Installation and Configuration [6]

This chapter describes installation and configuration procedures for the UNICOS under UNICOS feature. This chapter is only useful for understanding UNICOS under UNICOS configuration issues. Step-by-step instructions are described in Chapter 7, page 23.

6.1 Installation

The UNICOS under UNICOS feature is installed with the base UNICOS product. No special kernel configuration or build is required. To install UNICOS, see the *UNICOS Installation Guide*, Cray Research publication SG–2112.

6.2 Configuration

The following sections describe considerations for configuring a guest system.

6.2.1 Guest feature configuration

The UNICOS under UNICOS feature is configured by using the UNICOS Installation/Configuration Menu System. An example configuration session is shown in Section 7.1. In this section, the term *guest user* refers to any user who has the user database (UDB) privileges required to boot a guest kernel. These privileges are discussed in detail in section Section 7.1.5, page 29.

This menu system performs the following functions:

- Controls disk media access by user
- Converts old structures to new ones
- Imports existing UNICOS under UNICOS configuration information into the menu system configuration database

For this feature, you will need to specify site-specific information in the following areas:

- UNICOS under UNICOS (guest) configuration

  Allows you to configure the options of the UNICOS under UNICOS feature.

- Guest defaults

Sets global default values for all guest users.

- Guest logical device authorization

  Validates users to mount and unmount specific logical disk devices by using the `guest`(1) command.

- Guest file link configuration

  Allows you to specify a list of files that should be linked at multiuser startup to a host or guest counterpart, depending on the running system type.

- Guest user validation

  Allows you to authorize guest users and to further restrict or enhance their capabilities from configured guest defaults.

For information on using the menu system, see the *UNICOS System Configuration Using ICMS*, Cray Research publication SG–2412.

6.2.2 File system considerations

This section describes things you should consider when preparing your file systems for use by a guest.

- General information

  Although physical disks can be shared between host and guest, a disk or SSD slice opened on the host cannot be opened on the guest. The host ensures that this requirement is met. An attempt to do so causes an open error on the guest.

  Your `/tmp` and `/swap` space will need to be sufficient to support whatever size load you intend to run on the guest.

  Note: Nonsecure file systems cannot be mounted under a UNICOS multilevel security (MLS) host or guest. Nonsecure file systems may be network file system (NFS) mounted, and in this case, the file systems are restricted to one security label that is defined in the network access list (NAL) entry for the NFS host. If a process is executing with a security label that is unequal to that of the NFS server, the MLS system mandatory access control (MAC) policy will prevent write operations to the NFS-mounted files.

- Guest systems require the following file systems:

  ```
  root
  usr
  swap
  ```

  Typically, `/swap` space can be allocated from unused (available) disk or SSD space. For information on restrictions on SSD usage in a guest, see Section 7.1.1, page 23

- You are advised to have a `/tmp` file system.

- To minimize the impact of having a guest environment coexisting on your hardware platform, you should consider how you want to divide and configure your resources (because a backup or build root file system probably will be used on a guest).

  Traditionally, it has been recommended that you keep your backup root (and backup `/usr`) on a separate device. However, to minimize channel contention and to maintain peak performance when your guest is running, you should consider dividing your host and guest file systems, as shown in Figure 2.

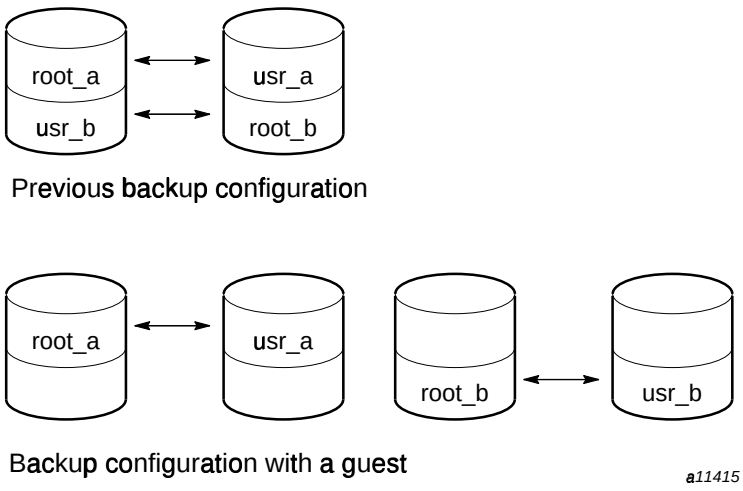

Figure 2. File system disk location

- When mounting the home or other file system(s) for use on a guest, you may consider NFS mounting the host's user file system(s). This provides users immediate access to their existing directories and files.

  Note: If you choose this method for home or other file systems, be sure that users understand that the file system is NFS mounted and is not a virtual copy. All changes will take effect on the host file system. Applications and scripts that usually write to these directories may appear to have failed when run simultaneously on the host and the guest. To avoid this, work in the `$TMPDIR` directory, write output files to `$TMPDIR` (which is local to each system), or append the system's `uts` node name (obtained with `uname -n`) to output file names.

  The user `root` does not have any special permission on an NFS-mounted file system unless you specify: `root=`*hostname* in the `/etc/exports` file. See the `exportfs`(8) man page for more information. If you do not give the guest system NFS-root permission on the host, programs that run as `root` and attempt to create or change files on these NFS file systems will exit abnormally. This can be avoided by running in the `$TMPDIR` directory as well.

6.2.3 IOS parameter files

Before running a guest, you may have to make some minor modifications to your current system's parameter file. The changes are discussed using excerpts from the parameter files. Changes also can be managed by using the UNICOS Installation/Configuration Menu System.

For complete parameter file information and examples, see Section 7.1.3, page 24.

6.2.4 MLS considerations

When a UNICOS multilevel security (MLS) guest runs under a non-MLS UNICOS host, or a non-MLS UNICOS guest runs under a UNICOS MLS host, the full protection of UNICOS MLS is not available. Users of the non-MLS component may be able to gain access to resources controlled by the MLS component, thereby compromising MLS security policies. Although such a configuration is suitable for experimental use of UNICOS MLS, it is not recommended for an MLS production environment.

In a mixed MLS/non-MLS environment, certain file systems are labeled for use under UNICOS MLS, and other file systems are not. Unless a file system is labeled, UNICOS MLS will reject attempts to mount it.

Under non-MLS UNICOS, a secure file system may be mounted only if the `SECURE_MOUNT` configuration option is disabled. Note that MLS attributes of files are not maintained by non-MLS UNICOS, nor are the MLS security policies enforced. As a result, the security of MLS file systems may be compromised if they are mounted under non-MLS UNICOS.

When a UNICOS MLS guest is run with a UNICOS MLS host, the security protections for file systems and data are maintained. However, this configuration is not part of the Cray ML-Safe system configuration.

6.2.5 Configuration links

The UNICOS under UNICOS feature allows you to specify a list of files that should be linked at multiuser startup to host and guest counterparts (such as `.host` or `.guest`) depending on the running system type. It is generally best to configure **all** root file systems on your system to run as both a host or a guest. But when getting started, the configuration links are only required on the root file system, which will be run as a guest.

Although guest and host versions of selected configuration files are not necessary, they do facilitate the use of a single root as either a host or a guest root. By doing this you will facilitate future installations. Take, for example, `/etc/fstab`. Because a guest is not allowed to access physical disk slices mounted on the host, retaining the same `fstab`(5) file (for both host and guest) will result in a significant number of open errors at guest multiuser startup. To avoid such errors, you should create multiple versions of the `/etc/fstab` file so that only the appropriate file systems are mounted when the root is run as either a guest or a host.

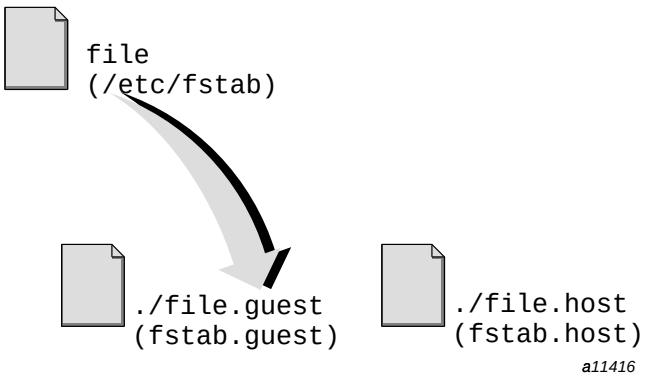

Figure 3. Example link for a system running as a guest

Note: These steps are instructional in nature and **should not** be executed at this time.

To create this link, take the following steps:

1. Invoke the UNICOS Installation/ Configuration Menu System by entering the following commands:

   ```
   cd /mntl/etc/install
   ./install
   ```

2. These commands get you into the main installation menu. Select the following from the menu:

   ```
   M-> Configure System
   ```

3. Select the following option:

   ```
         Asynchronous libraries configuration ==>
         Dumpsys utility configuration ==>
   M->   UNICOS under UNICOS (guest) configuration ==>
         Miscellaneous software configuration ==>
         Import the configuration ...
         Activate the configuration ...
   ```

4. Add `/etc/fstab` to the list of guest configuration files in the `Guest File Link Configuration` menu.

5. Activate the guest configuration.

6. Select and execute `Create Guest and Host versions of files`. This creates the `/etc/fstab.host` and `/etc/fstab.guest` files.

7. Go back to the `Activation Utility` menu, select `Activation Options`, and then select `Activate host or guest versions`. Toggle the selection to `guest` as shown:

```
.   Utilities
.   .   Activation Utility
.   .   .   Activation Options
     Activation root mount poin

     Stop activation on error?                          YES
S->  Activate host or guest versions                    guest
     Activate host or guest versions.
```

8. Go back to the `Import Utility` menu, select `Import Options`, and then select `Import host or guest versions`. Toggle the selection to `guest` as shown:

```
.   Utilities
.   .   Import Utility
.   .   .   Import Options

     Import root mount point                             /
     Stop import on error?                               NO?
S-> Import host or guest versions?                      guest
Reload default import table ...
Activate host or guest versions.
```

9. To import the `fstab` configuration by using the UNICOS Installation/Configuration Menu System, enter the following update screen:

```
.   Configure System
.   .   File System (fstab) Configuration
```

   You are now ready to edit the guest `fstab` information.

10. Remove references to the file systems not needed on the guest system, and activate the `fstab`(5) configuration.

    With the `guest` attribute set in the activation utility, files listed in `/etc/config/guest_config` will be linked to their `.guest` counterparts before the activation. Do not be alarmed if the activation says that it is activating to `/etc/fstab` if your intent is to update `/etc/fstab.guest`.

When a system is booted on this root, / `etc/brc.guest` determines the system type (host or guest) and appropriately sets the soft file links for all files listed in `/etc/config/guest_config.`

11. Return to host `Import/Activate` mode by repeating steps 7 and 8. Choose `host` instead of `guest`.