IBM Security Access Manager for Web
Version 7.0

Troubleshooting Guide

GC27-2717-01

IBM Security Access Manager for Web
Version 7.0

Troubleshooting Guide

GC27-2717-01

Note

Before using this information and the product it supports, read the information in "Notices" on page 197.

Edition notice

Note: This edition applies to version 7, release 0, modification 0 of IBM Security Access Manager (product number 5724-C87) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

About this publication

IBM Security Access Manager for Web, formerly called IBM Tivoli Access Manager for e-business, is a user authentication, authorization, and web single sign-on solution for enforcing security policies over a wide range of web and application resources.

The *IBM Security Access Manager for Web: Troubleshooting Guide*, provides a comprehensive set of procedures and reference information for troubleshooting Security Access Manager.

Intended audience

This guide is for system administrators and field support personnel responsible for troubleshooting a Security Access Manager environment.

Readers should be familiar with the following:

- PC and UNIX operating systems
- Database architecture and concepts
- Security management
- Internet protocols, including HTTP, TCP/IP, File Transfer Protocol (FTP), and Telnet
- Lightweight Directory Access Protocol (LDAP) and directory services
- A supported user registry
- Authentication and authorization
- Secure Sockets Layer (SSL) protocol, key exchange (public and private), digital signatures, cryptographic algorithms, and certificate authorities.

Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security Access Manager for Web library."
- Links to "Online publications" on page xiii.
- A link to the "IBM Terminology website" on page xiii.

IBM Security Access Manager for Web library

The following documents are in the IBM Security Access Manager for Web library:

- *IBM Security Access Manager for Web Quick Start Guide*, GI11-9333-01

  Provides steps that summarize major installation and configuration tasks.
- *IBM Security Web Gateway Appliance Quick Start Guide* – Hardware Offering

  Guides users through the process of connecting and completing the initial configuration of the WebSEAL Hardware Appliance, SC22-5434-00
- *IBM Security Web Gateway Appliance Quick Start Guide* – Virtual Offering

  Guides users through the process of connecting and completing the initial configuration of the WebSEAL Virtual Appliance.
- *IBM Security Access Manager for Web Installation Guide*, GC23-6502-02

  Explains how to install and configure Security Access Manager.

- *IBM Security Access Manager for Web Upgrade Guide*, SC23-6503-02

  Provides information for users to upgrade from version 6.0, or 6.1.x to version 7.0.
- *IBM Security Access Manager for Web Administration Guide*, SC23-6504-02

  Describes the concepts and procedures for using Security Access Manager. Provides instructions for performing tasks from the Web Portal Manager interface and by using the **pdadmin** utility.
- *IBM Security Access Manager for Web WebSEAL Administration Guide*, SC23-6505-02

  Provides background material, administrative procedures, and reference information for using WebSEAL to manage the resources of your secure Web domain.
- *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*, SC23-6507-02

  Provides procedures and reference information for securing your Web domain by using a Web server plug-in.
- *IBM Security Access Manager for Web Shared Session Management Administration Guide*, SC23-6509-02

  Provides administrative considerations and operational instructions for the session management server.
- *IBM Security Access Manager for Web Shared Session Management Deployment Guide*, SC22-5431-00

  Provides deployment considerations for the session management server.
- *IBM Security Web Gateway Appliance Administration Guide*, SC22-5432-00

  Provides administrative procedures and technical reference information for the WebSEAL Appliance.
- *IBM Security Web Gateway Appliance Configuration Guide for Web Reverse Proxy*, SC22-5433-00

  Provides configuration procedures and technical reference information for the WebSEAL Appliance.
- *IBM Security Web Gateway Appliance Web Reverse Proxy Stanza Reference*, SC27-4442-00

  Provides a complete stanza reference for the IBM® Security Web Gateway Appliance Web Reverse Proxy.
- *IBM Security Access Manager for Web WebSEAL Configuration Stanza Reference*, SC27-4443-00

  Provides a complete stanza reference for WebSEAL.
- *IBM Global Security Kit: CapiCmd Users Guide*, SC22-5459-00

  Provides instructions on creating key databases, public-private key pairs, and certificate requests.
- *IBM Security Access Manager for Web Auditing Guide*, SC23-6511-02

  Provides information about configuring and managing audit events by using the native Security Access Manager approach and the Common Auditing and Reporting Service. You can also find information about installing and configuring the Common Auditing and Reporting Service. Use this service for generating and viewing operational reports.
- *IBM Security Access Manager for Web Command Reference*, SC23-6512-02

  Provides reference information about the commands, utilities, and scripts that are provided with Security Access Manager.

- *IBM Security Access Manager for Web Administration C API Developer Reference*, SC23-6513-02

  Provides reference information about using the C language implementation of the administration API to enable an application to perform Security Access Manager administration tasks.
- *IBM Security Access Manager for Web Administration Java Classes Developer Reference*, SC23-6514-02

  Provides reference information about using the Java™ language implementation of the administration API to enable an application to perform Security Access Manager administration tasks.
- *IBM Security Access Manager for Web Authorization C API Developer Reference*, SC23-6515-02

  Provides reference information about using the C language implementation of the authorization API to enable an application to use Security Access Manager security.
- *IBM Security Access Manager for Web Authorization Java Classes Developer Reference*, SC23-6516-02

  Provides reference information about using the Java language implementation of the authorization API to enable an application to use Security Access Manager security.
- *IBM Security Access Manager for Web Web Security Developer Reference*, SC23-6517-02

  Provides programming and reference information for developing authentication modules.
- *IBM Security Access Manager for Web Error Message Reference*, GI11-8157-02

  Provides explanations and corrective actions for the messages and return code.
- *IBM Security Access Manager for Web Troubleshooting Guide*, GC27-2717-01

  Provides problem determination information.
- *IBM Security Access Manager for Web Performance Tuning Guide*, SC23-6518-02

  Provides performance tuning information for an environment that consists of Security Access Manager with the IBM Tivoli Directory Server as the user registry.

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Access Manager for Web Information Center
The http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.isam.doc_70/welcome.html site displays the information center welcome page for this product.

IBM Publications Center
The http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss site offers customized search functions to help you find all the IBM publications that you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Related publications

This section lists the IBM products that are related to and included with the Security Access Manager solution.

Note: The following middleware products are not packaged with IBM Security Web Gateway Appliance.

IBM Global Security Kit

Security Access Manager provides data encryption by using Global Security Kit (GSKit) version 8.0.x. GSKit is included on the *IBM Security Access Manager for Web Version 7.0* product image or DVD for your particular platform.

GSKit version 8 includes the command-line tool for key management, GSKCapiCmd (**`gsk8capicmd_64`**).

GSKit version 8 no longer includes the key management utility, iKeyman (**`gskikm.jar`**). iKeyman is packaged with IBM Java version 6 or later and is now a pure Java application with no dependency on the native GSKit runtime. Do not move or remove the bundled `*java*/jre/lib/gskikm.jar` library.

The *IBM Developer Kit and Runtime Environment, Java Technology Edition, Version 6 and 7, iKeyman User's Guide for version 8.0* is available on the Security Access Manager Information Center. You can also find this document directly at:

> http://download.boulder.ibm.com/ibmdl/pub/software/dw/jdk/security/60/iKeyman.8.User.Guide.pdf

Note:

GSKit version 8 includes important changes made to the implementation of Transport Layer Security required to remediate security issues.

The GSKit version 8 changes comply with the Internet Engineering Task Force (IETF) Request for Comments (RFC) requirements. However, it is not compatible with earlier versions of GSKit. Any component that communicates with Security Access Manager that uses GSKit must be upgraded to use GSKit version 7.0.4.42, or 8.0.14.26 or later. Otherwise, communication problems might occur.

IBM Tivoli Directory Server

IBM Tivoli Directory Server version 6.3 FP17 (6.3.0.17-ISS-ITDS-FP0017) is included on the *IBM Security Access Manager for Web Version 7.0* product image or DVD for your particular platform.

You can find more information about Tivoli Directory Server at:

> http://www.ibm.com/software/tivoli/products/directory-server/

IBM Tivoli Directory Integrator

IBM Tivoli Directory Integrator version 7.1.1 is included on the *IBM Tivoli Directory Integrator Identity Edition V 7.1.1 for Multiplatform* product image or DVD for your particular platform.

You can find more information about IBM Tivoli Directory Integrator at:

http://www.ibm.com/software/tivoli/products/directory-integrator/

IBM DB2 Universal Database™

IBM DB2 Universal Database Enterprise Server Edition, version 9.7 FP4 is provided on the *IBM Security Access Manager for Web Version 7.0* product image or DVD for your particular platform. You can install DB2® with the Tivoli Directory Server software, or as a stand-alone product. DB2 is required when you use Tivoli Directory Server or z/OS® LDAP servers as the user registry for Security Access Manager. For z/OS LDAP servers, you must separately purchase DB2.

You can find more information about DB2 at:

http://www.ibm.com/software/data/db2

IBM WebSphere® products

The installation packages for WebSphere Application Server Network Deployment, version 8.0, and WebSphere eXtreme Scale, version 8.5.0.1, are included with Security Access Manager version 7.0. WebSphere eXtreme Scale is required only when you use the Session Management Server (SMS) component.

WebSphere Application Server enables the support of the following applications:

- Web Portal Manager interface, which administers Security Access Manager.
- Web Administration Tool, which administers Tivoli Directory Server.
- Common Auditing and Reporting Service, which processes and reports on audit events.
- Session Management Server, which manages shared session in a Web security server environment.
- Attribute Retrieval Service.

You can find more information about WebSphere Application Server at:

http://www.ibm.com/software/webservers/appserv/was/library/

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Visit the IBM Accessibility Center for more information about IBM's commitment to accessibility.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

The *IBM Security Access Manager for Web Troubleshooting Guide* provides details about:

- What information to collect before you contact IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The **Community and Support** tab on the product information center can provide more support resources.

Part 1. Introduction to troubleshooting

Chapter 1. Getting started with troubleshooting

Problem determination, or troubleshooting, is a process of determining why a product is not functioning in the expected manner.

This guide provides information to help you identify and resolve problems with Security Access Manager and its prerequisite products.

How do I troubleshoot?

Follow these shortcuts to get started:

- Chapter 3, "Troubleshooting installation and uninstallation," on page 15
- Chapter 4, "Troubleshooting configuration," on page 27
- Chapter 7, "Validating and maintaining policy databases," on page 45
- "Basic SPNEGO troubleshooting" on page 119

Troubleshooting new features in version 7.0

See the following sections to troubleshoot new features in IBM Security Access Manager for Web, version 7.0:

- Chapter 21, "Risk-Based Access External Authorization Service plug-in," on page 151
- "Windows Launchpad installation recovery" on page 21
- "Windows Launchpad configuration recovery" on page 32
- Chapter 22, "Troubleshooting certificate compliance issues," on page 153
- Chapter 25, "Collecting data with IBM Support Assistant," on page 167

Troubleshooting Common Audit Service

For troubleshooting information about the Common Audit Service, see the *IBM Security Access Manager for Web Audit Guide*.

Troubleshooting Web Gateway Appliance

For troubleshooting the virtual or hardware IBM Security Web Gateway Appliance, see the *IBM Security Web Gateway Appliance Administration Guide*.

Avoiding potential problems

If you plan the deployment of your software, you can often prevent problems before they happen.

Before you install or upgrade Security Access Manager, review the *IBM Security Access Manager for Web Release Notes*®. This document contains the following information:

- Supported operating system levels
- Prerequisite software requirements
- Required software patches
- Minimum memory requirements

- Disk space requirements
- Upgrade considerations
- Known problems, limitations, and recovery procedures
- Customer support contact information

After you install Security Access Manager, ensure that you have a comprehensive backup and system recovery strategy in place. When you create your backup and recovery strategy, include the following information to help avoid the possibility of running into problems:

- Perform regular periodic backups of Security Access Manager by using the **pdbackup** command.
- Periodically back up the user registry by following the instructions that are provided by the user registry vendor.
- Maintain information about your environment, including system topology, IP addresses, host names, and which components are installed on each system.
- Maintain updated information that describes the key system resources that are being managed by Security Access Manager and the security policies that are being applied to them by Security Access Manager.
- Periodically check that all systems that are running Security Access Manager have sufficient disk space for runtime and problem determination data. As your security policy grows, and the number of users, groups, and protected objects increase, the space requirements for the policy databases, message logs, trace logs, and any auditing information can increase as well.
- Regularly check for the availability of fix packs and install them as they become available. Information about fix packs and other useful information can be found on the IBM Software Support site at the following Web address:

  http://www.ibm.com/support/entry/portal/overview/software/other_software/ibm_security_access_manager_for_web

Chapter 2. Diagnosing problems with diagnostic tools

When problems do occur, use the information about diagnostic tools to learn how to identify and possibly resolve them.

If you are unable to correct the problem, gather the relevant diagnostic information and then contact IBM Support to get further assistance.

IBM Security Access Manager contains several tools in addition to the operating system tools to help you determine the source of problems you encounter:

- "Messages"
- "Logs" on page 6
- "Creating directories with Tivoli Common Directory" on page 7
- "Viewing log files with the XML Log Viewer" on page 9
- "Using the Messages Guide to resolve errors" on page 10

Messages

All messages issued by Security Access Manager adhere to a Message Standard. The Message Standard specifies a standard format for all messages issued by this product. The standard, based on the IBM Message Standard, is intended to provide a consistent and meaningful way for identifying messages across the entire IBM product set. Messages issued by Security Access Manager, along with detailed explanations and suggested actions, can be found in the *IBM Security Access Manager for Web: Error Message Reference*.

Message types

Security Access Manager is written in both the C and Java programming languages, with different types of messages for each programming language.

Applications that use the Security Access Manager APIs are also written in these programming languages.

Security Access Manager produces the following types of messages:

Runtime messages
Messages that are generated by applications, commands, and utilities that use the Security Access Manager Runtime component, and messages that are generated from the C language-based Security Access Manager components, such as WebSEAL. These messages are written to the runtime message logs based on their severity levels.

IBM Security Access Manager Runtime for Java messages
Messages that are generated by applications, commands, and utilities that use the IBM Security Access Manager Runtime for Java component, and messages that are generated from the Java language-based Security Access Manager components. These messages are written to the IBM Security Access Manager Runtime for Java message logs. These messages tend to provide exception and stack trace information from the JRE.

Server messages
Messages that are generated by the Security Access Manager daemons and

servers. Messages from the policy server, authorization server, WebSEAL servers, and policy proxy server are written to the server message logs.

Installation and configuration messages

Messages that are generated during installation and by the configuration utilities. Some of these messages follow the message standard and have an associated ID. These messages are written to the log files described in Chapter 3, “Troubleshooting installation and uninstallation,” on page 15 during installation.

WebSEAL HTTP messages

WebSEAL provides the capability of logging HTTP messages. This message log capability is described in the *IBM Security Access Manager for Web Auditing Guide*.

Message format

A message consists of a message identifier (ID) and message text and an error code. The error code is a unique 32-bit value. The error code is either a decimal or hexadecimal number and indicates that an operation was not successful.

All messages that follow the message standard are listed in the *IBM Security Access Manager for Web Error Message Reference*. Each of these messages has a detailed explanation and suggested actions.

Message identifiers

A message ID consists of 10 alphanumeric characters that uniquely identify the message. The message ID consists of the following parts:

- A 3-character product identifier (see Table 1 for the list of identifiers that are used by Security Access Manager)
- A 2-character component or subsystem identifier
- A 4-digit serial or message number
- A 1-character type code that indicated one of the following message severities:

  W Warning

  E Error

  I Information

Table 1. Product identifiers that are used by Security Access Manager

Product identifier	Security Access Manager component
HPD	Security Access Manager servers
DPW	Security Access Manager WebSEAL
AMZ	Security Access Manager Plug-in for Web Servers
CTG	Security Access Manager Session Management Server

Logs

Use log files to retrieve information about a problem in your environment.

Enable the collection of detailed log and trace information to troubleshoot problems. You can collect and review standard informational log messages or detailed trace messages to help determine the root cause of a problem.

For more information about using logs, see Part 3, “Using log files for troubleshooting,” on page 47.

Creating directories with Tivoli Common Directory

Security Access Manager supports the use of Tivoli Common Directory logging for a consistent location of serviceability information across IBM Tivoli® and Security products.

Security Access Manager does not enable logging for the Tivoli Common Directory unless you select this option during the installation of the product.

If you select Tivoli Common Directory logging, the installation process determines the log location in the following way:

- If Tivoli Common Directory is already in use on the system, the existing default location for log files is used.
- If Tivoli Common Directory is not already in use, the directory that is specified during installation becomes the Tivoli Common Directory where log files for Security Access Manager and other IBM products are stored.

When enabled, all message log files are in the Tivoli Common Directory location. Other types of application log files continue to be in their installation directories.

Note: After you define the Tivoli Common Directory location, you cannot change it.

Location of the Tivoli Common Directory properties file

If any product on the system uses Tivoli Common Directory, the parent directory is defined in the `log.properties` file. Depending on your operating system, the `log.properties` file is in one of the following default locations:

AIX, Linux, and Solaris operating systems

```
/etc/ibm/tivoli/common/cfg/log.properties
```

Windows operating systems

```
c:\program files\ibm\tivoli\common\cfg\log.properties
```

On a AIX, Linux, or Solaris operating system, this file must have the `664` permission and be owned by group `tivoli`.

Common directories used by Security Access Manager

During configuration of the Security Access Manager C runtime or Java runtime, the default log location displays. If Security Access Manager is the first IBM product on this system to use Tivoli Common Directory, you can change this location. If another product already defined this location, this location is displayed and cannot change.

After you enabled Tivoli Common Directory, Security Access Manager uses the `/logs` subdirectory to store message and trace logs.

Security Access Manager does not use the `/ffdc` or `/scripts` subdirectories.

The logs files can be found at the following default location:

`*common_directory*/*xxx*/logs/`

where:

common_directory
Represents the parent directory for serviceability data. This directory is defined by the first IBM product that uses Tivoli Common Directory.

The default values, if Security Access Manager is the first IBM product, is one of the following platform-specific directories:

AIX, Linux, and Solaris operating systems
`/var/ibm/tivoli/common`

Windows operating systems
`c:\program files\ibm\tivoli\common\`

Note: On a AIX, Linux, or Solaris operating system, this directory must have the `771` permissions and be owned by the `tivoli` group.

xxx Represents the three-letter identifier to use for the product-specific message log files. Security Access Manager uses the following identifiers:

HPD The identifier for Security Access Manager

DPW The identifier for Security Access Manager WebSEAL

AMZ The identifier for Security Access Manager Plug-in for Web Servers

CTG The identifier for Security Access Manager Session Management Server

logs The subdirectory that is used for Security Access Manager message and trace log files. Only one subdirectory, `/logs`, is defined for these log files.

Configuration settings used by Security Access Manager

When configured for Tivoli Common Directory, the `tivoli_common_dir` stanza entry of the `pd.conf` configuration file would be similar to one of the following entries:

AIX, Linux, and Solaris operating systems

```
[pdrte]
tivoli_common_dir = /var/ibm/tivoli/common/
```

Windows operating systems

```
[pdrte]
tivoli_common_dir = c:\Program Files\IBM\Tivoli\common\
```

When configured for Tivoli Common Directory, the `log-file` stanza entry of the server-specific configuration file contains the fully qualified names of the log files. For example, when configured for Tivoli Common Directory, the `log_file` stanza entry for the authorization server log files would be similar to one of the following entries:

AIX, Linux, and Solaris operating systems

```
[ivacld]
log-file = /var/ibm/tivoli/common/HPD/logs/msg__pdacld_utf8.log
```

Windows operating systems

```
[ivacld]
log-file = c:\Program Files\IBM\Tivoli\common\HPD\logs
\msg__pdacld_utf8.log
```

Viewing log files with the XML Log Viewer

The XML Log Viewer is a standard tool available with many IBM products. The viewer provides an HTML interface for log files that are created in the standard XML log format.

The C-based components of Security Access Manager support message and trace information in this standard XML format. For these components, you can use the XML Log viewer to view and filter messages and traces for any of the following categories:

- Time
- Severity
- Message ID
- Component
- Log text (the message text for messages and traces maps to this element)
- Server (host name)
- Product ID
- Product instance

The `XMLFILE`, `XMLSTDERR`, and `XMLSTDOUT` format in the routing file are used to produce XML message logs and XML trace logs.

Information that is produced by different products can be analyzed and converted into ASCII or HTML that use the XML Log Viewer.

The XML Log Viewer is not installed during a Security Access Manager installation. You must separately install the XML Log Viewer.

Note: Java language-based Security Access Manager components and applications cannot produce messages or traces in the XML log format.

Installing the XML Log Viewer

About this task

Security Access Manager includes the XML Log Viewer as part of the product offering. The XML Log Viewer is provided as a Java archive file called `setup.jar`.

Because the XML Log Viewer is a Java application, you must install a JRE before you install and run the viewer. You can use the same JRE that is used by Security Access Manager for the XML Log Viewer. If a different JRE is used, that JRE must be at version 1.2.2 or later.

Procedure

1. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage®.
2. From a command prompt, go to the `/`*`package_path`*`/`*`operating_system`*`/xmllogviewer` directory where *package_path* is the mount point for your DVD or file location, and *operating_system* specifies the directory for your operating system.
3. Enter the following command:

   ```
   java -cp setup.jar run
   ```

4. Follow the prompts panels to select a location for the XML Log Viewer and install the viewer.
5. After the installation program completes, you can add the XML Log Viewer directory to the search path.
6. On AIX, Linux, and Solaris operating systems, you might need to explicitly set run permissions on the `viewer.sh` file:

   ```
   chmod +x viewer.sh
   ```

Viewing logs with the XML Log Viewer

Information about using the XML Log Viewer, including how to filter the output or uninstall it, is in the `readme.html` file. The `readme.html` file is provided in the `/xmllogviewer` directory.

To run the XML Log Viewer, use the **`viewer`** script and specify the name of one or more XML files. Output is directed to `STDOUT` in either HTML or text format.

The following examples describe how to use the viewer with Security Access Manager:

- To create an HTML file that contains all of the messages from the Security Access Manager policy and authorization servers and sorts them chronologically, enter the following command:

  ```
  viewer msg__pdmgrd.xml msg__pdacld.xml > msg_19Oct2012_report.html
  ```

- To display messages from the Security Access Manager policy server in text format, run the following command:

  ```
  viewer -s text msg__pdmgrd.xml
  ```

Using the Messages Guide to resolve errors

The *IBM Security Access Manager for Web Error Message Reference* contains a list of messages in the IBM Security Access Manager logs, graphical user interfaces, and the command line.

Use the unique message ID associated with a message to locate detailed explanations and suggested operator responses in the guide.

For example, if you see the following error message in the message log:

```
HPDBA0200E The server Distinguished Name (DN) specified in the configuration
file does not match the DN in the certificate received from the server.
```

Search for `HPDBA0200E` in the guide for information about why the error occurred and how to resolve it. For example, the previous error message has the following information in the *IBM Security Access Manager for Web Error Message Reference*:

```
HPDBA0200E The server Distinguished Name (DN) specified in the configuration
file does not match the DN in the certificate received from the server.

Explanation: The DN specified in the "master-dn" attribute of the
"manager" stanza of the configuration file does not match the DN
in the certificate received from the server.

Action: Verify that the server's hostname, port number, and
Distinguished Name are correct and that the correct server
certificate is being used.

Name: mts_server_auth_failed

Number: 0x106520c8 (275062984)
```

```
Severity: Fatal

Component: bas / bas_s_mts
```

DB2, WebSphere Application Server, and other software program error log messages are not in the *IBM Security Access Manager for Web Error Message Reference*.

Part 2. Deployment

Chapter 3. Troubleshooting installation and uninstallation

This chapter describes problems that you might encounter while you install or uninstall Security Access Manager and provides information about how to determine the origin of the problem. After you determine what caused the problem, you can use the information that is provided to resolve this problem.

Before you list some of the common Security Access Manager problems that you might encounter during installation or uninstallation, it is worthwhile to mention that the cause of most common installation and uninstallation problems is one of the following failures:

- Failure to install the following prerequisite and corequisite software:
  - Operating system software
  - Operating system patches
  - Prerequisite software products
  - Prerequisite software product level and patches
- Failure to install all of the required software components for any type of Security Access Manager system
- Failure to install or configure any of the prerequisite and corequisite items properly
- Failure to adhere to all hardware prerequisites such as disk space and memory requirements

Mixed level environment

You are not required to have all Security Access Manager components in your secure domain at a 7.0 level. However, if you upgrade to any Security Access Manager 7.0 component on one system, then all components on that system must be at the 7.0 level.

For best results, keep all Security Access Manager components at the same level, including fix pack level.

Installation directories

The installation directory for each of the following Security Access Manager components is specified during installation:

- Security Access Manager base components
- Session Management Server components
- WebSEAL
- Plug-in for Web Servers

Security Access Manager

When you install Security Access Manager, one or more of the following components can be installed:

- Security Access Manager Policy Server
- Security Access Manager Policy Proxy Server
- Security Access Manager Authorization Server
- Security Access Manager Runtime

- Security Access Manager Runtime for Java
- Security Access Manager Web Portal Manager
- Security Access Manager Application Development Kit (ADK)

The default installation location for Security Access Manager files is platform-dependent:

Windows operating systems
```
C:\Program Files\Tivoli\Policy Director
```

AIX, Linux, and Solaris operating systems
```
/opt/PolicyDirector
```

During the installation of Security Access Manager, the PD_HOME environment variable is set to the installation directory on Windows operating systems. No environment variable is set on AIX, Linux, and Solaris operating systems. After installation, ensure that only trusted users and groups have access to this directory and its subdirectories.

Session Management Server

The default installation location for the Session Management Server is platform-dependent:

Windows operating systems
```
C:\Program Files\Tivoli\PDSMS
```

AIX, Linux, and Solaris operating systems
```
/opt/pdsms
```

After installation, ensure that only trusted users and groups have access to this directory and its subdirectories.

WebSEAL

The default installation location for WebSEAL files is platform-dependent:

Windows operating systems
```
C:\Program Files\Tivoli\PDWeb
```

AIX, Linux, and Solaris operating systems
```
/opt/pdweb
```

After installation, ensure that only trusted users and groups have access to this directory and its subdirectories.

Plug-in for Web Servers

The default installation location for Plug-in for Web Servers files is platform-dependent:

Windows operating systems
```
C:\Program Files\Tivoli\PDWebPI
```

AIX, Linux, and Solaris operating systems
```
/opt/pdwebpi
```

After installation, ensure that only trusted users and groups have access to this directory and its subdirectories.

Common installation problems

This section describes problems that you might encounter while you install Security Access Manager and provides information about how to manage the problem.

Insufficient disk space

Installation and use of Security Access Manager requires adequate disk space.

If you do not have sufficient disk space during installation, an error message stops the installation and alerts you that there is not enough space.

If you encounter this error message, see the *IBM Security Access Manager for Web Release Notes* for detailed information about required disk space. Clear adequate space on the disk, or select a root directory on a partition with more space, and run the installation process again.

Without adequate disk space, Security Access Manager cannot install or function as expected.

Windows disk space

On Windows operating systems, concerns for adequate disk space include the following directories:

- The Security Access Manager installation directory
- The Security Access Manager WebSEAL installation directory
- The Security Access Manager Plug-in for Web Servers installation directory

AIX, Linux, and Solaris disk space

On AIX, Linux, and Solaris operating systems, concerns for adequate disk space include the `/opt` and the `/var` directories.

Use the **`df`** command with the **–k** option to display the free disk space for each file system. The **–k** option causes the disk space to be displayed in kilobytes.

Installation of the license fails on Linux x86_64 systems

If the installation of the license fails when you use the isamLicense script on a 64-bit Linux system, ensure that the following 32-bit libraries are installed from the *i686.rpm packages:

```
ld-linux.so.2
libstdc++.so.6
```

Error displays after you successfully install WebSphere Application Server with an automated script

A previous installation failure might cause an error message after you successfully install WebSphere Application Server with an automated script on AIX®, Linux, and Solaris.

The `install_was.sh` script can perform an unattended WebSphere Application Server installation. Before you run the script, you must add environment details to the `WASInstall_`*`platform`*`_ppc.xml` file, where *`platform`* is either `solaris`, `aix_ppc` or `linux_x86`.

If an incorrect or nonexistent repository location is listed in the .xml file, the installation script fails. Following the correction of the repository location in the .xml file, installation is successful. However, the system displays traces of the previous error.

The error does not affect the successful installation.

The following text is an example of the error from this situation:

```
for example:- repository location = /opt/images/WebS1phere

[root@paix287 /opt/images/installer]# ./install_was.sh
Installing Installation Manager...
Installed com.ibm.cic.agent_1.5.1000.20111128_0824 to the
/opt/IBM/InstallationManager/eclipse directory.
Installing WebSphere...
ERROR: The com.ibm.websphere.ND.v80 8.0.0.20110503_0200 package
specified in the /opt/images/installer/./WASInstall_aix_ppc.xml
file cannot be found.
CRIMA1002W WARNING: The following repositories are not connected:
-/opt/images/WebS1phere
.
Error> Failed to install WebSphere
```

Now, edit the WASInstall_aix_ppc.xml file with the correct repository location variable and re-execute the install_was.sh script. Observe that the installation succeeds with following message which contains the traces of the previous error message:

```
[root@paix287 /opt/images/installer]# ./install_was.sh
Installation Manager already installed
Installing WebSphere...
Installed com.ibm.websphere.ND.v80_8.0.0.20110503_0200 to the
/opt/IBM/WebSphere/AppServer directory.
CRIMA1002W WARNING: The following repositories are not connected:
-/opt/images/WebS1phere
```

Multiple network interfaces

Some operating systems can be configured with multiple network interfaces. When there are multiple network interface aliases, there might be more than one route to the policy server. In these situations, the operating system might choose a different route for each communication.

When the operating system routes each communication differently, the policy server might not be able to definitively identify the client. When the policy server cannot identify the client, the communication between the client and the policy server might fail with a message similar to the following error:

```
The server lost the client authentication, because of session expiration.
```

This communication failure can happen between the following components:

- An authorization API server in local mode with the policy server
- An authorization API server in remote mode with the policy server
- An authorization API server in remote mode with the authorization server
- The **pdadmin** utility with the policy server
- An administration API with the policy server
- The policy server with any authorization API server, such as the authorization server or WebSEAL
- The **svrsslcfg** utility with the policy server

To prevent this problem, use one of the following mechanisms:

- Change the operating system routing table so that the same route is always selected. For example, if there are three routes, two of these routes must be downgraded so that one route is always selected. For more information about route commands and metrics that are used in routing tables, see your operating system documentation.
- Set the PD_FIXED_CLIENT_IP environment variable to the IP address of a valid network interface on the operating system. This value must be in the IP version 4 (IPv4) or IP version 6 (IPv6) format. The PD_FIXED_CLIENT_IP environment variable can be set on all the supported operating systems. See RFC 2460 at the following website to determine what constitutes a valid representation of an IPv6 address:

  http://www.faqs.org/rfcs/rfc2460.html

Java error on Windows during Launchpad or script installation

On some Windows 2008 systems, the IBM Java Runtime fails to install during a silent installation. Security Access Manager component installations on Windows require IBM Java Runtime to complete.

If IBM Java Runtime failed to install during a Launchpad or script installation, Security Access Manager component installations fail with the following error message:

```
Unable to find Java executable file (javaw.exe or java.exe).
Install the IBM SDK for Java or make sure a Java version 1.4 or
higher is accessible from the current PATH.
```

To continue with the installation, ensure that IBM Java is available in the environment. Install IBM Java manually by completing the procedure for installing IBM Java Runtime on Windows in the *IBM Security Access Manager for Web Installation Guide*.

GSKit installation failure on Windows

During installation on Windows, GSKit can fail to install if the user ID is not correct and UAC settings are set to notify you when a program tries to make changes to the computer.

When this issue occurs from Launchpad, the `ISAMGskitInstall.log` shows an error such as the following error:

```
C:\build\bin\../windows/GSKit/gsk8ssl64.exe /s /v/quiet
1625
```

This error can also be seen when you run the GSKit installation from the `install_isam.bat` script.

This issue can be caused by using the user ID "administrator" instead of "Administrator."

To resolve this issue, run the Launchpad installation with the user ID of "Administrator" with a capital "A."

Alternatively, you can do one of the following options:

- Run the `gsk8ssl64.exe` installer manually.

- Disable UAC before installing GSKit. This method can require a system restart.

Installation stalls on Windows

When you install components on Windows, the installation program might appear stalled on the Welcome page.

After the Welcome page is displayed, the license is displayed. Check all open windows. The license page is in a separate window that might be hidden behind the Welcome page window. Minimize or move the Welcome page window, read and accept the license, and then return to the installation window to continue the installation.

"Stop the script" message on Windows

When you install components on Windows using Launchpad, a message might be displayed that asks if you want to stop the running script.

The message indicates that the running script is causing the web browser to run slowly. Answer `No` to this message to continue installing IBM Security Access Manager.

Installation logs

When you install and configure Security Access Manager components, log files are created. If you natively install and configure, there are separate log files for installation and configuration.

Command line installation log files

Security Access Manager native installation log files contain the completion status for the installation tasks performed. If the components are installed with the installation programs that are provided with the operating system, these are the only installation log files that are created. These native installation log files contain messages that are generated during the installation of the product.

The names and locations of the native installation log files are shown in Table 2.

Table 2. Native installation log files

Operating system	Command line installation log file
AIX	`/smit.log`
Linux	`/tmp/install.log` or `/var/tmp/install.log`
Solaris	See the contents of the `pkginfo` files that are stored in the subdirectories of the `/var/sadm/pkg` directory.
Windows	`%PD_HOME%\log\msg__PDInstall.log` **Note:** There are two underscore characters (_) in the file name. WebSEAL has its own command-line installation log: `%PDWEB%\PDWeb_install.log`

Launchpad Recovery on Windows

This section contains recovery information for Launchpad installation and configuration issues on Windows systems.

IBM Security Access Manager for Web version 7.0 uses a graphical user interface that is called Launchpad for installations on Windows systems. Launchpad provides step-by-step installation and initial configuration.

This section contains recovery information for issues that are encountered when you use the Launchpad for installation or configuration.

Windows Launchpad installation recovery

Installation failures with Launchpad on Windows require understanding and correction of the root cause. After correction, complete the installation with the Launchpad interface.

Steps for troubleshooting failed installation

To recover from a failed Launchpad installation on Windows, do the following steps:

1. Make note of the failed component name, installation log file name, and any return error code that is shown by Launchpad.
2. Exit Launchpad.
3. Open the installation log file for the failed component. Search the log for the cause of the error.
4. Correct any problems that are listed in the return error code or installation log file.
5. Restart and resume Launchpad installation and configuration.

Windows Launchpad installation log files

The following table lists the installation log file name and location for each component.

If you encounter an issue during Launchpad installation, locate the log file and examine the contents for information about the cause of the error.

Table 3. Windows Launchpad installation log files

Component	Installation log file and default location

Tivoli Directory Server	`ldapinst.log`
	The default destination directory is:
	`C:\Program Files\IBM\LDAP\V6.3\var`
	If the default installation directory was not created before the installation failed, the `ldapinst.log` file might be in a temporary directory. To find it, search for "`ldapinst.log`".

Security Access Manager components	`msg__PDinstall.log`
	This log is in the following directory:
	`C:\Program Files\Tivoli\Policy Director\log\`

Security Access Manager Security Utilities	`msg__TivSecUtlInstall.log`
	This log is in the following directory:
	`C:\Program Files\Tivoli\Policy Director\log\`

Table 3. Windows Launchpad installation log files (continued)

Component	Installation log file and default location
Session Management Server and WebSphere Application Server	Check the Installation Manager installation logs: • IMInstall.log • IMInstallLog.xml These logs are in the *USERPROFILE* directory. Typically, the path is C:\Users\Administrator\. Additional installation information is in the LaunchIMforWAS.log file.
Global Secure ToolKit (GSKit)	ISAMGskitInstall.log This log is in the following directory: %USERPROFILE%\ISAMGskitInstall.log
Security Access Manager Language Pack	ISAMLangPackInstall.log This log is in the following directory: %USERPROFILE%\ISAMLangPackInstall.log

Opening a log file in Launchpad

You can view Launchpad log data from within Launchpad.

To view a log of the Launchpad process:
With Launchpad open, hold down the Ctrl key, and left-click over the **IBM Security Access Manager for Web** banner in the top panel. A log section opens at the bottom panel. You can print or save the log. By default, only serious errors are collected.

To collect detailed Launchpad debug information:
Open a Windows command prompt and issue the following command:

```
set LaunchPadLogFilter=FSEWTC
CD to the ISAM install image
Run launchpad64.exe
```

A log section opens at the bottom panel in Launchpad. You can print, save, or copy and paste the log information to a file.

Additional Tivoli Directory Server installation information

For complete information about Tivoli Directory Server installation issues, see the Tivoli Directory Server documentation.

Additional Security Access Manager component installation information

The following base components capture installation information in the msg__PDinstall.log file:

- Security Access Manager policy server
- Security Access Manager runtime
- Security Access Manager runtime for Java
- Security Access Manager license
- Security Access Manager Application Development Kit
- Security Access Manager authorization server
- Security Access Manager policy proxy server

- Security Access Manager Web Portal Manager

Additional Security Access Manager logs with installation information are in the *PD_HOME*\log subdirectory.

Additional Session Management Server installation information

Session Management Server uses Installation Manager for installation.

The LaunchIMforWAS.log file uses the following return codes:

- 1 = IBM Installation Manager is not installed, or the program was not able to read the registry.
- 2 = Problem starting Installation Manager.
- 3 = IBM WebSphere Application Server is not installed, or the program was not able to read the registry.

Additional WebSphere Application Server installation information

WebSphere Application Server uses Installation Manager for installation.

The LaunchIMforWAS.log file uses the following return codes:

- 1 = IBM Installation Manager is not installed, or the program was not able to read the registry.
- 2 = Problem starting Installation Manager.
- 3 = IBM WebSphere Application Server is not installed, or the program was not able to read the registry.

For complete information about WebSphere Application Server installation issues, see the WebSphere Application Server documentation.

Common uninstallation problems

This section describes problems that you might encounter while you uninstalling Security Access Manager and provides information about how to manage the problem.

Language pack uninstallation leaves registry entries

The language pack uninstallation can leave behind registry entries in the Windows registry. After you uninstall a language pack, review the Windows registry entries under the HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\ directory and remove any entry for a language pack you have removed.

Registry entries

This section lists the registry entries that are created when you install Security Access Manager with Launchpad on Windows.

Attention: Do not modify any registry entry unless directed by IBM Support.

Registry entries for Security Access Manager are stored under the following directory:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\
```

If part of a registry key is missing or a key is not removed during uninstallation, there can be problems with installing or upgrading the product. See "Launchpad Recovery on Windows" on page 20.

Registry entries

Security Access Manager creates the following registry entries:

Access Manager Plug-in for Microsoft Internet Information Services:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Access Manager Plug-in for
Microsoft Internet Information Services
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Access Manager Plug-in for
Microsoft Internet Information\7.0.0
      Path  install_location
      Version 7.0.0.0
```

Access Manager Plug-in for Web Servers:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Access Manager Plug-in for
Web Servers
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Access Manager Plug-in for
Web Servers\7.0.0
      Path  install_location
      Version 7.0.0.0
```

Access Manager Session Management Command Line:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Access Manager Session Management
Command Line
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Access Manager Session Management
Command Line\7.0.0
      Configured   Yes/No
```

Access Manager Session Management Server:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Access Manager Session
Management Server
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
```

Access Manager Web Security Runtime:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Access Manager Web
Security Runtime
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Access Manager Web
Security Runtime\7.0.0
      Path  install_location
      Version 7.0.0.0
```

Access Manager WebSEAL:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Access Manager WebSEAL
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Access Manager WebSEAL\7.0.0
      Configured yes/no
      Path  install_location
      Version 7.0.0.0
```

Policy Director Web Portal Manager:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director Web
Portal Manager
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director Web
Portal Manager\7.0.0
      Path  install_location
      Version 7.0.0.0
```

License

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director License
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director License\7.0.0
      Path  install_location
      Version 7.0.0.0
```

Policy Server:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director Management
Server
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director Management
Server\7.0.0
      Configured   Yes/No
      Path  install_location
      Version 7.0.0.0
```

Runtime:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director Runtime
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director Runtime\7.0.0
      Configured   Yes/No
      Path  install_location
      Version 7.0.0.0
```

Application Development Kit:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director
Authorization Toolkit
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director
Authorization Toolkit\7.0.0
      Path  install_location
      Version 7.0.0.0
```

Java Runtime:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director
Java Runtime
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director
Java Runtime\7.0.0
      Path  install_location
      Version 7.0.0.0
```

Policy Proxy Server:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Access Manager Policy
Proxy Server
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Proxy
Server\7.0.0
      Configured   Yes/No
      Path  install_location
      Version 7.0.0.0
```

Authorization Server:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director
Authorization Server
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Policy Director
Authorization Server\7.0.0
      Configured   Yes/No
      Instance_name-Configured   Yes/no
     Instances   instance_name
      Path  install_location
      Version 7.0.0.0
```

Security Utilities:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Tivoli
Security Utilities
     MajorVersion 7.0
     Path  install_location
     Version 7.0.0.0
```

Chapter 4. Troubleshooting configuration

Solve problems or issues related to configuration of IBM Security Access Manager for Web 7.0.

Command-line configuration log files

The Security Access Manager **pdconfig** command is used to configure Security Access Manager. Similar configuration commands are used for the Web Security components. Messages that are generated during the configuration process are stored within Security Access Manager configuration log files.

The locations of these configuration log files are listed in Table 4 for Windows operating systems and Table 5 for AIX, Linux, and Solaris operating systems.

Table 4. Default locations for command-line configuration log files on Windows

Component	Command-line configuration log file on Windows
• Policy Server • Authorization server • Policy proxy server • C runtime	`%PD_HOME%\log\msg__config.log`
Session management server (SMS)	*pdsms_install_dir*`\log\msg__pdsms_config.log`
Session management command-line interface	*pdsms_install_dir*`\log\msg__pdsmsclicfg.log`
Web Portal Manager	`%PD_HOME%\log\msg__amwpmcfg.log` `%PD_HOME%\log\amwpmcfg1.log`
Runtime for Java	`%PD_HOME%\log\msg__PDJrteCfg1.log`
WebSEAL	`%PD_WEB%\log\msg__amweb_config.log`
Plug-in for Web Servers	*pdwebpi_install_dir*`\log\msg__pdwpicfg.log`

Table 5. Default locations for command-line configuration log files on AIX, Linux, or Solaris

Component	Command-line configuration log file on AIX, Linux, or Solaris
• Policy Server • Authorization server • Policy proxy server • C runtime	none
Session management service (SMS)	`/var/pdsms/log/msg__pdsms_config.log`
Session management command-line interface	`/var/pdsms/log/msg__pdsmsclicfg.log`

Table 5. Default locations for command-line configuration log files on AIX, Linux, or Solaris (continued)

Component	Command-line configuration log file on AIX, Linux, or Solaris
Web Portal Manager	/var/PolicyDirector/log/msg__amwpmcfg.log /var/PolicyDirector/log/amwpmcfg1.log
Runtime for Java	/var/PolicyDirector/log/msg__PDJrteCfg1.log
WebSEAL	/var/pdweb/log/msg__amweb_config.log
Plug-in for Web Servers	/var/pdwebpi/log/msg__pdwpicfg.log

Common configuration problems

This section details common problems that you might encounter during configuration of Security Access Manager.

Post-ivbase_setup.exe configuration error

On Windows, after you install the runtime with **ivbase_setup.exe**, you must open a new window for configuration.

If you use the installation window for configuration, Security Access Manager generates the following error message:

```
ivbase_setup.exe - Unable to locate component

This application has failed to start because win32msg.dll was not
found. Re-installing the application may fix this problem.
```

To resolve this issue, complete the following steps:

1. Click **OK** to close the installation window.
2. Open a new window to continue the configuration.

Invalid LDAP management domain location DN causes error

Security Access Manager uses the LDAP client `ldapsearch` command to verify the validity of the DN location. Under the following condition, `ldapsearch` generates a success message instead of an error:

- The error that is returned from the LDAP server is related to a referral chasing error.

As a result, Security Access Manager generates the following misleading error message during configuration:

```
A policy server is already configured to this LDAP server.
A second would be used as standby server only.
```

To resolve this issue, enter a valid value for the LDAP management domain location DN during the Security Access Manager policy server configuration.

Timing out during configuration

About this task

If you encounter an error between Security Access Manager and Tivoli Directory Server while a policy proxy server is being configured, a timeout occurs at the policy proxy server. Although you might receive a message that states that the policy proxy server was configured successfully, the policy proxy server is in a partially configured state. In this case, you cannot use the **pdconfig** utility to unconfigure the policy proxy server.

To configure the policy proxy server, complete the following steps:

1. Change the value of the ssl-io-inactivity-timeout stanza entry in the pd.conf file to 0.
2. Add the following statement to the [aznapi-configuration] stanza of the pdmgrproxyd.conf file:

   ```
   aznapp-host = proxy_hostname
   ```

   where *proxy_hostname* is the host name of the policy proxy server.
3. Use the **pdconfig** utility to unconfigure the policy proxy server.
4. Increase the value of the ssl-io-inactivity-timeout stanza entry in the pd.conf file to a value that is higher than the default timeout setting.
5. Use the **pdconfig** utility to configure the policy proxy server.

Reconfigure Runtime for Java before you unconfigure Web Portal Manager

You cannot unconfigure the Web Portal Manager if you already unconfigured the Java Runtime.

The Security Access Manager Runtime for Java must be configured with the same WebSphere Application Server Runtime for Java to which the Web Portal Manager is configured.

If you unconfigured the Runtime for Java first, and then try to unconfigure the Web Portal Manager, the unconfiguration fails with the following error:

```
Enter the IBM WebSphere Application Server or Deployment Manager
installation full path [/opt/IBM/WebSphere/AppServer]:
HPDBF0030W   The JRE (/opt/IBM/WebSphere/AppServer//java/jre) is not
configured for the Security Access Manager Runtime for Java.
Enter the IBM WebSphere Application Server or Deployment Manager
```

To resolve this issue, do the following steps:

1. Reconfigure the Security Access Manager Runtime for Java. See "Setting up a Security Access Manager Runtime for Java system" in the *IBM Security Access Manager for Web Installation Guide*.

   Note: The Security Access Manager Runtime for Java must be configured with the same WebSphere Application Server Runtime for Java to which the Web Portal Manager is configured.
2. Unconfigure Web Portal Manager. See "Unconfiguring Security Access Manager components" in the *IBM Security Access Manager for Web Installation Guide*.
3. Unconfigure the Security Access Manager Runtime for Java. See "Unconfiguring Security Access Manager components" in the *IBM Security Access Manager for Web Installation Guide*.

Recovering an LDAP server

About this task

When you create a LDAP server, you need to complete the following steps:

Procedure

1. Reconfigure the policy server
2. Reconfigure IBM Security Access Manager Runtime for Java
3. Reconfigure Web Portal Manager

Results

If you do not reconfigure IBM Security Access Manager Runtime for Java before reconfiguring Web Portal Manager or any other application that relies on this runtime, the Java runtime attempts to use old certificates instead of the new certificates that were created when Web Portal Manager registered with the policy server using the `com.tivoli.pd.jcfg.SvrSslCfg` Java class.

Tivoli Directory Server configuration fails contacting LDAP server

If automated configuration scripts for IBM Tivoli Directory Server fail or if configuration fails from the Launchpad, review the logs to examine the cause of failure.

For example, the log can show the following error:

```
/opt/IBM/ldap/V6.3/bin/idsldapadd -p 389 -D cn=root -w \? -f /tmp/org_ldif
Enter password ++>
ldap_simple_bind: Can't contact LDAP server
The return code is : 81
ERROR: Problem adding the sample ldif file :/tmp/org_ldif
```

If the log shows a return code of 81 from an automated configuration scripts command such as **`IDSConfigServerSSL.sh`**, this code indicates that the LDAP server cannot be contacted. From the Launchpad, you might see the message `Error: The configuration failed with return code: 5` displayed. This error is often a timing issue.

For more information about IBM Tivoli Directory return codes, see the IBM Tivoli Directory Server documentation.

To resolve the issue, run the command that is listed in the log as failing from command line. If the error happens from Launchpad, retry the command by clicking the **Configure IBM Tivoli Directory Server** button.

Recovering from failed Tivoli Directory Server automated script configuration on Solaris

The **`idsdefinst`** script might fail to create the Tivoli Directory Server default instance and suffix if you did not properly set the kernel parameters. DB2 requires sufficient memory to complete the request.

About this task

If DB2 has insufficient memory, then an error, similar to the following error, is in the `db2cli.log` file:

```
2012-08-29-09:08:53.native retcode = -1084; state = "57019"; message = "SQL1084C
Shared memory segments cannot be allocated.  SQLSTATE=57019
```

You must clean your system before you run the **`idsdefinst`** script again.

Procedure

1. Verify the installation path of DB2. For example:

   ```
   # /usr/local/bin/db2ls

   Install Path        Level     Fix Pack    Install Date            Installer UID
   -------------------------------------------------------------------------------
   /opt/ibm/db2/V9.7   9.7.0.5      5    on Dec 12 16:25:10 2011 CST       0cd
   ```

2. Run the **db2ilist**, **db2idrop**, and **db2iset** commands from the DB2 instance directory to remove the instance. The following example uses:
   - The installation path from step 1.
   - dsrdbm01 as the instance.

   ```
   # cd /opt/ibm/db2/V9.7/instance
   # ./db2ilist
   dsrdbm01

   #./db2idrop dsrdbm01

   # ./db2iset -d dsrdbm01
   ```

3. Confirm that the instance is removed by issuing the following command:

   ```
   # ./db2ilist
   ```

4. Open the system variables file in the /etc/system directory.
5. Add the following lines to the end of the file to set the kernel parameters appropriately. The following values are suggested as starting values:

   ```
   set msgsys:msginfo_msgmax = 65535
   set msgsys:msginfo_msgmnb = 65535
   set shmsys:shminfo_shmmax = 2134020096
   ```

   For more information, see the Solaris tuning documentation.

6. Remove any Tivoli Directory Server instance by using the following command:

   ```
   idsidrop -I instance_name -r
   ```

   where *instance_name* is the name of the instance. The idsidrop file is in the /opt/IBM/ldap/V6.3/sbin directory.

7. Run the **idsdefinst** script again to define the default database instance.

Unable to configure the policy server

There are many possible causes for not being able to configure the policy server.

Unable to communicate with user registry

The policy server might be unable to communicate with the configured user registry. Examine the following possible causes:

- Verify that the user registry is not stopped.
- If you use LDAP for your user registry, verify that the LDAP client on your system can still communicate with the LDAP server. Issue an LDAP command, such as the following (entered as one line), to learn whether the LDAP server is responsive:

  ```
  ldapsearch -h ldapserver-hostname -p 389 -D "ldapadmin-DN" \
  -w ldapadmin-password -b "" -s base objectclass=*
  ```

  Note: On Windows operating systems, if this command fails, ensure that the **ldapsearch** command comes from the Tivoli Directory Server client.

- Keep in mind that the output of this command can vary depending upon which supported LDAP server you are using. The previous command assumes that the LDAP server is configured to listen on port 389. Also, verify that the user registry is still configured to communicate over the same port that is specified to Security Access Manager during the configuration of the Security Access Manager Runtime component.

Configuration fails with LDAP server

About this task

The configuration of the policy server can fail if Security Access Manager is unable to create the `secAuthority=Default` suffix for Tivoli Directory Server.

Complete the following steps before you configure Security Access Manager:

1. Create the `secAuthority=Default` suffix.
2. Stop and restart Tivoli Directory Server to enable the Tivoli Directory Server server to recognize the newly created suffix

When command-line installation is used, these steps must be completed manually.

Failure to complete these steps before configuring the policy server results in a configuration failure.

Windows Launchpad configuration recovery

Configuration failures while using Launchpad on Windows require understanding and correction of the root cause. After correction, complete the configuration with the command line.

Steps for troubleshooting failed configuration

To recover from a failed Launchpad configuration on Windows, do the following steps:

1. Make note of the failed component name, configuration log file name, and return error code that is shown by Launchpad.
2. Exit Launchpad.
3. Check the return error code descriptions. See Table 6 on page 33. If the return error code description does not provide the root cause, open the configuration log file for the failed component. Search the log for the cause of the error.
4. Correct any problems that are listed in the return error code or configuration log file.
5. Use the command line to complete configuration for the component, following the procedure in the *IBM Security Access Manager for Web Installation Guide*.

   Note: Do not use Launchpad to complete configuration after a failed configuration. Launchpad does not list a component that is already installed. Following an error, complete the configuration with the command line or with the **`pdconfig`** UI.

Windows Launchpad configuration scripts, error codes, and log files

The following table lists the configuration script name, script location, and return error codes for each component. The table also lists the configuration log file name and location for each component.

If you encounter an issue during Launchpad configuration, use the following table for the return error code description. Next, locate the log file and examine the contents for further information about the cause of the error.

Table 6. Windows Launchpad configuration scripts, error codes, and log files

Component	Configuration script and location	Error codes that are used by script	Configuration log file and default location
Tivoli Directory Server	`install_directory` `\Scripts\` `ISAMConfigTDS.bat`	• 2 = IBM Tivoli Directory Server is not installed, or there is a problem reading the registry. • 3 = Problem adding default suffix. The default suffix is `secAuthority=Default`. • 4 = Problem starting the LDAP server. • 5 = Problem adding the sample `ldif` file: `\bin\org_ldif`.	`ConfigTDSforISAM.log` This log is in the *USERPROFILE* directory. Typically, the path is `C:\Users\Administrator\` `ConfigTDSforISAM.log`.
Security Access Manager Runtime for Java	`\bin\launchPDJRTECFG.bat`	• 1 = IBM Java Development Kit is not installed, or the registry was not read. • 2 = IBM Security Java Runtime is not installed, or the registry was not read. • 3 = The **pdjrtecfg** command did not start.	`ConfigJRTEforISAM.log` This log is in the *USERPROFILE* directory. Typically, the path is `C:\Users\Administrator\` `ConfigJRTEforISAM.log`.
Security Access Manager component	`\bin\launchPDCONFIG.bat`	• 1 = Security Access Manager Runtime is not installed, or the registry was not read. • 2 = GSKit is not installed, or the registry was not read. • 3 = Security Utilities is not installed, or the registry was not read. • 4 = The **pdconfig.exe** command did not start.	`LaunchPDConfigforISAM.log` This log is in the *USERPROFILE* directory. Typically, the path is `C:\Users\Administrator\` `LaunchPDConfigforISAM.log`.
Session Management Server	`\bin\launchSMSCFG.bat`	• 1 = Internal Error. The required parameter, *path to WebSphere Application Server*, is missing. • 2 = IBM Security Access Manager Session Management Server is not installed, or there is a problem reading the registry. • 3 = Problem running the **smscfg** command.	`deploySMSconsole.log` This log is in the *USERPROFILE* directory. Typically, the path is `C:\Users\Administrator\` `deploySMSconsole.log`.
Configuration of runtime for Java to WebSphere Application Server	**PDJRTE**	• 1 = IBM Security Java Runtime is not installed, or the registry was not read. • 2 = The **pdjrtecfg** command did not start.	`ConfigJRTEforWAS.log` This log is in the *USERPROFILE* directory. Typically, the path is `C:\Users\Administrator\` `ConfigJRTEforWAS.log`.

Table 6. Windows Launchpad configuration scripts, error codes, and log files (continued)

Component	Configuration script and location	Error codes that are used by script	Configuration log file and default location
Web Portal Manager runtime for Java	**amwpmcfg**	• 1 = IBM Security Access Manager Web Portal Manager is not installed, or the registry was not read. • 2 = The **amwpmcfg** command did not start.	ConfigAMWPM.log This log is in the *USERPROFILE* directory. Typically, the path is C:\Users\Administrator\ConfigAMWPM.log.

Opening a log file in Launchpad

You can view Launchpad log data from within Launchpad.

To view a log of the Launchpad process:

With Launchpad open, hold down the Ctrl key, and left-click over the **IBM Security Access Manager for Web** banner in the top panel. A log section opens at the bottom panel. You can print or save the log. By default, only serious errors are collected.

To collect detailed Launchpad debug information:

Open a Windows command prompt and issue the following command:

```
set LaunchPadLogFilter=FSEWTC
CD to the ISAM install image
Run launchpad64.exe
```

A log section opens at the bottom panel in Launchpad. You can print, save, or copy and paste the log information to a file.

Additional Tivoli Directory Server configuration information

For complete information about Tivoli Directory Server configuration issues, see the Tivoli Directory Server documentation.

Additional Security Access Manager configuration information

The Security Access Manager component configuration script, launchPDCONFIG.bat, configures the following Security Access Manager components:

- Security Access Manager policy server
- Security Access Manager runtime
- Security Access Manager Application Development Kit
- Security Access Manager authorization server
- Security Access Manager policy proxy server

Additional Session Management Server configuration information

If deployment fails with the Launchpad, you can deploy from the command line with the following command:

```
install_directory\bin\smscfg
```

See the *IBM Security Access Manager for Web Command Reference Guide* for options in using the **smscfg** command.

Additional configuration of runtime for Java to WebSphere Application Server information

The **PDJRTE** command configures runtime for Java to WebSphere Application Server and places PD.jar in WebSphere Application Server. Errors are written to the ConfigJRTEforWAS.log file.

Chapter 5. Troubleshooting upgrade

The following sections contain troubleshooting information for upgrade.

When you upgrade IBM Security Access Manager for Web to version 7.0, you migrate data and configuration from an earlier version to the current version.

For a successful upgrade and migration, ensure the following criteria:

- Create a valid backup directory for both the Tivoli Access Manager environment that you intend to migrate, and the user registry.
- Ensure that the required files are available in the backup directory.
- Ensure that your version of Tivoli Access Manager is supported for a migration to 7.0. Supported versions include: 6.0, 6.1, and 6.1.1.

To identify the root cause of an upgrade or migration failure, check the following information:

- The error messages that are displayed.
- The log files.
- Run migration with trace mode ON and redirect the trace output to a file. Use the trace output to determine the reason for migration failure.

Upgrade common problems

This section details common problems that you might encounter when you upgrade Security Access Manager.

Cannot create users or groups after upgrade

Security Access Manager does not have authority to create users and groups after Tivoli Directory Server is upgraded. If Tivoli Directory Server is your user registry, and you are upgrading Security Access Manager, then the Tivoli Directory Server component must be migrated first, if all components are on the same machine.

Complete the migration of Tivoli Directory Server by following the instructions in the *IBM Security Access Manager for Web Upgrade Guide*.

These instructions guide you through the process of backing up the current data with the **db2ldif** utility, upgrading the Tivoli Directory Server, and restoring the data with the **bulkload** utility.

When you use the **bulkload** utility, specify the **–A yes** option to have it properly process Access Control List (ACL) updates. If the ACLs are not loaded properly, Security Access Manager does not have the authority to complete the needed tasks to create and maintain user and group information.

If bulkload fails to update the ACLs properly and these symptoms occur, you can create the ACLs manually by following the "Applying Access Manager ACLs to new LDAP suffixes" procedure in the *IBM Security Access Manager for Web Administration Guide*. Using the Web Administration Tool, apply the ACLs to all existing LDAP suffixes and `secAuthority=Default` entries below all defined users in the LDAP server. Applying these ACLs restores the correct authority to allow Security Access Manager to continue.

pdbackup seems to hang on Windows 2008

The **`pdbackup`** utility requires user input on Tivoli Access Manager for e-business versions 6.0, 6.1, or 6.1.1 that run on Windows 2008. It might seem to hang.

If you encounter this issue, use either of the following approaches:

- Type an `A` in the command window. The utility resumes normally.
- Apply the appropriate fix pack and rerun the **`pdbackup`** utility:
  - Tivoli Access Manager 6.0: Fixpack 28 or later
  - Tivoli Access Manager 6.1: Fixpack 08 or later
  - Tivoli Access Manager 6.1.1: Fixpack 04 or later

Note: Installing the fix pack is a permanent fix.

Chapter 6. Verifying the deployment

The installation of Security Access Manager involves the installation and configuration of a number of prerequisites.

These prerequisites can include Security Access Manager components. Operational failures can result from the failure to install or correctly configure a prerequisite.

If you have a failure in the following instances, always examine your installed software:

- A new Security Access Manager installation fails to work properly
- An existing Security Access Manager installation fails to work properly after you update a prerequisite or Security Access Manager components

The *IBM Security Access Manager for Web Release Notes* provides detailed information about specific software requirements that must be satisfied before Security Access Manager can be successfully installed and configured. These requirements include supported operating systems, prerequisite software, and required patches. Be sure to note the release or level of each software item.

System types in a deployment

A typical deployment of Security Access Manager involves the installation and configuration of a number of systems.

All Security Access Manager deployments include several types of Security Access Manager systems that are set up in a secure domain, including:

- Base systems
- Web Security systems
- Distributed Session Management systems

Each system type has software prerequisites that include Security Access Manager components. You must successfully install and configure both the prerequisites and Security Access Manager components to avoid operational problems in your environment.

For example, the Security Access Manager policy server requires installation of the following components:

- IBM Global Security Kit (GSKit)
- IBM Tivoli Directory Server client (depending on the registry used)
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Policy Server

For a complete listing of the system types and their related components, see the *IBM Security Access Manager Installation Guide*.

Checking installed software

Security Access Manager provides commands and utilities to help you determine whether the correct software, and software level, is installed on any operating system.

Use the **pdversion** utility to list Security Access Manager components that are installed on the system along with their version number. This utility does not list prerequisite software, such as IBM Global Security Kit (GSKit).

You can also determine the presence or absence of prerequisite software with operating system utilities. The utilities, by operating system, are as follows:

AIX The **lslpp –l** command

Linux The **rpm –qa** command

Solaris
The **pkginfo –l** command

Windows
The Add/Remove Programs facility from the Control Panel

Use these tools with the software requirements that are listed in the *IBM Security Access Manager for Web Release Notes* to ensure that all the required software is installed on each system in your Security Access Manager deployment.

Note: Even with these utilities, certain software might still be difficult to locate.

Verifying Global Security Kit

The two most common problems with the IBM Global Security Kit (GSKit) include:

- GSKit was not installed
- The wrong version of GSKit is installed, left over from a previous installation

GSKit on Windows operating systems does not add an entry to the Add/Remove Program list. On Windows operating systems, GSKit is typically installed in the following directory:

```
C:\Program Files\IBM\gsk8
```

Use the following command on Windows operating systems to display the GSKit version:

```
C:\Program Files\IBM\gsk8\bin\gsk8ver_64
```

You can validate the correct installation of GSKit by checking its version as described in “IBM Global Security Kit” on page 157.

Verifying user registries

This section provides information about verifying the different Security Access Manager user registries.

Tivoli Directory Server

This section provides information about verifying Tivoli Directory Server when it is used as the Security Access Manager user registry.

Verifying the server

Communication between the Tivoli Directory Server client and the LDAP server can be tested by using the **ldapsearch** command. This command also reveals the version of the LDAP server software. This command (entered as one line) can be run from any machine with Tivoli Directory Server client installed. The structure of the **ldapsearch** command different when you use SSL.

Without SSL

The following sample command is appropriate when the LDAP server is configured for non-SSL communication:

```
ldapsearch -h ldapserver-hostname -p 389 -D "ldapadminDN" \
-w ldapadmin-password -b "" -s base objectclass=*
```

Note: If this command fails on a Windows operating system, check that the **ldapsearch** command is the one that is provided by Tivoli Directory Server client.

The output of this command varies depending on which supported LDAP server you are using.

With SSL

The following sample command is appropriate when the LDAP server is configured for SSL communication:

```
ldapsearch -h ldapserver-hostname -p 636 -D "ldapadminDN" \
-w ldapadmin-password -Z -K client-keyfile \
-P key-password -b "" -s base objectclass=*
```

The output of this command varies depending on which supported LDAP server you are using.

Verifying the client

The previous verification procedure for the LDAP server used the Tivoli Directory Server client that was installed on the LDAP server system itself. However, unless you are using Active Directory server for your Security Access Manager user registry, each Security Access Manager system requires the installation of the Tivoli Directory Server client, not just the machine with the LDAP server installed.

The previous verification procedure for the LDAP server is also appropriate for verifying the functions of the Tivoli Directory Server client on each Security Access Manager system.

Microsoft Active Directory

This section provides information about verifying Microsoft Active Directory when it is used as the Security Access Manager user registry.

Verifying the configuration

Server Start the MMC for Active Directory by selecting **Start** → **Program** → **Administrative Tools** → **Active Directory Users and Computers**.

If the Active Directory management console started and you can browse all the objects in Active Directory, the Active Directory server completed its configuration correctly. Otherwise, you can complete the procedures to unconfigure and reconfigure Active Directory as described in the *IBM Security Access Manager for Web Installation Guide*.

Client Configure the client into an existing Active Directory domain to complete Security Access Manager configuration. To ensure that the client system is part of the Active Directory domain, you can use System Properties to ensure the correct configuration of the client machine by selecting **Start → Settings → Control Panel → System → System Properties**.

In the Control Panel, double-click on System icon. The System Properties window is displayed. On the System Properties windows, click the Network Identification menu. If the Domain on the Network Identification contains the correct Active Directory domain, it indicates that the client machine is properly configured into the Active Directory domain.

Verifying version numbers

Server Active Directory is included with Windows Advanced Server installation. Therefore, only one version of this software is possible. After successfully configuring the Active Directory server, it is started automatically during the reboot process.

Client Active Directory is included with Windows Advanced Server installation. Therefore, only one version of this software is possible.

Confirming connectivity

Install Windows 2008 Support Tools from the `\support\tools` directory on the Windows 2008 operating system DVD. From that directory, run **`setup.exe`** and follow the installation guide to complete the installation.

Activate the ADSI Edit MMC window by selecting **Start → Programs → Windows 2008 Support Tools → Tools → ADSI Edit**.

The user can set up the server connection by selecting **Action → Settings**.

Additionally, click **Advanced** on the Connection window to input the administrator ID and password to connect to the remote Active Directory server. If the connection is successful, the client machine will be able to communicate with the Active Directory server using ADSI.

Verifying base systems

At a high level, you can determine which Security Access Manager servers are configured and which are running.

On AIX, Linux, and Solaris operating systems, use the following command:

```
# pd_start status
```

On Windows operating systems, check the Security Access Manager entries in the Services window. To open this window, select **Control Panel → Administrative Tools → Services**.

Verifying the policy server

The **`pdadmin`** command can be used to verify the correct operation of the policy server.

About this task

Enter the following command to log in as a Security Access Manager administrator:

```
pdadmin –a sec_master –p password
```

Assuming that WebSEAL is configured on the machine, at the **pdadmin** prompt, complete the following steps:

1. List the servers with the **server list** command. For this purpose, this command has the following syntax:
   ```
   pdadmin> server list webseald-machinename
   ```
2. List the objects with the **object list** command without options, as follows:
   ```
   pdadmin> object list
   ```
3. List ACLs with the **acl list** command without options, as follows:
   ```
   pdadmin> acl list
   ```
4. List users with the **user list** command. For this purpose, this command has the following syntax:
   ```
   pdadmin> user list name count
   ```

Verifying the authorization server

The Security Access Manager application development toolkit (ADK) includes the `authzn_demo` demonstration program. You can use this program, in remote mode, to validate the correct operation of the authorization server.

See the `README` file that accompanies this demonstration program for setup and execution instructions. The `README` file is in the following directory:

```
authzn-adk-install-dir/example/auth_demo/cpp
```

Verifying the runtime

The Security Access Manager Runtime can be installed on a system with only GSKit and Tivoli Directory Server client. In this case, the verification procedure for the Security Access Manager Runtime is the same as that described in "Verifying the policy server" on page 42.

Verifying Web security systems

You can verify whether Web security systems are operating properly by connecting from your browser to a URL.

Verifying WebSEAL

You can use a browser to verify that WebSEAL is operating properly. To verify, enter the following URL into your browser:

```
https://webseal-machinename
```

Because a port number is not specified, it is assumed that WebSEAL is listening on port 443 (HTTPS).

Your browser might give you the following warnings:

1. The certificate received from this Web server is issued by a company that you have not yet chosen to trust
2. The name within the certificate received from WebSEAL does not match the name of the system from which it was received

If these warnings occur, they indicate that you did not yet purchase your own server certificate for your WebSEAL server. Your browser is complaining that it received a default server certificate from WebSEAL which contains default names for the issuing certificate authority and the name of the Web server.

Next, the browser prompts you to specify a Security Access Manager user name and password. Enter `sec_master` for the user name and the password that you configured for **sec_master** during installation. If authentication is successful, an image that is labeled Security Access Manager for WebSEAL displays.

Verifying Plug-in for Web Servers

You can use your browser to verify that Security Access Manager Plug-in for Web Servers is operating properly. To verify, enter the following URL into your browser:

```
http://websvrplugin_machinename
```

Because a port number is not specified, it is assumed that the Plug-in for Web Servers is listening on port 80 (HTTP).

Next, your browser prompts you to specify a Security Access Manager user name and password. Enter `sec_master` for the user name and the password that you configured for **sec_master** during installation. If successful, the default Web server page displays.

Chapter 7. Validating and maintaining policy databases

The **pdacld_dump** command validates and maintains the Security Access Manager policy database and database replicas.

Attention: The **pdacld_dump** command requires an understanding of the policy database components and structure. Always work with the advice and assistance of IBM Software Support when you use the **pdacld_dump** command.

The **pdacld_dump** command examines the content and structure of a policy database. Security Access Manager policy databases include the following databases:

- Master policy database, named `master_authzn.db`, controlled by the policy server.
- Replica databases that are used by all instances of the Security Access Manager authorization server and by any C-language applications that are running in local mode.

Each domain that is associated with Security Access Manager has a policy database. The policy database might have replica databases.

The **pdacld_dump** command provides the following functions:

- Transform the binary content of a specified database file into readable text. By default, the output is directed to standard output, but it can be redirected to a file.
- Create a summary report that describes the conditions of a specified database.
- Examine a specified database for corrupted content, defragment the structure of the database, and produce a valid, updated version of the database.
- Provide two levels of validation checking.

This command is located under the installation directory in the `/sbin` subdirectory and is installed as part of the policy server. This command is not yet translated.

Displaying all database contents

You can obtain a readable copy of the contents of a policy database with the **pdacld_dump** command.

For example, to examine the policy database for the `Zebra` domain on Windows, enter the following command:

```
pdacld_dump -f "C:\Program Files\Tivoli\Policy Director\db\Zebra.db"
```

Note: On Windows operating systems, the path and file name must be enclosed in double quotation marks.

Displaying summary reports

The summary report from the **pdacld_dump** command reveals important information about the condition of a policy database. The summary report includes the following information:

- The DB Sequence Number line contains the database sequence number. The sequence number changes each time the that database is updated. If you compare this number with the sequence number in the master policy database, you can determine whether the two databases are synchronized.
- The Dumped line indicates whether the file contains the complete database. It is possible for a database to be truncated.
- The invalid objects were encountered line indicates the validity of the database contents.

To obtain a summary report of a policy database, use the **–s** option of the **pdacld_dump** command. For example, to obtain the summary of the policy database for the default management domain on a AIX, Linux, or Solaris operating system, enter the following command:

```
pdacld_dump -f /var/PolicyDirector/db/master_authzn.db -s
```

Repairing a damaged policy database

If the policy database becomes damaged or corrupted, use the **pdacld_dump** command to create a policy database.

Attention: The **pdacld_dump** command requires an understanding of the policy database components and structure. Always work with the advice and assistance of IBM Software Support when you use the **pdacld_dump** command.

Create the policy database with only the valid data recovered from the damaged policy database.

For example, if the policy database for the OutCenter domain becomes damaged, use the following command to recover the valid information from the existing policy database and write it to the new RepairedOutCenter.db policy database:

```
pdacld_dump -f /var/PolicyDirector/db/OutCenter.db \
-r /var/PolicyDirector/db/RepairedOutCenter.db
```

Additionally, this option de-fragments the content of the new policy database.

Replacing a damaged policy database

About this task

To replace the damaged policy database with the repaired one, complete the following steps:

Procedure

1. Stop the policy server or the authorization server.
2. Rename the damaged policy database (OutCenter.db in the previous example) or move it to a different directory.
   ```
   ren OutCenter.db DamagedOutCenter.db
   ```
3. Rename the repaired file to have the same name as the original policy database.
   ```
   ren RepairedOutCenter.db OutCenter.db
   ```
4. Restart the policy server or authorization server.

Part 3. Using log files for troubleshooting

Chapter 8. Collecting events to diagnose or audit server operations

You can collect events for diagnostic and auditing purposes of the servers.

Events for diagnostics and auditing are for operations of the Security Access Manager servers.

These events are not for installation of the servers. For installation activity events, see "Installation logs" on page 20.

To enable diagnostics and auditing, you define which types of events to capture. When events are captured, they can be written to:
- Log file
- Standard output (STDOUT) device
- Standard error (STDERR) device
- Combination of these destinations.

Beyond these destinations, when events are captured, they can be redirected to a remote server or redirected to an application for processing with log agents.

Diagnostic events

For collecting diagnostic information, define which *message events* and which *trace events* to capture. These events can help you troubleshoot problems.

A *message event* is a record of a noteworthy event that occurred, such as a failure to connect error message.

A *trace event* is a capture of information about the current operating environment at the time that a component or application failed to operate as intended.

Trace event logs provide IBM Support with information that relates to the condition of the system at the time a problem occurred. Trace logging enablement can cause large amounts of data to collect in a short amount of time. Therefore, enable trace events only at the direction of IBM Support.

To configure message or trace events, define *statements* in the routing file or Java properties file for the server:
- For message events, define the statements by severity level.
- For trace events, define the statements by trace level and, optionally, by component.

Auditing events

For auditing purposes, define audit, statistic, or other type of events for capture in a log file.

Auditing provides tracking and archiving of auditable events. These events create records of various server activities. Configure audit event logs by using either the base Security Access Manager or Common Audit Service.

Configure audit events by defining stanza entries in configuration files. Define stanza entries in configuration files:

- For base Security Access Manager auditing: define `logcfg` entries in the `[pdaudit-filter]` stanza.
- For Common Audit Service: define entries in the `[cars-filter]` stanza.

For WebSEAL, you can also log HTTP events by using the `[logging]` stanza in the WebSEAL configuration file.

For more information about audit events, see the *IBM Security Access Manager for Web Auditing Guide*.

Chapter 9. Customize logging events with routing files

Routing files are ASCII files that customize the logging of message and trace events for C language-based servers, daemons, and other C-language programs and applications.

To customize logging of message and trace events for Java applications, see Chapter 10, "Java properties files," on page 57.

At application startup, the application-specific routing file is read. With the routing file content, you can control the following aspects of logging event activity:

- Whether to enable logging for specific event classes.
- Where to direct the output for each event class.
- How many log files to use for each event class.
- How large each log file can be for each event class.

Location of routing files

You can locate routing files to control the logging of both message events and trace events.

Table 7 lists the default location for the routing files.

Table 7. Default location of routing files

Component	Default name and location of routing file

Runtime environment	**Windows**
	`%PD_HOME%\etc\routing`
	AIX, Linux, and Solaris
	`/opt/PolicyDirector/etc/routing`

Policy server	**Windows**
	`%PD_HOME%\etc\pdmgrd_routing`
	AIX, Linux, and Solaris
	`/opt/PolicyDirector/etc/pdmgrd_routing`

Authorization server	**Windows**
	`%PD_HOME%\etc\pdacld_routing`
	AIX, Linux, and Solaris
	`/opt/PolicyDirector/etc/pdacld_routing`
	Note: `pdacld_routing` applies to the default authorization server. If there are multiple instances of the authorization server, the routing file name is prefixed with the instance name, such as, *`instance1`*`-pdacld_routing`.

Policy proxy server	**Windows**
	`%PD_HOME%\etc\pdmgrproxyd_routing`
	AIX, Linux, and Solaris
	`/opt/PolicyDirector/etc/pdmgrproxyd_routing`

Table 7. Default location of routing files (continued)

Component	Default name and location of routing file

WebSEAL server	**Windows**
	`%PD_WEB%\etc\routing`
	AIX, Linux, and Solaris
	`/opt/pdweb/etc/routing`

Note:

- For WebSEAL, the `routing` file is created from the `routing.template` file during installation. The `routing` and `routing.template` file are in the same directory.
- For WebSEAL, if you do not want to modify the default routing file (`/etc/routing`), you can use the `PD_SVC_ROUTING_FILE` environment variable to define an alternative routing file. If the file defined by this environment variable does not exist or is not accessible, the default routing file (`/etc/routing`) is used.
- The Plug-in for Web Servers component programmatically sets the information that is typically contained in a routing file. Therefore, Plug-in for Web Servers has no routing file of its own.

Setting trace for multiple instances of WebSEAL

If you have multiple instances of WebSEAL, you can define an environment variable to trace each instance. Set the `PD_SVC_ROUTING_FILE` environment variable for the startup of each instance.

For example, write a script with the following contents:

```
PD_SVC_ROUTING_FILE=name_of_routing_file
export PD_SVC_ROUTING_FILE
/opt/pdweb/bin/pdweb_start start instance_name
```

Routing file entries

Each routing file contains entries that control the logging of message events and trace events. However, the format of these entries differs by event type.

Use one of the following formats (entered on a single line without spaces) when you define entries in routing files:

Message events

```
severity:destination:location [[;destination:location]...]
[;GOESTO:{other_severity | other_component}]
```

Trace events

```
component:subcomponent.level[[,subcomponent.level]...]
:destination:location [[;destination:location]...]
[;GOESTO:{other_severity | other_component}]
```

Where:

component:*subcomponent*.*level*[[,*subcomponent*.*level*]...]

Specifies the component, subcomponents, and reporting levels of trace events to log. For trace events only.

For the component portion, you can specify an asterisk (*) to log trace data for all components.

For the subcomponent portion, you can specify an asterisk (*) to log trace data for all subcomponents of the specified component.

For the level portion, specify the reporting level to log. This value is a number 1 - 9. A level of 1 indicates the least number of details, and a level of 9 indicates the greatest number of details.

destination

Specifies where to log the events. For each destination, you need to specify a location. When you specify multiple destination-location pairs, separate each pair with a semicolon (;). The following destinations are valid:

DISCARD

Discards the events.

FILE

Writes the events as ASCII text in the current code page and locale to the specified location. When you use this destination, you must specify a location for the file. Optionally, you can follow the `FILE` destination by a period and two numbers that are separated by a period (for example, `FILE.10.100`). The first value indicates the number of files to use. The second value indicates the number of events each file can contain. If you do not specify these values, there is only one log file that grows without limit.

The average size of an ASCII event is 200 bytes. Because the maximum size of a log file is 2 GB, limit the maximum number of events to approximately 10,000,000 events.

STDERR

Writes the events as ASCII text in the current code page and locale to the standard error device.

STDOUT

Writes the events as ASCII text in the current code page and locale to the standard output device.

TEXTFILE

Same as `FILE`.

UTF8FILE

Writes the events as UTF-8 text to the specified location. When you use this destination, you must specify a location for the file. Optionally, you can follow the `UTF8FILE` destination by a period and two numbers that are separated by a period (for example, `UTF8FILE.10.100`). The first value indicates the number of files to use. The second value indicates the number of events each file can contain. If you do not specify these values, there is only one log file that grows without limit.

The average size of a UTF-8 event is 200 bytes. Because the maximum size of a log file is 2 GB, limit the maximum number of events to approximately 10,000,000 events.

Note: When the operating system does not use a UTF-8 code page, the conversion to UTF-8 can result in data loss. When data loss occurs, the log file contains a series of question mark (?) characters at the location where the data conversion was problematic.

XMLFILE

Writes events to the specified location in the XML log format. When you use this destination, you must specify a location for the file. Optionally, you can follow the `XMLFILE` destination by a period and two numbers that are separated by a period (for example, `XMLFILE.10.100`). The first value indicates the number of files to use. The second value indicates the number of events each file can contain. If you do not specify these values, there is only one log file that grows without limit.

The average size of an XML message event is 650 bytes, and the average size of an XML trace event is 500 bytes. Because the maximum size of a log file is 2 GB, limit the maximum number of events to approximately 3,000,000 message events or 4,000,000 trace events.

XMLSTDERR

Writes events to the standard error device in the XML log format.

XMLSTDOUT

Writes events to the standard output device in the XML log format.

GOESTO:{*other_severity* | *other_component*}**]**

Specifies to route events to the same destination and location as either message events of the specified severity or trace events of the specified component.

location

Specifies the name and location of the log file. When the destination is `TEXT`, `TEXTFILE`, `UTF8FILE` or `XMLFILE`, you must specify a location. When the destination is `DISCARD`, `STDERR`, `STDOUT`, `XMLSTDERR` or `XMLSTDOUT`, you must specify a hyphen (-).

When you specify a fully qualified file name, you can use the `%ld` character string to insert the process ID into the file name.

When the number of files is specified as part of the destination, a period and the file number are appended to the specified log file.

Note: On Windows operating systems, the file name must not end with a period. If the file name ends with a period, when the file number is appended, the file name contains two consecutive periods. File names with two consecutive periods are not valid.

On AIX, Linux, and Solaris operating systems, the file name must be followed by file permissions, the user who owns the file, and the group that owns the file. Use the following format:

```
location:permissions:owner:group
```

To specify the location for message events from the policy server and write them to the default UTF-8 log file, you can specify the following location:

```
/var/PolicyDirector/log/msg__pdmgrd_utf8.log:644:ivmgr:ivmgr
```

severity

Specifies the severity of the message events to log. For message events only.

The following message severities are valid:

- `FATAL`
- `ERROR`
- `WARNING`
- `NOTICE`

- NOTICE_VERBOSE

You can specify an asterisk (*) to log messages regardless of severity.

For complete details about the severity of message events, see “Severity of message events” on page 63.

Chapter 10. Java properties files

Java properties files are ASCII files that are used to customize event logs for Java based Security Access Manager servers, daemons, and other Java-language programs and applications. Beyond customizing logs, these properties files are used to configure other aspects of the application.

The contents of the properties file enables the user to control the following aspects of message logs:

- Whether event logs are enabled
- Where to direct the output
- If the output is to a file, the number of files to use and the size of each file

Lines in the file that start with a number sign (#) are comments and do not affect logging.

The application name (*app_name*) is part of each logging property for a Java application. The application name is specified when you use the `com.tivoli.pd.jcfg.SvrSslCfg` command.

Location of Java properties files

The default locations for the Java properties files for Security Access Manager components are shown in Table 8.

Table 8. Location of Java properties files

Component	Default file name
Java application that is configured by using the `com.tivoli.pd.jcfg.SvrSslCfg` class.	The output application configuration file as specified in the `com.tivoli.pd.jcfg.SvrSslCfg` class.
Java based Security Access Manager commands, such as the **pdjrtecfg** command and `com.tivoli.pd.jcfg.SvrSslCfg` or applications not explicitly configured.	`$JAVA_HOME/PolicyDirector/PDJLog.properties`

Web Portal Manager	**Windows**
	`%PD_HOME%\java\export\pdwpm\pdwpm.properties`
	AIX, Linux, and Solaris
	`/opt/PolicyDirector/java/export/pdwpm/pdwpm.properties`

Note: If the `com.tivoli.pd.jcfg.SvrSslCfg` command was not run, no application-specific configuration file exists. If there is no configuration file, the `PDJLog.properties` file is used.

Application-specific logging of Java applications

Configuration of message and trace logs for the IBM Security Access Manager Runtime for Java (AMJRTE) component is completed on a per-application basis. This configuration removes the file contention and ownership problems that are encountered in previous versions of Security Access Manager.

In addition to existing configuration properties, the application properties file created by the com.tivoli.pd.jcfg.SvrSslCfg command contains logging properties that are associated with the application-logging properties for the application.

The names of the logging objects and the log files in this configuration file contain the application server name that is supplied by the **appSvr** parameter of com.tivoli.pd.jcfg.SvrSslCfg. Thus, each application has a unique set of objects and log files. If the configuration file for an application is not being used (for instance, when the **pdjrtecfg** command is used), message log and tracing properties are taken from the existing PDJLog.properties file.

In addition, the size and the number of files that are used for messages and trace entries are now configurable.

Configuring message events with the Java properties file

To capture message events for Java applications, you need to configure the Java properties file.

Message loggers and file handlers

Each properties file contains properties for one or more message loggers. The isLogging property specifies whether message logs are enabled. To turn on logging for a specific message logger, use:

```
baseGroup.PDJapp_nameMessageLogger.isLogging=true
```

To disable logging for a specific message logger, use:

```
baseGroup.PDJapp_nameMessageLogger.isLogging=false
```

Associated with each message logger is at least one file handler. A file handler specifies the destination for messages. After message logs are enabled by the message logger, the file handler properties are examined to determine whether to log messages, and if so, how and where. The properties that are associated with a file handler are:

```
baseGroup.PDJapp_nameFileHandler.fileName=
baseGroup.PDJapp_nameFileHandler.maxFileSize=
baseGroup.PDJapp_nameFileHandler.maxFiles=
```

where:

fileName
Specifies the fully qualified file name to be used as the base name for message log files. The file can be in any location accessible by the Java application.

maxFileSize
Specifies the maximum size, in kilobytes, of each message log file. Default is 512.

maxFiles
Specifies the maximum number of files to be used for message logs. Default is 3.

To specify what classes of messages to log, use the MessageAllMaskFilter.mask property as illustrated in Figure 1 on page 59.

```
baseGroup.PDJapp_nameMessageAllMaskFilter.mask=FATAL
 | ERROR | WARNING | NOTICE | NOTICE_VERBOSE
```

Figure 1. Specifying what messages to log in a properties file

When PDJLog.properties is used

The `$JAVA_HOME/PolicyDirector/PDJLog.properties` file is used to define message and trace log properties in the following cases:

- For non-application-related Java commands, such as **pdjrtecfg** and `com.tivoli.pd.jcfg.SvrSslCfg`.
- If a Java application was not explicitly configured with the `com.tivoli.pd.jcfg.SvrSslCfg` command.
- If the application-specific properties file is inaccessible or does not exist.
- If a required property in the application-specific properties file is not found.

When you use the default `PDJLog.properties` file, message logs are enabled only for `FATAL`, `ERROR`, and `WARNING` messages. This is shown in the portion of the `PDJLog.properties` file in Figure 2. Logging can be enabled for `NOTICE` and `NOTICE_VERBOSE` messages by changing the `isLogging` property to `true` for the last two properties that are shown in Figure 2.

```
baseGroup.PDJMessageLogger.isLogging=true
baseGroup.PDJFatalFileHandler.isLogging=true
baseGroup.PDJErrorFileHandler.isLogging=true
baseGroup.PDJWarningFileHandler.isLogging=true
baseGroup.PDJNoticeFileHandler.isLogging=false
baseGroup.PDJNoticeVerboseFileHandler.isLogging=false
```

Figure 2. Portion of the default `PDJLog.properties` file

On a AIX, Linux, or Solaris operating system, to enable both `NOTICE` and `NOTICE_VERBOSE` messages, and to change the destination properties of `NOTICE_VERBOSE` messages, the following changes can be made, as indicated in **bold**:

```
baseGroup.PDJNoticeFileHandler.isLogging=true

baseGroup.PDJNoticeVerboseFileHandler.fileName=
/tmp/logs/msg__amjrte_verbose.log
baseGroup.PDJNoticeVerboseFileHandler.maxFileSize=1024
baseGroup.PDJNoticeVerboseFileHandler.maxFiles=4
baseGroup.
PDJNoticeVerboseFileHandler.isLogging=true
```

After you make these changes, `NOTICE_VERBOSE` messages are written to the `/tmp/logs/msg__amjrte_verbose.log1` file. After that file reaches 1024 KB, the file is renamed `/tmp/logs/msg__amjrte_verbose.log2` and logging continues with a new `/tmp/logs/msg__amjrte_verbose.log1` log file. A maximum of four message log files is used.

(The procedure would be the same on a Windows operating system. The file name just needs to be changed to reflect a fully qualified file name on Windows operating systems.)

Console handler and console message logging

A console handler and a message console handler also are configured in the `$JAVA_HOME/PolicyDirector/PDJLog.properties` file. Both are disabled by default. To send messages to the console, set both `isLogging` properties to `true`:

```
baseGroup.PDJConsoleHandler.isLogging=true
baseGroup.PDJMessageConsoleHandler.isLogging=true
```

Tailoring message logs in Web Portal Manager

The Java properties file for Web Portal Manager is `pdwpm.properties`. This properties file is in one of the following operating system-specific directories:

Windows operating systems
`%PD_HOME%\java\export\pdwpm`

AIX, Linux, and Solaris operating systems
`/opt/PolicyDirector/java/export/pdwpm`

By default, message logs are enabled:

```
baseGroup.PDJamwpm-host_nameMessageLogger.isLogging=true
```

Note: Do not modify this property file except at the explicit direction of IBM Software Support.

Configuring trace events with the Java properties file

To capture trace events for Java applications, you need to configure the Java properties file.

Trace loggers and file handlers

Each properties file contains properties for one or more trace loggers. The `isLogging` property specifies whether trace logs are enabled. To turn on tracing for a specific trace logger, use:

```
baseGroup.trace_logger_name.isLogging=true
```

To disable logging for a specific trace logger, use:

```
baseGroup.PDJapp_nameTraceLogger.isLogging=false
```

Associated with each trace logger is at least one file handler. A file handler specifies the destination for a specific class, or severity, of messages. After trace logs are enabled by the trace logger, the file handler properties are examined to determine whether to log traces, and if so, how and where. The properties for a file handler are:

```
baseGroup.PDJapp_nameTraceFileHandler.fileName=
baseGroup.PDJapp_nameTraceFileHandler.maxFileSize=
baseGroup.PDJapp_nameTraceFileHandler.maxFiles=
```

where:

fileName
Specifies the fully qualified file name to be used as the base name for trace log files. The file can be in any location accessible by the Java application.

maxFileSize
Specifies the maximum size, in KB, of each trace log file. Default is `512`.

maxFiles

Specifies the maximum number of files to be used for trace logs. Default is 3.

Enabling trace in a Runtime for Java environment

Trace logging for components that use the Security Access Manager Runtime for Java environment is controlled through the application-specific properties file or, for applications that are not explicitly configured with the `com.tivoli.pd.jcfg.SvrSslCfg` command, the `$JAVA_HOME/PolicyDirector/PDJLog.properties` file. To enable tracing:

```
baseGroup.PDJapp_nameTraceLogger.isLogging=true
```

For each trace logger, the properties file defines a mask attribute, `baseGroup.PDJ`*`app_name`*`TraceAllMaskFilter.mask`, that determines what levels of tracing are enabled. Valid mask values are 1 through 9. The precise meaning of any specified mask value is unimportant. The general intention is that ascending from a lower mask value to a higher mask value (for example, 1 to 2) increases the level of information detail that is traced.

Setting the mask value to a particular level means that all tracing levels up to and including the specified level are enabled. For example, if the mask value is 4, then tracing levels 1, 2, 3, and 4 are traced.

Enabling trace in Web Portal Manager

The Java properties file for Web Portal Manager is `pdwpm.properties`. This properties file is in one of the following operating system-specific directories:

Windows operating systems

`%PD_HOME%\java\export\pdwpm`

AIX, Linux, and Solaris operating systems

`/opt/PolicyDirector/java/export/pdwpm`

By default, trace logs are disabled:

```
baseGroup.PDJamwpm-host_nameTraceLogger.isLogging=false
```

Note: Do not modify this property file except at the explicit direction of IBM Software Support.

Chapter 11. Message event logging

The contents of log files can be useful sources of information when you monitor or troubleshoot Security Access Manager servers.

You can use log files to capture any Security Access Manager message.

- Message logging for the C-language portions of Security Access Manager is controlled through *routing files*.
- Message logging for the Java language portions is controlled through *Java properties files*.

When relevant, the distinctions between these methods are mentioned.

Use the statements within routing files to control which messages to log, the location of the log files, and format of the messages. Use the information in this chapter to learn the configuration syntax that is used in the routing files and defines the default file name and location of the message log files. The directory location for message log files can be different, depending on whether Tivoli Common Directory is configured.

Severity of message events

In the message log file, each message event has an associated severity level. The following message severities are valid:

- `FATAL`
- `ERROR`
- `WARNING`
- `NOTICE`
- `NOTICE_VERBOSE`

FATAL messages

An unrecoverable error occurred, such as a database corruption. The process that encounters the error usually terminates and might produce a core file. This error might require manual intervention to recover or require special recovery actions. Depending on the nature of the failure, IBM Software Support might need to be consulted.

The identifier for these messages uses the error (`E`) message severity.

ERROR messages

An unexpected or nonterminal event, such as a timeout, or correctable event that requires manually intervention occurred. The product continues to function, but some services or functions might not be available. This severity also indicates that a particular request or action was not completed. Administrative action might be required.

The identifier for these messages uses the error (`E`) message severity.

WARNING messages

An event occurred that is possibly not the wanted or requested result, such as a configuration file not being found and a default value used instead. The program continues to function normally. This severity also indicates a condition that might be an error if the effects are unwanted or indicates a condition, which if not corrected, can result in an error. For example, a low memory or disk space condition.

The identifier for these messages uses the warning (`W`) message severity.

NOTICE messages

An event took place that does not directly require action, such as starting a server. The event conveys general information about running state or normal actions.

The identifier for these messages uses the information (`I`) message severity.

NOTICE_VERBOSE messages

This event is similar to `NOTICE`, but the events that are logged might contain more detailed information.

The identifier for these messages uses the information (`I`) message severity.

Location of message logs

The location of the runtime and server message log files depends on whether Tivoli Common Directory support is requested during the installation.

Location with Tivoli Common Directory

If Tivoli Common Directory support is requested, the existing Tivoli Common Directory is used for storing most of the message logs. If this directory did not exist, one is created during the installation at the specified location. Assuming that the user accepted the default value, Table 9 shows the location for the message logs.

Table 9. Default location of the Tivoli Common Directory message files

Component	Default log location with Tivoli Common Directory

Runtime environment
Policy server
Authorization server
Policy proxy server
	Windows
	`c:\program files\ibm\tivoli\common\HPD\logs`
	AIX, Linux, and Solaris
	`/var/ibm/tivoli/common/HPD/logs`

WebSEAL server	**Windows**
	`c:\program files\ibm\tivoli\common\DPW\logs`
	AIX, Linux, and Solaris
	`/var/ibm/tivoli/common/DPW/logs`

Plug-in for Web Servers	**Windows**
	`c:\program files\ibm\tivoli\common\AMZ\logs`
	AIX, Linux, and Solaris
	`/var/ibm/tivoli/common/AMZ/logs`

Table 9. Default location of the Tivoli Common Directory message files (continued)

Component	Default log location with Tivoli Common Directory

Session Management Server	**Windows**
	`c:\program files\ibm\tivoli\common\CTGSM\logs`
	AIX, Linux, and Solaris
	`/var/ibm/tivoli/common/CTGSM/logs`

Location without Tivoli Common Directory

If Tivoli Common Directory is not used, the message logs are in the directories that are specified in Table 10.

Table 10. Location of message log files without Tivoli Common Directory

Component	Default log location
Runtime environment Policy server Authorization server Policy proxy server	**Windows** *base_install_dir*`\log` **AIX, Linux, and Solaris** `/var/PolicyDirector/log`
WebSEAL server	`$PD_WEB/log`
Plug-in for Web Servers	`$PD_WEBPI/log`
Attribute retrieval service	`$WAS_HOME`
Session Management Server	**Windows** *pdsms_install_dir*`\log` **AIX, Linux, and Solaris** `/var/pdsms/log`

Names of message logs

The names of the message log files depend on whether the log is for the Runtime component or a server component. The messages for the Runtime component are separated into severity-specific files, while the messages for the server components are written to the same file.

Names of runtime logs

IBM Security Access Manager runtime messages are messages that are produced by applications, commands, and utilities that use the Security Access Manager Runtime component. The sources include the C language-based utilities, such as the **pdadmin** commands and the **svrsslcfg** utility.

Table 11 lists the names of the default message log files for both C and Java language applications.

Table 11. Message severity levels and associated message logs

Message severity	Default log name

FATAL	**C runtime log name**
	`msg__fatal.log`
	Java runtime log name
	`msg__`*app_nameN*`.log`
	WebSEAL log name
	Written to the standard error file (STDERR)

Table 11. Message severity levels and associated message logs (continued)

Message severity	Default log name
ERROR	**C runtime log name** msg__error.log **Java runtime log name** msg__*app_nameN*.log **WebSEAL log name** Written to the standard error file (STDERR)
WARNING	**C runtime log name** msg__warning.log **Java runtime log name** msg__*app_nameN*.log **WebSEAL log name** Written to the standard error file (STDERR)
NOTICE	**C runtime log name** msg__notice.log **Java runtime log name** msg__*app_nameN*.log **WebSEAL log name** msg__notice_*PID*.log **Note:** Logging is not enabled by default.
NOTICE_VERBOSE	**C runtime log name** msg__verbose.log **Note:** Logging is not enabled by default. **Java runtime log name** msg__*app_nameN*.log **WebSEAL log name** msg__verbose_*PID*.log **Note:** Logging is not enabled by default.

Notes:

- When WebSEAL is running as a background process, FATAL, ERROR, and WARNING messages are redirected to the server message log file for that WebSEAL instance (msg__webseald–*instance_name*.log).
- If an application-specific configuration file does not exist for a Java application, message logs are controlled by the $JAVA_HOME/PolicyDirector/PDJLog.properties file. In these cases, messages are written to the following files:

  FATAL
  msg__amj_fatal*N*.log

  ERROR
  msg__amj_error*N*.log

  WARNING
  msg__amj_warning*N*.log

  NOTICE
  msg__amj_notice*N*.log

  NOTICE_VERBOSE
  msg__amj_verbose*N*.log

Note: By default, logging of NOTICE and NOTICE_VERBOSE messages is not enabled.

Based on the severity level, runtime messages from C-language applications are written to different log files. For example, WARNING messages are written to the msg__warning.log file and FATAL messages are written to msg__fatal.log file. Error messages from WebSEAL are written to STDERR, unless WebSEAL is running in the background. In this case, the messages are written to the WebSEAL server log file.

Runtime message log files that are associated with C-language applications are allowed to grow without bound. Periodically check the available disk space and adjust as necessary, perhaps by archiving or pruning the log files. You can change the name, location, and put size constraints on the runtime message log files, as explained in "Routing file entries" on page 52.

Runtime message log files for Java language applications can grow to a maximum size of 512 KB. A maximum of three message files can exist, with the most recent messages always being in the file that ends in "1". When the file reaches its maximum size, the files are renamed. For example, when the msg__*appname*1.log file reaches 512 KB, the following process occurs:

1. The msg__*appname*3.log file is deleted, if it exists
2. The msg__*appname*2.log file, if it exists, is renamed to msg__*appname*3.log
3. The msg__*appname*1.log file is renamed msg__*appname*2.log
4. A new msg__*appname*1.log file is created

The names, location, number, and size of the Java runtime logs can be changed, as explained in Table 8 on page 57.

Names of server logs

Server messages are messages that are generated by the daemons and servers that are associated with Security Access Manager. Unlike runtime messages from C applications, which are written to different log files based on severity, server messages are always written to the message log for that particular server. Thus, all FATAL, WARNING, ERROR, NOTICE, and NOTICE_VERBOSE messages for the policy server are written to the msg__pdmgrd_utf8.log file. Similarly, WebSEAL messages are written to the msg__webseald-*instance_name*.log file.

Table 12 lists the default names for the server message log files.

Table 12. Message log files that are associated with servers

Server	Default message log file
Security Access Manager policy server	msg__pdmgrd_utf8.log
Security Access Manager authorization server	msg__pdacld_utf8.log
Security Access Manager WebSEAL	msg__webseald-*instance_name*.log
Security Access Manager Plug-in for Web Servers	msg__pdwebpi.log
Security Access Manager policy proxy server	msg__pdmgrproxyd_utf8.log
Security Access Manager Attribute Retrieval Service	msg__amwebars_exceptions.log

By default, the Security Access Manager server message log files (the ones that start with `msg__`) are allowed to grow without bound. Be sure to periodically check the available disk space and adjust as necessary. You might want to archive or prune the log files on a periodic basis as well.

You can change the name, location, and put size constraints on the server message log files as explained in "Routing file entries" on page 52.

For the Security Access Manager Plug-in for Web Servers component, message log entries are always written, by default, to the same set of files when Tivoli Common Directory is not configured. These entries include:

Authorization server

- **Windows operating systems**
  - *webpi-install-dir*`\log\msg__pdwebpi.log`
- **AIX, Linux, and Solaris operating systems**
  - `/var/pdwebpi/log/msg__pdwebpi.log`

IIS plug-in

- **Windows operating systems**
  - *webpi-install-dir*`\log\msg__pdwebpi-iis.log`

Watchdog server

- **AIX, Linux, and Solaris operating systems**
  - `/var/pdwebpi/log/msg__pdwebpimgr.log`

Format of messages in logs

To configure Security Access Manager message logs and trace logs to produce output in an XML log format, see "Sending messages to multiple places in different formats" on page 79 and "Trace logging in XML log format" on page 83.

See "Viewing log files with the XML Log Viewer" on page 9 for information about viewing message logs that are written in XML log format.

Messages in text format

Figure 3 shows an example of a message log entry. This log entry is a sample of a server message in text format.

```
2005-10-26-20:09:10.984-06:00I----- 0x1354A41E pdmgrd ERROR
ivc socket e:\am600\src\mts\mtsclient.cpp 1832 0x000001c4
HPDCO1054E  Could not connect to the server acld2 on port 7137.
```

Figure 3. Sample message log entry in text format

The following list explains the log entry fields that are shown in Figure 3:

2005-10-26-20:09:10.984-06:00I

Indicates the timestamp of the message entry. The timestamp is in the following format:

```
YYYY–MM–DD–hh:mm:ss.fff[+|–]hh:mmI
```

where:

YYYY-MM-DD

Specifies the date in year, month, and day.

hh:mm:ss.fff

Specifies the time in hours, minutes, seconds, and fractional seconds.

hh:mmI
Specifies the time inaccuracy factor.

0x1354A41E
Indicates the 32-bit message number in hexadecimal.

pdmgrd
Indicates the name of the process that created the entry.

ERROR
Indicates the severity of the message.

ivc Indicates the component for the process that generated the entry.

socket Indicates the subcomponent for the process that generated the entry.

e:\am600\src\mts\mtsclient.cpp
Indicates the name of the source file that generated the entry.

1832 Indicates the exact line number in the source file.

0x000001c4
Indicates the 32–bit thread ID in hexadecimal.

HPDCO1054E
Indicates the message ID.

Could not connect to the server acld2 on port 7137.
Indicates the message text.

Messages in XML log format

Figure 4 uses the message from Figure 3 on page 68, but shows the message in the XML log format.

```
<Message Id="HPDCO1054E" Severity="ERROR">
<Time Millis="1067220550984">2005-10-26-20:09:10.984</Time>
<Component>ivc/socket</Component>
<LogAttribs><KeyName><![CDATA[Message Number]]]</KeyName>
<Value><![CDATA[0x1354A41E]]]</Value>
</LogAttribs>
<Source
FileName="e:\am600\src\mts\mtsclient.cpp"
Method="unknown" Line="1832">
</Source>
<Process>pdmgrd</Process>
<Thread>0x000001c4</Thread>
<TranslationInfo
Type="XPG4" Catalog="pdbivc.cat" SetId="1" MsgKey="1354a41e">
<Param><![CDATA[acld2]]]</Param>
<Param><![CDATA[7137]]]</Param>
</TranslationInfo>
<LogText>
<![CDATA[HPDCO1054E Could not connect to the server acld2 on port 7137.]]
</LogText>
</Message>
```

Figure 4. Sample message entry in the XML log format

Environment variables

The message log behavior that is specified by a routing file can be changed by using environment variables. The PD_SVC_ROUTING_FILE environment variable can specify a fully qualified file name for a routing file to replace the one currently in use. If the file is not accessible, or does not exist, no change in logging messages is made.

Routing for messages of a specific severity can be manipulated by using environment variables as well. Set the appropriate message log entry format string to the wanted environment variable:

- SVC_FATAL
- SVC_ERROR
- SVC_WARNING
- SVC_NOTICE
- SVC_NOTICE_VERBOSE

For example, on Windows operating systems, the following command overrides the setting in the corresponding routing file and directs `WARNING` messages to the standard error device and a file:

```
SET SVC_WARNING="STDERR:-;FILE:D:\MSGS\MSG__WARNING.LOG"
```

See "Routing file entries" on page 52 for a description of message log entry format strings.

Displaying and not displaying environment variables in the log

On the computer on which the Security Access Manager server is running, you can configure environment variables to display or not display in the server log. Use the `PD_SVC_DISPLAY_ENV_VARS` or `PD_SVC_DONT_DISPLAY_ENV_VARS` environment variable to display or not display environment variables as required. Separate the environment variable keys by the "`|`" character.

PD_SVC_DISPLAY_ENV_VARS

Displays only the specified environment variables.

The following example shows how to set this environment variable on an AIX, Linux, or Solaris system:

```
export PD_SVC_DISPLAY_ENV_VARS="PATH|HOME|PWD"
```

The log displays only the `PATH`, `HOME`, and `PWD` environment variables display when the Security Access Manager server starts.

PD_SVC_DONT_DISPLAY_ENV_VARS

Displays all available environment variables except the specified environment variables.

The following example shows how to use this environment variable on an AIX, Linux, or Solaris system:

```
export PD_SVC_DONT_DISPLAY_ENV_VARS="LANG|PATH|PWD"
```

The log displays all environment variables except `LANG`, `PATH`, and `PWD` when the Security Access Manager server starts.

Notes:

- The PD_SVC_DISPLAY_ENV_VARS option takes precedence over the PD_SVC_DONT_DISPLAY_ENV_VARS option.
- If the value of one of the specified environment variables keys does not exist, Security Access Manager ignores that key.

Routing files for message events

Logging of message events is controlled by a routing file. Entries in the routing file for a server determine which message events to log. The server configuration files pick up the information from the routing files. If for any reason a routing file is deleted, the `log-file` stanza entry for the appropriate server is used instead.

Within routing files, you can disable or enable any type of message logs by adding or removing the comment character (#) at the beginning of the line in the routing file.

C runtime routing file

AIX, Linux, or Solaris: default routing file

```
FATAL:STDERR:-;FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__fatal.log
:644:ivmgr:ivmgr
ERROR:STDERR:-;FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__error.log
:644:ivmgr:ivmgr
WARNING:STDERR:-;FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__warning.log
:644:ivmgr:ivmgr
NOTICE:FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__notice.log
:644:ivmgr:ivmgr
#NOTICE_VERBOSE:STDERR:-;FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__verbose.log
:644:ivmgr:ivmgr
```

Windows: default routing file

```
FATAL:STDERR:-;FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__fatal.log
ERROR:STDERR:-;FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__error.log
WARNING:STDERR:-;FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__warning.log
NOTICE:FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__notice.log
#NOTICE_VERBOSE:STDERR:-;FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__verbose.log
```

Policy server pdmgrd_routing file

AIX, Linux, or Solaris: default routing file

```
FATAL:STDOUT:-;UTF8FILE:/pd_install_dir/log/msg__pdmgrd_utf8.log
:644:ivmgr:ivmgr
ERROR:STDOUT:-;UTF8FILE:/pd_install_dir/log/msg__pdmgrd_utf8.log
:644:ivmgr:ivmgr
WARNING:STDOUT:-;UTF8FILE:/pd_install_dir/log/msg__pdmgrd_utf8.log
:644:ivmgr:ivmgr
NOTICE:STDOUT:-;UTF8FILE:/pd_install_dir/log/msg__pdmgrd_utf8.log
:644:ivmgr:ivmgr
#NOTICE_VERBOSE:STDOUT:-;UTF8FILE:/pd_install_dir/log/
msg__pdmgrd_utf8.log:644:ivmgr:ivmgr
```

where *pd_install_dir* is either `/var/PolicyDirector` or the Tivoli Common Directory location.

Windows: default routing file

```
FATAL:STDERR:-;FILE:pd_install_dir\log\msg__pdmgrd_utf8.log
ERROR:STDERR:-;FILE:pd_install_dir\log\msg__pdmgrd_utf8.log
WARNING:STDERR:-;FILE:pd_install_dir\mog\msg__pdmgrd_utf8.log
NOTICE:FILE:pd_install_dir\log\msg__pdmgrd_utf8.log
#NOTICE_VERBOSE:STDOUT:-;UTF8FILE:pd_install_dir\log\
msg__pdmgrd_utf8.log
```

where *pd_install_dir* is either the directory where Security Access Manager is installed or the Tivoli Common Directory.

Authorization server pdacld_routing file

AIX, Linux, or Solaris: default routing file

```
FATAL:STDOUT:-;UTF8FILE:/pd_install_dir/log/msg__pdacld_utf8.log
:644:ivmgr:ivmgr
ERROR:STDOUT:-;UTF8FILE:/pd_install_dir/log/msg__pdacld_utf8.log
:644:ivmgr:ivmgr
WARNING:STDOUT:-;UTF8FILE:/pd_install_dir/log/msg__pdacld_utf8.log
:644:ivmgr:ivmgr
NOTICE:STDOUT:-;UTF8FILE:/pd_install_dir/log/msg__pdacld_utf8.log
:644:ivmgr:ivmgr
#NOTICE_VERBOSE:STDOUT:-;UTF8FILE:/pd_install_dir/log/
msg__pdacld_utf8.log:644:ivmgr:ivmgr
```

where *pd_install_dir* is either `/var/PolicyDirector` or the Tivoli Common Directory location.

Note: A log file name such as `msg__pdacld_utf8.log` applies to a default instance of the authorization server. If multiple instances of the authorization server exist, each log file contains the specified instance name. For example, if an authorization server instance name is `instance1`, the log file is called `msg__instance1-pdacld_utf8.log`.

Windows: default routing file

```
FATAL:STDOUT:-;UTF8FILE:pd_install_dir\log\msg__pdacld_utf8.log
ERROR:STDOUT:-;UTF8FILE:pd_install_dir\log\msg__pdacld_utf8.log
WARNING:STDOUT:-;UTF8FILE:pd_install_dir\log\msg__pdacld_utf8.log
NOTICE:STDOUT:-;UTF8FILE:pd_install_dir\log\msg__pdacld_utf8.log
#NOTICE_VERBOSE:STDOUT:-;UTF8FILE:pd_install_dir\log\
msg__pdacld_utf8.log
```

where *pd_install_dir* is either the directory where Security Access Manager is installed or the Tivoli Common Directory.

Note: A log file name such as `msg__pdacld_utf8.log` applies to a default instance of the authorization server. If multiple instances of the authorization server exist, each log file contains the specified instance name. For example, if an authorization server instance name is `instance1`, the log file is called `msg__instance1-pdacld_utf8.log`.

Policy proxy server pdmgrproxyd_routing file

AIX, Linux, or Solaris: default routing file

```
FATAL:STDOUT:-;UTF8FILE:/pd_install_dir/log/msg__pdmgrproxyd_utf8.log
:644:ivmgr:ivmgr
ERROR:STDOUT:-;UTF8FILE:/pd_install_dir/log/msg__pdmgrproxyd_utf8.log
:644:ivmgr:ivmgr
WARNING:STDOUT:-;UTF8FILE:/pd_install_dir/log/msg__pdmgrproxyd_utf8.log
```

```
:644:ivmgr:ivmgr
NOTICE:STDOUT:-;UTF8FILE:/pd_install_dir/log/msg__pdmgrproxyd_utf8.log
:644:ivmgr:ivmgr
#NOTICE_VERBOSE:STDOUT:-;UTF8FILE:/pd_install_dir/log/
msg__pdmgrproxyd_utf8.log:644:ivmgr:ivmgr
```

where *pd_install_dir* is either /var/PolicyDirector or the Tivoli Common Directory location.

Windows: default routing file

```
FATAL:STDOUT:-;UTF8FILE:pd_install_dir\log\msg__pdmgrproxyd_utf8.log
ERROR:STDOUT:-;UTF8FILE:pd_install_dir\log\msg__pdmgrproxyd_utf8.log
WARNING:STDOUT:-;UTF8FILE:pd_install_dir\log\msg__pdmgrproxyd_utf8.log
NOTICE:STDOUT:-;UTF8FILE:pd_install_dir\msg__pdmgrproxyd_utf8.log
#NOTICE_VERBOSE:STDOUT:-;UTF8FILE:pd_install_dir\log\
msg__pdmgrproxyd_utf8.log
```

where *pd_install_dir* is either the directory where Security Access Manager is installed or the Tivoli Common Directory.

WebSEAL routing file

By default WebSEAL writes all messages to the standard error device. When WebSEAL is running in the background, standard error is redirected to the msg__webseald-*instance_name*.log file.

AIX, Linux, or Solaris: default routing file

```
FATAL:STDERR:-
ERROR:STDERR:-
WARNING:STDERR:-
#NOTICE:FILE.10.100:pdweb_install_dir/log/msg__notice_%ld.log
:644:ivmgr:ivmgr
#NOTICE_VERBOSE:FILE.10.100:pdweb_install_dir/log/msg__verbose_%ld.log
:644:ivmgr:ivmgr
```

where *pdweb_install_dir* is either /var/pdweb or the Tivoli Common Directory location.

Windows: default routing file

```
FATAL:STDERR:-
ERROR:STDERR:-
WARNING:STDERR:-
#NOTICE:FILE.10.100:pdweb_install_dir/log/msg__notice_%ld.log
#NOTICE_VERBOSE:FILE.10.100:pdweb_install_dir/log/msg__verbose_%ld.log
```

where *pdweb_install_dir* is the value of the PD_WEB environment variable. The PD_WEB environment variable is set the WebSEAL installation directory during the initialization of the WebSEAL runtime environment.

Message routing files

To understand how default message logs work, review several of the default routing files.

C runtime routing file on Windows

The default routing file for the C runtime on a Windows operating system, %PD_HOME%\etc\routing, contains message log specifications similar to the specifications in Figure 5 on page 74.

```
FATAL:STDERR:-;FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__fatal.log
ERROR:STDERR:-;FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__error.log
WARNING:STDERR:-;FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__warning.log
NOTICE:FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__notice.log
#NOTICE_VERBOSE:STDERR:-;FILE:C:/PROGRA~1/Tivoli/POLICY~1/log/msg__verbose.log
```

Figure 5. Sample C runtime routing file

Using this routing file, messages are logged in the following manner:

- FATAL messages are sent to the standard error device as ASCII text in the current code page and locale and also are written to the C:/PROGRA~1/Tivoli/POLICY~1/log/msg__fatal.log file in the same format.
- ERROR messages are sent to the standard error device as ASCII text in the current code page and locale and also are written to the C:/PROGRA~1/Tivoli/POLICY~1/log/msg__error.log file in the same format.
- WARNING messages are sent to the standard error device as ASCII text in the current code page and locale and also are written to the C:/PROGRA~1/Tivoli/POLICY~1/log/msg__warning.log file in the same format.
- NOTICE messages are written to the C:/PROGRA~1/Tivoli/POLICY~1/log/msg__notice.log file only.
- NOTICE_VERBOSE messages are not captured, because this line starts with the number sign (#).

Policy server routing file on AIX, Linux, or Solaris

The default routing file for the policy server on a AIX, Linux, or Solaris operating system, /opt/PolicyDirector/etc/pdmgrd_routing, contains message log specifications similar to the specifications in Figure 6.

```
FATAL:STDOUT:-;UTF8FILE:/var/PolicyDirector/log/msg__pdmgrd_utf8.log:
644:ivmgr:ivmgr
ERROR:STDOUT:-;UTF8FILE:/var/PolicyDirector/log/msg__pdmgrd_utf8.log:
644:ivmgr:ivmgr
WARNING:STDOUT:-;UTF8FILE:/var/PolicyDirector/log/msg__pdmgrd_utf8.lo
g:644:ivmgr:ivmgr
NOTICE:STDOUT:-;UTF8FILE:/var/PolicyDirector/log/msg__pdmgrd_utf8.log
:644:ivmgr:ivmgr
#NOTICE_VERBOSE:STDOUT:-;UTF8FILE:/var/PolicyDirector/log/msg__pdmgrd
_utf8.log:644:ivmgr:ivmgr
```

Figure 6. Sample policy server routing file

With this routing file, messages are logged as follows:

- FATAL messages are written to the standard output device as ASCII text in the current code page and locale and written as UTF-8 text to the /var/PolicyDirector/log/msg__pdmgrd_utf8.log file. When the file is initially created, user ivmgr is the owner, ivmgr is the group, and 644 is the file permission.
- ERROR messages are written to the standard output device as ASCII text in the current code page and locale and written as UTF-8 text to the /var/PolicyDirector/log/msg__pdmgrd_utf8.log file. When the file is initially created, user ivmgr is the owner, ivmgr is the group, and 644 is the file permission.

- WARNING messages are written to the standard output device as ASCII text in the current code page and locale and written as UTF-8 text to the /var/PolicyDirector/log/msg__pdmgrd_utf8.log file. When the file is initially created, user ivmgr is the owner, ivmgr is the group, and 644 is the file permission.
- NOTICE messages are written to the standard output device as ASCII text in the current code page and locale and written as UTF-8 text to the /var/PolicyDirector/log/msg__pdmgrd_utf8.log file. When the file is initially created, user ivmgr is the owner, ivmgr is the group, and 644 is the file permission.
- NOTICE_VERBOSE messages are not written, because this line starts with the number sign (#).

WebSEAL routing file on AIX, Linux, or Solaris

The default routing file for a WebSEAL server on a AIX, Linux, or Solaris operating system, /opt/pdweb/etc/routing, contains message log specifications similar to the specifications in Figure 7.

```
FATAL:STDERR:-
ERROR:STDERR:-
WARNING:STDERR:-
#NOTICE:FILE.10.100:/var/pdweb/log/msg__notice_%ld.log
:644:ivmgr:ivmgr
#NOTICE_VERBOSE:FILE.10.100:/var/pdweb/log/msg__verbose_%ld.log
:644:ivmgr:ivmgr
```

Figure 7. Sample WebSEAL routing file

By removing the number sign (#) from the NOTICE specification and stopping and then restarting the WebSEAL server, NOTICE messages are written to a set of 10 files. Assuming that the process ID of the WebSEAL server is 1017, the names of the 10 files would be:

```
/var/pdweb/log/msg__notice_1017.log.1
/var/pdweb/log/msg__notice_1017.log.2
/var/pdweb/log/msg__notice_1017.log.3
/var/pdweb/log/msg__notice_1017.log.4
/var/pdweb/log/msg__notice_1017.log.5
/var/pdweb/log/msg__notice_1017.log.6
/var/pdweb/log/msg__notice_1017.log.7
/var/pdweb/log/msg__notice_1017.log.8
/var/pdweb/log/msg__notice_1017.log.9
/var/pdweb/log/msg__notice_1017.log.10
```

Message logging starts with the first file, /var/pdweb/log/msg__notice_1017.log.1. After 100 NOTICE messages are logged to that file, messages are written to the next file, /var/pdweb/log/msg__notice_1017.log.2. Message logging continues in this manner until 100 messages are written to the /var/pdweb/log/msg__notice_1017.log.10 file. At that point, the messages in the first file are deleted, and logging resumes again to the /var/pdweb/log/msg__notice_1017.log.1 file.

Note: By default WebSEAL writes all messages to the standard error device. When WebSEAL is running in the background, standard error is redirected to the msg__webseald-*instance_name*.log file.

Limiting the size of message logs

By default, message logs grow without limit. Limiting message log size requires that the directories and file systems that contain message log files must be checked on a periodic basis to ensure that enough space is available, and to prune the log files or make more space available as necessary.

The routing files can be modified to limit the amount of disk space that is used for message logs.

Consider the routing specification that is shown in Figure 8.

```
FATAL:STDOUT:-;UTF8FILE.10.100:/var/PolicyDirector/log/msg__pd
mgrd_fatal_utf8.log:644:ivmgr:ivmgr
ERROR:STDOUT:-;UTF8FILE.10.100:/var/PolicyDirector/log/msg__pd
mgrd__error_utf8.log:644:ivmgr:ivmgr
WARNING:STDOUT:-;UTF8FILE.5.1000:/var/PolicyDirector/log/msg__
pdmgrd_warning_utf8.log:644:ivmgr:ivmgr
NOTICE:STDOUT:-;UTF8FILE.5.1000:/var/PolicyDirector/log/msg__p
dmgrd_notice_utf8.log:644:ivmgr:ivmgr
NOTICE_VERBOSE:STDOUT:-;XMLFILE.10.500:/var/PolicyDirector/log
/msg__pdmgrd_verbose_utf8.xml:644:ivmgr:ivmgr
```

Figure 8. Multiple log files

All message files that are produced by this message log specification are of a determinate size, thus the maximum disk space that can be used by all of the files can be calculated.

Estimating the size of message logs

Each entry in a message log file with a destination of `FILE`, `TEXTFILE`, or `UTF8FILE` is an average of 200 bytes in size. The maximum size of any log file is 2 GB. To estimate the size of all the log files, in bytes, use the following equation:

```
200 × (Number of log files) × (Number of entries per log file)
```

For example, given the following specification:

```
NOTICE:UTF8FILE.10.1000:E:\LOGS\PDPROXYMGRD.LOG
```

The maximum size for the `PDPROXYMGRD.LOG` file would be approximately (`200 × 10 × 1000`) or 2,000,000 bytes.

Each entry in a message log file with a destination of `XMLFILE` is an average of 650 bytes in size. Therefore, the maximum size of a log file, in bytes, can be estimated using the following equation:

```
650 × (Number of log files) × (Number of entries per log file)
```

For example, given the following specification:

```
NOTICE:XMLFILE.10.500:E:\LOGS\MSG__NOTICE.XML
```

The maximum size for the `MSG__NOTICE.XML` file would be approximately (650 × 10 × 500) or 3,250,000 bytes.

Changing the location of log files

About this task

To change the directory for a server-specific message log file, complete the following steps:

Procedure

1. Go to the directory where the routing file is located. The default location for the Security Access Manager servers is one of the following operating system-specific locations:

   AIX, Linux, and Solaris operating systems
   `/opt/PolicyDirector/etc/`

   Windows operating systems
   `%PD_HOME%\etc\`

   The default location for a WebSEAL server is one of the following operating system-specific locations:

   AIX, Linux, and Solaris operating systems
   `/opt/pdweb/etc/`

   Windows operating systems
   `%PD_WEB%\etc\`

2. Edit the appropriate server-related routing file. The following list contains the names of the routing files:

   `pdmgrd_routing`
   The routing file for the policy server

   `pdacld_routing`
   The routing file for the authorization server

   `pdmgrproxyd_routing`
   The routing file for the policy proxy server

   `routing`
   The routing file that is used for the C runtime

   `routing`
   The routing file for the WebSEAL server

   Note: Although the routing file for the C runtime and the WebSEAL server have the same file name, these files are in different directories.

3. Locate the statement that define message logs, and change the location for the message log files. The following example changes the routing file for the policy server on a UNIX system to log all messages (except `NOTICE_VERBOSE` to `/myTAMlogs/msg__pdmgrd_utf8.log` log file:

   ```
   FATAL:STDOUT:-;UTF8FILE:/myTAMlogs/msg__pdmgrd_utf8.log:644:ivmgr:ivmgr
   ERROR:STDOUT:-;UTF8FILE:/myTAMlogs/msg__pdmgrd_utf8.log:644:ivmgr:ivmgr
   WARNING:STDOUT:-;UTF8FILE:/myTAMlogs/msg__pdmgrd_utf8.log:644:ivmgr:ivmgr
   NOTICE:STDOUT:-;UTF8FILE:/myTAMlogs/msg__pdmgrd_utf8.log:644:ivmgr:ivmgr
   #NOTICE_VERBOSE:STDOUT:-;UTF8FILE:/myTAMlogs/msg__pdmgrd_utf8.log
      :644:ivmgr:ivmgr
   ```

4. Save and exit the routing file.

Results

Tip: Periodically prune the log files to prevent them from becoming too large. The maximum file size is 2 GB.

Logging all messages the same way

To send all runtime messages to a single file regardless of severity, the routing specification that is shown in Figure 9 can be used in the /opt/PolicyDirector/etc/routing file.

```
*:UTF8FILE:/tmp/msg__amrte_utf8.log:666:ivmgr:ivmgr
```

Figure 9. Sending all messages to one location

Using GOESTO statements

To send all policy server messages to a single file and also send FATAL and ERROR messages to the standard error device, the /opt/PolicyDirector/etc/pdmgrd_routing file can be modified as shown in Figure 10.

```
FATAL:STDERR:-;GOESTO:NOTICE_VERBOSE
ERROR:STDERR:-;GOESTO:NOTICE_VERBOSE
WARNING:GOESTO:NOTICE_VERBOSE
NOTICE:GOESTO:NOTICE_VERBOSE
NOTICE_VERBOSE:UTF8FILE:/tmp/msg__pdmgrd_utf8.log:644:ivmgr:ivmgr
```

Figure 10. Using GOESTO to send messages

FATAL messages are sent to STDERR, and then to the same destinations as NOTICE_VERBOSE messages, namely written as UTF-8 text to the /tmp/msg__pdmgrd_utf8.log file.

Changing the message format in log files

About this task

To change the message format for a server-specific message log file, complete the following steps:

Procedure

1. Go to the directory where the routing file is located. The default location for the Security Access Manager servers is one of the following operating system-specific locations:

   AIX, Linux, and Solaris operating systems

   /opt/PolicyDirector/etc/

   Windows operating systems

   %PD_HOME%\etc\

   The default location for a WebSEAL server is one of the following operating system-specific locations:

   AIX, Linux, and Solaris operating systems

   /opt/pdweb/etc/

Windows operating systems
%PD_WEB%\etc\

2. Edit the appropriate server-related routing file. The following list contains the names of the routing files:

   pdmgrd_routing
   The routing file for the policy server

   pdacld_routing
   The routing file for the authorization server

   pdmgrproxyd_routing
   The routing file for the policy proxy server

   routing
   The routing file that is used for the C runtime

   routing
   The routing file for the WebSEAL server

   Note: Although the routing file for the C runtime and the WebSEAL server have the same file name, these files are in different directories.

3. Find the statement that defines how to log messages of a specific severity. For example, find the ERROR statement in the routing file to change the logging of error messages. The ERROR statement might be similar the following statement:

   ```
   ERROR:STDOUT:-;UTF8FILE:pd_install_dir/log/msg__pdmgrd_utf8.log
   :644:ivmgr:ivmgr
   ```

   where *pd_install_dir* is either /var/PolicyDirector or the directory that is defined by the tivoli_common_dir stanza entry of the pd.conf configuration file (/var/ibm/tivoli/common).

   For example, to log error messages in the XML format and to log these messages to the msg__error.log file, make the following changes:

   a. Change UTF8FILE to XMLFILE
   b. Change msg__pdmgrd_utf8.log to msg__error.log

   The following statement is the result of these changes:

   ```
   ERROR:STDOUT:-;XMLFILE:pd_install_dir/log/msg__error.log
   :644:ivmgr:ivmgr
   ```

4. Save and exit the routing file.

Results

After this statement is changed, ERROR messages are written to the standard output device in ASCII text and written to the msg__error.log file in the XML format.

Sending messages to multiple places in different formats

To send FATAL, ERROR, and WARNING messages from the authorization server to the standard output device as ASCII text, to a file as UTF-8 text, and to another file in XML log format, the specification that is shown in Figure 11 on page 80 can be used in the %PD_HOME%\etc\msg__pdacld.routing file.

```
FATAL:STDOUT:-;UTF8FILE:C:\LOGS\MSG__PDACLD_%LD.LOG;XMLFILE:C:\XMLLO
GS\MSG__PDACLD_%LD.XML
ERROR:STDOUT:-;UTF8FILE:C:\LOGS\MSG__PDACLD_%LD.LOG;XMLFILE:C:\XMLLO
GS\MSG__PDACLD_%LD.XML
WARNING:STDOUT:-;UTF8FILE:C:\LOGS\MSG__PDACLD_%LD.LOG;XMLFILE:C:\XML
LOGS\MSG__PDACLD_%LD.XML
NOTICE:UTF8FILE:C:\LOGS\MSG__PDACLD_%LD.LOG;XMLFILE:C:\XMLLOGS\MSG__
PDACLD_%LD.XML
NOTICE_VERBOSE:UTF8FILE:C:\LOGS\MSG__PDACLD_%LD.LOG;XMLFILE:C:\XMLLO
GS\MSG__PDACLD_%LD.XML
```

Figure 11. Sending messages to standard output to file in UTF-8, and to file in XML format

After you stop and restart the authorization server to pick up the changes to the routing file and assuming that the process ID of the authorization server is 1253, the following files are created to contain messages:

- `C:\PDACLD_LOGS\MSG__PDACLD_1253.LOG`
- `C:\PDACLD_XMLLOGS\MSG__PDACLD_1253.XML`

You can use the XML Log Viewer to analyze the XML file. For instructions on installing and using this viewer, see “Viewing log files with the XML Log Viewer” on page 9.

Chapter 12. Trace event logs

Security Access Manager provides configurable tracing capabilities that can aid in problem determination. Unlike message logs, trace logs (or tracing) are *not* enabled by default.

Trace data is intended primarily for use by IBM Software Support. Trace data might be requested as part of diagnosing a reported problem. However, experienced product administrators can use trace data to diagnose and correct problems in a Security Access Manager environment.

Attention: Use trace with caution. It is intended as a tool to use under the direction of IBM Software Support. Messages from tracing are sometimes cryptic, are not translated, and can severely degrade system performance.

Trace logs are best suited to situations where a problem is easily reproduced, is short-lived in duration, and can be produced without significant trace generation from other system activity. Enabling tracing can adversely affect the performance of Security Access Manager and its associated products and applications.

Tracing can be activated when servers, daemons, and applications start by using routing files and Java properties files. In some cases, tracing can be activated dynamically by using the **`server task trace`** command with the **`set`** option.

Note: Tracing from the C-language portions of Security Access Manager is controlled through routing files. Similarly, tracing from the Java language portions of Security Access Manager is controlled through Java properties files. When relevant, the distinction between these two methods of trace handling is mentioned.

Mechanisms for controlling trace logs

There are different trace log techniques that are used, depending on which component is being logged.

Tracing can be controlled by using the following mechanisms:

routing file
A routing file can be used to control tracing of the policy server, authorization server, policy proxy server, WebSEAL, and runtime components. An affected component must be stopped and restarted for modifications to the routing file to take effect.

Note: Plug-in for Web Servers has no routing file. Plug-in for Web Servers programmatically sets the information that is typically contained in a routing file.

Java properties file
A Java properties file can be used to control tracing of the IBM Security Access Manager Runtime for Java and Web Portal Manager components.

trace command
The **`server task trace`** command can be used to dynamically control trace operations for the authorization server, policy proxy server, WebSEAL, and

Plug-in for Web Servers components. This command can also be used to control trace operations for custom C applications that were developed by using the Security Access Manager authorization C APIs.

WebSphere Application Server trace log
Trace logging for the session management server is handled by using the WebSphere Application Server trace log facilities. See "Trace logging for session management" on page 88 for more information.

Managing Trace

Tracing can be activated either through a routing file or through a Security Access Manager server task administrative command.

The following information outlines details of the second method. For details on how to activate tracing through a routing file, see Chapter 9, "Customize logging events with routing files," on page 51.

The **`server task trace`** command can be used to dynamically control trace operations. As with other Security Access Manager administrative functions, the trace command can be issued through either the **`pdadmin`** utility or programmatically through the Security Access Manager Administrative API.

Different **`pdadmin`** commands are available to:

- List all of the available trace points.
- Change the level and destination for specific trace points.
- Retrieve the trace point level for specific trace points.

Listing all trace commands

To list all of the trace components that are offered by a server, issue the trace list command:

```
server task server name trace list
```

Where *server name* specifies the name of the server on which you want to collect trace information.

```
pdadmin> server task PDWebPI-webpi.gc.au.ibm.com trace list
pdwebpi.request
pdwebpi.response
...
```

Adjusting the trace level of a component

To change the level and destination for a specific trace point, use the following command:

```
server task <server name> trace set <component> \
<level> [file path=file|other-log-agent-config]
```

Where:

server name
Specifies the name of the server on which you want to collect trace information.

component
Specifies the name of trace component as shown by the list command.

level Controls the amount of detail to be gathered, in the range of 1 to 9, with 1 collecting the least number of traces, and 9 collecting the most number of traces.

file path
The optional **`file path`** parameter specifies the location for trace output. If this parameter is not supplied, the trace output is sent to the `stdout` stream of the server.

The following example sets the trace level to 9 for the **`pdwebpi.request`** component. Any output that is generated is sent to the `/tmp/log.txt` file on the WebPI server.

```
pdadmin> server task PDWebPI-wpi.com trace set pdwebpi.request 9
file path=/tmp/log.txt
```

Retrieving the current trace level of a component

To show the names and levels for all enabled trace components, use the following command:

```
server task server-name trace show [component]
```

If the optional **`component`** parameter is omitted, the output lists the name and level of all of the enabled trace components.

```
pdadmin>server task PDWebPI-wpi.ibm.com trace show pdwebpi.request 9
```

Routing file examples

To illustrate features available with the routing files, several examples are provided.

Trace logging in XML log format

To send trace output for the authorization server to a single file in XML log format, the `install_dir/etc/msg__pdacld.routing` file can be modified as follows:

```
*:*.9:XMLFILE:E:\PDACLD_XMLTRACE\TRACE__PDACLD_%LD.XML
```

After you stop and restart the authorization server to pick up the routing file change, and assuming that the process ID of the authorization server is 412, trace output is written to the following file:

```
E:\PDACLD_XMLTRACE\TRACE__PDACLD_412.XML
```

Use the XML Log Viewer to analyze the XML file produced. See "Viewing log files with the XML Log Viewer" on page 9 for instructions on installing and using the viewer.

Trace logging to multiple files

By default, trace logs grow without limit. This requires that the directories and file systems that contain trace log files be checked on a periodic basis to ensure that enough space is available, and to prune the log files or make more space available as necessary.

The routing files can be modified to limit the amount of disk space that is used for trace logs.

To send runtime trace output, from reporting levels 1 through 5, to 10 different files, each containing a maximum of 10000 trace entries, the routing specification that is shown in Figure 12 on page 84 can be used in the `/opt/PolicyDirector/`

`etc/routing` file.

```
*:*.5:UTF8FILE.10.10000:/tmp/trace__am_utf8.log:666:ivmgr:ivmgr
```

Figure 12. Sending trace output to multiple files

Tracing starts with the first file, `/tmp/trace__am_utf8.log.1`. After 10000 trace entries are logged to that file, trace entries are written to the second file, `/tmp/trace__am_utf8.log.2`. Tracing continues in this manner until 10000 trace entries are written to the `/tmp/trace__am_utf8.log.10` file. At that point, the trace entries in the first file are deleted, and tracing resumes again to the `/tmp/trace__am_utf8.log.1` file.

Tracing a particular component

At the direction of IBM Software Support, you might be asked to enable tracing for a particular component of Security Access Manager. For example, if asked to trace the `mgr` component of the policy server, the `/opt/PolicyDirector/etc/pdmgrd_routing` file can be modified as shown in Figure 13.

```
mgr:*.9:UTF8FILE:/tmp/trace__pdmgrd_mgr_9_utf8.log:644:ivmgr:ivmgr
```

Figure 13. Tracing a component

Determining maximum size of a trace log

Each entry that is made to a trace log file created that uses a destination of `FILE`, `TEXTFILE`, or `UTF8FILE` is an average of 200 bytes in size. The maximum size of a log file, in bytes, can be estimated as follows:

```
200 × (Number of log files) × (Number of entries per log file)
```

For example, given a specification of:

```
*:*.9:TEXTFILE.10.10000:C:/PROGRA~1/Tivoli/POLICY~1/log/trace__%ld.log
```

The maximum size would be approximately (`200 × 10 × 10000`) or 20,000,000 bytes.

Trace entries that are written in XML log format are an average of 500 bytes in size, thus for a specification of:

```
*:*.9:XMLFILE.10.10000:/var/dbug20031028A/trace__%ld.xml
```

The maximum size would be approximately (`500 × 10 × 10000`) or 50,000,000 bytes.

Enabling trace

About this task

To enable tracing during startup and be able to view trace records, complete the following steps:

Procedure

1. Edit the appropriate routing file for the server. The following list contains the names of the routing files

   `pdmgrd_routing`
   The routing file for the Security Access Manager policy server

pdacld_routing
The routing file for the Security Access Manager authorization server

pdmgrproxyd_routing
The routing file for the Security Access Manager policy proxy server

2. Add a line similar to the following to the routing file:

   ```
   *:*.9:TEXTFILE:pd_install_dir/log/trace_%ld.log
   ```

   where, on a Windows operating system, *pd_install_dir* is either the directory where Security Access Manager is installed or the Tivoli Common Directory location.

   Or, remove the number sign (#) at the beginning of this line, if it exists in the routing file, to allow viewing of trace records.
3. Change this line, if you want to log in this debug trace data XML log format. For example, you can change the line to send the output to an XML file instead of a text file:

   ```
   *:*.9:XMLFILE.10.1000:pd_install_dir/log/trace__%ld.log;XMLSTDERR:-
   ```

   where, on a AIX, Linux, or Solaris operating system, *pd_install_dir* is either `/var/PolicyDirector` or the Tivoli Common Directory location.

Using the trace commands

Use the **server tasks trace** command that is provided as by the **pdadmin** utility to manage trace components. You can use the **trace** command to complete the following operations:

trace list
List all available trace components

trace set
Enable the trace level and trace message destination for a component and its subordinates

trace show
Show the name and level for all enabled trace components or for the specified component

For more information about the **server task trace** command, see “server task trace” on page 176.

Listing available trace components

List the specified component or all components available to gather and report trace information.

```
trace list [component]
```

The trace components themselves are organized in a hierarchical fashion. If trace is activated for a parent trace component, it will automatically be activated for all children trace components. As an example, if you activate trace for the component: *pdweb.snoop*, tracing for the sub-component, *pdweb.snoop.jct* will also be activated.

Enabling trace

Use the **server task trace set** command to enable the gathering of trace information for the specified component and level.

```
trace set component level [file path=file | log_agent]
```

where:

component
: The trace component name. This required argument indicates the component to be enabled. WebSEAL components are prefixed with `pdweb`.

level Reporting level. This required argument must be in the range of 1 to 9. The *level* argument specifies the number of details that are gathered by the **trace** command. Level 1 indicates the least detailed output, and level 9 indicates the most detailed output.

file The fully qualified name of the file to which trace data is written.

log_agent
: Optionally specifies a destination for the trace information that is gathered for the specified component. See the event log information in the *IBM Security Access Manager for Web Administration Guide* for details.

Showing enabled trace components

List all enabled trace components or a specific enabled component. If a specified component is not enabled, no output is displayed.

```
trace show [component]
```

Example:

```
pdadmin> server task webseald-instance trace set pdweb.debug 2
pdadmin> server task webseald-instance trace show pdweb.debug 2
```

Changing the name and location of trace files

Trace log file locations and names depends on which Security Access Manager component is being traced. For the Security Access Manager authorization server, the trace log file can be explicitly specified by the user in the following command:

```
pdadmin> server task server-name trace set component level [file path=file]
```

where *server-name* is the name of the authorization server that is displayed by the **server list** command, and *file* is the fully qualified trace file name.

Alternatively, if the Security Access Manager routing file is being used to enable and disable tracing, then the location and name of this trace log file can be defined within the routing file.

For WebSEAL, the trace log file can be explicitly specified by the user in the following command:

```
pdadmin> server task server-name trace set component level [file path=file]
```

where *server-name* is the name of the WebSEAL server that is displayed by the **server list** command, and *file* is the fully qualified trace file name.

Alternatively, if the WebSEAL routing file is being used to enable and disable tracing, then the location and name of this trace log file can be defined within the routing file.

For the Security Access Manager Plug-in for Web Servers component, message log entries and trace log entries are always written, by default, to the same set of files when the Tivoli Common Directory is not configured. These include:

Windows operating systems
: Log for the authorization server: *`webpi_install_dir`*`\log\msg__pdwebpi.log`

Log for the IIS plug-in: `*webpi_install_dir*\log\msg__pdwebpi-iis.log`

AIX, Linux, and Solaris operating systems

Log for the authorization server: `/var/pdwebpi/log/msg__pdwebpi.log`

Log for the watchdog server: `/var/pdwebpi/log/msg__pdwebpimgr.log`

Format of trace entry in logs

Figure 14 shows an example of a trace entry that is taken from a Security Access Manager trace log file.

```
2005-10-29-18:01:06.984-06:00I——- pdmgrd DEBUG8 mgr general
e:\am600\src\ivmgrd\pdmgrapi\MrMgmtDomainMan.cpp 736 0x000007d0
CII ENTRY: MrMgmtDomainMan::setCurrentDomainName
```

Figure 14. Sample trace log entry in text format

The following list describes the trace entry that is shown in Figure 14.

2005-10-29-18:01:06.984-06:00I

Indicates the timestamp of the trace entry. Timestamp is in the following format: `YYYY–MM–DD–hh:mm:ss.fff[+|–]hh:mmI`

where:

YYYY-MM-DD

Specifies the date in year, month, and day.

hh:mm:ss.fff

Specifies the time in hours, minutes, seconds, and fractional seconds.

hh:mmI

Specifies the time inaccuracy factor

pdmgrd

Indicates the name of the process which created the entry.

DEBUG8

Indicates the reporting level of the trace entry.

mgr Indicates the component for the process that generated the entry.

general

Indicates the subcomponent for the process that generated the entry.

e:\am600\src\ivmgrd\pdmgrapi\MrMgmtDomainMan.cpp

Indicates the name of the product source file that generated the entry.

736 Indicates the exact line number in source file.

0x000007d0

Indicates the thread ID in hexadecimal.

CII ENTRY: MrMgmtDomainMan:setCurrentDomainName

Indicates the text of the trace entry.

Trace logging for session management

Trace logging for the session management server is handled with the WebSphere Application Server trace log facilities. For each instance of a session management server, you can configure a trace component by using the administrative console. Use the following name to configure a trace component for a session management server instance:

```
com.tivoli.am.sms.instance_idtrace
```

Session management server trace output is stored in the same file as other WebSphere Application Server trace output, usually `trace.log` in the server log directory.

Trace output for a Security Access Manager session management server instance is generated in three levels of detail: fine (event), finer (entryExit), and finest (debug). For performance reasons, do not set session management trace logs to generate a finer or finest level of detail unless you are directed to do so by IBM Software Support.

Information about configuring WebSphere Application Server for trace logs is available in the WebSphere Application Server information center:

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp

Trace logging for WebSEAL

This section describes some of the options available for trace logs for WebSEAL.

WebSEAL provides the following components to trace HTTP requests:
- pdweb.debug
- pdweb.snoop

Note: The amount of data that is produced by the trace options, especially by the snoop trace command, can be large.

pd.ivc.ira trace for LDAP server interaction

The **`pd.ivc.ira`** component traces Security Access Manager interaction with the LDAP server. This trace component can apply to both WebSEAL and Plug-in for Web Servers.

The trace helps with determining problems that occur during authentication. This trace can show the following information:
- The LDAP search path that is used during the search for a user
- Whether authentication succeeded for the user
- Whether any policy (for example, password, time-of-day) took effect

This information helps to identify Security Access Manager problems that originate from the LDAP server. The trace also shows the general interaction with the local user registry cache.

If the trace level is set to 7, approximately 30 lines of trace are produced for every transaction. This trace level mostly shows the authentication process. It can be used to determine whether a DN for the user was successfully located, and whether authentication for the user succeeded.

If the trace level is set to 8, approximately 170 lines of trace are produced for every transaction. In addition to the authentication process, this trace level logs the steps that are involved in validating the user policy. It also shows some interaction with the local user registry cache.

The following sample output is an extract of the trace that is produced during a standard authentication for a trace level of 8. The output shows that the user, `scotte`, was successfully authenticated and that the DN of the user is `cn=Scott Exton,o=ibm,c=au`.

Example pd.ivc.ira output (extract)

```
...
2007-03-09-14:31:00.329+10:00I----- thread(2) trace.pd.ivc.ira:8 /project/am610/build/am61
0/src/ivrgy/ira_auth.c:1221: CII ENTRY: ira_get_dn_utf8() parm: scotte
...
2007-03-09-14:31:00.329+10:00I----- thread(2) trace.pd.ivc.ira:7 /project/am610/build/am61
0/src/ivrgy/ira_entry.c:2879: ira_ldap_search_ext_s() base: SECAUTHORITY=DEFAULT scope: 2
filter: (secDomainId=Default%scotte)
2007-03-09-14:31:00.329+10:00I----- thread(2) trace.pd.ivc.ira:7 /project/am610/build/am61
0/src/ivrgy/ira_ldap.c:3009: ira_ldap_search_ext_s(): No timeout - calling ldap_search_ext
_s
2007-03-09-14:31:00.331+10:00I----- thread(2) trace.pd.ivc.ira:7 /project/am610/build/am61
0/src/ivrgy/ira_ldap.c:3029: ira_ldap_search_ext_s: Returning LDAP rc x0
...
2007-03-09-14:31:00.332+10:00I----- thread(2) trace.pd.ivc.ira:8 /project/am610/build/am61
0/src/ivrgy/ira_auth.c:1738: CII ENTRY: ira_authenticate_user3() parm: cn=Scott Exton,o=ib
m,c=au
...
2007-03-09-14:31:00.334+10:00I----- thread(2) trace.pd.ivc.ira:8 /project/am610/build/am61
0/src/ivrgy/ira_auth.c:1596: CII EXIT ira_auth_passwd_compare() with status:  0x00000000
...
2007-03-09-14:31:00.334+10:00I----- thread(2) trace.pd.ivc.ira:8 /project/am610/build/am61
0/src/ivrgy/ira_cache.c:1588: CII EXIT ira_cache_user_get_account_state() with status:  0x
00000000
...
2007-03-09-14:31:00.340+10:00I----- thread(2) trace.pd.ivc.ira:8 /project/am610/build/am61
0/src/ivrgy/ira_auth.c:2160: CII EXIT ira_authenticate_user3() with status:  0x00000000
```

pdweb.debug trace of HTTP header requests and responses

The pdweb.debug component traces the HTTP headers for requests and responses.

The pdweb.debug component operates at level 2 only. To log the message body, see "pdweb.snoop trace of HTTP traffic with WebSEAL" on page 90.

The following example command starts the trace utility for the pdweb.debug component at level 2 and directs the output to a file:

```
pdadmin> server task webseald-instance trace set pdweb.debug 2 \
file path=/opt/pdweb/log/debug.log
```

Sample output of this command as it displays in the `debug.log` file:

```
2012-08-10-23:42:19.725+00:00I----- thread(7) trace.pdweb.debug:2
/amweb600/src/wand/wand/log.c:278: ------------- Browser ===> PD -------------
Thread_ID:27
GET /junction/footer.gif HTTP/1.1
Accept: */*
Referer: https://bevan/junction/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
If-Modified-Since: Wed, 11 Jul 2009 21:11:14 GMT
If-None-Match: "abe09-3c8-3b4cc0f2"
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705)
Host: bevan
Connection: Keep-Alive
--------------------------------------------------
```

```
2012-08-10-23:42:19.736+00:00I----- thread(7) trace.pdweb.debug:2
/amweb600/src/wand/wand/log.c:278: ------------- PD ===> BackEnd -------------
Thread_ID:27
GET /footer.gif HTTP/1.1
via: HTTP/1.1 bevan:443
host: blade.cruz.ibm.com:444
user-agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705)
accept: */*
accept-language: en-us
accept-encoding: gzip, deflate
if-none-match: "abe09-3c8-3b4cc0f2"
referer: https://bevan/blade/
if-modified-since: Wed, 11 Jul 2009 21:11:14 GMT
connection: close
---------------------------------------------------

2012-08-10-23:42:19.739+00:00I----- thread(7) trace.pdweb.debug:2
/amweb600/src/wand/wand/log.c:278: ------------- PD <=== BackEnd -------------
Thread_ID:27
HTTP/1.1 304 Not Modified
date: Wed, 10 Aug 2012 23:34:17 GMT
etag: "abe09-3c8-3b4cc0f2"
server: IBM_HTTP_SERVER/1.3.19.1Apache/1.3.20 (Unix)
connection: close
---------------------------------------------------

2012-08-10-23:42:19.740+00:00I----- thread(7) trace.pdweb.debug:2
/amweb600/src/wand/wand/log.c:278: ------------- Browser <=== PD ------------
Thread_ID:27
HTTP/1.1 304 Not Modified
date: Wed, 10 Aug 2012 23:34:17 GMT
etag: "abe09-3c8-3b4cc0f2"
server: IBM_HTTP_SERVER/1.3.19.1Apache/1.3.20 (Unix)
---------------------------------------------------
```

pdweb.snoop trace of HTTP traffic with WebSEAL

The pdweb.snoop component traces HTTP traffic. This component logs the HTTP headers and the message body for requests and responses.

Note: The snoop component traces the entire request and response as it is read off the socket. This trace might contain sensitive information.

The pdweb.snoop component has the following subcomponents:

pdweb.snoop.client
Traces data that is sent between WebSEAL and clients.

pdweb.snoop.jct
Traces data that is sent between WebSEAL and junctions.

To trace only the message headers, see “pdweb.debug trace of HTTP header requests and responses” on page 89.

The following example command starts the trace utility for the pdweb.snoop component at level 9 and directs the output to a file:

```
pdadmin> server task webseald-instance trace set pdweb.snoop 9 \
file path=/tmp/snoop.out
```

The following sample output shows the WebSEAL server that is sending 2137 bytes of data to a client at IP address 10.4.5.12:

```
----------------------------------------
2012-08-10-19:35:18.541+00:00I----- thread(5) trace.pdweb.snoop.client:1
/home/amweb600/src/pdwebrte/webcore/amw_snoop.cpp:159:
----------------------------------------
Thread 2828; fd 22; local 10.4.5.10:443; remote 10.4.5.12:1250
Sending 2137 bytes
0x0000   4854 5450 2f31 2e31 2034 3033 2046 6f72        HTTP/1.1.403.For
0x0010   6269 6464 656e 0d0a 6461 7465 3a20 5475        bidden..date:.We
0x0020   652c 2032 3820 4f63 7420 3230 3033 2031        d,.10.Aug.2005.1
0x0030   393a 3335 3a31 3820 474d 540d 0a73 6572        9:35:18.GMT..ser
0x0040   7665 723a 2057 6562 5345 414c 2f35 2e31        ver:.WebSEAL/5.1
0x0050   2e30 2e30 2028 4275 696c 6420 3033 3130        .0.0.(Build.0310
0x0060   3230 290d 0a63 6163 6865 2d63 6f6e 7472        20)..cache-contr
0x0070   6f6c 3a20 6e6f 2d63 6163 6865 0d0a 7072        ol:.no-cache..pr
0x0080   6167 6d61 3a20 6e6f 2d63 6163 6865 0d0a        agma:.no-cache..
0x0090   636f 6e74 656e 742d 6c65 6e67 7468 3a20        content-length:.
0x00a0   3139 3038 0d0a 7033 703a 2043 503d 224e        1908..p3p:.CP="N
0x00b0   4f4e 2043 5552 204f 5450 6920 4f55 5220        ON.CUR.OTPi.OUR.
0x00c0   4e4f 5220 554e 4922 0d0a 636f 6e74 656e        NOR.UNI"..conten
...
```

pdweb.wan.azn trace for transaction authorization decisions

The **pdweb.wan.azn** component traces authorization decisions for all transactions.

The trace information includes:

- Credential details upon which the authorization decision is made.
- The resource that is accessed.
- The result of the authorization decision.

The following sample output is an extract of the trace which is produced from a single authorization decision.

Example pdweb.wan.azn output (extract)

```
...
2007-03-09-16:12:35.195+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:95: [10.251.140.1] Dumping attrlist: creds
2007-03-09-16:12:35.195+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AUTHENTICATI
ON_LEVEL , Value: 1

2007-03-09-16:12:35.195+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_AUT
HNMECH_INFO , Value: LDAP Registry

2007-03-09-16:12:35.195+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_AUT
HZN_ID , Value: cn=Scott Exton,o=ibm,c=au

2007-03-09-16:12:35.196+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_AUT
H_METHOD , Value: password

2007-03-09-16:12:35.196+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_BRO
WSER_INFO , Value: curl/7.12.1 (i386-redhat-linux-gnu) libcurl/7.12.1 OpenSSL/0.9.7a zlib/
1.2.1.2 libidn/0.5.6

2007-03-09-16:12:35.196+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_IP_
FAMILY , Value: AF_INET

2007-03-09-16:12:35.196+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_MEC
H_ID , Value: IV_LDAP_V3.0

2007-03-09-16:12:35.196+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_NET
WORK_ADDRESS_BIN , Value: 0x0afb8c01
```

```
2007-03-09-16:12:35.196+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_NET
WORK_ADDRESS_STR , Value: 10.251.140.1

2007-03-09-16:12:35.196+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_PRI
NCIPAL_DOMAIN , Value: Default

2007-03-09-16:12:35.196+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_PRI
NCIPAL_NAME , Value: scotte

2007-03-09-16:12:35.196+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_PRI
NCIPAL_UUID , Value: ad987b08-cdf4-11db-a51a-000c29e9c358

2007-03-09-16:12:35.196+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_QOP
_INFO , Value: SSK: TLSV1: 35

2007-03-09-16:12:35.196+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_REG
ISTRY_ID , Value: cn=Scott Exton,o=ibm,c=au

2007-03-09-16:12:35.196+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_USE
R_INFO , Value:

2007-03-09-16:12:35.197+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:AZN_CRED_VER
SION , Value: 0x00000600

2007-03-09-16:12:35.197+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:tagvalue_log
in_user_name , Value: scotte

2007-03-09-16:12:35.197+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:117: [10.251.140.1] Attr Name:tagvalue_ses
sion_index , Value: 2c5bfdba-ce05-11db-bba0-000c29e9c358

...

2007-03-09-16:12:35.197+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:233: [10.251.140.1] INPUTS - protected_res
ource=/WebSEAL/webpi.vwasp.gc.au.ibm.com-default/index.html, operation=r

...

2007-03-09-16:12:35.198+10:00I----- thread(5) trace.pdweb.wan.azn:9 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:254: [10.251.140.1] OUTPUT - permission=0

...

2007-03-09-16:12:35.198+10:00I----- thread(5) trace.pdweb.wan.azn:8 /project/amwebrte610/b
uild/amwebrte610/src/pdwebrte/webcore/amw_azn.c:261: [10.251.140.1] CII EXIT amw_azn_decis
ion_access_allowed_ext with status=0x00000000
```

Setting trace for Security Access Manager SPNEGO issues

When a problem occurs, IBM Support might ask you to enable trace for SPNEGO.

Before you begin

Ensure enough disk space is available in the `/var` directory.

About this task

When directed by IBM Support, collect the SPNEGO diagnostic data when WebSEAL does not start.

Procedure

1. Add an entry to the WebSEAL routing file. The routing file is in *WebSEAL_installation_directory*/etc/routing. Example entry that directs output to the spnegotrace.log file:

   ```
   bst:*.9:TEXTFILE:WebSEAL_installation_directory/log/spnegotrace.log
   ```

2. Turn on per-process trace to diagnose WebSEAL start-up issues:
   a. Open the /opt/pdweb/etc/routing file.
   b. Uncomment the last line by removing the # symbol. For example:

   ```
   #Route to a per-process text file
   *:*.9:TEXTFILE.10.1000:/var/pdweb/log/trace__%ld.trace.log:644:ivmgr:ivmgr
   ```

   c. Stop and restart WebSEAL.
   d. Check the output in the following file: /var/pdweb/log/trace__*pid*.trace.log.

   Note: If you start WebSEAL with the **pdweb_start** command, there are two traces with different pids.

Trace Logging for Plug-in for Web Servers

This section describes some of the trace components that are supported by Plug-in for Web Servers.

pdwebpi.azn

The **pdwebpi.azn** component traces the authorization decision for all transactions. This includes details that are related to the credential upon which the authorization is made, the resource that is being accessed, and the authorization decision result. The following sample output shows the information which is traced for a single authorization decision.

Example pdwebpi.azn output

```
2012-03-09-14:57:09.587+10:00I----- thread(2) trace.pdwebpi.azn:5 /mnt/amraid/TAMDev/sandb
oxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/rh/WPIVirtualHost.cpp:1729: [webp
i.vwasp.gc.au.ibm.com] [10.251.140.1] Testing [PDWebPI]r permission on /PDWebPI/webpi.vwas
p.gc.au.ibm.com for user scotte

2012-03-09-14:57:09.588+10:00I----- thread(2) trace.pdwebpi.azn:2 /mnt/amraid/TAMDev/sandb
oxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/rh/WPIVirtualHost.cpp:1515: [webp
i.vwasp.gc.au.ibm.com] [10.251.140.1] Authorization decision:
    Request:  GET http://webpi.vwasp.gc.au.ibm.com/
    Session:  5PnKH-rN2xGrqgAMKenDWA==
    Username: scotte
    Credential attributes:
        AUTHENTICATION_LEVEL = 1
        AZN_CRED_AUTHNMECH_INFO = LDAP Registry
        AZN_CRED_AUTHZN_ID = cn=Scott Exton,o=ibm,c=au
        AZN_CRED_AUTH_METHOD = password
        AZN_CRED_BROWSER_INFO = Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.2)
        AZN_CRED_IP_FAMILY = AF_INET
        AZN_CRED_MECH_ID = IV_LDAP_V3.0
        AZN_CRED_NETWORK_ADDRESS_BIN = 0x0afb8c01
        AZN_CRED_NETWORK_ADDRESS_STR = 10.251.140.1
        AZN_CRED_PRINCIPAL_DOMAIN = Default
        AZN_CRED_PRINCIPAL_NAME = scotte
        AZN_CRED_PRINCIPAL_UUID = ad987b08-cdf4-11db-a51a-000c29e9c358
        AZN_CRED_QOP_INFO = None
        AZN_CRED_REGISTRY_ID = cn=Scott Exton,o=ibm,c=au
        AZN_CRED_USER_INFO =
        AZN_CRED_VERSION = 0x00000600
```

```
    Object:   /PDWebPI/webpi.vwasp.gc.au.ibm.com
    Action:   [PDWebPI]r
    Input attributes:
 -null-
    Result:   GRANTED
    Output attributes:
        -null-

2012-03-09-14:57:09.588+10:00I----- thread(2) trace.pdwebpi.azn:5 /mnt/amraid/TAMDev/sandb
oxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/rh/WPIVirtualHost.cpp:1740: [webp
i.vwasp.gc.au.ibm.com] [10.251.140.1] [PDWebPI]r permission to /PDWebPI/webpi.vwasp.gc.au.
ibm.com for user scotte GRANTED
```

pdwebpi.proxy-cmd

The Plug-in for Web Servers architecture has two main components: the plug-in, and the proxy component. The plug-in component is within the hosting Web server itself and communicates with the Web server. The proxy component runs as a separate process on the system and controls all of the authorization and authentication processing for a request. The proxy component exerts control over the HTTP request and response through the use of commands'. These commands are passed to the plug-in component, which in turn communicates these commands to the hosting Web server.

Example `pdwebpi.proxy-cmd` output

```
2012-03-09-15:17:21.462+10:00I----- thread(2) trace.pdwebpi.proxy-cmd:5 /mnt/amraid/TAMDev
/sandboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/msg/proxy/WPIWebTransAnswerMarsha
ller.cpp:63: [] =============== New Request ==========================

2012-03-09-15:17:21.486+10:00I----- thread(2) trace.pdwebpi.proxy-cmd:5 /mnt/amraid/TAMDev
/sandboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/msg/proxy/WPIWebTransAnswerMarsha
ller.cpp:136: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] cmd(wpi_req_set_web_log_user): [0
] scotte [1] - [2] %25t

2012-03-09-15:17:21.487+10:00I----- thread(2) trace.pdwebpi.proxy-cmd:5 /mnt/amraid/TAMDev
/sandboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/msg/proxy/WPIWebTransAnswerMarsha
ller.cpp:136: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] cmd(wpi_req_remove_header): Autho
rization

2012-03-09-15:17:21.487+10:00I----- thread(2) trace.pdwebpi.proxy-cmd:5 /mnt/amraid/TAMDev
/sandboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/msg/proxy/WPIWebTransAnswerMarsha
ller.cpp:136: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] cmd(wpi_req_remove_header): If-Mo
dified-Since

2012-03-09-15:17:21.487+10:00I----- thread(2) trace.pdwebpi.proxy-cmd:5 /mnt/amraid/TAMDev
/sandboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/msg/proxy/WPIWebTransAnswerMarsha
ller.cpp:136: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] cmd(wpi_req_remove_header): If-Ma
tch

2012-03-09-15:17:21.487+10:00I----- thread(2) trace.pdwebpi.proxy-cmd:5 /mnt/amraid/TAMDev
/sandboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/msg/proxy/WPIWebTransAnswerMarsha
ller.cpp:136: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] cmd(wpi_req_remove_header): If-No
ne-Match

2012-03-09-15:17:21.487+10:00I----- thread(2) trace.pdwebpi.proxy-cmd:5 /mnt/amraid/TAMDev
/sandboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/msg/proxy/WPIWebTransAnswerMarsha
ller.cpp:136: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] cmd(wpi_req_remove_header): If-Ra
nge

2012-03-09-15:17:21.487+10:00I----- thread(2) trace.pdwebpi.proxy-cmd:5 /mnt/amraid/TAMDev
/sandboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/msg/proxy/WPIWebTransAnswerMarsha
ller.cpp:136: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] cmd(wpi_req_remove_header): If-Un
modified-Since
```

```
2012-03-09-15:17:21.487+10:00I----- thread(2) trace.pdwebpi.proxy-cmd:5 /mnt/amraid/TAMDev
/sandboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/msg/proxy/WPIWebTransAnswerMarsha
ller.cpp:136: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] cmd(wpi_req_set_header): Name: Co
okie - Value: w3ibmProfile=200508042136420894-553226052|gASP|616|616|en;%20s_nr=1158564023
064;%20IBMISP=e70885cd950911d9a3a7ed228d15f2c0-e70885cd950911d9a3a7ed228d15f2c0-f887f64332
23bf1363af6c84803c14a5;%20WLS_ibmintra_USERID=scotte@au1.ibm.com;%20PDWPI-SESSION-COOKIE=J
Es7df3N2xGFrAAMKenDWA==ccIA46Br5bT05GRy30wBTKtAihAJi6zKRTeYSLb1MBA=

2012-03-09-15:17:21.487+10:00I----- thread(2) trace.pdwebpi.proxy-cmd:5 /mnt/amraid/TAMDev
/sandboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/msg/proxy/WPIWebTransAnswerMarsha
ller.cpp:136: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] cmd(wpi_rsp_add_header): Name: Se
t-Cookie - Value: PDWPI-SESSION-COOKIE=JEs7df3N2xGFrAAMKenDWA==ccIA46Br5bT05GRy30wBTKtAihA
Ji6zKRTeYSLb1MBA=;%20Path=/

2012-03-09-15:17:21.487+10:00I----- thread(2) trace.pdwebpi.proxy-cmd:4 /mnt/amraid/TAMDev
/sandboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/msg/proxy/WPIWebTransAnswerMarsha
ller.cpp:267: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] response code: wpi_continue
```

pdwebpi.request

The **pdwebpi.request** component traces the HTTP requests that are received by the system. If a trace level of 2 is specified, only the requested URL and HTTP method are traced. If a trace level of 9 is specified, the entire HTTP request is traced. The following sample output shows the information that is traced for a single HTTP request.

Example pdwebpi.request output

```
2012-03-09-15:26:40.751+10:00I----- thread(2) trace.pdwebpi.request:2 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/rh/WPIProxyRequestHandler.cpp
:442: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] Handling request: GET http://webpi.vwasp.
gc.au.ibm.com/

2012-03-09-15:26:40.751+10:00I----- thread(2) trace.pdwebpi.request:9 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/rh/WPIProxyRequestHandler.cpp
:496: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] HTTP request buffer [812 bytes]:
GET / HTTP/1.1
Host: webpi.vwasp.gc.au.ibm.com
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.2) Gecko/20070220 Firefox
Accept: text/xml,application/xhtml+xml,text/html;q=0.9,text/plain;*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: w3ibmProfile=200508042136420894-553226052|gASP|616|616|en; s_nr=1158564023064; IBM
ISP=e70885cd950911d9a3a7ed228d15f2c0-e70885cd950911d9a3a7ed228d15f2c0-f887f6433223bf1363af
6c84803c14a5; WLS_ibmintra_USERID=scotte@example.ibm.com; PDWPI-SESSION-COOKIE=JEs7df3N2xGFrAA
MKenDWA==ccIA46Br5bT05GRy30wBTKtAihAJi6zKRTeYSLb1MBA=
Authorization: Basic c2NvdHRlOnBhc3N3b3JkMQ==
Pragma: no-cache
Cache-Control: no-cache
```

pdwebpi.session

The **pdwebpi.session** component traces details that pertain to a user session. In particular, it traces the contents of the user session, along with session expiration details and any changes that might be made to a user session. The contents of the session itself are traced whenever it is retrieved from the session cache (that is, on each HTTP request). The following sample output shows the information that is traced whenever a new session is created.

Example pdwebpi.session output

```
2012-03-09-15:32:47.205+10:00I----- thread(2) trace.pdwebpi.session:8 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/module/session/WPISession.cpp
:650: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] WPISession::setAuthType - 4241

2012-03-09-15:32:47.209+10:00I----- thread(2) trace.pdwebpi.session:3 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/module/session/WPISession.cpp
:1779: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] WPISession::addAuthenticationData  - No
authentication level set by CDAS

2012-03-09-15:32:47.209+10:00I----- thread(2) trace.pdwebpi.session:3 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/module/session/WPISession.cpp
:1833: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] WPISession::addAuthenticationData Settin
g authentication level to 1

2012-03-09-15:32:47.209+10:00I----- thread(2) trace.pdwebpi.session:3 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/module/session/WPISession.cpp
:1981: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] WPISession::addAuthenticationData - addi
ng user session info UERXZWJQSS13ZWJwaS52d2FzcC5nYy5hdS5pYm0uY29t_gMcBnf-N2xGZ3QAMKenDWA==

2012-03-09-15:32:47.209+10:00I----- thread(2) trace.pdwebpi.session:8 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/module/session/WPISession.cpp
:626: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] WPISession::setAuthModuleName - BA

2012-03-09-15:32:47.209+10:00I----- thread(2) trace.pdwebpi.session:8 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/module/session/WPISession.cpp
:599: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] WPISession::setAuthModuleID - 1

2012-03-09-15:32:47.210+10:00I----- thread(2) trace.pdwebpi.session:8 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/module/session/WPISession.cpp
:352: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] WPISession::getIdleTimeout - 0

2012-03-09-15:32:47.210+10:00I----- thread(2) trace.pdwebpi.session:8 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/module/session/WPISession.cpp
:368: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] WPISession::setIdleTimeout - 600

2012-03-09-15:32:47.210+10:00I----- thread(2) trace.pdwebpi.session:8 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/module/session/WPISession.cpp
:378: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] WPISession::getLifetimeTimeout - 0

2012-03-09-15:32:47.210+10:00I----- thread(2) trace.pdwebpi.session:8 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/module/session/WPISession.cpp
:394: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] WPISession::setLifetimeTimeout - 11734219
67

2012-03-09-15:32:47.210+10:00I----- thread(2) trace.pdwebpi.session:7 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/module/session/WPISession.cpp
:309: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1] WPISession::lock - new expiration time -
1173418967

2012-03-09-15:32:47.211+10:00I----- thread(2) trace.pdwebpi.session:7 /mnt/amraid/TAMDev/s
andboxes/amwebpi/nightly/amwebpi610.061205/src/pdwebpi/proxy/module/session/WPISession.cpp
:2049: [webpi.vwasp.gc.au.ibm.com] [10.251.140.1]
========================================
Session (0x9E6CAEC): scotte
Session Data: eb - sms (has changed)
   com.tivoli.am.webpi.session.auth-type = 0x4241
   com.tivoli.am.eb.auth-type = basicAuthRFC2617
   com.tivoli.am.eb.credential = BAKs3DCCA/EMADCCA+swggPnAgIGADAsMCgwHgIErZh7CAIDAM30AgIR2
   wICAKUCARoEBgAMKenDWAwGc2NvdHRlMAACAQEwggOuMIIDqjAiDBRBVVRIRU5USUNBVElPTl9MRVZFTDAKMAgC
   AQQMATEEADAxDBdBWk5fQ1JFRF9BVVRITk1FQ0hfSU5GTzAWMBQCAQQMDUxEQVAgUmVnaXN0cnkEADA4DBJBWk5
   fQ1JFRF9BVVRIWk5fSUQwIjAgAgEEDBljbj1TY290dCBFeHRvbixvPWlibSxjPWF1BAAwKQwUQVpOX0NSRURfQV
   VUSF9NRVRIT0QwETAPAgEEDAhwYXNzd29yZAQAMHQMFUFaTl9DUkVEX0JST1dTRVJfSU5GTzBbMFkCAQQMUk1ve
   mlsbGEvNS4wIChYMTE7IFU7IExpbnV4IGk2ODY7IGVuLVVTOyBydjoxLjguMS4yKSBHZWNrby8yMDA3MDIyMCBG
   aXJlZm94LzIuMC4wLjIEADAmDBJBWk5fQ1JFRF9JUF9GQU1JTFkwEDAOAgEEDAdBRl9JTkVUBAAwKQwQQVpOX0N
   SRURfTUVDSF9JRDAVMBMCAQQMDElWX0xEQVBfVjMuMAQAMDMMHEFaTl9DUkVEX05FVFdPUktfQUREUkVTU19CSU
   4wEzARAgEEDAoweDBhZmI4YzAxBAAwNQwcQVpOX0NSRURfTkVUV09SS19BRERSRVNTX1NUUjAVMBMCAQQMDDEwL
   jI1MS4xNDAuMQQAMC0MGUFaTl9DUkVEX1BSSU5DSVBBTF9ET01BSU4wEDAOAgEEDAdEZWZhdWx0BAAwKgwXQVpO
   X0NSRURfUFJJTkNJUEFMX05BTUUwDzANAgEEDAZzY290dGUEADBIDBdBWk5fQ1JFRF9QUklOQ0lQQUxfVVVJRDA
   tMCsCAQQMJGFkOTg3YjA4LWNkZjQtMTFkYi1hNTFhLTAwMGMyOWU5YzM1OAQAMCIMEUFaTl9DUkVEX1FPUF9JTk
   ZPMA0wCwIBBAwETm9uZQQAMDoMFEFaTl9DUkVEX1JFR0lTVFJZX0lEMCIwIAIBBAwZY249U2NvdHQgRXh0b24sb
   z1pYm0sYz1hdQQAMB8MEkFaTl9DUkVEX1VTRVJfSU5GTzAJMAcCAQQMAAQAMCcMEEFaTl9DUkVEX1ZFUlNJT04w
   EzARAgEEDAoweDAwMDAwNjAwBAAwaAwWdGFndmFsdWVfc2Vzc2lvbl9pbmRleDBOMEwCAQQMRVVFUlhaV0pRU1M
   xM1pXSndhUzUyZDJGemNDNW5ZeTVoZFM1cFltMHVZMjl0X2dNY0JuZi1OMnhHWjNRQU1LZW5EV0E9PQQA
   com.tivoli.am.eb.expiry = 0x45f0ff8f
Session Data: session - session (has changed)
   com.tivoli.am.webpi.session.auth-module = com.tivoli.am.webpi.session.auth-module-id
   com.tivoli.am.webpi.session.auth-module-id = 0x1
   com.tivoli.am.webpi.session.term-audit-action = 0x67
   com.tivoli.am.webpi.session.is-secondary = false
   com.tivoli.am.sms.creation-time = 0x45f0f17f
   com.tivoli.am.sms.session-index = gMcBnf-N2xGZ3QAMKenDWA==
   com.tivoli.am.webpi.session.is-proxy = unknown
   com.tivoli.am.webpi.session.no-logout = true
   com.tivoli.am.webpi.session.prior-authn-level = 0x0
   com.tivoli.am.webpi.session.primary-auth-module-id = 0x0
   com.tivoli.am.webpi.session.logout-pwd-change = false
Session Data: trans - session (has changed)
   com.tivoli.am.webpi.trans.reauth = false
   com.tivoli.am.webpi.trans.reauth-grace-applied = false
   com.tivoli.am.webpi.trans.restore-on-auth = true
   com.tivoli.am.webpi.trans.reauth-reset-lifetime = false
   com.tivoli.am.webpi.trans.is-initial-authn = true
   com.tivoli.am.webpi.trans.authn-uri = /
   com.tivoli.am.webpi.trans.mfa = 0x0
   com.tivoli.am.webpi.trans.password-expired = false
   com.tivoli.am.webpi.trans.post-auth-url =
   com.tivoli.am.webpi.trans.can-be-terminated = true
Session Data: ba-authenticated - BA (has changed)
   com.tivoli.am.webpi.ba-authenticated.header = Basic c2NvdHRlOnBhc3N3b3JkMQ==
Session Data: web-log - web-log

========================================
```

Available trace components

The following table contains all trace components that are common to all Security Access Manager servers:

Table 13. Common trace components

Component	Description
pd.bst.general	Used to trace the Kerberos authentication process.
pd.acl.general	The general trace for the authorization API.
pd.acl.client	Used to trace the plug-in services for the authorization server.
pd.acl.authzn	Used to trace the authorization decision.
pd.acl.adminsvc	Used to trace the interface into the administration service plug-in.
pd.acl.remsvc	Used to trace the authorization decision during remote mode operation.
pd.acl.aznapi	Used to trace the usage of the Security Access Manager authorization API.
pd.acl.aznsvc	Used to trace the plug-in services that are provided by the authorization server.
pd.idb.database	Used to trace access to the Security Access Manager policy database.

Table 13. Common trace components (continued)

Component	Description
pd.ivc.ira	The IRA is the Security Access Manager interface into the LDAP server. This trace component is used to trace the Security Access Manager communication with the LDAP server.
pd.mgr.general	Used to trace the Security Access Managerr administration commands in the Policy Server.
pd.mgr.svrmgmt	Used to trace the management of the authorization servers within the policy server.
pd.mgr.uraf	Used to trace the usage of the user registry access framework when accessing user registries other than LDAP.
pd.ias.general	User to trace the Security Access Manager supplied authentication mechanisms, otherwise known as CDASs.
pd.ras.exception.trace	Used to trace any exceptions that might be caught by the server.

The following table contains all available pdadmin trace components:

Table 14. The pdadmin trace components

Component	Description
pdweb.bca.general	Used to trace the client side of the Security Access Manager authorization API.
pdweb.bca.user	Used to trace the client side of **user** pdadmin command.
pdweb.bca.group	Used to trace the client side of **group** pdadmin command.
pdweb.bca.acl	Used to trace the client side of **acl** pdadmin command.
pdweb.bca.protobj	Used to trace the client side of **object** pdadmin command.
pdweb.bca.protobjspace	Used to trace the client side of **objectspace** pdadmin command.
pdweb.bca.appsvrcfg	Used to trace the client side of **user** config command.
pdweb.bca.ssoresource	Used to trace the client side of **user** rsrc command.
pdweb.bca.ssoresourcegroup	Used to trace the client side of **rsrcgroup** pdadmin command.
pdweb.bca.ssocred	Used to trace the client side of **rscrcred** pdadmin command.
pdweb.bca.action	Used to trace the client side of **action** pdadmin command.
pdweb.bca.server	Used to trace the client side of **server** pdadmin command.
pdweb.bca.pop	Used to trace the client side of **pop** pdadmin command.
pdweb.bca.domain	Used to trace the client side of **domain** pdadmin command.
pdweb.bca.authzrule	Used to trace the client side of **authzrule** pdadmin command

The following table contains all available WebSEAL trace components:

Table 15. The WebSEAL trace components

Component	Description
pdweb.wan.ssl	Used to trace the SSL connection between WebSEAL and junctioned web servers.
pdweb.wns.session	Used to trace the WebSEAL sessions, as they are stored within the session cache and retrieved or removed from the session cache.
pdweb.wns.authn	Used to trace the authentication processing. **Note:** This trace component includes the header information that WebSEAL uses for header-based authentication. This header might contain sensitive information. For example, a BA header.
pdweb.adm.config	Used to trace the configuration for e-community SSO.
pdweb.wan.bool	Used to trace the WebSEAL processing of Security Access Manager authorization rules.
pdweb.wns.compress	Used to trace the WebSEAL compression of HTTP messages.
pdweb.cas.general	Used to trace the interface between WebSEAL and a custom-written CDAS shared library.
pdweb.wco.azn	Used to trace the entitlements service, which manages the maximum concurrent web session policy. The policy is used with SMS to limit the number of times a particular user can create a session concurrently.
pdweb.debug	Used to trace the HTTP headers sent between WebSEAL and the client. **Note:** The pdweb.debug trace could contain sensitive information.
pdweb.snoop.client	Used to trace the HTTP packets that are transmitted between WebSEAL and the client. **Note:** This component traces each request and response in its entirety as it is read off the socket. This trace might contain sensitive information.
pdweb.snoop.jct	Used to trace the HTTP packets that are transmitted between WebSEAL and the junctioned back-end web server. **Note:** This component traces each request and response in its entirety as it is read off the socket. This trace might contain sensitive information.
pdweb.url	Used to trace the creation and parsing of the URL.
pdweb.wan.azn	Used to trace the WebSEAL authorization decision.
pdweb.wan.ltpa	Used to trace the management of LTPA cookies.
pdweb.oauth	Used to trace OAuth EAS authorization decisions. **Note:** This component traces the data that passes into the EAS, which is governed by the **`[azn-decision-info]`** stanza. This trace might contain sensitive information.
pdweb.http.transformation	Used to trace HTTP transformation processing. **Note:** This component traces the header information in the request, which might contain sensitive information. For example, a Basic Authentication header.

Part 4. Common problems with base components

Chapter 13. Common Security Access Manager problems

Check the following information for issues with any of the following Security Access Manager base components:

- Security Access Manager policy server
- Security Access Manager policy proxy server
- Security Access Manager authorization server
- Security Access Manager Runtime
- Security Access Manager Runtime for Java
- Security Access Manager Application Development Kit (ADK)
- Security Access Manager Web Portal Manager

Environment information messages in the server log file at startup

In Security Access Manager, the severity level of the startup environment dump information added to the server process log is **WARNING**. When a Security Access Manager server starts, a series of **WARNING** messages display information about the environment and AIX, Linux, or Solaris `ulimit`. These messages are informational. The support team uses these messages to diagnose problems.

The following example shows a warning:

```
2009-08-27-03:54:43.017+00:00I----- 0x1354A0CD pdmgrd WARNING ivc
general azn_maint.cpp 4977 0x00000001 HPDCO0205W  ------------------------
2009-08-27-03:54:43.017+00:00I----- 0x1354A0CC pdmgrd WARNING ivc
general azn_maint.cpp 4998 0x00000001 HPDCO0204W  Informational Message -
The environment variable for the running process :
_=/opt/PolicyDirector/bin/pdmgrd
...
TCD_PRODNAME=HPD
MAILMSG=[You have new mail]
PDCONFOBF=/opt/PolicyDirector/etc/pd.conf.obf
PWD=/
TZ=CST6CDT
PD_SVC_ROUTING_FILE=/opt/PolicyDirector/etc/pdmgrd_routing
....
2009-08-27-03:54:43.018+00:00I-----
0x1354A0CD pdmgrd WARNING ivc general azn_maint.cpp 505
0 0x00000001 HPDCO0205W  getrlimit():
RLIMIT_DATA (rlim_cur: 134217728 ; rlim_max: 2147483647)
2009-08-27-03:54:43.019+00:00I----- 0x1354A0CD
pdmgrd WARNING ivc general azn_maint.cpp 505
0 0x00000001 HPDCO0205W  getrlimit(): RLIMIT_STACK
(rlim_cur: 33554432 ; rlim_max: 2147483646)
2009-08-27-03:54:43.019+00:00I----- 0x1354A0CD
pdmgrd WARNING ivc general azn_maint.cpp 505
0 0x00000001 HPDCO0205W  getrlimit():
RLIMIT_AS (rlim_cur: 2147483647 ; rlim_max: 2147483647)
2009-08-27-03:54:43.019+00:00I-----
0x1354A0CD pdmgrd WARNING ivc general azn_maint.cpp 503
1 0x00000001 HPDCO0205W  --------------------
----------------------------
```

Unable to create new user

One of the most common error messages that you might see when you create a user is as follows:

```
Could not perform the administration request.
Error: Password rejected due to the Minimum Non-Alphabetic Characters policy
(status 0x13212131)
```

This error indicates, for example, that the password "abc" that was specified when you attempt to create the user does not comply with one of the user password policies that is defined. To view the help text for the Security Access Manager policy commands, enter the following command:

```
pdadmin> help policy
```

The previous password policy error can be solved by using one of the following solutions:

- Determine the minimum non-alphabetic character policy with the following command:

  ```
  pdadmin> policy get min-password-non-alphas
  ```

  Using this value, create the user with a password that contains the required minimum number of non-alphabetic characters.
- Modify the Security Access Manager non-alphabetic character policy before creating the user with the following command:

  ```
  pdadmin> policy set min-password-non-alphas number
  ```

Unable to authenticate user

About this task

After you create a user, this user cannot authenticate immediately with the new Security Access Manager user identity until the account is modified. Security Access Manager user definitions are initially created with the account disabled (`Account valid = no`).

This condition is frequently the cause of authentication failures. To modify the account, complete the following steps:

1. Use the **user modify** command to enable the account:

   ```
   pdadmin> user modify user-name account-valid yes
   ```
2. Use the **user show** command to verify this change:

   ```
   pdadmin> user show user-name
   ```

Unexpected access to resources

Accesses to a protected system resource are either being unexpectedly granted or denied. It is always wise to first validate that the Security Access Manager processes are started and running normally. Also check to ensure that the Security Access Manager message log files do not flag any operational problems. If Security Access Manager seems operationally sound, the problem is likely due to the policies that have been defined and applied to that system resource.

There are three Security Access Manager policy mechanisms that can be used to control access to your protected resources: ACLs, POPs, and authorization rules. Use the **pdadmin** commands to learn which ACL in your protected object space hierarchy has control over the access to the protected resource.

ACL commands

Security Access Manager access control depends on the following conditions:

- The ACL that controls the requested object must contain appropriate access permissions for the requesting user.
- The requested object must be accessible to the requesting user.

  Accessibility to protected objects is controlled by the traverse (**T**) permission. The traverse permission is only applied to container objects in the protected object space. The traverse permission specifies that a user, group, any-other, or unauthenticated user, that is identified in the ACL entry, has permission to pass through this container object to gain access to a protected resource object that is below it in the hierarchy.

If an ACL is directly attached to the protected object, this ACL defines the ACL policy for that object. If an ACL is not directly attached to the protected object, the controlling ACL is the nearest one that is above it in the protected object hierarchy.

Listing ACLs

Lists all ACLs that are defined in Security Access Manager:

```
padmin> acl list
```

Finding ACLs

Displays where each of those ACLs is attached within the protected object space hierarchy:

```
pdadmin> acl find acl_name
```

Showing ACLs

Examines the controlling ACL to check that it is correct for the type of enforcement wanted:

```
pdadmin> acl show acl_name
```

Correct the ACL definition if needed.

POP commands

A protected object is accessible to a requester if the requester possesses the traverse permission on each ACL attached to container objects above the requested resource on the path towards root and including root.

Additionally, use the **pdadmin** command to learn which POP (if any) within your protected object space hierarchy controls access to the protected resource in question.

If a POP is directly attached to the protected object in question, this POP defines the POP policy for that object. If a POP is not directly attached to the protected object in question, the controlling POP is the nearest one that is above it in the protected object hierarchy.

Listing POPs

The following command lists all of the POPs which are defined for Security Access Manager:

```
padmin> pop list
```

Finding POPs

The following command enables you to learn where a particular POP is attached within the protected object space hierarchy:

```
pdadmin> pop find pop_name
```

Showing POPs

Examine the controlling POP with the following command to ensure that it is correct for the type of enforcement desired:

```
pdadmin> pop show pop_name
```

Correct the POP definition if needed.

Authorization rule commands

If an authorization rule is directly attached to the protected object in question, this authorization rule defines the rule policy for that object. If an authorization rule is not directly attached to the protected object in question, the controlling rule is the nearest one that is above it in the protected object hierarchy.

Listing rules
The following command lists all of the authorization rules defined for Security Access Manager:

```
padmin> authzrule list
```

Finding rules
The following command enables you to learn where a particular authorization rule is attached within the protected object space hierarchy:

```
pdadmin> authzrule find authznrule_name
```

Showing rules
Use the following command to examine the controlling authorization rule and to ensure that it is correct for the type of enforcement required:

```
pdadmin> authzrule show authznrule_name
```

Correct the rule definition if needed.

Processes terminate abruptly on Intel 64-bit processor

The ibmslapd, idsldapsearch, pdmgrd, and pdadmin processes crash intermittently on servers that use an Intel 64-bit XEON processor if the hyper-threading option is enabled and the appropriate resolution package is not installed. (This problem does not occur on servers using an AMD 64-bit processor.) In this case, if a junction is created with the -c flag, IV_GROUPS are no longer passed to the backend server via the junction after WebSEAL is restarted.

This issue can be resolved either by disabling the hyper-threading option or by installing the package appropriate to your operating system:

- microcode_ctl-1.12-1.4.x86_64.rpm (SUSE Linux Enterprise Server)
- kernel-utils-2.4-13.1.80.x86_64.rpm (Red Hat Enterprise Linux)

Memory exhaustion on AIX Security Access Manager servers

The AIX environment variable `MALLOCMULTIHEAP` can cause memory fragmentation that results in crashing, coring, or exiting because of memory exhaustion.

Multithreaded applications often allocate memory in one thread and free the memory in another thread. AIX MALLOCMULTIHEAP has the following design limitation:

1. One thread allocates memory in a particular heap, Heap "A".
2. If the memory is freed by another thread, then it might be freed in a different heap, Heap "B".

This process permanently reduces the amount of memory in Heap "A". The fragmented memory never coalesces. When threads use Heap "A" to allocate more memory, Heap "A" must allocate more memory from the process heap. In some scenarios, this cycle can exhaust all the available memory for the process in a short period.

Security Access Manager applications cannot support the AIX MALLOCMULTIHEAP environment variable due to the negative affect on availability and stability. If you experience problems with crashing, coring, or exiting of Security Access Manager applications on AIX, ensure that this environment variable is disabled. After you disable the MALLOCMULTIHEAP environment variable, ensure that you restart WebSEAL by using the **`pdweb`** command. For example, `pdweb restart default` where `default` is the WebSEAL instance name.

Password change does not work in a multidomain environment

Specific configuration conditions for policy server, subdomains, and WebSEAL can cause password changes to fail.

About this task

A WebSEAL instance cannot change user passwords under all the following conditions because of the absence of ACL settings that are required to search domain locations:

- You configured the policy server in a nondefault location that is a location other than `secAuthority=Default`.
- You create Security Access Manager subdomains under the new location.
- You configured a WebSEAL instance in any of the new subdomains.

Complete the following steps to set the correct ACL with the following assumptions:

- The management domain name is `Default`.
- The `Default` domain is in an LDAP suffix that is called `O=IBM,C=US`.
- The subdomain names are `Domain1`, `Domain2`, and so on.

1. Place the following in a file called `aclEntry.ldif`:

   ```
   ##------ START: Do not include this line -----##
   dn: secAuthority=Default,o=ibm,c=us
   changetype: modifyI
   add: aclentry
   aclentry:group:cn=SecurityGroup,SecAuthority=Domain1,cn=SubDomains
   ,SecAuthority=Default,O=IBM,C=US,O=IBM,C=US:object:ad:normal
   :rwsc:sensitive:rwsc:critical:rwsc:system:rsc
   aclentry:group:cn=SecurityGroup,SecAuthority=Domain2,cn=SubDomains,
   SecAuthority=Default,O=IBM,C=US,O=IBM,C=US:object:ad
   :normal:rwsc:sensitive:rwsc:critical:rwsc:system:rsc
   ##------ END: Do not include this line -------##
   ```

   You must replace the management domain name `Default`, suffix `O=IBM,C=US`, and subdomains `Domain1`, `Domain2`, and so on, with the corresponding name of the current installation.

2. Update the ACL by running the following command:`ldapmodify -h host -p port -D cn=root -w pwd -i aclEntry.ldif`

Blank help window in Web Portal Manager with WebSphere Application Server 7

Help panels from Web Portal Manager might be blank when you use a WebSphere Application Server that is earlier than 7.0.0.11.

The following URL describes the problem:

http://www-01.ibm.com/support/docview.wss?uid=swg1PM10056

This issue does not occur in WebSphere Application Server, version 8.

To resolve the issue, complete one of the following options:

- Apply the WebSphere Application Server, Service Pack 7.0.0.11 or later.

--OR--

- Complete the workaround to create the missing `iehs.properties` file as described on the following website:

  http://www-01.ibm.com/support/docview.wss?uid=swg1PM10056

Product pages might not display in browser if website is not trusted

Product pages might not display in a browser if the website is not trusted. For example, if the administrative console pages for Security Access Manager are empty even though the product is working, the issue might be caused by an untrusted website.

To resolve this issue, add the product website to the list of trusted websites in the security settings of your browser.

For example, if your URL to access Web Portal Manager is `http://wpm14.example.com:9060/ibm/console`, add the website to your list of trusted websites in the security settings of your browser.

Chapter 14. Disaster recovery of the master authorization database

Disaster recovery involves policies and procedures for how to recover or continue an environment infrastructure that is critical to a business. Complete these steps to create a backup and disaster recovery plan for the master authorization database, `master_authzn.db`.

Before you begin

Ensure that you have a backup directory location that provides enough space and has appropriate security control in place. If you do not already have a backup directory, create one.

About this task

Disaster recovery consists of having a backup of the main database available in the event of a failure. If a disaster occurs, you can restore the data from the backup, secondary, data server to avoid loss of data and productivity.

This focus in this procedure is on the master authorization database, `master_authzn.db`. The master authorization database is controlled by the policy server, **pdmgrd**. For a successful disaster recovery plan, you must make regular backups of `master_authzn.db` along with other critical Security Access Manager files.

Use the following procedure as a guideline for creating data backups, and testing the backups on a standby policy server.

Procedure

Back up your data

1. In your backup directory, create a file named *BackupDir*/`PDMGRD-Input.lst`.
2. Open the `PDMGRD-Input.lst` file and add the following file names to specify the files that you want to back up:
   - For AIX, Linux, or Solaris systems:
     ```
     ./opt/PolicyDirector/etc/ivmgrd.conf
     ./opt/PolicyDirector/etc/ivmgrd.conf.obf
     ./var/PolicyDirector/keytab/ivmgrd.kdb
     ./var/PolicyDirector/keytab/ivmgrd.sth
     ./var/PolicyDirector/db/master_authzn.db
     ./var/PolicyDirector/db/subdomain.db
     ```
   - For Windows systems:
     ```
     C:\Program Files\Tivoli\Policy Director\etc\ivmgrd.conf
     C:\Program Files\Tivoli\Policy Director\etc\ivmgrd.conf.obf
     C:\Program Files\Tivoli\Policy Director\keytab\ivmgrd.kdb
     C:\Program Files\Tivoli\Policy Director\keytab\ivmgrd.sth
     C:\Program Files\Tivoli\Policy Director\db\master_authzn.db
     C:\Program Files\Tivoli\Policy Director\db\subdomain.db
     ```

   Where *subdomain* is used only if your environment has a subdomain.

   If LDAP SSL is enabled, also include the `.kdb` file that is specified as the `[ldap]ssl-keyfile` value in the `ivmgrd.conf` file.

3. Create the backup `.tar` file by completing the following steps:
   a. Stop the primary policy server.
   b. Run the **`pdacld_dump`** command to check the integrity of the master authorization database. On AIX, Linux, or Solaris, **`pdacld_dump`** is in the `/opt/PolicyDirector/sbin` directory. On Windows, **`pdacld_dump`** is in the `C:\Program Files\Tivoli\Policy Director\sbin` directory. For example,
      - AIX, Linux, or Solaris:
        ```
        pdacld_dump -f /var/PolicyDirector/db/master_authzn.db -s
        ```
      - Windows:
        ```
        pdacld_dump -f C:\Program Files\Tivoli\Policy Director\ /
        db\master_authzn.db -s
        ```
   c. Examine the output for errors. If errors are reported, go to step 6 on page 111, otherwise continue to step 4. For example, check for the following error terms:
      - Invalid objects
      - Object output mismatch
      - Dumped objects mismatch
      - Unable to retrieve all objects
   d. Create the backup file by running the following command:
      ```
      cd /
      tar -cvf BackupDir/PDMGRD-Filesdate.tar -L BackupDir/PDMGRD-Input.lst
      ```

      where *`BackupDir`*`/PDMGRD-Input.lst` was created in step 1 on page 109
   e. Transfer the *`BackupDir`*`/PDMGRD-Files`*`date`*`.tar` file securely to the designated backup server or standby policy server.
   f. Restart the primary policy server.

Routinely back up your data

4. Establish a routine backup schedule for policy server and critical files by completing the following steps:
   a. Establish a backup interval. Backups can be completed nightly, weekly, and so on. Consider an acceptable amount of data loss in the event of an issue that occurs between backups. Adjust the backup interval according to this consideration.
   b. Stop the primary policy server during database backups to maintain integrity in the files to be backed up.
   c. Routinely back up the primary server and store the backup file in a standby server according to your backup interval plan.

Test your backup data

5. Test the backup files in the standby policy server by completing the following steps:
   a. Stop the primary policy server.
   b. If you not already completed, copy and transfer the backup `.tar` file, *`BackupDir`*`/PDMGRD-Files`*`date`*`.tar`, created in step 3 to the standby policy server.
   c. On the standby policy server, back up the same files as described in step 2 on page 109. The file locations must be the same in the standby and primary policy server.
      ```
      cd /
      tar -cvf BackupDir/Test-PDMGRD-Filesdate.tar -L BackupDir/PDMGRD-Input.lst
      ```

d. Run a command to extract the *BackupDir*/PDMGRD-Files*date*.tar image that was copied from the primary policy server machine. Verify the appropriate ownership/permission of the extracted/copied files.

e. Start the standby server and test the policy server by completing the following steps:

CAUTION:
Caution: Do not start the standby policy server unless the primary policy server is shut down.

1) Stop the primary policy server.
2) Make appropriate changes in network settings (such as the DNS/F5/Load balancer) to point to the standby policy server.
3) Start the standby policy server.
4) Log in by using **pdadmin**, and then run simple commands to ensure that the server is working properly.
5) Run any appropriate test suite for further verification.
6) After the readiness of the standby policy server is verified, stop the standby policy server.
7) Change the network settings (such as the DNS/F5/Load balancer) to point back to the primary policy server.
8) Restart the primary policy server.

Validating and maintaining policy databases:

6. Review and follow the practices described in Chapter 7, “Validating and maintaining policy databases,” on page 45.

Repairing a damaged policy database:

7. If the policy database becomes damaged or corrupted, use the **pdacld_dump** command to create a policy database. This new policy database contains only the valid data that is recovered from the damaged policy database. The **pdacld_dump** command will not be able to recover the lost data because of corruption. For example, if the policy database for the default domain becomes damaged, use the following command to recover the valid information from the existing policy database and write it to the new Repaired_master_authzn.db policy database:

```
pdacld_dump -f /var/PolicyDirector/db/master_authzn.db \
   -r /var/PolicyDirector/db/Repaired_master_authzn.db
```

Additionally, this option de-fragments the content of the new policy database.

Replacing a damaged policy database:

8. Replace a damaged policy database with a repaired one by completing the following steps:

a. Stop the policy server or the authorization server.

b. Rename the damaged policy database (master_authzn.db in the previous example) or move it to a different directory.

```
mv master_authzn.db Damaged_master-authzn.db
```

c. Rename the repaired file to have the same name as the original policy database.

d. Copy the Repaired_master_authzn.db to appropriate location:

```
mv Repaired_master_authzn.db master-authzn.db
```

e. Verify the appropriate ownership/permission of master-authzn.db.

f. Restart the policy server or authorization server.

Chapter 15. Common user registry problems

This chapter details common user registry or directory server problems that you might encounter when you use Security Access Manager.

Tivoli Directory Server common problems

This section details common problems that you might encounter when you use IBM Tivoli Directory Server as the user registry.

Location of error logs

When a problem occurs that seems to be related to Tivoli Directory Server, check for error messages that are related to that product. You can find locations of Tivoli Directory Server log files that are described at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.IBMDS.doc%2Fpdguide24.htm

Tivoli Directory Server error log warnings

Tivoli Directory Server error log indicates several “does not exist” warnings.

When the policy server is configured, the policy server is first unconfigured as part of this configuration process to ensure that it was cleaned up completely.

The unconfiguration step attempts to remove entries in the directory server.

When the policy server configuration is not yet completed, these entries are not yet created and might not exist in the LDAP registry. The Tivoli Directory Server logs these entry removal attempts as warnings in its error log. These warnings are therefore normal and can be safely ignored.

Tivoli Directory Server Instance Administration tool does not display instance on Red Hat Enterprise Linux 6

After you install Tivoli Directory Server with the installation wizard typical installation path, the default instance is created. However, on Red Hat Linux, version 6, the Instance Administration tool started at the end of installation does not display the instance.

To verify that the default instance is listed in the configuration, use the **idsilist** command. By default, this command is in the /opt/ibm/ldap/V6.3/sbin/ directory. For details about the command, see the IBM Tivoli Directory Server, version 6.3 Information Center:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm

Although the instance does not display in the UI, you can follow the command-line tool configuration steps as documented in the *IBM Security Access Manager for Web Installation Guide*.

To use an instance other than the default instance that is created by the Tivoli Directory Server installer, use command-line tools to create and configure a non-default instance. See the Tivoli Directory Server documentation for more information.

Setting up SSL

For information about configuring Tivoli Directory Server to use SSL communication, see the *IBM Tivoli Directory Server Administration Guide* in the Tivoli Directory Server Infocenter:

> http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml

LDAP common problems

About this task

This section details common problems that you might encounter when you use an LDAP-based user registry, such as Tivoli Directory Server. For common problems that are specific to Tivoli Directory Server, see "Tivoli Directory Server common problems" on page 113.

LDAP does not start after suffix is created

After you create the `secAuthority=Default` suffix Tivoli Directory Server does not start.

The following steps are required to prepare an LDAP server for use with Security Access Manager. These steps must be completed before you configure Security Access Manager:

1. Create the `secAuthority=Default` suffix.
2. Stop and restart the Tivoli Directory Server to enable the server to recognize the newly created suffix

When command-line installation is used, these steps must be completed manually.

If the user attempts to create the `secAuthority=Default` suffix and restart Tivoli Directory Server before you apply the schema modifications that are required by Security Access Manager, Tivoli Directory Server fails to restart.

When the server fails to restart it logs an error message to the `slapd.errors` file. This message indicates that the **secAuthority** attribute is not defined. The `slapd.errors` file is in the `/tmp` directory on AIX, Linux, and Solaris operating systems and in the `*ldap_install_dir*\tmp` directory on Windows operating systems, where *ldap_install_dir* is the directory where Tivoli Directory Server was installed.

Insufficient privileges to perform operations

You are receiving the following error:

```
Insufficient LDAP access privileges to perform operation.
```

This message indicates that a supplied LDAP suffix does not have the correct ACLs attached. The following reasons are possible causes for this problem:

- During configuration, Security Access Manager was unable to attach ACLs to the existing suffix because the directory entries necessary to instantiate the suffix were not created.

- The suffix was added after the initial configuration of the Security Access Manager management server and the required ACLs were not added manually.

The Web Administration Tool provided with the Tivoli Directory Server client can be used to check the suffix and to add the appropriate ACLs manually. For information about how to accomplish this, see the *IBM Security Access Manager for Web: Administration Guide*.

Correct the ACLs on the suffix, and run the command again.

Active Directory common problems

This section details common problems that you might encounter when you use Active Directory as the user registry.

Receiving HPDRG0100E for Active Directory operations

During Security Access Manager configuration, you might receive the following HPDRG0100E error message:

```
HPDRG0100E The operation in the Active Directory registry for operation_id
failed with return error nnnnnnnn.
```

This message is issued when an Active Directory error cannot be resolved during configuration.

Use the following problem determination suggestions to resolve this error before you restart configuration.

- An error message HPDRG0100E that is similar to the following content refers to a schema write failure:

  ```
  HPDRG0100E The operation in the Active Directory registry for
  adschema_update.exe: ADSCHEMA_SET_SCHEMA_WRITE failed with return error
  35.
  ```

  For this case, ensure that the Remote Registry Windows service is running on the root Active Directory domain controller system. During configuration, the Active Directory schema is updated, which requires the Remote Registry Windows service to be running. If the service is not running, start the service and complete configuration. You can stop the service after the configuration is finished.
- If the HPDRG0100E error message contains an 8-digit return code that begins with 8007, use the Microsoft **net helpmsg** command to display relevant help text. Convert the last four digits (digits that are *nnnn* of the return code of the form 8007*nnnn*) from hexadecimal format to decimal format and issue the command by using decimal format for the last four digits of the return code:

  ```
  net helpmsg nnnn
  ```
- Pursue the problem with Microsoft support by using the Active Directory return code value provided in the HPDRG0100E error message.

After you resolve the cause of this error, you can restart the configuration operation.

Receiving HPDRG0101E The user password violates the Active Directory user password policies

The Security Access Manager HPDRG0101E error message can occur during Security Access Manager configuration or during password change operations. This error can occur even if the Active Directory Domain account password policy "Password must meet complexity requirements" is set to "Disabled."

To resolve this error, ensure that the password meets the requirements of the Microsoft account password complexity policy. To learn more about Microsoft account password complexity policy, search the Microsoft knowledge base.

Part 5. Common problems with Web security components

Chapter 16. Single sign-on Issues: Windows Desktop single sign-on, Kerberos, and SPNEGO

Use the following information to troubleshoot and resolve single sign-on issues that involve Windows Desktop single sign-on, Kerberos, and SPNEGO.

Windows Desktop single sign-on, on the client end, uses the Simple and Protected GSS-API Negotiation (SPNEGO) authentication protocol over HTTP to authenticate with WebSEAL and Plug-in for Web Servers components.

SPNEGO authentication works by wrapping a Kerberos authentication token, obtained by the windows Desktop browser, and sending it in an HTTP header to the target web server without the need for user action. The user signs on to their Windows Desktop, and the browser can use the sign on to send the Kerberos token by means of SPNEGO to the web server for single sign-on, assuming the Web Server can handle SPNEGO or Kerberos.

WebSEAL and Plug-in for Web Servers components on AIX, Linux, or Solaris use Kerberos to validate SPNEGO authentication data.

Problems with SPNEGO

Use the following troubleshooting tips for issues that involve SPNEGO authentication.

Basic SPNEGO troubleshooting

When presented with any SPNEGO authentication problem, there are several questions that need to be asked. First, ask yourself the following question:

> Are you on an AIX, Linux, Solaris, or Windows operating system?

If your answer is either an AIX, Linux, or Solaris operating system, see "AIX, Linux, and Solaris workflow." If your answer is a Windows operating system, see "Windows workflow" on page 120.

AIX, Linux, and Solaris workflow

If your answer is AIX, Linux or Solaris, ask yourself the following questions:

1. Is the **am_kinit** command failing? If yes, there is a Kerberos configuration problem either with initializing the Kerberos libraries or with obtaining initial credentials. If the **am_kinit** command fails because it cannot initialize the Kerberos libraries, see the following topics:
   - "Cannot open configuration file" on page 124
   - "Improper format of configuration file" on page 124

   If the **am_kinit** command fails because it cannot obtain initial credentials, see the following topics:
   - "Cannot resolve address of key distribution center" on page 125
   - "Cannot contact the key distribution center" on page 125
   - "Clocks are not synchronized" on page 126
   - "Pre-authentication failure" on page 126
   - "Client not found or locked out" on page 126

2. Is the Web security server (WebSEAL or Web Server Plug-in) not starting? If yes, see the following topics:
   - "Authentication method not configured" on page 121
   - "No match to principal in key table" on page 121
3. Is authentication failing? If yes, see the following topics:
   - "Ticket not yet valid" on page 128
   - "Cannot acquire credentials" on page 128
   - "Wrong principal in request" on page 129
   - "Encryption type not permitted" on page 130
   - "Key version is incorrect" on page 130
   - "Cannot authenticate by using NTLM" on page 130
   - "Cannot complete authentication" on page 131

Windows workflow

If your answer is Windows, ask yourself the following questions:

1. Is the Web security server (WebSEAL or Web Server Plug-in) not starting? If yes, see "Authentication method not configured" on page 121.
2. Is authentication failing? If yes, see the following topics:
   - "Cannot authenticate by using NTLM" on page 130
   - "Cannot complete authentication" on page 131

Web security server not starting

The following information describes debugging SPNEGO configuration problems with a Plug-in for Web Servers or WebSEAL configuration where one of the Web security servers does not start. If the Plug-in for Web Servers or WebSEAL server fails to start, the server log file for that server contains messages that describe the problem.

Collecting data for Security Access Manager: WebSEAL (SPNEGO issues)

When WebSEAL does not start because of a SPNEGO issue, you might need to collect data for problem determination.

About this task

When directed by IBM Support, collect the SPNEGO diagnostic data when WebSEAL does not start.

Procedure

1. Turn on trace for each process by removing the # on the last line of the `/opt/pdweb/etc/routing` file. The last three lines of the routing file are shown:

   ```
   #
   # Route to a per-process text file
   #*:*.9:TEXTFILE.10.1000:/var/pdweb/log/trace__%ld.trace.log:644:ivmgr:ivmgr
   This will create a file in '/var/pdweb/log/trace __%ld.trace.log'
   ```

   Note: Ensure that enough disk space is available in the `/var` directory. If WebSEAL is started with the **`pdweb_start`** command, there are two traces with different `pids`.
2. Start WebSEAL to recreate the issue.
3. Turn off trace for each process by replacing the # at the beginning of the last line of the `/opt/pdweb/etc/routing` file.

4. Collect the following files:
   - `Webseald-`*`instance_name`*`.conf`
   - `msg__webseald-`*`instance_name`*`.log`
   - `trace_`*`pid`*`.trace.log`
   - The `krb5.conf` file if WebSEAL is on AIX, Linux, or Solaris
   - The Keytab file if WebSEAL is on AIX, Linux, or Solaris
   - `ldap.conf` for WebSEAL
   - `Activedir_ldap.conf` if Active Directory is the user registry
5. Collect the following information:
   - The output of the **pdversion** command on the WebSEAL server system
   - If WebSEAL is on AIX, Linux, or Solaris: **kinit** output when you use the keytab file
   - The **ktpass** command that is issued to create the keytab file
   - Active Directory Server version
6. Archive the data and send to support as directed by IBM Support.

Authentication method not configured

The server did not start, and the log file contains the following error:

```
HPDIA0126W Authentication method () is not configured.
```

The `[authentication-mechanisms]` stanza in the configuration file does not contain an entry for the authentication method. Add the following entry to the `[authentication-mechanisms]` stanza:

```
kerberosv5 = library_name
```

where *library_name* is the fully qualified name of the `stliauthn` shared library. The location and name of this library is operating-system specific.

- On AIX, Linux, and Solaris operating systems, the `stliauthn` library is in the `/opt/PolicyDirector/lib/` directory.

  Because different platforms use different file extensions, use the **ls** command to determine the library name.
- On Windows operating systems, the `stliauthn.dll` library is in the `c:\program files\tivoli\policy director\bin\` directory.

No match to principal in key table

The server did not start, and the log file contains the following error:

```
HPDST0130E The security service function gss_import_name returned
the error 'No principal in keytab matches desired name'
(code 0x1cff2901/486484225)
```

The principal name for the SPNEGO service that is defined in the Security Access Manager server configuration file does not have a matching key in the SPNEGO key table. This error can occur for various reasons.

The algorithm to map the service principal name to the key in the SPNEGO key table completes the following processes:

1. Completes forward and reverse name resolution for the host name that is defined in the `spnego-krb-service-name` entry of the `[spnego]` stanza to discover the canonical host name.
2. Compares canonical host name to the realms defined in the `[domain_realm]` stanza of the `krb5.conf` configuration file.

3. Validates the principal key in the SPNEGO key table.

For details about these processes, see "Algorithm to resolve host names."

The server configuration file for WebSEAL and Plug-in for Web Server contains the `[spnego]` stanza. This stanza contains the following entries to examine:

spnego-krb-service-name
Defines the service principal name in the following format:

```
HTTP@hostname
```

The following example shows a definition of this entry in the configuration file:

```
HTTP@diamond.subnet2.ibm.com
```

spnego-krb-keytab-file
Defines the SPNEGO key table. This file contains principal keys in the following format:

```
HTTP/canonical_hostname@realm
```

The following example shows a key in the key table:

```
HTTP/diamond.subnet2.ibm.com@IBM.COM
```

The Kerberos `krb5.conf` configuration file contains the `[domain_realm]` stanza. This stanza contains entries that define the supported Kerberos realms. For details about this configuration file, see your Kerberos documentation.

Algorithm to resolve host names

The following process is used to map a service principal name to a key in the SPNEGO key table:

1. Resolve the host name to an IP address. The mapping process depends on your host name resolution configuration. Typically, the `/etc/hosts` file is checked first followed by the DNS server that is configured in the `resolv.conf` file.

   If the resolution succeeds, the process continues with step 2.

   If the resolution fails, the canonical name is assumed to be the same as the host name. The process continues with step 3 on page 123.

2. Resolve the IP address to the canonical name. The mapping process depends on your host name resolution configuration. Typically, the `/etc/hosts` file is checked first followed by the DNS server that is configured in the `resolv.conf` file.

   If the IP address is found in the `/etc/hosts` file, the canonical name is set to the first host name that is listed.

   If the IP address is not found in the `/etc/hosts` file, the DNS server is queried to complete a reverse lookup on the IP address. If the DNS server returns a host name for this IP address, this host name becomes the canonical name.

   If the IP address is not found in the `/etc/hosts` file and if the DNS server does not return a host name for this IP address, the canonical name is assumed to be the same as the host name.

   Common error
   The `/etc/hosts` file lists the short name of the host before the fully qualified host name, the format of the `/etc/hosts` file is incorrect. Entries in the `/etc/hosts` file are in the following format:

IP_address fully_qualified_hostname short_name

When the format is incorrect, host name resolution might return the short name. The canonical name is then set to this short name. When this issue occurs, the Web server searches for the wrong key in the key table. The canonical name must be set to match the host name that clients use to contact the Web server.

Resolution
Contact your AIX, Linux, or Solaris system administrator on how to change entries in the following files:
- `/etc/hosts`
- `resolv.conf`

3. Map the canonical name from step 1 on page 122 or step 2 on page 122 to the realm name by checking the `[domain_realm]` stanza of the `/opt/PolicyDirector/etc/krb5.conf` file. Each entry in this stanza maps a host name or domain name to a realm name.

   The canonical host name if checked against each of the host entries. If a matching host entry is found, the realm name becomes the realm that is specified for the host. If no matching host entry is found, the domain entries are checked. If a matching domain entry is found, the realm name becomes the realm that is specified for that domain.

   If no matching domain entry is found, the realm name becomes the value of the `[libdefaults] default_realm` entry in the `/opt/PolicyDirector/etc/krb5.conf` file.

   Common error
   The entries in the `[domain_realm]` stanza of the `/opt/PolicyDirector/etc/krb5.conf` file are incorrect.

   Resolution
   Verify that the realm name specified in the `[domain_realm]` stanza is correct, and verify that the canonical name matches a host or domain entry in this stanza.

4. Verify that the key table contains this entry.

   Common error
   The key table does not contain a matching entry.

   Resolution
   Use the **am_klist** command or the **am_ktutil** program to check the SPNEGO key table for an entry in the following format:

   ```
   HTTP/canonical_name@realm_name
   ```

   For details about using the **am_ktutil** program, see "Validating keys in key tables" on page 126. For details about using the **am_klist** command, see "Listing keys in key tables" on page 127.

Problems with Kerberos

The following information can assist you when troubleshooting issues that concern Kerberos authentication.

Kerberos initialization failing

The following information describes debugging problems with the Kerberos **am_kinit** command. If the **am_kinit** command completes, it generates no output, but you can use the Kerberos **am_klist** command to view the principals in the ticket cache. If the **am_kinit** command fails, the error message provides the following details:

- The primary cause for the failure
- A hexadecimal status code
- The specific reason for the failure

The most common primary causes for the **am_kinit** command to fail are the following reasons:

- Failure to initialize the Kerberos libraries
- Unable to obtain initial credentials

Kerberos configuration

Problem: am_kinit crashes when running `am_kinit -k -t`

Solution: Some versions of **am_kinit** do not deal properly with problems when an entry is not found in a keytab file. Double-check that the keytab file has the exact same entry you are passing to **am_kinit**.

Unable to initialize Kerberos libraries

When you run the **am_kinit** command, you might receive an error message that states the following primary reason:

```
Initializing kerberos libraries failed.
```

The most common causes that the initial credentials cannot be obtained are the following reasons:

- Cannot open configuration file
- Improper format of configuration file

Cannot open configuration file: When you use the **am_kinit** command, you receive the following error:

```
Initializing kerberos libraries failed. Status 0x96c73a87
Cannot open or find the Network Authentication Service
configuration file.
```

The `/opt/PolicyDirector/etc/krb5.conf` file does not exist or cannot be opened. Verify that file exists and is readable by all users.

Improper format of configuration file: When you use the **am_kinit** command, you receive the following error:

```
Initializing kerberos libraries failed. Status 0x96c73a88
Improper format of Network Authentication Service
configuration file.
```

The `/opt/PolicyDirector/etc/krb5.conf` file contains a syntax error. No details about the syntax error are available. Edit the configuration file to identify and correct the syntax error.

Other configuration items to check when problems occur:

Problems can result because of configuration errors. Check the following configuration items when problems occur.

Other configuration items to check when problems occur:

- Check that the file permissions and ownership of the keytab file allow access by the plug-in authorization server. See the section on mapping a Kerberos principal to the Active Directory user in the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
- Check that the keytab file contains valid data and keys for the correct principal name by using the **am_ktutil** utility to display information that is contained in the keytab file.
- Check that the DNS configuration for the entire domain (domain controller and clients) is correct and that names resolve correctly and match the values in the service principal name configuration items in various locations (such as keytab file, and plug-in configuration file).
- Check that system clocks are synchronized and that a distributed time service is maintaining clock synchronization on all systems in the domain.
- Check that the network configuration is correct and that there are no issues such as congestion, incorrect routing, or name collision. Ensure that the latency is within tolerable limits. Be sure that firewalls, NAT, and other network security services do not interfere with the operation of the domain.

Unable to obtain initial credentials

When you run the **am_kinit** command, you might receive an error message that states the following primary reason:

```
Unable to obtain initial credentials.
```

The most common causes that the initial credentials cannot be obtained are the following reasons:

- Cannot resolve the network address of the key distribution center (KDC)
- Cannot contact the KDC
- Clocks are not synchronized
- Pre-authentication failure
- Client not found in authentication database, or client that is locked out

Cannot resolve address of key distribution center: When you use the **am_kinit** command, you receive the following error:

```
Unable to obtain initial credentials. Status 0x96c73adc
Cannot resolve network address for KDC in requested realm.
```

The host name for the key distribution center (KDC) that is defined in the /opt/PolicyDirector/etc/krb5.conf file is not valid. Edit this configuration file to correct the host name for the KDC.

Cannot contact the key distribution center: When you use the **am_kinit** command, you receive the following error:

```
Unable to obtain initial credentials. Status 0x96c73a9c
Cannot contact any KDC in requested realm.
```

The host name for the key distribution center (KDC) that is defined in the /opt/PolicyDirector/etc/krb5.conf file is valid, but the KDC cannot be contacted. Verify the following conditions:

- Ensure that the krb5.conf configuration file defines the correct host name and port for the KDC.
- Ensure that the KDC is running.
- Ensure that there is network connectivity between the client and the KDC.

Clocks are not synchronized: When you use the **am_kinit** command to test an AIX, Linux, or Solaris server key table, you receive the following error:

```
Unable to obtain initial credentials. Status 0x96c73a25
Clock skew too great.
```

To resolve this condition, keep system clocks synchronized. For a permanent solution, deploy a time synchronization service on your systems. For a temporary solution, adjust the clocks on the systems so they are within one minute of each other.

Pre-authentication failure: When you use the **am_kinit** command to test an AIX, Linux, or Solaris server key table, you receive the following error:

```
Unable to obtain initial credentials. Status 0x96c73a18
Preauthentication failed.
```

The key in the key table is incorrect. A common reason is that the password for the principal in the Active Directory server was changed. In this case, regenerate the key table. If the password was not changed, make sure that you generated the key table correctly by using the correct principal name, Active Directory user name, and path.

Client not found or locked out: When you use the **am_kinit** command to test an AIX, Linux, or Solaris server key table, you receive the following error:

```
Unable to obtain initial credentials. Status 0x96c73a06
Client not found in Network Authentication Service database
or client locked out.
```

The key table does not have a key for the specified principal. Check whether an error was made when the principal was typed, or whether the key table was generated incorrectly. You can use the Kerberos **am_ktutil** commands to check which keys are in the key table. For details about this procedure, see "Validating keys in key tables."

Useful Kerberos procedures

Use the following procedures to help troubleshoot a SPNEGO or Kerberos problem.

Validating keys in key tables

About this task

To validate keys in a key table, complete the following steps:

Procedure

1. Start the interactive **am_ktutil** program by entering the following command:

   ```
   /usr/krb5/sbin/am_ktutil
   ```

2. Read the key table. To specify the `spnego.keytab` file, enter the following command:

   ```
   read_kt /var/pdweb/keytab-default/spnego.keytab
   ```

3. List the keys in the key table. To list the keys in the `spnego.keytab` file, enter the following command:

   ```
   am_ktutil# list
   ```

   The generated list might show the following output:

   ```
   slot   KVNO   Principal
   ------ ------ --------------------------------------
   1      1      HTTP/diamond.example.ibm.com@IBM.COM
   ```

4. Close the interactive session by entering the following command:

   ```
   am_ktutil# quit
   ```

Results

For more information about the **am_ktutil** program, see your Kerberos documentation.

Listing caches, principals, and service principals

If you enter the Kerberos **am_klist** command without options, the command displays your credential cache, your principal name, and any ticket that grants ticket (TGT). As an example, this command can display the following output:

```
Ticket cache: /var/tmp/krb5cc_wxyz
Default principal: your_name@YOUR.REALM

  Valid starting      Expires         Service principal
24-Sep-12 12:58:02 24-Sep-12 20:58:15 krbtgt/YOUR.REALM@YOUR.REALM
24-Sep-12 13:03:33 24-Sep-12 20:58:15 host/newhost.domain@YOUR.REALM
```

For more information about the **am_klist** command, see your Kerberos documentation.

Listing keys in key tables

You can use the **am_klist** command to list the keys in the key table. To list the keys in the key table, use the following command:

```
am_klist -k key_table_name
```

You can specify the **–e** option to display the encryption types of the session key and the ticket for each key in the key table.

For more information about the **am_klist** command, see your Kerberos documentation.

Listing tickets in credential caches

You can use the **am_klist** command to list the Kerberos principal and the Kerberos tickets that are held in the credential cache. To list the Kerberos principal and the Kerberos tickets that are held in the credential cache, use the following command:

```
am_klist -c cache_name
```

If *cache_name* is not specified, the command displays the credentials in the default credential cache. If you do not know the name of the cache, run the **am_klist** command without options.

You can specify the **–e** option to display the encryption types of the session key and the ticket for each credential in the credential cache.

For more information about the **am_klist** command, see your Kerberos documentation.

Plug-in for Web Servers Configuration

The following problems and solutions can help with configuration issues for the Plug-in for Web Servers component.

Security Access Manager Plug-in for Web Servers configuration

- When a problem occurs, consider enabling trace for SPNEGO. Add an entry to the routing file. The routing file is located under the installation directory, in `etc/routing`. Example entry:

  ```
  bst:*.9:TEXTFILE:install_path/log/spnegotrace.log
  ```

  On AIX, Linux, or Solaris, the default plug-in installation directory is `/opt/pdwebpi`. Substitute the path for your installation directory. Stop and restart the plug-in. Look for error messages in the trace file.
- **Problem**: The plug-in does not start. The error message is:

  ```
  The security service function gss_import_name returned major error code 131072
  and minor error code -1765328168.
  ```

  Solution: The principal name that is specified in the configuration file was invalid. Use the form `HTTP@`*`host_name`* where *host_name* is the fully qualified DNS name of a computer which is configured into the Kerberos realm.
- **Problem**: The plug-in server does not start. The error message is:

  ```
  The security service function gss_acquire_cred returned major error code 851968
  and minor error code 39756033.
  ```

  Solution: The principal name in the configuration file does not match any of the keys in the specified keytab file. The keys in the keytab file have names like `HTTP/`*`host_name`*`@REALM`. The principal name format must be `HTTP@`*`host_name`*.

Unable to authenticate

If a user attempts to authenticate to WebSEAL or Plug-in for Web Servers by using SPNEGO authentication and the authentication fails, an HTML error page is displayed and a message is added to the log.

Ticket not yet valid

A user attempts to access WebSEAL or Plug-in for Web Servers and receives an HTML page with the following error:

```
HPDIA0100E An internal error has occurred.
```

The trace log file contains the following one of the following messages:

- `HPDST0130E The security service function gss_accept_sec_context returned the error 'Ticket not yet valid' (code 0x96c73a21/-1765328351).`
- `HPDST0130E The security service function gss_accept_sec_context returned the error 'Clock skew too great' (code 0x96c73a25/-1765328347).`

The system clock on the client system is not synchronized with the system clock on the Active Directory server. When you use Kerberos, these clocks must be synchronized. For a permanent solution, deploy a time synchronization service on your system. For a temporary solution, adjust the clocks on the system so that they are within one minute of each other.

Cannot acquire credentials

A user attempts to access WebSEAL or Plug-in for Web Servers and receives an HTML page with the following error:

```
HPDIA0114E Could not acquire a client credential.
```

This same message is written to the log file.

The user exists in the Active Directory user registry and presented valid SPNEGO authentication data, but the user does not exist in the Security Access Manager user registry.

SPNEGO authentication requires that the user exists in both the Active Directory and the Security Access Manager user registries. If you believe that the user exists in both user registries, verify that the user ID produced by SPNEGO authentication matches what you expect.

To see the user ID, complete the following steps:

1. Enable the `pd.ias` authentication trace by using the following **pdadmin** command:

   ```
   pdadmin sec_master> server task serverName trace set  \
      pd.ias 9 file path=/tmp/ias.log
   ```

2. Have the same user attempt to access the Web server again. After this user receives the HPDIA0114E message, disable the authentication trace by using the following **pdadmin** command:

   ```
   pdadmin sec_master> server task server trace set pd.ias 0
   ```

3. Examine the `/tmp/ias.log` file for a message that is similar to the following message:

   ```
   Mapped name user@realm to am_user
   ```

4. Ensure that the *am_user* user is a defined user in the Security Access Manager user registry.

Wrong principal in request

A user attempts to access WebSEAL or Plug-in for Web Servers and receives an HTML page with the following error:

```
HPDIA0100E An internal error has occurred.
```

The trace log file contains the following message:

```
HPDST0130E The security service function gss_accept_sec_context returned
the error 'Wrong principal in request' (code 0x96c73a90/-1765328240).
```

The server principal name (SPN) supplied by the client in the SPNEGO authentication header does not match the SPN being used by the Web security server. This error can be caused in the following situations:

- The user did not specify the fully qualified host name (FQHN) when you contact the Web security server. Clients must use the FQHN so that the Active Directory server can provide the client with an appropriate Kerberos authentication ticket.
- The Web security server is configured to use the wrong SPN. The host name portion of the principal in the Kerberos key table must match the host name that is being used by the client to contact the Web security server. If the principal name in the key table is incorrect, the key table must regenerate on the key distribution center (KDC) by using the **ktpass** command with the **–princ** option. The value that is specified for the **–princ** option must be the same host name that client uses to contact the Web security server.

  For example, for clients to contact the Web security server at `https://diamond.example.ibm.com` and the Web security server is in the `IBM.COM` Kerberos realm, specify the following value for the **–princ** option:

  ```
  HTTP/diamond.example.ibm.com@IBM.COM
  ```

  You can use the **am_ktutil** program to examine the contents of the Kerberos key table.

Encryption type not permitted

A user attempts to access WebSEAL or Plug-in for Web Servers and receives an HTML page with the following error:

```
HPDIA0100E An internal error has occurred.
```

The trace log file contains the following message:

```
HPDST0130E The security service function gss_accept_sec_context returned
the error 'Encryption type not permitted' (code 0x96c73ae9/-1765328151).
```

The encryption type in the SPNEGO authentication header does not match any of the encryption types that the Kerberos libraries are configured to accept. To resolve the issue, ensure that the /opt/PolicyDirector/etc/krb5.conf configuration file defines the following entries in the [libdefaults] stanza:

```
default_tkt_enctypes = rc4-hmac des-cbc-md5 des-cbc-crc aes256-cts aes128-cts
default_tgs_enctypes = rc4-hmac des-cbc-md5 des-cbc-crc aes256-cts aes128-cts
```

After you save these changes, restart the Web security server

Key version is incorrect

A user attempts to access WebSEAL or Plug-in for Web Servers and receives an HTML page with the following error:

```
HPDIA0100E An internal error has occurred.
```

The trace log file contains the following message:

```
HPDST0130E The security service function gss_accept_sec_context returned
the error 'Key version number for principal in key table is incorrect'
(code 0x96c73ae3/-1765328157).
```

The key version in the Kerberos authentication header does not match the key version in the SPNEGO key table. This error might occur after the password for the Kerberos principal for the Web security server is changed in the Active Directory server. After you change this password, complete the following steps:

1. Regenerate the SPNEGO key table.
2. Replace this key table on the Web security server.
3. Restart the Web security server

For more information, see item 870987 in the Microsoft knowledge base.

Cannot authenticate by using NTLM

When you attempt to access a Web security server, you receive the following error messages:

```
DPWWA2403E Your browser supplied NTLM authentication data.
NTLM is not supported by WebSEAL. Ensure that your browser
is configured to use Integrated Windows Authentication.
```

WebSEAL does not support NT LAN Manager (NTLM) authentication. Some browsers support NTLM authentication only or are configured to send NTLM authentication tokens instead of SPNEGO tokens. A browser that supports SPNEGO might be sending NTLM tokens for the following reasons:

- Microsoft Internet Explorer is not configured with the WebSEAL server in the “Trusted sites” or “Local intranet” zone.
- Microsoft Internet Explorer is not configured for Integrated Windows Authentication.

- The client workstation and the WebSEAL server might be a member of different Active Directory domains (Kerberos realms).
- The client workstation is not logged in to the Active Directory domain.
- The client workstation is not specifying the correct host name to access the WebSEAL server. The value that is specified for the **–princ** option of the **`ktpass`** command must be the same host name that client uses to contact the Web security server.

  For example, for clients to contact the Web security server at `https://diamond.subnet2.ibm.com` and the Web security server is in the `IBM.COM` Kerberos realm, specify the following value for the **–princ** option:

  ```
  HTTP/diamond.subnet2.ibm.com@IBM.COM
  ```

Under certain circumstances, clients cannot be prevented from sending NTLM authentication tokens. Under these circumstances, you might not be able to directly use SPNEGO authentication with the WebSEAL server. Instead, you can configure the Web Server Plug-in for IIS to serve as an e-community SSO (ECSSO) master authentication server (MAS). In this configuration, the Web server plug-in must be configured to support both NTLM and SPNEGO tokens. The WebSEAL server can now receive ECSSO tokens from the MAS.

Cannot complete authentication

When you attempt to access a security Web server, you receive the following error messages:

```
HPDIA0220I Authentication requires continuation before
completion status can be determined.
```

This error occurs when the password used to encrypt the SPNEGO authentication data is not synchronized with the password that is used by the Web security server to decrypt the SPNEGO authentication data.

On AIX, Linux, and Solaris operating systems, this error can be caused for the following reasons:

- The password for the Web security principal in Active Directory changed. When this password is changed, you must regenerate the SPNEGO key table.
- The SPNEGO key table was updated, but the client is still presenting an old authentication token. To clear the cached copy of the authentication token because SPNEGO authentication tokens are cached, log the client out of the workstation and log back in or restart the workstation.

On Windows operating systems, this error can be caused for the following reasons:

- The Web security server might be running in the foreground instead of as a service. The Web security server must be running as a service to have access to the correct password needed to decrypt the security token.
- The password for the Web security principal in Active Directory changed. If the Windows service for the Web security server is configured to log on as the Local System account, you might need to restart the system. If the Windows service for the Web security server is configured to log on using a particular Active Directory domain account, you might need to update the Windows service "Logon as" configuration to specify the correct account and password.
- Both the password and the Windows service configuration were updated, but the client is still presenting an old authentication token. To clear the cached copy of the authentication token because SPNEGO authentication tokens are cached, log the client out of the workstation and log back in, or restart the workstation.

Chapter 17. Common problems with WebSEAL servers

The following information details the common problems with WebSEAL servers.

For more information about Security Access Manager WebSEAL, see the *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Cannot customize basic authentication response

When you use basic authentication (BA-auth) with Security Access Manager, you cannot customize the acct_locked.html file to contain more images. Although you can embed images in the file, subsequent requests to access the embedded images fail.

To customize user authentication for your environment, use other authentication methods. For example, you can use forms authentication to bypass the authentication check when images from the error page are requested.

WebSEAL not responding on ports 80 or 443

WebSEAL does not respond on either port 80 or port 443.

Determine whether you have another web server that is installed on the WebSEAL system. For example, the IBM HTTP Server is commonly installed during the installation of Tivoli Directory Server. If another Web server is on the same system as WebSEAL, reconfigure it to listen on ports other than the ports that are used by WebSEAL.

Servers fail to start because of exceeded LDAP replica server limit

Security Access Manager supports a maximum of one host and nine LDAP replica servers, which are in the ldap.conf file.

If more than nine LDAP replica entries are listed in the ldap.conf file, the Security Access Manager servers cannot start. The following errors indicate this problem:

- **For the policy server:**

  ```
  HPDC00190E  Unable to configure LDAP replica
  "ldap10.ibm.com,3899,readonly,5" \
  into server, errorcode=0xe9.
  ```

  where "ldap10.ibm.com,3899,readonly,5" indicates the 10th replica entry in the ldap.conf file.
- **For WebSEAL:**

  ```
  DPWWA0314E Initialization of authorization API failed. Major status =0x1, \
  minor status = 0x1005b3a3
  ```
- **For the authorization server:**

  ```
  HPDAC0180E The Security Access Manager authorization server could not
  be started (0x1005b3a3).
  Please consult "Error Message Reference Guide" for explanation of
  minor error status 0x1005b3a3.
  ```

To resolve the error, specify no more than nine replica LDAP servers in the replica entry of the [ldap] stanza in the ldap.conf file.

For information about the `replica` entry of the `[ldap]` stanza in the `ldap.conf` file, see the *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Multiple logins with e-community

WebSEAL e-community users are prompted to log in more than one time.

This problem can occur if two WebSEAL servers are configured in the same domain. In these cases, one WebSEAL server is configured as the Master Authentication Server (MAS), and the other WebSEAL server is configured to use the MAS for authentication. Attempts to access the latter might require the user to log in more than one time if the difference in system times between the two WebSEAL servers is too great.

To address this concern, synchronize the system time on each WebSEAL server that participates in an e-community.

e-Community SSO Master Authentication Server configured with EAI

You can configure e-Community single sign-on (SSO) so that the master authentication server (MAS) uses an external authentication service (EAI) to create a token for a consumer server.

To use this configuration:

1. Specify the MAS server as the default server.
2. Enable EAI in the WebSEAL default configuration file.
3. If you use virtual hosts, configure the WebSEAL virtual hosts configuration file (`webseal-vh.conf`) to use e-Community SSO.

This configuration works for any virtual host junction that is defined in the virtual hosts configuration that is in the same domain that is defined for e-Community SSO.

Verifying junctioned, third-party Web server

Verifying the correct operation of a junctioned, third-party Web application server is similar to the procedure for WebSEAL. Enter the following URL into your browser to verify that the third-party Web server is functioning properly:

```
    http://junctioned-webserver-machinename
```

Do not specify a port number so that you can determine if the server is listening on port 80 (HTTP). If successful, the `index.html` page of the third-party Web server is displayed.

The WebSEAL junction for the Web server is created with a **`pdadmin`** command. In the following example, the junction points to the third-party Web server in the WebSEAL `/myjunction` file space:

```
pdadmin> server task webseald-webseal-machinename create -t tcp \
-p junctioned-server-port -h junctioned-webserver-machinename \
-c iv_user,iv_groups /myjunction
```

Try to access the `index.html` page on the junctioned Web server through WebSEAL with the following URL:

```
webseal-machinename/myjunction
```

If you configured the junction to use secure communication (**–t** ssl), your browser might issue warnings about the WebSEAL server certificate and prompt you for a user name and password. Enter sec_master for the user name and the appropriate password. If successful, the index.html page of the third-party Web server is displayed.

WebSEAL performance is degraded during file downloads

In Security Access Manager, you can use the io-buffer-size parameter in the **[junction]** stanza to configure the buffer size for reading and writing data to-and-from the junction. This value limits the amount of data that can be written from the socket to a junctioned server.

The optimum value for this io-buffer-size parameter is 8191 bytes (one byte less than the typical TCP buffer size of 8 KB). Severe performance degradation might occur if the value of the io-buffer-size is larger than 8191.

Similarly, you can use the io-buffer-size parameter in the **[server]** stanza to control the buffer size to read and write data to-and-from the client. The amount of data that can be written from the socket to an HTTP browser depends on the value of this parameter.

For either of these io-buffer-size parameters, a small value (for instance, 10 bytes) can hurt performance by causing frequent calls to the low-level read/write APIs. Up to a certain point, larger values improve performance. However, if the io-buffer-size exceeds the size of low-level I/O functions, there is no longer any improvement in performance. Using an io-buffer-size value that is too high degrades performance.

WebSEAL does not start after configuration to use PKCS #11

After WebSEAL is configured to use the PKCS #11 cryptographic token interface with an SSL accelerator card (such as IBM 4960), a WebSEAL startup error might occur: GSK_ERROR_PKCS11_TOKEN_NOTPRESENT.

This error is typically caused by inadequate process memory size. On AIX systems, the number of segments that a process is allotted to use limits the process memory size. You can increase process memory by increasing the maximum number of data segments. To resolve this WebSEAL startup error, set the environment variable LDR_CNTRL=MAXDATA:

```
#export LDR_CNTRL=MAXDATA=0x60000000
#/opt/pdweb/bin/pdweb_start start
```

Set the environment variable LDR_CNTRL=MAXDATA before you start WebSEAL.

DPWWA0305E inconsistent message severity

The WebSEAL message log might include an entry such as the following that is recorded as a WARNING but that the code indicates is an ERROR and the error reference reports as FATAL.

```
2006-09-04-07:17:35.188+02:00I----- 0x38CF0131 webseald WARNING wwaserver
s:\amweb600\src\pdweb\webseald\http\server\WsTcpListener.cpp
3930x000007c8 DPWWA0305E     The 'pd_tcp_write' routine failed for
'WsTcpConnector::write', errno = 10054
```

This issue is a common connection reset error. The error message reports that the other end of the connection terminated the connection. The correct severity level is WARNING.

For more information about severity levels, see "Severity of message events" on page 63.

Error when you create an LTPA junction

When you create a lightweight third-party authentication (LTPA) junction, you might receive an error that WebSEAL is unable to parse the LTPA key.

WebSphere Application Server does not add the "realm" component to a token unless global security is enabled, and WebSEAL expects this component to be present. To resolve this issue, configure global security for the LDAP registry in WebSphere and then regenerate the LTPA keyfile; WebSEAL can then successfully load the keyfile.

Password change fails in a multi-domain environment

In a multi-domain environment, WebSEAL can fail to change a user password because of insufficient ACL settings.

About this task

WebSEAL does not have correct ACL settings to search the Management Domain information in environments where:

- Security Access Manager Policy Server is configured in a non-default location. That is, a location other than **secAuthority=Default**.
- Security Access Manager subdomains exist.
- The WebSEAL instance is configured in one of the subdomains.

In this situation, WebSEAL cannot successfully change user passwords because of the lack of correct ACL settings.

You must set the correct ACLs so that WebSEAL can search the Management Domain and change user passwords in a multi-domain environment.

The provided procedure is based on the following environment:

- The Management Domain name is **Default**.
- The Management Domain is in an LDAP Suffix that is called **O=IBM,C=US**.
- There are two subdomains that are called **Domain1** and **Domain2**.

Note: You must modify the following steps to use the domain names and locations that match your environment.

Procedure

1. Create a file called `aclEntry.ldif`.
2. Copy the following contents into the file:

   Note: The two entries that start with `aclentry:` must each be entered as one line.

```
##------ START: Do not include this line -----##
dn: secAuthority=Default,o=ibm,c=us
changetype: modify
add: aclentry
aclentry:group:cn=SecurityGroup,SecAuthority=Domain1,cn=SubDomains,
  SecAuthority=Default,O=IBM,C=US,O=IBM,C=US:object:ad:normal:
  rwsc:sensitive:rwsc:critical:rwsc:system:rsc
aclentry:group:cn=SecurityGroup,SecAuthority=Domain2,cn=SubDomains,
  SecAuthority=Default,O=IBM,C=US,O=IBM,C=US:object:ad:normal:
  rwsc:sensitive:rwsc:critical:rwsc:system:rsc
##------ END: Do not include this line -------##
```

3. Save the file.
4. Run the following command to update the ACL:

   ```
   ldapmodify -h host -p port -D cn=root -w pwd -i aclEntry.ldif
   ```

Results

WebSEAL can now successfully change user passwords.

Chapter 18. Common problems with Plug-in for Web Servers

The following information can assist you when troubleshooting common problems that you might encounter with Security Access Manager Plug-in for Web Servers.

For more information about Security Access Manager Plug-in for Web Servers, see the *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.

Setting cache controls for Web servers

Configure Web servers to ensure that content that requires authorization to access is not cached between the Web server and the browser or possibly at all. Whether you must set the Web server Cache-Control setting to `private` or `no-cache` depends on the individual web pages that are served by the Web server.

Part 6. Common problems with distributed session management components

Chapter 19. Session Management Servers

The following information can assist you in troubleshooting issues with the session management server component.

You can turn on trace logs for use in debugging SMS. See “Trace logging for session management” on page 88.

The **smsbackup** gathers information to help IBM Software Support in problem determination.

Note: This utility is for use by support personnel.

MustGather information for the Session Management Server component

MustGather documents assist IBM Support in problem determination. As directed by IBM Support, gather the information that is described in this procedure for issues with the Session Management Server component.

Procedure

1. Enable the following WebSphere Application Server trace level on the DMgr and each Session Management Server: `com.tivoli.am.sms.*=all`
2. Recreate the problem.
3. Gather the following information from the system that has the Security Access Manager policy server:
   - **pdversion** > /tmp/PDVersion-PS.txt
   - All logs from the /var/PolicyDirector/log directory
   - If you use Tivoli Common Directory: All logs from the *tcd_dir*/HPD/logs directory
4. Gather the following information from the system that has WebSEAL:
   - **pdversion** > /tmp/PDVersion-WebSEAL.txt
   - All logs from the /var/pdweb/log directory
   - If you use Tivoli Common Directory, gather all logs from the *tcd_dir*/DPW/logs directory
   - /opt/pdweb/etc/webseald-instancename.conf
5. Gather the following information from the system that has the DMgr, and from each Session Management Server system:
   - **pdversion** output > /tmp/SMSLevels.txt. Depending on setup, the **pdversion** command might not exist.
   - /opt/pdsms/bin/smsservicelevel.sh /opt/pdsms >> /tmp/SMSLevels.txt
6. Collect the following files. Replace the directories, host names, and cell names in the example with the ones from your environment:

```
cd $WAS_HOME ##For example /usr/IBM/WebSphere/AppServer
tar -cvf /tmp/Ppppp.bbb.ccc.tar ./systemApps/isclite.ear/smsisc.war
tar -rvf /tmp/Ppppp.bbb.ccc.tar ./profiles/Dmgr01/config/cells/hulksterCell01/applications/DSess.ear
tar -rvf /tmp/Ppppp.bbb.ccc.tar ./profiles/Dmgr01/logs/dmgr
tar -rvf /tmp/Ppppp.bbb.ccc.tar ./profiles/Dmgr01/logs/ffdc
tar -rvf /tmp/Ppppp.bbb.ccc.tar ./profiles/AppSrv01/installedApps/hulksterCell01/DSess.ear
tar -rvf /tmp/Ppppp.bbb.ccc.tar ./profiles/AppSrv01/config/cells/hulksterCell01/applications/DSess.ear
tar -rvf /tmp/Ppppp.bbb.ccc.tar ./profiles/AppSrv01/config/cells/hulksterCell01/clusters
tar -rvf /tmp/Ppppp.bbb.ccc.tar ./profiles/AppSrv01/config/cells/hulksterCell01/nodes
tar -rvf /tmp/Ppppp.bbb.ccc.tar ./profiles/AppSrv01/logs/ffdc
tar -rvf /tmp/Ppppp.bbb.ccc.tar ./profiles/AppSrv01/logs/SMS-Server
cd /tmp
tar -rvf /tmp/Ppppp.bbb.ccc.tar ./SMSLevels.txt
cd /var/pdsms
tar -rvf /tmp/Ppppp.bbb.ccc.tar ./log
## If using Tivoli Common Directory
  cd $tcd_dir/CTGSM
  tar -rvf /tmp/Ppppp.bbb.ccc.tar ./logs

compress /tmp/Ppppp.bbb.ccc.tar
```

Note: By default, Session Management Server is deployed as the `DSess`application. You can deploy Session Management Server as a different name, such as `LabSess`. In this case, the previous directories are named `LabSess.ear`.

7. Archive the data, and provide to IBM Support as directed.

Language issue for Web Portal Manager or Session Management Server help

When online help panels do not display in the chosen language in a browser, you can set a browser option to resolve the issue. This issue can occur with the Web Portal Manager and Session Management Server components.

When this issue occurs, the system displays the language of the operating system locale. This problem occurs when browsers use different languages to access the console.

To resolve this issue, do the following steps:

For Internet Explorer:

1. Select **Tools** > **Internet Options**.
2. Under **Browsing History**, select **Settings** to open the **Temporary Internet Files and History Settings** window.
3. Select **Every time I visit the webpage** under **Check for newer versions of stored pages**.
4. Click **OK** twice.

For Firefox:

1. Enter `about:config` as the URL.

   Note: If you receive a warning about the warranty, you need to accept the warning to continue.
2. Scroll down to find the **browser.cache.check_doc_frequency** setting.
3. Double-click the **browser.cache.check_doc_frequency** setting and change the frequency to 1.
4. Click **OK**.

Note:

- If the help does not display in the locale that is set in the browser, you might need to first display a WebSphere help such as the Welcome help on the WebSphere banner. This display sets the locale so that the Web Portal Manager and SMS helps display correctly

- Helps in Arabic are not supported.

Part 7. Interoperability Issues

Chapter 20. Tivoli Common Reporting and BIRT reports

You can troubleshoot reporting problems by enabling the collection of detailed log and trace information.

If a report does not generate or generates incorrectly, click **View the report with errors** to diagnose of the underlying problem.

When you troubleshoot Tivoli Common Reporting problems, enable detailed logging. See the Tivoli Common Reporting documentation at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=%2Fcom.ibm.tivoli.tcr.doc_211%2Fic-home.html.

Location of log files

If you enable logging and tracing, the log and trace files are in the `\profiles\TIPProfile\logs\<serverName>` subdirectory of the Tivoli Common Reporting installation directory.

Standard informational log messages are written to the `SystemOut.log` file.

Detailed trace messages are written to the `trace.log` file.

Tivoli Common Reporting uses logger scripts to log during report generation. If you see JavaScript errors in the reports that you create, look for `Caused by` in the stack trace. This phrase indicates the line number of the script in the report design at which the error occurred. To see the SQL query that is generated by this error, look at the log file.

Chapter 21. Risk-Based Access External Authorization Service plug-in

The Risk-Based Access (RBA) External Authorization Service (EAS) component provides a runtime XACML EAS plug-in for WebSEAL to enforce a policy decision. WebSEAL becomes the authorization enforcement point to access resources protected by RBA.

The EAS collects context information about the user and the request, creates an XACML over SOAP decision request, and sends the information to the server.

Manage the EAS with entries in the `webseald.conf` file.

For more information about RBA-EAS, see the *IBM Security Access Manager for Web WebSEAL Administration Guide* in the IBM Security Access Manager for Web, version 7.0 Information Center at http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.isam.doc_70/welcome/html. Search for **Runtime security services external authorization service** for details.

For more information about risk-based access, see the *Installing, configuring, and administering risk-based access Guide* in the IBM Tivoli Federated Identity Manager information center at http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp.

For assistance in troubleshooting RBA EAS issues, you can enable tracing, then review the logs for information about any issue that might be occurring.

Enabling External Authorization Service tracing on WebSEAL

To enable tracing and logging for the XACML EAS plug-in, issue the following **pdadmin** command:

```
pdadmin > server task WebSEAL_server_name trace set xacml_eas_comp_name 9
filepath=path_to_log_file
```

where:

webseal_server_name
Is the name of the WebSEAL server.

xacml_eas_comp_name
Is the name of the XACML EAS component.

path_to_log_file
Is the directory where you want to store the trace log file.

For example:

```
pdadmin > server task default-webseald-localhost
trace set pdweb.xacml 9 file path=/tmp/xacml.log
```

Note: Tracing is disabled when you restart WebSEAL.

Chapter 22. Troubleshooting certificate compliance issues

When you enable Security Access Manager applications to implement a security compliance standard, certain settings are required.

The required settings apply to the standards of the following security settings:

- FIPS 140-2
- NIST Special Publications 800-131a (or SP 800-131a) Transition
- NIST SP800-131a Strict
- National Security Agency (NSA) Suite B 128 bit
- NSA Suite B 192 bit

To ensure a successful regeneration of the Security Access Manager side of the certificates, see the instructions in the *IBM Security Access Manager for Web Base Administration Guide*.

WebSphere Application Server, version 8.0, requires certain settings to properly enable compliance. See

> http://publib.boulder.ibm.com/infocenter/ieduasst/v1r1m0/index.jsp?topic=/com.ibm.iea.was_v8/was/8.0.0.3/Security/WASV8003_SecurityCryptoSignatureAlgorithm/player.html

For support for NIST SP 800-131 and NSA Suite B, you must use IBM WebSphere Application Server, version 8.0.0.3 or later.

Other troubleshooting tips:

- **Check browser configuration**

  Your browser might not support or not be configured to support the TLS protocol.

  TLS 1.2 is not enabled by default. Check your browser documentation for instructions on how to enable TLS version 1.2.

  For example, for Internet Explorer, version 8 on Windows 7 and Windows 2008, go to **Tools** > **Internet Options** > **Advanced (Tab)** > **Security** and select **Use TLS 1.2**.
- **Check user registry configuration**

  Changing an SSL protocol to TLS, version 1.2, can affect communication between WebSphere Application Server and the user registry. If you receive an error message about failed connection, check your user registry configuration.

  The user registry must support TLS, version 1.2, if you use an SSL connection.

Part 8. Collecting troubleshooting data

Chapter 23. Gathering initial diagnostic information

One of the first steps in diagnosing a problem is to determine the state of your environment, which includes locating the diagnostic tools and utilities and determining what products at what versions are installed and configured.

For problems that you might encounter during installation or initial configuration, see Chapter 3, “Troubleshooting installation and uninstallation,” on page 15.

Locating diagnostic utilities

Many of the commands, tools, scripts, and daemons that are associated with Security Access Manager are installed under the installation directory in the `/bin` and `/sbin` subdirectories. To run most of the Security Access Manager commands, you must have access to these directories and their files.

Commands can be run from any command prompt or shell. You can explicitly change to the wanted directory and run the command, or you can add the two directories to your PATH environment variable or command search path, which enables the commands to be run from any directory.

The one exception is the XML Log Viewer. This viewer is installed separately and, by default, located in its own directory. For details about this viewer, see “Viewing log files with the XML Log Viewer” on page 9.

Gathering version information

Use the information in the following sections to determine the version of the various components and products that can be installed in a Security Access Manager environment.

Security Access Manager

The **pdversion** command displays a list of Security Access Manager components and indicates the version number for any component that is installed on the system.

Sample output from the command is as follows:

```
IBM Security Access Manager for Web Runtime                      7.0.0.0
IBM Security Access Manager for Web Policy Server                7.0.0.0
IBM Security Access Manager for Web Web Portal Manager           7.0.0.0
IBM Security Access Manager for Web Application Development Kit  7.0.0.0
IBM Security Access Manager for Web Authorization Server         Not Installed
IBM Security Access Manager for Web Java Runtime Environment     7.0.0.0
IBM Security Access Manager for Web Policy Proxy Server          Not Installed
```

For reference information about the **pdversion** utility, see “pdversion” on page 185.

IBM Global Security Kit

Global Security Kit (GSKit) provides Secure Sockets Layer (SSL) communication in Security Access Manager.

Each version of Security Access Manager potentially provides a different level of GSKit. In some cases, you might:

- Apply updates to GSKit when you apply fix packs or other service.
- Install other versions of GSKit with other IBM products.

Note:

The connection might silently fail with no error message provided if both of the following circumstances are met:

- If Security Access Manager connects through Secure Sockets Layer (SSL) to an external component.
- The server runs an earlier version of GSKit.

The connection failure might be caused by version incompatibility between Transport Layer Security (TLS) supported by Security Access Manager and the external component.

Security Access Manager uses GSKit version 8, which includes important changes that are made to the implementation of Transport Layer Security required to remediate security issues.

The GSKit version 8 changes comply with the Internet Engineering Task Force (IETF) Request for Comments (RFC) requirements. However, it is not compatible with earlier versions (1.1 or 1.2) of Transport Layer Security. Any component that communicates with Security Access Manager that uses GSKit, must be upgraded to use GSKit version 7.0.4.42, or later. Otherwise, communication problems might occur.

To determine the version of GSKit 8 that is installed, use the **gsk8ver_64** command. The default location is platform-dependent:

AIX `/usr/bin`

Linux `/usr/local/ibm/gsk8_64/bin`

Solaris
`/usr/bin`

Windows
`C:\Program Files\IBM\gsk8\bin`

The **gsk8ver_64** command uses all of the GSKit shared libraries and displays version information about each library.

User registries

The Tivoli Directory Server client is used by Security Access Manager to communicate with any LDAP user registry, not just with Tivoli Directory Server. The client is not needed if Microsoft Active Directory server is being used as the Security Access Manager user registry. The Tivoli Directory Server client is installed on any system that communicates with an LDAP user registry.

To determine the version of the Tivoli Directory Server client that is installed, use the **ldapsearch** command:

```
ldapsearch –e
```

To determine the version information of the user registries, see "Verifying user registries" on page 40 for complete details.

Gathering system information

The **pdbackup** command gathers diagnostic information about your Security Access Manager system. For reference information about the **pdbackup** command, see "pdbackup" on page 179.

Note: In previous versions of Security Access Manager, the **pdinfo** command was used for this purpose. The **pdinfo** command is no longer provided as part of the product.

Chapter 24. Collecting troubleshooting data

Collecting certain kinds of information can help find a solution to your problem. If you encounter a problem that cannot be resolved with the troubleshooting documentation, contact IBM Software Support.

For details about contacting Software Support, see “Support information” on page xvi.

General information to collect

Collect the following data so that it is available for IBM Software Support:

- A brief description of the class of problem, such as installation, configuration, audit, system failure, or performance
- A detailed description of the problem, whether the problem can be re-created, and if so, the steps that are required to re-create the problem
- The hardware configuration, which includes the following data:
  - The machines make and model number of the systems where the Security Access Manager servers and the user registry server are installed
  - The operating system type, operating system version number, and patch levels of each of the involved servers
  - The output from the **pdversion** utility for each system where a Security Access Manager server is installed
  - The network connectivity to these systems
  - Whether any of the servers is configured with multiple IP addresses
  - The locale information
- The time frame in which the problem occurred so that the timestamps relate back to the log entries
- Log file of each of the involved servers

Collect this information, but do not send it until you are directed to do so by IBM Software Support.

Collecting trace information

About this task

When you report a defect, complete the following basic procedure to collect the information:

- Enable tracing on the system that is running the affected Security Access Manager server. This server can be the policy server, the policy proxy server, or the authorization. Choose the server where you have an operation that is causing the problem.
- Restart the affected server or the combination of the affected servers.
- Enable tracing on the system where you are running the application or test case that started the operations that failed.
- Restart the application or test case.
- Run the operations that failed.

To enable tracing, you need to edit the appropriate routing file. For detailed information about the available routing files and customizing the trace facility, see Chapter 12, “Trace event logs,” on page 81.

Collecting trace information by server

After you enable tracing, as explained in “Collecting trace information” on page 161, you can collect the necessary files individually instead of using the **pdbackup** utility. Depending on the type of operations that failed, you need to collect different files.

For operations that fail when you use the **pdadmin** commands, the administration C API, or the authorization C API, use the procedures in the following sections to collect the individual files:

- “Collecting the policy server trace file”
- “Collecting the authorization server trace file” on page 163
- “Collecting the policy proxy server trace file”
- “Collecting the WebSEAL trace files” on page 163
- “Collecting the C-language trace file” on page 163
- “Collecting the message files” on page 164

For operations that fail when you use the administration Java API or the authorization Java API, use the procedures in the following sections to collect the individual files:

- “Collecting the policy server trace file”
- “Collecting the authorization server trace file” on page 163
- “Collecting the policy proxy server trace file”
- “Collecting the Java language trace files” on page 164

Collecting the policy server trace file

About this task

To collect the trace files for the policy server, complete the following steps:

Procedure

1. Enter the following commands:

   Windows:

   ```
   cd installation_directory/log
   cat ivmgrd.pid
   ```

   AIX, Linux, or Solaris:

   ```
   cd /var/PolicyDirector/log
   cat ivmgrd.pid
   ```

2. From the output of this command, make note of the process ID (`pid`).
3. Collect the *pid*`.trace.log.*` files

Collecting the policy proxy server trace file

About this task

To collect the trace files for the policy proxy server, complete the following steps:

Procedure

1. Enter the following commands:

   Windows:

   ```
   cd installation_directory/log
   cat pdmgrproxyd.pid
   ```

   AIX, Linux, or Solaris:

   ```
   cd /var/PolicyDirector/log
   cat pdmgrproxyd.pid
   ```

2. From the output of this command, make note of the process ID (`pid`).
3. Collect the *pid*`.trace.log.*` files.

Collecting the WebSEAL trace files

HTTP request and response activity can be traced for the WebSEAL `pdweb.debug` and `pdweb.snoop` components. See "Trace logging for WebSEAL" on page 88 for information about collecting WebSEAL trace information.

Collecting the authorization server trace file

About this task

To collect the trace files for the authorization server, complete the following steps:

Procedure

1. Enter the following commands:

   Windows:

   ```
   cd installation_directory/log
   cat ivacld.pid
   ```

   AIX, Linux, or Solaris:

   ```
   cd /var/PolicyDirector/log
   cat ivacld.pid
   ```

2. From the output of this command, make note of the process ID (`pid`).
3. Collect the *pid*`.trace.log.*` files.

Collecting the C-language trace file

About this task

To collect the trace files for the C API or **pdadmin** command, complete the following steps.

Procedure

1. Make note of the process ID (`pid`) of the **pdadmin** process or the process ID of the application or test case that started the C API.
2. Enter the following command:

   Windows:

   ```
   cd installation_directory/log
   ```

   AIX, Linux, or Solaris:

   ```
   cd /var/PolicyDirector/log
   ```

3. Collect the *pid*`.trace.log.*` files.

Collecting the Java language trace files

About this task

To collect the trace files for the Java API, complete the following steps:

Procedure

1. Enter the following command:

   Windows:

   ```
   cd installation_directory/log
   ```

   AIX, Linux, or Solaris:

   ```
   cd /var/PolicyDirector/log
   ```
2. Collect the `trace__`*`app_name`*`.log` files.

Collecting the message files

About this task

The servers-specific message logs can help isolate problems that can occur in communication between Security Access Manager components. Table 16 lists the default names for the server-specific message log files.

Table 16. Message log files that are associated with servers

Server	Default message log file
Security Access Manager policy server	`msg__pdmgrd_utf8.log`
Security Access Manager authorization server	`msg__pdacld_utf8.log`
Security Access Manager WebSEAL	`msg__webseald–`*`instance_name`*`.log`
Security Access Manager Plug-in for Web Servers	`msg__pdwebpi.log`
Security Access Manager policy proxy server	`msg__pdmgrproxyd_utf8.log`
Security Access Manager Attribute Retrieval Service	`msg__amwebars_exceptions.log`

For the Security Access Manager Plug-in for Web Servers component, message log entries are always written, by default, to the same set of files when Tivoli Common Directory is not configured. The log files include:

Authorization server

Windows operating systems

`webpi-install-dir``\log\msg__pdwebpi.log`

AIX, Linux, and Solaris operating systems

`/var/pdwebpi/log/msg__pdwebpi.log`

IIS plug-in

Windows operating systems

`webpi-install-dir``\log\msg__pdwebpi-iis.log`

Watchdog server

AIX, Linux, and Solaris operating systems

/var/pdwebpi/log/msg__pdwebpimgr.log

To collect the message files on all the systems that run Security Access Manager servers and applications, complete the following steps:

1. Enter the following command:

   Windows:

```
cd installation_directory/log
```

AIX, Linux, or Solaris:

```
cd /var/PolicyDirector/log
```

2. Collect the following files:
   - `msg__notice*log`
   - `msg__warning*log`
   - `msg__error*log`
   - `msg__fatal*log`

Submitting your gathered data to IBM

If IBM Software Support assigns a PMR number to your problem, use the PMR number to submit the information you gathered about the problem.

Upload the information to the `/toibm/tivoli` directory on `ftp.emea.ibm.com` and specify the PMR number in the file name, *`nnnnn.bbb.ccc.description`*`.ext`.

For complete instructions on submitting PMR information, go to the following website, or consult with your IBM Software Support representative:

> http://www.ibm.com/de/support/ecurep/other.html

Chapter 25. Collecting data with IBM Support Assistant

IBM[®] Support Assistant Data Collector 2.0.1 helps you to troubleshoot IBM Security Access Manager for Web.

The tool automatically collects data so you can identify and investigate problems.

This tool provides the following benefits. You can

- Collect data with the following methods:
  - **Non-download mode** collects data from the system on which the browser is running.
  - **Download mode** downloads, extracts, and runs in either **Browser** or **Interactive command-line console** mode. Use this option when a system does not have direct access to the internet.
- Upload the data collection files to IBM Support or to another FTP server.

To use the tool, see:

- Using the IBM Support Assistant in non-download mode
- Using the IBM Support Assistant in browser mode
- Using the IBM Support Assistant in console mode

Collecting data with IBM Support Assistant in non-download mode

Use IBM Support Assistant from a browser to collect and analyze problem determination information from the system on which the browser is running.

Before you begin

You must:

- Install IBM Security Access Manager for Web 7.0.
- Install the Java 1.6 plug-in (The Java plug-in must be enabled in the browser).
- Have one of the supported browsers:
  - Internet Explorer 8 or higher
  - Firefox 3.6.3 or higher

Note: If the target system is Windows 2008, you must take one of the following actions to run IBM Support Assistant Data Collector:

- Use the command-line console mode.
- Install a Microsoft test fix on the Windows 2008 system: http://support.microsoft.com/kb/948698.
- Upgrade to Windows Server 2008 R2 edition.

About this task

This procedure requires no download or extraction. Use this procedure to collect problem determination data for systems that encountered a problem and also have internet connection.

Procedure

1. Open the IBM Support Assistant Data Collector 2.0.1 website: http://public.dhe.ibm.com/software/isa/isadc/
2. From the pull-down menu, choose **Security Access Manager**.
3. Select **this system using the current browser**
4. Select to accept the license agreement terms.
5. Click **Start Collection**.

   This step:

   - Starts the Java Applet.
   - Downloads any necessary files that are associated with the Security Access Manager collector.
   - Might prompt for permission to run the Java applet, depending on your browser.
6. In the collection menu, select one of the following collection types:
   - Collect all information.
   - Collect network information.
   - Collect registry and installed software information.
   - Collect system data information.
   - Collect user environment information.
   - Collect software/hardware inventory.
7. Click **Start**.
8. Provide any environmental information or data locations that help with troubleshooting.
9. In the Transfer Data window, choose one of the following options:
   - To transfer the file to IBM support:
     a. Select **Transfer to IBM**.
     b. Choose FTP or HTTPS. FTP is not encrypted; HTTPS is encrypted.
     c. Click **Transfer**.
   - To transfer the file to another server:
     a. Select **Transfer to another server via FTP**.
     b. Click **Transfer**.
   - To cancel the transfer, select **Do Not Transfer**.

Collecting data with the IBM Support Assistant in browser mode

You can use a graphical user interface to collect data with IBM Support Assistant.

Before you begin

You must:

- Install IBM Security Access Manager for Web 7.0
- Install the Java 1.6 plug-in (The Java plug-in must be enabled in the browser).
- Have one of the supported browsers:
  - Internet Explorer 8 or higher
  - Firefox 3.6.3 or higher

Note: If the target system is Windows 2008, you must take one of the following actions to run IBM Support Assistant Data Collector:

- Use the command-line console mode.
- Install a Microsoft test fix on the Windows 2008 system: http://support.microsoft.com/kb/948698.
- Upgrade to Windows Server 2008 R2 edition.

About this task

This procedure downloads the IBM Support Assistant Data Collector tool. You can transfer the tool to another system for data collection.

Procedure

1. Open the IBM Support Assistant Data Collector 2.0.1 website: http://public.dhe.ibm.com/software/isa/isadc/
2. From the pull-down menu, choose **Security Access Manager**.
3. Select **this or another system using a downloadable utility**
4. Select to accept the license agreement terms.
5. Select one of the following options that are based on the platform of the target system to download and save the compressed archive file:
   - **Download Windows**
   - **Download Unix/Linux**
6. Extract the tool to any directory. The extraction creates a subdirectory `\isadc` in the target directory.
7. Open the `index.html` file in the `/isadc` installation directory into a web browser to start the IBM Support Assistant Data Collector. This step
   - Starts a graphical user interface.
   - Starts the Java Applet.
   - Downloads any necessary files that are associated with the Security Access Manager collector.
   - Might prompt for permission to run the Java Applet, depending on your browser.
8. In the collection menu, select one of the following collection types:
   - Collect all information.
   - Collect network information.
   - Collect registry and installed software information.
   - Collect system data information.
   - Collect user environment information.
   - Collect software/hardware inventory.
9. Click **Start**.
10. Provide any environmental information or data locations that help with troubleshooting.
11. In the Transfer Data window, choose from the following options:
    - To transfer the data collection archive to IBM support:
      a. Select **Transfer to IBM**.
      b. Choose FTP or HTTPS. FTP is not encrypted; HTTPS is encrypted.
      c. Click **Transfer**.
    - To transfer the file to another server:
      a. Select **Transfer to another server via FTP**.
      b. Click **Transfer.**

- To cancel the transfer, select **Do Not Transfer**.

Collecting data with the IBM Support Assistant in console mode

You can collect data with IBM Support Assistant in console mode.

Before you begin

You must:

- Install IBM Security Access Manager for Web 7.0.
- Install Java Runtime Environment 1.6.

About this task

When IBM Support Assistant Data Collector runs in command-line console mode, there are no selection lists or entry fields for user input. Instead, available choices are presented as numbered lists.

Procedure

1. On the target system, ensure that the Java environment is configured correctly:
   a. Verify that the Java runtime environment is at level 1.6.0 or higher.
   b. Determine whether the location of the Java runtime environment is included in the PATH environment setting. If the location is not included in the path, set the variable *`JAVA_HOME`* to point to the Java runtime environment.

Table 17. Specifying JAVA_HOME for your environment

Operating system	Sample command
Windows	For example, if you have a Java Development Kit that is installed at `C:\jre1.6.0`, use the command: `SET JAVA_HOME=C:\jre1.6.0`
AIX, Linux, or Solaris	For example, if you use the bash shell and have a Java Development Kit that is installed at `/opt/jre160`, use the command: `export JAVA_HOME=/opt/jre160`

2. Open the IBM Support Assistant Data Collector 2.0.1 website:http://public.dhe.ibm.com/software/isa/isadc/
3. From the pull-down menu, choose **Security Access Manager**.
4. Select **this or another system using a downloadable utility.**
5. Select to accept the license agreement terms.
6. Select one of the following options that are based on the platform of the target system to download the compressed archive file:
   - **Download Windows**
   - **Download Unix/Linux**
7. Extract the tool to any directory. The extraction creates a subdirectory `\isadc` in this target directory.
8. Start the IBM Support Assistant tool:
   a. Open a command window,
   b. Change the directory to the `\isadc` directory.
   c. Enter one of the following commands:

a.

Table 18. Running IBM Support Assistant

Operating system type	Command
Windows	`isadc.bat`
AIX, Linux, or Solaris	`./isadc.sh`

Note: If you need assistance, use one of the following commands:

Operating System type	Command
Windows	`isadc.bat -help`
AIX, Linux, or Solaris	`./isadc.sh -help`

The IBM Support Assistant now starts in console mode.

9. In the collection menu, select one of the following collection types:
   - Collect all information.
   - Collect network information.
   - Collect registry and installed software information.
   - Collect system data information.
   - Collect user environment information.
   - Collect software/hardware inventory.
10. When prompted, type the number of your selection and press`Enter`.
11. Provide any environmental information or data locations that help with troubleshooting.
12. In the Transfer Data window, choose from the following options:
    - To transfer the data collection archive to IBM support:
      a. Select **Transfer to IBM**.
      b. Choose FTP or HTTPS. FTP is not encrypted; HTTPS is encrypted.
      c. Click **Transfer**.
    - To transfer the file to another server:
      a. Select **Transfer to another server via FTP**.
      b. Click **Transfer.**
    - To cancel the transfer, select **Do Not Transfer**.

Part 9. Appendixes

Appendix A. Serviceability commands

The following reference information describes the serviceability and problem determination **pdadmin** commands and utilities.

Reading syntax statements

The reference documentation uses the following special characters to define syntax:

[ ]	Identifies optional options. Options that are not enclosed in brackets are required.
...	Indicates that you can specify multiple values for the previous option.
|	Indicates mutually exclusive information. You can use the option to the left of the separator or the option to the right of the separator. You cannot use both options in a single use of the command.
{ }	Delimits a set of mutually exclusive options when one of the options is required. If the options are optional, they are enclosed in brackets ([ ]).
\	Indicates that the command line wraps to the next line. It is a continuation character.

The options for each command or utility are listed alphabetically in the Options section or Parameters section. When the order of the options or parameters must be used in a specific order, this order is shown in the syntax statements.

Serviceability and problem determination commands

Table 19 lists the serviceability and problem determination commands that are available with the **pdadmin** utility.

Table 19. Serviceability and problem determination commands

Command	Description
"server list"	Lists all registered Security Access Manager servers.
"server task trace" on page 176	Enables the gathering of trace information for components of installed Security Access Manager servers or server instances that support debug event tracing.

For information about the command modes for the **pdadmin** utility, see the *IBM Security Access Manager for Web Command Reference*.

server list

Lists all registered Security Access Manager servers.

Requires authentication (administrator ID and password) to use this command.

Syntax

```
server list
```

Description

Lists all registered Security Access Manager servers. The name of the server for all server commands must be entered in the exact format as it is displayed in the output of this command. The **server list** command does not have such a requirement.

Options

None.

Return codes

0 The command completed successfully.

1 The command failed. When a command fails, the **pdadmin** command provides a description of the error and an error status code in hexadecimal format (for example, 0x14c012f2). See the *IBM Security Access Manager for Web Error Message Reference*. This reference provides a list of the Security Access Manager error messages by decimal or hexadecimal codes.

Example

The following example lists registered servers:

```
pdadmin> server list
```

The output is as follows:

```
ivmgrd-master
ivacld-server1
ivacld-server2
```

where ivmgrd-master represents the Policy server; ivacld-server2 and ivacld-server1 represent Authorization server instances.

server task trace

Enables the gathering of trace information for components of installed Security Access Manager servers or server instances.

Requires authentication (administrator ID and password) to use this command.

Syntax

server task *server_name–host_name* **trace list** [*component*]

server task *server_name–host_name* **trace set** *component level* [*destination*]

server task *server_name–host_name* **trace show** [*component*]

Description

The **server task trace** command enables the gathering of trace information for components of installed Security Access Manager servers or server instances that support debug event tracing. The content of trace messages is generally undocumented and is intended to be used for debugging purposes only. The format and content of trace messages might vary between product releases.

Options

component
Specifies the component for which to enable (set) tracing.

destination
Specifies where the gathered statistics are written, where *destination* can be one of the following:

file path=*file_name*
Specifies the fully qualified file name.

log_agent
Specifies a destination for the statistics information gathered for the specified component. For more information about event logging, see the *IBM Security Access Manager for Web: Administration Guide*.

level
Specifies the level of tracing. The supported values for this option are `1` through `9`, with `9` reporting the most detailed level of information in the trace log.

server_name–*host_name*
Specifies the name of the server or server instance. You must specify the server name in the exact format as it is shown in the output of the **`server list`** command.

For example, if the configured name of a single WebSEAL server on host `cruz.dallas.ibm.com` is `default`, the *server_name* would be `default-webseald` and the *host_name* would be `cruz.dallas.ibm.com`. For this example, the name of the server would be `default-webseald-cruz.dallas.ibm.com`.

If there are multiple configured server instances on the same machine, for example, the host `cruz.dallas.ibm.com`, and the configured name of the WebSEAL server instance is `webseal2-webseald`, the *server_name* would be `webseal2-webseald` and the *host_name* would be `cruz.dallas.ibm.com`. For this example, the name of the server instance would be `webseal2-webseald-cruz.dallas.ibm.com`.

trace list [*component*]
Lists all enabled trace components that are available to gather and report trace information. If you specify the *component* option and the component is enabled, the output lists that component; otherwise, no output is displayed. If you do not specify the *component* option, the output lists all enabled components.

trace set *component level* [*destination*]
Sets the trace level and trace message destination for a specific *component* and its subordinates. The value for the *level* option is a single integer from `1` to `9`, with `9` reporting the most detailed level of information. The *destination* option specifies where the gathered trace information is written.

trace show [*component*]
Shows the names and levels for all enabled trace components. If you specify the *component* option, the output lists the name and level for the specified component.

Return codes

0
The command completed successfully.

1
The command failed. When a command fails, the **`pdadmin`** command

provides a description of the error and an error status code in hexadecimal format (for example, 0x14c012f2). Refer to the *IBM Security Access Manager for Web: Error Message Reference*. This reference provides a list of the Security Access Manager error messages by decimal or hexadecimal codes.

Examples

- The following example enables the pdweb.debug trace component to level 2. Then displays the output for all enabled components. Note that WebSEAL–specific components are prefixed with pdweb.

  ```
  pdadmin sec_master> server task webseald-instance_name trace set
  pdweb.debug 2

  pdadmin sec_master> server task webseald-instance_name trace show
  ```

  Output from the **trace show** command is similar to:

  ```
  pdweb.debug 2
  ```

- The following example enables the pdwebpi.module.session-cookie trace component to level 9. Then displays the output for all enabled components. Components that are specific to the Web server plug-ins are prefixed with pdwebpi.

  ```
  pdadmin sec_master> server task pdwpi-tivoli.com trace set
  pdwebpi.module.session-cookie 9

  pdadmin sec_master> server task pdwpi-tivoli.com trace show
  ```

  Output from the **trace show** command is similar to:

  ```
  pdwebpi.module.session-cookie 9
  ```

See also

"server list" on page 175

Serviceability and problem determination utilities

Table 20 lists the serviceability and problem determination utilities.

Table 20. Serviceability and problem determination utilities

Utility	Description
"pdbackup" on page 179	Backs up, restores, and extracts Security Access Manager data.
"pdjservicelevel" on page 183	Returns the service level of installed Security Access Manager files that use the IBM Security Access Manager Runtime for Java package.
"pdservicelevel" on page 184	Returns the service level of installed Security Access Manager files that use the Security Access Manager Runtime package.
"pdversion" on page 185	Lists the current version of Security Access Manager components that are installed on the system.
"pdwebpi" on page 186	Returns the current version of Security Access Manager Plug-in for Web Servers. Also, specifies whether to run Plug-in for Web Servers as a daemon or run it in the foreground.
"pdwpi-version" on page 187	Lists the version and copyright information for the Security Access Manager Plug-in for Web Servers installation.

pdbackup

Backs up, restores, and extracts Security Access Manager data.

Syntax

`pdbackup` –action backup –list *list_file* [**–path** *path*] [**–file** *filename*]

`pdbackup` –action restore –file *filename* [**–path** *path*]

`pdbackup` –action extract –file *filename* **–path** *path*

`pdbackup` –usage

`pdbackup` –?

Description

Use the **`pdbackup`** utility to back up and restore Security Access Manager data. As an alternative to a restore action, you can extract all archived files into a single directory. This utility is most commonly used for backing up, restoring, and extracting Security Access Manager component files.

Note: Before performing backup and restore actions, stop the Security Access Manager servers on the target machine to ensure a consistent snapshot, or replacement, of files. Stopping the Security Access Manager servers prevents the servers from updating, and possibly overwriting, the files that you want to backup or restore.

Note: On Windows 2008 systems with Tivoli Access Manager 6.0, 6.1, or 6.1.1: The **`pdbackup`** utility on Windows 2008 may hang while waiting for user input. If you encounter this issue, use either of the following approaches to continue restoring the policy server:

- Type an "A" in the command window. The utility resumes normally.
- Apply the following fix pack for your respective Tivoli Access Manager release, then rerun the **`pdbackup`** utility:
  - **Tivoli Access Manager 6.0**: Fixpack 28 or later
  - **Tivoli Access Manager 6.1**: Fixpack 08 or later
  - **Tivoli Access Manager 6.1.1**: Fixpack 04 or later

Parameters

You can shorten a parameter name, but the abbreviation must be unambiguous. For example, you can type `–a` for **–action** or `–l` for **–list**. However, values for parameters cannot be shortened.

–? Displays the syntax and an example for this utility.

–action [backup | restore | extract]
Specifies to action to be performed. This parameter supports one of the following values:

backup
Backs up the data, service information, or migration information to

an archive file. The archive file has a `tar` extension on AIX, Linux, and Solaris operating systems and a `dar` extension on Windows operating systems.

extract Extracts the data from an archive file to a specified directory. This action is used during a two-machine migration only.

restore
Restores the data from the archive file.

–file *filename*
Specifies the name of the archive file. When this parameter is required, its value must be the fully qualified name of the archive file. When this parameter is optional, its value must be the name of the archive file only. For the **extract** and **restore** actions, this parameter is required. For the **backup** action, this parameter is optional.

When using the **backup** action, specifies a file name other than the default name. The default name is the name of the service list file with a date and time of the file creation. On AIX, Linux, and Solaris operating systems, the default file name is *`list_file_ddmmmyyyy.hh_mm`*`.tar`. On Windows operating systems, the default file name is *`list_file_ddmmmyyyy.hh_mm`*`.dar`.

–list *list_file*
Specifies the fully qualified name of the list file. The list file is an ASCII file that contains the information about the various files and data to back up. These files are located in the `/etc` directory under the component-specific installation directory. The following list contains the default file name and location of each component-specific list file by operating system. The assumption is that the default installation directory was used during installation:

Security Access Manager data

On AIX, Linux, and Solaris operating systems:
`/opt/PolicyDirector/etc/pdbackup.lst`

On Windows operating systems:
`C:\Program Files\Tivoli\Policy Director\etc\pdbackup.lst`

Security Access Manager service information

On AIX, Linux, and Solaris operating systems:
`/opt/PolicyDirector/etc/pdinfo.lst`

On Windows operating systems:
`C:\Program Files\Tivoli\Policy Director\etc\pdinfo.lst`

WebSEAL data

On AIX, Linux, and Solaris operating systems:
`/opt/pdweb/etc/amwebbackup.lst`

On Windows operating systems:
`C:\Program Files\Tivoli\pdweb\etc\amwebbackup.lst`

WebSEAL service information

On AIX, Linux, and Solaris operating systems:
`/opt/pdweb/etc/pdinfo-amwebbackup.lst`

On Windows operating systems:
`C:\Program Files\Tivoli\pdweb\etc\pdinfo-amwebbackup.lst`

Plug-in for web servers data

On AIX, Linux, and Solaris operating systems:
`/opt/pdwebpi/etc/pdwebpi.lst`

On Windows operating systems:
`C:\Program Files\Tivoli\pdwebpi\etc\pdwebpi.lst`

Plug-in for web servers service information

On AIX, Linux, and Solaris operating systems:
`/opt/pdwebpi/etc/pdinfo-pdwebpi.lst`

On Windows operating systems:
`C:\Program Files\Tivoli\pdwebpi\etc\pdinfo-pdwebpi.lst`

–path *path*

Specifies the target directory for the specified action. This parameter is required with the **extract** action, but is optional with the **backup** and **restore** actions.

When specified with the **backup** action, specifies the target directory for the archive file. When not specified, the command uses the default directory for the component. The following list contains the default directory for each component by operating system:

On AIX, Linux, and Solaris operating systems
`/var/PolicyDirector/pdbackup/`

On Windows operating systems:
`C:\Program Files\Tivoli\Policy Director\pdbackup\`

With the **extract** action, specifies the directory where the files that are extracted from the archive file are stored. There is no default value for the **–path** parameter when used for an **extract** action.

- On AIX, Linux, and Solaris operating systems only, when specified with the **restore** action, specifies the directory where the files from the archive file are restored. By default, this path is one used during the backup process. On Windows operating systems, the restore process does not support the **–path** parameter. On Windows operating systems, the files are restored to their original directory.

–usage

Displays the syntax and an example for this utility.

Availability

This utility is located in one of the following default installation directories:

On AIX, Linux, and Solaris operating systems:

`/opt/PolicyDirector/bin`

On Windows operating systems:

`C:\Program Files\Tivoli\Policy Director\bin`

When an installation directory other than the default is selected, this utility is located in the `/bin` directory under the installation directory (for example, *`installation_directory`*`/bin`).

Return codes

0 The utility completed successfully.

1 The utility failed. When a utility fails, a description of the error and an error status code in hexadecimal format is provided (for example, `0x15c3a00c`). See the *IBM Security Access Manager for Web: Error Message Reference*. This reference provides a list of the Security Access Manager error messages by decimal or hexadecimal codes.

Examples

- The following example backs up the Security Access Manager data on a Windows operating system. The example uses default values for the archive files:

  ```
  pdbackup -a backup -list \
  C:\Program Files\Tivoli\Policy Director\etc\pdbackup.lst
  ```

  If the command is run on 22 December 2011 at 10:22 AM, the pdbackup.lst_22dec2011.10_22.dar archive file is created and stored in the C:\Program Files\Tivoli\Policy Director\pdbackup\ directory.
- The following example:
  - Backs up the WebSEAL service information about an AIX, Linux, or Solaris operating system.
  - Stores the archive in the /var/backup directory.

  ```
  pdbackup -a backup -list \
  /opt/pdweb/etc/pdinfo-amwebbackup.lst \
  -path /var/backup
  ```

  If the command is run on 22 December 2011 at 10:22 AM, the pdinfo-amwebbackup.lst_22dec2011.10_22.tar archive file is created and stored in the /var/pdbackup directory.
- The following example:
  - Backs up the plug-in for web servers files on a Linux operating system.
  - Creates the webpi.tar file in the /var/pdback directory.

  ```
  pdbackup -a backup -list \
  /opt/pdwebpi/etc/pdwebpi.lst \
  -f webpi -p /var/pdback
  ```

  Independent of when the command is run, the webpi.tar file is created in the /var/pdback directory. The .tar file extension is added to file name during the backup process.
- The following example restores the pdbackup.lst_22dec2011.10_22.dar archive file on a Windows operating system from the default location.

  ```
  pdbackup -a restore -f C:\Program Files\Tivoli\Policy \
  Director\pdbackup\pdbackup.lst_22dec2011.10_22.dar
  ```

  The file is restored to its original location. On Windows operating systems, files cannot be restored to another location.
- The following example restores the amwebbackup.lst_22dec2011.10_22.tar archive file that is stored in the /var/pdbackup directory to the /amwebtest directory:

  ```
  pdbackup -a restore -f \
  /var/pdbackup/amwebbackup.lst_22dec2011.10_22.tar \
  -p /amwebtest
  ```
- The following example extracts the amwebbackup.lst_22dec2011.10_22.tar archive file that is stored in the /var/pdbackup directory to the /amwebextracttest directory:

  ```
  pdbackup -a extract -f \
  /var/pdbackup/amwebbackup.lst_22dec2011.10_22.tar \
  -p /amwebextracttest
  ```

pdjservicelevel

Returns the service level of installed Security Access Manager files that use the IBM Security Access Manager Runtime for Java package.

Note: This utility is for use by support personnel.

Syntax

```
pdjservicelevel directory
```

Description

The **pdjservicelevel** utility recursively scans the specified directory and returns the name and service level for each file to standard output. Only executable programs, shared libraries, archives, and other such files have a service level.

If the service level for a file cannot be determined, the string "Unknown" is written to standard output. Generally, ASCII files and other such files do not have service levels.

Note: For this utility to determine the service level of a JAR file, the Java **jar** utility must exist in the system PATH statement. When the **jar** utility cannot be found, the service level that is reported for all JAR files is "Unknown".

Parameters

directory
Specifies the fully qualified name of the directory.

Availability

This utility is installed as part of the IBM Security Access Manager Runtime for Java package. It is in one of the following default installation directories:

- On AIX, Linux, and Solaris operating systems:
  `/opt/PolicyDirector/sbin`
- On Windows operating systems:
  `C:\Program Files\Tivoli\Policy Director\sbin`

When an installation directory other than the default is selected, this utility is in the `/sbin` directory under the installation directory (for example, *installation_directory*/sbin).

Return codes

0 The utility completed successfully.

1 The utility failed. When a utility fails, a description of the error and an error status code in hexadecimal format is provided (for example, `0x15c3a00c`). See the *IBM Security Access Manager for Web Error Message Reference*. This reference provides a list of the Security Access Manager error messages by decimal or hexadecimal codes.

pdservicelevel

Returns the service level of installed Security Access Manager files that use the Security Access Manager Runtime package.

Note: This utility is for use by support personnel.

Syntax

`pdservicelevel` *directory*

Description

The **`pdservicelevel`** utility recursively scans the specified directory and returns the name and service level for each file to standard output. Only executable programs, shared libraries, archives, and other such files have a service level.

If the service level for a file cannot be determined, the string `"Unknown"` is written to standard output. Generally, ASCII files and other such files do not have service levels.

Note: For this utility to determine the service level of a JAR file, the Java **`jar`** utility must exist in the system PATH statement. When the **`jar`** utility cannot be found, the service level that is reported for all JAR files is `"Unknown"`.

Parameters

directory
Specifies the fully qualified name of the directory.

Availability

This utility is installed as part of the Security Access Manager Runtime package. It is located in one of the following default installation directories:

- On AIX, Linux, and Solaris operating systems:
  `/opt/PolicyDirector/sbin`
- On Windows operating systems:
  `C:\Program Files\Tivoli\Policy Director\sbin`

When an installation directory other than the default is selected, this utility is located in the `/sbin` directory under the installation directory (for example, *`installation_directory`*`/sbin`).

Return codes

0 The utility completed successfully.

1 The utility failed. When a utility fails, a description of the error and an error status code in hexadecimal format is provided (for example, `0x15c3a00c`). See the *IBM Security Access Manager for Web: Error Message Reference*. This reference provides a list of the Security Access Manager error messages by decimal or hexadecimal codes.

pdversion

Lists the current version of Security Access Manager components that are installed on the system.

Syntax

pdversion [–key *key1, key2...keyX*] [–separator *delimiter_character*]

Parameters

–key *key1, key2...keyX*

Specifies the component or components of the current version. (Optional) The following are possible values of –key:

- pdacld – Security Access Manager Authorization Server
- pdauthadk – Security Access Manager Application Developer Kit
- pdjrte – Security Access Manager Runtime for Java
- pdmgr – Security Access Manager Policy Server
- pdmgrprxy – Security Access Manager Policy Proxy Server
- pdrte – Security Access Manager Runtime
- pdsms – Security Access Manager Session Manager Server
- pdweb – Security Access Manager WebSEAL
- pdwebars – Security Access Manager Attribute Retrieval Service
- pdwebadk – Security Access Manager Web Security ADK
- pdwebrte – Security Access Manager Web Security Runtime
- pdwebpi – Security Access Manager Plug-in for Web Servers
- pdwebpi.apache – Security Access Manager Plug-in for Apache
- pdwebpi.ihs – Security Access Manager Plug-in for IBM HTTP Server
- pdwpm – Security Access Manager Web Portal Manager
- tivsecutl – IBM Tivoli Security Utilities

The version information for the various blades shows up when the blade packages are installed on the system. The following components are basic components:

- Security Access Manager Runtime
- Security Access Manager Policy Server
- Security Access Manager Web Portal Manager
- Security Access Manager Application Developer Kit
- Security Access Manager Authorization Server
- Security Access Manager Runtime for Java
- Security Access Manager Policy Proxy Server

The following components are blades:

- Security Access Manager Plug-in for web Servers
- Security Access Manager WebSEAL
- Security Access Manager web Security Runtime
- Security Access Manager web Security ADK
- Security Access Manager Session Manager Server
- Security Access Manager Attribute Retrieval Service

–separator *delimiter_character*

Specifies the separator that is used to delimit the description of the component from its version. (Optional)

Availability

This utility is in one of the following default installation directories:

- On AIX, Linux, and Solaris operating systems:
  ```
  /opt/PolicyDirector/bin
  ```
- On Windows operating systems:
  ```
  C:\Program Files\Tivoli\Policy Director\bin
  ```

When an installation directory other than the default is selected, this utility is in the /bin directory under the installation directory (for example, *installation directory*/bin).

Return codes

0 The utility completed successfully.

1 The utility failed. When a utility fails, a description of the error and an error status code in hexadecimal format is provided (for example, 0x15c3a00c). See the *IBM Security Access Manager for Web Error Message Reference*. This reference provides a list of the Security Access Manager error messages by decimal or hexadecimal codes.

Examples

- The following example lists the base components of Security Access Manager:
  ```
  > pdversion
  ```

```
Security Access Manager Runtime                                   7.0.0.0

Security Access Manager Policy Server                             7.0.0.0

Security Access Manager Web Portal Manager                        7.0.0.0

Security Access Manager Application Developer Kit                 7.0.0.0

Security Access Manager Authorization Server                      7.0.0.0

Security Access Manager Runtime for Java                          7.0.0.0

Security Access Manager Policy Proxy Server                       7.0.0.0

IBM Tivoli Security Utilities                                     7.0.0.0
```

- The following example lists the Security Access Manager Runtime package (PDRTE) and specifies X as the delimiter to separate the component description from its version:
  ```
  > pdversion -key pdrte -separator X
  Security Access Manager
   RuntimeX7.0.0.0
  ```

pdwebpi

Returns the current version of Security Access Manager plug-in for web servers. Also specifies whether to run plug-in for web servers as a service or run it in the foreground.

Syntax

pdwebpi [–foreground] [–version]

Description

The **pdwebpi** utility returns the current version of Security Access Manager plug-in for web servers. Also, specifies whether to run plug-in for web servers as a daemon or run it in the foreground.

Note: When you use Windows Remote Desktop Connection, you must run the plug-in as a service.

Parameters

–foreground
: Runs the Plug-in for the binary file of the web server in the foreground as opposed to running it as a daemon. (Optional)

–version
: Specifies the version information for the plug-in for web servers installation. (Optional)

Availability

This utility is in the following default installation directories:

- On AIX, Linux, and Solaris operating systems:
  `/opt/pdwebpi/bin`
- On Windows operating systems:
  `C:\Program Files\Tivoli\pdwebpi\bin`

When an installation directory other than the default is selected, this utility is in the `/bin` directory under the installation directory (for example, *`installation directory`*`/bin`).

Return codes

0 The utility completed successfully.

1 The utility failed. When a utility fails, a description of the error and an error status code in hexadecimal format is provided (for example, `0x14c012f2`). See the *IBM Security Access Manager for Web Error Message Reference*. This reference provides a list of the Security Access Manager error messages by decimal or hexadecimal codes.

pdwpi-version

Lists the version and copyright information for plug-in for web servers.

Syntax

`pdwpi-version` [`–h`] [`–V`] [`–l`|`binary` [*`binary`* ...]]

Parameters

–h Displays a help or usage message. (Optional)

–l Specifies the long list version of all installable files, not just the package version. (Optional)

–V Displays the version information for the **`pdwpi-version`** installable file. (Optional)

binary [*binary*]
Displays version information for the specified installable files. If no installable file is specified, displays all files. (Optional)

Availability

This utility is in one of the following default installation directories:

- On AIX, Linux, and Solaris operating systems:
  `/opt/pdwebpi/bin`
- On Windows operating systems:
  `C:\Program Files\Tivoli\pdwebpi\bin`

When an installation directory other than the default is selected, this utility is in the `/bin` directory under the installation directory (for example, *installation directory*`/bin`).

Return codes

0 The utility completed successfully.

1 An error occurred.

Appendix B. Support Information

To isolate and resolve problems with your IBM products, you can use the troubleshooting and support information. This information contains instructions for using the problem-determination resources that are provided with your IBM products, including Security Access Manager.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When you start to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?

- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or were not fully tested together.

When does the problem occur?

Develop a detailed timeline of events that led up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:
- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:
- Does the problem always occur when the same task is being completed?
- Does a certain sequence of events need to happen for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might occur around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business affect, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications that encounter the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the information center for this product. However, sometimes you need to look beyond the information center to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

- Search for content by using the IBM Support Assistant (ISA).

  ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.
- Find the content that you need by using the IBM Support Portal.

  The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.
- Search for content about this product by using one of the following additional technical resources:
  - Security Access Manager Support website
- Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the **Search** field at the top of any ibm.com® page.
- Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

  Tip: Include “IBM” and the name of the product in your search if you are looking for information about an IBM product.

Getting fixes

A product fix might be available to resolve your problem.

About this task

Procedure

To find and install fixes:

1. Obtain the tools required to get the fix.
2. Determine which fix you need.
3. Download the fix. Open the download document and follow the link in the "Download package" section.
4. Apply the fix. Follow the instructions in the "Installation Instructions" section of the download document.
5. Subscribe to receive weekly email notifications about fixes and other IBM Support information.

Getting fixes from Fix Central

You can use Fix Central to find the fixes for various products, including Security Access Manager. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. A Security Access Manager product fix might be available to resolve your problem.

About this task

Procedure

To find and install fixes:

1. Obtain the tools that are required to get the fix. If it is not installed, obtain your product update installer. You can download the installer from Fix Central. This site provides download, installation, and configuration instructions for the update installer.
2. Select Security Access Manager as the product, and select one or more check box that are relevant to the problem that you want to resolve.
3. Identify and select the fix that is required.
4. Download the fix.
   a. Open the download document and follow the link in the "Download Package" section.
   b. When downloading the file, ensure that the name of the maintenance file is not changed. This change might be intentional, or it might be an inadvertent change that is caused by certain web browsers or download utilities.
5. Apply the fix.
   a. Follow the instructions in the "Installation Instructions" section of the download document.
   b. For more information, see the "Installing fixes with the Update Installer" topic in the product documentation.
6. Optional: Subscribe to receive weekly email notifications about fixes and other IBM Support updates.

Contacting IBM Support

IBM Support assists with product defects, answers FAQs, and helps users resolve problems with the product.

Before you begin

After you try to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before you contact IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the “*Software Support Handbook*”.

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):
   - Online through the IBM Support Portal: You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
   - By telephone for critical, system down, or severity 1 issues: For the phone number to call in your region, see the Directory of worldwide contacts web page.

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

What to do next

Exchanging information with IBM

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Sending information to IBM Support

To reduce the time that is required to resolve your problem, you can send trace and diagnostic information to IBM Support.

Procedure

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR).
2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data manually or automatically:
   - Collect the data manually.
   - Collect the data automatically.
3. Compress the files by using the `.zip` or `.tar` file format.
4. Transfer the files to IBM. You can use one of the following methods to transfer the files to IBM:
   - IBM Support Assistant
   - The Service Request tool
   - Standard data upload methods: FTP, HTTP
   - Secure data upload methods: FTPS, SFTP, HTTPS
   - Email

   All of these data exchange methods are explained on the IBM Support website.

Receiving information from IBM Support

Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as `anonymous`. Use your email address as the password.
2. Change to the appropriate directory:
   a. Change to the `/fromibm` directory.
      ```
      cd fromibm
      ```
   b. Change to the directory that your IBM technical-support representative provided.
      ```
      cd nameofdirectory
      ```
3. Enable binary mode for your session.
   ```
   binary
   ```
4. Use the **`get`** command to download the file that your IBM technical-support representative specified.
   ```
   get filename.extension
   ```
5. End your FTP session.
   ```
   quit
   ```

Subscribing to Support updates

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

About this task

By subscribing to receive updates about this product, you can receive important technical information and updates for specific IBM Support tools and resources. You can subscribe to updates by using one of two approaches:

RSS feeds and social media subscriptions

RSS feeds and social media subscriptions are available for IBM Security Access Manager for Web.

For general information about RSS, including steps for getting started and a list of RSS-enabled IBM web pages, visit the IBM Software Support RSS feeds site.

My Notifications

With My Notifications, you can subscribe to Support updates for any IBM product. (My Notifications replaces My Support, which is a similar tool that you might have used in the past.) With My Notifications, you can specify that you want to receive daily or weekly email announcements. You can specify what type of information you want to receive (such as publications, hints, and tips, product flashes (also known as alerts), downloads, and drivers). My Notifications enable you to customize and categorize the products about which you want to be informed and the delivery methods that best suit your needs.

Procedure

To subscribe to Support updates:

1. Subscribe to the Security Access Manager RSS feeds by accessing the IBM Software Support RSS feeds site and subscribe to the product feed.
2. Subscribe to My Notifications by going to the IBM Support Portal and click **My Notifications** in the **Notifications** portlet.
3. Sign in using your IBM ID and password, and click **Submit**.
4. Identify what and how you want to receive updates.
   a. Click the **Subscribe** tab.
   b. Select the appropriate software brand or type of hardware.
   c. Select one or more products by name and click **Continue**.
   d. Select your preferences for how to receive updates, whether by email, online in a designated folder, or as an RSS or Atom feed.
   e. Select the types of documentation updates that you want to receive, for example, new information about product downloads and discussion group comments.
   f. Click **Submit**.

Results

Until you modify your RSS feeds and My Notifications preferences, you receive notifications of updates that you requested. You can modify your preferences when needed (for example, if you stop using one product and begin using another product).

Related information

- IBM Software Support RSS feeds
- Subscribe to My Notifications support content updates
- My Notifications for IBM technical support
- My Notifications for IBM technical support overview

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:

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 might 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites 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
2Z4A/101
11400 Burnet Road
Austin, TX 78758 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 measurement 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. 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 IBM's application programming interfaces.

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_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

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.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

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

Index

Printed in USA