AIX Version 6.1

IBM Systems Director Console for AIX

AIX Version 6.1

IBM Systems Director Console for AIX

Note
Before using this information and the product it supports, read the information in "Notices" on page 29.

This edition applies to AIX Version 6.1 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this document

The IBM Systems Director Console for AIX allows for the web-enabled administration of AIX management tasks. The console can be accessed from any supported web browser. A programmer, system administrator, or service representative should use this guide when installing, configuring, or performing problem determination.

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.

Case-sensitivity in AIX

Everything in the AIX® operating system is case-sensitive, which means that it distinguishes between uppercase and lowercase letters. For example, you can use the **ls** command to list files. If you type `LS`, the system responds that the command `is not found`. Likewise, **FILEA**, **FiLea**, and **filea** are three distinct file names, even if they reside in the same directory. To avoid causing undesirable actions to be performed, always ensure that you use the correct case.

ISO 9000

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

IBM Systems Director Console for AIX

IBM® Systems Director Console for AIX is a Web-based application that provides a graphical interface with which you can administer AIX servers remotely. IBM Systems Director Console for AIX is installed as part of the system management bundle.

You can access the IBM Systems Director Console for AIX from the following supported Web browsers: Internet Explorer 7, or later, on Windows, Mozilla Firefox 2.0, or later, on Windows, and Mozilla Firefox 1.5.0.10, or later, on AIX.

The IBM Systems Director Console for AIX console window contains two primary panels. The panel on the left displays the tasks you can perform from the console. This panel is called the navigation tree. The panel on the right, called the work area, displays results that are based on the item that is selected in the navigation tree. When you select a task in the navigation tree, the work area is updated to show the available choices.

IBM Systems Director Console for AIX concepts

Before you start working with IBM Systems Director Console for AIX you need a basic understanding of the user interface, system requirements, and accessibility features.

System requirements

IBM Systems Director Console for AIX has the following system requirements:

Server

- AIX 6.1, or later
- 80 MB of disk space
- Java™ 5

Client

- Internet Explorer 7, or later, on Windows
- Mozilla Firefox 2.0, or later, on Windows
- Mozilla Firefox 1.5.0.10, or later, on AIX

IBM Systems Director Console for AIX user interface layout

The IBM Systems Director Console for AIX user interface layout has three major elements, the banner and tool bar, the navigation tree, and the work area.

Banner and tool bar

The banner and tool bar display a common image across IBM Systems Director Console for AIX installations. The banner and toolbar includes a greeting to the user who is logged in and links to log out of the console and to open console help.

Navigation tree

The navigation tree lists the tasks that are available in the console. Tasks are grouped into organizational nodes that represent categories of tasks (for example, **OS Management** or **Settings**). The organizational nodes can be nested in multiple levels.

The navigation tree only displays tasks to which you have access, according to the authorizations you have been given. When you select a task in the navigation tree, a page containing one or more modules for completing the task is displayed in the work area.

Work area

When you initially log in to the console, the work area displays a welcome page. After you launch a task from the navigation tree, the contents of the task are displayed in a page in the work area. A page contains one or more console modules that are used to perform operations. Each console module has its own navigation controls. Some pages include a control to close the page and return to the welcome page.

Navigating the IBM Systems Director Console for AIX

This topic describes how to navigate pages and modules in IBM Systems Director Console for AIX.

IBM Systems Director Console for AIX navigation includes the following tasks:

- Launching pages from the navigation tree
- Using the title bar controls
- Accessing help
- Using the console help controls

Launching pages from the navigation tree

The console navigation tree provides a hierarchical view of all of the applications or tasks available in the console. A task is a page in the work area. All of the modules to start and complete the task are provided on the page. To open a task, press the task name in the navigation tree. The task is opened in a new page in the work area.

The following table describes the controls for the console navigation tree and entries in the tree:

Icon	Function
+	Represents an organizational node in the navigation tree that contains pages or other navigation nodes. Click the icon to expand the node.
-	Closes an organizational node.
None	This is an elementary administrative task. When you click on this type of node, the work area will display all of the necessary selectors and dialogs to perform the action, as well as suggestions for contents.

Using the title bar controls

Each page contains one or more Web applications or console modules. A console module enables you to perform an operation, such as displaying a list or stopping a managed system. The title and the controls for the module are displayed on the title bar. The functions supported by the module determine which icons are displayed.

In addition to the controls on the title bar, a module can include controls for other actions, such as a button to submit input. Some modules have controls that launch other modules. If a module launches another module, the newly launched module is displayed on the same page in an area near the bottom of the page.

Accessing help

Help is available for the entire console or for a specific module in the console. To access console help, perform the following steps:

1. Press Help on the console toolbar. The help is displayed in a separate browser window.
2. In the help navigation tree, select the help set you want to view. For example, press **Console help** to view topics that provide helpful information for new console users. Use the console help controls as needed.

To access help for a module on a page, perform the following steps:

1. On the title bar for the module, click the ? icon. This icon is displayed only if help is available for the module. The help is displayed in a separate browser window.
2. Close the help window when you are finished viewing the help.

Console settings

The **Console Settings** category in the navigation tree contains tasks for setting and modifying console properties such as user-to-role assignments and enabling logging.

IBM Systems Director Console for AIX accessibility

The IBM Systems Director Console for AIX user interface runs in your browser. Consult the documentation for your browser for information about your browser's accessibility features.

The following features are provided for vision-impaired users:

- Supports interfaces commonly used by screen readers (Microsoft® Windows® systems only)
- Can be operated by using only the keyboard
- Communicates all information independent of color
- Supports interfaces commonly used by screen magnifiers (Microsoft Windows systems only)
- Supports the attachment of alternate output devices
- Provides help information in an accessible format

The following features are provided for users who have mobility impairments or limited use of their hands:

- Allows the user to request more time to complete timed responses
- Can be operated by using only the keyboard
- Supports the attachment of alternative input and output devices

The following features are provided for the deaf and hard-of-hearing users:

- Supports alternatives to audio information
- Supports adjustable volume control

The IBM Systems Director Console for AIX help system has the following accessibility features:

- Uses the accessibility support enabled by the browser that is used to display the help
- Enables navigation by using the keyboard

IBM Systems Director Console for AIX language settings

The language environment of a session is determined by your browser's language preferences, the available languages installed on the managed machine and your AIX account's LANG setting in your ~/.profile or /etc/environment.

The installed languages for **bos.help.msg** are used to determine what languages are available. The first language on your browser's preference list that is installed is used. If your LANG setting is for that language, then the closest matching installed codeset, country code and variant will be used. Otherwise a preference is given to UTF-8 codesets.

Not all messages have been translated to every language. Untranslated messages will appear in English. This is consistent with SMIT behavior. The translated messages come from multiple installable images, depending on the features involved. Be careful to install the needed language(s) using the System Environment Plug-in. Some English messages are not installed by default. They must be installed as part of the en_US or EN_US locale.

Console administrator role

The administrator role is a special console role that can access all console tasks. By default, the root user ID is assigned to the console administrator role.

Since root is authorized to perform any task in AIX, as console administrator, root can select and complete any of the console tasks. If you want to authorize additional users to access all of the console tasks, you can use the Console User Authority task to add them to the console administrator role. This authorization allows them to select any task and gives them the **aix** authorization, which is equivalent to being root.

Installing IBM Systems Director Console for AIX

IBM Systems Director Console for AIX installation and configuration includes installing the required and optional filesets, enabling the IBM Systems Director Console for AIX runtime, and changing port values if needed.

To use IBM Systems Director Console for AIX, it must installed on each managed server. IBM Systems Director Console for AIX is included in the System Management bundle (SystemMgmtClient.bnd) and is part of the default operating system installation.

To verify that IBM Systems Director Console for AIX is installed, you can use the SMIT List Installed Software menus or the operating system command line tools. For example, you can run the following command:

```
lslpp –h sysmgt.pconsole.rte
```

If IBM Systems Director Console for AIX is not installed, you can install it using the SMIT Software Installation menus or the operating system command line tools. For example, you can run the following command:

```
/usr/lib/instl/sm_inst installp_cmd –a –d /dev/cd0 –f sysmgt.pconsole –c –N –g -X
```

This installs the required filesets for IBM Systems Director Console for AIX. The following are the required filesets:

- lwi.runtime
- sysmgt.pconsole.rte
- sysmgt.pconsole.apps.pda
- sysmgt.pconsole.apps.wsmit
- sysmgt.pconsole.apps.wdcem
- sysmgt.pconsole.apps.wrbac
- sysmgt.pconsole.apps.websm

Enabling the runtime

The IBM Systems Director Console for AIX runtime is registered as a subsystem under the control of the system resource controller (SRC). It is started by default at system start up.

You can check, stop, and start the runtime using the SMIT -> Processes & Subsystems -> Subsystems menus or the command line tools for SRC. For example, run the following command to check the runtime:

```
lssrc –s pconsole
```

To stop the runtime, run the following command:

```
stopsrc –s pconsole
```

To start the runtime, run the following command:

```
startsrc –s pconsole
```

Changing port values

IBM Systems Director Console for AIX uses the http: 5335 and https: 5336 ports.

Modify the following properties in the `/pconsole/lwi/conf/overrides/config.properties` file and then restart **pconsole** to change these ports:

- com.ibm.pvc.webcontainer.port=5335
- com.ibm.pvc.webcontainer.port.secure=5336

Also modify `/pconsole/lwi/conf/webcontainer.properties`. Change all occurrences of 5336 to the secure port you wish to use.

Configuring Secure Sockets Layer between the IBM Systems Director Console for AIX and Web browser

By default, the IBM Systems Director Console for AIX provides a Secure Sockets Layer (SSL) certificate that enables HTTPS connections between the IBM Systems Director Console for AIX and the Web browser client.

To ensure server authentication, data privacy, and data integrity, you need to replace the default certificate with either a self-signed certificate or a certificate that is signed by a certificate authority (CA) and change the keystore password. Configuring SSL ensures data integrity and data confidentiality between the server and the Web browser client. This is especially important if you access the IBM Systems Director Console for AIX from outside your network.

Note: Ensure that the host name you specify in the Common Name (**CN**) field of the Secure Sockets Layer (SSL) certificate matches the host name that you specify in the URL you use to access the Web interface. For example, if you specify a long name for the host name in the **CN** field of the certificate, you need to specify a long name in the URL. If these host names do not match, you may receive errors when you try to open the Web interface or start Launch-in-Context tasks. Follow the instructions in the following tasks to ensure that you specify the correct host name in the **CN** field of the certificate.

To replace the default certificate with a new certificate and change the keystore password for Secure Sockets Layer (SSL), perform one of the following tasks.

Configuring Secure Sockets Layer between the IBM Systems Director Console for AIX and the Web browser client using CA-signed certificates

You can replace the default certificate with a certificate signed by a certificate authority (CA). Use this method if you are working with the IBM Systems Director Console for AIX in a production environment.

By default, the IBM Systems Director Console for AIX provides a Secure Sockets Layer (SSL) certificate that enables HTTPS connections between the console and the Web browser client. However, to ensure server authentication, data privacy, and data integrity, you need to replace the default certificate with either a self-signed certificate or a CA-signed certificate and change the keystore password.

You can request a digital certificate from a certificate authority (CA). Since certificate authorities are public entities that issue certificates to identify other entities, CA-signed certificates provide a level of public trust. Therefore, this type of certificate is best suited for a production environment.

The process of replacing your default certificate and password involves the following tasks:

- Stopping the IBM Systems Director Console for AIX server.
- Using the key management utility (iKeyman) to perform the following tasks:
  - Open the default keystore file.
  - Delete the default certificate.
  - Create a certificate signing request (CSR).
  - Send the CSR to a CA.
  - Receive the CA-signed certificate.
  - Add the public version of the CA-signed certificate to the Web browser's truststore file.
  - Change the default password for the keystore file.
- Updating the web container properties.
- Restarting the IBM Systems Director Console for AIX server.
- Updating the browser with the new certificate.

Perform the following steps:

Note: Back up any files before you edit the files.

1. Enter the following commands on the AIX command line to stop the IBM Systems Director Console for AIX server:
   a. stopsrc -s pconsole
   b. lssrc -s pconsole
2. Perform the following steps to start the key management utility (iKeyman):
   Install_Location/**jre/bin/ikeyman.exe**
   Where *Install_Location* is the location of the Java 5 installation directory. The default installation directory is `/usr/java5`.
3. In iKeyman, perform the following steps:
   a. Open the default keystore file:
      1) From the menu bar, select **Key Database File > Open** and select or specify the following information:
         - For **Key Database Type**, select **JKS**.
         - For the **File Name** and **Location** fields, click **Browse...** and select the default keystore file as follows:
           *Install_Location***/lwi/security/keystore/ibmjss2.jks**

Where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is `/pconsole`.

- Click **Open** and click **OK**.
- In the **Password Prompt** window, specify the default password for the default keystore file and click **OK**. The default keystore file password for IBM Systems Director Console for AIX is **ibmpassw0rd**.

2) Perform the following step to delete the default certificate:

   In the **Key Database Content** window, select the default personal certificate named **lwiks** and click **Delete**.

3) Create a certificate signing request (CSR). You need to create a certificate signing request (CSR) so you can request a digital certificate from a CA.
   - From the menu bar, click **Create > New Certificate Request...**.
   - In the **Create New Key and Certificate Request** window, specify the following required information and click **OK**:

     Key Label
     Specify a label for the new certificate (for example, AIXConsole)

     Key Size
     Accept the default value

     Common Name
     Specify the fully qualified host name of the server for which you are creating the CA-signed certificate.

     Note: This host name must match the host name that appears in the URL you specify in your browser to reach the IBM Systems Director Console for AIX. In most cases, you need to specify the fully qualified host name. However, if you use a short name in your URL, you must specify a short name for the Common Name.

     Organization
     Specify the name of your organization.

     Country or region
     Accept the default value.

     – Specify or click **Browse...** to select the name of a file in which to store the certificate request (for example, **AIXConsoleSecPubCertreq.arm**)

4) Send the CSR to a CA. You need to submit the certificate signing request (CSR) to a CA. You can request either a test certificate or a production certificate from the CA. However, in a production environment, you need to request a production certificate. Send the file that you created earlier to the CA by following the instructions provided for requesting a new certificate provided by the CA. You can refer to the CA website for specific instructions.

5) Receive the CA-signed certificate. After the CA accepts the certificate signing request, the CA processes the request and verifies your identity. The CA sends the signed certificate back to you via e-mail. Receive and save the new certificate in the default keystore file.
   - If the CA sends the new certificate to you as part of an e-mail message, cut and paste the certificate from the e-mail message and save it in a certificate file (for example, AIXConsoleSecPubCert.cert).

     Note: The e-mail message from the CA might include supplemental text in front of the certificate and after the certificate. For example you might see the text BEGIN CERTIFICATE in front of the certificate and END CERTIFICATE after the certificate. In this case, ensure that you cut and paste the supplemental text along with the certificate text.

Save the certificate file in the *Install_Location*/**lwi/security/keystore**, where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is `/pconsole`.

- Open the default keystore file if it is not already open.

  Note: Start the key management utility (iKeyman) if you have not done so already.

  a) From the menu bar, select **Key Database File > Open**, and select or specify the following information:
     - For **Key Database Type**, select **JKS**.
     - For the **File Name** and **Location** fields, click **Browse...** and select the *Install_Location*/**lwi/security/keystore/ibmjss2.jks** default keystore file, where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is `/pconsole`.

  b) Click **Open** and click **OK**.

  c) In the **Password Prompt** window, specify the default password for the default keystore file and click **OK**. The default keystore file password for IBM Systems Director Console for AIX is **ibmpassw0rd**.

- In the **Key Database Content** section of the **iKeyman** window, select **Personal Certificates**.
- Click **Receive...**.
- In the **Receive Certificate from a File** window, select or specify the following information:

  Data type
  Select **Base64-encoded ASCII data**.

  Certificate file name
  Specify the name of the certificate file that you created when you received the certificate from the CA (for example, **AIXConsoleSecPubCert.cert**).

  Location
  Specify the directory path to the certificate file (*Install_Location*/**lwi/security/keystore**, where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is `/pconsole`.

- Click **OK**.
- In the **Enter a Label** window, specify a label for the certificate (for example, **AIXConsoleSec**).
- Click **OK**.

6) (Optional) Add the public version of the CA-signed certificate to the Web browser's truststore file. The public version of the certificate contains all identifying information as well as the public key associated with the certificate.

   This optional step can provide additional security within your SSL configuration. The Web browser can determine whether the server presents a certificate that is signed by a trusted signer. If the browser determines that the certificate is not signed by a trusted signer, the browser displays a warning that alerts you to a possible security breach. Configuring SSL for the browser is browser-specific. Consult your browser documentation for instructions.

7) Change the default keystore file password.

   a) From the menu bar, click **Key Database File > Change Password**.

   b) In the **Change Password** window, specify and confirm a new password and click **OK**.

8) Exit iKeyman.

b. Update the web container properties. Since you changed the password, you need to update the web container properties with the new password.

   To update the web container properties, do not edit properties directly within the `webcontainer.properties` file. Instead, create a file named **sslconfig** in the same directory, edit the

properties in the **sslconfig** file, and restart the IBM Systems Director Console for AIX. The process of restarting the IBM Systems Director Console for AIX encrypts the new password in the web container properties.

To update the web container properties, perform the following steps:

1) Change to the *Install_Location*/**lwi/conf** directory, where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is `/pconsole`.
2) Change the name of the **webcontainer.properties** file to **webcontainer.properties.bak**.
3) In the same directory, create a file named **sslconfig** and copy the contents of the **webcontainer.properties.bak** file to the **sslconfig** file.
4) Open the **sslconfig** file with a text editor and change the properties as follows:
   - **com.ibm.ssl.keyStorePassword.5336=***New_Password*, where *New_Password* is the password you previously set.
   - **com.ibm.ssl.trustStore.5336=/../../security/keystore/ibmjsse2.jks**
   - **com.ibm.ssl.trustStorePassword.5336=***New_Password*, where *New_Password* is the password you previously set.
   - Remove the line **sslEnabled=true** from the **sslconfig** file.
5) Save the **sslconfig** file.

   When you restart IBM Systems Director Console for AIX, the **sslconfig** file is used to automatically create a new **webcontainer.properties** file and encrypt the new password in this file. After the new **webcontainer.properties** file has been created, IBM Systems Director Console for AIX deletes the **sslconfig** file since it is no longer needed.

   Note: After you start and connect to the IBM Systems Director Console for AIX, you can delete the **webcontainer.properties.bak** file manually.

c. Restart the IBM Systems Director Console for AIX server by performing the following steps:
   1) startsrc -s pconsole
   2) lssrc -s pconsole
d. Update the Web browser with the new certificate.

   Note: Skip the next step if the public version of the CA-signed certificate is already stored in the browser truststore file. Some browsers contain the public version of well-known CA-signed certificates.

   1) In a Web browser, enter the following to point to the IBM Systems Director Console for AIX:

      http://*Your_Server_Name***:***Port_Number***/ibm/console**

      Where Your_Server_Name is the host name of the IBM Systems Director Console for AIX server and Port_Number is the port for the IBM Systems Director Console for AIX server. The default port is 5335.

      A security alert is displayed. For example, you might see the following message:

      ```
      The security certificate was issued by a company you have not chosen to trust.
      View the certificate to determine whether you want to trust the certifying
      authority.
      ```

   2) In the **Security Alert** window, click **View Certificate**.
   3) In the **Certificate** window, click **Install Certificate**.
   4) Complete the **Certificate Import Wizard**. In the **Security Warning** window, click **Yes**. In the **Certificate Import Wizard** window, click **OK**. In the **Certificate** window, click **OK**. In the **Security Alert** window, click **Yes**.

Note: Messages and settings might differ depending on your browser and the version of Java Web Start that you are running.

Configuring Secure Sockets Layer between the IBM Systems Director Console for AIX and the Web browser client using self-signed certificates

You can replace the default certificate with a self-signed certificate. Use this method if you are working with the IBM Systems Director Console for AIX in a test environment.

By default, the IBM Systems Director Console for AIX provides a Secure Sockets Layer (SSL) certificate that enables HTTPS connections between the IBM Systems Director Console for AIX and the Web browser client. However, to ensure server authentication, data privacy, and data integrity, you need to replace the default certificate with either a self-signed certificate or a CA-signed certificate and you need to change the keystore password.

Self-signed certificates are certificates that you create yourself for private use. After you create them, you can use them immediately. Because anyone can create self-signed certificates, they are not considered publicly trusted certificates. Therefore, use self-signed certificates only on a temporary basis while testing your environment.

The process of replacing your default certificate and password involves the following tasks:

- Stopping the IBM Systems Director Console for AIX server.
- Using the key management utility (iKeyman) to perform the following tasks:
  - Open the default keystore file.
  - Delete the default certificate.
  - Create a self-signed certificate for a test environment.
  - Change the default password for the keystore file.
- Updating the web container properties.
- Restarting the IBM Systems Director Console for AIX server.
- Updating the browser with the new certificate.

Complete the following steps:

Note: Back up any files before you edit the files.

1. Stop the IBM Systems Director Console for AIX server by completing the entering the following commands on the AIX command line:
   a. stopsrc -s pconsole
   b. lssrc -s pconsole
2. Run the following command to start the key management utility (iKeyman):

   *Install_Location***/jre/bin/ikeyman.exe**

   Where *Install_Location* is the location of your Java 5 installation directory. The default installation directory is `/usr/java5`.
3. In iKeyman, perform the following steps:
   a. Open the default keystore file:
      1) From the menu bar, select **Key Database File > Open**, and select or specify the following information:
         - For **Key Database Type**, select **JKS**.
         - For the **File Name** and **Location** fields, click **Browse...** and select the *Install_Location***/lwi/security/keystore/ibmjss2.jks** default keystore file, where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is `/pconsole`.
      2) Click **Open** and click **OK**.

3) In the **Password Prompt** window, specify the default password for the default keystore file and click **OK**. The default keystore file password for IBM Systems Director Console for AIX is **ibmpassw0rd**.

b. Delete the default certificate. In the **Key Database Content** window, select the default personal certificate named **lwiks** and click **Delete**.

c. Create a new self-signed certificate:

From the menu bar, select **Create > New Self-Signed Certificate.....** In the **Create New Self-Signed Certificate** window, specify the following required information, and click **OK**:

Key Label
Specify a label for the new certificate (for example, AIXConsole).

Version
Select X509 V3

Key Size
Accept the default value

Common Name
Specify the fully qualified host name of the server for which you are creating the self-signed certificate

Note: The host name must match the host name that appears in the URL you specify in your browser to reach the IBM Systems Director Console for AIX. In most cases, you must specify the fully qualified host name. However, if you use a short name in your URL, you need to specify a short name for the **Common Name**.

Organization
Specify the name of your organization

Country or region
Accept the default value

Validity Period
Specify the lifetime of the certificate in days or accept the default value

d. Change the default keystore file password.

1) From the menu bar, select **Key Database File > Change Password**. In the **Change Password** window, specify and confirm a new password and click **OK**.

e. Exit iKeyman.

4. Update the web container properties. Since the password was changed in the previous step, you need to update the web container properties with the new password.

To update the web container properties, do not edit properties directly within the **webcontainer.properties** file. Instead, create a file named **sslconfig** in the same directory, edit the properties in the **sslconfig** file, and restart the IBM Systems Director Console for AIX. The process of restarting the IBM Systems Director Console for AIX encrypts the new password in the web container properties.

To update the web container properties, perform the following steps:

a. Change to the *Install_Location*/**lwi/conf** directory, where *Install_Location* is the location of your IBM Systems Director Console for AIX installation directory. The default installation directory is `/pconsole`.

b. Change the name of the **webcontainer.properties** file to **webcontainer.properties.bak**.

c. In the same directory, create a file named **sslconfig** and copy the contents of **webcontainer.properties.bak** file to the **sslconfig** file.

d. Open the **sslconfig** file with a text editor and change the properties as follows:

Note: Specify only plaintext values for the passwords in the **sslconfig** file.

Note: In this example, the following properties indicate that IBM Systems Director Console for AIX is using secure port 5336. If you are using a secure port other than 5336, your properties will indicate a different port. Do not change the port indicated in the properties.

- **com.ibm.ssl.keyStorePassword.5336=***New_Password*, where *New_Password* is the password you previously set.
- **com.ibm.ssl.trustStore.5336=/../../security/keystore/ibmjsse2.jks**
- **com.ibm.ssl.trustStorePassword.5336=***New_Password*, where *New_Password* is the password you previously set.
- Remove the line **sslEnabled=true** from the **sslconfig** file.

e. Save the **sslconfig** file.

When you restart IBM Systems Director Console for AIX, the **sslconfig** file is used to automatically create a new **webcontainer.properties** file and encrypt the new password in this file. After the new **webcontainer.properties** file has been created, IBM Systems Director Console for AIX deletes the **sslconfig** file since it is no longer needed.

Note: After you start and connect to the IBM Systems Director Console for AIX, you can manually delete the **webcontainer.properties.bak** file.

5. Restart the IBM Systems Director Console for AIX server by performing the following steps:
   a. startsrc -s pconsole
   b. lssrc -s pconsole
6. Update the Web browser with the new certificate.
   a. In a Web browser, type the following to point to the IBM Systems Director Console for AIX:

   http://*Your_Server_Name***:***Port_Number***/ibm/console**

   Where *Your_Server_Name* is the host name of the IBM Systems Director Console for AIX server and *Port_Number* is the port for the IBM Systems Director Console for AIX server. The default port is 5335.

   A Security Alert is displayed. For example, you might see the following message:

   ```
   The security certificate was issued by a company you have not chosen to trust.
   View the certificate to determine whether you want to trust the certifying
   authority.
   ```

   b. In the **Security Alert** window, click **View Certificate**.
   c. In the **Certificate** window, click **Install Certificate**.
   d. Complete the **Certificate Import Wizard**.
   e. In the **Security Warning** window, click **Yes**.
   f. In the **Certificate Import Wizard** window, click **OK**.
   g. In the **Certificate** window, click **OK**.
   h. In the **Security Alert** window, click **Yes**.

Note: Messages and settings might differ depending on your browser and the version of Java Web Start that you are running.

Starting IBM Systems Director Console for AIX

You can access the IBM Systems Director Console for AIX from the following supported Web browsers: Internet Explorer 7, or later, on Windows, Mozilla Firefox 2.0, or later, on Windows, and Mozilla Firefox 1.5.0.10, or later, on AIX

1. To start the console, open a browser and go to http://**HostName**:5335/ibm/console, where **HostName** is your server name.

   Note: You must use https:// if you configured the IBM Systems Director Console for AIX to work with Secure Sockets Layer (SSL).

2. On the login page, enter your user name and password for this system.
3. Click **Log in**.

Note: To display help information for any of the pages in the IBM Systems Director Console for AIX, click the help icon  .

Troubleshooting IBM Systems Director Console for AIX

The following table lists some troubleshooting information for IBM Systems Director Console for AIX.

Table 1. General problems

Issue	Possible causes and solutions
My connection keeps timing out when trying to connect to the console URL.	Try to telnet to the server to make sure it's not behind a firewall. Since the console is not on port 80, you may not be automatically prompted for your firewall credentials.
My session keeps invalidating.	Since the console only allows one instance per user, somebody could be logging in with the same username and invalidating your session.
You cannot log in	Verify that you have a user account on the server. Log in to the server on a directly attached terminal or with the **telnet** command.

The console is very slow to load the first time I launch it.	If you are connecting to a WPAR, the console runtime is not started until the first connection. The **pconsoleProxy** subsystem intercepts the request and starts the console runtime. Verify that the **pconsoleProxy** subsystem is active. You can query the status of the **pconsoleProxy** subsystem by running
	`lssrc –s pconsoleProxy`
	
	You can query the status of the pconsole subsystem by running
	`lssrc –s pconsole`

When I try to connect to the console URL, I get an "Unable to Connect" or "the page cannot be loaded" message.	Check whether the console subsystem is active by running **lssrc –s pconsole**. If it is not active, try to start it by running **startsrc –s pconsole**. If it does not start and you get a message such as " *The pconsole Subsystem could not be started. The Subsystem's user id could not be established. Please check the Subsystem's user id and try again.*",check that the pconsole user account has not been removed and that the UID matches the UID that owns the files under /pconsole. If the user account is missing, reinstall sysmgt.pconsole.rte so that the account is recreated with the required attributes. If the user account exists, but the UID is incorrect, remove the user account and reinstall sysmgt.pconsole.rte.
You see only the **Welcome** page.	There are no other tasks in the navigation tree. Your user ID is not authorized for tasks in the console. Contact the console administrator (usually the root user) to add your user ID to the desired console roles.
The task you are trying to execute fails.	Many of the tasks in the OS Management category are based on SMIT. If a task fails in the console, try the task in SMIT or smitty to see it it also fails there. Log in to the system on a local terminal or via telnet and try the task in SMIT/smitty. If it also fails in SMIT/smitty, then the problem may be in SMIT or in the commands or scripts executed by SMIT. Use the "Show Command" function (F6) to show the command and if possible try to perform the task using the command line to see if the failure is caused by the command or by SMIT/smitty.

Table 1. General problems (continued)

Issue	Possible causes and solutions
Some tasks appears to be missing from the navigation area.	You will not be able to see tasks in the navigation area unless your login id has been added to the console roles. The console administrator id (usually root) can add users to console roles. When you are logged in as console administrator (by default root) all tasks are visible.
You are having problems with login and authentication.	1. If someone is already logged into the console with the same user id, authentication will fail. The console allows only one session per user-id, per system. The console gives you the option of ending the current session and starting a new one, or waiting until it is ended by the person who initiated it. 2. Verify that the user has an account on the system you are connecting to. To do this, login to the system and list all users. If the user is not listed, add them to the system. 3. Verify that the user's password has not expired. If the user does not have a password (for example, if it is a new account) or if the password has expired, the user will not be able to log in to the console. To resolve this, the user must log in to the system via telnet or a local terminal and set the password.
You get AIX authorization errors when performing a task.	If you are not logged in as root and enhanced RBAC is enabled (it is enabled by default), most administrative commands require you to have specific aix authorizations. If you encounter authorization errors please try the following: • Check that you have the authorizations required for the task. • Try the task using smitty or on the command line to determine if the authorization errors also occur outside of the console. • If you discover that authorizations are needed for the task, but they are not included by the Console User Authority application, use the Users and Security task to add the authorizations to the user's role. Open a problem report so the lab can fix applications authorization descriptor. • If you discover administrative tasks that fail because they are not instrumented for enhanced RBAC. For example, they have hard coded checks for root or uid 0, open a problem report so the lab can fix the code.

You accidentally delete the user pconsole.	All of the files belonging to IBM Systems Director Console for AIX belong to the userid pconsole. On most machines (those running with Enhanced RBAC) the console runs as the user pconsole. If you delete this user, then the console will not be able to run. If pconsole's user id and group id has not be re-used for some other purpose you can recreate the pconsole user and group by specifying the original ids. You can see the ids by:
	`#ls -l /pconsole`
	
	If recreating the pconsole user and group does not work then you should reinstall the console, using the original installation media via:
	`#installp -agXd`
	`<install device> sysmgt.pconsole`

You don't see all of the menus that you see in smitty.	This is most likely due to additional software being installed after the console was started. You should restart the console while logged in as root with:
	`#stopsrc -s pconsole`
	`#startsrc -s pconsole`

Table 1. General problems (continued)

Issue	Possible causes and solutions
Your /var or $HOME filesystem becomes full.	Log files for the console are stored in /var/log/pconsole. In addition, each user of the console will have a wsmit.log and wsmit.script file in their home directory. Deleting these files will not free up memory until the user logs out of the console, however instead of deleting the file you empty it via: `#echo "" > <path_to_log_file>` Additional files are stored in $HOME/dcem. These files include output results, scripts and command specs.
You are having problems with the editor.	There are a small number of instances where a user is placed in an editor while in the SMIT Command Output panel. There is a problem with the console's terminal emulator that causes the vi paste command (Esc + p) to paste a blank line instead of what is in the paste buffer.
You can not find a way to change memory heap size.	The default maximum memory heap size is 512 MB. You can configure this value by editing /pconsole/lwi/conf/overrides/pconsole.javaopt.

Table 2. Problems unique to DCEM

Issue	Possible causes and solutions
You are unable to execute new jobs, generate scripts, or save command specification.	Check to see if any of the filesystems have run out of free space. DCEM stores command specs, results, and scripts in $HOME/dcem.
Your filesystem is filling up when you are executing jobs with DCEM.	DCEM stores all of the output/results in $HOME/dcem. If you're executing jobs that produce a lot of output, you may need to increase your $HOME filesystem size.
All of your jobs are failing and the output says that "Permission is Denied."	Make sure you have the correct permissions by executing a job via the command line. Also, the shell that you're using for authentication on the remote hosts (rsh or ssh) must be specified on the 'Options' tab in DCEM.

Table 3. Problems unique to Role Based Access Control applications

Issues	Possible causes and solutions
Task links on the Role Based Access Control application Welcome Page are not active.	• Check that enhanced RBAC is enabled by running the lsauth ALL command. If enhanced RBAC is enabled, authorization attributes will be listed and the return code will be 0. • Check that you are logged into the console as the console administrator.
The roles and authorizations that I have added have not taken effect.	Run the **Synchronize Data** task to update the RBAC Security Table. Then have the user log in and activate their new or modified roles using the **swrole** command.

Problem Determination Advisor

The Problem Determination Advisor is an application in IBM Systems Director Console for AIX that quickly solves system problems by running well-defined, structured procedures based on best practices.

Problem Determination Advisor monitors specified subsystems using a set of extensible probes that run periodically to check system health or other user-defined conditions. When a probe discovers a problem, it triggers a problem determination rule to collect real-time information about the problem. Problem determination rules are themselves composed of probes, each of which collect a specific piece of information to help diagnose the current problem. This approach performs detailed probing only when it is relevant to the problem at hand, thus avoiding the overhead of collecting such data all the time. A key

feature of Problem Determination Advisor is the ability to extend it with new problem determination rules and associated probes to tailor it to a particular environment.

Accessing Problem Determination Advisor

You can access the Problem Determination Advisor application from the IBM Systems Director Console for AIX console.

Problem Determination Advisor is a portal that displays an overview of the system status. You can get a detailed understanding of the system status by clicking **Probe Status**. In addition, you can manage the collected information and problem diagnosis rules by using the **Probe Manager** and **Rule Manager**.

To access Problem Determination Advisor from the IBM Systems Director Console for AIX console, complete the following steps:

1. To start the console, open a browser and go to http://**HostName**:5335/ibm/console, where **HostName** is your server name.
2. On the log in page, enter your user name and password for this system, and click **Log in**.
3. In the navigation tree, expand **Monitoring** and select **Problem Determination Advisor**.

   Note: To display help information for any of the pages in the Problem Determination Advisor, click the help icon  .

Problem Determination Advisor Probes

Probes are scripts that can gather any available system information, typically using utilities and commands from the operating system.

Data collected from probes must follow a specified structure for correct communication to Problem Determination Advisor. Problem Determination Advisor provides the user with a template and a set of support libraries to assist with output formatting for probes written in the Perl scripting language.

Although all probes in Problem Determination Advisor are implemented in the same way, and have the same features, it is useful to think about probes in terms of their role in problem determination. For example, probes that are enabled for periodic monitoring of the system can be thought of as monitoring probes. Other probes that are used to collect specific pieces of information in problem determination advisor rules can be thought of as diagnostic probes. Problem Determination Advisor allows any probe to be used for either monitoring or diagnosis, however, guidelines should be followed to ensure that appropriate probes are used for monitoring and diagnosis purposes.

When a Problem Determination Advisor monitoring probe is enabled, it can be associated with a rule that runs when the probe detects a non-normal condition. Monitoring probes can be enabled immediately when they are created, or later from the Probe Manager page. Not every monitoring probe needs to be associated with a problem determination rule, however, a rule must be associated to a monitoring probe in order to be triggered. Each probe can trigger one rule. However, an individual rule can be assigned to more than one probe.

Viewing Problem Determination Advisor probes

You can view the status of each probe, an analysis of problems detected by the probe, and the history of the data collected by the probe.

To view Problem Determination Advisor probe status, complete the following steps:

1. Access the Problem Determination Advisor.
2. Click **Probe Status**.
3. Click the name of the probe for which you want to view status. The **Report** tab is selected by default and displays a graphical report of the data collected by the probe.

Note: Use the **Data Point** field to specify how many graphical entries you want displayed. Use the **Chart Type** field to change the types of graphs displayed.

4. Click the **Analysis** tab to view the output of the problem diagnosis rule associated with the probe.
5. Click the **History** tab to view all of the data collected by the probe up to the current time.

Note: To display help information for any of the pages in the Problem Determination Advisor, click the help icon  .

Related tasks:

"Accessing Problem Determination Advisor" on page 16
You can access the Problem Determination Advisor application from the IBM Systems Director Console for AIX console.

Creating Problem Determination Advisor probes

The Problem Determination Advisor provides considerable freedom and simplicity in creating probe scripts.

Review the following guidelines for information on creating a successful probe:

Design probes to operate in a read-only fashion
Design probes to collect information to aid in monitoring key subsystems, or to collect data that helps in problem diagnosis. Avoid creating probes that change system parameters or configuration automatically, without the involvement of the system operator.

Test probes carefully before deploying
Run probe scripts in test or non-production environments to ensure they run correctly without any adverse effects. After verifying that they operate as intended, probes can be deployed in Problem Determination Advisor using the probe creation facility.

Set monitoring probe frequency conservatively
Monitoring probes run continuously with regular frequency that can be specified individually for each probe. In general, the least frequent execution schedule that meets the problem detection goal should be specified. For example, most monitoring probes should be run using a minute timescale.

Monitoring probes should be simple
Monitoring probes run periodically, use caution to ensure they do not impose high computational, memory, or I/O overhead on the system. Probes that are used as diagnostic probes, which are executed by a problem determination rule only when a problem occurs, can be more complex because they do not run continuously.

To create a new Problem Determination Advisor probe, complete the following steps

1. Access the Problem Determination Advisor.
2. Click **Probe Manager**.
3. Click **Create**.
4. Complete all required fields and click **Submit**.

Note: To display help information for any of the pages in the Problem Determination Advisor, click the help icon  .

Related tasks:

"Accessing Problem Determination Advisor" on page 16
You can access the Problem Determination Advisor application from the IBM Systems Director Console for AIX console.

Managing Problem Determination Advisor probes

Once you have created a probe you can edit, delete, enable, disable, and reset the probe.

To manage Problem Determination Advisor probes, complete the following steps:

1. Access the Problem Determination Advisor.
2. Click **Probe Manager**.
3. Select the probe that you want to manage from the table.
4. Click **Actions**, and select the managing task you want to complete.

Note: To display help information for any of the pages in the Problem Determination Advisor, click the help icon  .

Related tasks:

"Accessing Problem Determination Advisor" on page 16
You can access the Problem Determination Advisor application from the IBM Systems Director Console for AIX console.

Example: Processor use probe

This example displays a simple probe that collects processor use information and returns it to Problem Determination Advisor in a structured format. The probe also returns the raw output so that you can view it.

```
#!/usr/bin/perl -w
use lib /opt/pconsole/pda/bin/cache;
use pdaprint;

#----------------------------------
# Program Name: cpu_util.pl
#----------------------------------

@result = `vmstat 1 2`;
$which = $#result;
@data = split(" ", $result[$which]);

$raw = join("", @result);

$structured{"UTIL(%)"} = 100 - $data[15];
$structured{"WAIT(%)"} = $data[16];
$structured{"SYSTEM(%)"} = $data[14];
$structured{"USR(%)"} = $data[13];

&PDAPrint::doPrint($raw, %structured);
```

The probe uses the **vmstat** command and creates a Perl associative array that contains the desired data items. The keys are of the form LABEL (units) so that the user can specify the units when the probe results are shown on the console. The raw data is returned as a simple string.

The option to indicate different severity levels is provided when you are enabling a monitoring probe using the **Probe Manager** dialog. For example, it allows conditions (thresholds) to be set on one of the structured data item that corresponds to different severity levels. The table below shows an example:

Table 4. Severity levels

Data item	Condition	Value	Severity
WAIT	Default		Normal
WAIT	>	30	Warning
WAIT	>	75	Critical

If neither the Warning nor Critical severity condition is met, the result is considered to be Normal and will show green. In this example, a CPU I/O wait time of 40% would show as a Warning on the Probe Status page, while a value of 81% would show as Critical.

Note: The thresholds used here are examples. Actual values should be adjusted based on your system's workload.

Various properties of probes can also be modified, such as severity conditions, which probe results to show in graphs, and the probe code.

Problem Determination Advisor Rules

Problem determination rules in Problem Determination Advisor are structured in a decision tree format that collects information based on the results of a previous step. This allows you to use or create a detailed problem diagnosis procedure that incorporates conditional checks.

Problem Determination Advisor rules allow you to capture structured repeatable procedures for collecting system information to aid in problem diagnosis. While Problem Determination Advisor includes a number of useful rules for common types of problems, it also provides a simple way to create new rules that are suited for a particular environment, or a different type of problem.

When a rule is triggered, Problem Determination Advisor collects data according to the decision tree, where the traversed path through the tree represents the series of diagnostic steps for the problem. Each step involves the execution of a diagnostic probe, and evaluation of the results of the probe. The next step is based on the condition being checked and the output of the current probe.

A rule is triggered by a specified monitoring probe that serves as the root node of the rule decision tree. The trigger can be a threshold violation, inability to reach a remote machine, or other detected problems. Each rule can be associated with one monitoring probe, though not all probes need to have a corresponding problem determination rule.

Creating Problem Determination Advisor rules

A rule collects a set of probes together to implement a problem diagnosis procedure.

Execution of a rule is typically triggered or activated by a periodic probe. For example, a periodic probe could check if memory usage is above a certain threshold. Once a rule is triggered, it conducts a series of conditional checks, each of which is implemented as a one-time probe. Therefore, a rule requires that each check that should be performed during the problem determination procedure has a corresponding probe defined to collect the necessary data.

To create Problem Determination Advisor rules, complete the following steps:

1. Access the Problem Determination Advisor.
2. Click **Rules Manager**.
3. Click **Create**.
4. Complete all required fields and click **Submit**.

   Note: To display help information for any of the pages in the Problem Determination Advisor, click the help icon  .

Related tasks:

"Accessing Problem Determination Advisor" on page 16
You can access the Problem Determination Advisor application from the IBM Systems Director Console for AIX console.

Managing Problem Determination Advisor rules

Once you have created a Problem Determination Advisor rule, you can edit, view, or delete rules.

To manage Problem Determination Advisor rules, complete the following steps:

1. Access the Problem Determination Advisor.
2. Click **Rules Manager**.
3. Select the rules that you want to manage from the table.
4. Click **Actions**, and select the managing task you want to complete.

Note: To display help information for any of the pages in the Problem Determination Advisor, click the help icon  .

Related tasks:

"Accessing Problem Determination Advisor" on page 16
You can access the Problem Determination Advisor application from the IBM Systems Director Console for AIX console.

Uploading Problem Determination Advisor rules

You can use the Problem Determination Advisor Rule Manager to upload an XML file directly without losing context.

To upload Problem Determination Advisor rules, complete the following steps:

1. Access the Problem Determination Advisor.
2. Click **Rule Manager**.
3. Click **Actions**, and select **Upload**.
4. Enter the existing XML schema.
5. Click **Submit** to upload the rule.

Note: To display help information for any of the pages in the Problem Determination Advisor, click the help icon  .

Related tasks:

"Accessing Problem Determination Advisor" on page 16
You can access the Problem Determination Advisor application from the IBM Systems Director Console for AIX console.

Example: Problem Determination Advisor rule

Problem Determination Advisor rules are constructed with existing probes that collect diagnosis data at each step. Rules are triggered by an associated probe that is enabled for monitoring.Problem Determination Advisor rules are expressed using a simple XML schema that encodes the nodes of the decision tree making up the rule.

Consider a simple rule that checks reachability for a designated host. The logic of such a rule may look like the following:

```
if ping_by_hostname <myhost.com> == true
  host is responding; no further action needed
else if ping_by_hostIPaddress <IP address of myhost.com> == true
  host is reachable by IP; check DNS configuration
else if ping_localgateway <gateway IP> == true
```

```
  gateway is reachable; check for routing problems
else
  network is inaccessible; check local host network config
```

In this simplified example, remote host connectivity is diagnosed using a series of checks, each of which collects an additional piece of information depending on the result of a previous check.

Translating this into a Problem Determination Advisor rule requires the necessary set of probes first be created, for example:

```
ping_by_hostname, ping_by_hostIPaddress, and ping_localgateway.
```

These probes should be written to test the corresponding host names, and addresses should have the following XML representation:

```
<tns:rule xmlns:tns="http://www.example.org/RuleSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.example.org/RuleSchema RuleSchema.xsd ">
 <name>check-host</name>
 <version>1.0</version>
 <platform>AIX</platform>
 <description>Simple host network PD</description>
 <nodes>
  <node>
   <node_id>0</node_id>
   <true_node_id>1</true_node_id>
   <false_node_id>2</false_node_id>
   <probe_name> ping_by_host_name.pl</probe_name>
   <probe_version>1.0</probe_version>
   <probe_args>myhost.com</probe_args>
   <conditions>
    <condition>
     <event_name>REACHABLE()</event_name>
     <operator>==</operator>
     <event_value>1</event_value>
    </condition>
   </conditions>
   <action_explanation>check host reachability</action_explanation>
  </node>
  <node>
   <node_id>1</node_id>
   <action_explanation>host responding</action_explanation>
  </node>
  <node>
   <node_id>2</node_id>
   <true_node_id>3</true_node_id>
   <false_node_id>4</false_node_id>
   <probe_name>ping_by_hostIPaddress.pl</probe_name>
   <probe_version>1.0</probe_version>
   <probe_args>10.100.0.12</probe_args>
   <conditions>
    <condition>
     <event_name>REACHABLE()</event_name>
     <operator>==</operator>
     <event_value>1</event_value>
    </condition>
   </conditions>
   <action_explanation>check IP addr reachable</action_explanation>
  </node>
  <node>
   <node_id>3</node_id>
   <action_explanation>check DNS configuration</action_explanation>
  </node>
  <node>
   <node_id>4</node_id>
   <true_node_id>5</true_node_id>
   <false_node_id>6</false_node_id>
```

```
   <probe_name>ping_localgateway.pl</probe_name>
   <probe_version>1.0</probe_version>
   <probe_args>10.1.0.2</probe_args>
   <conditions>
    <condition>
     <event_name>REACHABLE()</event_name>
     <operator>==</operator>
     <event_value>1</event_value>
    </condition>
   </conditions>
   <action_explanation>check gw reachable</action_explanation>
  </node>
  <node>
   <node_id>5</node_id>
   <action_explanation>
    likely routing configuration problem
   </action_explanation>
  </node>
  <node>
   <node_id>6</node_id>
   <action_explanation>
    network is inaccessible
   </action_explanation>
  </node>
 </nodes>
</tns:rule>
```

In this example, each node in the rule specifies either a diagnostic probe and associated condition (node 1), or an outcome with an associated explanation (node 6). When you are using a diagnostic probe, the condition is specified based on one of the output values returned by the probe. If the condition is true, the node specified in the `<true_node_id>` section runs. If the condition is false, the node in `<false_node_id>` runs. The conditions supported in PDA are shown in the following table.

Table 5. Available conditional operators in rules

Operator	Condition
==	numeric equality
>,<,<=,<=	numeric inequality
!=	numeric not equal to
eq	string equality
exc	string does not include
gt, lt, le, ge	string inequality
inc	string includes
ne	string not equal to

Task History

Task History lets you view the history of tasks that ran on the system. You can use the Task History application for security logging, creating a prototype for a shell script, and aiding problem resolution.

You can also use Task History for the following tasks:

- Delete task entries
- Export task entries as plain text or XML.
- Paste task entries to the IBM Systems Director Console for AIX Distributed Command Execution Manager (DCEM) for execution on other machines.

Note: The logging ability is similar to the task log in Web-based System Manager or the smit.log in System Management Interface Tool (SMIT). Not every command run by the console is logged in the Task History application, only the ones that make a change to the system.

Accessing Task History

You can access Task History from the IBM Systems Director Console for AIX console.

The Task History application is only available if you are running AIX Version 6.1 with the 6100-02 Technology Level or later.

To access Task History from the IBM Systems Director Console for AIX console, complete the following steps:

1. To start the console, open a browser and go to http://**HostName**:5335/ibm/console, where **HostName** is your server name.
2. On the login page, enter your user name and password for this system.
3. In the navigation tree, expand **Monitoring** and select **Task History**.

   Note: To display help information for any of the pages and fields in Task History, click the help icon  .

Modify Task History settings

You can only access Task History settings if you are logged in as an administrator. Any changes you make will apply to all users.

To edit the settings for Task History, complete the following steps:

1. Access Task History.
2. Click **Edit Settings** and specify any changes.
3. Click **Ok** to save your changes.

   Note: To display help information for any of the pages and fields in Task History, click the help icon  .

Related tasks:

"Accessing Task History"
You can access Task History from the IBM Systems Director Console for AIX console.

Deleting Task History entries

You can delete any task entry you do not want displayed in the Task History table.

To delete tasks from the Task History table, complete the following steps:

1. Access Task History.
2. Select the task entries you want to remove from the table.

   Note: If you want to delete every task entry from the table, click **Actions** and select **Select All**.
3. Click **Delete** to remove selected task entries.

   Note: To display help information for any of the pages and fields in Task History, click the help icon  .

Related tasks:

"Accessing Task History"
You can access Task History from the IBM Systems Director Console for AIX console.

Managing Task History entries

You can use Task History to view task entries, print task entries, save task entries, and run task entries with Distributed Command Execution Manager (DCEM).

To manage tasks from the Task History table, complete the following steps:

1. Access Task History.
2. Select the task entries you want to view, print, save, or run from DCEM in the table.
3. Click **Actions** and select the management task you want to complete.

   Note: To display help information for any of the pages and fields in Task History, click the help icon .

Related tasks:

"Accessing Task History" on page 23
You can access Task History from the IBM Systems Director Console for AIX console.

Using Distributed Command Execution Manager with Task History

The Distributed Command Execution Manager (DCEM) provides a variety of services for a network of distributed machines. You can select any command from the Task History application and send the command to DCEM for execution on multiple target machines.

To send a command to DCEM from Task History, complete the following steps:

1. Access Task History.
2. Select the task entry you want to send to DCEM.

   Note: You can only select a single task at a time to send to DCEM.
3. Select **Actions** > **Send to DCEM**.

   Note: To display help information for any of the pages and fields in Task History, click the help icon .

Related tasks:

"Accessing Task History" on page 23
You can access Task History from the IBM Systems Director Console for AIX console.

Console User Authority

Console User Authority for IBM Systems Director Console for AIX allows a console administrator to modify the roles assigned to console users (any valid system users).

The administrator can add or remove roles from individual users. You can log into IBM Systems Director Console for AIX as root, which gives you the authority to perform all tasks, or you can designate certain tasks to non-root users. You can use the Console User Authority to give non-root users access to applications and tasks in the navigation area and the AIX authorizations for the actions performed for a particular task.

Accessing Console User Authority

Only users with administrator privileges can access Console User Authority from the IBM Systems Director Console for AIX console.

The Console User Authority application is only available if you are running AIX Version 6.1 with the 6100-02 Technology Level or later.

To access Console User Authority from the IBM Systems Director Console for AIX console, complete the following steps:

1. To start the console, open a browser and go to http://**HostName**:5335/ibm/console, where **HostName** is your server name.
2. On the login page, enter your user name and password for this system.
3. In the navigation tree, expand **Settings** and select **Console User Authority**.

   Note: To display help information for any of the pages and fields in Console User Authority, click the  icon.

Adding users to Console User Authority

You can authorize any user access to specific applications and tasks using the Console User Authority application.

To add a user to the Console User Authority application, complete the following steps:

1. Access the Console User Authority.
2. Click **Add User**.
3. Specify the name of the user if you know it, or click **Browse** to select the user from a list of all users on the system.
4. Click **Add** for the corresponding role you want to assign the user.

   Note: Click **Details** for a description of the role and a list of the AIX RBAC authorizations that will be assigned to the new user.
5. Click **OK**.

   Note: To display help information for any of the pages and fields in Console User Authority, click the  icon.

Related tasks:

"Accessing Console User Authority" on page 24
Only users with administrator privileges can access Console User Authority from the IBM Systems Director Console for AIX console.

Removing users from the Console User Authority application

You can remove a user's access to the system using the Console User Authority application.

To remove a user from the Console User Authority application, complete the following steps:

1. Access the Console User Authority.
2. Select one or more users in the table that you want to remove.
3. Click **Remove Users**.

   Note: To display help information for any of the pages and fields in Console User Authority, click the  icon.

Related tasks:

"Accessing Console User Authority" on page 24
Only users with administrator privileges can access Console User Authority from the IBM Systems Director Console for AIX console.

Role Based Access Control for IBM Systems Director Console for AIX

Role Based Access Control (RBAC) for IBM Systems Director Console for AIX allows you to create, assign, modify, and delete user roles, authorizations, and privileges on the system by using a browser in a server-client environment.

Using RBAC, system administrators can parse a subset of super-user permissions and capabilities and assign them to roles. A user can then assume those roles. This allows a user with the appropriate roles to perform tasks on the system that normally require super-user authority. Thus, RBAC provides a more secure alternative to the traditional approach of using super-user authority for all system administration tasks.

Related information:

Role Based Access Control (RBAC)

Accessing Role Based Access Control

You can access Role Based Access Control (RBAC) from the IBM Systems Director Console for AIX console.

The RBAC application is only available if you are running AIX 6.1 or later.

To access RBAC from the IBM Systems Director Console for AIX console, complete the following steps:

1. To start the console, open a browser and go to http://**HostName**:5335/ibm/console, where **HostName** is your server name.
2. On the login page, enter your user name and password for this system.
3. In the navigation tree, expand **OS Management** and select **Role Based Access Control**.

Related tasks:

"Creating Role Based Access Control authorizations"
You can create user-defined authorizations on the system by using the Role Based Access Control (RBAC) application in the IBM Systems Director Console for AIX console.

"Creating Role Based Access Control roles" on page 27
You can create new roles on the system by using the Role Based Access Control (RBAC) application in the IBM Systems Director Console for AIX console.

"Managing Role Based Access Control authorizations" on page 27
You can view, edit, and delete user authorizations that exist on the system by using the Role Based Access Control (RBAC) application in the IBM Systems Director Console for AIX console.

"Managing Role Based Access Control roles" on page 27
You can view, edit, and delete roles that exist on the system by using the Role Based Access Control (RBAC) application in the IBM Systems Director Console for AIX console.

Related information:

Role Based Access Control (RBAC)

Creating Role Based Access Control authorizations

You can create user-defined authorizations on the system by using the Role Based Access Control (RBAC) application in the IBM Systems Director Console for AIX console.

To create a new user-defined authorization on the system, complete the following steps:

1. Access Role Based Access Control.
2. Click **New user defined authorization**.
3. Complete all required fields and click **OK**.

Related tasks:

"Accessing Role Based Access Control" on page 26
You can access Role Based Access Control (RBAC) from the IBM Systems Director Console for AIX console.

Related information:

RBAC Authorizations

Administering enhanced RBAC

Creating Role Based Access Control roles

You can create new roles on the system by using the Role Based Access Control (RBAC) application in the IBM Systems Director Console for AIX console.

To create a new role on the system, complete the following steps:

1. Access Role Based Access Control.
2. Click **New role**.
3. Complete the wizard and click **Finish**.

Related tasks:

"Accessing Role Based Access Control" on page 26
You can access Role Based Access Control (RBAC) from the IBM Systems Director Console for AIX console.

Related information:

RBAC roles

Administering enhanced RBAC

Managing Role Based Access Control authorizations

You can view, edit, and delete user authorizations that exist on the system by using the Role Based Access Control (RBAC) application in the IBM Systems Director Console for AIX console.

To manage user-defined authorizations that currently exist on the system, complete the following steps:

1. Access the Role Based Access Control.
2. Click **Manage user defined authorizations**.
3. Select the user-defined authorization that you want to manage and click one of the following management tasks to perform:
   - **Properties** to view the properties of the selected authorization and to edit the description of the selected authorization.
   - **Delete** to delete the selected authorization.
   - **View Roles** to view and edit the roles that include the selected authorization.

Related tasks:

"Accessing Role Based Access Control" on page 26
You can access Role Based Access Control (RBAC) from the IBM Systems Director Console for AIX console.

Related information:

RBAC Authorizations

Administering enhanced RBAC

Managing Role Based Access Control roles

You can view, edit, and delete roles that exist on the system by using the Role Based Access Control (RBAC) application in the IBM Systems Director Console for AIX console.

To manage roles that exist on the system, complete the following steps:

1. Access the Role Based Access Control.
2. Click **Manage roles**.
3. Select the role that you want to manage and click one of the following management tasks to perform:
   - **Properties** to view and edit the selected role.
   - **Delete** to delete the selected role.

Related tasks:

"Accessing Role Based Access Control" on page 26
You can access Role Based Access Control (RBAC) from the IBM Systems Director Console for AIX console.

Related information:

RBAC roles

Administering enhanced RBAC

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 character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

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. 903
11501 Burnet Road
Austin, TX 78758-3400
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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as the customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Index

Printed in USA