IBM

Distributed SMIT 2.2 for AIX: Guide and Reference

Distributed SMIT 2.2 for AIX: Guide and Reference

Contents

About This Book

This book provides information about the Distributed System Management Interface Tool (DSMIT). DSMIT adds functionality to the System Management Interface Tool (SMIT). It allows the SMIT interface to build commands for distribution to other machines on a network.

Who Should Use This Book

This book is intended for system administrators performing tasks related to the operation of the DSMIT program. Readers are expected to have a basic knowledge of the System Management Interface Tool (SMIT). For information on using SMIT, see ″System Management Interface Tool (SMIT): Overview″ in *AIX 5L Version 5.1 System Management Guide: Operating System and Devices*.

Highlighting

The following highlighting conventions are used in this book:

Bold	Identifies commands, subroutines, keywords, files, structures, directories, and other items whose names are predefined by the system. Also identifies graphical objects such as buttons, labels, and icons that the user selects.
Italics	Identifies parameters whose actual names or values are to be supplied by the user.
`Monospace`	Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of portions of program code similar to what you might write as a programmer, messages from the system, or information you should actually type.

ISO 9000

ISO 9000 registered quality systems were used in the development and manufacturing of this product.

Related Publications

The following books contain information about or related to DSMIT:
- *Experiences Using DSMIT in Heterogenous Environment and Visual System Management Under AIX Version 4*
- *AIX 5L Version 5.1 System Management Guide: Operating System and Devices*
- *AIX 5L Version 5.1 System Management Guide: Communications and Networks*
- *AIX 5L Version 5.1 General Programming Concepts: Writing and Debugging Programs*
- *AIX 5L Version 5.1 Commands Reference*
- *AIX 5L Version 5.1 Files Reference*

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:
- AIX
- IBM
- Other company, product, or service names may be the trademarks or service marks of others.

Chapter 1. Distributed System Management Interface Tool

The Distributed System Management Interface Tool (DSMIT) adds functionality to the System Management Interface Tool (SMIT) by allowing the SMIT interface to build commands for system management and distribute them to other clients on a network. DSMIT has most of the functionality of the SMIT program, such as fast paths, log files, and flags. The DSMIT facility runs in two interfaces, ASCII (nongraphical) or AIXwindows (graphical).

The DSMIT server runs on AIX Version 4 and the DSMIT clients support the following operating systems:

- AIX 4.1, AIX 4.2, and subsequent versions
- Sun OS 4.1.3
- HP-UX 9.0 700 series
- Solaris 2.3 and 2.4

> **Note:** You must install the DSMIT 2.2 client code with the DSMIT Version 2.2 server. The client code from previous versions of DSMIT does not contain the security enhancements that allow it to interoperate with DSMIT Version 2.2. For the same reason, you cannot install the DSMIT Version 2.2 client code with the server code from previous versions of DSMIT.

Terminology

The following terminology is important in understanding the DSMIT program:

Client or managed machine	Specifies the machines that run commands built by the DSMIT server. The clients wait for the server to issue the information on what commands to run.
Server or managing machine	Specifies the machines that build and distribute commands for running on client machines.
Working collective	Specifies a current list of clients to /receive commands built by DSMIT. The working collective is a temporary list and must be reset with each new DSMIT session.
Domain of clients	Specifies a permanent group of clients on which DSMIT can run commands. Domains are different from the working collective because they do not need to be reset with each new DSMIT session.
Exclude	Excludes members from the working collective, preventing them from receiving commands.
Include	Restores excluded members to the working collective, allowing them to receive commands.
Heterogeneous clients	Specifies a network in which not all clients have the same operating systems.
Homogeneous network	Specifies a network in which all clients have the same operating system. In this case, they can be this operating system, HP, Solaris, or Sun OS.
Intersection	Specifies the list of machines that meet all of the selected criteria.
Union	Specifies the list of machines that meet any of the selected criteria.
DSMIT configuration file server	Specifies the machine that holds the DSMIT security configuration files.

Network Access

The DSMIT program uses networks that support the TCP/IP and UDP/IP communication protocols. DSMIT sends information using sockets.

Network Security

DSMIT security is based on well-established crypto routines and DSMIT specific (modeled after MIT's Kerberos) communication protocols. It provides an ongoing secure DSMIT operation and supports secure modification of the security configuration and updates of passwords and keys.

The DSMIT security characteristics are:

Single Sign-on When single sign-on is enabled, the credentials that allow the DSMIT administrator to run DSMIT are created when the administrator logs in to the system. This is optional. If the DSMIT administrator chooses a DSMIT password different from their system password, the DSMIT password must be provided each time their DSMIT credentials have expired.

Authentication Only the user authenticated as the DSMIT administrator can run DSMIT. A root user on the managing system does not have root access to the managed systems unless the root ID is registered as a DSMIT administrator. Communications between the managing and managed systems are authenticated.

Data Integrity DSMIT uses the Message Authentication Code (MAC) to protect against unauthorized changes or substitutions to data transmissions between the managing and managed systems.

Data Confidentiality Passwords, DSMIT commands, and their output are not passed over the network in the clear. To mask data between the managing and managed systems, DSMIT uses the Commercial Data Masking Facility (CMDF) technology.

Audit Logging DSMIT maintains a log of significant events to keep track of the start and end of DSMIT sessions and the identity of the administrator and the managed and managing systems.

Usage

DSMIT runs in both concurrent and sequential modes. *Concurrent* mode means that the DSMIT server builds a command and routes it to the clients simultaneously. *Sequential* mode means that the DSMIT server builds a command and routes it to the clients one machine at a time. After you build a command on the server and press the Enter key, a menu appears asking in which mode you wish to run DSMIT.

When you use the concurrent mode to submit commands, ASCII DSMIT displays a spinning-wheel graphic to indicate it is processing the commands.

Files

The following DSMIT files are essential to configuration:

/usr/share/DSMIT/domains Defines the groups of clients that the DSMIT server supports.

/usr/share/DSMIT/dsmitos Defines the operating systems that the DSMIT server supports.

/usr/share/DSMIT/hosts Defines the clients that the DSMIT server supports.

/usr/share/DSMIT/security/v5srvtab Stores the local machine's unique DSMIT principal key. This file is present on each managing and managed system. The default location for this file is **/usr/share/DSMIT/security/v5srvtab**.

/usr/share/DSMIT/security/admin.cfg Stores the DSMIT administrator's keys. This file is used by the managing systems. The location for this file is in **/usr/share/DSMIT/security** on the system designated as the DSMIT configuration file server.

/usr/share/DSMIT/security/managing.cfg Stores the intermediate keys. This file is used by the managing systems. The location for this file is in **/usr/share/DSMIT/security** on the system designated as the DSMIT configuration file server.

/usr/share/DSMIT/security/managed.cfg Stores the managed machine's DSMIT principal keys. This file is used by the managing systems. The location for this file is in **/usr/share/DSMIT/security** on the system designated as the DSMIT configuration file server.

/usr/share/DSMIT/security/dsmit.ptr Stores the name of the DSMIT configuration file server. This file is present on each managing system. The location for this file is **/usr/share/DSMIT/security/dsmit.ptr**.

Environment Variables

DSMIT exports the variable **SMIT=d**, which indicates that DSMIT rather than SMIT is running.

If the environment variable **DSMIT_USE_PREV_WC** is set, DSMIT saves the current working collective in its current state to the file **$HOME/.dsmit_prev_wc**. The next time DSMIT is invoked (and the environment variable is still set), DSMIT retrieves the information in **$HOME/.dsmit_prev_wc** to use as the current working collective.

The **$HOME/.dsmit_prev_wc** file is overwritten with the current working collective each time DSMIT exits.

The **-w** and **-W** flags take precedence over **DSMIT_USE_PREV_WC**.

Databases

The DSMIT program uses the same Object Data Manager (ODM) databases that SMIT uses. The databases are located in the **/usr/lib/objrepos** file. If you add any stanzas to the ODM database, DSMIT uses these stanzas to expand its functionality.

Sun-, Solaris-, and HP-specific stanzas are located in the **/usr/share/DSMIT/SunOS_4.1.3**, **/usr/share/DSMIT/Solaris**, and **/usr/share/DSMIT/HP-UX_9.0** directories, respectively. The system creates these directories when the client software is installed for either Sun, Solaris, or HP clients. The **dsmitos** file defines the available operating system types. This file is updated with the SMIT ODM database directory name when the DSMIT client software is installed on the DSMIT server system. During installation of the DSMIT server software, the Symbol.dsmit ODM database directory is linked into the **/usr/share/DSMIT** directory and is added to the **dsmitos** file.

If the systems that are being managed are at a different version, release, or level than the managing system, such as the managing system is running AIX 4.1.3 and the managed system is running AIX 4.1.2, you will need to copy the SMIT stanzas from the managed system to the managing system. This will help you to avoid problems that may occur due to differences in the operating system levels. For example, if a SMIT task uses a new parameter added to a command in AIX 4.1.3, the command will not be understood by previous levels of the operating system. Use the following steps to add support for specific levels of the operating system:

1. On the DSMIT server:
    a. change the current directory to **/usr/share/DSMIT**:

        cd /usr/share/DSMIT

    b. create a new directory in the **/usr/share/DSMIT** directory:

        mkdir NewLevelDirectory

        Note: *NewLevelDirectory* is a specific level of the operating system.
    c. use the **echo** command to write the name of the new directory to the **dsmitos** file:

        echo "NewLevelDirectory" >> dsmitos

    d. change the current directory to the new directory:

        cd NewLevelDirectory

2. Copy an existing SMIT database from the client or a host of the desired level to the server:

    rcp root@client:/usr/lib/objrepos/sm* .

3. Verify that DSMIT client codeis installed on the client. Use SMIT to list the installed software on the client.

    Note: You must install the DSMIT 2.2 client code. The client code from previous versions of DSMIT does not contain the security enhancements that allow it to interoperate with DSMIT Version 2.2.

4. On the server, merge the domain management and working collective dialogs with the SMIT database copied from the client. Temporarily set your ODM path (the directory to access when you run your ODM commands) and add required DSMIT dialogs:

```
ODMDIR=. /usr/bin/odmadd /usr/share/DSMIT/add_files/*.add
```

This is important if the commands being executed has changed between levels of operating system. For example, AIX 4.1.3 of installp will not run on AIX 4.1.1 due to syntax changes in the flags. So it is important that the correct SMIT database that is being used on a managing machine corresponds to the correct level of operating system of the managed machine.

Related Information

"Installing DSMIT".

"Security Configuration for DSMIT" on page 7.

"Modifying DSMIT Security Configuration" on page 9.

"Establishing Single Sign-On" on page 11.

"Starting and Stopping the DSMIT (ASCII or AIXwindows) Interface" on page 13.

"Using the DSMIT Interfaces" on page 14.

"Defining Clients" on page 15, "Defining the Working Collective" on page 15, "Saving the Current Working Collective as a Domain" on page 21.

"Creating a Domain" on page 17, "Changing a Domain" on page 18, "Removing a Domain" on page 20.

"DSMIT Troubleshooting" on page 21.

"Examples of Tasks Performed with DSMIT" on page 25.

The **chdsmitd** command, **dsmit** command, **lsdsmitd** command, **lsdsmitm** command, **mkdsmitd** command, **rmdsmitd** command.

Installing DSMIT

The Distributed System Management Interface Tool (DSMIT) program provides the following software installation package for DSMIT servers and clients:

DSMIT Server   Must be installed on systems designated as DSMIT servers. During installation the following DSMIT configuration files are created:

- **/usr/share/DSMIT/dsmitos**
- **/usr/share/DSMIT/hosts**

> **Note:** Do not install the Distributed SMIT server package operating system on a system that has been defined as a diskless workstation client.

DSMIT Client   You must install the DSMIT 2.2 client code. The client code from previous versions of DSMIT does not contain the security enhancements that allow it to interoperate with DSMIT Version 2.2.

DSMIT provides the following software installation packages to establish DSMIT clients:

DSMIT AIX 4.1 Client   Must be installed on AIX 4.1 systems designated as DSMIT clients.

> **Note:** If you are reinstalling the DSMIT client software package over an existing DSMIT client, do not use DSMIT to do this. You must use the standard installation procedures.

DSMIT Sun OS 4.1.3 Client   Must be installed on systems designated as DSMIT servers for systems running Sun Microsystems' Sun OS 4.1.3 operating system. The installation provides the necessary configuration for DSMIT to support Sun clients.

The installation process creates a shell script and a tar image in the **/usr/share/DSMIT/SunOS_4.1.3/inst.images** directory, which must be copied to the Sun clients. The install script provides the procedures to extract the files from the tar image and update the appropriate system files required to run DSMIT. The tar image contains the DSMIT daemons and programs. Managing devices and subsystems on the Sun system may require special system configuration. See ″System Configuration for Sun OS and HP″ for more information.

DSMIT Solaris Client   Must be installed on systems designated as DSMIT servers for systems running Solaris 2.3 or Solaris 2.4 operating system. The installation provides the necessary configuration for DSMIT to support Solaris clients.

The installation process creates a shell script and a tar image in the **/usr/share/DSMIT/Solaris/inst.images** directory, which must be copied to the Solaris clients. The install script provides the procedures to extract the files from the tar image and update the appropriate system files required to run DSMIT. The tar image contains the DSMIT daemons and programs. Managing devices and subsystems on the Solaris system does not require special system configuration.

DSMIT HP-UX 9.0 Client   Must be installed on systems designated as DSMIT servers for systems running Hewlett-Packard's (HP) HP-UX 9.0 700 series operating system. The installation provides the necessary configuration for DSMIT to support HP clients.

The installation process creates a shell script and a tar image in the **/usr/share/DSMIT/HP-UX_9.0/inst.images** directory, which must be copied to the HP clients. The install script provides the procedures to extract the files from the tar image and update the appropriate system files required to run DSMIT. The tar image contains the DSMIT daemons and programs. Managing devices and subsystems on the HP system may require special system configuration. See ″System Configuration for Sun and HP″ for more information.

> **Note:** If you wish to use the same system as both a DSMIT server and a DSMIT client, you must install both the server and client software packages.

Hardware Requirements

- The following hardware is required for systems installed with the Distributed SMIT server package:
  - POWER family, POWER2, or PowerPC machine configured with at least one supported display and keyboard. For other hardware systems, see your sales representative or your point of sale.
  - A network adapter that supports the TCP/IP and UDP/IP communication protocols such as ethernet or token ring
  - 16MB RAM
  - 2MB of fixed-disk storage
- The following hardware is required for systems installed with the DSMIT client package for AIX 4.1 or later:
  - POWER family, POWER2, or PowerPC machine configured with at least one supported display and keyboard. For other hardware systems, see your sales representative or your point of sale.

- – A network adapter that supports the TCP/IP and UDP/IP communication protocols such as ethernet or token ring
  - – 16MB RAM
  - – 1MB of fixed-disk storage
- The following hardware is required for systems installed with the DSMIT client package for Sun OS 4.1.3:
  - – Sun SPARC system configured with at least one supported display and keyboard
  - – A network adapter that supports the TCP/IP and UDP/IP communication protocols such as ethernet or token ring
  - – Minimum of 16MB RAM
  - – 1.5MB of fixed-disk storage
  - – 2.3MB of fixed-disk storage on the system configured as the DSMIT server
- The following hardware is required for systems installed with the DSMIT client package for Solaris 2.3 or Solaris 2.4:
  - – Solaris 2.3 or Solaris 2.4 system configured with at least one supported display and keyboard
  - – A network adapter that supports the TCP/IP and UDP/IP communication protocols such as ethernet or token ring
  - – Minimum of 16MB RAM
  - – 1.5MB of fixed-disk storage
  - – 2.3MB of fixed-disk storage on the system configured as the DSMIT server
- The following hardware is required for systems installed with the DSMIT client package for HP-UX 9.0:
  - – HP Series 700 system configured with at least one supported display and keyboard
  - – Minimum of 16MB RAM
  - – A network adapter that supports the TCP/IP and UDP/IP communication protocols such as ethernet or token ring
  - – 1.5MB of fixed-disk storage
  - – 2MB of fixed-disk storage on the system configured as the DSMIT server

Software Requirements

- The following software is required for systems installed with both the Distributed SMIT server package and DSMIT client package for AIX 4.1 or later:
  - – AIX 4.1 or later
  - – TCP/IP installed and properly configured (TCP/IP, UDP/IP, and related network protocols)
  - – NFS (optional)
- The following software is required for systems installed with the DSMIT client package for AIX 3.2 client:
  - – AIX 3.2
  - – TCP/IP installed and properly configured (TCP/IP, UDP/IP, and related network protocols)
  - – NFS (optional)
  - – PTF U418283 is required for AIX 3.2 or earlier
- The following software is required for systems installed with the DSMIT client package for Sun OS 4.1.3:
  - – Sun OS 4.1.3
  - – TCP/IP installed and properly configured (TCP/IP, UDP/IP, and related network protocols)
- The following software is required for systems installed with the DSMIT client package for Solaris:
  - – Solaris 2.3 or Solaris 2.4
  - – TCP/IP installed and properly configured (TCP/IP, UDP/IP, and related network protocols)
- The following software is required for systems installed with the DSMIT client package for HP-UX 9.0:

- HP-UX 9.0 700 series
- TCP/IP installed and properly configured (TCP/IP, UDP/IP, and related network protocols)

Software Installation Specifications

When you install the client software, the **/etc/inetd.conf** and **/etc/services** files are updated on client systems. The updates contain information necessary for the correct operation of the DSMIT daemons. The following lines are added to the **inetd.conf** file during installation:

```
rexs dgram udp wait root /usr/dsmit/bin/crexd crexd -t30
rexs stream tcp nowait root /usr/dsmit/bin/srexd srexd -i
```

Two flags are passed to the daemons upon invocation. The **-t** flag (optional) indicates the number of seconds the system waits after processing the last request before terminating. After 30 seconds the **crexd** daemon shuts down. It starts again on the next call to **crexd**.

The **-i** flag indicates that **inetd** started **srexd**. Do not remove it.

The following lines are added to the **services** file during installation:

```
rexs 6126/tcp #srexd port
rexs 6125/udp #crexd port
```

The system changes these files automatically when you issue the **installp** command.

Once the **inetd.conf** and **services** files have been updated, the DSMIT daemons must be started. The installation program will refresh the **inetd** daemon.

For more information on installing optional software on systems, see the *AIX 5L Version 5.1 Installation Guide*.

DSMIT Server Installation

If you plan to have more than one managing system, you should install the DSMIT server code on one of them and initialize the security configuration before installing the other managing system.

If you plan to manage AIX 3.2, HP-UX 9.0, Sun OS 4.1.3, Solaris 2.3, or Solaris 2.4 systems, you should also install the DSMIT client packages for these systems on the managing system at this time.

Related Information

"Chapter 1. Distributed System Management Interface Tool" on page 1.

The **installp** command.

The **inetd** daemon.

The **inetd.conf** file format, **services** file format.

Security Configuration for DSMIT

This procedure requires you to respond to a series of interactive prompts and to perform a set of offline actions on the managing and managed systems.

Before you begin with the following procedure, identify the systems that will be managed. If you had a previous version of DSMIT, the **/usr/share/DSMIT/hosts** file on the managing system will contain the names of the managed systems. Otherwise, if you have a large number of managed systems, you should enter their names in a file to use in the following procedure.

To start DSMIT security configuration, follow these step s:

1. At the command prompt, enter:

   ```
   dsmit-init
   ```

   A screen appears with options to initialize or modify the DSMIT security configuration.

2. Select **Initialize DSMIT Security Configuration**.

   A screen appears where you can select the following options:

   Easy Initialization
   > Use if you plan to have only one managing system.

   Custom Initialization
   > Use if you plan to have multiple managing systems sharing DSMIT configuration files from a central DSMIT configuration files server.

   > **Notes:**
   > a. If you select **Easy Initialization** now, you can add managing machines later using the "Modifying DSMIT Security Configuration" on page 9 procedure.
   > b. There are sample programs located in **/usr/dsmit/samples** that can assist you in performing the off-line actions.

Easy Initialization

When you select the **Easy Initialization** option, the system where you are running this task is configured as the managing system and DSMIT configuration file server.

1. **DSMIT ADMINISTRATORS** appears. Enter the login ID and password for the DSMIT administrator.

   Note: You must enter a unique password for each DSMIT administrator you specify. If you want to establish single sign-on for a DSMIT administrator, the DSMIT password must be the same as the login password. See "Establishing Single Sign-On" on page 11 procedure for more information.

2. **DSMIT MANAGED MACHINES** appears. Enter the hostnames for the machines you want managed.

   Note: If you have a file containing the names of the managed machines, enter its filename. Otherwise, you can enter the machine names one at a time.

3. **OFFLINE ACTIONS** appears. Perform the specified tasks on the managed machines to complete the DSMIT security configuration.

4. Erase the files in **/tmp/dsmit** on the managing machine when you have successfully completed the offline actions.

Custom Initialization

When you select the **Custom Initialization** option, the prompt for **DSMIT CONFIGURATION FILE SERVER** appears.

1. Enter the system name where you want to store the DSMIT configuration files. The DSMIT server code must be installed on the system, but it does not have to be designated as a managing system.

2. **DSMIT ADMINISTRATORS** appears. Enter the login ID and password for the DSMIT administrator.

   Note: You must enter a unique password for each DSMIT administrator you specify. If you want to establish a single sign-on for a DSMIT administrator, the DSMIT password must be the same as the login password. See "Establishing Single Sign-On" on page 11 procedure more information.

3. **DSMIT MANAGING MACHINES** appears. Enter the hostname of the managing machine.

> **Note:** You can specify more than one managing system. They will all share the DSMIT configuration data stored on the DSMIT configuration file server.

4. **DSMIT MANAGED MACHINES** appears. Enter the hostnames for the machines you want managed.

5. **OFF-LINE ACTIONS** appears. You must perform the specified tasks on the managing and managed machines to complete DSMIT security configuration.

6. Erase the files in **/tmp/dsmit** on the system where you are running the **dsmit-init** command.

> **Note:** The offline actions are saved in **/tmp/dsmit.offline**.

Related Information

"Chapter 1. Distributed System Management Interface Tool" on page 1.

The **installp** command.

The **inetd** daemon.

The **inetd.conf** file format, **services** file format.

Modifying DSMIT Security Configuration

DSMIT allows you to modify the DSMIT security configuration by adding or removing DSMIT administrators, managed machines, or managing machines.

> **Note:** You must be a registered DSMIT administrator to modify the DSMIT security configuration.

To start DSMIT security configuration, follow these steps:

1. At the command prompt, enter:

   ```
   dsmit--init
   ```

   A screen appears with options to initialize or modify the DSMIT security configuration.

2. Select **Modify DSMIT Security Configuration**.

   A menu will appear providing the following options:

   Change / Show Administrators

   Change / Show Managed Machines

   Change / Show Managing Machines

3. Make your modifications.

   > **Note:** If you add a new administrator, you will be prompted for the DSMIT administrator's password. Enter the password for the new administrator you are adding.

4. **OFF-LINE ACTIONS** appears. A list of offline actions will appear after you make the modifications and exit these menus. You must perform the specified tasks to complete the modifications to the DSMIT security configuration.

5. Erase the files in **/tmp/dsmit** on the system where you are running the **dsmit-init** command when you have successfully completed the offline actions.

   > **Note:** The offline actions are saved in **/tmp/dsmit.offline**.

System Configuration for Sun OS and HP

DSMIT requires specific conventions on the Sun Microsystems and Hewlett-Packard (HP) systems to assist the configuration and management of devices, subsystems, and system builds. These conventions are used to reconfigure the system's **/etc/rc.*** files and system-configuration files.

On both the Sun Microsystems and Hewlett-Packard (HP) systems, restructure the **/etc/rc.*** files to resemble the standard System V Release 3 **/etc/rc.*** files by following these steps:

1. Create your clients. See "Defining Clients" on page 15.
2. Use the **dsmit** command to start DSMIT with the desired clients:

   ```
   dsmit -W DomainOfClients
   ```
3. Select the **System Management** option from the initial menu.
4. Select the **System Configuration** option from the System Management menu.
5. Select the **Reorganize RC Boot Files** option from the System Configuration menu.
6. Use the Tab key to select the **yes** option. Press the Enter key.
7. Restart the client systems and exit DSMIT.

The restructuring of the **/etc/rc.*** files requires the definition of the **/etc/rc0.d**, **/etc/rc1.d**, **/etc/rc2.d**, and **/etc/rc3.d** directories. These directories contain shell scripts that perform the functions normally found in the system's **/etc/rc.*** files. The shell programs perform specific tasks and are named with a leading sequential number to provide task-sequencing. When you start the system, the tasks in the **/etc/rc*.d** directories are run sequentially.

Reconfiguring the **/etc/rc.*** files allows DSMIT to add and remove NFS and TCP/IP tasks from the startup procedure.

The system-configuration files are designed to emulate the customized database and to provide a single source for system hardware and software configuration. The Sun or HP user supplies the information used to construct these files. For HP systems, use the **/etc/conf/d** file without modifications. For Sun systems, construct the configuration files with information from the configuration files used to build the operating system and with the information found and reported by the autoconfiguration process during system startup.

After the system has restarted, build the configuration files.

For Sun systems, follow these steps:

1. Use the **dsmit** command to start DSMIT with the desired clients:

   ```
   dsmit -W DomainOfClients
   ```
2. Select the **System Management** option from the initial menu.
3. Select the **System Configuration** option from the System Management menu.
4. Select the **Build Configuration Database** option from the System Configuration menu.
5. Press the F4 key to get the path name for the directory containing the system configuration. The following is an example of the path name:

   ```
   /usr/share/sys/sun4c/conf
   ```

   Press the Enter key.
6. Press the F4 key at the **Get configuration filename : Enter Configuration Filename** option to display a list of selections.

   The configuration files usually have an all-uppercase name, such as **GENERIC**. The file used to build the current operating system can be recovered from the version string within the operating system. The output from the **dmesg** program for a name enclosed in parenthesis following the string SunOS

`Release 4.1.3`. The Sun configuration-file syntax is not in a form that can be easily parsed with a shell script, so it is reformatted to make configuration information easier to find and update.

> **Note:** In most cases, selecting **GENERIC** from the list will work. However, selecting **GENERIC** won't work when software products have been installed that do not use a generic kernel. Refer to the documents supplied from other vendors on the type of configuration file needed for their product. For more information on Sun systems configuration files, refer to the **/usr/share/sys/arch -k/conf/README** file.

7. Select **GENERIC** and press the Enter key.
8. Press the F4 key at the **Get devices filename : Enter Devices Filename** option to display the list of selections. In most cases, selecting **devices** from the list will work.
9. Press the F4 key at the **Get files filename : Enter Files Filename** option to display the list of selections. In most cases, selecting **files** from the list will work.
10. At the **Get loadable modules directory pathname : Enter Loadable Modules Directory Pathname** option, press the Enter key to create the configuration database using the default value. Once the command completes, you are able to run DSMIT commands on the configured Sun system clients.

DSMIT uses the **dmesg** program during the **/etc/rc.*** file startup sequence to recover the information reported by the autoconfiguration process at system startup and saves it in the **/etc/dmesg.boot** file. DSMIT processes this information to determine which adapters were installed by the autoconfiguration process. This information, along with the information from the system configuration file, is formatted and placed in the **/usr/share/SMIT/configdb** file.

For HP machines, building the configuration files is optional. If you want to build the configuration files, follow these steps:

1. Use the **dsmit** command to start DSMIT with the desired clients:

   `dsmit -W DomainOfClients`

2. Select the **System Management** option from the initial menu.
3. Select the **System Configuration** option from the System Management menu.
4. Select the **Build Configuration Database** option from the System Configuration menu.
5. Press the Enter key to run the command using the **/hp-ux** default value.

When DSMIT changes information found in the **configdb** file, it writes a **confgdb** update record in the file named **/usr/share/SMIT/configdb_***XXXX*, where *XXXX* is a date stamp constructed with the **date** command.

Related Information

"Chapter 1. Distributed System Management Interface Tool" on page 1.

Establishing Single Sign-On

Single sign-on is the ability to create DSMIT credentials automatically whenever a valid DSMIT administrator logs onto a valid DSMIT managing machine.

To perform this task:

1. Follow the steps in "Security Configuration for DSMIT" on page 7 to create a valid administrator and managing machine.
2. On each managing machine:
   a. become root
   b. edit the **/etc/security/login.cfg** file and add the following lines:

```
dsmitlogin:
    program = /usr/dsmit/bin/dsmit-41log
```

  c. edit the **/etc/security/user** file for each DSMIT administrator (this assumes the user already exists). Add the following lines:

```
SYSTEM = "compat AND dsmitlogin"
```

For example, if `bob` is the DSMIT administrator on the managing machine M1, then on M1 the entry in **/etc/security/user** should look like the following:

```
bob:
SYSTEM = "compat AND dsmitlogin"
```

If a SYSTEM line for `bob` already exists, modify it and add `dsmitlogin`. There may be additional lines associated with `bob` that do not pertain to DSMIT.

Related Information

"Chapter 1. Distributed System Management Interface Tool" on page 1.

Chapter 2. Learning to Use DSMIT

The following sections contain detailed information about using DSMIT:

- "Starting and Stopping the DSMIT (ASCII or AIXwindows) Interface"
- "Using the DSMIT Interfaces" on page 14
- "Defining Clients" on page 15
- "Defining the Working Collective" on page 15
- "Creating a Domain" on page 17
- "Changing a Domain" on page 18
- "Removing a Domain" on page 20
- "Saving the Current Working Collective as a Domain" on page 21
- "DSMIT Troubleshooting" on page 21
- "Examples of Tasks Performed with DSMIT" on page 25

Starting and Stopping the DSMIT (ASCII or AIXwindows) Interface

Start the Distributed System Management Interface Tool (DSMIT) program by entering the **dsmit** command for the ASCII interface or the **mdsmit** for the AIXwindows interface at the command line. When you start the DSMIT program, you must define the working collective of clients. See "Defining the Working Collective" on page 15 for more information.

DSMIT provides a simple mechanism for exiting. The function keys enable you to exit a particular screen or to stop DSMIT when you complete a task.

Prerequisite Conditions

1. A DSMIT server must reside on your system.
2. DSMIT client software must reside on the clients.
3. You must be registered as a DSMIT administrator.

Start DSMIT

Enter the **dsmit** or **mdsmit** command at the command line.

> **Note:** The DSMIT administrator will always be authenticated by means of the local system security file. If the information for you is not correct, you are prompted for your DSMIT administrator password.

For further explanation of all of the **dsmit** or **mdsmit** command options, consult the **dsmit** command .

Stop DSMIT

- To exit from the current DSMIT screen to the previous menu level, press the F3 key for ASCII or click on the **Cancel** button for AIXwindows.
- To exit DSMIT entirely, press the F10 key for ASCII or select **Exit** for AIXwindows.

  > **Note:** You cannot use the F10 key to exit DSMIT if you are in a help message screen.

Related Information

"Chapter 1. Distributed System Management Interface Tool" on page 1.

Using the DSMIT Interfaces

The Distributed System Management Interface Tool (DSMIT) interface is similar to the SMIT interface except that it has additional function key sequences. The DSMIT facility runs in two interfaces, ASCII (nongraphical) or AIXwindows (graphical).

For more information about using the SMIT interface, see the System Management Interface Tool (SMIT): Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

DSMIT in the ASCII Interface

The additional function key sequences include:

Esc-M   Enables you to change a field in a common dialog screen by client machine name.
Esc-F   Enables you to change a field in a command dialog screen by field name.
Esc-C   Enables you to either include or exclude a particular client from the working collective of clients.

  After pressing the Esc-C key sequence, you can include or exclude specific clients, operating systems, or domains in the Current Inclusion/Exclusion Status field. You can also display the current inclusion or exclusion status of each client.

The mechanics of using the DSMIT interface are the same as those for SMIT. Select command options from the menus and use the Tab key to cycle through the fields in a command screen. If a field is marked with a + (plus sign), you can press F4 to get a list of options to enter. To make selections in a multiple selection list, use F7 to tag each of your selections and press the Enter key to select them.

To execute system management tasks on the managed systems, select the **System Management** option from the initial menu. The **Domain Management** option lets you manage the DSMIT environment such as domains and working collectives.

DSMIT in the AIXwindows Interface

A Visual System Management (VSM) application is started when you start DSMIT in the graphical interface. It allows you to define and select the machines or groups of machines to perform DSMIT tasks on.

The additional function key sequences include:

Common View   Enables you to change a field in a common dialog screen by client machine name.

  In the Common View, an option button appears on the left side of the dialog options. Select this button, the value can be changed and is common to all the machines. Deselect the button, the value cannot be changed and is not common to all machines.
Machine View   Enables you to change a field by client machine.
Option View   Enables you to change a field by the field name.

In the windowing version of DSMIT, you use standard mouse-driven window conventions to manipulate the menu-based format, which guides you through tasks.

Related Information

"Chapter 1. Distributed System Management Interface Tool" on page 1.

Defining Clients

Defining clients for the Distributed System Management Interface Tool (DSMIT) program enables clients to run commands built by the DSMIT server. To define a client, you must add it to the **/usr/share/DSMIT/hosts** file by editing the file directly or with the DSMIT interface.

Prerequisite Conditions

1. A DSMIT server must reside on your system.
2. The DSMIT client installation packages must be installed on your server.

Define a Client Using the Command Line

Add the name of the client to the **/usr/share/DSMIT/hosts** file in the following format:

```
Machine:OperatingSystem:0
```

The machine name should be a TCP/IP host name. If you add a fully qualified network name to the **/usr/share/DSMIT/hosts** file, you must use this name as the client name when using the **dsmit** command.

The operating system name should be listed in the **/usr/share/DSMIT/dsmitos** file.

Do not put spaces within the machine name or the operating system name. Substitute spaces with underscores. The following are examples of correct entries:

```
m1:AIX_4.1:0
m2:SunOS_4.1.3:0
```

Define a Client Using the DSMIT Interface

1. Enter the **dsmit** command at the command line.
2. Select the **Domain Management** option from the initial menu.
3. Select the **Configure DSMIT on a Local Machine** option from the Domain Management menu.
4. Select the **Add Machines with DSMIT Installed** option from the Configure DSMIT on a Local Machine menu.
5. Add the clients you want the DSMIT server to manage. Insert a tab, space, or multiple spaces between the client names to separate them. You can add clients on one operating system at a time. Press the F4 key to display the available operating system.

Related Information

"Chapter 1. Distributed System Management Interface Tool" on page 1.

"Creating a Domain" on page 17.

Defining the Working Collective

The working collective specifies the current list of clients that receive commands built by the Distributed System Management Interface Tool (DSMIT) program. The working collective is a temporary list of clients and must be respecified with each new DSMIT session. By default, the server is the only machine in the working collective when you start DSMIT.

Prerequisite Conditions

1. A DSMIT server must reside on your system.
2. DSMIT clients must be installed on the remote hosts.
3. The DSMIT client installation packages must be installed on your server.

4. A domain must already be created when defining the working collective from a domain.

Define the Working Collective Using the Command Line

Enter the **dsmit** command with the **-W** or **-w** flag. For example, to define the working collective that contains the `floor_1` domain and clients `M1` and `M2`, enter the following:

```
dsmit -W floor_1 -w M1,M2
```

> **Note:** Do not put spaces between client names.

The **-W** flag specifies the names of domains to include in the working collective. The **-w** flag specifies the names of clients to include in the working collective.

Define the Working Collective Using the DSMIT ASCII Interface

1. Enter the **dsmit** command. A menu appears with the **System Management** and **Domain Management** options.
2. Select the **Domain Management** option to enter the Domain Management menu. If you select the **System Management** option, the System Management Interface Tool appears.
3. Select the **Manage Working Collective of Machines** option to enter the Working Collective of Machines menu.
4. Select the **Add Working Collective Members** option to add clients to the collective of working machines.

> **Note:** When defining a working collective for operating systems other than this one, you must select the **Redefine Working Collective Members** option rather than the **Add Working Collective Members** option. Once the new operating system is defined with the list specified in the Redefine Working Collective Members menu, you can add or remove members with that operating system.

5. Once you have created a list of clients, return to the first menu containing the **System Management** and **Domain Management** options. From this menu, you can access the rest of the menus.

The Manage Working Collective of Machines menu has the following options in addition to the **Add Working Collective Members** option:

Show Working Collective Member
    Displays the member list of the working collective.

Show Responding Status of Working Collective Members
    Displays the inclusion or exclusion status of clients and whether they responded to the last command.

Remove Working Collective Members
    Removes a member of the working collective.

Redefine Working Collective Members
    Removes all members of the present working collective and adds members based on new menu selection criteria.

Exclude Working Collective Members
    Excludes members from the working collective, preventing commands from being sent to the excluded member.

Include Working Collective Members
    Restores excluded members so they can receive commands.

Save Working Collective as Domain
    Saves the current working collective to a domain that can be reused.

Define the Working Collective Using the DSMIT Graphical Interface

1. Enter the **dsmit** command. A Visual System Management (VSM) application appears with machine and domain objects.
2. Select the machine or domain objects you want to include in the working collective.
3. To perform system management tasks on the machines in the working collective, double click on the DSMIT icon in the Action area or drag the selected objects and drop them on the DSMIT icon in the action area. The system management menus will appear.

Related Information

"Chapter 1. Distributed System Management Interface Tool" on page 1.

"Saving the Current Working Collective as a Domain" on page 21.

Creating a Domain

The working collective is a temporary group of clients and must be reset each session. Domains are permanent groups. Creating a domain enables you to group clients logically and provides a convenient access to them. To create a domain, use either the **mkdsmitd** command, the Distributed System Management Interface Tool (DSMIT) ASCII interface, or the DSMIT graphical interface. When you use the graphical interface, you can view the domain and its clients in the domain while you are creating it. The **List All Domains** option from the Manage Domains of Machines menu provides a list of available domains.

> **Note:** Domains must be homogeneous, consisting only of clients whose operating systems are of the same type.

Prerequisite Conditions

A DSMIT server must reside on your system.

Create a Domain Using the Command Line

1. Use the **mkdsmitd** command to create domains.
   - Enter the **mkdsmitd** command without a flag to create a new empty domain. For example:
     ```
     mkdsmitd floor1
     ```
   - To add clients while creating a new domain, enter the **mkdsmitd -m** command and specific client names. For example:
     ```
     mkdsmitd -m M1,M2,M3 floor1
     ```

     > **Note:** Do not put spaces between client names.

   For further explanation of all **mkdsmitd** command options, see the **mkdsmitd** command .
2. Edit the **/usr/share/DSMIT/domains** file and add the domain names in the following format:
   ```
   domain:machine1,machine2
   ```

   > **Note:** Do not put spaces between client names.

   Domain names must begin with an alphanumeric character and can only contain the following characters:

   A-Z

   a-z

   0-9

_ (underscore)

- (dash)

Create a Domain Using the DSMIT Interface

1. Select the **Manage Domains of Machines** option from the Domain Management menu.
2. Select the **Add Domain** option from the Manage Domains of Machines menu.
3. Enter the new domain name in the fields provided. Use the arrow keys to move to the client information fields.
4. Enter the client name, operating system name, or domain name in the fields provided.

    Note: The client name must already be listed in the **/usr/share/DSMIT/hosts** file, the operating system must already be listed in the **/usr/share/DSMIT/dsmitos** file, and the domain name must already be listed in the **/usr/share/DSMIT/domains** file. A line entry in a **/usr/share/DSMIT/domains** file cannot exceed 2048 characters.

5. To designate whether to take the intersection or union of a client or domain, press F4 or use the Tab key to get a list of the **union** or **intersection** options.
6. Once you have entered the information, press the Enter key and an output message appears. If you entered the information correctly, the message screen tells you that the domain has been added. A message will tell you if you entered something incorrectly.

Create a Domain Using the DSMIT Graphical Interface

1. Enter the **dsmit** command. A Visual System Management (VSM) application appears with machine and domain objects.
2. Click on the domains icon in the types pane.
3. Drag the new domain object from the Templates area and drop it on the domains work area. A dialog will appear for the domain name and membership criteria.
4. Enter a name for the domain.
5. To add a machine to a domain, drag a machine object from the machines work area and drop it on a domain object in the domains work area.

Related Information

"Chapter 1. Distributed System Management Interface Tool" on page 1.

"Defining Clients" on page 15.

"Changing a Domain".

"Removing a Domain" on page 20.

Changing a Domain

The Distributed System Management Interface Tool (DSMIT) program allows you to change a domain. You can add a new client to the domain, delete a client from the domain, or redefine the domain's member list entirely. Use the **chdsmitd** command or the graphical interface to change a domain. When you use the interface, you can view the domain and any changes you are making to them. The Manage Domains of Machines menu provides the following options to assist in altering domains:

Show Domain Members	Displays a member list of a domain.
Add Domain Members	Adds members to a domain.
Remove Domain Members	Removes members from a domain.

Redefine Domain Members Removes all members of a domain and adds members based on new menu selection criteria.

Prerequisite Conditions

A DSMIT server must reside on your system.

Change a Domain Using the Command Line

1. Enter the **chdsmitd** command to change a domain:

    *   To add a client to a domain, enter the **chdsmitd -a** command. You must also enter the **-m** flag followed by the client name and the domain name. The **-a** flag designates that you are adding to a domain. It does not specify the client name. Use the following format:

        ```
        chdsmitd -a -m NewMachine Domain1
        ```

    *   To delete a client from a domain, enter the **chdsmitd -s** command. You must also enter the **-m** flag followed by the client name and the domain name. The **-s** flag designates that you are deleting from a domain. It does not specify the client name. Use the following format:

        ```
        chdsmitd -s -m OldMachine Domain1
        ```

    For further explanation of all of the **chdsmitd** command options, consult the **chdsmitd** command .

2. Edit the **/usr/share/DSMIT/domains** file by making any of the following changes:

    *   To add clients M1, M2, and M3 to the floor1 domain, enter the client names after the domain name, separating the domain and the clients with a colon. For example:

        ```
        floor1:M1,M2,M3
        ```

        Note: Do not put spaces between the client names.

    *   To remove clients M1 and M2 from the floor1 domain, remove the clients from the line that defines the floor1 domain, leaving only the M3 client. For example:

        ```
        floor1:M3
        ```

Change a Domain Using the DSMIT Interface

1. Select the **Manage Domains of Machines** option from the Domain Management menu.

2. Highlight the option corresponding to the change you want to make. For example, you can make specific changes such as adding or removing a domain, adding or removing domain members, or redefining a domain member list.

        Note: An asterisk (*) designates fields that require input.

3. Once you have entered the information, press the Enter key and an output message screen appears. If you entered the information correctly, the message screen tells you that the domain has been changed. Otherwise, a message tells you if you entered an incorrect value.

Change a Domain Using the DSMIT Graphical Interface

1. Enter the **dsmit** command. A Visual System Management (VSM) application appears with machine and domain objects.

2. Double click on the domain object in the domain work area to show domain members.

3. To add domain members, drag one or more machine objects from the machines work area and drop them on the desired domain object in the domain work area.

Related Information

"Chapter 1. Distributed System Management Interface Tool" on page 1.

"Creating a Domain" on page 17.

Removing a Domain

To remove a domain from the member list, use either the **rmdsmitd** command or a DSMIT interface. When you use a graphical interface, you can view which clients are being removed from the member list.

> **Note:** Once you remove a domain, the DSMIT server can still manage the clients that were part of the domain name you removed. However, each individual client must be specified rather than just the domain name.

Prerequisite Conditions

A DSMIT server must reside on your system.

Remove a Domain Using the Command Line

1. Enter the **rmdsmitd** command to remove a domain.
   - To remove an empty domain, enter the **rmdsmitd** command with the domain name. For example:

     ```
     rmdsmitd floor1
     ```
   - To remove a nonempty domain, enter the **rmdsmitd -f** command with the domain name. For example:

     ```
     rmdsmitd -f group1
     ```

   For further explanation of all **rmdsmitd** command options, see the **rmdsmitd** command .
2. Edit the **/usr/share/DSMIT/domains** file, and remove the domain and its client machines.

Remove a Domain Using the DSMIT Interface

1. Select **Manage Domains of Machines** from the Domain Management menu.
2. Select **Remove Domains** from the Manage Domain of Machines menu.

   > **Note:** An asterisk (*) designates fields that require input.
3. Select **Current Domain Members** and press F4 to display a list of machines currently in the domain.
4. Select one or more of the three criteria options and press F4 to display entry lists.
5. Use the F7 key to tag selections for removal from these lists and press Enter. An output message confirms the completion of the command.

Remove a Domain Using the DSMIT Graphical Interface

1. Enter the DSMIT command. A Visual System Management (VSM) application appears with machine and domain objects.
2. Drag the domain object from the domain work area to the trash can object to remove a domain.

Related Information

"Chapter 1. Distributed System Management Interface Tool" on page 1.

"Creating a Domain" on page 17.

"Changing a Domain" on page 18.

Saving the Current Working Collective as a Domain

The Distributed System Management Interface Tool (DSMIT) program enables you to save the current working collective as a domain. By saving the working collective as a domain, you can run DSMIT on the same set of clients without having to add each client to the working collective every time you start a new session.

Prerequisite Conditions
A DSMIT server must reside on your system.

Procedure
1. Once you have defined the working collective, select the **Manage Working Collective** option.

   Note: An asterisk (*) designates fields that require input.
2. Select the **Save Working Collective** option from the Domain from the Manage Working Collective menu.
3. Enter the name of the domain in the Domain Name field.
4. Enter **yes** or **no** in the Replace Existing Domain field. If you enter **yes**, DSMIT replaces an existing domain. If you enter **no**, DSMIT asks that you redefine the domain or enter **yes**.
5. Once you have entered the domain name, press the Enter key. An output message screen appears. If the information is correct, the message screen indicates that the domain has been added. If the information is incorrect, the message displays the incorrect information to change.

Related Information
"Chapter 1. Distributed System Management Interface Tool" on page 1.

"Defining the Working Collective" on page 15.

DSMIT Troubleshooting

Use the following suggestions if you encounter problems while connecting to a client, listing domain members, or defining a working collective. A `Failed` prompt in the Command Status field of the output screen indicates that one or more systems reported a failure.

Clean Up After Abnormal Termination
If the front end of DSMIT/crex/srex abnormally terminates, the following may not have been cleared:
- Files in **/tmp/dsmit** that were created during startup and removed during exit.
- Contents of the counter file **/usr/share/DSMIT/security/dslock.ctr**.
- **/usr/share/DSMIT/security/dslock** may exist.

Concurrent **DSMIT/crex/srex** sessions may have similar side effects and they must be resolved. The following information is intended as a guide for cleaning up processes that abnormally terminated:
1. Remove the files in **/tmp/dsmit** that belong to the failing process.
2. Use the **dsmit-dec** command to decrement by 1 the value of the counter in the **/usr/share/DSMIT/security/dslock.ctr** file.
3. Remove **/usr/share/DSMIT/security/dslock** lock file.

If You Cannot Connect to a Client

Many of the problems associated with Distributed System Management Interface Tool (DSMIT) arise when you cannot connect to one or all of the clients. Consult the following list if you cannot connect to the DSMIT clients:

- Check to see if the network is down. From the command line, issue the **ping** command to the client to which you cannot connect:

  ```
  ping ClientName
  ```

  If the client responds, then the network is active. If the client does not respond, follow the problem determination steps defined by TCP/IP.

- Ensure that the **inetd** daemon is active on both the server and client. To ensure that the **inetd** daemon is active, check the processes for the server and client, or issue the following command from the command line:

  ```
  rsh HostName ps -ef | grep inetd
  ```

  If the **inetd** daemon does not exist or the **rsh** command fails, start it using the following appropriate method:

  - On a local Sun or Solaris system, enter: `/usr/etc/inetd`
  - On a local HP system, enter: `/etc/inetd`

  For this operating system, check to see if the **inetd** daemon is active by locally entering `lssrc -s inetd`. If the **inetd** daemon is not active, start it by entering `startsrc -s inetd`. If the **inetd** daemon is active, refresh it using the following methods:

  - On local installations of this operating system, enter:

    ```
    /usr/bin/refresh -s inetd
    ```

  - On remote installations of this operating system, enter:

    ```
    rsh HostName /usr/bin/refresh -s inetd
    ```

  - On local Sun or Solaris systems, enter:

    ```
    ps -aux | grep inetd
    kill -1 Process_id_of_inetd
    ```

  - On remote Sun or Solaris systems, enter:

    ```
    rsh Hostname ps -aux | grep inetd
    rsh Hostname kill -1 Process_id_of_inetd
    ```

  - On local HP systems, enter:

    ```
    /etc/inetd -c
    ```

  - On remote HP systems, enter:

    ```
    rsh Hostname /etc/inetd -c
    ```

  - Check that the DSMIT ports are active, enter:

    ```
    netstat -Aan | grep 6125
    netstat -Aan | grep 6126
    ```

    Output should look similar to this:

    ```
    <HexNumber> udp 0     0     *.6125   *.*
    <HexNumber> tcp 0     0     *.6126   *.*      LISTEN
    ```

  - If you are using Network Information Service (NIS), add the entries into **/etc/services** and **/etc/inetd.conf** on the NIS server and rebuild the NIS maps. Refer to the NIS Overview in the *AIX 5L Version 5.1 System Management Guide: Communications and Networks* for further information.

  - Check the **/etc/inetd.conf** file on both the server and clients for the following two lines:

    ```
    rex dgram udp wait root /usr/dsmit/bin/crexd crexd -t30
    rex stream tcp nowait root /usr/dsmit/bin/srexd srexd -i
    ```

If these lines are not present in the file, add them to the file and refresh the **inetd** daemon.

– Check the **/etc/services** file on both the server and clients for the following two lines:

```
rex 6126/tcp #srexd port
rex 6125/udp #crexd port
```

If these lines are not present in the file, add them to the file and refresh the **inetd** daemon.

– Ensure that the server name is accessible to the client system by issuing the following command:

```
ping Server HostName
```

If the system returns the server's TCP/IP address, the network is working correctly. If it does not, add the server host name to the **/etc/hosts.equiv** or **/etc/hosts** file. If the system is using a name server, the problem could be the result of name server failure. See TCP/IP Name Resolution in *AIX 5L Version 5.1 System Management Guide: Communications and Networks* for more information on name servers.

– Sun, Solaris, and HP systems may report **/usr/share/SMIT/configdb** files not found. System configuration is required before you can use DSMIT management devices and TCP/IP or NFS subsystems.

– Sun, Solaris, and HP support require that the default shell contained by the **/bin/sh** file is the Bourne Shell.

If You Cannot Establish a Secure Session

If a message such as ″establishing secure session failed″ is displayed, refer to the following steps:

1. Be sure the system you are trying to establish a session with is defined as a managed machine. On the DSMIT server, do the following:

   a. Type `dsmit env`.

   b. Select **List All Machines**.

      OR

   c. Type `lsdsmitm`.

      Note: If the machine you are trying to establish a session with does not appear in the list of managed machines, you should add it. See "Modifying DSMIT Security Configuration" on page 9 for more information.

2. Install a new key on the managed machine:

   a. Remove the managed machine.

   b. Add the machine.

   c. Install the new key.

      Note: See "Modifying DSMIT Security Configuration" on page 9 for more information.

If You Cannot List All Members of A Domain

If the output from the **lsdsmitd** command does not include all of the hosts that were added to a domain, check the **/usr/share/DSMIT/hosts** file for spaces between client names. Remove all spaces in the definition of a domain.

If You Cannot Define A Working Collective

If you cannot define a working collective because you get the message:

```
All the hosts should have one and the same Operating System
```

• Check that the clients included in the working collective have the same operating system.

- If you are attempting to define a working collective that does not use this operating system, you must use the Redefine Working Collective Members menu to redefine the working collective. Do not include this local operating system in the working collective.

If You See Double Entries in the Domain Management Menus

Double entries can occur if you completed step 4 in the Database ("Databases" on page 3) section even though DSMIT was installed on the `HostWithNewLevel`. To correct this situation, remove the `NewLevelDirectory` and complete all the steps except step 4 in the "Database" section.

If You Cannot Connect to the File Server

If you get messages such as the following:

`Cannot acquire exclusive lock`

Or

`Cannot connect to the file server`

Enter the **dsmit-unlock** and **dsmit-dec** commands on the file server.

If You Cannot Run dsmit-addkey on a Client

If you cannot run the **dsmit-addkey** command because you get the message:

`dsmit-addkey: Problems with /tmp/new-v5srvtab -- exiting.`

- Be sure that you copy the correct **new-v5srvtab** file from the managing machine to the client. It should come from the **/tmp/dsmit** directory on the managing machine.
- Be sure the hostname of the client matches exactly the hostname from the security configuration on the managing machine. For example M1.austin.ibm.com. must be written out in full; it can only be abbreviated as `M1` if it is abbreviated as such on the managing machine.

If You Cannot Access/Open File /tmp.installp_cmd

If you get the `Cannot access/open file /tmp.installp_cmd` message when trying to install a software package, the version of installp on the remote machine is different than the SMIT database version on the local machine. To fix this, install the correct version of the database on the local machine. Refer to "Databases" on page 3.

If You Cannot Select the Next Screen

You may get the following message cause you cannot select the next:

`There is a conflict in selecting the next screen - Make other selections in previous screens and/or exclude some hosts from the collective`

The next menu to display is not exactly the same on all machines in the working collective. This indicates one of the following:
- Dialog IDs are different for each machine
- Number of options are different for each machine
- Options are different for each machine.

For example, for the menu Change/Show Characteristics of a Tape Drive, the working collective is defined to be `M1` and `M2`. On `M1`, a 4.0 GB 4mm tape drive exists and on `M2`, a 2.3 GB 8mm tape drive exists. When DSMIT attempts to display a menu, you will get the above error message. This is because of the different dialog type options. On the 4.0 GB tape drive, it has the extra option **Use data COMPRESSION** and on the 8.0 GB, it has the **Use EXTENDED file marks** option. DSMIT cannot display different dialogs at once. Each dialog must be the same to work.

To correct this problem, you must work with each group of machines that have the same dialogs by temporarily excluding the machines that are different and working with them later.

If You Cannot Get Solaris Machines Into Working Collective

If you cannot get Solaris 2.3 and Solaris 2.4 machines into the same working collective, check **/usr/share/DSMIT/hosts** to be sure all machines are listed as Solaris and not Solaris_2.3.

Related Information

"Chapter 1. Distributed System Management Interface Tool" on page 1.

"Installing DSMIT" on page 4.

Examples of Tasks Performed with DSMIT

Create a User

This example shows how to create a user, `bob`, on client `M1` with a user ID of `300` on client `M3` with a user ID of `301`.

1. Enter:

   ```
   dsmit -w M1,M3 mkuser
   ```

2. Type the user name `bob` in the username field.
3. Use the arrow keys to move down to the User ID field.
4. Press the Esc-F key sequence.
5. Specify a value of `300` for client `M1` and a value of `301` for client `M3`.
6. Press the Enter key to return to the Common Dialog menu.
7. Press the Enter key to run the command.

Add a Directory to the Exports List for NFS

This example shows how to add the **/inst.images** directory to the exports list for Network File System (NFS) on all clients defined in the `floor_1` and `floor_2` domains. The export for the `M3` client is read-only, while the exports for the rest of the clients are read-write. The `M1` client is set so that it does not export the **/inst.images** directory.

1. Enter:

   ```
   dsmit -W floor_1,floor_2 mknfsexp
   ```

2. Press the Esc-C key sequence.
3. Select the **Exclude** option from the Include or Exclude clients from the Collective menu option.
4. Use an arrow key to move to the client name field and enter the name of the `M1` client.
5. Press the Enter key once and the F3 key twice to return to the Common Dialog screen.
6. Enter the **/inst.images** file in the PATHNAME of directory to export field.
7. Press the Esc-M key sequence and select the `M3` client name.
8. Change the permissions of the node to read-only.
9. Press the Enter key twice to run the command.

Related Information

"Chapter 1. Distributed System Management Interface Tool" on page 1.

System Management Interface Tool (SMIT): Overview in *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*.

System Management Interface Tool for Programmers in *AIX 5L Version 5.1 General Programming Concepts: Writing and Debugging Programs*.

The **installp** command, **ping** command in *AIX 5L Version 5.1 Commands Reference*.

The **inetd** daemon in *AIX 5L Version 5.1 Commands Reference*.

The **hosts.equiv** file format for TCP/IP, **inetd.conf** file format for TCP/IP, **.rhosts** file format for TCP/IP, **services** file format for TCP/IP in *AIX 5L Version 5.1 Files Reference*.

Appendix. Notices

This information was developed for products and services offered in the U.S.A.
IBM may not offer the products, services, or features discussed in this document in other countries.
Consult your local IBM representative for information on the products and services currently available in
your area. Any reference to an IBM product, program, or service is not intended to state or imply that only
that IBM product, program, or service may be used. Any functionally equivalent product, program, or
service that does not infringe any IBM intellectual property right may be used instead. However, it is the
user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.
IBM may have patents or pending patent applications covering subject matter described in this document.
The furnishing of this document does not give you any license to these patents. You can send license
inquiries, in writing, to:
IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property
Department in your country or send inquiries, in writing, to:
IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such
provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION
PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR
IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT,
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer
of express or implied warranties in certain transactions, therefore, this statement may not apply to you.
This information could include technical inaccuracies or typographical errors. Changes are periodically
made to the information herein; these changes will be incorporated in new editions of the publication. IBM
may make improvements and/or changes in the product(s) and/or the program(s) described in this
publication at any time without notice.

IBM may use or distribute any of the information you supply in any way it believes appropriate without
incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the
exchange of information between independently created programs and other programs (including this one)
and (ii) the mutual use of the information which has been exchanged, should contact:
IBM Corporation
Dept. LRAS/Bldg. 003
11400 Burnet Road
Austin, TX 78758-3498
U.S.A.
Such information may be available, subject to appropriate terms and conditions, including in some cases,
payment of a fee.
The licensed program described in this document and all licensed material available for it are provided by
IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any
equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their
published announcements or other publicly available sources. IBM has not tested those products and

cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Index

Readers' Comments — We'd Like to Hear from You

Distributed SMIT 2.2 for AIX: Guide and Reference

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you?   ☐ Yes   ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

_____   _____
Name   Address

_____   _____
Company or Organization

_____   _____
Phone No.

Readers' Comments — We'd Like to Hear from You

IBM

Fold and Tape   **Please do not staple**   Fold and Tape

PLACE
POSTAGE
STAMP
HERE

IBM Corporation
Publications Department
Internal Zip 9561
11400 Burnet Road
Austin, TX
 78758-3493

Fold and Tape   **Please do not staple**   Fold and Tape

Readers' Comments — We'd Like to Hear from You

IBM

Printed in U.S.A