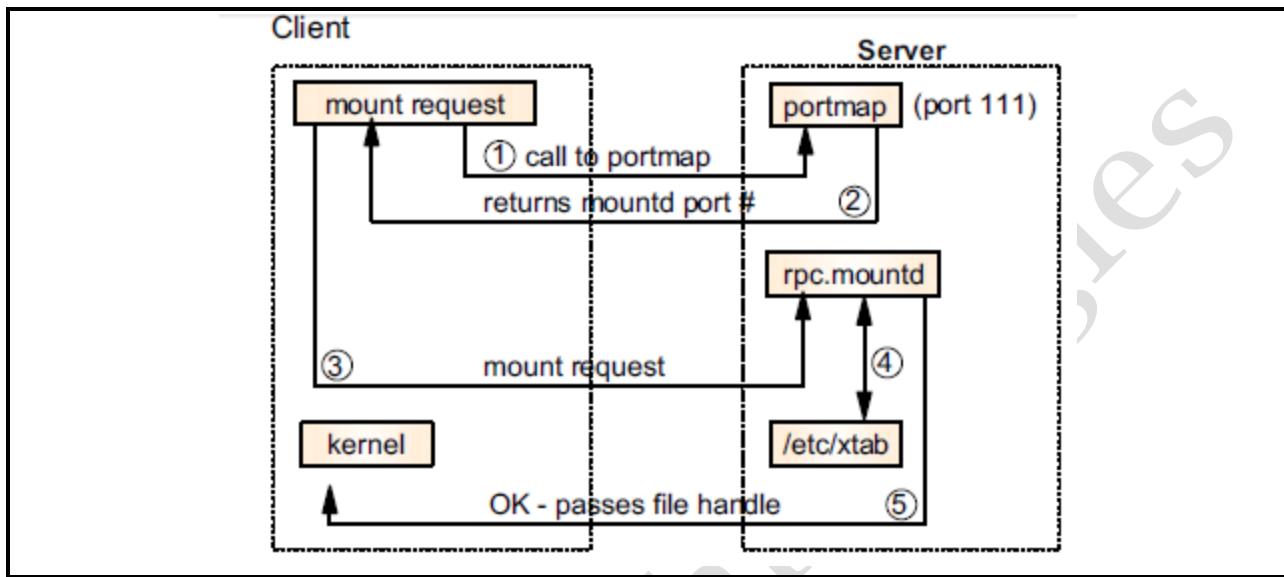
## **portmap Daemon:**

The portmap daemon must run on all systems running RPC Servers



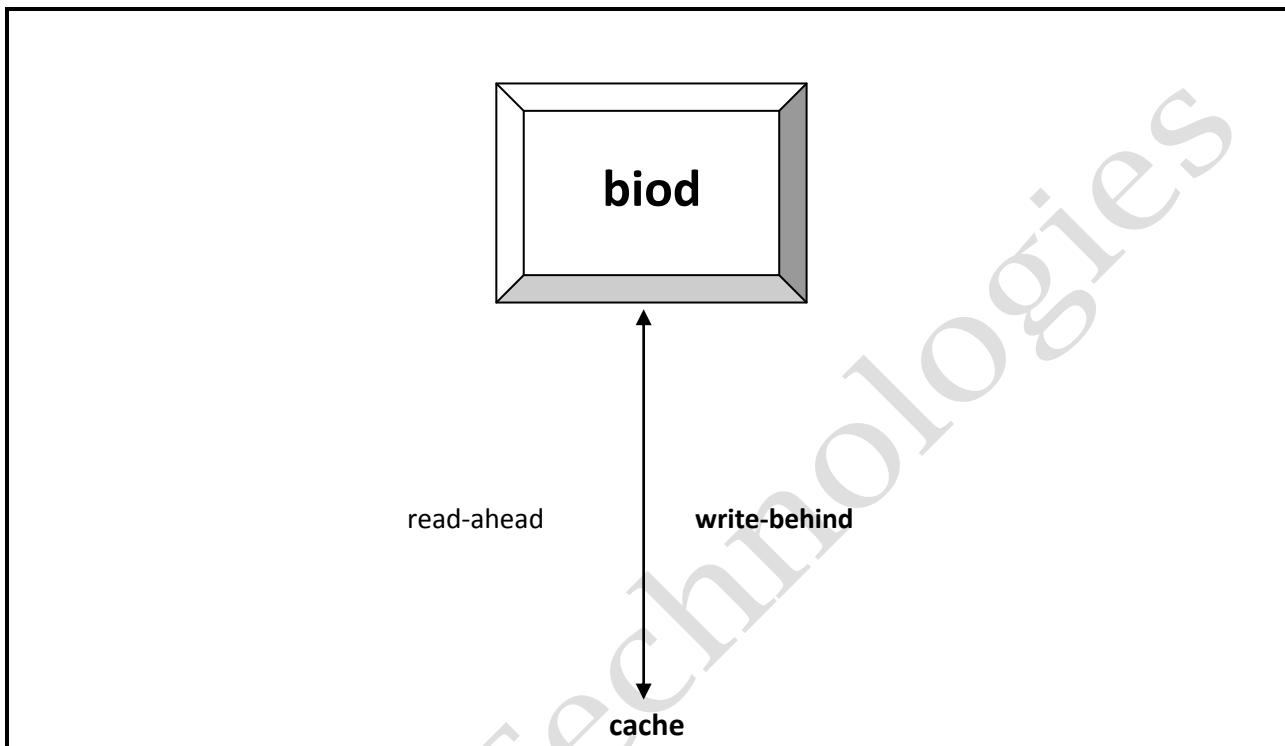
- ☞ **portmap** is a network service that provides clients with a standard way of looking up a port number associated with a specific program.
- ☞ When services on a server come up, they register with the **portmap** daemon as an available service. **portmap** then maintains a table of program-to-port pairs. It includes a program number, version number, protocol to be used, port number and service name.
- ☞ When the client tries to make a request of the server, it first contacts the **portmap** daemon to see where the server resides. The **portmap** daemon listens on a well-known port so the client can easily contact it. The **portmap** daemon responds to the client with the port of the service that the client is requesting. The client, upon receipt of the port number, is able to make all its future requests directly to the application.
- ☞ It is started in **/etc/rc.tcpip** before **inetd** and the RPC servers. Thus, when the RPC servers start they can register with **portmap**.

## Mountd:



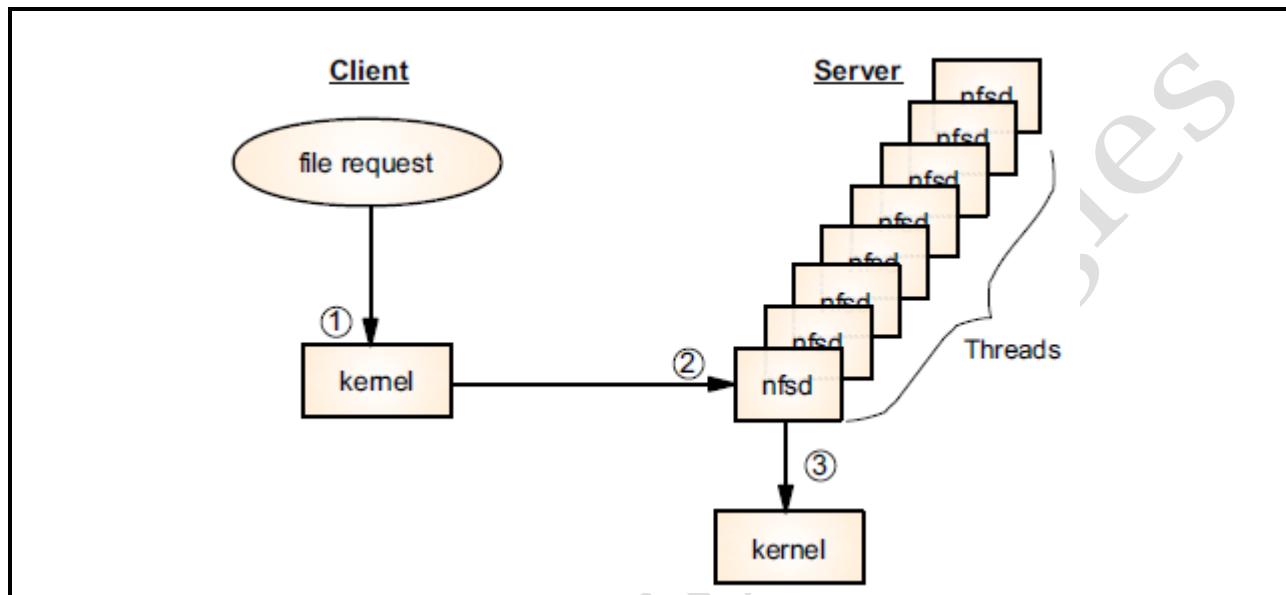
- ↳ **mountd** is a server daemon and an RPC that answers a client's request to mount a server's exported file system or directory. The **mountd** daemon finds out which file system is available by reading the **/etc/xtab** file.
- ↳ The mount process takes place as shown in the diagram:
  1. Client mount makes call to server's portmap daemon to find the port number assigned to the rpc.mountd daemon.
  2. portmap passes the port number to the client.
  3. Client mount then contacts the server rpc.mountd daemon directly and passes the name of the desired directory.
  4. The server rpc.mountd checks /etc/xtab (built by exportfs -a a command which reads /etc/exports) to verify availability and permissions on the requested directory.
  5. If all is verified, the server rpc.mountd gets a file handle (pointer to file system directory) for the exported directory and passes it back to the client's kernel.

## **biod (Block I/O Daemon)**



- ☞ The biod daemon improves NFS performance by filling or emptying the buffer cache on behalf of the NFS client. The daemon provides read-ahead and write-behind function, bringing data over in chunks (NFS V2 - 8k max, 32k default on NFS V3).
  - ☞ The biod function is performed by kernel threads. These threads are created and destroyed dynamically. The maximum number of biod threads can be controlled by:  
**#mount -o boids=n**
- where n is the number of threads specified. The default is four biod threads per mount point.

## nfsd



- ◀ **nfsd** is a server daemon that handles client requests for file system operations. Each **nfsd** handles one request at a time. When an **nfsd** is done passing a request to the kernel, it is free to accept another. This way a server is always able to accept a new nfs request as long as there is at least one **nfsd** running.
- ◀ Threads are dynamically created and are limited by the number specified in the startup file `/etc/rc.nfs` or **nfsd** settings.

## Auto mounting in NFS:

- ↳ An **automounter** is any program or software facility which automatically mounts filesystems in response to access operations by user programs. An automounter system utility (daemon under Unix), when notified of file and directory access attempts under selectively monitored subdirectory trees, dynamically and transparently makes local or remote devices accessible.
- ↳ Whenever NFS is created, exported and mounted over a remote system, it continuously uses the system resources i.e. network resources for mounting a dir on a remote host, irrespective of whether it is accessed or not by the user over remote system. Unnecessarily, the network resources will be busy and cannot be used for any other process. To overcome such situation automount is used. By using auto mount option an NFS will be mounted automatically on the remote system only when a user enters into mount point and perform some activity (say #ls) , and whenever the mount point is idle for a long time automatically it will be unmounted and will be mounted only when user starts doing some activity.

## Remote Mount Table Entry

#	mount	node	mounted	mounted over	vfs	date	options
	/dev/hd4		/		jfs2	Jun 02 13:49	rw,log=/dev/hd8
	/dev/hd2		/usr		jfs2	Jun 02 13:49	rw,log=/dev/hd8
	/dev/hd9var		/var		jfs2	Jun 02 13:49	rw,log=/dev/hd8
	/dev/hd3		/tmp		jfs2	Jun 02 13:49	rw,log=/dev/hd8
	/dev/hd1		/home		jfs2	Jun 02 13:50	rw,log=/dev/hd8
	/proc		/proc		procfs	Jun 02 13:50	rw
	/dev/hd10opt		/opt		jfs2	Jun 02 13:50	rw,log=/dev/hd8
	/etc/auto.indirect		/publishing		autofs	Jun 02 16:01	rw,ignore
	/etc/auto.direct		/kt1		autofs	Jun 02 16:01	ignore
	ktaix15	/kt		/publishing/backup	nfs3	Jun 02 16:50	rw

- ↳ Looking at the mount table, we see that the original **/publishing** parent mount point entry exists.
- ↳ The node column shows the server name of **ktaix15**. The mounted over column shows that the remote directory has been mounted over the local mount point, **/publishing/backup**.

## NFS Commands

<u>Command</u>	<u>Description</u>	<u>Daemon</u>
showmount	Displays what clients have mounted	rpc.mountd
rpcinfo	Displays what portmap has listed	portmap
nfsstat	Displays status of NFS and RPC calls	calls

↳ **showmount** displays a list of all clients that have mounted remote file systems.

↳ **rpcinfo** queries **portmap** daemon for information on services registered with **portmap**.

↳ **nfsstat** displays statistical information about NFS and RPC calls

### showmount

```
#showmount -e ktaix15
```

```
# showmount -e ktaix15
export list for ktaix15:
/home/files (everyone)
/kt          ktaix16
```

- ↳ The **showmount** command provides information about a server's mount information or what a server has exported.
- ↳ The **-e** option lists what is currently exported by a specific server.
- ↳ The **-a** option lists the client name and directory path name that has been remotely mounted.

**Task:** Raise a ticket to configure nfs server and client.

- a.Create a filesystem
- b.Share it to client
- c.Check /etc/exports
- d.mount on client and close the ticket.

## Rpcinfo

```
# rpcinfo -p ktaix15
  program vers proto port service
  100000 4 udp    111  portmapper
  100000 3 udp    111  portmapper
  100000 2 udp    111  portmapper
  100000 4 tcp    111  portmapper
  100000 3 tcp    111  portmapper
  100000 2 tcp    111  portmapper
```

```
# rpcinfo -u ktaix15 nfs 2
program 100003 version 2 ready and waiting
```

```
# rpcinfo -b autofs 1
192.168.10.15 ktaix15
192.168.10.16 ktaix16
127.0.0.1 loopback
192.168.10.15 ktaix15
192.168.10.16 ktaix16
127.0.0.1 loopback
```

- ↳ rpcinfo queries the remote portmap daemon.
- ↳ rpcinfo can be used to detect and debug failures such as:
  - Dead or hung servers caused by improper configuration or a failed daemon
  - Bogus or renegade RPC servers
  - Broadcast-related problems
- ↳ If the portmap daemon on the remote host has failed, this command times out.
- ↳ The -u option makes a call to the specific program and version number on a specific host using UDP and reports whether the program is ready and waiting for requests.
- ↳ The -b option makes an RPC broadcast of the specified program and version number and reports all hosts that respond.

## nfsstat

```
# nfsstat

Server rpc:
Connection oriented
calls      badcalls    nullrecv   badlen     xdrcall    dupchecks  dupreqs
0          0            0           0           0           0           0           0
Connectionless
calls      badcalls    nullrecv   badlen     xdrcall    dupchecks  dupreqs
0          0            0           0           0           0           0           0

Server nfs:
calls      badcalls    public_v2  public_v3
0          0            0           0
Version 2: (0 calls)
null      getattr     setattr    root       lookup     readlink   read
0 0%     0 0%        0 0%      0 0%      0 0%      0 0%      0 0%
wrcache   write       create     remove    rename    link      symlink
0 0%     0 0%        0 0%      0 0%      0 0%      0 0%      0 0%
mkdir     rmdir       readdir   statfs
0 0%     0 0%        0 0%      0 0%
Version 3: (0 calls)
null      getattr     setattr    lookup    access    readlink   read
0 0%     0 0%        0 0%      0 0%      0 0%      0 0%      0 0%
write    create      mkdir     symlink  mknod    remove    rmdir
```

- ↳ nfsstat is a command that displays NFS server and client statistics. Both for RPC and NFS it shows the different procedure calls that can be made, and how often these have been made.
- ↳ The output of nfsstat is very extensive by default, and the visual only shows a fraction of it. You can limit the output of nfsstat with various options.
- ↳ It is a good idea to gather nfsstat output regularly, so that you can compare “typical” output of a normally-running server to the output of that same server in case of problems.

### **Lab Activities:**

Make NFS between two servers and share some data. And also try to add some data from client side (client IP: 192.168.10.16) and check whether it is updated in Host Server (server IP: 192.168.10.15)

**Step1:** update **/etc/hosts** file with the client IP address and hostname in Host server and vice versa

#vi /etc/hosts → to add the following entries.

```
192.168.10.15    ktaix15
192.168.10.16    ktaix16

"/etc/hosts" 83 lines, 1893 characters
```

**Step2:** Make an LV on existing Vg or create new Vg and a file system on top of LV and add some data to it.

```
# mkvg -f -y ktvg -s 32 hdisk1
ktvg
# mklv -y ktlv -t jfs2 ktvg 10
ktlv
# crfs -v jfs2 -d ktlv -m /kt
File system created successfully.
327464 kilobytes total disk space.
New File System size is 655360
# mount /kt
# cd /kt
# ls
lost+found
# touch 1 2 3 4
# ls
1          2          3          4          lost+found
```

**Step3:** Start Nfs services at host server and add directory to nfs export list.

```
# startsrc -g nfs
0513-029 The biod Subsystem is already active.
Multiple instances are not supported.
0513-029 The nfsd Subsystem is already active.
Multiple instances are not supported.
0513-029 The rpc.mountd Subsystem is already active.
Multiple instances are not supported.
0513-059 The nfsrgyd Subsystem has been started. Subsystem PID is 585950.
0513-059 The gssd Subsystem has been started. Subsystem PID is 516214.
0513-029 The rpc.lockd Subsystem is already active.
Multiple instances are not supported.
0513-029 The rpc.statd Subsystem is already active.
Multiple instances are not supported.
```

### **Adding directory to export list using smitty.**

#smitty mknfsexp and change the following attributes

```
Add a Directory to Exports List

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP] [Entry Fields]
* Pathname of directory to export [/kt]
  Anonymous UID [-2]
  Public filesystem? no
* Export directory now, system restart or both both
  Pathname of alternate exports file []
  Allow access by NFS versions []
  External name of directory (NFS V4 access only) []
  Referral locations (NFS V4 access only) []
  Replica locations []
  Ensure primary hostname in replica list yes
  Allow delegations? no
* Security method [sys]
* Mode to export directory read-write
  Hostname list. If exported read-mostly []
  Hosts & netgroups allowed client access [ktaix16]
  Hosts allowed root access [ktaix16]
```

### **Command for above procedure:**

```
#mknfsexp -d /kt -S sys -c ktaix16 -r ktaix16
```

### **Check if the directory is in export list by using following:**

```
#pg /etc/exports (#pg /etc/xtab can also be used to see the same)
```

```
# pg /etc/exports
/ktaix16 -sec=sys,access=ktaix16,root=ktaix16
```

### **Now go to the client side (192.168.10.16).**

Create a directory where you mount the nfs directory.

```
#mkdir /kt_client
```

Now mount this local directory (kt\_client) to filesystem which is residing on the server:

```
#mount ktaix16:/kt /kt_client → & check whether data is there.
```

Now add some data to it

```
#cd /kt_client
```

```
# ls
```

```
#touch 5 6
```

Go to Server side (192.168.10.15) and check whether directory is updated or not.

### Unmounting Remote Mounts:-

#umount allr → will unmount all remotely mounted file systems.

#umount -n ktaix16 → to unmount all file system on particular client (where n is for node and ktaix16 is the name of client node)

### Perform auto mounting:

Step1: create an NFS server as above and directory to nfs export list but do not mount it on remote system, instead follow the steps below.

- ↳ Go to client (ktaix16)
- ↳ Create a file called “**auto.indirect**” in /etc folder and add the following attributes

```
# pg /etc/auto.indirect
backup  ktaix15:/kt
```

Directory                      Nfs server:/directory

- ↳ Create one more file “**auto.direct**” in /etc folder and add the following

```
# pg /etc/auto.direct
/kt1    -rw   ktaix15:/kt
```

Mount Point                      Permissions                      Nfs server:/directory

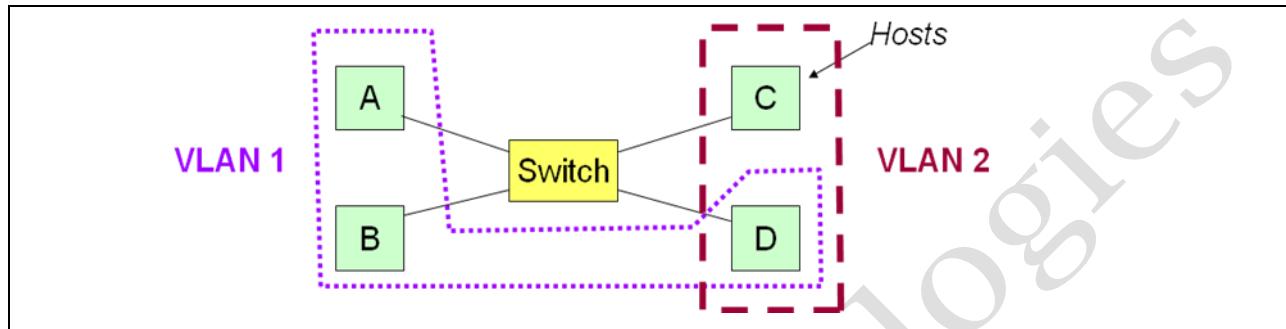
- ↳ Finally, make another file “**auto\_master**” in /etc folder and add the following

```
# pg /etc/auto_master
/publishing      /etc/auto.indirect -rw
/-                /etc/auto.direct
```

- ↳ After completing above process, run the following command to start automount  
#automount -v -t -i

## Virtual LAN

- Virtual LAN (VLAN) establishes virtual network segments on top of physical switch devices
- Virtual and dedicated network devices can be used simultaneously for communication
- VLAN is described by the IEEE 802.1Q standard



Virtual LAN is a technology used for establishing virtual network segments on top of physical switch devices. Multiple VLAN logical devices can be configured on a single system. Each VLAN logical device constitutes an additional Ethernet adapter instance. These logical devices can be used to configure the same types of Ethernet IP interfaces as are used with physical Ethernet adapters. Virtual Ethernet connections supported in POWER5 and POWER6 systems use VLAN technology to ensure that the partitions can only access data directed to them.

**VLANs (Virtual Local Area Networks)** can be thought of as logical broadcast domains. A VLAN splits up groups of network users on a real physical network onto segments of logical networks.

This implementation supports the IEEE 802.1Q VLAN tagging standard with the capability to support multiple VLAN IDs running on Ethernet adapters. Each VLAN ID is associated with a separate Ethernet interface to the upper layers (IP, etc.) and creates unique logical Ethernet adapter instances per VLAN, for example ent1, ent2 and so on.

The IEEE 802.1Q VLAN support can be configured over any supported Ethernet adapters. The adapters must be connected to a switch that supports IEEE 802.1Q VLAN.

You can configure multiple VLAN logical devices on a single system. Each VLAN logical devices constitutes an additional Ethernet adapter instance. These logical devices can be used to configure the same Ethernet IP interfaces as are used with physical Ethernet adapters. As such, the no option, ifsize (default 8), needs to be increased to include not only the Ethernet interfaces for each adapter, but also any VLAN logical devices that are configured. See the no command documentation.

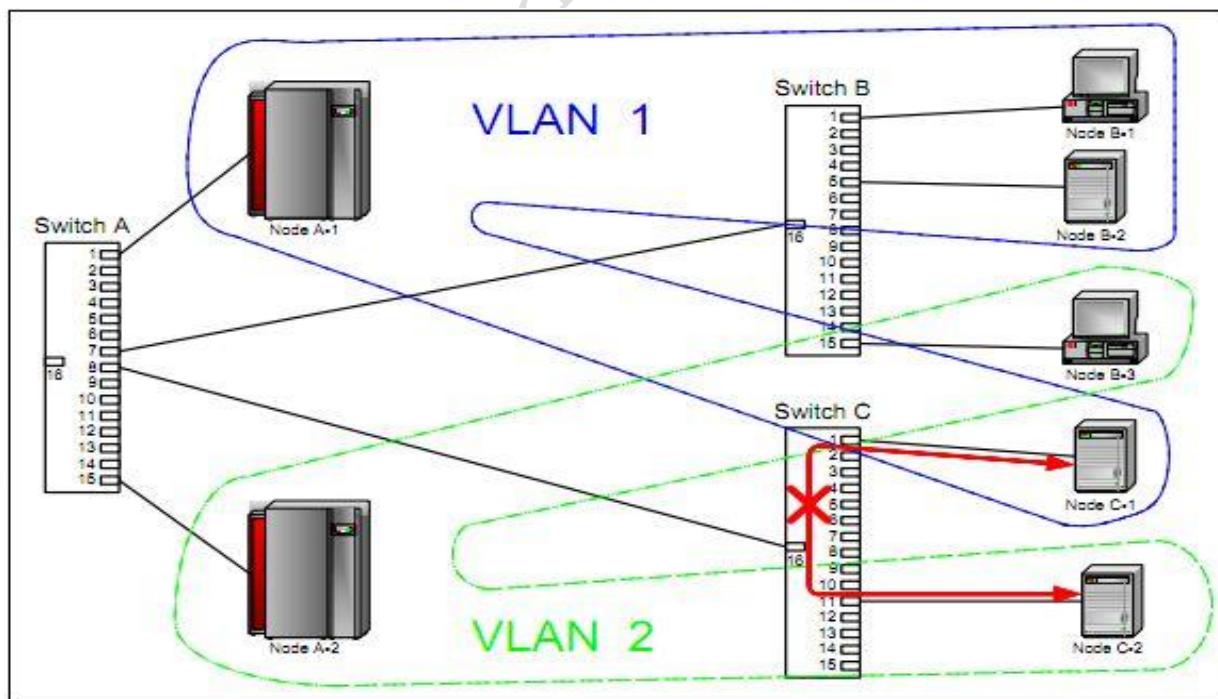
Each VLAN can have a different maximum transmission unit (MTU) value even if sharing a single physical Ethernet adapter.

VLAN support is managed through SMIT. Type the **smit vlan** fast path from the command line and make your selection from the main VLAN menu. Online help is available.

After you configure VLAN, configure the IP interface, for example, en1 for standard Ethernet or et1 for IEEE 802.3, using Web-based System Manager, SMIT, or commands.

AIX® 5.3 and later supports virtual Ethernet using a virtual I/O switch as a method to perform in-memory communication between partitions in a POWER5 or POWER6 system. The switch also supports IEEE 802.1Q tagging, which allows the virtual Ethernet adapters to belong different VLANs on the switch. Virtual Ethernet adapters are created and configured on partitions using the Hardware Management Console (HMC). After it is created, the partition will see the virtual Ethernet adapter in the open firmware tree when it scans for devices. After it is detected, the virtual Ethernet adapter is configured and used just like a physical Ethernet adapter. For more information, see the hardware documentation for your POWER5 system.

For example, two VLANs (VLAN 1 and 2) are defined on three switches (Switch A, B, and C). Although nodes C-1 and C-2 are physically connected to the same switch C, traffic between two nodes can be blocked. To enable communication between VLAN 1 and 2 some routing or bridging device is needed.



## AIX support for 802.1Q VLAN

```
#smitty vlan
```

```
Add A VLAN
```

```
Select adapter "ent4 Available EtherChannel/IEEE 802.3ad Link Aggregation"
```

```
VLAN Base Adapter ent4
```

```
* VLAN Tag ID [839]
```

```
root@aix2: / # lsdev -Cc adapter
```

```
ent0 Available 07-08 2-Port 10/100/1000 Base-TX PCI-X Adapter (14108902)
ent1 Available 07-09 2-Port 10/100/1000 Base-TX PCI-X Adapter (14108902)
ent2 Available 09-08 2-Port 10/100/1000 Base-TX PCI-X Adapter (14108902)
ent3 Available 09-09 2-Port 10/100/1000 Base-TX PCI-X Adapter (14108902)
ent4 Available EtherChannel / IEEE 802.3ad Link Aggregation
ent5 Available VLAN
```

```
root@aix2: / # lsattr -El ent5
```

```
base_adapter ent4 VLAN Base Adapter True
vlan_priority 0 VLAN Priority True
vlan_tag_id 839 VLAN Tag ID True
```

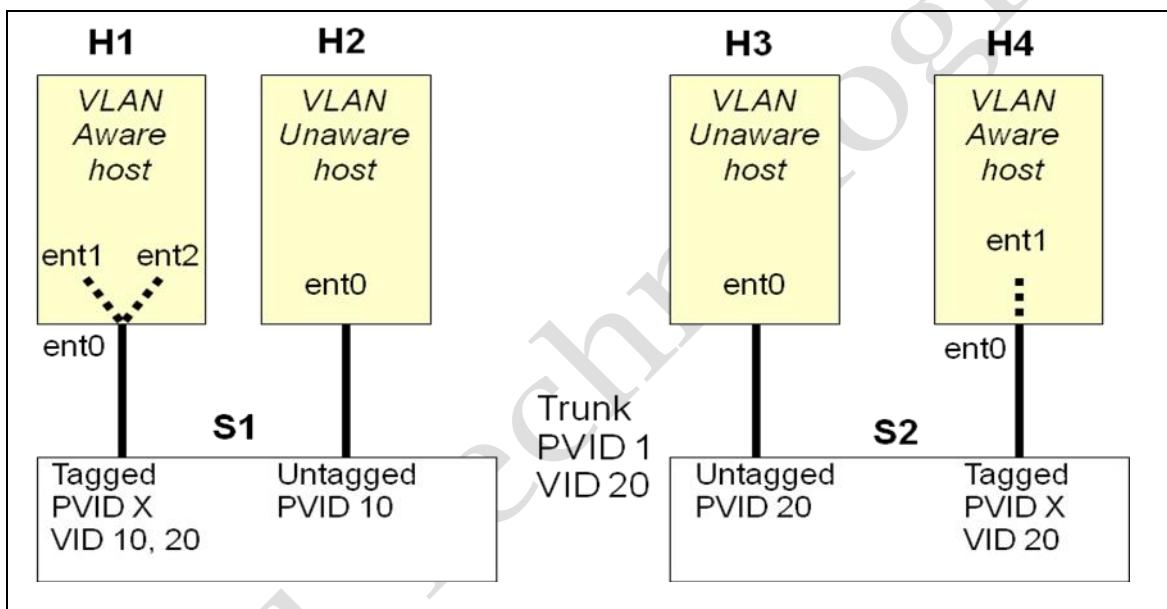
## IEEE 802.1Q VLAN

Layer 2 connectivity restricted to members of the same VLAN

- ISO OSI Model: structured seven layer networking model
- IP (and thus IP addresses and IP routing) is at Layer 3

**VID = VLAN ID - Identifies a VLAN**

**PVID = Port VLAN ID - Default VID of a port**



Virtual Local Area Network (VLAN) is described by the IEEE 802.1Q standard. VLAN is a method to logically segment a physical network such that Layer 2 connectivity is restricted to members that belong to the same VLAN. This separation is achieved by tagging Ethernet packets with their VLAN membership information and then restricting delivery to members of that VLAN. In the visual, Ethernet Switches S1 and S2 share VLAN 20 through tagged trunk ports. Hosts H1 and H2 share network VLAN 10. Hosts H1, H3 and H4 share network VLAN 20.

## **Quick review of ISO OSI model**

The seven layers of the ISO OSI model provide structure for network communications.

### **Layer 1 – Physical**

Physical layer defines the cable or physical medium itself, for example, thinnet, thicknet, unshielded twisted pairs (UTPs). All media are functionally equivalent. This layer conveys the bit stream from Layer 2.

### **Layer 2 - Data Link**

Data Link layer defines the format of data on the network. A network data frame, or packet, includes checksum, source and destination address, and data. The largest packet that can be sent through a data link layer defines the maximum transmission unit (MTU). A host connected to an Ethernet would have an Ethernet interface to handle connections. At this layer, data packets are encoded and decoded into bits.

### **Layer 3 – Network**

On TCP/IP networks, the internetwork protocol (IP) part is the network layer interface. IP is responsible for routing, directing datagrams from one network to another.

### **Layer 4 - Transport**

Transport layer subdivides user-buffer into network-buffer sized datagrams and enforces desired transmission control. Two transport protocols, transmission control protocol (TCP) and User Datagram Protocol (UDP), sit at the transport layer.

### **Layer 5 – Session**

The session protocol defines the format of the data sent over the connections. For example, NFS uses the remote procedure call (RPC) for its session protocol. RPC may be built on either TCP or UDP.

### **Layer 6 – Presentation**

External data representation (XDR) sits at the presentation level. It converts local representation of data to its canonical form and vice versa. The canonical uses a standard byte ordering and structure packing convention, independent of the host.

### **Layer 7 – Application**

This layer provides network services to the users. Mail, ftp, telnet, Domain Name System (DNS), Network Information Service (NIS), and network file system (NFS) are examples of network applications.

## **IEEE 802.1Q VLAN**

- Ethernet packets are tagged with their VLAN membership information
- Ethernet switch restricts delivery to members of that VLAN
- The VID can be added to an Ethernet packet either by:
  - i. VLAN aware host
  - ii. The switch (in the case of VLAN unaware hosts)
- Recommendation: – Single network per adapter, use untagged port and PVID – Multiple networks per adapter; use VID

### **Terminology**

The VLAN tag information is referred to as a VLAN ID (VID). Ports on a switch are configured as being members of the VLAN designated by the VID for that port. The default VID for a port is referred to as the Port VID (PVID).

### **Method**

The VID can be added to an Ethernet packet either by a VLAN aware host or by the switch in the case of VLAN unaware hosts. Therefore ports on an Ethernet switch have to be configured with information indicating whether the host connected is VLAN aware or unaware.

For VLAN unaware hosts, a port is set up as untagged and the switch will tag all packets entering through that port with the Port VLAN ID (PVID). It will also untag all packets exiting that port before delivery to the VLAN unaware host. A port used to connect VLAN unaware hosts is called an untagged port, and it can only be a member of a single VLAN identified by its PVID.

Hosts that are VLAN aware can insert and remove their own tags and can be members of more than one VLAN. These hosts are typically attached to ports that do not remove the tags before delivering the packets to the host, but will insert the PVID tag when an untagged packet enters the port. A port will only allow packets that are untagged or tagged with the tag of one of the VLANs the port belongs to.

These VLAN rules are in addition to the regular MAC address based forwarding rules followed by a switch. Therefore, a packet with a broadcast or multicast destination MAC will also get delivered to member ports that belong to the VLAN that is identified by the tags in the packet. This mechanism ensures the logical separation of the physical network based on membership in a VLAN.

## **Recommendation**

In general, configuration is simpler when ports are untagged and only the PVID is configured because the attached hosts do not have to be VLAN aware and they do not require any VLAN configuration. However this scenario has the limitation that a host can access only a single network using a single adapter. When accessing a single network per Ethernet adapter, using untagged ports with a PVID only is preferred. Additional VIDs should be used only when multiple networks are being accessed through a single Ethernet adapter.

## **SAMBA**

- Samba is an open source free, software suite that provides seamless file and print services between Windows clients and UNIX-like platforms.
- Samba uses the TCP/IP protocol that is installed in the host server. When configured, this server software allows the host machine to share files and printers and make them accessible from Windows clients.
- Samba binaries for AIX are available in the AIX 61D Expansion pack CD.

### **Installation requirements:**

Samba on AIX requires the following packages:

Image	File set	Description
Samba. base	Samba. base	Samba server
Samba. license	Samba. license	Samba licenses
Samba. man	Samba. man	Man pages for Samba

### **Practicals:**

#smitty installp

```
Install and Update Software

Move cursor to desired item and press Enter.

Install Software
Update Installed Software to Latest Level (Update All)
Install Software Bundle
Update Software by Fix (APAR)
Install and Update from ALL Available Software
```

- After selecting Install software, Now select the device from which you want to install the samba file sets i.e. “/dev/cd0”

### Install Software

Type or select a value for the entry field.  
Press Enter AFTER making all desired changes.

\* INPUT device / directory for software

[Entry Fields]  
[]

F1=Help  
F5=Reset  
F9=Shell

```
+-----  
| INPUT device / directory for software  
|  
| Move cursor to desired item and press Enter.  
|  
| /dev/cd0          (Virtual SCSI Optical Served by VIO Server)  
|  
| F1=Help           F2=Refresh           F3=Cancel  
| F8=Image           F10=Exit            Enter=Do  
| /=Find            n=Find Next  
+-----
```

- Now at “**SOFTWARE to install**” select three file sets i.e.
  1. Samba. base
  2. Samba. license
  3. Samba. man
- Next “**ACCEPT new license agreements? – Yes**” & Press enter, It will start installing the samba.

### Install Software

Type or select values in entry fields.  
Press Enter AFTER making all desired changes.

\* INPUT device / directory for software  
\* SOFTWARE to install  
PREVIEW only? (install operation will NOT occur)  
COMMIT software updates?  
SAVE replaced files?  
AUTOMATICALLY install requisite software?  
EXTEND file systems if space needed?  
OVERWRITE same or newer versions?  
VERIFY install and check file sizes?  
Include corresponding LANGUAGE filesets?  
DETAILED output?  
Process multiple volumes?  
ACCEPT new license agreements?  
Preview new LICENSE agreements?

[Entry Fields]  
/dev/cd0  
[samba.base]  
no  
yes  
no  
yes  
yes  
no  
no  
no  
yes  
no  
yes  
yes  
no  
yes  
yes  
no

#### WPAR Management

Perform Operation in Global Environment yes  
Perform Operation on Detached WPARs no  
    Detached WPAR Names [\_all\_wpars]  
Remount Installation Device in WPARs yes  
Alternate WPAR Installation Device []

- In order to be able to connect to the Samba server, you must create users and shares. The configuration file that stores information of shares is **/usr/lib/smb.conf**.

### **Starting the Samba server:**

- Samba has two daemons, **nmbd** and **smbd**, that need to be running in order for Samba to work correctly.
- **nmbd** is a server that understands and can reply to NetBIOS over IP name service requests, like those produced by SMB/CIFS clients such as Windows 95/98/ME, Windows NT, Windows 2000, Windows XP, and LanManager clients. It also participates in the browsing protocols that make up the Windows Network Neighborhood view.
- **smbd** is the server daemon that provides the file-sharing and printing services to Windows clients. The server provides filesystem and printer services to clients using the SMB (or CIFS) protocol.

These can be started from the command line as follows:

```
# nmbd
# smbd
```

- The logs of these daemons can be found in the **/var** directory as **log.nmbd** and **log.smbd**, respectively.
- These daemons can also be started automatically during system reboot by adding an entry into **/etc/inittab**, as follows:

```
mkitab nmb:2:once:/usr/sbin/nmbd
mkitab smb:2:once:/usr/sbin/smbd
```

- Now the two daemons get started during every reboot. The daemons get listed in the process lists:

```
# ps -ef | grep mbd
root 667870 708792 0 12:49:24 - 0:00 smbd
root 675974 1 0 12:49:24 - 0:00 nmbd
root 708792 1 0 12:49:24 - 0:00 smbd
```

### **Creating users:**

- First create a normal user(**ktuser**) in the server

<b># mkuser ktuser</b>
------------------------

- Then make it as a samba user & assign password to the samba user.

```
# smbpasswd -a ktuser
New SMB password:Retype new SMB password:#
```

- Now edit the samba configuration file “/usr/lib/smb.conf” & add the following lines

[public]	→ Share Name
Path=/samba	→ Directory which is going to be shared with windows
Public=no	→ No Public Access
Valid users=ktuser	→ Samba user who's going to access the Share directory
Writable=yes	→ Permission
Host allow=192.168.10.	→ Hosts from “192.168.10.” Network can be allowed

```
# vi /usr/lib/smb.conf

# IBM_PROLOG_BEGIN_TAG
# This is an automatically generated prolog.
#
# 61smb320 src/samba/usr/lib/smb.conf 1.1
#
# Licensed Materials - Property of IBM
#
# Restricted Materials of IBM
#
# COPYRIGHT International Business Machines Corp. 2008
# All Rights Reserved
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
# IBM_PROLOG_END_TAG
#
[public]
path=/samba
public=no
valid users=ktuser
writable=yes
host allow=192.168.10.
~
```

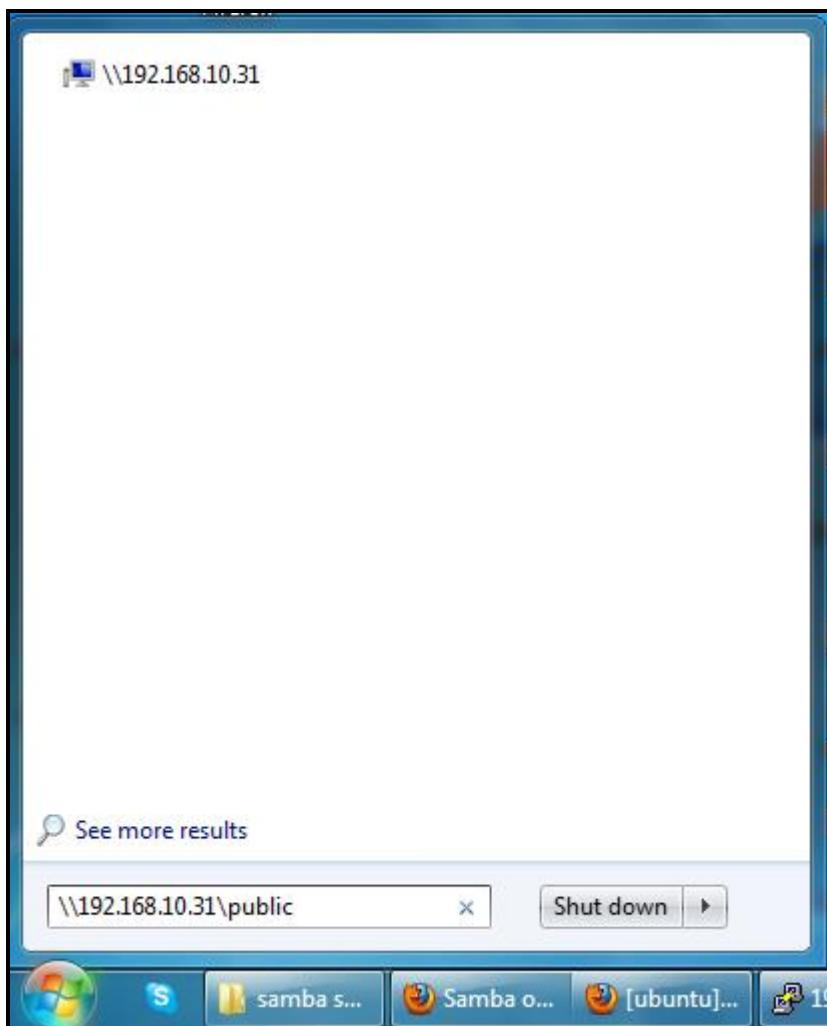
- After giving entry in **smb.conf** file, then create a directory i.e. **/samba**( which is a share directory)
- Also create some files in **/samba** directory

```
# mkdir /samba  
#  
# cd /samba  
# touch f1 f2 f3  
# ls  
f1 f2 f3
```

- Now assign full permissions for the share directory (**/samba**) & restart the services.

```
# chmod 777 /samba  
  
# nmbd  
# smbd
```

- Now go to **Windows system -> start -> in run type “\\192.168.10.31\public”**  
(which is “ \\ip address of samba server\share name”)



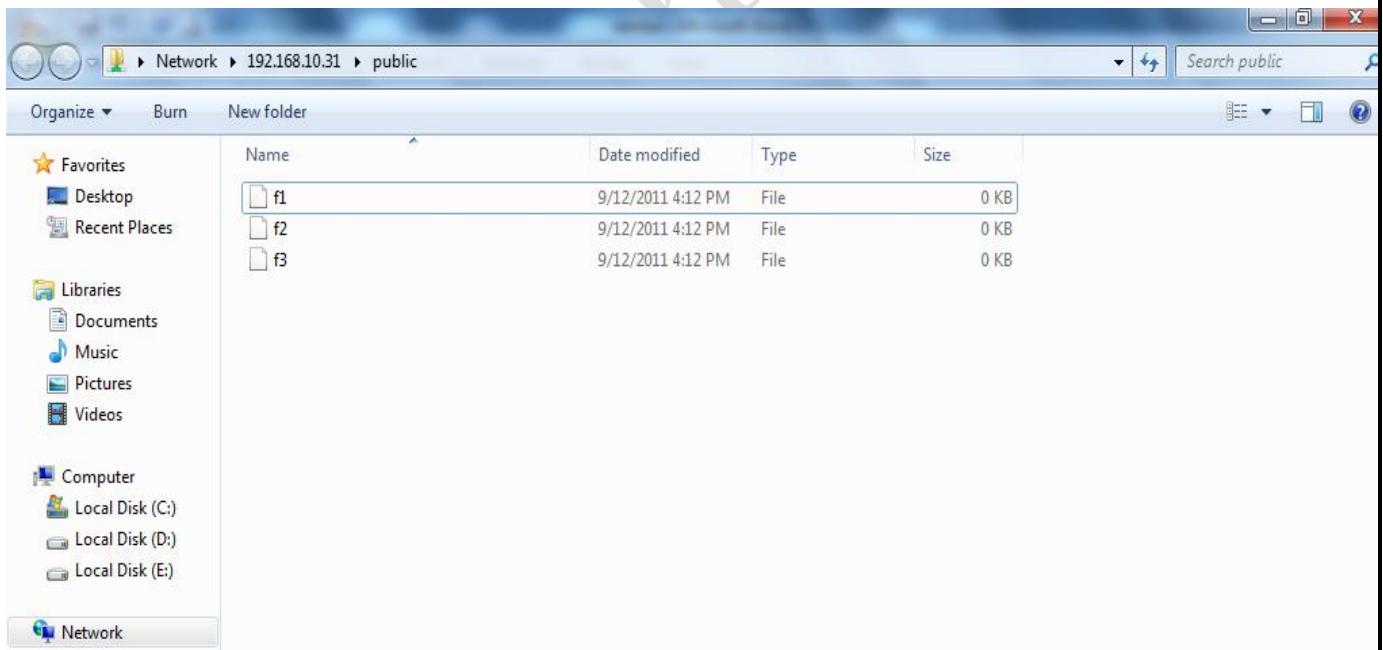
- Now you will be prompted to enter the samba user name & password

**Username:** ktuser

**Password:** \*\*\*\*

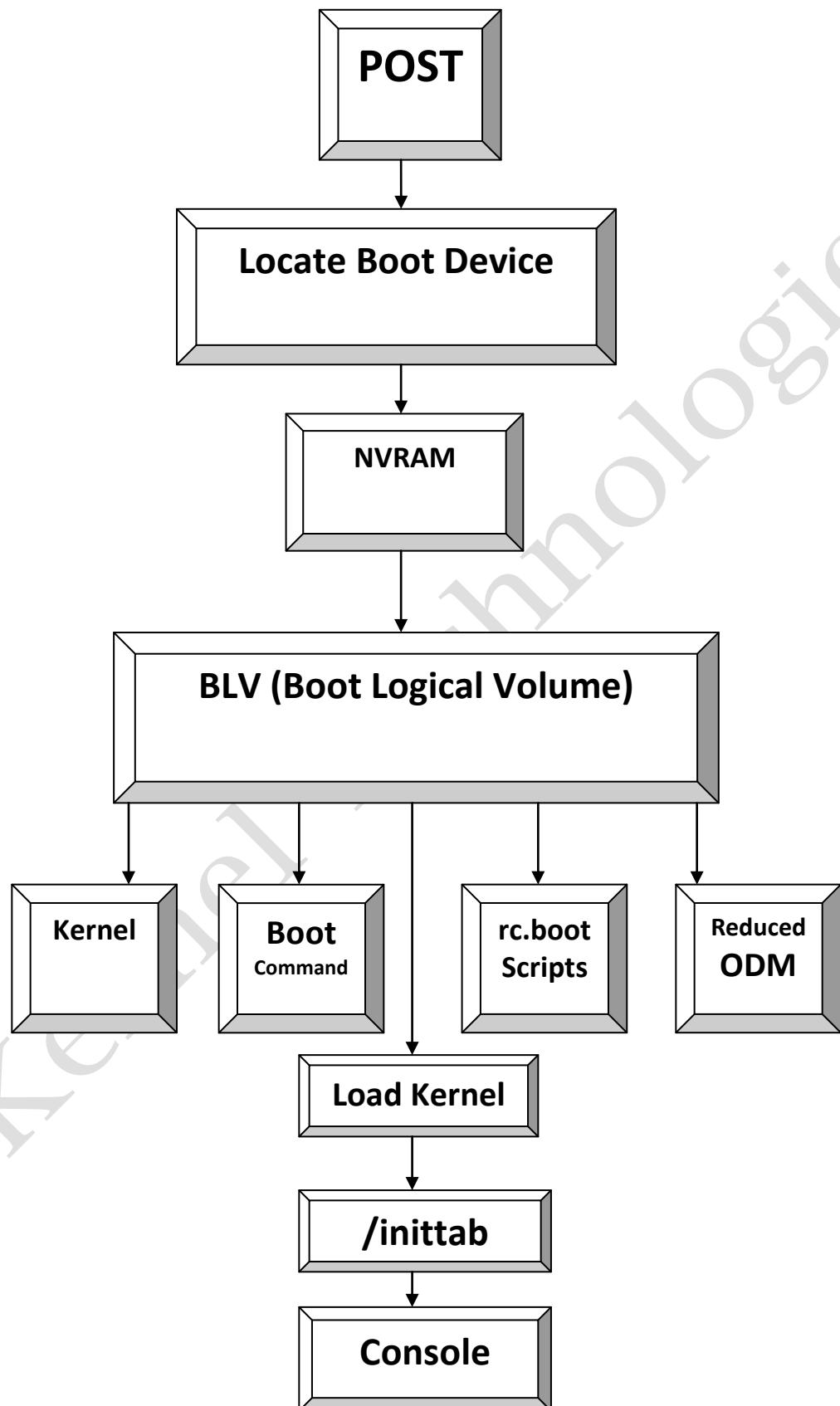


- After pressing enter you will be seeing the files which you have created in AIX i.e. in /samba directory.



- Now you can also create files in this above path i.e. in windows, similarly see the changes in AIX i.e. in /samba.

## BOOTING PROCEDURE



## **BOOTING PROCEDURE:**

### **Loading the boot image of AIX**

- After POST, the firmware (System Read Only Storage) detects the 1st bootable device stored in the bootlist. (hdisk0)
- Then the bootstrap code (software ROS) i.e. 1st 512 bytes of the hard disk loads to the RAM.
- Bootstrap code locates the Boot Logical Volume (BLV = hd5) from the harddisk
- BLV contains AIX kernel, rc.boot Script, Reduced ODM and Boot commands.
- Then BLV in the RAM is uncompressed and Kernel releases from it.
- Then AIX Kernel gets control.
- AIX Kernel creates a RAM File System (rootvg still not activated).
- Kernel starts init process from the BLV.
- init executes rc.boot script from the BLV in the RAM.
- Init with rc.boot 1 configures base devices.

### **rc.boot 1**

- init process from RAMFS executes rc.boot 1 (if any error LED=c06)
- restbase command copies ODM from BLV to RAMFS.(success LED=510, error LED=548)
- cfgmgr -f calls config rules ( which are in phase 1) and activates all base devices.
- runs command bootinfo -b to check last boot device ( success LED=511).
- Then rc.boot 2 activates rootvg from hard disk.

### **rc.boot 2**

- Starts rc.boot 2 (LED 551)
- ipl\_varyon to activate rootvg (success LED= 517, error LED=552,554,556)
- runs command fsck -f /dev/hd4 to check whether "/" unmounted uncleanly in the last shutdown ( error LED=555).
- mount /dev/hd4 (/) to RAMFS (error LED=557 due to corrupted jfslog)
- fsck -f /dev/hd2 i.e. "/usr" ( error LED=518).
- mount /dev/hd2 in RAMFS.
- fsck -f /dev/hd9var i.e. check "/var"
- mount /var
- copycore command checks whether dump has occurred, Then copy dump from primary dump device paging space (/dev/hd6) to /var/adm/ras/.
- umount /var
- swapon /dev/hd6 i.e. activate primary paging space.

Now the condition is /dev/hd4 is mounted on / in the RAMFS, cfgmgr -f configures all base devices. So now the configuration data has been written to ODM from RAMFS.

- mergedev is called and copy /dev from RAMFS to disk.
- copy customized ODM from RAMFS to hard disk(at this stage both ODM from hd5 and hd4 are sync now)
- mount /var.
- Boot messages are copied to file (/var/adm/ras/bootlog) on the hard disk.

To view bootlog type: alog -t boot -o

Now /, /usr and /var are mounted in rootvg on the hard disk. Then

- Kernel removes RAMFS
- init process starts from / in the rootvg

Here completes rc.boot 2, now the condition is kernel has removed RAMFS and accessing rootvg filesystems from the hard disk. Then init file from BLV replaces the init file on hard disk

- In rc.boot 3, the init process is started (/etc/inittab) and remaining devices are configured.

### **rc.boot 3**

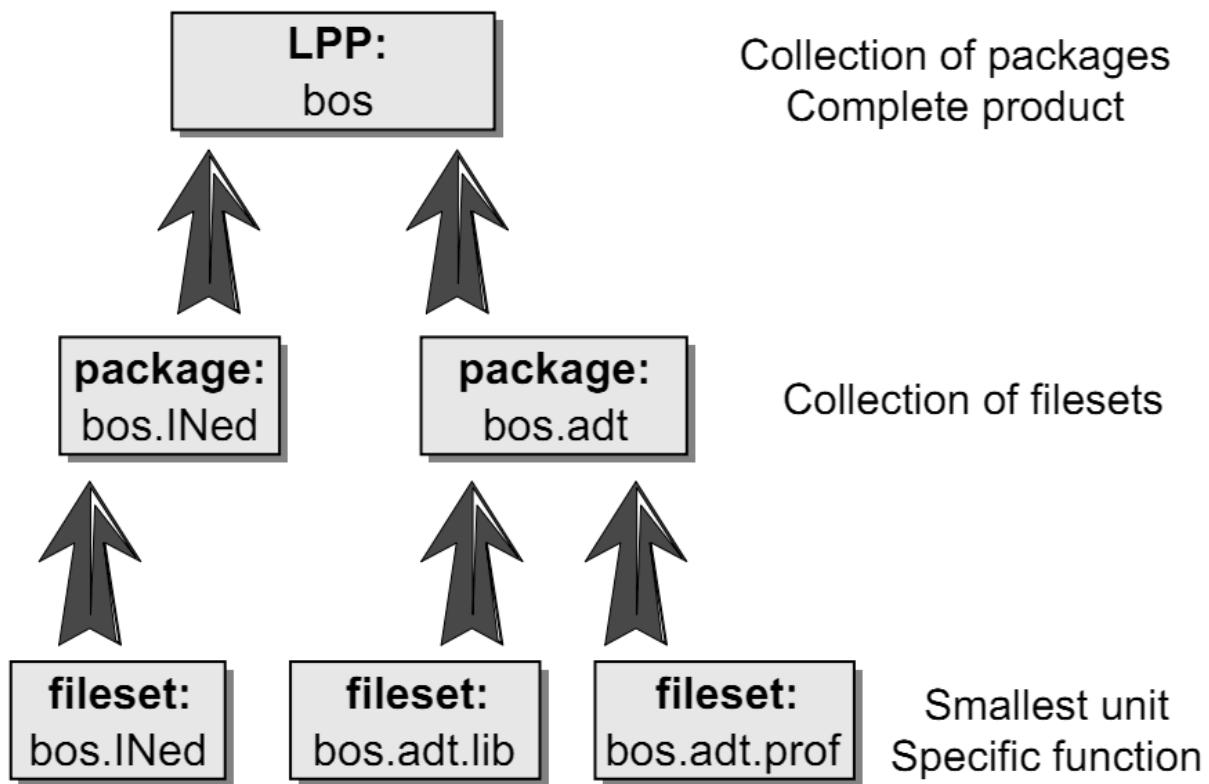
- /etc/init starts and reads /etc/inittab (LED=553)
- runs /sbin/rc.boot 3
- fsck -f /dev/hd3 i.e. check /tmp.
- mount /tmp
- sysncvg rootvg &; i.e. run syncvg in background and report stale PPs.
- cfgmgr -P2 i.e. runs cfgmgr in phase 2 in normal startup.
- cfgmgr -P3 i.e. runs cfgmgr in phase 3 in service mode.
- All remaining devices are configured now.
- cfgcon configures console (LED= c31 select console, c32 lft, c33 tty, c34 file on disk). If CDE mentioned in /etc/inittab we will get graphical console.
- savebase calls to sync ODM from BLV with / FS (i.e. /etc/objrepos).
- syncd daemon started. All data from cache memory to disk saves in every 60 seconds.
- starts errdemon for error logging.
- LED display turned OFF.
- rm /etc/nologin i.e. if the file is not removed, then login is not possible.
- If any device are in missed state, (in Cudv chgstatus=3) display it.

Next displays as "system initialization completed"

**NOTE:**Raise a ticket to enter into datacenter to see the booting procedure.

## SOFTWARE INSTALLATION

### Packaging definitions



- ☞ **Fileset:** A fileset is the smallest installable base unit. Fileset includes all files that make a complete product. It is available in backup file format (bff).
- ☞ **Package:** It is a group of separately installable filesets that provide set of related functions.
- ☞ **Licensed Program Product (LPP):** It is a complete software product collection, which includes all packages associated with license program.
- ☞ **Bundle:** A bundle is a collection of packages and filesets suited for a particular environment. For example, if you have developing application, the App-Dev bundle would be the logical choice to install.

**NOTE:** You will have realtime problem discussion in class for issues related to software installation.

### **Lab Activities:**

1. Find out to check if java is installed in the system, If yes when it was installed.

```
↳ #lslpp -l |grep -l java  
#lslpp -h all |more    (see the date of installation)
```

Doing the same thing through smitty

#smitty install → select the following:

```
Software Installation and Maintenance  
  
Move cursor to desired item and press Enter.  
  
Install and Update Software  
List Software and Related Information  
Software Maintenance and Utilities  
Software Service Management  
Network Installation Management  
EZ NIM (Easy NIM Tool)  
System Backup Manager  
Alternate Disk Installation  
EFIX Management
```

Under it select the following

```
Move cursor to desired item and press Enter.  
  
List Installed Software and Related Information  
List Software on Media and Related Information
```

Now select List the installed software as shown below

```
Move cursor to desired item and press Enter.  
  
List Installed Software  
List Installed Software by Bundle  
List Applied but Not Committed Software Updates  
Show Software Installation History  
Show Fix (APAR) Installation Status  
List Fileset Requisites  
List Fileset Dependents  
List Files Included in a Fileset  
List Fileset Containing File  
Show Installed License Agreements
```

Finally enter the following attributes.

```
Type or select values in entry fields.  
Press Enter AFTER making all desired changes.  
  
[Entry Fields]  
* SOFTWARE name [all]  
SHOW superseded levels? no
```

The list will be displayed as below:

COMMAND STATUS					
Command:	stdout:	stderr:			
Before command completion, additional instructions may appear below.					
[TOP]	Fileset	Level	State	Type	Description (Uninstaller)
<hr/>					
Java14.sdk	1.4.2.20	C	F		Java SDK 32-bit
Tivoli_Management_Agent.client.rte	3.7.1.0	C	F		Management Framework Endpoint Runtime"
X11.Dt.ToolTalk	5.3.0.0	C	F		AIX CDE ToolTalk Support
X11.Dt.bitmaps	5.3.0.0	C	F		AIX CDE Bitmaps
X11.Dt.helpmin	5.3.0.0	C	F		AIX CDE Minimum Help Files
X11.Dt.helprun	5.3.0.0	C	F		AIX CDE Runtime Help
X11.Dt.lib	5.3.0.30	C	F		AIX CDE Runtime Libraries
X11.Dt.rte	5.3.0.30	C	F		AIX Common Desktop Environment (CDE) 1.0
X11.adt.bitmaps	5.3.0.0	C	F		AIXwindows Application Development Toolkit Bitmap Files
X11.adt.imake	5.3.0.30	C	F		AIXwindows Application

## 2. Remove java from the system (smitty remove)

↳ #smitty remove → change the following attributes

```
Type or select values in entry fields.  
Press Enter AFTER making all desired changes.  
  
[Entry Fields]  
* SOFTWARE name [Java14.sdk]  
PREVIEW only? (remove operation will NOT occur) no  
REMOVE dependent software? no  
EXTRACT file systems if space needed? no  
DETAILED output? yes
```

3. Raise a ticket to Upgrade system from TL4 to TL5 & also apply service pack(sp1) for TL5.

Step1: Check the current TL on server by following command

```
#oslevel -r
```

```
# 5300-04 (If the output is like this, it means it is TL4 installed)
```

Step2: Download TL5 from IBM website and transfer it to server (say TL folder in /tmp)

Now move to the TL folder and follow the steps

Run #inutoc . so that it may create a toc file.(toc stands for table of content)

```
#smitty installp and select the following
```

```
Install and Update Software

Move cursor to desired item and press Enter.

Install Software
Update Installed Software to Latest Level (Update All)
Install Software Bundle
Update Software by Fix (APAR)
Install and Update from ALL Available Software
```

Select [...] for installing from current directory.

```
Update Installed Software to Latest Level (Update All)

Type or select a value for the entry field.
Press Enter AFTER making all desired changes.

* INPUT device / directory for software [Entry Fields] [...]
```

Change the following attributes

```
Update Installed Software to Latest Level (Update All)

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

* INPUT device / directory for software [Entry Fields] .
* SOFTWARE to update _update_all
  PREVIEW only? (update operation will NOT occur) no
  COMMIT software updates? no
  SAVE replaced files? yes
  AUTOMATICALLY install requisite software? yes
  EXTEND file systems if space needed? yes
  VERIFY install and check file sizes? no
  DETAILED output? no
  Process multiple volumes? yes
  ACCEPT new license agreements? yes
  Preview new LICENSE agreements? no
```

After the completion of installation restart the server and check for the version of TL as above.

\*Applying of service pack (sp1) is also same as TL installation.

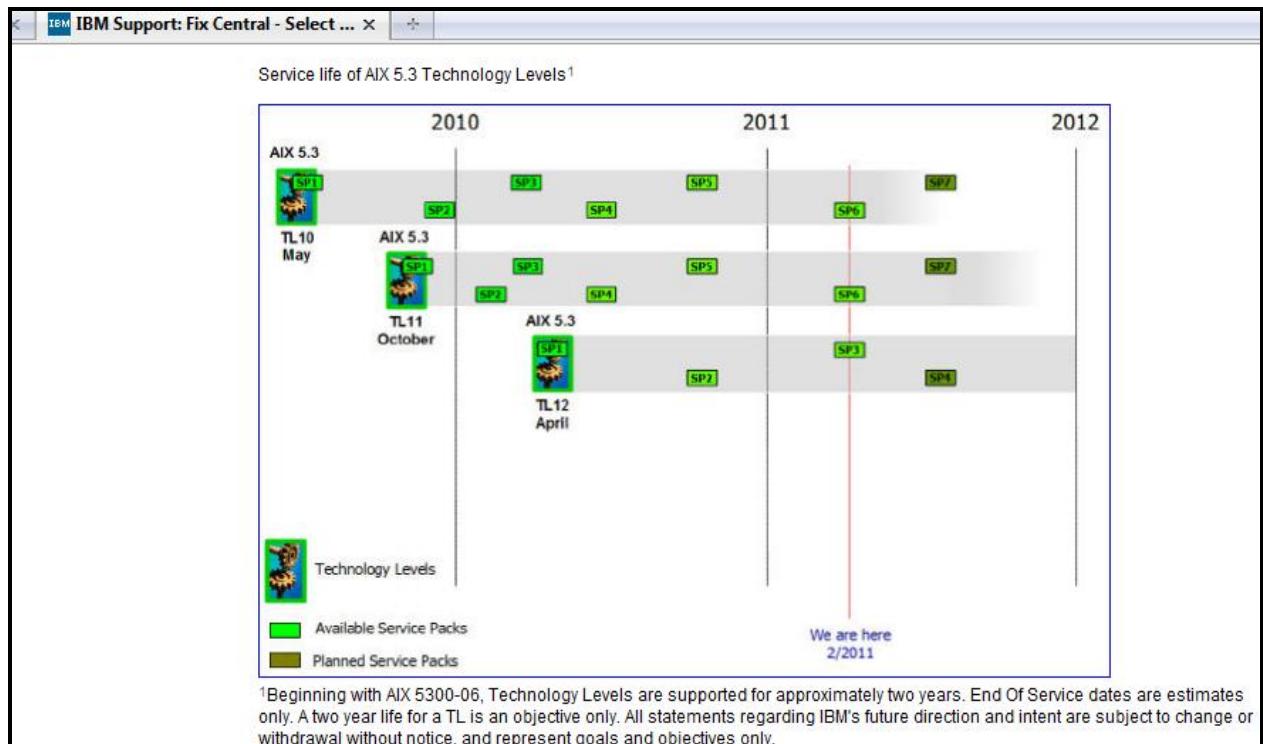
4. Visit IBM website to download latest TL & service packs, also look into life cycle of TL.

Go to <http://www-933.ibm.com/support/fixcentral/> and select the following

The screenshot shows the 'Fix Central' page on the IBM Support Portal. The left sidebar includes links for 'Supported products', 'Enhancements', 'Help', and 'Feedback'. The main content area has a heading 'Fix Central' and a brief description: 'Fix Central provides fixes and updates for your system's software, hardware, and operating system.' It instructs users to 'Select the product below. When using the keyboard to navigate the page, use the Alt and down arrow keys to navigate the selection lists.' Below this, there are 'Related links' for System p, BladeCenter, and System i. The search form on the right includes dropdowns for 'Product Group' (set to AIX), 'Version' (set to 5.3), and 'Fix type' (set to Fix packs). A 'Continue' button is at the bottom of the form.

The screenshot shows the 'Select fixes' page for 'Operating Systems, AIX (5.3)'. The left sidebar includes 'Change your selection' options for 'Change your selected product' and 'Applies to version' (set to 5.3), along with a 'Submit' button. The main content area has a heading 'Select fixes' and a message: 'The following results match your request. Select the fixes you wish to download.' It includes a 'Generate a link to this page' link and 'Refine results' and 'View results' dropdowns. Below this, it shows '1-10 of 79 results' and a 'Next' button. On the right, it shows 'Results per page: 10 | 20 | 40 | All' and a date 'Feb 23, 2011'. A list of fixes is shown, starting with '1. Service pack: 5300-12-03-1107' (version 5300-12-03-1107), with links for 'Compare report', 'Fix details', 'Installation instructions', 'View cross product recommendations for this fix', and 'Show requisite fixes'.

The life cycle of an TL will be situated at the bottom of the same page



## 5. How to check if APAR is installed.

↳ #smitty install and go to following

```
Software Installation and Maintenance

Move cursor to desired item and press Enter.

Install and Update Software
List Software and Related Information
Software Maintenance and Utilities
Software Service Management
Network Installation Management
EZ NIM (Easy NIM Tool)
System Backup Manager
Alternate Disk Installation
E FIX Management
```

```
Move cursor to desired item and press Enter.

List Installed Software and Related Information
List Software on Media and Related Information
```

```
List Installed Software and Related Information

Move cursor to desired item and press Enter.

List Installed Software
List Installed Software by Bundle
List Applied but Not Committed Software Updates
Show Software Installation History
Show Fix (APAR) Installation Status
List Fileset Requisites
List Fileset Dependents
List Files Included in a Fileset
List Fileset Containing File
Show Installed License Agreements
```

\*Select the APAR you want to check as following (generate list by pressing F8 or Esc8)

```
Show Fix (APAR) Installation Status

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

* FIX ID

[Entry Fields]           FIX ID
Move cursor to desired item and press Enter. Use arrow keys to scroll.

[TOP]
5.3.0.0_AIX_ML      AIX 5.3.0.0 Release
5300-01_AIX_ML      AIX 5300-01 Update
5300-02_AIX_ML      AIX 5300-02 Update
5300-03_AIX_ML      AIX 5300-03 Update
5300-04_AIX_ML      AIX 5300-04 Update
IY58143              Required fixes for AIX 5.3
IY58614              Cannot manage backup/restore of extended attribut
IY58615              Root passwd is set on Next if nothing has been en
IY58617              NFS: No error message in working dialog
IY58618              Start all queues for non-root fails without messa
IY58621              System crash during boot
```

6. How to install a new APAR.

- ↳ #smitty installp & follow the steps shown below (download APAR same as TL5 and being in the APAR's directory run "smitty installp" and install it same as TL5)

```
Install and Update Software

Move cursor to desired item and press Enter.

Install Software
Update Installed Software to Latest Level (Update All)
Install Software Bundle
* Update Software by Fix (APAR)
Install and Update from ALL Available Software
```

Select [...] for installing from current directory.

```
Update Installed Software to Latest Level (Update All)

Type or select a value for the entry field.
Press Enter AFTER making all desired changes.

* INPUT device / directory for software [.] [Entry Fields]
```

\*Rest is same as TL up gradation.

7. List out if there is any emergency fix in a system.

(Note: before we upgrade TL check if any emergency fix is there on the system, remove emergency fix)

- ↳ #emgr -l -L all (Through command Line)

#smit emgr

```
EFIX Management

Move cursor to desired item and press Enter.

List EFIXES and Related Information
Install EFIX Packages
Remove Installed EFIXES
Check Installed EFIXES
```

```

List EFIXES and Related Information

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
[ALL]
[1]
no

```

8. Check how to commit applied software.

 #smits install

```

Software Installation and Maintenance

Move cursor to desired item and press Enter.

Install and Update Software
List Software and Related Information
Software Maintenance and Utilities
Software Service Management
Network Installation Management
EZ NIM (Easy NIM Tool)
System Backup Manager
Alternate Disk Installation
E FIX Management

```

```

Software Maintenance and Utilities

Move cursor to desired item and press Enter.

Commit Applied Software Updates (Remove Saved Files)
Reject Applied Software Updates (Use Previous Version)
Remove Installed Software

Rename Software Images in Repository
Clean Up Software Images in Repository

Copy Software to Hard Disk for Future Installation
Copy Software Bundle to Hard Disk for Future Installation

Check Software File Sizes After Installation
Verify Software Installation and Requisites

Clean Up After Failed or Interrupted Installation

Service Update Management Assistant (SUMA)

```

#Select the name of software you want to commit as following

```

Commit Applied Software Updates (Remove Saved Files)

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
[Java]
no
yes
yes
yes

```

9. Check how to reject applied software.  
↳ Ref Q.NO 8 and instead of commit, select Reject Applied Software.

10. What command will you run to clean up the failed installations?

↳ #installp -C

11. How will you check if there is no inconsistency in software installation?

↳ #lppchk -v

12. Raise a ticket to update java and install C++ compiler on server.

Kernel Technologies

## Installation of JAVA Version 6 in Aix6.1

- First Download java software from IBM web site:  
<http://www.ibm.com/developerworks/java/jdk/aix/service.html>

The screenshot shows the IBM developerWorks website. The top navigation bar includes links for English, Sign in (or register), and a search bar. Below the header, there's a secondary navigation bar with links for Technical topics, Evaluation software, Community, and Events. The main content area is titled "AIX Download and service information" and describes "Developer Kits, User Guides and Service information for Java Standard Edition on AIX". On the left, a sidebar under "Java technology" lists categories like New to Java technology, Downloads & products, Open source projects, Standards, Technical library, Forums, and Events. The main content area lists download options for Java SE Version 7, Java SE Version 6, Java SE Version 5, Java SE Version 4.2, IBM WebSphere Real Time V3 on AIX, IBM WebSphere Real Time V2 on AIX, Java SE and IBM WebSphere Real Time minimum AIX support levels, Java service information, and More resources.

- Then Select the Java software whether it is 32bit or 64bit.

The screenshot shows two tables on the IBM developerWorks website. The first table is for "Java SE Version 6" and the second is for "Java SE Version 5". Both tables have columns for Platform, Base image, SDK fixes (PTFs), Latest fixes list<sup>1</sup>, User guides, Filesets, Install directory, Web Start support, and Plug-in support. The "Latest fixes list" column contains links to "fixes.html" files. The "User guides" column contains links to "sdkguide security guide" files. The "Install directory" column contains paths like "Java6.\* /usr/java6" and "Java6\_64.\* /usr/java6\_64". The "Web Start support" and "Plug-in support" columns both contain "Yes". In the Java SE Version 6 table, the "Java 6 32-bit" row has "Java 6 32-bit" in the "Base image" column and "Fix Info" in the "SDK fixes (PTFs)" column. The "Java 6 64-bit" row has "Java 6 64-bit" in the "Base image" column and "Fix Info" in the "SDK fixes (PTFs)" column. A note below the tables states: "These images may be specific to an AIX release. See the [Java SE and IBM WebSphere Real Time minimum AIX level support](#) section." A note at the bottom of the Java SE Version 6 table says: "1. IBM J9 2.6: If your IBM product includes an [Java 6 SDK with an IBM J9 2.6 virtual machine](#) please refer to this [fixes list](#). Enter `java -version` on the command line to obtain information about the J9 virtual machine build level." A "Back to top" link is also present.

- Provide the authentication information(IBM UserID and Password) for downloading the java.

The screenshot shows the IBM website for the AIX Developer Kit and Runtime, Java Technology Edition. At the top, there's a navigation bar with links for Home, Solutions, Services, Products, Support & downloads, and My IBM. The main title "IBM AIX Developer Kit and Runtime, Java Technology Edition" is displayed prominently. On the left, there's a sidebar with "Related links" including "Warranties and maintenance". The central area has two forms: one for "Returning visitors" asking for an "IBM ID: (usually e-mail address)\*" and a "Password\*", with links to forgot password and sign in. Another form for "Not registered?" explains the benefits of having an IBM Registration ID and provides a link to register here. At the bottom, there's a footer with links for About IBM, Privacy, Contact, Terms of use, Accessibility, IBM Feeds, and Jobs.

- Agree license and confirm

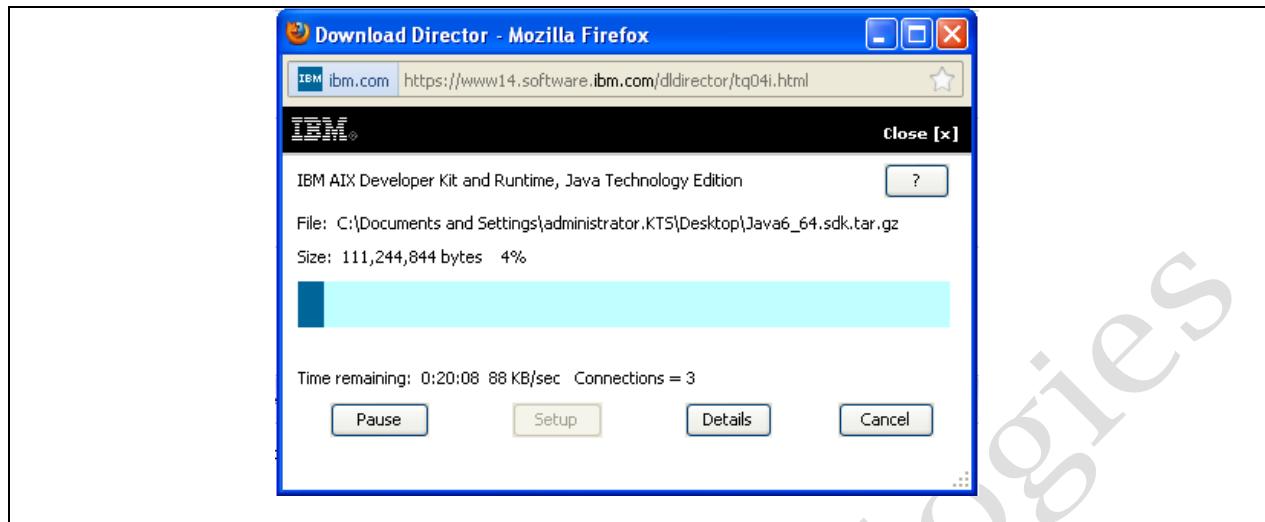
The screenshot shows two sequential steps in a process. The first step, "Privacy", contains text about IBM using information for product updates, three checkboxes for communication preferences ("by e-mail.", "by telephone.", "by postal mail."), and a statement about agreeing to IBM's privacy statement. The second step, "License", contains text about viewing the license, a link to "View license", a statement about agreeing to terms, an "I agree" checkbox, and two buttons at the bottom: "I confirm" and "I cancel".

- Select the java software “Java6\_64.sdk.tar.gz (111244844)” then accept license and confirm.

	<b>IBM Java6 64-bit SDK installps / smit install for AIX, latest base images</b>	
	<p><input type="checkbox"/> <b>Base SDK (required)</b> Java6_64.sdk.tar (156344320)</p> <hr/> <p><input checked="" type="checkbox"/> <b>OR</b> Java6_64.sdk.tar.gz (111244844)</p> <hr/> <p><input type="checkbox"/> <b>Demos</b> Java6_64.samples.tar (16742400)</p> <hr/> <p><input type="checkbox"/> <b>OR</b> Java6_64.samples.tar.gz (11844065)</p> <hr/> <p><input type="checkbox"/> <b>Src.jar</b> Java6_64.source.tar (8734720)</p> <hr/> <p><input type="checkbox"/> <b>OR</b> Java6_64.source.tar.gz (8412612)</p>	

	<b>IBM 64-bit SDK for AIX, latest code for redistribution, IHO-AIX installp / IHO-smit install format</b>	
	<p><input type="checkbox"/> <b>Readme</b> <a href="#">readme.html</a></p> <hr/> <p><input type="checkbox"/> <b>Latest code</b> j64redist.bin (112042275) <a href="#">View license</a></p> <hr/> <p><input type="checkbox"/> <b>Latest code</b> jre64redist.bin (165801516) <a href="#">View license</a></p>	
	<p><b>License</b></p> <p>By checking "I agree" box below you agree that (1) you have had the opportunity to review the license and (2) you agree to be bound by its terms. If you disagree, click "I cancel" below.</p> <p><input checked="" type="checkbox"/> I agree</p> <hr/> <p>By clicking the "I confirm" button below, I confirm my acceptance of the license. By clicking the "I cancel" button, I cancel my acceptance of the license.</p> <p> <b>I confirm</b>  <b>I cancel</b></p>	

- Now the java is going to download on the given location.



- After the download is successful
- Extract the java fileset

```
#gunzip Java6_64.sdk.tar.gz
#tar -xvf Java6_64.sdk.tar
```

```
# cd /tmp/java
# ls
Java6_64.sdk.tar
#
```

```
# cd /tmp/java
# ls
Java6_64.sdk.tar
#
#
# tar -xvf Java6_64.sdk.tar
x Java6_64.sdk, 156336128 bytes, 305344 media blocks.
#
# ls
Java6_64.sdk      Java6_64.sdk.tar
```

- After the file is successfully extracted, install the fileset using “smitty installp”

```
#smitty installp

Install Software

* INPUT device / directory for software [ . ]

SOFTWARE to install [Java6_64.sdk]

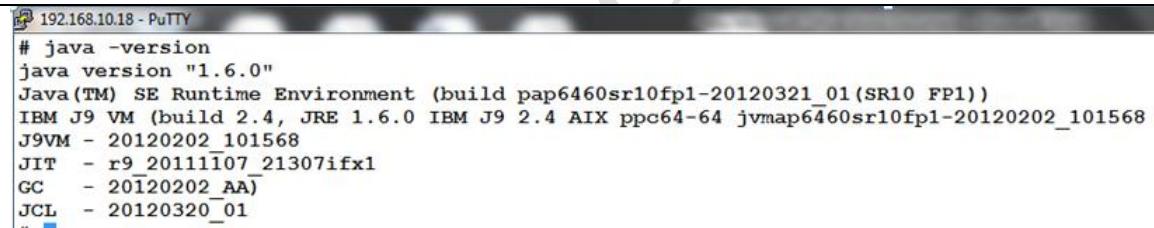
ACCEPT new license agreements? yes
```

- After the installation is successfull, set the path for java in **/etc/environment** file.

```
#vi /etc/environment
```

```
PATH=/usr/bin:/etc:/usr/sbin:/usr/ucb:/usr/bin/X11:/sbin:/usr/java6_64/jre/bin:/usr/java6_64/bin
TZ=CST6CDT
LANG=en_US
LOCPATH=/usr/lib/nls/loc
NLSPATH=/usr/lib/nls/msg/%L/*N:/usr/lib/nls/msg/%L/*N.cat
LC_FASTMSG=true
```

- Re-login to the same system once again.
- Now check the new java version using command “java –version”



```
# java -version
java version "1.6.0"
Java(TM) SE Runtime Environment (build pap6460sr10fp1-20120321_01(SR10 FP1))
IBM J9 VM (build 2.4, JRE 1.6.0 IBM J9 2.4 AIX ppc64-64 jvmap6460sr10fp1-20120202_101568
J9VM - 20120202_101568
JIT - r9_20111107_21307ifx1
GC - 20120202_AA)
JCL - 20120320_01
```

## REAL TIME 3<sup>RD</sup> PARTY TOOLS INSTALLATION

### Bash Installation:-

- ↳ Step1:- go to the directory where you have stored bash as following

```
# cd /opt/bash  
# ls  
bash-3.2-1.aix5.2.ppc.rpm  
#
```

- ↳ Step2:- Type “install” to install bash and select the following.

```
Install and Update Software  
  
Move cursor to desired item and press Enter.  
  
Install Software  
Update Installed Software to Latest Level (Update All)  
Install Software Bundle  
Update Software by Fix (APAR)  
Install and Update from ALL Available Software
```

- ↳ To install from the current directory type (.), (Dot) in the following field.

```
Install Software  
  
Type or select a value for the entry field.  
Press Enter AFTER making all desired changes.  
  
* INPUT device / directory for software [Entry Fields] [.]
```

- ↳ Now, select the software to be installed on your machine as following

```
Type or select values in entry fields.  
Press Enter AFTER making all desired changes.  
  
* INPUT device / directory for software [Entry Fields] .  
* SOFTWARE to install [_all_latest]  
PREVIEW only? (install operation will NOT occur) no  
  
SOFTWARE to install  
  
Move cursor to desired item and press F7. Use arrow keys to scroll.  
ONE OR MORE items can be selected.  
Press Enter AFTER making all selections.  
  
> bash-3.2 [ALL]  
    @R:bash-3.2 3.2
```

◀ After making your selection accept the License Agreement as shown below.

```
Install Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]

* INPUT device / directory for software .
* SOFTWARE to install [bash-3.2]
PREVIEW only? (install operation will NOT occur) no
COMMIT software updates? yes
SAVE replaced files? no
AUTOMATICALLY install requisite software? yes
EXTEND file systems if space needed? yes
OVERWRITE same or newer versions? no
VERIFY install and check file sizes? no
Include corresponding LANGUAGE filesets? yes
DETAILED output? no
Process multiple volumes? yes
ACCEPT new license agreements? yes
Preview new LICENSE agreements? no
```

◀ Finally press enter for two times and wait for installation to get completed.

```
COMMAND STATUS

Command: OK          stdout: yes          stderr: no

Before command completion, additional instructions may appear below.

geninstall -I "a -cgNQqwXY -J" -Z -d . -f File 2>&1

File:
  bash-3.2
  bash-3.2

Validating RPM package selections ...

bash #####
```

◀ Step3:- Now you are completed with the installation, to invoke the shell just type the name of the shell as “bash” bash will be activated.

```
#  
#  
#  
# bash  
bash-3.2# 
```

- ↳ To make bash your default shell you need to change the following attributes.
- ↳ Add the address of bash i.e. **/usr/bin/bash** in **/etc/security/login.cfg**
- ↳ #vi /etc/security/login.cfg

```
user: shells = /bin/sh,/bin/bsh,/bin/csh,/bin/ksh,/bin/tsh,/bin/ksh93,/usr/bin/sh,/usr/bin/bsh,/usr/bin/csh,/usr/bin/ksh,/usr/bin/tsh,/usr/bin/ksh93,/usr/bin/rksh,/usr/bin/rksh93,/usr/sbin/uucp/uucico,/usr/sbin/sliplogin,/usr/sbin/snappd,/usr/bin/bash
```

- ↳ Add the same **/usr/bin/bash** in **/etc/shells** file
- ↳ #vi /etc/shells

```
/bin/csh  
/bin/ksh  
/bin/psh  
/bin/tsh  
/bin/bsh  
/usr/bin/csh  
/usr/bin/ksh  
/usr/bin/psh  
/usr/bin/tsh  
/usr/bin/bsh  
/usr/bin/bash
```

- ↳ Run chsh command change the following so that it becomes your default shell.
- ↳ # chsh

```
bash-3.2# chsh  
Current available shells:  
/bin/sh  
/bin/bsh  
/bin/csh  
/bin/ksh  
/bin/tsh  
/bin/ksh93  
/usr/bin/sh  
/usr/bin/bsh  
/usr/bin/csh  
/usr/bin/ksh  
/usr/bin/tsh  
/usr/bin/ksh93  
/usr/bin/rksh  
/usr/bin/rksh93  
/usr/sbin/uucp/uucico  
/usr/sbin/sliplogin  
/usr/sbin/snappd  
/usr/bin/bash  
root's current login shell:  
/usr/bin/ksh  
Change (yes) or (no) ? > yes  
To?>/usr/bin/bash
```

## ENHANCED USER SECURITY WITH SUDO

### SUDO

- Configuring a system with enhanced security, so that the system can allow users what they need to do and disallow what they don't need to do. This can be achieved by a tool called sudo.
- The sudo command stands for "superuser do". Using sudo, system administrators can give certain users or groups access to some or all commands without those users having to know the root password.
- It also logs all commands and arguments so there are records of who used it for what, and when.
- To use the sudo command, at the command prompt, enter:  
sudo command  
Eg. sudo mkuser ktuser1
- Let us first install sudo fileset on AIX.
- Follow the below steps to install sudo on AIX.

```
# ls
sudo168p12.tar
# tar -xvf sudo168p12.tar
x sudo168p12
x sudo168p12/DESC, 27 bytes, 1 tape blocks
x sudo168p12/README.1st, 143 bytes, 1 tape blocks
x sudo168p12/install.sh, 2657 bytes, 6 tape blocks
x sudo168p12/sudo168p12.tar.gz, 111787 bytes, 219 tape blocks
x sudo168p12/sudoers, 608 bytes, 2 tape blocks
x sudo168p12/sudoers.eds, 519 bytes, 2 tape blocks
```

```
# ls
sudo168p12      sudo168p12.tar
# cd sudo168p12
# ls
DESC           README.1st       install.sh
# ./install.sh
x ./usr/local/bin/sudo, 146054 bytes, 286 tape blocks
./usr/local/bin/sudoedit linked to ./usr/local/bin/sudo
x ./usr/local/libexec/sudo_noexec.a, 8454 bytes, 17 tape blocks
x ./usr/local/libexec/sudo_noexec.la, 775 bytes, 2 tape blocks
x ./usr/local/man/man5/sudoers.5, 57536 bytes, 113 tape blocks
x ./usr/local/man/man8/sudo.8, 25790 bytes, 51 tape blocks
x ./usr/local/man/man8/visudo.8, 12044 bytes, 24 tape blocks
x ./usr/local/sbin/visudo, 95827 bytes, 188 tape blocks
Please run ". /etc/environment" at command line so that the new
changes in /etc/environment will be effective.
# . /etc/environment
```

- The **sudoers** file located at: **/etc/sudoers**, contains the rules that users must follow when using the **sudo** command.
- Do not edit the **/etc/sudoers** directly, instead use "**visudo**" command to edit the **sudoers** file.
- There are two reasons for that it prevents two users from editing the file at the same time, and it also provides limited syntax checking. Even if you are the only root user, you need the syntax checking, so use "**visudo**".

The two best advantages about using **sudo** command are:

- Restricted privileges
- Logs of the actions taken by users

In order to use **sudo** first there is a need to configure the sudoers file. The sudoers file is located at **/etc/sudoers**. And you should not edit it directly, you need to use the **visudo** command.

Once you enter **visudo** command, you will see something like this:

```
# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the sudoers man page for the details on how to write a sudoers file.
#
# Host alias specification
#
# User alias specification
#
# Cmnd alias specification
#
# Defaults specification
#
# Runas alias specification
#
# User privilege specification
root    ALL=(ALL) ALL
```

- Almost all lines are commented out, the one that matters in this sudoers file example is:  
**root ALL=(ALL) ALL**
- This line means: The root user can execute from **ALL** terminals, acting as **ALL** (any) users, and run **ALL** (any) command.
- The first part is the user, the second is the terminal from where the user can use **sudo** command, the third part is which users he may act as, and the last one, is which commands he may run when using **sudo**.

- Check that the sudo path is installed in the default location, where all the binaries are located.
- If sudo is not found in the default location where binaries are stored, add a soft link for sudo path i.e **/usr/local/bin/sudo** to **/usr/bin** or **/usr/sbin**.
- The procedure to add a soft link is shown below:

```
# which sudo
/usr/local/bin/sudo
#
# ln -s /usr/local/bin/sudo /usr/bin/
#
# ls -l /usr/bin/sudo
lrwxrwxrwx 1 root system 19 Apr 10 10:23 /usr/bin/sudo -> /usr/local/bin/sudo
```

- Let us first give privileges to the user **ktuser** as root.
- To assign root privileges to ktuser, add a line in sudoers file using visudo command.  
**#visudo** (save the sudoers file as we save a vi file using “wq!”)

```
# Runas alias specification

# User privilege specification
root    ALL=(ALL) ALL
ktuser  ALL=(ALL) ALL
```

- Now login as ktuser and try to run some of the super user commands.
- Here using ktuser trying to create another user using mkuser command, it is not allowing to ktuser to create a new user.

```
# su - ktuser
$
$ mkuser ktuser2
ksh: mkuser: cannot execute
```

- Let us try the same command using sudo.

```
$ sudo mkuser ktuser2
$ sudo passwd ktuser2
Changing password for "ktuser2"
ktuser2's New password:
Re-enter ktuser2's new password:
```

- The mkuser command was executed successfully and passwd was also assigned to that user using sudo.

- Now let's allow a group called **ktgroup** to run commands as a super user.
- Let us check the users in ktgroup.

```
#cat /etc/group
```

```
# cat /etc/group
system:!:0:root,pconsole,esaadmin
staff:!:1:ipsec,esaadmin,ktuser,ktuser2,ktuser3
bin:!:2:root,bin
sys:!:3:root,bin,sys
adm:!:4:bin,adm
uucp:!:5:uucp,nuucp
mail:!:6:
security:!:7:root
snapp:!:13:snapp
ipsec:!:200:
pconsole:!:14:pconsole
ktgroup:!:201:ktuser,ktuser2,ktuser3
```

- As we have know what are the users in ktgroup.
- Let's add a line in sudoers file to give root privileges to the users in ktgroup.

```
## EDS Level 3 Linux Support Pre-Enrollment Sudo Access
%techsup      ALL=(ALL) NOPASSWD:  ALL
%ktgroup      ALL=(ALL) NOPASSWD:  ALL
```

- Now, login as a one of the user in ktgroup and try to run some of the super user commands.

```
# su - ktuser3
$
$ mkvg -y datavg -s 64 hdisk5
ksh: mkvg: cannot execute
$ sudo mkvg -f -y datavg -s 64 hdisk5
datavg
```

- We can see that the user **ktuser3** from **ktgroup** was trying to execute **mkvg** command which was not successful, but it was successful when he executed the same command using sudo.
- Now let's restrict **ktuser** to run only some specific commands like "**mkuser**, **rmuser** and **chuser**"
- First find out the complete path for the commands using 'which command'

```
# which mkuser
/usr/bin/mkuser
# which rmuser
/usr/sbin/rmuser
# which chuser
/usr/bin/chuser
```

- Now let us add a line in sudoers file, to restrict ktuser to execute only these three commands.

```
# User privilege specification
root    ALL=(ALL)  ALL
ktuser  ALL=(ALL)  /usr/bin/mkuser, /usr/sbin/rmuser, /usr/bin/chuser
```

```
# su - ktuser
$ sudo mkuser user1
$ sudo passwd user1
Sorry, user ktuser is not allowed to execute '/usr/bin/passwd user1' as root on
ktaix28.
$
$ sudo rmuser user1
$ sudo mkvg -y datavg2 -s 64 hdisk1
Sorry, user ktuser is not allowed to execute '/usr/sbin/mkvg -y datavg2 -s 64 hd
isk1' as root on ktaix28.
```

- We can see that **ktuser** was executing **mkuser** which was successful and he was restricted when trying to assign password using **passwd** command.
- Similarly, **ktuser** was executing **rmuser** which was successful and he was restricted when trying to execute **mkvg** command.

#### Command Aliases in the sudoers File:

- A command alias is a list of commands. They're labeled with the string Cmnd\_Alias. Here, we have an alias that includes all the commands necessary to create, change and remove user.  
Eg. **Cmnd\_Alias USERADMIN = /usr/bin/mkuser, /usr/bin/chuser, /usr/sbin/rmuser**
- Here **USERADMIN** is the alias name which contains set of commands i.e **mkuser**, **chuser** and **rmuser**.
- Let us add the same line in sudoers file.

```
# Host alias specification

# User alias specification

# Cmnd alias specification
Cmnd_Alias USERADMIN = /usr/bin/mkuser, /usr/bin/chuser, /usr/sbin/rmuser

# Defaults specification

# Runas alias specification

# User privilege specification
root    ALL=(ALL)  ALL
ktuser  ALL=(ALL)  USERADMIN
```

- Now let's login as ktuser, and try to execute the commands which were given in **USERADMIN** alias.

```
# su - ktuser
$ sudo mkuser user4
Password:
$
$ sudo passwd user4
Sorry, user ktuser is not allowed to execute '/usr/bin/passwd user4' as root on ktaix28.
```

- We can see that **ktuser** was trying to assign password for a newly created user **user4**, which was not executed.
- Reason: is that in the **USERADMIN** command alias the **passwd** command was not added as a list of commands.

#### User Aliases in the sudoers File:

- User aliases are groups of users from different groups, and are labeled with the string **User\_Alias**. They contain a list of users that are in that alias.  
Eg. **User\_Alias ADMINS = ktuser, ktuser2, ktuser3**
- Here **ADMINs** is the user\_alias name, which contains three users: **ktuser, ktuser2, ktuser3**.

```
# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the sudoers man page for the details on how to write a sudoers file.
#

# Host alias specification
User_Alias ADMINs = ktuser, ktuser2, ktuser3

# User alias specification

# Cmnd alias specification
Cmnd_Alias USERADMIN = /usr/bin/mkuser, /usr/bin/chuser, /usr/sbin/rmuser

# Defaults specification

# Runas alias specification

# User privilege specification
root    ALL=(ALL) ALL
ADMINs  ALL=(ALL) USERADMIN
```

- Now let's login as one of the user in **ADMINs** alias, and try to execute one of the commands in **USERADMIN** alias.

```

# su - ktuser2
$ 
$ sudo chuser pgrep=system user4
$ 
$ sudo passwd user4
Sorry, user ktuser2 is not allowed to execute '/usr/bin/passwd user4' as root on
ktaix28.

```

- Here now logged in as **ktuser2**, which was included in **ADMINS** alias and trying to execute **chuser** command which was successful and when trying to execute **passwd** command it was restricted.

#### LogFile for sudo users:

- To check the log of the commands executed by the sudo users, just add this line “**Defaults logfile=/var/log/sudo.log**” in sudoers file.

```

# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the sudoers man page for the details on how to write a sudoers file.
#
Defaults logfile=/var/log/sudo.log

# Host alias specification
User_Alias ADMINS = ktuser, ktuser2, ktuser3

# User alias specification

# Cmnd alias specification
Cmnd_Alias USERADMIN = /usr/bin/mkuser, /usr/bin/chuser, /usr/sbin/rmuser

# Defaults specification

# Runas alias specification

# User privilege specification
root    ALL=(ALL) ALL
ADMINS  ALL=(ALL) USERADMIN

```

- Now whatever commands that are executed by the sudo users, will be logged into **/var/log/sudo.log** file.

```

# cat /var/log/sudo.log
Apr 12 10:10:28 : ktuser2 : TTY=pts/1 ; PWD=/home/ktuser2 ; USER=root ;
COMMAND=/usr/bin/chuser pgrep=system user4
Apr 12 10:10:33 : ktuser2 : command not allowed ; TTY=pts/1 ; PWD=/home/ktuser2
; USER=root ; COMMAND=/usr/bin/passwd user4

```

- We can see the status of the commands (i.e whether the command is executed or not) that the sudo users are trying to execute by just opening the **/var/log/sudo.log** file.

## Secure Shell and Secure Copy:

### SSH Protocol:

- ↳ Two client programs:
    - ↳ ssh -> remote login, remote execution
    - ↳ scp -> remote copy
  - ↳ One server program: **sshd**
  - ↳ Uses encryption to protect data in transit
    - ↳ Support for various encryption methods
    - ↳ Sniffing attack no longer practical
  - ↳ Uses public key algorithms to authenticate server
    - ↳ Prevents against man-in-the-middle attack
  - ↳ Can use public key algorithms to authenticate user too
    - ↳ Account passwords no longer needed
- 
- ↳ A solution to the problems in the previous visual is the SSH protocol. It was invented by a Finnish company, not coincidentally called ssh. They submitted the protocol description to the IAB (Internet Architecture Board), where it now lives as an Internet Draft. This is an interim status in which standards can exist before an RFC number is assigned.
  - ↳ The SSH protocol provides you with all the capabilities mentioned before.
  - ↳ SSH uses strong encryption to encrypt the data in transit and to authenticate the client, the server and optionally the user as well. This prevents against sniffers and man-in-the-middle attacks and can also spare the user from the ordeal of having multiple passwords for all his accounts. A user is no longer authenticated based on his password but based on public key algorithms.
  - ↳ A typical SSH implementation consists of two client programs:
    - ↳ ssh, which is used for remote logins and remote command execution.
    - ↳ scp, which is used for remote copy.
  - ↳ In addition to this, you need to run a server program called sshd.
  - ↳ Both ssh and scp have the same syntax and capabilities as rsh and rcp. In fact, for ease of use, most ssh implementations offer replacements for rsh and rcp, which actually use the SSH protocol.

## Enabling SSH on AIX:

- ↳ Installation Filesets
  - ↳ openssh.base.client
  - ↳ openssh.base.server
  - ↳ openssh.license
- ↳ OpenSSH is included in the Base cd of aix, but it is not installed with OS. Therefore you need to install it separately, which is shown later in this chapter.

## Usage of ssh:

- ↳ Syntax: **ssh [options] [user@]hostname [command]**
- ↳ E.g. **ssh-l root ktaix16** (ip can also be used instead of hostname).
- ↳ Interprets command line options:
  - ↳ -c <cipher>: Encryption to be used (blowfish, 3des)
  - ↳ -p <port>: Remote port number
  - ↳ -P: Use local port > 1023
  - ↳ -C: Use compression
- ↳ Reads config file \$HOME/.ssh/config
- ↳ Reads config file /etc/ssh/ssh\_config
- ↳ Connects to hostname
- ↳ Asks password
- ↳ Executes command (optional)
- ↳ The ssh command allows you to remote login to a system, and optionally allows you to execute a command automatically. By default it tries to log you in using the same username as you are currently using, but this can be changed by specifying "user@hostname".

## Usage of Scp:

- ↳ Syntax: **scp [options] [sourcefile] ... [destinationfile]**
- ↳ E.g **scp root@ktaix16:/filename /filename**
- ↳ Copying a dir: **scp -r root@ktaix16:/dirname /dirname** (destination)
- ↳ Options:
  - ↳ -c <cipher>: Encryption to be used (blowfish, 3des)
  - ↳ -p: Preserve modification times and modes
  - ↳ -r: Recursively copy subdirectories
  - ↳ -C: Use compression
  - ↳ -P <port>: Remote port number
- ↳ Filenames specified as: [[user@]host:]filename

## Usage of sshd:

- ↳ Daemon process directly on port 22
  - ↳ Does not use inetd
- ↳ When started:
  - ↳ Read config from **/etc/ssh/sshd\_config**
  - ↳ Read host-specific RSA key from **/etc/ssh/ssh\_host\_key**
  - ↳ Create session-specific RSA key (never stored on disk)
- ↳ When a client connection is started:
  - ↳ Negotiate session key with client
  - ↳ Encrypt all communications with session key
  - ↳ Authenticate client
  - ↳ Log in, execute command or copy file/files
- ↳ The sshd daemon process should be running on the server. It is usually not run out of inetd, because it needs to generate an RSA key each time it starts, and this takes some seconds.

### ssh/sshd Host Authentication:

- ↳ Every sshd host needs to generate a host key pair
  - ↳ Private key stored in **/etc/ssh/ssh\_host\_key**
  - ↳ Public key stored in **/etc/ssh/ssh\_host\_key.pub**
- ↳ Upon first connection, the public key is transferred to the client
  - ↳ User gets warning: Unknown host. Accept (yes/no)?
  - ↳ When user accepts, public key stored in **\$HOME/.ssh/known\_hosts**
- ↳ Upon subsequent connections, keypairs verified
- ↳ When option StrictHostKeyChecking is set, you can only connect to hosts whose public key is stored in **/etc/ssh/known\_hosts** or **\$HOME/.ssh/known\_hosts**. Prevents against man-in-the-middle attack
- ↳ Every sshd host (server) needs to generate a host key pair. This was done at install time with the make host-key command. This key pair is stored in **/etc/ssh/ssh\_host\_key** (private key) and **/etc/ssh/ssh\_host\_key.pub** (public key).
- ↳ When a client first connects to the server, the public key of the host is transferred to the client. The client then gets a warning that this host is unknown, and is able to accept or not. When the user accepts, the public key is stored in **\$HOME/.ssh/known\_hosts**. Upon subsequent connections, the keypairs are verified and the user is warned if the keys don't match.

- When the StrictHostKeyChecking option is set either in \$HOME/.ssh/config or in /etc/ssh/ssh\_config, the user can only connect to hosts whose public key is stored in /etc/ssh/known\_hosts or \$HOME/.ssh/known\_hosts. This effectively prevents against man-in-the-middle attacks

## sshd User Authentication

- There are four methods which can be used for user authentication.
  - .rhost authentication (normally disabled)
    - Requires the hostname to be stored in .rhosts or /etc/hosts.equiv (insecure - vulnerable to IP spoofing)
  - .rhosts with RSA host authentication (normally disabled)
    - Requires the hostname to be stored in .rhosts or /etc/hosts.equiv and requires the client host to have the correct RSA certificate (fairly insecure - only authenticates host, not the user)
  - RSA challenge-response authentication
    - Requires the user to have the correct RSA key pair
  - Password based authentication
    - Requires the user to supply the correct password
- After host authentication, user authentication is done. This is a four step process:
  - The first step is to verify whether the hostname (possibly in combination with the username) is stored in \$HOME/.rhosts or /etc/hosts.equiv. This works exactly the same as rsh, rcp or rlogin and is considered very insecure. It is disabled by default.
  - The next step is .rhosts authentication combined with RSA authentication. This is considered fairly insecure and normally disabled.
  - The third step is RSA challenge-response authentication. This basically comes down to the fact that the user has to have the correct RSA key pair to be able to login. This is pretty secure, arguably more secure than password authentication. The user needs to set it up though.
  - The last step is password based authentication. Most implementations of SSH will also check for the existence of /etc/hosts.equiv and \$HOME/.rhosts in addition to /etc/hosts.equiv and \$HOME/.rhosts in the first two steps.

## RSA Challenge-Response Authentication

- ↳ User generates RSA keypair on client with **ssh-keygen -t rsa**
  - ↳ Private key stored in **/.ssh/id\_rsa**
  - ↳ Public key stored in **/.ssh/id\_rsa.pub**
- ↳ Can be protected with passphrase
- ↳ Can contain comment
- ↳ Transfers public key to server and adds it to
  - ↳ **\$/ssh/authorized\_keys**
- ↳ By Creating above file in second machine, and copying id\_rsa.pub of first server in second machine User Can login without password. Ref SSH configuring and ssh keygen chapter.
- ↳ RSA Challenge-Response Authentication requires each user to generate a keypair on the client host with the ssh-keygen command. This command then stores the private key in \$HOME/.ssh/identity and the public key in \$HOME/.ssh/identity.pub. The usage of this key can be protected with a passphrase (so the system administrator cannot use them)
- ↳ The user then transfers the public key to the server and adds it to \$HOME/.ssh/authorized\_keys. After that, the user can login without needing to supply a password to authenticate itself. (Note however that if the key is protected with a passphrase, he still has to type that one.)
- ↳ The advantage of this scheme is that a user is no longer required to authenticate himself to a server using a password, but is authenticated based on public key algorithms. This greatly simplifies account administration, both for the user and the system administrator. The only drawback is that the users private key has to be kept secret. That's why this key is usually protected with a passphrase.

## DSA Challenge-Response Authentication

- ↳ SSH Protocol Version 2 can use DSA instead of RSA
- ↳ To generate a DSA key, use **ssh-keygen -t dsa**
  - ↳ Private key stored in **\$/ssh/id\_dsa**
  - ↳ Public key stored in **\$/ssh/id\_dsa.pub**
- ↳ Transfers public key to server and add it to  
**\$HOME/.ssh/authorized\_keys2**  
**Note:** Create the above file and copy the id\_dsa.pub as done in RSA authentication.
- ↳ User can then login without password

## **Protecting Your Private Key**

- ↳ Anyone who can use your private key (identity or id\_dsa) can login to any system where you are authorized
  - ↳ Important to password-protect your private key
  - ↳ Disadvantage: Need to type password every time the key is used
- 
- ↳ Solution:
    - ↳ ssh-agent is a client-side daemon who retains unlocked private keys in memory and activates them when one of its child processes needs it.
    - ↳ ssh-add manages the private keys that are retained in memory by ssh-agent.
      - ↳ Use ssh-add [<filename>] to add a key
      - ↳ Use ssh-add -l to list all keys
      - ↳ Use ssh-add -d [<filename>] to remove a key
- 
- ↳ The ssh-agent client-side daemon retains all unlocked private keys in its memory space, and activates them when one of its client processes needs them. This means that the ssh-agent has to be started as the parent process of all shells and other programs that make use of it.
  - ↳ There are two methods of starting ssh-agent:
    - ↳ First, you can start ssh-agent in a regular shell with the command ssh-agent bash. This will start ssh-agent, and will start a bash shell as its child. Any commands typed in this shell will, if necessary, use ssh-agent.
    - ↳ Second, you can integrate ssh-agent into the startup scripts of X. This means that if you login via xdm, ssh-agent is started automatically and will serve the needs of any X client that you start.
  - ↳ When ssh-agent has been started properly, you also need to unlock and upload your private keys. This is done with the ssh-add command.

## **SSH INSTALLATION:-**

- ↳ Step1:- Install Open ssh in the same passion that of bash
- ↳ If it is in tar.Z format run # gunzip filename.tar.Z - it will remove .Z from the file
- ↳ Then do #tar -xvf filename - to untar the file.

```
openssh_5.2p1_aix61.tar.Z
# gunzip openssh_5.2p1_aix61.tar.Z
# tar -xvf openssh_5.2p1_aix61.tar
```

Install it from current dir as done for bash and select the following

```
Install Software

Type-----  
Pr|           SOFTWARE to install  
|  
[T] Move cursor to desired item and press F7. Use arrow keys to scroll.  
*   ONE OR MORE items can be selected.  
*   Press Enter AFTER making all selections.  
  
> openssh.base          ALL  
+ 5.2.0.5300  Open Secure Shell Commands  
+ 5.2.0.5300  Open Secure Shell Server  
  
> openssh.license        ALL  
+ 5.2.0.5300  Open Secure Shell License  
  
> openssh.man.en US      ALL  
+ 5.2.0.5300  Open Secure Shell Documentation - U.S. English
```

```
Install Software

Type or select values in entry fields.  
Press Enter AFTER making all desired changes.

[TOP]                                     [Entry Fields]  
* INPUT device / directory for software .  
* SOFTWARE to install [openssh.base] >  
  PREVIEW only? (install operation will NOT occur)  
  COMMIT software updates?  
  SAVE replaced files?  
  AUTOMATICALLY install requisite software?  
  EXTEND file systems if space needed?  
  OVERWRITE same or newer versions?  
  VERIFY install and check file sizes?  
  Include corresponding LANGUAGE filesets?  
  DETAILED output?  
  Process multiple volumes?  
  ACCEPT new license agreements? [yes]
```

Procedure for password free login between two servers:-

**Step1:** Generate the ssh keys with following command which will be used for

Password free login

#ssh-keygen -t rsa - don't type any filename and passphrase just press enter  
To ignore it and you will be seeing output as follows.

```

# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (//.ssh/id_rsa):
Created directory ' //.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in // .ssh / id _ rsa .
Your public key has been saved in // .ssh / id _ rsa . pub .
The key fingerprint is:
65:0b:01:fe:f1:45:ff:87:27:f2:d3:eb:b5:01:47:6b root@ktaix33
The key's randomart image is:
+-- [ RSA 2048 ] --+
|   . . . |
|   . . . |
|   . o o . . |
|   . * o . o .|
|   S o ..oE+|
|       o++ .|
|       o.o |
|       .= |
|       .+ |
+-----+
#

```

- ☞ **Step2:-** As a result of key generation a dir (.ssh) will be created under root (/) Containing two files as follows.

```

# cd .ssh
# ls
id_rsa      id_rsa.pub
#

```

- ☞ **Step3:-** Generate the keys on ther ssh installed server.

- ☞ **Step4:-** On first server copy the **id\_rsa.pub** key as follows

```

id_rsa      id_rsa.pub
# pg id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA2pmI2zG1YK8pLA+QpLyNUZofWzkp5z9YXofNbyTii99o
QnDj9kdubGdh2cMV3oWZBQsSIG12aiYNDv7/KFVItim+VyCeBVBA6ShMyjE96TU8UN6LUkyRBFC11dOi
TXsrqX5TrOCzf8rI66VnWD1bKVcvB1VA8tcGIUKhh/AFAHsTC/qSIV60XGN7YU5GRPBqcA2oaIIrIPgV
xpAgtJz/+3eL8sVcl0tO2XoANfCRSlxXRnHsW5igOHyzWAEWeqrTZ+3uP1zmKHC/Oof4pzgJp+fZ6Eqx
Wn6Svh2yy5fWwcmW3FD5rKf13TGabQRNwpPNvL6n9JRXHIsclIqoPD/4Q== root@ktaix33
(EOF) :

```

- ☞ **Step 4:-** On second Server side under .ssh dir create a file named as “**authorized\_keys**” and paste the **id\_rsa.pub** key here.

```

# cd .ssh
# ls
id_rsa      id_rsa.pub
# vi authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA2pmI2zG1YK8pLA+QpLyNUZofWzkp5z9YXofNbyTii99o
QnDj9kdubGdh2cMV3oWZBQsSIG12aiYNDv7/KFVItim+VyCeBVBA6ShMyjE96TU8UN6LUkyRBFC11dOi
TXsrqX5TrOCzf8rI66VnWD1bKVcvB1VA8tcGIUKhh/AFAHsTC/qSIV60XGN7YU5GRPBqcA2oaIIrIPgV
xpAgtJz/+3eL8sVcl0tO2XoANfCRSlxXRnHsW5igOHyzWAEWeqrTZ+3uP1zmKHC/Oof4pzgJp+fZ6Eqx
Wn6Svh2yy5fWwcmW3FD5rKf13TGabQRNwpPNvL6n9JRXHIsclIqoPD/4Q== root@ktaix33

```

- ☞ **Step 5:-** Now try to login from 1<sup>st</sup> server into the 2<sup>nd</sup> Server by following command

☞ #ssh -l root 192.168.10.31 - (assuming the other server's ip is 192.168.10.31)

- ☞ **Note:-** For first time it may ask permission type yes and continue, it will not Prompt for the password.

## Role Based Access Control

- AIX V6 introduces Enhanced RBAC, which is a method to delegate roles and authorizations among one or more general user accounts.
- RBAC provides the system administrator with the ability to designate tasks to general users that traditionally would be performed by the root user, or through setuid/setgid.
- One benefit of RBAC is the minimizing of the use of the setuid/setgid programs by restricting the privileges assigned to a command to only those privileges that the command needs to execute its task.
- There is no specific install package in AIX V6 for either Legacy or Enhanced Mode RBAC. The majority of the Enhanced RBAC commands are included in the bos.rte.security fileset.

### **Authorizations**

- In Enhanced RBAC, an authorization is a text string associated with security related functions or commands. Authorizations provide a mechanism to grant rights to users to perform privileged actions and to provide different levels of functionality to different classes of users. Authorizations are assigned to roles, which may then be assigned to user.
- When a command that is governed by an authorization is executed, access is only granted if the invoking user has the required authorization. For this reason, an authorization can be thought of as a key that is able to unlock one or more commands.

### **Roles**

- Roles are the mechanism used to assign authorizations to a user and to group a set of system administration tasks together. An AIX® role is primarily a container for a collection of authorizations.
- Assigning a role to a user allows the user to access the role and use the authorizations that are contained in the role. A system administrator can assign a role to multiple users and can assign multiple roles to a user. A user who has been assigned multiple roles can activate more than one role (**up to a maximum of eight roles**) simultaneously if necessary to perform system management functions.
- AIX provides a set of predefined roles for system management. However it is expected that customers will need to create their own custom roles or modify the existing predefined roles. Several role-management commands are available to list, create, modify, and remove AIX roles. Roles can be created with the [mkrole](#) command, modified with the [chrole](#) command, removed with the [rmrole](#) command, and displayed with the [lsrole](#) command.

**When creating a new AIX role, consider the following issues:**

- What will be the name of the role?
- The role name is a text string, but should provide some insight into the role's capabilities. Role names can contain a maximum of 63 printable characters.
- What authorizations are required for the role? Consider whether authorizations should be directly assigned to the role or indirectly assigned to the role through a sub-role.
- Should the user be required to authenticate when activating the role?

**Predefined enhanced RBAC roles**

- A predefined set of roles is defined in the local role database (`/etc/security/roles`) on the new AIX® Version 6.1 and later installation. This set of roles is intended to group typical administrative responsibilities.

<b>Role Name</b>	<b>Role Description</b>
<b>Isso</b>	The ISSO role is responsible for creating and assigning roles and is thus the most powerful user-defined role on the system. Some of the ISSO responsibilities include: <ul style="list-style-type: none"><li>- Establishing and maintaining security policy</li><li>- Setting passwords for users</li><li>- Network configuration</li><li>- Device administration</li></ul>
<b>Sa</b>	The SA role provides the functionality for daily administration and is responsible for: <ul style="list-style-type: none"><li>- User administration (except password setting)</li><li>- File system administration</li><li>- Software installation update</li><li>- Network daemon management</li><li>- Device allocation</li></ul>
<b>So</b>	The SO role provides the functionality for day to day operations and is responsible for: <ul style="list-style-type: none"><li>- System shutdown and reboot</li><li>- File system backup, restore, and quotas</li><li>- System error logging, trace, and statistics</li><li>- Workload administration</li></ul>
<b>AccountAdmin</b>	The AccountAdmin role provides the functionality for users and group definitions and is responsible for: <ul style="list-style-type: none"><li>- Define, modify and remove users</li><li>- Define modify and remove groups</li></ul>
<b>BackupRestore</b>	The BackupRestore role provides the functionality for backup and restore operations for file systems using various commands such as: <ul style="list-style-type: none"><li>- cpio, pax, tar, backup and restore</li></ul>
<b>DomainAdmin</b>	The DomainAdmin role provides the functionality for managing network security mechanisms such as: <ul style="list-style-type: none"><li>- kerberos, ldap, NIS, and PKI</li></ul>

<b>FSAdmin</b>	The FSAdmin role provides the functionality for managing file systems and has the ability to: <ul style="list-style-type: none"> <li>- Create, modify and remove file systems</li> <li>- Mount and unmount file systems</li> <li>- Defrag file systems</li> <li>- Format file system logs</li> <li>- Manage file system user quotas</li> <li>- Create and manage JFS2 snapshots</li> </ul>
<b>SecPolicy</b>	The SecPolicy role provides the functionality for security administration and is responsible for most of what the ISSO covers, except for: <ul style="list-style-type: none"> <li>- Domain Administration</li> <li>- System Configuration</li> </ul>
<b>SysBoot</b>	The SysBoot role provides the functionality system shutdown and booting via the facilities for: <ul style="list-style-type: none"> <li>- halt, shutdown, and reboot</li> </ul>
<b>SysConfig</b>	The SysConfig role provides the functionality for system configuration and is responsible for such components as: <ul style="list-style-type: none"> <li>- inittab</li> <li>- System console</li> <li>- Kernel extensions</li> <li>- uname</li> <li>- Resource sets</li> <li>- Date and time zone</li> <li>- Software license management</li> <li>- Performance tunables</li> <li>- Diagnostics</li> </ul>

#### Configuring the RBAC operating mode:

- As discussed, when AIX V6 is installed, RBAC is, by default, activated in Enhanced Mode.
- To determine the current mode in which RBAC is operating, display the enhanced\_RBAC mode of the sys0 resource.

Display the currently active RBAC mode using the **lsattr** command and the sys0 resource.

```
# lsattr -El sys0 -a enhanced_RBAC
enhanced RBAC true Enhanced RBAC Mode True
```

#### Planning for user defined roles:

- The predefined roles are provided as a suggested means of dividing administrative duties.
- The predefined roles may be modified or removed, and new roles may be created as deemed suitable for the individual environment.
- While these predefined roles may be suitable for many administrative needs, there may be instances where a further, more granular separation of duties is required. In such instances, Enhanced RBAC allows for the creation of user defined roles.

When creating a user defined role, consideration should be given to the following points:

**The name of the role:** The name of the role should include some description or insight into the capabilities of the role. Role names are limited to 63 printable characters.

**Authorizations:** Consider which authorizations should be assigned to the role.

**Subroles:** Consider whether the role should contain subroles. Subroles are a convenient way of assigning one or more pre-existing roles to a user defined role.

**Authentication:** Should the user be required to authenticate when assuming the role through the **swrole** command.

#### To create a user defined role:

- First we need to find out what are the authorizations that we want to include in our role.
- So in order to find out the authorizations, first we need to find out the complete path of the commands which we want to include in the role.
- Here let's include three commands i.e **mkuser**, **chuser** and **rmuser** in the role.
- Complete path for these three commands can be achieved through a command "which command"

Eg. #which mkuser

Similarly find out the path for the remaining two commands, as shown below.

```
# which mkuser  
/usr/bin/mkuser  
# which rmuser  
/usr/sbin/rmuser  
# which chuser  
/usr/bin/chuser
```

- After finding out the complete path, now it is time for us to find out the authorizations for the above commands.
- The authorizations can be found using a command "**Issecattr -c -F complete path of command**"

Eg. Issecattr -c -F /usr/bin/mksuser

```

# lssecattr -c -F /usr/bin/mkuser
/usr/bin/mkuser:
  euid=0
  egid=7
  accessauths=aix.security.user.create.admin,aix.security.user.create.normal
  innateprivs=PV_AU_ADD,PV_AU_ADMIN,PV_AU_PROC,PV_AZ_ROOT,PV_DAC_O,PV_DAC_R,
PV_DAC_W,PV_DAC_X,PV_DEV_LOAD,PV_DEV_QUERY,PV_FS_CHOWN,PV_KER_ACCT,PV_NET_CNTL,PV_
NET_PORT,PV_PROC_CRED,PV_PROC_ENV,PV_PROC_PRIO,PV_PROC_PRIV,PV_PROC_RAC,PV_PROC_RS
ET,PV_PROC_RTCLK,PV_PROC_SIG,PV_PROC_VARS,PV_TCB
  inheritprivs=PV_DAC_O,PV_DAC_W,PV_FS_CHOWN,PV_TCB
  secflags=FSF_EPS

# lssecattr -c -F /usr/sbin/rmuser
/usr/sbin/rmuser:
  accessauths=aix.security.user.remove
  innateprivs=PV_AU_ADD,PV_AU_ADMIN,PV_AU_PROC,PV_AZ_CHECK,PV_DAC_O,PV_DAC_R
,PV_DAC_W,PV_DAC_X,PV_DEV_LOAD,PV_DEV_QUERY
  secflags=FSF_EPS

# lssecattr -c -F /usr/bin/chuser
/usr/bin/chuser:
  euid=0
  egid=0
  accessauths=aix.security.user.change
  innateprivs=PV_AU_ADD,PV_AU_ADMIN,PV_AU_PROC,PV_DAC_R,PV_DAC_W,PV_DAC_X,PV
_DEV_LOAD,PV_DEV_QUERY
  secflags=FSF_EPS

```

- Similarly find out authorizations for the other two commands.
- Now take down the authorization information through the option **accessauths**, which is also highlighted in the above.

As we have got the authorization information for all the commands, let's create our own role.

# smit rbac

→ Roles

→ Add a role

#### Add a Role

Type or select values in entry fields.  
Press Enter AFTER making all desired changes.

\* Role NAME  
Role ID  
AUTHORIZATIONS  
Role LIST  
GROUPS  
SMIT SCREENS  
VISIBILITY  
Message CATALOG  
Message SET  
Message NUMBER  
Description

[Entry Fields]  
[USERADMIN]  
[] #  
[aix.security.user.change] +  
[] +  
[] +  
[] +  
[1] +#  
[] #  
[] #  
[user can create, remove] #

- The user defined role “**USERADMIN**” has now been defined.
- The role name here we have mentioned as “**USERADMIN**” and in the “**AUTHORIZATIONS**” field, mention whatever authorizations we have collected earlier.

### Update the Kernel Security Tables:

- When operating in Enhanced RBAC mode, authorization and privilege checks are performed in the AIX kernel. If an addition or modification is made to the RBAC role table, then this requires that the RBAC security database be updated into the AIX kernel before the modifications are available for use.
- AIX V6 and Enhanced RBAC introduces the **setkst** command to update the RBAC tables into the AIX kernel.
- The **setkst** command reads the RBAC security database files and loads the information from the database files into the Kernel Security Tables (KST). By default, all the security databases are sent to the KST.

```
# setkst
Successfully updated the Kernel Authorization Table.
Successfully updated the Kernel Role Table.
Successfully updated the Kernel Command Table.
Successfully updated the Kernel Device Table.
```

**Note:** A role may be assigned to a user without an update to the KST. The role will not be available to the user until updated to the KST.

- We use the **lsrole** command to list the **USERADMIN** role. The role contains only the aix.security.user.change, aix.security.user.create.admin, aix.security.user.create.normal, aix.security.user.remove authorizations.

### #lsrole -f rolename

```
# lsrole -f USERADMIN
USERADMIN:
    authorizations=aix.security.user.change,aix.security.user.create.admin,aix
    .security.user.create.normal,aix.security.user.remove
    rolelist=
    groups=
    visibility=1
    screens=*
    dfltmsg=user can create, remove and delete users
    msgcat=
    auth_mode=INVOKER
    id=13
```

- Now let's create a new user and assign the role to the user.
- A user **ktuser1** was created and assigning the role to the ktuser1.
- Shows the **lsuser** command output prior to the **USERADMIN** role being assigned to the ktuser1 user. The ktuser1 user currently has the no role assigned.
- RBAC roles may be assigned with the **chuser** command.

```
# mkuser ktuser1
# passwd ktuser1
Changing password for "ktuser1"
ktuser1's New password:
Re-enter ktuser1's new password:
#
# lsuser -a roles ktuser1
ktuser1 roles=
# chuser roles=USERADMIN ktuser1
```

```
# lsuser -a roles ktuser1  
ktuser1 roles=USERADMIN
```

- By default, a role is not active until the user logs into the system and activates the role with the **swrole** command. If the **ktuser1** user were to execute the **mkuser** command without activating the **USERADMIN** role, the **mkuser** command would attempt to execute as the **ktuser1** user.
- When **ktuser1** was trying to execute **mkuser**, **chuser** or **rmuser** commands, he was restricted because he needs to activate the role using **swrole** command.

```
# su - ktuser1  
$  
$ mkuser user1  
ksh: mkuser: cannot execute  
$ rmuser  
ksh: rmuser: cannot execute  
$ chuser  
ksh: chuser: cannot execute
```

- The **rolelist -a** command can be used to list the assigned roles to the user but they may not be effective.

```
$ rolelist -a  
USERADMIN      aix.security.user.change  
                  aix.security.user.create.admin  
                  aix.security.user.create.normal  
                  aix.security.user.remove
```

- The **rolelist -e** command can be used to list the effective role and authorizations.
- Which currently says that the user has no active role.

```
$ rolelist -e  
rolelist: There is no active role set.
```

- To activate a role, we use the **swrole** command.
- The **swrole** command will start a new role-session shell that will require that the user authenticate with their password.
- Once the password is authenticated, the role will be active and commands that are included in the authorizations defined to the role will be executed as privileged commands.
- Once the **USERADMIN** role is active, the **rolelist -e** command can be used to list the effective role and authorizations.

```
$ swrole USERADMIN  
ktuser1's Password:  
$  
$ rolelist -e  
USERADMIN      user can create, remove and delete users
```

- The **ktuser1** user now has the **USERADMIN** role active and may execute the **mkuser**, **chuser** and **rmuser** commands.

```
$ mkuser user1
$ passwd user1
You are not authorized to change "user1's" password.
$
$ lsuser -a pgrp user1
user1 pgrp=staff
$
$ chuser pgrp=system user1
$
$ lsuser -a pgrp user1
user1 pgrp=system
```

## Backup and Restore

- ◀ The data on a computer is usually far more important and expensive to replace than the machine itself. Many companies have gone out of business because they did not plan for disaster recovery.
- ◀ Backup to tape is the cheapest alternative but a duplicate disk or complete system would also provide protection and fast recovery from a disaster. Backups should be taken before installing/maintaining hardware/software, in case a disk or files accidentally get damaged.
- ◀ Backups are not just used for disaster recovery. One way of transferring a number of files from one machine to another is to back those files up to diskette, tape or a file on disk and then transfer that backup media to another machine.
- ◀ When reorganizing the file systems on the disk you need to backup file systems so that they can be deleted and moved to another location.

### Types of Backup:

- ◀ **System backup:**  
The system backup (system image backup) records and preserves all system data, including logical volume inter/intra allocation policies, striping, file system setup (nbpi, compression, fragment size) and paging setup.
- ◀ **Full backup**  
A full backup is similar to a system backup, but it is for user data.
- ◀ **Incremental backup**  
There are two types of incremental backups:
  - ◀ The first method is to do a full backup. For example, do a full backup on Sunday, and then for the rest of the week, only backup the changes from the previous day. This method has the advantage of being quick, but there are a lot of tapes involved. Should one of the tapes be missing, you may have problems restoring using the remaining tapes.
  - ◀ The second method again involves taking a full backup on Sunday. However, the other days of the week backup only the changes made since the full backup; that is, since Sunday. The backups take slightly longer than the previous method, and towards the end of the week, if most of your system has changed, then the time taken is similar to a full backup. The restoration procedure does not depend on the tape from the previous day.

## **Methods of Backup:**

### **Mksysb:**

- ↳ Creates a complete backup of **rootvg**.
- ↳ If image is saved to tape, the tape is bootable and can be used to completely clone the machine.
- ↳ If you need to restore a mksysb image to a machine of a different architecture than the one you made the image on, you must use a special clone disk.
- ↳ You can also set up a NIM (Network Installation Management) server for network installs.

### **Alternate Disk**

- ↳ Cloning the **rootvg** to an alternate disk can have many advantages. One advantage is having an online backup available, in case of a disaster. Another benefit of **rootvg** cloning is in applying new maintenance levels or updates. A copy of the **rootvg** is made to an alternate disk, then a maintenance level is installed on the copy. The system runs uninterrupted during this time. When it is rebooted, the system will boot from the newly updated **rootvg** for testing. If the maintenance level causes problems, the old **rootvg** can be retrieved by simply resetting the **boot** list and rebooting.

### **Rootvg Mirroring:**

- ↳ If your **rootvg** is on one disk, you get a **single point of failure**; that means, if this disk fails, your machine is not available any longer.
- ↳ If you mirror **rootvg** to a second (or third) disk, and one disk fails, there will be another disk that contains the mirrored **rootvg**. You increase the availability of your system.

**NOTE:** In realtime alerts will be generated and automated. Ticket will be raised for backup failure. Raise a ticket for backup failure. Resolve the issue and close the ticket.

## **Lab Activities:**

### **Mksysb backup:**

1. How to take mksysb backup from rootvg in a file system?

↳ **Step1:** Make a filesystem of atleast 4GB as shown below.

In order to create a filesystem, we need to create a logical volume of 4GB.

check the pp size of volume group in which you are creating lv by

#lsvg volumegroup name

```
# lsvg rootvg
VOLUME GROUP:          rootvg
VG STATE:              active
VG PERMISSION:         read/write
MAX LVs:               256
LVs:                   18
OPEN LVs:              9
TOTAL PVs:             1
STALE PVs:             0
ACTIVE PVs:            1
MAX PPs per VG:        32512
MAX PPs per PV:         1016
LTG size (Dynamic):   256 kilobyte(s)
HOT SPARE:             no
VG IDENTIFIER:         0009506c00004c000000012ec7a2b2dc
PP SIZE:               64 megabyte(s)
TOTAL PPs:              548 (35072 megabytes)
FREE PPs:               447 (28608 megabytes)
USED PPs:               101 (6464 megabytes)
QUORUM:                 2
VG DESCRIPTORS:         2
STALE PPs:              0
AUTO ON:                yes
MAX PVs:                32
AUTO SYNC:              no
BB POLICY:              relocatable
```

#Create a logical volume of 4 GB as per the calculation

4X1024/64 = 64. Now create an lv with 64 pp's

```
#mklv -y backuplv -t jfs2 rootvg 64 - (The same can be done using smitty also ref LVM )
```

Now create a filesystem on top of backuplv

```
#crfs -v jfs2 -d backuplv -m /ktbkp
# crfs -v jfs2 -d backuplv -m /ktbkp
File system created successfully.
4193972 kilobytes total disk space.
New File System size is 8388608
```

**Step2:** Now mount the mount point as following.

```
#mount /ktbkp
```

Check the size of the filesystem by using

```
#df -g
```

**Step3:** Now get into your directory i.e. /ktbkp and create an empty file where you will be taking mksysb backup.

```

# cd /ktbkp
# ls
lost+found
# touch aix6.1_mksysb
# ls
aix6.1_mksysb  lost+found
#

```

**Step 4:** Use smitty or command line to take mksysb.

#### Using smitty:

```

#smitty mksysb
                                         Back Up the System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]

WARNING: Execution of the mksysb command will
          result in the loss of all material
          previously stored on the selected
          output medium. This command backs
          up only rootvg volume group.

* Backup DEVICE or FILE
  Create MAP files?                                     [/ktbkp/aix6.1_mksysb]
  no
  yes
  yes
  yes
  no
  yes
  no
  yes
  []

```

#### Using command line:

#mksysb -ie /ktbkp/aix6.1\_mksysb - (if you want to see the processing add “v” with “ie” i.e. ive)

#### 2. Take a backup of a normal vg using savevg command.

- ↳ **Step1:** Create a filesystem on a different vg mostly rootvg is preferred for such task. Also create a file under your filesystem where you want to take the backup of the vg as shown below.

```

# mklv -y savelv -t jfs2 rootvg 10
savelv
# crfs -v jfs2 -d savelv -m /ktsave
File system created successfully.
655136 kilobytes total disk space.
New File System size is 1310720
# mount /ktsave
# cd /ktsave
# ls
lost+found
# touch ktvg bkp

```

**Step2:** Now take the backup of the vg either by using smitty or command line

#### Using smitty:

[Entry Fields]	
DEVICE or FILE	/ktsave/ktvg bkp
VOLUME GROUP	ktvg
BACKUP ONLY	no

Type or select values in entry fields.  
Press Enter AFTER making all desired changes.

[MORE...5]

\* Backup DEVICE or FILE  
\* VOLUME GROUP to back up  
List files as they are backed up?  
Generate new vg.data file?  
Create MAP files?  
EXCLUDE files?  
EXPAND /tmp if needed?  
Disable software packing of backup?  
Backup extended attributes?  
Number of BLOCKS to write in a single output  
(Leave blank to use a system default)  
Verify readability if tape device?  
Back up Volume Group information files only?

[TOP] [BOTTOM]

#### Using Command line:

```
#savevg -iv -f /ktsave/ktvg_bkp ktvg
```

### 3. Restore a Normal VG.

↳ **Step1:** Create a vg say ktvg and also create an lv and filesystem on top of it.

```
#mkvg -y ktvg -s 32 hdisk1
```

```
#mklv -y ktlv -t jfs2 ktvg 10
```

```
#crfs -v jfs2 -d ktlv -m /kt
```

Mount the files system and store some data in the folder i.e. /kt.

```
# ls
# mount /kt
# cd /kt
# ls
lost+found
# touch 1 2 3 4 5 6 7 8 9 10
# ls
1          2          4          6          8          lost+found
10         3          5          7          9
```

**Step 2:** Make another VG, LV, Filesystem, and mount it, make a file under it to take backup of first vg i.e. ktvg

```
# mkvg -y backupvg -s 32 hdisk2
# mklv -y backuplv -t jfs2 backupvg 20
backuplv
# crfs -v jfs2 -d backuplv -m /backup
File system created successfully.
655136 kilobytes total disk space.
New File System size is 1310720
# mount /backup
# cd /backup
# touch ktvg_backup
# ls
ktvg_backup  lost+found
```

**Step 3:** Create the backup for ktvg under ktvg\_backup

```
# savevg -f /backup/ktvg_backup ktvg
Creating list of files to back up.
Backing up 6 files
6 of 6 files (100%)
0512-038 savevg: Backup Completed Successfully.
```

**Step 4:** Now delete ktvg and restore it as shown below.

```
# umount /kt
# reducevg -df ktvg hdisk1
rmlv: Logical volume loglv01 is removed.
rmlv: Logical volume ktlv is removed.
ldeletepv: Volume Group deleted since it contains no physical volumes.
```

#### Creation of Alternate disk :

4. Create an Alt disk and set it as first boot disk in boot list.

↳ **Step1:** For making an Alt disk you should have a disk whose size is at least equal to or greater than hdisk0. First check the size of hdisk0 and the disk you want to make Alt disk.

```
#bootinfo -s hdisk0
```

```
#bootinfo -s hdisk1
```

```
# bootinfo -s hdisk0  
35074  
# bootinfo -s hdisk1  
35074
```

if it matches then run the following command to make an Alt disk.

```
#alt_disk_install -BC hdisk1
```

```
# alt_disk_install -BC hdisk1  
+-----+  
ATTENTION: calling new module /usr/sbin/alt_disk_copy. Please see the alt_disk_copy man page  
and documentation for more details.  
Executing command: {/usr/sbin/alt_disk_copy -B -d "hdisk1"}  
+-----+  
Calling mkszfile to create new /image.data file.  
Checking disk sizes.  
Creating cloned rootvg volume group and associated logical volumes.  
Creating logical volume alt_hd5  
Creating logical volume alt_hd6  
Creating logical volume alt_hd8  
Creating logical volume alt_hd4  
Creating logical volume alt_hd2  
Creating logical volume alt_hd9var  
Creating logical volume alt_hd3  
Creating logical volume alt_hd10opt  
Creating logical volume alt_dump_pri  
Creating logical volume alt_dump_sec  
Creating logical volume alt_moto_dump  
Creating logical volume alt_moto_dump2  
Creating /alt_inst/ file system.  
Creating /alt_inst/opt file system.  
Creating /alt_inst/tmp file system.  
Creating /alt_inst/usr file system.  
Creating /alt_inst/var file system.
```

**Step2:** Once the task gets completed change the bootlist to hdisk1 hdisk0 as shown below

```
# bootlist -m normal -o  
hdisk0 blv=hd5  
# bootlist -m normal hdisk1 hdisk0  
# bootlist -m normal -o  
hdisk1 blv=hd5  
hdisk0 blv=hd5
```

To wake up the Alt disk use the following command.

```
#alt_disk_install -W hdisk1
```

To make the Alt disk sleep use the following command.

```
#alt_disk_install -S hdisk1
```

To Delete the Alt disk from the system use the following command.

```
#alt_disk_install -X (name of the disk is not required)
```

5. Make a mirror copy of rootvg and boot the server with the mirrored vg and unmirror it.

↳ **Step1:** extend rootvg with a disk which is having same size that of hdisk0.

```
# bootinfo -s hdisk0  
35074  
# bootinfo -s hdisk1  
35074
```

#extendvg rootvg hdisk1

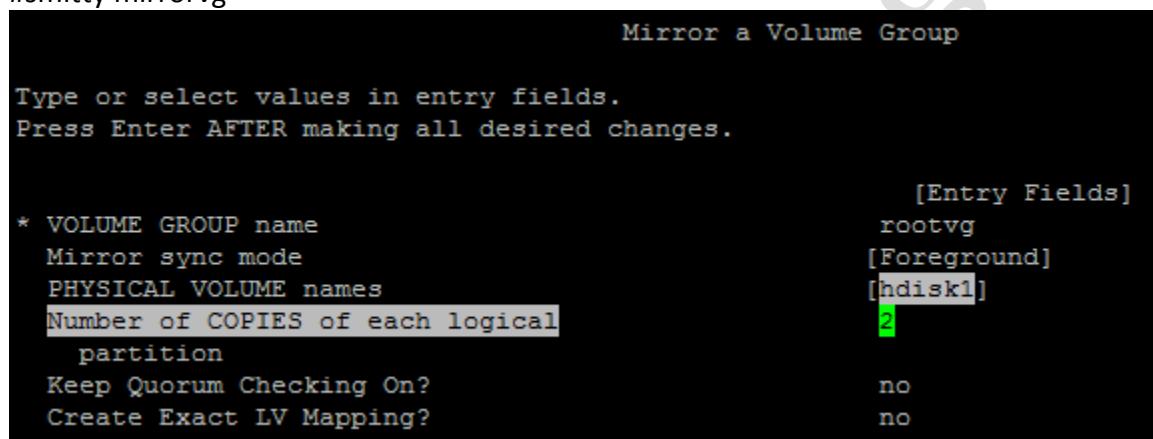
**Step2:** mirroring can be done either by command line or smitty.

**Command Line:**

```
#mirrorvg rootvg hdisk1
```

**Smitty:**

```
#smitty mirrorvg
```



**Note:** check the bootlist and change it back to hdisk0

```
COMMAND STATUS

Command: running      stdout: yes      stderr: no

Before command completion, additional instructions may appear below.

0516-1124 mirrorvg: Quorum requirement turned off, reboot system for this
                      to take effect for rootvg.
0516-1126 mirrorvg: rootvg successfully mirrored, user should perform
                      bosboot of system to initialize boot records. Then, user must modify
                      bootlist to include: hdisk0 hdisk1.

COMMAND STATUS

Command: OK      stdout: yes      stderr: no

Before command completion, additional instructions may appear below.

0516-1124 mirrorvg: Quorum requirement turned off, reboot system for this
                      to take effect for rootvg.
0516-1126 mirrorvg: rootvg successfully mirrored, user should perform
                      bosboot of system to initialize boot records. Then, user must modify
                      bootlist to include: hdisk0 hdisk1.
```

**Step3:** Now add the boot image to the mirrored disk.

```
#bosboot -ad hdisk1
```

```
# bosboot -ad hdisk1  
bosboot: Boot image is 18484 512 byte blocks.  
#
```

**Change the bootlist to hdisk1 hdisk0 and reboot the server.**

```
#bootlist -m normal hdisk1 hdisk0
```

#### Unmirroring rootvg:

**Command line unmirroring:**

```
#unmirrorvg rootvg hdisk1
```

#### Unmirroring via Smitty:

```
#smitty unmirrorvg - (and select the following)
```

```
Unmirror a Volume Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
* VOLUME GROUP name          rootvg
  PHYSICAL VOLUME names      [hdisk1] +
  Number of COPIES of each logical partition      1 +
```

```
COMMAND STATUS

Command: OK      stdout: yes      stderr: no

Before command completion, additional instructions may appear below.

0516-1246 rmlvcopy: If hd5 is the boot logical volume, please run 'chpv -c <disk name>'  
as root user to clear the boot record and avoid a potential boot off an old boot image that may reside on the disk from which this logical volume is moved/removed.  
0516-1132 unmirrorvg: Quorum requirement turned on, reboot system for this to take effect for rootvg.  
0516-1144 unmirrorvg: rootvg successfully unmirrored, user should perform bosboot of system to reinitialize boot records. Then, user must modify bootlist to just include: hdisk0.
```

◀ LAN Free Backup through SAN Agent will be discussed in class by faculty.

# Mutlibos

- Two alternate AIX base operating systems (BOS) in a single rootvg
- Standby BOS created as copy of active BOS
- Modify standby BOS without affecting active BOS
  - Apply maintenance to standby BOS
  - Mount and modify standby BOS
  - Start interactive shell working in standby BOS
- Can alternate on reboot which BOS is active

## Overview:

The main purpose of using multibos is to have the type of alternate BOS (base operating system) capabilities that are available with the alternate disk technology, without having to use another disk. The operating system filesets do not occupy enough space to justify allocating another entire disk for that purpose. With multibos, you can have the two BOS versions on the same disk.

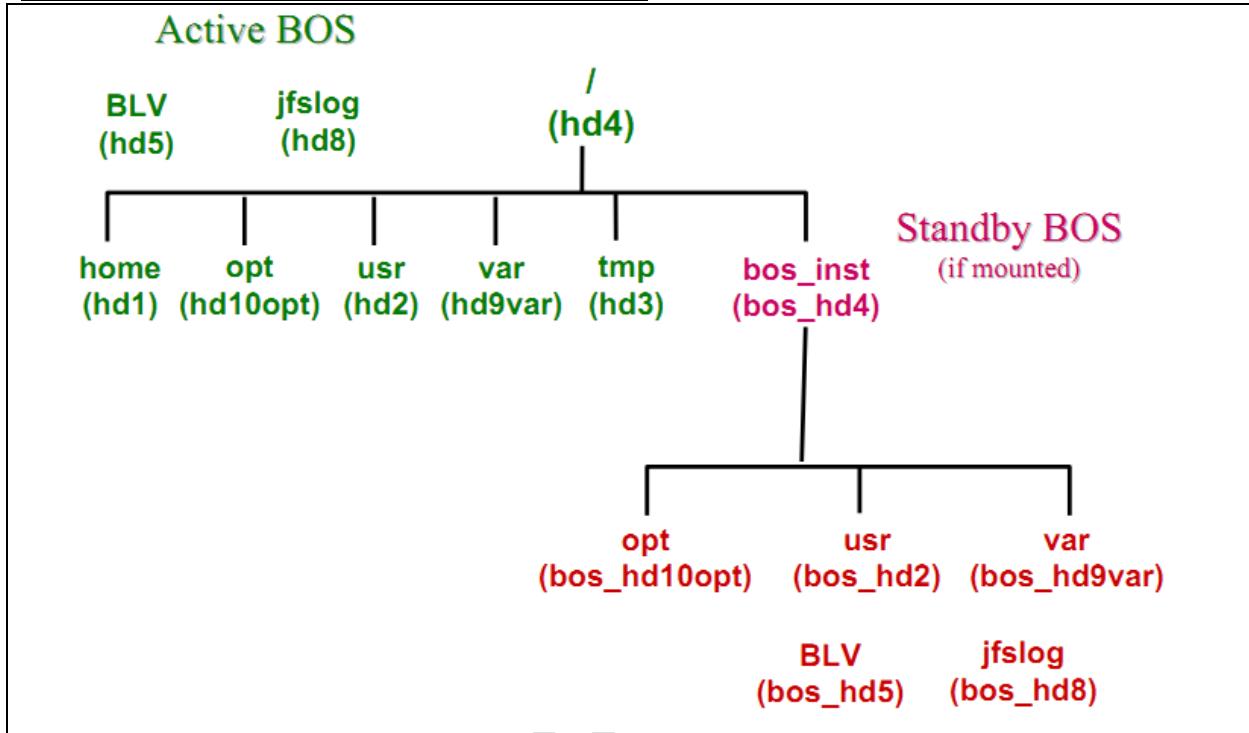
This is accomplished by creating copies of the effected (by an OS update) base operating system logical volumes (active BOS) with a different file name path. Note that these copies are in the one and only rootvg.

Another advantage to multibos is that there is lower overhead to the cloning operation since it does not need to clone all the LVs in the rootvg.

Once you have created the alternate BOS, changes, such as applying maintenance, can be made to these copies, without changing the level of code being used in the active BOS. In addition to applying maintenance, you can access and make configuration changes to the standby BOS through two techniques: mounting the standby BOS and starting an interactive shell (chroot) for the standby BOS.

When you would like to test the standby BOS, you simply reboot using the standby copy of the boot logical volume (BLV). If there is a problem with the changes that were made, configure the bootlist to use the original BLV and a reboot will return you to the original version of the BOS.

### Active and standby BOS logical volumes:



### Standby BOS structure:

The standby BOS needs to mimic the structure of the live BOS file system structure, yet we do not want it to replace the active file systems. To handle this, multibios creates a logical volume to match each of the BOS logical volumes. This includes not only the file systems, but also the JFSlogs and the boot logical volume. The names are modified by prepending a prefix of `bos_` to the front of the standard logical volume names. For the standby BOS file systems, the file system mount point is changed to have a root path of `/bos_inst/`.

If we mount the standby BOS, then we will use this modified path (beginning with `/bos_inst`). If we use the chrooted shell access or if we reboot to make the standby BOS the active BOS, then the (formally standby BOS) file systems will have a root path of `/`.

- Pre-validate that there is sufficient rootvg free space
- Special logical volumes and file systems created for the standby OS
  - `bos_<lvname>`
  - `/bosinst/<mount point>`
- Copies BOS file systems – backup and restore

### **The LVs Cloned are:**

The multibos facility does not clone all the LVs in the rootvg (unlike the alternate disk facility). Some of the system defined logical volumes and all user defined logical volumes are accessed in common between the active BOS and the standby BOS.

The logical volumes which are cloned are:

- /dev/hd5 (BLV)
- /dev/hd4 (root file system)
- /dev/hd2 (/usr)
- /dev/hd9var (/var)
- /dev/hd10opt (/opt)

Before Performing the multibos, check logical volumes and filesystems in rootvg.  
Also check if there is sufficient free space in rootvg to create Standby BOS.

# lsvg -l rootvg	rootvg:	LV NAME	TYPE	LPs	PPs	PVs	LV STATE	MOUNT POINT
		hd5	boot	1	1	1	closed/syncd	N/A
		hd6	paging	8	8	1	open/syncd	N/A
		hd8	jfs2log	1	1	1	open/syncd	N/A
		hd4	jfs2	17	17	1	open/syncd	/
		hd2	jfs2	80	80	1	open/syncd	/usr
		hd9var	jfs2	18	18	1	open/syncd	/var
		hd3	jfs2	97	97	1	open/syncd	/tmp
		hd1	jfs2	11	11	1	open/syncd	/home
		hd10opt	jfs2	33	33	1	open/syncd	/opt

**To perform a standby BOS setup operation preview, type:**

#multibos -Xsp

**To perform a standby BOS setup operation, type:**

#multibos -Xs

```
# multibos -Xs
Initializing multibos methods ...
Initializing log /etc/multibos/logs/op.alog ...
Gathering system information ...

+-----
Setup Operation
+-----
Verifying operation parameters ...
Creating image.data file ...

+-----
Logical Volumes
+-----
Creating standby BOS logical volume bos_hd5
Creating standby BOS logical volume bos_hd4
Creating standby BOS logical volume bos_hd2
Creating standby BOS logical volume bos_hd9var
Creating standby BOS logical volume bos_hd10opt

+-----
File Systems
+-----
Creating all standby BOS file systems ...
Creating standby BOS file system /bos_inst on logical volume bos_hd4
Creating standby BOS file system /bos_inst/usr on logical volume bos_hd2
Creating standby BOS file system /bos_inst/var on logical volume bos_hd9var
Creating standby BOS file system /bos_inst/opt on logical volume bos_hd10opt

+-----
Mount Processing
+-----
Mounting all standby BOS file systems ...
Mounting /bos_inst
Mounting /bos_inst/usr
Mounting /bos_inst/var
Mounting /bos_inst/opt

+-----
BOS Files
+-----
Including files for file system /
Including files for file system /usr
Including files for file system /var
Including files for file system /opt

Copying files using backup/restore utilities ...
Percentage of files copied:  0.00%
Percentage of files copied:  1.23%
Percentage of files copied:  2.46%
```

After successful completion, you can check the logical volumes and filesystems which are cloned:

```
# lsvg -l rootvg
rootvg:
LV NAME      TYPE    LPs    PPs    PVs   LV STATE    MOUNT POINT
hd5          boot     1      1      1   closed/syncd N/A
hd6          paging   8      8      1   open/syncd  N/A
hd8          jfs2log  1      1      1   open/syncd  N/A
hd4          jfs2     17     17     1   open/syncd  /
hd2          jfs2     80     80     1   open/syncd  /usr
hd9var        jfs2     18     18     1   open/syncd  /var
hd3          jfs2     97     97     1   open/syncd  /tmp
hd1          jfs2     11     11     1   open/syncd  /home
hd10opt       jfs2    33     33     1   open/syncd  /opt
bos_hd5       boot     1      1      1   closed/syncd N/A
bos_hd4       jfs2     17     17     1   closed/syncd /bos_inst
bos_hd2       jfs2     80     80     1   closed/syncd /bos_inst/usr
bos_hd9var    jfs2     18     18     1   closed/syncd /bos_inst/var
bos_hd10opt   jfs2    33     33     1   closed/syncd /bos_inst/opt
```

### **Mounting and unmounting standby BOS:**

To access and modify the standby BOS, Mount the standby BOS, type:

```
#multibos -m
```

```
# multibos -m
Initializing multibos methods ...
Initializing log /etc/multibos/logs/op.alog ...
Gathering system information ...

+-----
BOS Mount Operation
+-----
Verifying operation parameters ...

+-----
Mount Processing
+-----
Mounting all standby BOS file systems ...
Mounting /bos_inst
Mounting /bos_inst/usr
Mounting /bos_inst/var
Mounting /bos_inst/opt

Log file is /etc/multibos/logs/op.alog
Return Status = SUCCESS
```

Similarly to unmount the standby BOS, type:

```
#multibos -u
```

```
# multibos -u
Initializing multibos methods ...
Initializing log /etc/multibos/logs/op.alog ...
Gathering system information ...

+-----
BOS Unmount Operation
+-----
Verifying operation parameters ...

+-----
Mount Processing
+-----
Unmounting all standby BOS file systems ...
Unmounting /bos_inst/opt
Unmounting /bos_inst/var
Unmounting /bos_inst/usr
Unmounting /bos_inst

Log file is /etc/multibos/logs/op.alog
Return Status = SUCCESS
```

**To access Standby BOS shell, type:**

```
#multibos -S
# multibos -S
Initializing multibos methods ...
Initializing log /etc/multibos/logs/op.alog ...
Gathering system information ...

+-----
Multibos Shell Operation
+-----
Verifying operation parameters ...

+-----
Mount Processing
+-----
Mounting all standby BOS file systems ...
Mounting /bos_inst
Mounting /bos_inst/usr
Mounting /bos_inst/var
Mounting /bos_inst/opt

+-----
Multibos Root Shell
+-----
Starting multibos root shell ...
Active boot logical volume is hd5.
Script command is started. The file is /etc/multibos/logs/scriptlog.11120217
MULTIBOS>
MULTIBOS>
MULTIBOS>
```

It will return to Active BOS if you type “exit” on standby BOS.

### **Booting to either standby BOS or active BOS:**

The bootlist command supports multiple BLVs. As an example, to boot from disk hdisk0 and BLV bos\_hd5, you would enter the following.

```
# bootlist -m normal hdisk0 blv=bos_hd5  
#Shutdown -Fr
```

After the system is rebooted from the standby BOS, the standby BOS logical volumes are mounted over the usual BOS mount points, such as /, /usr, /var, and so on. The set of BOS objects, such as the BLV, logical volumes, file systems, and so on that are currently booted are considered the active BOS, regardless of logical volume names. The previously active BOS becomes the standby BOS in the existing boot environment.

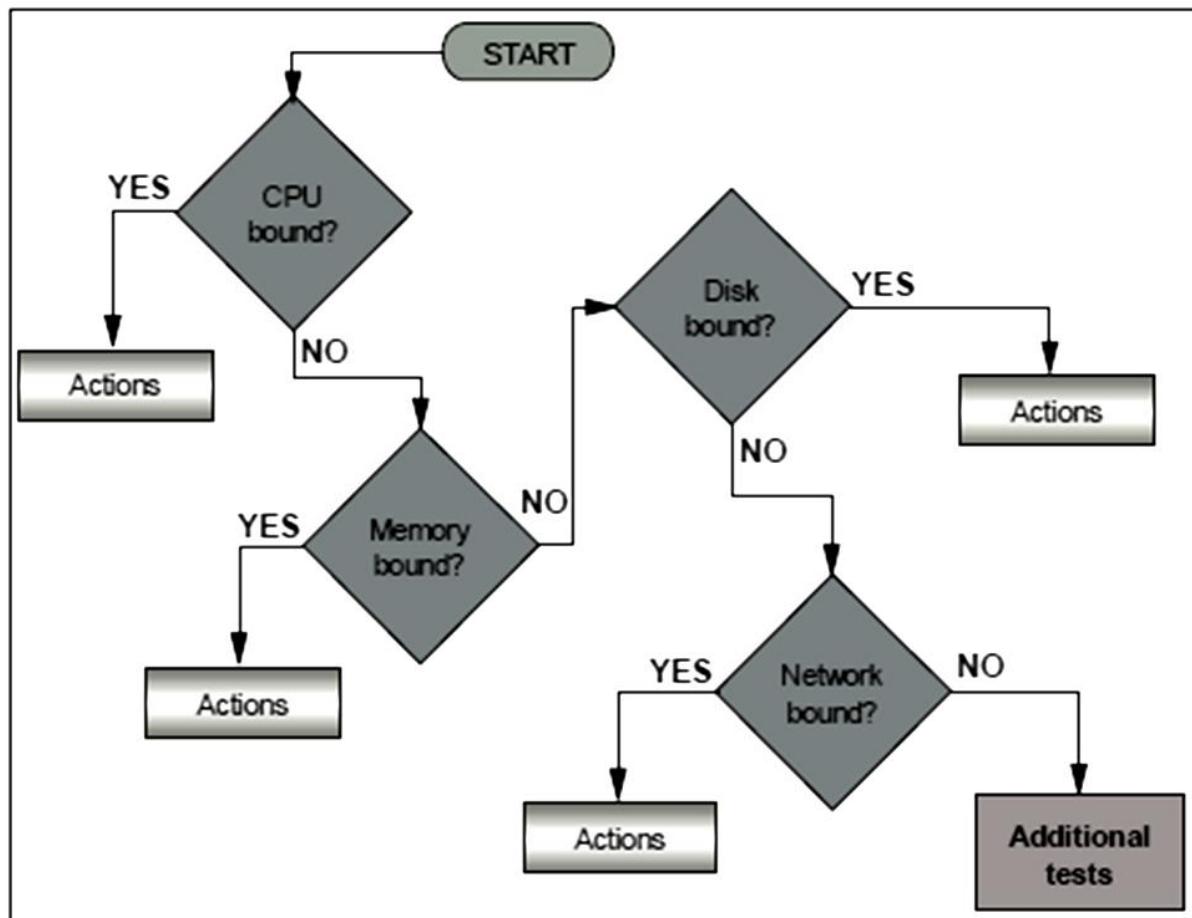
### **Removing a standby BOS:**

The remove operation, using the -R flag, deletes all standby BOS objects, such as BLV, logical volumes, file systems, and so on.

```
#multibos -R
```

## PERFORMANCE TUNING

- ↳ When a system in a productive environment still meets the performance expectations for which it was initially designed, but the demands and needs of the utilizing organization have outgrown the system's basic capacity, performance tuning is performed to avoid and/or delay the cost of adding or replacing hardware.
- ↳ Remember that many performance-related issues can be traced back to operations performed by somebody with limited experience and knowledge, which unintentionally restricted some vital logical or physical resource of the system.



## Critical Resources: The Four Bottlenecks



- |                       |                |                  |                                 |
|-----------------------|----------------|------------------|---------------------------------|
| • Number of processes | • Real memory  | • Disk balancing | • NFS used to load applications |
| • Process-Priorities  | • Paging       | • Types of disks | • Network type                  |
|                       | • Memory leaks | • LVM policies   | • Network traffic               |

The performance of a given workload is determined by the availability and speed of different system resources. These resources that most often affect performance are:

◀ **CPU (Central Processing Unit):**

Is the CPU able to handle all the processes or is the CPU overloaded? Are there any processes that run with a very high priority that manipulates the system performance in general? Is it possible to run certain processes with a lower priority?

◀ **Memory:**

Is the real memory sufficient or is there a high paging rate? Are there faulty applications with memory leaks?

◀ **Disk I/O:**

Is the CPU often waiting for disk I/O? Are the disks in good balance? How good is the disk performance? Can I change LVM policies, to improve the performance (for example, to use striping)?

◀ **Network:**

How much is NFS used on the system? What kinds of networks are used? How much network traffic takes place? , Any faulty network cards? Note that we cannot cover any network-related performance issues in this course. This goes beyond the scope of the class.

## **Lab Activities:**

### **1. Identify the CPU- Intensive Programs**

↳ #ps aux

```
# ps aux
USER      PID %CPU %MEM   SZ   RSS   TTY STAT   STIME TIME COMMAND
root     8196 95.8  0.0    40    40   - A 09:26:50 577:33 wait
root    229512  0.2  1.0  2752 2796   - A 09:28:10 1:06 /usr/es/sbin/clu
root    122948  0.2  0.0  1500 1532   - A 09:28:03 1:04 dtgreet
root    45078  0.0  0.0   116   116   - A 09:26:50 0:18 gil
root      0  0.0  0.0    64    64   - A 09:26:50 0:14 swapper
root    94352  0.0  0.0   508   516   - A 09:27:43 0:10 /usr/sbin/syncd
root   475372  0.0  1.0  3088 3096   - A 14:32:30 0:02 /usr/es/sbin/clu
```

### **2. Identify High-Priority Processes**

↳ #ps -elf

```
# ps -elf
F S      UID      PID  PPID  C PRI NI ADDR      SZ  WCHAN   STIME   TTY TIME CMD
200003 A    root      1      0  0 60 20 1c02c 756          09:27:07   - 0:01 /etc/init
340001 A    root  65630 159876  0 39 20 20006276 2192 f100070f10004b40 09:28:05   - 0:00 /usr/sbin/rsct/bin/rmcd -a
IBM.LPCommands -r
240001 A    root  86064      1  0 60 20 2000b19b  96  10e9490 09:27:44   - 0:00 /usr/ccs/bin/shlap64
200001 A    root  90220 176280  0 60 20 200076d7 700          15:29:23   - 0:00 telnetd -a
240001 A    root  94352      1  0 60 20 2000d11d 508          * 09:27:43   - 0:10 /usr/sbin/syncd 60
40001 A    root  98474      1  0 60 20 20015245 416          09:28:02   - 0:00 /usr/lpp/diagnostics/bin/diagd
40001 A    root 102510      1  0 60 20 20019129 460          09:27:31   - 0:00 /usr/dt/bin/dtlogin -daemon
40401 A    root 118852      1  0 60 20 2001e18e 484  10a09e0 09:27:43   - 0:00 /usr/lib/errdemon
240001 A    root 122948 131140  0 60 20 20014164 1500          09:28:03   - 1:04 dtgreet
40001 A    root 131140 102510  0 60 20 20017147 588 f1000100142721a8 09:27:31   - 0:00 dtlogin <:0> -daemon
```

### **3. How will monitor CPU usage.**

↳ #sar -u 2 5 (where 2 is interval and 5 no. of times)

```
# sar -u 2 5
AIX kt2a      3 5 0009502C4C00      06/04/11
System configuration: lcpu=1

19:44:24      %usr      %sys      %wio      %idle
19:44:26      0          0          0          100
19:44:28      0          0          0          100
19:44:30      0          0          0          100
19:44:32      0          0          0          100
19:44:34      0          0          0          100

Average        0          0          0          100
```

#### 4. Monitor memory usage on your system

```
↳ #vmstat 5
```

```
# vmstat 5

System configuration: lcpu=1 mem=1024MB

kthr      memory          page        faults       cpu
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
r   b    avm    fre   re   pi   po   fr   sr   cy   in   sy   cs   us   sy   id   wa
0   0  75920 156135   0   0   0   0   0   0   0   6  316   74   0   0   99   0
0   0  75922 156132   0   0   0   0   0   0   0   1  319   64   0   0   99   0
1   0  75922 156132   0   0   0   0   0   0   0   1  315   65   1   1   98   0
1   0  75922 156132   0   0   0   0   0   0   0   0  327   65   0   0   99   0
0   0  75922 156132   0   0   0   0   0   0   0   0  330   66   0   0   99   0
0   0  75922 156132   0   0   0   0   0   0   0   1  325   67   0   0   99   0
```

#### 5. Try Monitoring Disk I/O on your system

```
↳ #iostat 5 2
```

```
System configuration: lcpu=1 drives=14 paths=0 vdisks=0

          tin      tout      avg-cpu: % user % sys % idle % iowait
          0.0      11.8           0.0     0.0     100.0      0.0

Disks:    % tm_act    Kbps      tps      Kb_read      Kb_wrtn
hdisk1     0.0      0.0      0.0          0          0
hdisk3     0.0      0.0      0.0          0          0
hdisk4     0.0      0.0      0.0          0          0
hdisk5     0.0      0.0      0.0          0          0
hdisk2     0.0      0.0      0.0          0          0
hdisk8     0.0      0.0      0.0          0          0
hdisk7     0.0      0.0      0.0          0          0
hdisk9     0.0      0.0      0.0          0          0
hdisk11    0.0      0.0      0.0          0          0
hdisk12    0.0      0.0      0.0          0          0
hdisk6     0.0      0.0      0.0          0          0
hdisk0     0.0      0.8      0.2          4          0
cd0        0.0      0.0      0.0          0          0
hdisk10    0.0      0.0      0.0          0          0

          tin      tout      avg-cpu: % user % sys % idle % iowait
          0.0     217.4           0.0     0.2     99.8      0.0

Disks:    % tm_act    Kbps      tps      Kb_read      Kb_wrtn
hdisk1     0.0      0.0      0.0          0          0
hdisk3     0.0      0.0      0.0          0          0
hdisk4     0.0      0.0      0.0          0          0
hdisk5     0.0      0.0      0.0          0          0
hdisk2     0.0      0.0      0.0          0          0
hdisk8     0.0      0.0      0.0          0          0
hdisk7     0.0      0.0      0.0          0          0
hdisk9     0.0      0.0      0.0          0          0
hdisk11    0.0      0.0      0.0          0          0
hdisk12    0.0      0.0      0.0          0          0
hdisk6     0.0      0.0      0.0          0          0
hdisk0     0.0      0.8      0.2          4          0
cd0        0.0      0.0      0.0          0          0
hdisk10    0.0      0.0      0.0          0          0
```

6. How will you monitor all the four bottle neck of sys at the same time?

↙ #topas

Topas Monitor for host: kt2a_nsvc2				EVENTS/QUEUES		FILE/TTY	
				Cswitch	64	Readch	0
Sat Jun 4 19:57:25 2011		Interval:	2	Syscall	350	Writech	145
Kernel	0.5	#		Reads	0	Rawin	0
User	0.0			Writes	0	Ttymout	145
Wait	0.0			Forks	0	Igets	0
Idle	99.5	#####		Execs	0	Namei	0
				Runqueue	0.0	Dirblk	0
Network	KBPS	I-Pack	O-Pack	KB-In	KB-Out	Waitqueue	0.0
en0	0.3	1.0	0.5	0.1	0.2		
en1	0.1	0.5	0.0	0.1	0.0	PAGING	MEMORY
lo0	0.0	0.0	0.0	0.0	0.0	Faults	0 Real,MB 1024
						Steals	0 % Comp 32.6
Disk	Busy%	KBPS		TPS	KB-Read	KB-Writ	
hdisk3	0.0	0.0		0.0	0.0	PgspIn	0 % Noncomp 9.5
hdisk4	0.0	0.0		0.0	0.0	PgspOut	0 % Client 12.0
hdisk5	0.0	0.0		0.0	0.0	PageIn	0
hdisk2	0.0	0.0		0.0	0.0	PageOut	0 PAGING SPACE
hdisk8	0.0	0.0		0.0	0.0	Sios	0 Size,MB 512
hdisk7	0.0	0.0		0.0	0.0		% Used 1.0
hdisk1	0.0	0.0		0.0	0.0	NFS (calls/sec)	% Free 98.9
hdisk9	0.0	0.0		0.0	0.0	ServerV2	0
hdisk10	0.0	0.0		0.0	0.0	ClientV2	0 Press:
hdisk11	0.0	0.0		0.0	0.0	ServerV3	0 "h" for help
hdisk12	0.0	0.0		0.0	0.0	ClientV3	0 "q" to quit
hdisk6	0.0	0.0		0.0	0.0		
hdisk0	0.0	0.0		0.0	0.0		
Name	PID	CPU%		PgSp	Owner		
topas	405582	0.3		1.2	root		
dtgreet	122948	0.2		1.4	root		
gil	45078	0.1		0.1	root		
xmgc	36882	0.0		0.0	root		
clstrmgrp	475372	0.0		1.2	root		
X	139342	0.0		3.2	root		
clcomd	229512	0.0		2.5	root		
rpc.lock	344124	0.0		0.2	root		
hostmibd	483366	0.0		0.6	root		
n4bg	143474	0.0		0.0	root		
netm	40980	0.0		0.0	root		

7. How will you monitor NFS activities in your system?

↳ #nfsstat

Server rpc:							
Connection oriented		nullrecv	badlen	xdrcall	dupchecks	dupreqs	
calls	badcalls	0	0	0	0	0	
0	0						
Connectionless							
calls	badcalls	nullrecv	badlen	xdrcall	dupchecks	dupreqs	
0	0	0	0	0	0	0	
Server nfs:							
calls	badcalls	public_v2	public_v3				
0	0	0	0				
Version 2: (0 calls)							
null	getattr	setattr	root	lookup	readlink	read	
0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	
wrcache	write	create	remove	rename	link	symlink	
0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	
mkdir	rmdir	readdir	statfs				
0 0%	0 0%	0 0%	0 0%				
Version 3: (0 calls)							
null	getattr	setattr	lookup	access	readlink	read	
0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	
write	create	mkdir	symlink	mknod	remove	rmdir	
0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	
rename	link	readdir	readdir+	fsstat	fsinfo	pathconf	
0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%	
commit							
0 0%							
Client rpc:							
Connection oriented		badxids	timeouts	newcreds	badverfs	timers	
calls	badcalls	0	0	0	0	0	
0	0						
nomem	cantconn	interrupts					
0	0	0					
Connectionless							
calls	badcalls	retrans	badxids	timeouts	newcreds	badverfs	
12	0	0	0	0	0	0	

NOTE: Rahul sir will run customized scripts to generate performance issues for CPU and Memory and Harddisk . You can see automate ticket generation . Raise a customer ticket for performance issues.

## **NIM: Creation of an LPP SOURCE and SPOT from Installation Media**

### **Introduction:**

What is Network Installation Manager (NIM), and why should you consider using it? NIM is a client/server application which uses object oriented technology. It provides an environment to install and manage AIX filesets on machines over the network. NIM provides an easy and efficient way for you to perform various installation and software maintenance tasks over several network types (such as Ethernet). Here are some examples:

- When you have more than two IBM eServer machines in your AIX 5L environment, you are working with a *cluster*, so you may be seeking a way to install and upgrade your IBM Eserver systems without the need for multiple CD-ROMs and tapes.
- You may be seeking a way to manage AIX 5L software installations and upgrades remotely, without actual physical access to the hardware.
- You may seeking a standard method for maintaining several AIX 5L operating systems images across many IBM Eserver systems.

For all these scenarios, NIM is the tool of choice.

### **NIM terminology:**

#### **Master**

Master refers the machine where you set up and maintain your NIM environment. You can also initiate installations from here (push mode). It is the key piece of the NIM environment.

#### **Client**

The NIM client can be the target for NIM master-initiated operations such as installation, updates, and so forth (push mode). Also, a client can initiate its own installation or update (pull mode). A NIM client automatically becomes a resource server when it holds NIM resources.

- The machine that will become the NIM master must have AIX installed.
- The NIM master should always have the highest version of AIX installed across the entire NIM environment. Using the same AIX level for master and client is acceptable.

To configure any AIX server as NIM server, we need these NIM filesets:

- i. bos.sysmgt.nim.client (installed by default with AIX)
- ii. bos.sysmgt.nim.master
- iii. bos.sysmgt.nim.spot

First check whether the required filesets are installed or not, using **lslpp** command:

```
# lslpp -l | grep -i bos.sysmgt.nim
bos.sysmgt.nim.client      6.1.5.1  COMMITTED  Network Install Manager -
bos.sysmgt.nim.client      6.1.5.1  COMMITTED  Network Install Manager -
```

So here we need to install two filesets i.e **bos.sysmgt.nim.master** & **bos.sysmgt.nim.spot** from AIX6.1 installation media:

```
# smit installlp
Install Software
INPUT device / directory for software          /dev/cd0
>bos.sysmgt.nim.master
>bos.sysmgt.nim.spot
ACCEPT new license agreements? Yes
```

After installing the filesets, check if the filesets are installed using **lslpp** command:

```
# lslpp -l | grep -i bos.sysmgt.nim
bos.sysmgt.nim.client      6.1.5.1  COMMITTED  Network Install Manager -
bos.sysmgt.nim.master      6.1.5.1  COMMITTED  Network Install Manager -
bos.sysmgt.nim.spot        6.1.5.0  COMMITTED  Network Install Manager -
bos.sysmgt.nim.client      6.1.5.1  COMMITTED  Network Install Manager -
```

Configure the selected machine as a NIM master:

```
# smit nim
Configure the NIM Environment
Advanced Configuration
Initialize the NIM Master Only
    Configure Network Installation Management Master Fileset

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

* Network Name [Entry Fields]
* Primary Network Install Interface [Nim-nw]
                                         [en0]

Allow Machines to Register Themselves as Clients? [yes]
Alternate Port Numbers for Network Communications
    (reserved values will be used if left blank)
Client Registration []
Client Communications []
```

The following list presents the basic resources needed for installing machines in your environment:

**SPOT:**

SPOT, or Shared Product Object Tree, is a directory of code (installed filesets) that is used during client booting procedure. It is equivalent in content to the code that resides in the /usr file system on a system running AIX 5L (binary objects - executables and libraries, header files and shell scripts). This resource (directory) replaces the content of the basic ramdisk image available on installation CDs.

The installation is performed over a network, and there are no AIX CDs available. Device drivers, the BOS install program, and other necessary code needed to perform a base operating system installation are found inside the SPOT.

During the installation, the client machine NFS mounts this resource in order to access the code needed for the installation process.

The SPOT also contains the code needed to generate the boot images (kernels, which will be stored in the /tftpboot directory) that the client uses until it can manage to NFS-mount the SPOT directory.

**Ipp\_source:**

An Ipp\_source is a directory similar to AIX install CDs. It contains AIX Licensed Program Products (LLPs) in Backup File Format (BFF) format and RPM Package Manager (RPM) filesets that you can install.

**Defining basic resources:**

First define the **Ipp\_source** resource, followed by the **SPOT**. The Ipp\_source resource is a directory containing installable filesets. Use the **smitty nim\_mkres** fastpath, select Ipp\_source, and enter the required values in the input screen shown below.

```

# smit nim
Configure the NIM Environment
Advanced Configuration
Create Basic Installation Resources
Create an LPP_SOURCE and SPOT from Installation Media
    Create Basic Installation Resources

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

* Resource SERVER [Entry Fields]
* Input device for installation images
  (specify the device on the resource server) master
[cd0]

* LPP_SOURCE Name [AIX6105LPP]
* LPP_SOURCE Directory [/export/lpp_source]
Create new filesystem for LPP_SOURCE?
Filesystem SIZE (MB) [yes]
[VOLUME GROUP for new filesystem] [650]
[rootvg]

* SPOT Name [AIX6105SPOT]
* SPOT Directory [/export/spot]
Create new filesystem for SPOT?
Filesystem SIZE (MB) [yes]
[VOLUME GROUP for new filesystem] [350]
[rootvg]
Create new bosinst_data resource? [no]
Create new installlp bundle resources? [no]
Prepend level to resource name [no]

Remove all newly added NIM definitions [no]
and filesystems if any part of this
operation fails?

```

To illustrate the contents of this NIM database, we use the **lsnim** command to extract the content (on a NIM master that is already set up and working), as shown below:

```

# lsnim
master      machines      master
boot       resources      boot
nim_script   resources   nim_script
Nim-Nw      networks      ent
AIX6105LPP  resources   lpp_source
AIX6105SPOT resources   spot

```

Shows the details of a resource retrieved using the **lsnim -l <resource name>** command.

```
# lsnim -l Nim-Nw
Nim-Nw:
  class      = networks
  type       = ent
  Nstate     = ready for use
  prev_state = information is missing from this object's definition
  net_addr   = 192.168.10.0
  snm        = 255.255.255.0
```

Details of a particular lpp\_source resource

```
# lsnim -l AIX6105LPP
AIX6105LPP:
  class      = resources
  type       = lpp_source
  arch       = power
  Rstate     = ready for use
  prev_state = unavailable for use
  location   = /export/lpp_source/AIX6105LPP
  simages    = yes
  alloc_count = 0
  server     = master
```

Details of a particular spot resource

```
# lsnim -l AIX6105SPOT
AIX6105SPOT:
  class      = resources
  type       = spot
  plat_defined = chrp
  arch       = power
  bos_license = yes
  Rstate     = ready for use
  prev_state = verification is being performed
  location   = /export/spot/AIX6105SPOT/usr
  version    = 6
  release    = 1
  mod        = 5
  oslevel_r  = 6100-05
  alloc_count = 0
  server     = master
  Rstate_result = success
  mk_netboot = yes
  mk_netboot = yes
```

### Defining the client:

After the two basic resources have been defined, add the first NIM client. Use the **smitty nim\_mkmac** fastpath, enter the name of the machine, and fill in the required fields in the SMIT panel as shown below.

```
# smit nim
Perform NIM Administration Tasks
Manage Machines
Define a Machine
* Host Name of Machine [ktaix30]

Define a Machine

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
* NIM Machine Name [ktaix30]
* Machine Type [standalone]
* Hardware Platform Type [chrp]
  Kernel to use for Network Boot [64]
  Communication Protocol used by client []
  Primary Network Install Interface []

* Cable Type bnc
  Network Speed Setting []
  Network Duplex Setting []
* NIM Network Nim-Nw
* Host Name ktaix30
  Network Adapter Hardware Address [0]
  Network Adapter Logical Device Name []
  IPL ROM Emulation Device []
  CPU Id []
  Machine Group []
```

After the client (ktaix30) is added to NIM master server, check the status using **lsnim** command:

```
# lsnim
master      machines    master
boot       resources   boot
nim_script resources nim_script
Nim-Nw     networks    ent
AIX6105LPP resources  lpp_source
AIX6105SPOT resources  spot
ktaix32    machines    standalone
ktaix30    machines    standalone
```

### Push and pull modes:

The push mode operation is initiated from the master. The pull mode operation is initiated from the client. The very first time a client is installed, only the pull mode can be used. Note the following points:

- In order for the push mode to be successful, the client must have a minimum AIX image already installed and TCP/IP configured.
- To use the pull mode, you need access to the clients' SMS menu. For this you either need a console attached to the machine, or for HMC-managed systems, you need access to the HMC.

### **Start the client installation:**

Use the **smitty nim\_task\_inst** fastpath, then select Install the Base Operating System on Standalone Clients, the client to be installed (**ktaix30**), rte as installation method, and the resources (**AIX6105SPOT** and **AIX6105LPP**), as shown below.

Starting base operating system installation on a client:

```
# smit nim
Perform NIM Software Installation and Maintenance Tasks
Install and Update Software
Install the Base Operating System on Standalone Clients
Select a TARGET for the operation : ktaix30
Select the installation TYPE: rte - Install from installation images
Select the LPP_SOURCE to use for the installation: AIX6105LPP
Select the SPOT to use for the installation: AIX6105SPOT

Install the Base Operating System on Standalone Clients

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP] [Entry Fields]
* Installation Target ktaix30
* Installation Type rte
* SPOT AIX6105SPOT
LPP_SOURCE [AIX6105LPP]
MKSYSB

BOSINST_DATA to use during installation []
IMAGE_DATA to use during installation []
RESOLV_CONF to use for network configuration []
Customization SCRIPT to run after installation []
Customization FB Script to run at first reboot []
ACCEPT new license agreements? [yes]
Remain NIM client after install? [yes]
Preserve NIM definitions for resources on
this target? [yes]

FORCE PUSH the installation? [no]

Initiate reboot and installation now? [no]
-OR-
Set bootlist for installation at the
next reboot? [no]
```

Accept the licence agreements and change the value of Initiate reboot and installation now? from yes to no. Also, because this is the very first time installing this machine, client network boot must be manually initiated (to allow the client to “pull” resources from the server).

After the resources are pushed onto the client, check the **Cstate** should be “**BOS installation has been enabled**”

```
# lsnim -l ktaix30
ktaix30:
    class          = machines
    type           = standalone
    connect        = shell
    platform       = chrp
    netboot_kernel = 64
    if1            = Nim-Nw ktaix30 0
    cable_type1   = bnc
    Cstate         = BOS installation has been enabled
    prev_state    = ready for a NIM operation
    Mstate         = not running

    boot           = boot
    lpp_source     = LPP_53_ML4
    nim_script     = nim_script
    spot           = SPOT_53_ML4
    cupid          = 001A85D24C00
    control         = master
```

Now start the client **ktaix30** in SMS mode:

- Main Menu: select **2. Setup Remote IPL (Initial Program Load)**
- NIC Adapters: select **1. Interpartition Logical LAN U8203.E4A.0609236-V4-C2-T1**
- Select Internet Protocol Version: select **1. IPv4 - Address Format 123.231.111.222**
- Select Network Service: select **1. BOOTP**
- Network Parameters: select **1. IP Parameters**

1. Client IP Address	[192.168.10.30]
2. Server IP Address	[192.168.10.29]
3. Gateway IP Address	[000.000.000.000]
4. Subnet Mask	[255.255.255.0]

- Network Parameters: select **3. Ping Test**
- Select: **1. Execute Ping Test** (here ping to NIM server should be successful) after this you can proceed to next step (or) if the ping is unsuccessful troubleshoot network issues.

After setting up the IP parameters, boot the server from network from the SMS menu:

- Main Menu: select **5. Select Boot Options**
- Multiboot: select **1. Select Install/Boot Device**
- Select Device Type: select **6. Network**
- Select Network Service: select **1. BOOTP**
- Select Device: select **1. - Interpartition Logical LAN**  
(loc=U8203.E4A.0609236-V4-C2-T1)
- Select Task: select **2. Normal Mode Boot**
- Are you sure you want to exit System Management Services? select **1. Yes**
- Now the client (**Ktaix30**) starts booting from network

Shows the installation flow which you can expect from an AIX LPAR environment. First the network boot (IPL) is initiated for the LPAR.

```
-----  
          Welcome to AIX.  
          boot image timestamp: 19:24 04/21  
          The current time and date: 18:40:27 04/23/2007  
          processor count: 1; memory size: 1024MB; kernel size: 27451313  
boot device: /vdevice/1-lan@30000002:speed=auto,duplex=auto,192.168.1.1.,,  
-----  
  
***** Please define the System Console. *****  
  
Type a 1 and press Enter to use this terminal as the  
system console.  
Pour definir ce terminal comme console systeme, appuyez  
sur 1 puis sur Entrée.  
Taste 1 und anschliessend die Eingabetaste druecken, um  
diese Datenstation als Systemkonsole zu verwenden.  
Premere il tasto 1 ed Invio per usare questo terminal  
come console.  
Escriba 1 y pulse Intro para utilizar esta terminal como  
consola del sistema.  
Escriviu 1 i premeu Intro per utilitzar aquest  
terminal com a consola del sistema.  
Digite um 1 e pressione Enter para utilizar este terminal  
como console do sistema.
```

Select the appropriate options to install an AIX Base Operating System:

```
>>> 1 Type 1 and press Enter to have English during install.
```

```
Welcome to Base Operating System  
Installation and Maintenance
```

```
Type the number of your choice and press Enter. Choice is indicated by >>>.
```

```
>>> 1 Start Install Now with Default Settings
```

```
2 Change/Show Installation Settings and Install
```

```
3 Start Maintenance Mode for System Recovery
```

```
4 Configure Network Disks (iSCSI)
```

```
5 Select Storage Adapters
```

```
88 Help ?
```

```
99 Previous Menu
```

```
>>> Choice [1]: 2
```

In this case the installation is made using NIM resources, as shown below:

```
Installing Base Operating System
```

```
Please wait...
```

Approximate % tasks complete	Elapsed time (in minutes)
---------------------------------	------------------------------



7	0	0% of mksysb data restored.
---	---	-----------------------------

## **PRINTERS IN AIX**

### **AIX print subsystem characteristics**

- ➲ Flexible printer drivers. AIX 5L printer drivers provide many printing options that can be easily controlled using the command-line options to the qprt command. Printer defaults can be easily managed using SMIT or the command line.
- ➲ System management tools. The AIX print subsystem includes mature and powerful system management, using the Web-based System Manager or SMIT, as well as the command line. System management tools for the System V print subsystem are less mature in this initial release. Some specific system management advantages using the AIX print subsystem are:
  - ➲ Limits fields and options validation
  - ➲ Easy printer customization
  - ➲ Single-step print device and queue creation
  - ➲ Support for dial-in administration

### **System V print subsystem characteristics**

- ➲ Long-term strategy. The IBM long-term printing strategy for AIX is to maintain compatibility with other UNIX systems.
- ➲ Standard PostScript filters. The System V print subsystem includes a number of filters for converting a number of different file formats to PostScript.
- ➲ Support for forms. The System V print subsystem provides a mechanism for mounting forms on printers and allowing or denying user access based on the form that is mounted. To provide this capability under AIX printing, you must create multiple queues and manage which queues are enabled while a form is mounted.
- ➲ Security. System V printing includes built-in capabilities for restricting user access to certain printers. Using the AIX 5L print subsystem, the back-end program must be customized to restrict user access.

## AIX Print Sub System V/S System V Print Sub System

<b>AIX Print Sub System</b>	<b>System V Print Sub System</b>
Powerful and flexible printer drivers	Higher compatibility due to support in various flavours of unix.
Single Step print device and queue mechanism	More interface, Higher security
Customize spooling subsystem, does not support form printing	Supports form printing

### **Concepts of Queues:**

- ↳ The purpose of the queuing system is to maintain a queue for jobs that are waiting for their turn to run
- ↳ Queues also give control to administrators over queuing mechanism, so system admin can perform tasks like cancelling jobs on queues, changing priorities of jobs.
- ↳ One print queue can print to **number** of printers.
- ↳ Users can submit their jobs to a number of different queues.

**Note:-** The **qdaemon** is started at boot time for the /etc/inittab file. The **qdaemon** is under Control of the system resource controller

### **Printer Data Flow:**

- ↳ The user can issue one of the printer commands **qprt**, **lp**, **lpr**, or **enq** to submit a print job.
- ↳ The entry point to the spooler is the **enq** command, which is responsible for processing the job request, creating a job description file and notifying the **qdaemon** of the new job.
- ↳ The **qdaemon** maintains a list of all of the defined queues and monitors the queues for newly submitted jobs.
- ↳ An entry is made in the **/var/spool/lpd/qdir** directory identifying the job to be run. The copy is placed in the spool directory **/var/spool/qdaemon**
- ↳ When a job reaches the top of the queue or the front of the line, the **qdaemon** reads information from **/etc/qconfig**.
- ↳ When the queue starts working on the job, the **qdaemon** sends an update to the job is active.
- ↳ The backend program for the queue is started by the qdaemon and receives the filename and the print options for the job, which is returned into a command line statement.

- ↳ The backend puts all of the pieces together. The files with the attributes are assembled together into a data stream, which is stored in virtual printer definitions in the **/var/spool/lpd/pio/@local** directory.
- ↳ The backend program sends its data stream to the device driver for the appropriate printer.

## Print related files and directories

The system files and directories used for printing include:

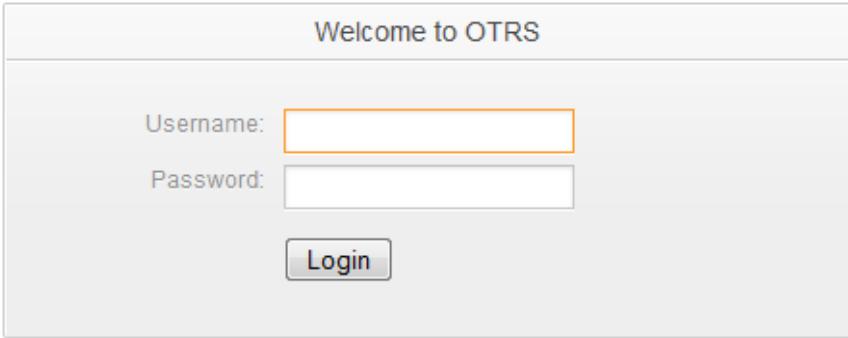
- ↳ The **/etc/qconfig** file describes the queues and devices available for use by the printing commands.
- ↳ The **/var/spool** directory contains files and directories used by the printing programs and daemons.
- ↳ The **/var/spool/lpd/qdir** directory contains information about files queued to print.
- ↳ The **/var/spool/qdaemon** directory contains copies of the files that are spooled to print.
- ↳ The **/var/spool/lpd/stat** directory is where the information on the status of jobs is stored. It is used by the qdaemon and backend programs.

## Lab Activities:

1. Check the current print subsystem.  
↳ `#switch.prt -d`
2. Change the current print subsystem.  
↳ `#switch.prt -s AIX` or `switch.prt -d System V`
3. How will you submit a job to a queue in both print sub system  
↳ `#lp > filename` in AIX print subsystem and  
↳ `#qprt > filename` in System V print subsystem
4. List the jobs in a queue in both print sub system  
↳ `#lpstat` in Aix print subsystem and  
↳ `#qchk` in System Vprint sub system.
5. Bring queues Up and Down  
↳ `#enable queue name`  
↳ `#disable queue name`  
↳ `#smitty spooler.`  
↳ `#smitty chpq`
6. Remove a queue from the queue list  
↳ `#smitty rmpq`

## **Ticket raising in OTRS regarding luns assignment from SAN**

- Login to the OTRS server using the following link.  
<http://192.168.10.107/otrs/index.pl>
- Specify the appropriate **Username** and **Password** to login.



Welcome to OTRS

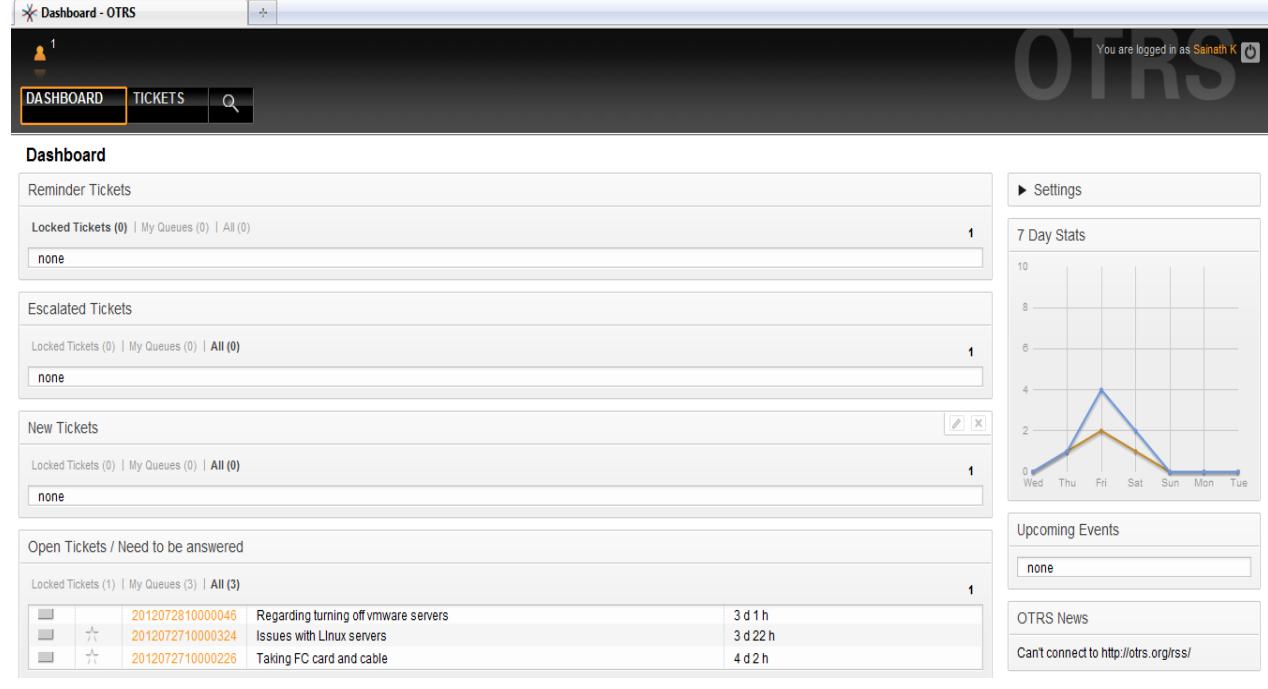
Username:

Password:

**Login**

[Lost your password?](#)

- Click on the “Dashboard” to check **Reminder Tickets**, **Escalated Tickets**, **New Tickets** and **Open tickets/Need to be answered**.
- Here check whether any tickets need to be answered by your team.



**Dashboard - OTRS**

You are logged in as Sanath K

**DASHBOARD** **TICKETS**

**Reminder Tickets**  
Locked Tickets (0) | My Queues (0) | All (0)  
none

**Escalated Tickets**  
Locked Tickets (0) | My Queues (0) | All (0)  
none

**New Tickets**  
Locked Tickets (0) | My Queues (0) | All (0)  
none

**Open Tickets / Need to be answered**  
Locked Tickets (1) | My Queues (3) | All (3)  
1  
201207281000046 Regarding turning off vmware servers 3 d 1 h  
2012072710000324 Issues with Linux servers 3 d 22 h  
2012072710000226 Taking FC card and cable 4 d 2 h

**Settings**

**7 Day Stats**

**Upcoming Events**  
none

**OTRS News**  
Can't connect to http://otrs.org/rss/

- Click on **Tickets → status** view to check the overview of all open tickets.

The screenshot shows the OTRS Status View - Ticket - OTRS interface. At the top, there's a header with the OTRS logo and a message saying "You are logged in as Sainath K". Below the header, there's a navigation bar with tabs: DASHBOARD, TICKETS (which is highlighted in orange), and a search icon. The main area is titled "Status View: open" and shows a table of open tickets. The table has columns: TICKET#, AGE, FROM / SUBJECT, STATE, LOCKED, QUEUE, OWNER, and CUSTOMERID. There are three open tickets listed:

	TICKET#	AGE	FROM / SUBJECT	STATE	LOCKED	QUEUE	OWNER	CUSTOMERID
<input type="checkbox"/>	201207281000046	3 d 1 h	OTRS System Regarding turning off vmware s[...]	open	lock	UNIX-KTS-SUPP	Sainath K	
<input type="checkbox"/>	2012072710000324	3 d 22 h	OTRS System Issues with Linux servers	open	lock	UNIX-KTS-SUPP	Hamza Sirajuddin	
<input type="checkbox"/>	2012072710000226	4 d 2 h	OTRS System Taking FC card and cable	open	unlock	UNIX-KTS-SUPP	Nickil kumar	

At the bottom left, it says "Powered by OTRS 3.0.11". At the bottom right, there's a link "Top of page".

- Let us take an example to raise a ticket from UNIX team, regarding the luns which are required on ktaix18 server.
- So to raise a ticket regarding luns from SAN, click on **Tickets → New email ticket**

The screenshot shows the OTRS Tickets interface. At the top, there's a navigation bar with tabs: DASHBOARD, TICKETS (highlighted in orange), and a search icon. A dropdown menu is open over the TICKETS tab, listing several options: Queue view, Status view, Escalation view, New phone ticket, New email ticket (which is highlighted in orange), and Search. To the right of the dropdown, there's a button labeled "Create new email ticket and send this out (outbound) (e)". Below the navigation bar, there are sections for "Reminder Tickets" and "Locked Tickets (0)".

- Select the appropriate team to raise the ticket (in our case it is UNIX-KTS-SUPP)
- In “To:” field Mention the email id of the SAN team who are suppose to assign the luns to ktaix18 server.
- Select the owner, by whom the ticket being raised.
- Mention proper subject and description in the mail regarding the luns assignment from the storage team.
- If any attachment of information is required while raising the ticket, it can be done by the “Attachment” field.

- Set the priority for the ticket as required, In OTRS the priority is given as follows:

- 1- High Priority
- 2- High
- 3- Normal
- 4- Below Normal
- 5- Low Priority

**Create New Email Ticket**

\* From queue: **UNIX-KTS-SUPP**

\* To: **admin@mon.kts.com**

Cc:

Bcc:

Owner: **Pochampalli Sairam (sairam)**

\* Subject: **Need luns from SAN**

Options: **[Address book]**

\* Text:

Hi San-team,  
Please assign 3 luns of 5GB each on ktaix18 server.  
regards,  
sairam.

Signature:

Your Ticket-Team  
--  
**Kernel Technologies**  
# 201, Sree Swathi Anukar, Ameerpet, Hyderabad - 500038.  
Email: vivek@kerneltech.com - Web: <http://www.kerneltech.com/>

Attachment:  Browse...

CustomerID:

Next ticket state: **open**

Pending Date (for pending\* states): **08 / 01 / 2012 15:46**

Priority: **2 High**

Time units (work units):

**Send mail!**

- When the ticket raised successful, the raised ticket can be viewed under **Tickets → Status view** can check the ticket with “**Ticket#2012073110000325**” as shown below.
- Check the ticket information such as status, priority etc...

**Ticket#2012073110000325 — Need luns from SAN**

1 Article(s)

Age: 0 m – Created: 07/31/2012 15:53

Back | Unlock | History | Print | Priority | Free Fields | Link | Owner | Customer | Note | Merge | Pending | Close | - Move -

NO.	TYPE	FROM	SUBJECT	CREATED
1	agent – email-external	OTRS System	Need luns from SAN	07/31/2012 15:53

#1 – Need luns from SAN  
Created: 07/31/2012 15:53

Forward | Bounce | Phone Call Outbound | Split | Print | - Reply -

From: OTRS System  
To: admin@mon.pts.com

Hi San-team,  
Please assign 3 luns of 5GB each on ktaix18 server.  
regards,  
sairam.

Your Ticket-Team  
--  
**Kernel Technologies**  
# 201, Sree Swathi Anukar, Ameerpet, Hyderabad - 500038.  
Email: vivek@kerneltech.com - Web: <http://www.kerneltech.com/>

**Ticket Information**

State: open  
Locked: lock  
Priority: 2 High  
Queue: UNIX-KTS-SUPP

CustomerID:  
Accounted time: 0  
Owner: Sairam Pochampalli

**Customer Information**  
none

**Linked Objects**  
none

- Checking the ticket assigned to the SAN team, the SAN team has assigned 3 Luns of 5GB each on ktaix18 server.
- The output from the server ktaix18 is shown below regarding the luns which are assigned from SAN.
- Below output confirms that hdisk3, hdisk4 and hdisk5 are assigned from NETAPP storage as the description is shown as “MPIO Other iSCSI Disk Drive”

```
bash-3.2# hostname
ktaix18
bash-3.2# lsdev -Cc disk
hdisk0 Available 1s-08-00-4,0 16 Bit LVD SCSI Disk Drive
hdisk1 Available 1s-08-00-5,0 16 Bit LVD SCSI Disk Drive
hdisk2 Available 1s-08-00-8,0 16 Bit LVD SCSI Disk Drive
hdisk3 Available MPIO Other iSCSI Disk Drive
hdisk4 Available MPIO Other iSCSI Disk Drive
hdisk5 Available MPIO Other iSCSI Disk Drive
```

- As the luns are successfully assigned to ktaix18 server, now close the ticket by giving the appropriate information for closing the ticket.

- To close the ticket, click on close (highlighted in red) and give the proper information why the ticket is being closed.

Ticket#2012073110000325 — Need luns from SAN

1 Article(s) Age: 0 m – Created: 07/31/2012 15:53

Back | Unlock | History | Print | Priority | Free Fields | Link | Owner | Customer | Note | Merge | Pending | **Close** | Move -

NO.	TYPE	FROM	SUBJECT	CREATED
1	agent – email-external	OTRS System	Need luns from SAN	07/31/2012 15:53

#1 – Need luns from SAN Created: 07/31/2012 15:53

Forward | Bounce | Phone Call Outbound | Split | Print | - Reply -

From: OTRS System  
To: admin@mon.kts.com

Hi San-team,  
Please assign 3 luns of 5GB each on ktaix18 server.  
regards,  
sairam.

Your Ticket-Team  
--  
**Kernel Technologies**  
# 201, Sree Swathi Anukar, Ameerpet, Hyderabad - 500038.  
Email: vivek@kerneltech.com - Web: <http://www.kerneltech.com/>

Close Ticket : 2012073110000325 - Need luns from SAN

[Cancel & close window](#)

Options

\*Subject:

\*Text:

Closing the ticket, luns have been successfully assigned to ktaix18 server.  
regards,  
sairam.

Attachment: output lspv.jpg (58.9 KBytes)

# Oracle 11g Database Installation on AIX

## Checking the Hardware Requirements

- [Memory Requirements](#)
- [System Architecture](#)
- [Disk Space Requirements](#)
- [Display Requirements](#)
- [Run Level Requirement](#)

### Memory Requirements

- The following are the memory requirements for installing Oracle Database 11g Release 2
  - Minimum: 1 GB of RAM
  - Recommended: 2 GB of RAM or more
- To determine the RAM size, enter the following command:  
`# /usr/sbin/lsattr -E -l sys0 -a realmem`
- If the size of the RAM is less than the required size, then you must install more memory before continuing.
- The following table describes the relationship between the installed RAM and the configured swap space recommendation.

RAM	Swap Space
Between 1 GB and 2 GB	1.5 times the size of the RAM
Between 2 GB and 16 GB	Equal to the size of the RAM
More than 16 GB	16 GB

- To determine the size of the configured swap space, enter the following command:  
`#/usr/sbin/lspvs -a`

### System Architecture

- To determine if the system architecture can run the software, enter the following command:  
`# /usr/bin/getconf HARDWARE_BITMODE`
- To determine if the system is started in 64-bit mode, enter the following command:  
`# bootinfo -K`

## **Disk Space Requirements**

- The following are the diskspace requirements for installing Oracle Database11g Release2
  - At least 1 GB of space in the /tmp directory
  - To determine the amount of space available in the /tmp directory, enter the following command:  
`# df -k /tmp`
- The following tables describe the disk space requirements for software files and data files for each installation type on AIX Based Systems:

<b>Installation Type</b>	<b>Requirement for Software Files (GB)</b>
Enterprise Edition	7.51
Standard Edition	7.07

<b>Installation Type</b>	<b>Disk Space for Data Files (GB)</b>
Enterprise Edition	1.75
Standard Edition	1.73

## **Display Requirements**

- The minimum resolution for Oracle Database 11g Release 2 (11.2) is 1024 x 768 or higher.

## **Run Level Requirement**

- Ensure that the system is started with run level 2.

## **Checking the Software Requirements**

- Depending on the products that you intend to install, verify that the following software is installed on your system:
  - [Operating System Requirements](#)
  - [Run Level Requirement](#)
  - [Additional Software Requirements](#)
  - [Patch Requirements](#)

### **Operating System Requirements**

- The following operating system versions (or later) are required for Oracle Database 11g Release
  - AIX 5L V5.3 TL 09 SP1 ("5300-09-01"), 64 bit kernel
  - AIX 6.1 TL 02 SP1 ("6100-02-01"), 64-bit kernel
  - AIX 7.1 TL 0 SP1 ("7100-00-01-1037"), 64-bit kernel

The following operating system filesets are required for AIX 5L:

- bos.adt.base
- bos.adt.lib
- bos.adt.libm
- bos.perf.libperfstat 5.3.9.0 or later
- bos.perf.perfstat
- bos.perf.proctools
- x1C.aix50.rte.10.1.0.0 or later
- gpfs.base 3.2.1.8 or later

The following operating system filesets are required for AIX 6.1:

- bos.adt.base
- bos.adt.lib
- bos.adt.libm
- bos.perf.libperfstat 6.1.2.1 or later
- bos.perf.perfstat
- bos.perf.proctools

- `xlc.aix61.rte:10.1.0.0` or later
- `xlc.rte.10.1.0.0` or later
- `gpfs.base 3.2.1.8` or later

The following operating system filesets are required for AIX 7.1:

- `bos.adt.base`
- `bos.adt.lib`
- `bos.adt.libm`
- `bos.perf.libperfstat`
- `bos.perf.perfstat`
- `bos.perf.proctools`
- `xlc.aix61.rte.10.1.0.0` or later
- `xlc.rte.10.1.0.0` or later
- `gpfs.base 3.3.0.11` or later

To determine the distribution and version of AIX installed, enter the following command:

```
# oslevel -s
```

- For AIX 5L: If the operating system version is lower than AIX 5.3 Technology Level 9 SP 1, then upgrade your operating system to this, or a later, level.
- For AIX 6.1: If the operating system version is lower than AIX 6.1 Technology Level 2 SP 1, then upgrade your operating system to this, or a later, level.
- For AIX 7.1: If the operating system version is lower than AIX 7.1 Technology Level 0 plus SP 1, then upgrade your operating system to this, or a later, level.

AIX maintenance packages are available from the following Web site:

<http://www-933.ibm.com/support/fixcentral/>

- To determine if the required filesets are installed and committed, enter a command similar to the following:

```
# lslpp -l bos.adt.base bos.adt.lib bos.adt.libm bos.perf.perfstat bos.perf.libperfstat  
bos.perf.proctools
```

- To determine the supported kernel mode, enter a command similar to the following:

```
# getconf KERNEL_BITMODE
```

## **Compiler Requirements**

- The following is the minimum compiler requirement for Pro\*C/C++, Oracle Call Interface, Oracle C++ Call Interface, and Oracle XML Developer's Kit (XDK) with Oracle Database 11g Release 2 (11.2):
- IBM XL C/C++ Enterprise Edition for AIX, V9.0 April 2008 PTF:
- You can download this software from the following link:

<http://www-01.ibm.com/support/docview.wss?uid=swg24015075>

## **Patch Requirements**

Installation Type or Product Requirement All installations  
Authorized Problem Analysis Reports (APARs) for AIX 5L:

If you are using the minimum operating system TL level for AIX 5L listed above, then install all AIX 5L V5.3 Authorized Problem Analysis Reports (APARs) for AIX 5L V5.3 TL 09 SP1, and the following AIX fixes:

- IZ42940
- IZ49516
- IZ52331

These 5.3 fixes are present in the following TL levels:

- AIX 5.3 TL-09 SP-05 and later
- AIX 5.3 TL-10 SP-02 and later
- AIX 5.3 TL-11

Authorized Problem Analysis Reports (APARs) for AIX 6L:

If you are using the minimum operating system TL level for AIX 6L listed above, then install all AIX 6L 6.1 Authorized Problem Analysis Reports (APARs) for AIX 6.1 TL 02 SP1, and the following AIX fixes:

- IZ41855
- IZ51456
- IZ52319
- IZ97457

- IZ89165

These 6.1 fixes are present in the following TL levels:

- AIX 6.1 TL-02 SP-04 and later
- AIX 6.1 TL-03 SP-02 and later
- AIX 6.1 TL-04

Authorized Problem Analysis Reports (APARs) for AIX 7L:

If you are using the minimum operating system TL level for AIX 7.1 listed above, then install all AIX 7L 7.1 Authorized Problem Analysis Reports (APARs) for AIX 7.1 TL 0 SP1, and the following AIX fixes:

- IZ87216
- IZ87564
- IZ89165
- IZ97035

### **Creating Custom Configuration Groups and Users for Job Roles**

- Login as root and create te user oracle which belongs to oinstall,dba,asmdba and asmadmin groups.

```
# mkgroup dba
# mkgroup oinstall
# mkgroup asmdba
# mkgroup asmadmin
```

- Choose the appropriate menu items to modify the `oracle` user.
- In the Primary GROUP field, specify the Oracle Inventory group, for example `oinstall`.
- In the Group SET field, specify the required secondary groups, for example `dba, asmdba`.
- To determine if an Oracle software owner user named `oracle`, or `grid` exists, enter a command similar to the following:

```
# id oracle
# id grid
```

- If the `oracle` user exists, then the output from this command is similar to the following:

`id=501(oracle) gid=501(oinstall) groups=502(dba),503(oper)`

- If the `grid` user exists, then the output from this command is similar to the following:

`uid=8001(grid) gid=8001(oinstall)
groups=8001(oinstall),8002(asmadmin),8003(asmdba),8006(dba)`

## Configure Shell Limits

- For AIX, it is the `ulimit` settings that determine process memory related resource limits.
- Verify that the shell limits displayed in the following table are set to the values shown:

Shell Limit (As Shown in smit)	Recommended Value
Soft FILE size	-1 (Unlimited)

Soft CPU time	-1 (Unlimited)
	Note: This is the default value.
Soft DATA segment	-1 (Unlimited)
Soft STACK size	-1 (Unlimited)
Soft Real Memory size	-1 (Unlimited)
Processes (per user)	<p>-1 (Unlimited)</p> <p>Note: This limit is available only in AIX 6.1 or later. Refer to "<a href="#">Configure System Configuration Parameters</a>" for information on configuration of processes per user limits.</p>

- To display the current value specified for these shell limits, and to change them if necessary perform the following steps:
- In the User NAME field, enter the user name of the Oracle software owner, for example `oracle`. Scroll down the list and verify that the value shown for the soft limits listed in the previous table is -1.
- If necessary, edit the existing value. To edit the values, you can use the `smit` utility. However, to set the value of Soft Real Memory size, you must edit the file `/etc/security/limits`. If you have permissions to run `smit` utility, then you automatically have the permissions to edit the `limits` file.

### **Configure System Configuration Parameters**

- If you cannot use the Fixup scripts, then verify that the kernel parameters shown in the following table are set to values greater than or equal to the minimum value shown. If the current value for any parameter is greater than the value listed in this table, then the Fixup scripts do not change the value of that parameter.

Parameter	Recommended Value
maxuprocs	16384
ncargs	128
tcp_ephemeral_low	32768
tcp_ephemeral_high	65535
udp_ephemeral_low	32768
udp_ephemeral_high	65535

## Creating an Oracle Base Directory

- Enter commands similar to the following to create the recommended subdirectories in the mount point directory that you identified and set the appropriate owner, group, and permissions on them:

```
# mkdir -p /mount_point/app/oracle_sw_owner
# chown -R oracle:oinstall /mount_point/app/oracle_sw_owner
# chmod -R 775 /mount_point/app/oracle_sw_owner
```

For example:

```
# mkdir -p /u01/app/oracle
# chown -R oracle:oinstall /u01/app/oracle
# chmod -R 775 /u01/app/oracle
```

## Configuring Display parameters

- **To install oracle Graphically we need to have xmanager.**
- **First we need to download and install on the local system.**
- If you are not installing the software on the local computer, then run the following command on the remote computer to set the `DISPLAY` variable:

Bourne, Bash or Korn shell:

```
$ export DISPLAY=local_host:0.0
```

C shell:

```
% setenv DISPLAY local_host:0.0
```

- In this example, `local_host` is the host name or IP address of the local computer to use to display Oracle Universal Installer.
- Run the following command on the remote system to check if the `SHELL` and the `DISPLAY` environment variables are set correctly:

```
echo $SHELL
```

```
echo $DISPLAY
```

- Now to enable X applications, run the following commands on the local computer:  
`$ xhost + fully_qualified_remote_host_name`
- To verify that the X applications display is set properly, run an X11-based program that comes with the operating system such as `xclock`:  
`$ xclock`
- In this example, you can find `xclock` at `/usr/X11R6/bin/xclocks`. If the `DISPLAY` environment variable is set correctly, then you can see `xclock` on your computer screen. If you get any display errors, see "[X Window Display Errors](#)".

## **Running the rootpre.sh Script**

- Switch user to `root`:
  - `$ su -`
  - `password:`
  - `#`
- Complete one of the following steps, depending on the location of the installation files:
  - If the installation files are on disc, enter a command similar to the following, where `directory_path` is the disc mount point directory or the path of the `db` directory on the DVD:
    - `# /directory_path/rootpre/rootpre.sh`
  - If the installation files are on the hard disk, change the directory to the location where `rootpre.sh` exists and enter the following command:
    - `# ./rootpre.sh`
- Exit from the `root` account:
  - `# exit`

## **Running the ./runInstaller Script**

- Switch user to `oracle`:
- Then execute the script `./runInstaller` installation will start.

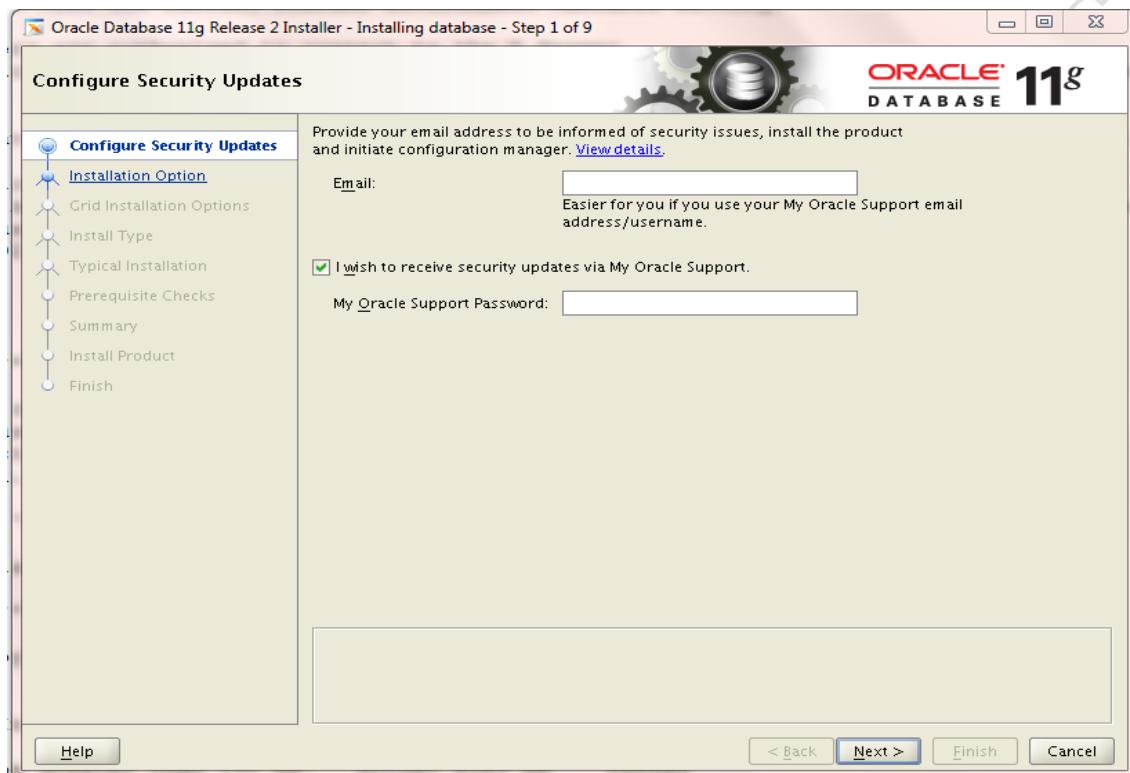
## Oracle Installation Steps

To install the Oracle software, you must use the Oracle Universal installer.

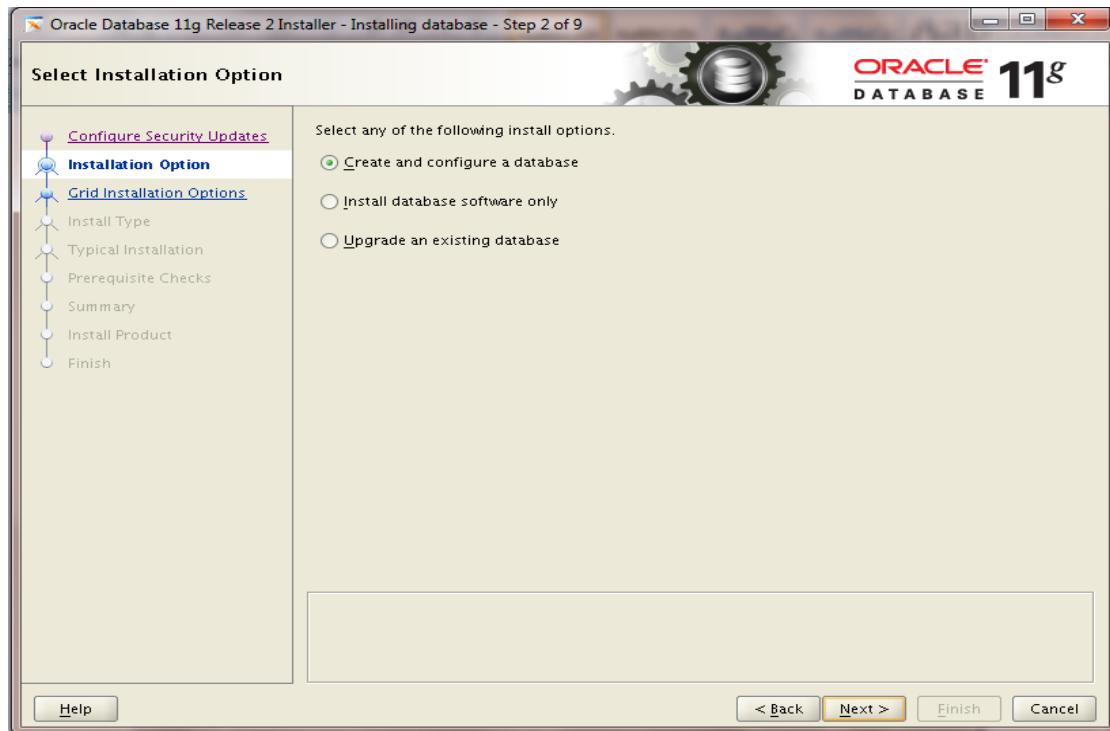
**1. For this installation, you need either the DVDs or a downloaded version of the ISOs.**

**In this tutorial, you install from the downloaded version. From the directory where the ISO files were unzipped, open a terminal window and enter the following:**

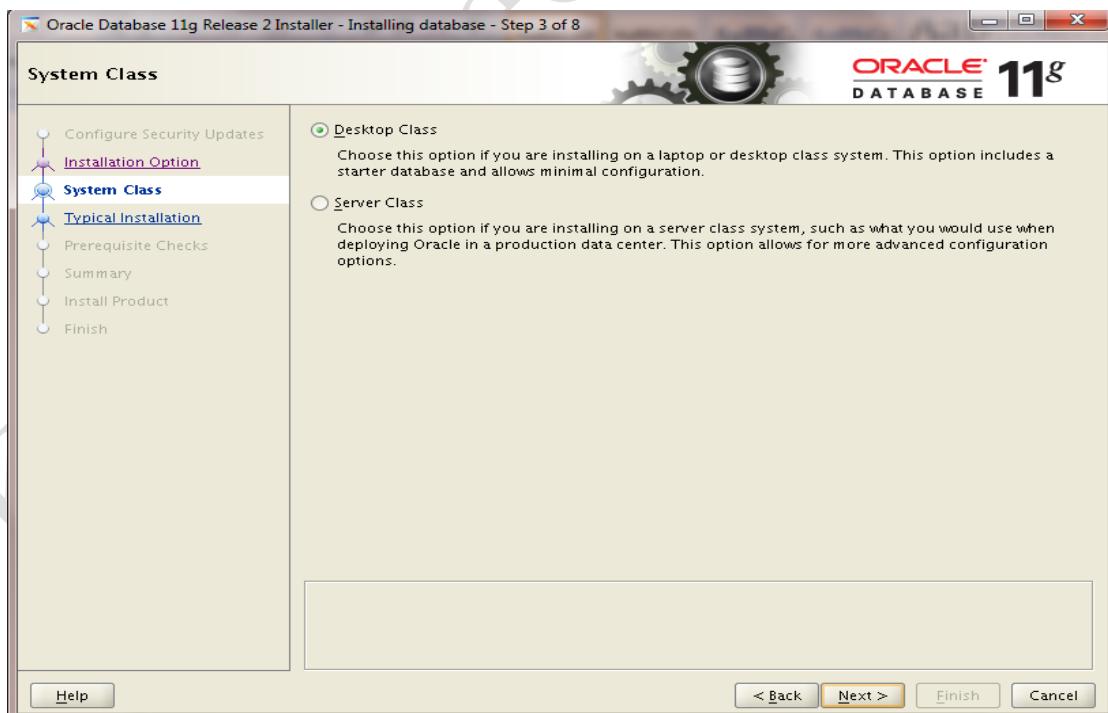
```
./runInstaller.sh
```



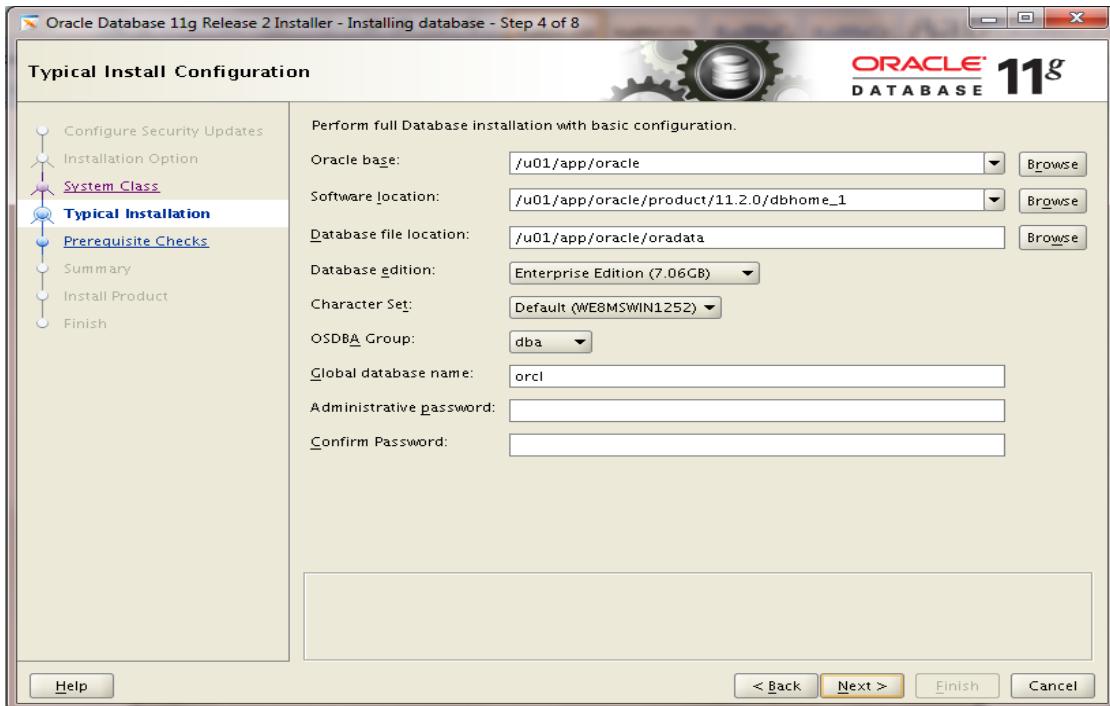
2. The product you want to install is Oracle Database 11g. Make sure the product is selected and click Next.



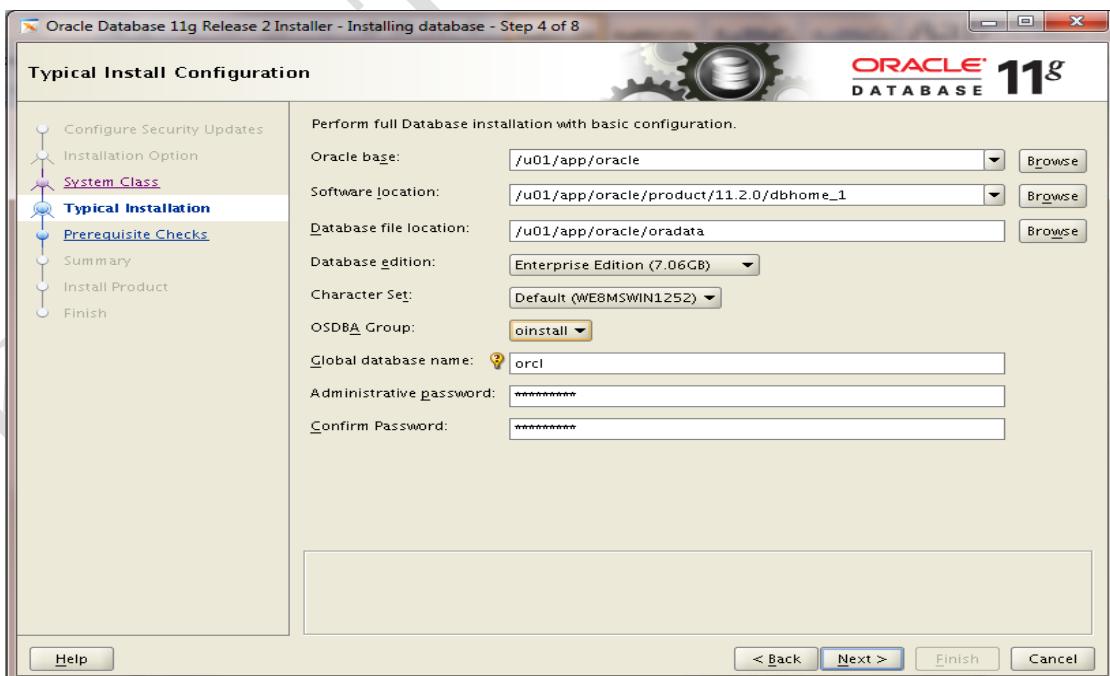
3. Select the class of Database.



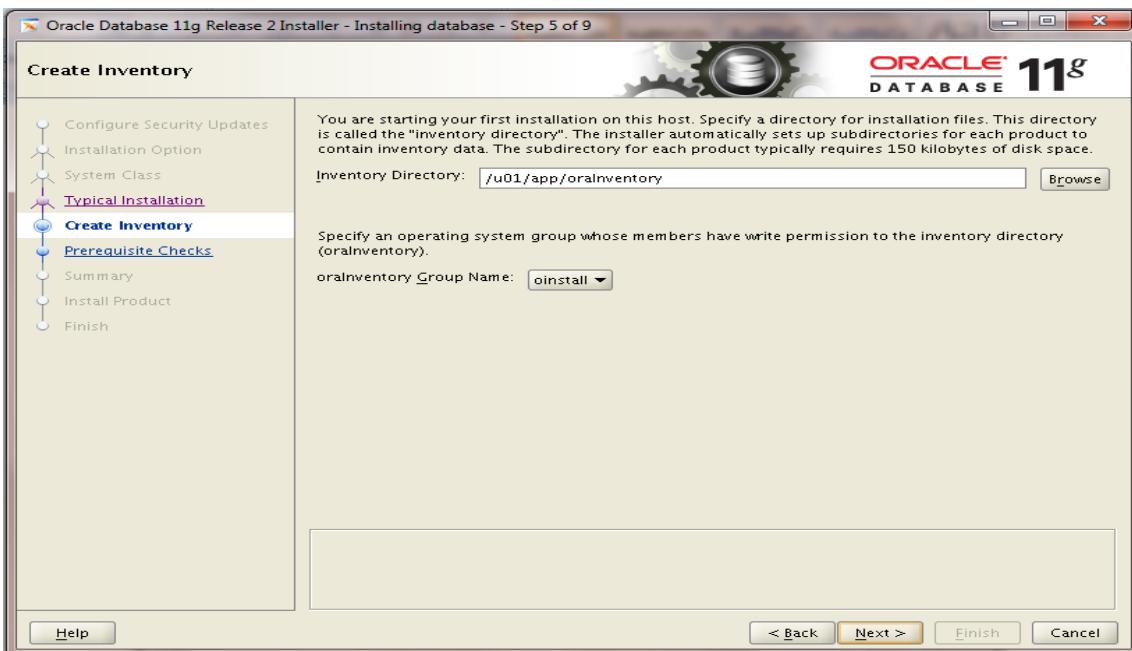
4. You will perform a basic installation with a starter database. Enter orcl for the Global Database Name and oracle for Database Password and Confirm Password. Then, click Next.



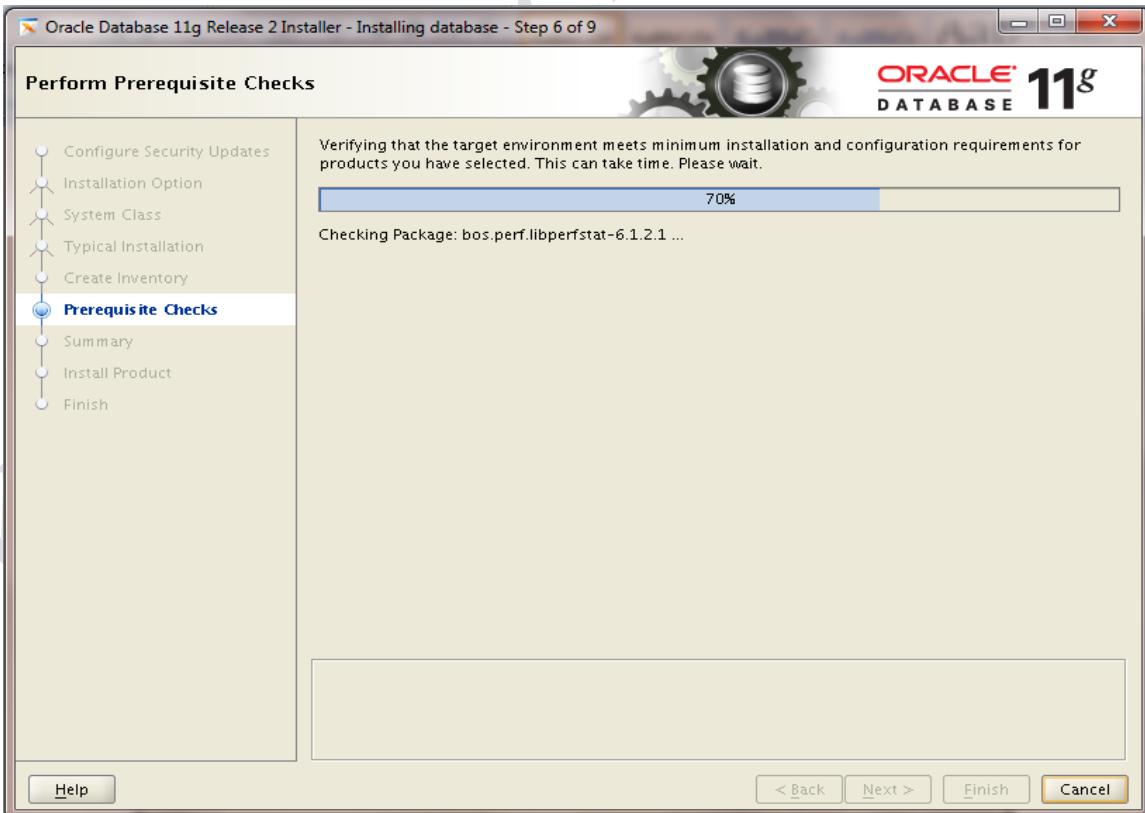
5. You need to specify your Inventory directory. The location should be set to /u01/app/oracle/oraInventory. Accept the default Operating System group name, oinstall. Then, click Next.



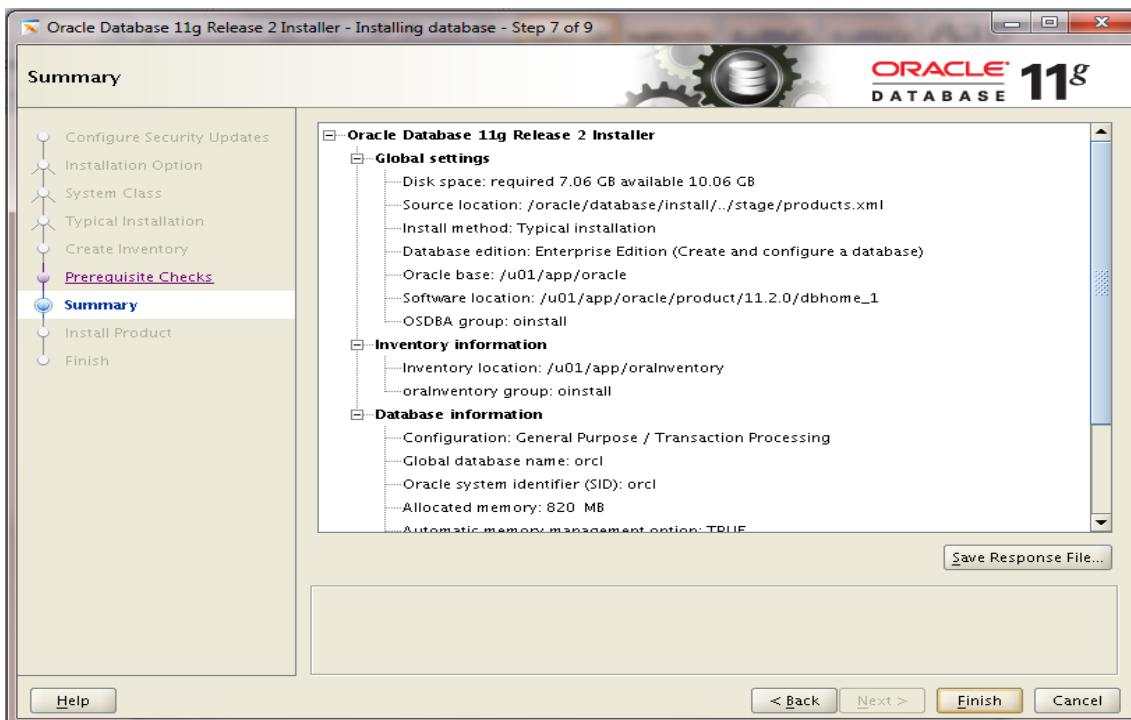
**6.Specify the Directory if installation path, click Next.**



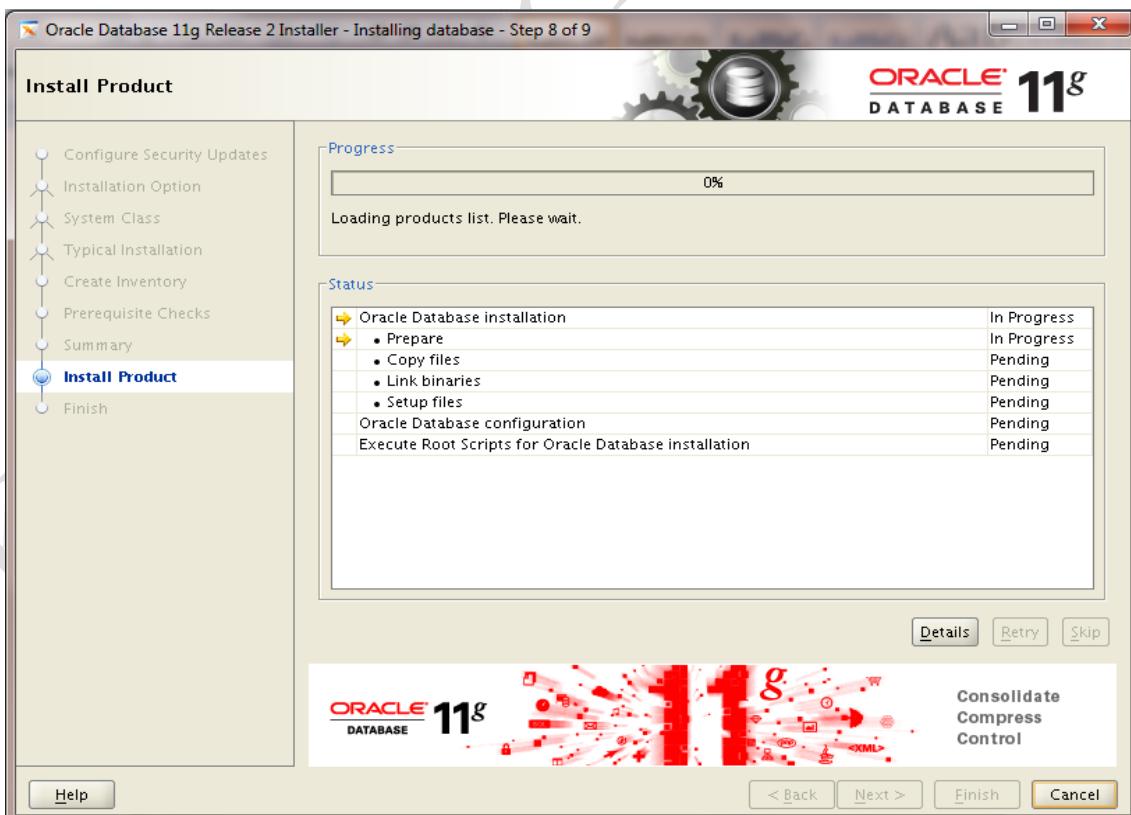
**7.The installer now verifies that the system meets all the minimum requirements for installing and configuring the chosen product. Please correct any reported errors before continuing. When the check successfully completes, click Next**



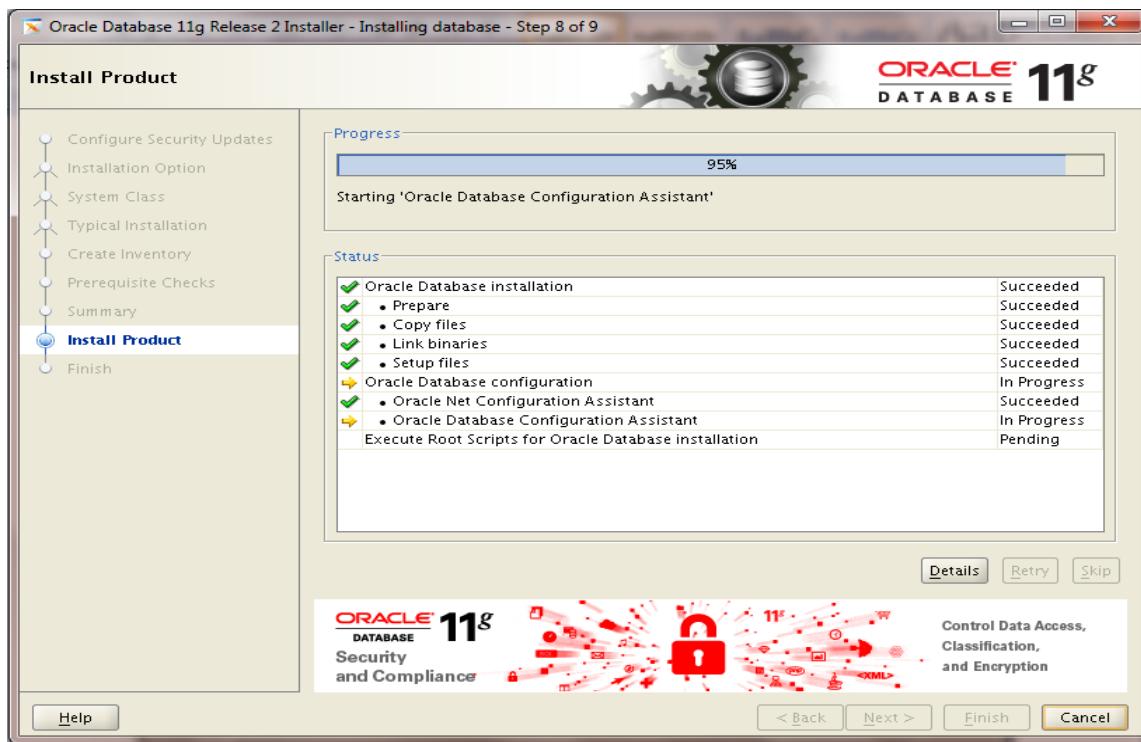
**8. Review the Summary window to verify what is to be installed. Then, click Install**



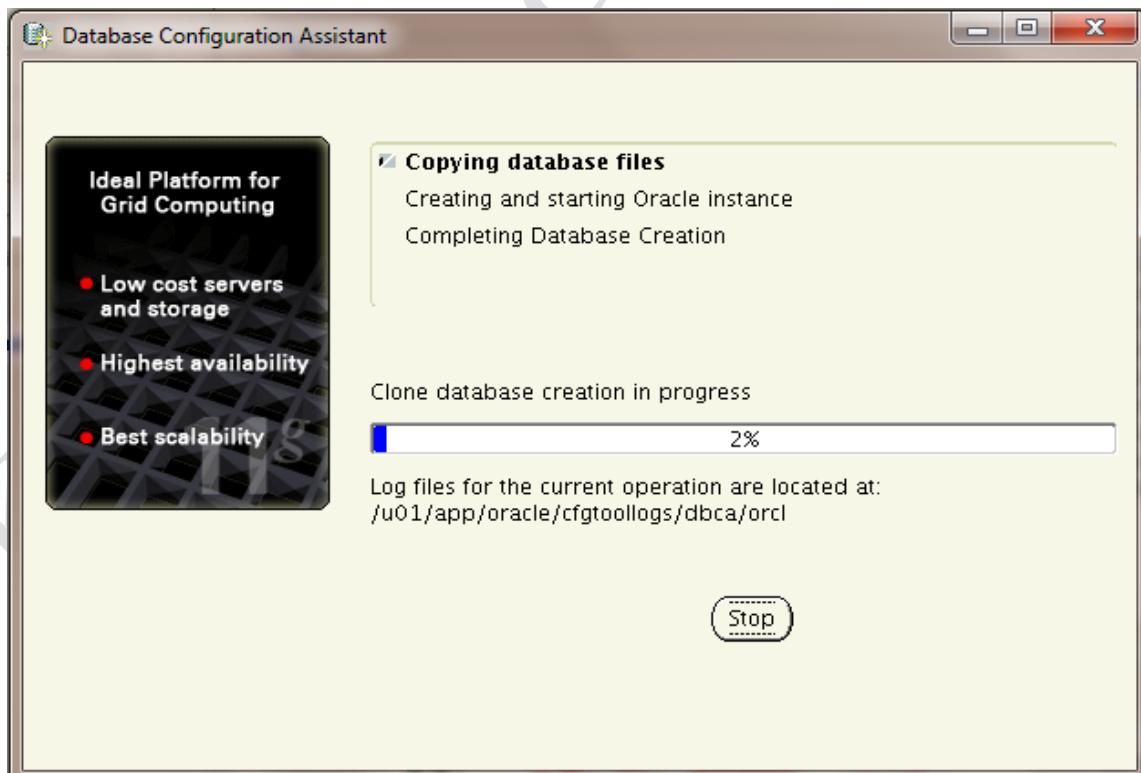
**9. The progress window appears**



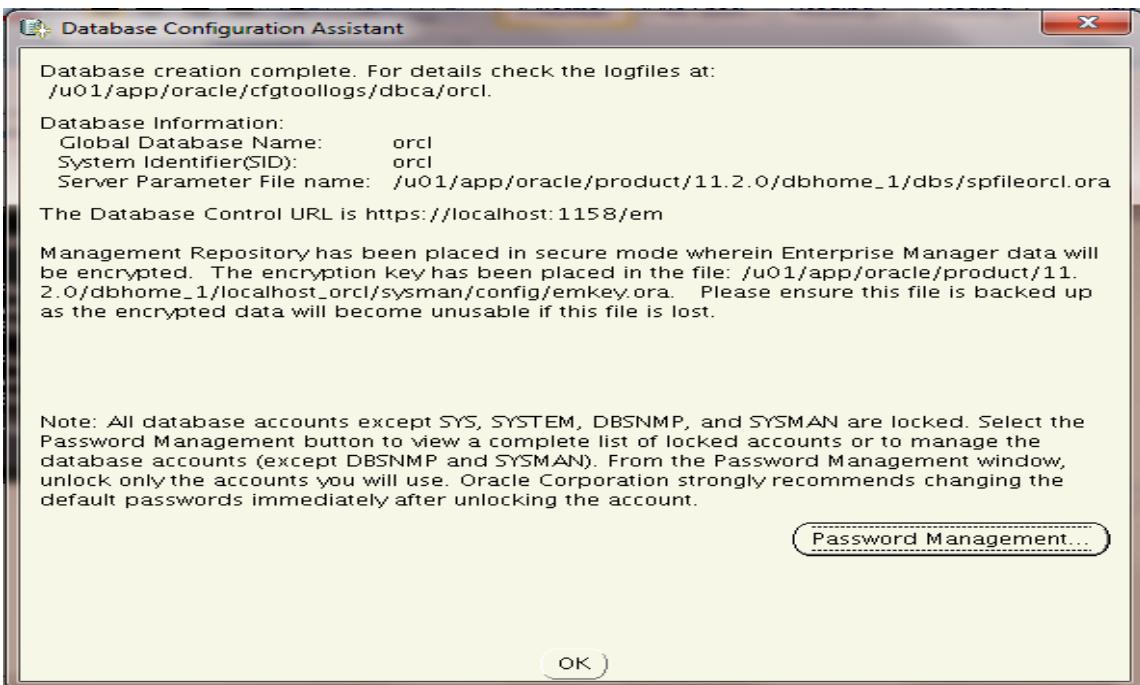
## 10.The Configuration Assistants window appears



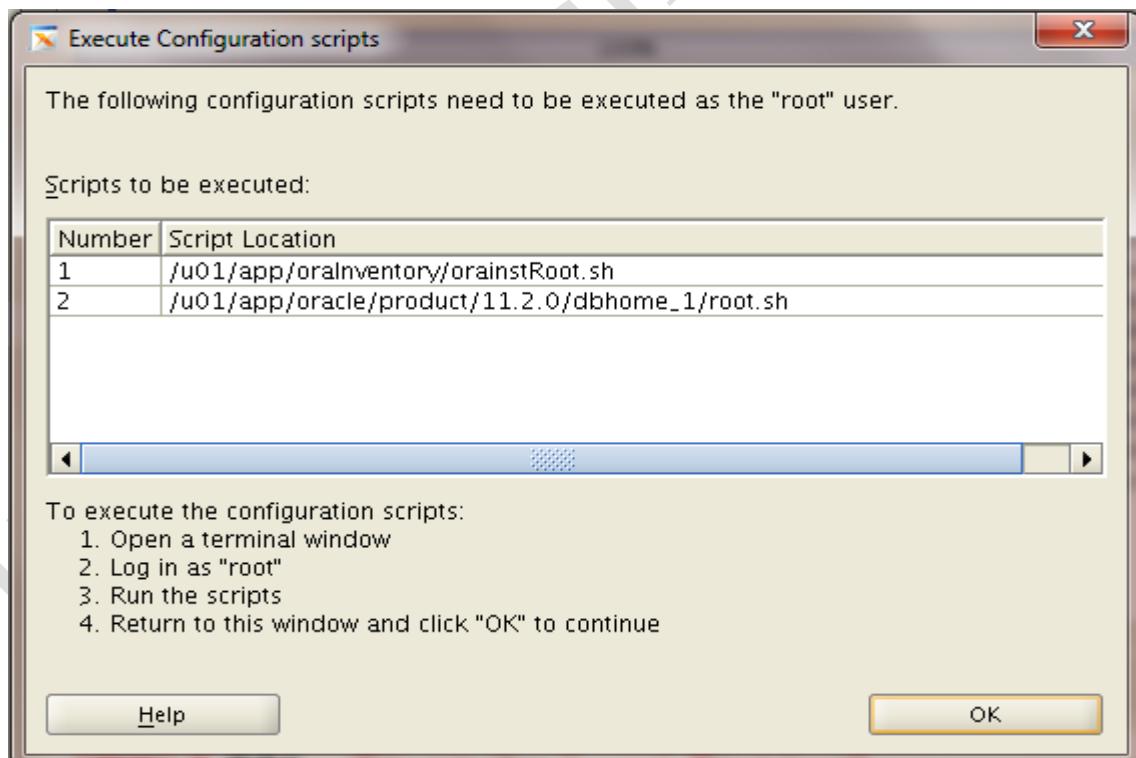
11. Your database is now being created



12. When the database has been created, you can unlock the users you want to use. Click **OK**.



13. You need to execute **orainstRoot.sh** and **root.sh** as the **root** user.



```
bash-3.2# /u01/app/oraInventory/orainstRoot.sh
Changing permissions of /u01/app/oraInventory.
Adding read,write permissions for group.
Removing read,write,execute permissions for world.

Changing groupname of /u01/app/oraInventory to oinstall.
The execution of the script is complete.
```

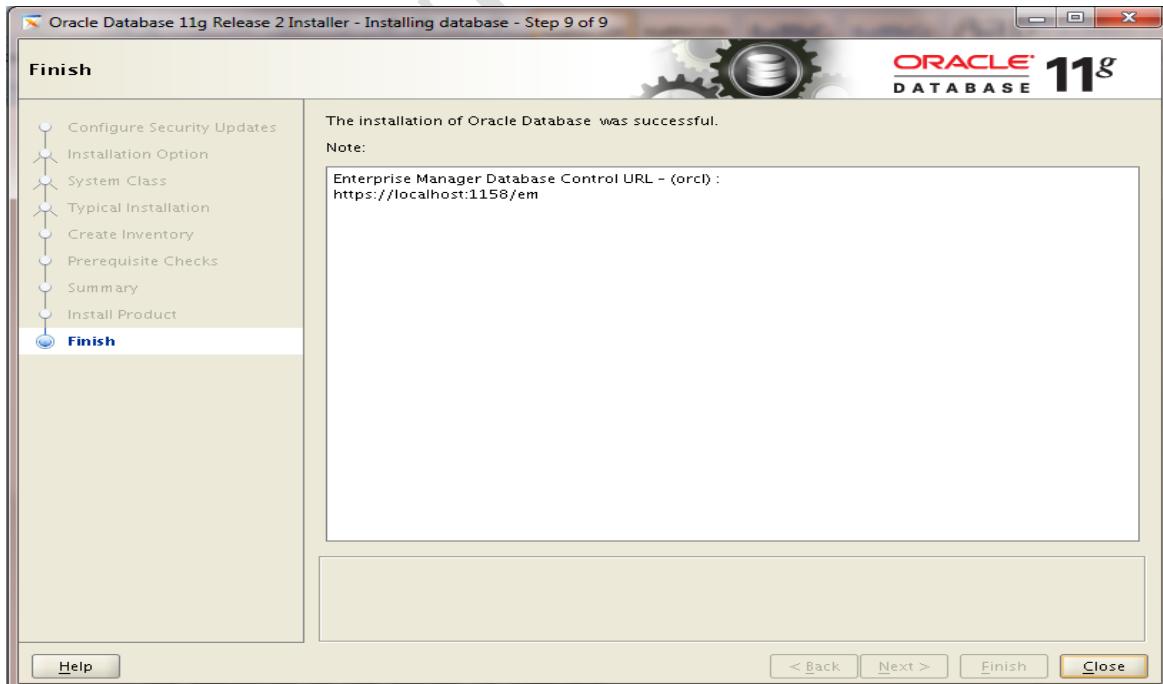
```
bash-3.2# /u01/app/oracle/product/11.2.0/dbhome_1/r
racg/      rdbms/    relnotes/ root.sh
bash-3.2# /u01/app/oracle/product/11.2.0/dbhome_1/root.sh
Running Oracle 11g root.sh script...

The following environment variables are set as:
  ORACLE_OWNER= oracle
  ORACLE_HOME=   /u01/app/oracle/product/11.2.0/dbhome_1

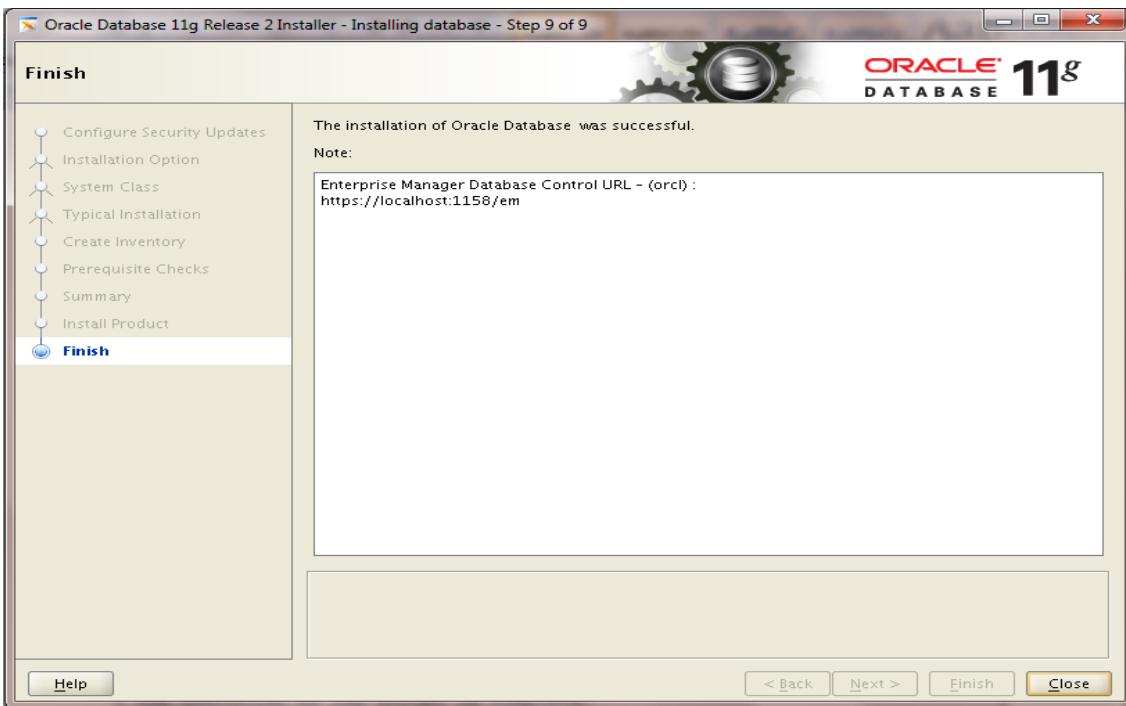
Enter the full pathname of the local bin directory: [/usr/local/bin]:
Copying dbhome to /usr/local/bin ...
Copying oraenv to /usr/local/bin ...
Copying coraenv to /usr/local/bin ...

Creating /etc/oratab file...
Entries will be added to the /etc/oratab file as needed by
Database Configuration Assistant when a database is created
Finished running generic part of root.sh script.
Now product-specific root actions will be performed.
Finished product-specific root actions.
bash-3.2#
```

14.Switch back to the Universal Installer and click **OK**.



## 15.Click Close to complete Installation.



## 16.Configuring oracle user environment.

```
bash-3.2$ . oraenv
ORACLE_SID = [root] ? orcl
The Oracle base for ORACLE_HOME=/u01/app/oracle/product/11.2.0/dbhome_1 is /u01/app/oracle
```

Now Database is ready to use.

To connect to Database issue following command.

```
bash-3.2$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.1.0 Production on Tue Aug 28 03:00:37 2012

Copyright (c) 1982, 2009, Oracle. All rights reserved.

Connected to an idle instance.

SQL> 
```

Now start the database by issuing following command

```
SQL> startup
ORACLE instance started.

Total System Global Area  855982080 bytes
Fixed Size                  2211584 bytes
Variable Size                545259776 bytes
Database Buffers            306184192 bytes
Redo Buffers                 2326528 bytes
Database mounted.
Database opened.
SQL> 
```

To see the databases in oracle issue the following command

```
SQL> select name from v$database;  
NAME  
-----  
ORCL
```

To view the database files

```
SQL> select name from v$datafile;  
NAME  
-----  
/u01/app/oracle/oradata/orcl/system01.dbf  
/u01/app/oracle/oradata/orcl/sysaux01.dbf  
/u01/app/oracle/oradata/orcl/undotbs01.dbf  
/u01/app/oracle/oradata/orcl/users01.dbf  
/u01/app/oracle/oradata/orcl/example01.dbf
```

To see the control files in database

```
SQL> select name from v$controlfile;  
NAME  
-----  
/u01/app/oracle/oradata/orcl/control01.ctl  
/u01/app/oracle/flash_recovery_area/orcl/control02.ctl  
SQL> ■
```

## MISCELLANEOUS COMMANDS IN AIX

### Devices

- ↳ List all devices on a system  
# lsdev
- ↳ List all disk devices on a system (See next item for a list of classes)  
# lsdev -Cc disk
- ↳ List all customized (existing) device classes (-P for complete list)  
#lsdev -C -r class
- ↳ Remove hdisk5  
# rmdev -dl hdisk5
- ↳ Get device address of hdisk1  
# getconf DISK DEVNAME hdisk1 (or) bootinfo -o hdisk1
- ↳ Get the size (in MB) of hdisk1  
# getconf DISK SIZE /dev/hdisk1 (or) bootinfo -s hdisk1
- ↳ List all disks belonging to scsi0  
# lsdev -Cc disk -p scsi0
- ↳ Find the slot of a PCI Ethernet adapter  
# lsslot -c pci -l ent0
- ↳ Find the (virtual) location of an Ethernet adapter  
# lscfg -l ent1
- ↳ Find the location codes of all devices in the system  
# lscfg
- ↳ List all MPIO paths for hdisk0  
# lspath -l hdisk0
- ↳ Find the WWN of the fcs0 HBA adapter  
# lscfg -vl fcs0 | grep Network
- ↳ Temporarily change console output to /console.out  
# swcons /console.out ! (Use swcons to change back.)
- ↳ Get statistics and extended information on fcs0  
# fcstat fcs0
- ↳ **Mount a CD/DVD ROM to /mnt**  
# mount -rv cdrfs /dev/cd0 /mnt ! (for a CD)  
# mount -v udfs -o ro /dev/cd0 /mnt ! (for a DVD)
  - Note the two di\_erent types of read-only ags. Either is Ok.
- ↳ **Create a VG, LV, and FS, mirror, and create mirrored LV**  
# mkvg -s 256 -y datavg hdisk1 (PP size is 1/4 Gig)  
# mklv -t jfs2log -y dataloglv datavg 1  
# logform /dev/dataloglv  
# mklv -t jfs2 -y data01lv datavg 8 ! (2 Gig LV)  
# crfs -v jfs2 -d data01lv -m /data01 -A yes  
# extendvg datavg hdisk2  
# mklvcopy dataloglv 2 ! (Note use of mirrorvg in next example)  
# mklvcopy data01lv 2

```
# syncvg -v datavg  
# lsvg -l datavg will now list 2 PPs for every LP  
# mklv -c 2 -t jfs2 -y data02lv datavg 8 ! (2 Gig LV)  
# crfs -v jfs2 -d data02lv -m /data02 -A yes  
# mount -a
```

↳ **Move a VG from hdisk1 to hdisk2**

```
# extendvg datavg hdisk2  
# mirrorvg datavg hdisk2  
# Wait for mirrors to synchronize  
# unmirrorvg datavg hdisk1  
# reducevg datavg hdisk1
```

↳ **Find the free space on PV hdisk1**

```
# lspv hdisk1! (Look for \FREE PPs")
```

## Networking

- ↳ The entX is the physical device. It is associated with physical layer settings such as link speed, and duplex. enX and etX determine the frame type run on entX . IP addresses are con\_gured on enX (Standard Ethernet) or etX (802.3). Typically only enX is used.
- ↳ The examples here assume that the default TCP/IP con\_guration (rc.net) method is used. If the alternate method of using rc.bsdnet is used then some of these examples may not apply.

↳ Determine if rc.bsdnet is used over rc.net

```
# lsattr -El inet0 -a bootup option
```

↳ TCP/IP related daemon startup script

```
# /etc/rc.tcpip
```

↳ To view the route table

```
# netstat -r
```

↳ To view the route table from the ODM DB

```
lsattr -EHI inet0 -a route
```

↳ Temporarily add a default route

```
# route add default 192.168.1.1
```

↳ Temporarily add an address to an interface

```
# ifconfig en0 192.168.1.2 netmask 255.255.255.0
```

↳ Temporarily add an alias to an interface

```
# ifconfig en0 192.168.1.3 netmask 255.255.255.0 alias
```

↳ To permanently add an IP address to the en1 interface

```
# chdev -l en1 -a netaddr=192.168.1.1 -a netmask=0xffffffff00
```

↳ Permanently add an alias to an interface

```
# chdev -l en0 -a alias4=192.168.1.3,255.255.255.0
↳ Remove a permanently added alias from an interface
# chdev -l en0 -a delalias4=192.168.1.3,255.255.255.0
↳ List ODM (next boot) IP configuration for interface
# lsattr -El en0
↳ Permanently set the hostname
# chdev -l inet0 -a hostname=kt
↳ List networking devices
# lsdev -Cc tcip
↳ List Network Interfaces
# lsdev -Cc if
↳ List attributes of inet0
# lsattr -Ehl inet0
↳ List (physical layer) attributes of ent0
# lsattr -El ent0
↳ List (networking layer) attributes of en0
# lsattr -El en0
↳ Set (desired) speed is found through the entX device
# lsattr -El ent0 -a media speed
↳ Find actual (negotiated) speed, duplex, and link
# entstat -d ent0
↳ The interface must be up (ifconfig en0 up) for stats to be valid
↳ Set the ent0 link to Gig full duplex
# chdev -l ent0 -a media speed=1000 Full Duplex -P
↳ Auto Negotiation is another option
↳ Turn o_Interface Speci_c Network Options
# no -p -o use isno=0
↳ Get (long) statistics for the ent0 device (remove -d for shorter results)
# entstat -d ent0 (or) netstat -v ent0
↳ The results of entstat vary by device type. Virtual, physical, and
↳ IVE (LHEA) devices all produce different results.
↳ List all open, and in use TCP and UDP ports
# netstat -anf inet
↳ List all LISTENing TCP ports
# netstat -na | grep LISTEN
↳ Remove all TCP/IP configuration from a host
# rmtcpip
↳ Flush the netcd DNS cache
# netcdctrl -t dns -e hosts -f
↳ Hostname lookup order is determined using /etc/irs.conf,
# /etc/netsvc.conf and then $NSORDER. irs.conf and $NSORDER
are typically not used.
↳ IP packets can be captured using iptrace / ipreport or tcpdump
```

## Error Logging

- ↳ Error logging is provided through: alog, errlog and syslog.  
# alog - boot, console messages, NIM, others  
# errlog - hardware, kernel, and some apps  
# syslog - Internet dameons, and apps
- ↳ Display the contents of the boot log  
# alog -o -t boot
- ↳ Display the contents of the console log  
# alog -o -t console
- ↳ List all log types that alog knows  
# alog -L
- ↳ Display the contents of the system error log  
# errpt (Add -a or -A for varying levels of verbosity)
- ↳ Clear all errors up until x days ago.  
# errclear x
- ↳ List info on error ID FE2DEE00 (IDENTIFIER column in errpt output)  
# errpt -aDj FE2DEE00
- ↳ Put a \tail" on the error log  
# errpt -c
- ↳ List all errors that happened today  
# errpt -s `date +%m%d0000%y`
- ↳ To list all errors on hdisk0  
# errpt -N hdisk0
- ↳ To list details about the error log  
# /usr/lib/errdemon -l
- ↳ To change the size of the error log to 2 MB  
# /usr/lib/errdemon -s 2097152
- ↳ syslog.conf line to send all messages to log \_le  
# debug /var/log/messages
- ↳ AIX uses \*.debug for all, not \*.\*

## Logical volume Manager

- ↳ Put a PVID on a disk  
# chdev -l hdisk1 -a pv=yes
- ↳ PVIDs are automatically placed on a disk when added to a VG
- ↳ Remove a PVID from a disk  
# chdev -l hdisk1 -a pv=clear
- ↳ List all PVs in a system (along) with VG membership  
# lspv
- ↳ Create a VG called datavg using hdisk1 using 64 Meg PPs  
# mkvg -y datavg -s 64 hdisk1
- ↳ Create a LV on (previous) datavg that is 1 Gig in size

```

# mklv -t jfs2 -y datalv datavg 16
↳ List all LVs on the datavg VG
# lsvg -l datavg
↳ List all PVs in the datavg VG
# lsvg -p datavg
↳ Take the datavg VG offline
# varyoffvg datavg
↳ Remove the datavg VG from the ODM
# exportvg datavg
↳ Import the VG on hdisk5 as datavg
# importvg -y datavg hdisk5
↳ Vary-on the new datavg VG (can use importvg -n)
# varyonvg datavg
↳ List all VGs (known to the ODM)
# lsvg
↳ List all VGs that are online
# lsvg -o
↳ Check to see if underlying disk in datavg has grown in size
# chvg -g datavg
↳ Move a LV from one PV to another
# migratepv -l datalv01 hdisk4 hdisk5
↳ Delete a VG by removing all PVs with the reducevg command.
# reducevg hdisk3 (-d removes any LVs that may be on that PV)
↳ Note: See additional examples in \tasks" section.

```

## **SMITTY FAST PATHS**

- ↳ Find a smitty Fast Path by walking through the smitty screens to get to the screen you wish. Then Hit F8. The dialog will tell you what Fast Path will get you to that screen. (F3 closes the dialog.)

lvm	- LVM Menu
mkvg	- Screen to create a VG
configtcp	- TCP/IP Configuration
eadap	- Ethernet adapter section
fcsdd	- Fibre Channel adapter section
chgsys	- Change / Show characteristics of OS
users	- Manage users (including ulimits)
devdrpci	- PCI Hot Plug manager

etherchannel - EtherChannel / Port Aggregation

↳ **System Resource Controller**

- ↳ Most SRC based services are started from /etc/rc.tcpip
  - # Start the xntpd service
  - # startsrc -s xntpd
- ↳ Stop the NFS related services
  - # stopsrc -g nfs
- ↳ Refresh the named service
  - # refresh -s named
- ↳ List all registered services on the system
  - # lssrc -a
- ↳ Show status of ctrmc subsystem
  - # lssrc -l -s ctrmc

↳ **Performance Monitoring (yDenotes trace based tools.)**

- ↳ **CPU**
  - # mpstat, topas -P, w, lparstat, ps, iostat -tT 1, tprofy, curty

↳ **Memory**

- # vmstat, svmon, ps -o fields , topas, ipcs -m

↳ **Network I/O**

- # [ent|tok|fddi|atm]stat, netstat, netpmony, topas -E

↳ **Disk I/O**

- # iostat, fcstat, lvmstat, filemon, fileplace, topas -D

↳ **Application**

- # truss, probevue, tprofy, svmon -P pid , ps -o fields -p pid topas

- ↳ The character toggles to nmon-mode in topas

↳ **Other**

- ↳ Check for disk stat history collection
- ↳ lsattr -HEI sys0 -a iostat
- ↳ Enable historical disk statistic collection
- ↳ chdev -l sys0 -a iostat=true

↳ **Working with Packages**

- ↳ List all \_les in bos.games \_leset.
- ↳ lspp -f bos.games
- ↳ Find out what \_leset \fortune" belongs to.
- ↳ lspp -w /usr/games/fortune
- ↳ List packages that are above the current OS level
- ↳ oslevel -g
- ↳ Find packages below a speci\_ed (ML/TL)
- ↳ oslevel -rl 5300-05

- ↳ List all \_lesets
- ↳ lslpp -L
- ↳ List all \_lesets in a grepable or awkable format
- ↳ lslpp -Lc
- ↳ Find the package that contains the \_lemon utility
- ↳ which fileset filemon
- ↳ Install the database (from CD/DVD) for which fileset
- ↳ installp -ac -d /dev/cd0 bos.content list
- ↳ Create a mksysb backup of the rootvg volume group
- ↳ mksysb -i /mnt/server1.mksysb.`date +%m%d%y`
- ↳ Cleanup after a failed install
- ↳ installp -C
  
- ↳ Memory / Swap\_le
- ↳ List size, summary, and paging activity by paging space
- ↳ lsps -a
- ↳ List summary of all paging space
- ↳ lsps -s
- ↳ List the total amount of physical RAM in system
- ↳ lsattr -El sys0 -a realmem
- ↳ Create a new paging device on rootvg of 64 PPs
- ↳ mkps -a -s 64 -n rootvg
- ↳ Extend the existing paging space by 8 PPs
- ↳ chps -s 8 hd6