IBM Security Access Manager for Web
Version 7.0

Upgrade Guide

SC23-6503-02

IBM Security Access Manager for Web
Version 7.0

Upgrade Guide

SC23-6503-02

Note
Before using this information and the product it supports, read the information in "Notices" on page 219.

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.

© Copyright IBM Corporation 2003, 2012.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 2003, 2012

Figures

© Copyright IBM Corp. 2003, 2012

Tables

© Copyright IBM Corp. 2003, 2012

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.

This guide explains how to upgrade from a previous Tivoli Access Manager level to Security Access Manager, version 7.0.

Intended audience

This guide is for system administrators responsible for the upgrade of Security Access Manager. Readers should be familiar with the following:

- Microsoft Windows, AIX, Linux, or Solaris 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
- Authentication and authorization

If you are enabling secure communication, you also should be familiar with secure communication protocols, 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 xi.
- A link to the "IBM Terminology website" on page xi.

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

© Copyright IBM Corp. 2003, 2012

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.

Chapter 1. Introduction

When you upgrade your existing Tivoli Access Manager version to Security Access Manager, version 7.0, consider the interdependencies among the Security Access Manager components and other software components.

For example, a user who logs on to WebSEAL might interact with the WebSEAL component directly. For the authentication to complete, WebSEAL must communicate with the registry server, such as an LDAP server. Consideration of this interdependency helps to maintain service continuity during the upgrade.

This guide takes a system-level approach to the upgrade process by considering the interaction of the various components that are in a production environment. There are many different ways to deploy the product components. This guide presents specific scenarios that apply to many Security Access Manager deployments.

Review the scenarios to determine the one that best matches your deployment.

If your environment does not exactly match a scenario, create a custom upgrade plan with the procedures in this guide. A custom upgrade plan must include enough detail to complete the upgrade. Thoroughly verify the successful upgrade in a test environment before you apply the upgrade in a production environment.

The following list provides suggestions for the type of information to include in a custom upgrade plan:

- Host names and IP addresses of servers
- Components that are installed on the servers
- Networking devices, such as firewalls and load balancers
- How to add and remove WebSEAL servers to and from load balancers
- Exact commands to run for each step of each procedure

You might not need more hardware. However, in some cases, more systems might reduce the risks that are involved in the upgrade, such as in a two-system upgrade.

Upgrading to the IBM Security Web Gateway Appliance

You can migrate a WebSEAL instance from a previous level of Tivoli Access Manager to the hardware or virtual version of IBM Security Web Gateway Appliance. There are no restrictions on the version or platform of the previous level of WebSEAL.

WebSEAL instance migration is performed by exporting the configuration and junction database from the Tivoli Access Manager software installation, and then importing the files into the appliance.

See the *IBM Security Web Gateway Appliance Administration Guide* for migration information and instructions.

© Copyright IBM Corp. 2003, 2012

Preparing for an upgrade

Before you upgrade to Security Access Manager, version 7.0, determine if you meet certain prerequisites.

Procedure

1. Verify that your current version of Tivoli Access Manager is one of the following supported versions for upgrade to Security Access Manager, version 7.0:
   - Tivoli Access Manager 6.1.1
   - Tivoli Access Manager 6.1
   - Tivoli Access Manager 6.0
2. Back up your installation.

   Note: If the upgrade fails, you must restore a backup of the product from before the upgrade, and then try the upgrade again.

   Back up the following data:
   - **Tivoli Access Manager servers**

     Follow the **pdbackup** steps in each component upgrade procedure.
   - **User registry data**

     For Tivoli Directory Server, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17; otherwise, consult the documentation for your supported registry server.
   - **Databases and DB2 settings**
3. Plan your upgrade approach.

   AIX®, Linux, and Solaris operating systems support single and two-system upgrade paths:

   Single-system approach
   Upgrades and migrates data to version 7.0 on the same system that is used by the existing level.

   Two-system approach
   Installs version 7.0 on a new system and migrates existing data.

   Note: Windows systems must use a two-system approach.
4. Upgrade your operating system to the minimum supported level. For information about minimum supported levels, see the *IBM Security Access Manager for Web Release Notes*.
5. Review the upgrade considerations for each component upgrade.

Mixed level environment

You are not required to have all Security Access Manager components in your secure domain at a 7.0 level.

Mixed level environment

To use Security Access Manager, version 7.0, you must have your policy server at the 7.0 level. You can configure your 6.0, 6.1 or 6.1.1 level components to the 7.0 policy server.

However, if you use a single system for multiple components, then when you upgrade any Security Access Manager component to the 7.0 level, 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.

If you want to keep an existing Tivoli Access Manager component at the 6.0, 6.1, or 6.1.1 level, but use the Security Access Manager 7.0 policy server, see:

- "Configuring a previous level component to a 7.0 policy server on Windows"
- "Configuring a previous level component to a 7.0 policy server on AIX, Linux, or Solaris" on page 5

Configuring a previous level component to a 7.0 policy server on Windows

You can configure a 6.0, 6.1 or 6.1.1 Tivoli Access Manager component to a Security Access Manager 7.0 policy server on Windows.

Before you begin

Upgrade the 7.0 policy server. See Chapter 3, "Upgrading the policy server," on page 21.

Back up critical Tivoli Access Manager data with the **pdbackup** utility. For more information about the **pdbackup** utility, see "pdbackup" on page 205.

About this task

The following procedure is for Windows systems. For AIX, Linux, or Solaris systems, see "Configuring a previous level component to a 7.0 policy server on AIX, Linux, or Solaris" on page 5.

Complete this procedure from the system with the previous level component.

Procedure

1. Stop all Tivoli Access Manager applications and services. For example, on Windows 2008 systems:
   a. Select **Start** > **Control Panel** > **Administrative Tools**.
   b. Double-click the **Services** icon.
   c. Stop all Tivoli Access Manager services that run on the local system, including applications, such as WebSEAL.
2. Complete the steps in Table 1 on page 4 for the component that you want to configure to the Security Access Manager 7.0 policy server.

Table 1. Configure previous level component to 7.0 policy server on Windows

Component	Steps to configure a previous level component with a 7.0 policy server
Authorization Server	1. Open each of the following configuration files: • *image_path*\etc\pd.conf • *image_path*\etc\ivacld.conf 2. In each file, change the master-host entry in the [manager] stanza to the following value: master-host=*host_name* where *host_name* is the fully qualified host name of the version 7.0 policy server. For example: master-host=server1.example.ibm.com 3. Save the files.
• Runtime • Development system	1. Open the following configuration file: *image_path*\etc\pd.conf 2. Change the master-host entry in the [manager] stanza to the following value: master-host=*host_name* where *host_name* is the fully qualified host name of the version 7.0 policy server. For example: master-host=server1.example.ibm.com 3. Save the file.
Runtime for Java	1. Unconfigure the Runtime for Java. 2. Configure the Runtime for Java for the 7.0 policy server.
Policy Proxy Server	1. Open each of the following configuration files: • *image_path*\etc\pd.conf • *image_path*\etc\pdmgrproxyd.conf 2. In each file, change the master-host entry in the [manager] stanza to the following value: master-host=*host_name* where *host_name* is the fully qualified host name of the version 7.0 policy server. For example: master-host=server1.example.ibm.com 3. Save the files.

Table 1. Configure previous level component to 7.0 policy server on Windows (continued)

Component	Steps to configure a previous level component with a 7.0 policy server
WebSEAL	1. Open each of the following configuration files: • *image_path*\etc\pd.conf • *image_path*\etc\webseald-*instance*.conf 2. In each file, change the master-host entry in the [manager] stanza to the following value: master-host=*host_name* where *host_name* is the fully qualified host name of the version 7.0 policy server for the domain to which WebSEAL belongs. For example: master-host=server1.example.ibm.com 3. Save the files.
SMS CLI	1. Open each of the following configuration files: • *image_path*\etc\pd.conf • *image_path*\opt\pdsms\etc\pdsmsclicfg.conf 2. In each file, change the master-host entry in the [manager] stanza to the following value: master-host=*host_name* where *host_name* is the fully qualified host name of the version 7.0 policy server. For example: master-host=server1.example.ibm.com 3. Save the files.

3. Start all Tivoli Access Manager applications and services. For example, on Windows 2008 systems:
   a. Select **Start** > **Control Panel** > **Administrative Tools**.
   b. Double-click the **Services** icon.
   c. Start all Tivoli Access Manager services that run on the local system, including applications, such as WebSEAL.
4. Optional: Confirm that the previous level component can contact the Security Access Manager 7.0 policy server. For example, run a sample **pdadmin** command:

```
pdadmin -a sec_master -p password
pdadmin sec_master> acl list
```

Configuring a previous level component to a 7.0 policy server on AIX, Linux, or Solaris

You can configure a 6.0, 6.1 or 6.1.1 Tivoli Access Manager component to a Security Access Manager 7.0 policy server on AIX, Linux, or Solaris.

Before you begin

Upgrade the 7.0 policy server. See Chapter 3, “Upgrading the policy server,” on page 21.

Back up critical Tivoli Access Manager data with the **pdbackup** utility. For more information about the **pdbackup** utility, see “pdbackup” on page 205.

About this task

The following procedure is for AIX, Linux, or Solaris systems. For Windows systems, see “Configuring a previous level component to a 7.0 policy server on Windows” on page 3.

Complete this procedure from the system with the previous level component.

Procedure

1. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```

2. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```

3. Complete the steps in Table 2for the component that you want to configure to the Security Access Manager 7.0 policy server.

Table 2. Configure previous level component to 7.0 policy server on AIX, Linux, or Solaris

Component	Steps to configure a previous level component with a 7.0 policy server
Authorization Server	1. Open each of the following configuration files: • `/opt/PolicyDirector/etc/pd.conf` • `/opt/PolicyDirector/etc/ivacld.conf` 2. In each file, change the `master-host` entry in the `[manager]` stanza to the following value: `master-host=`*`host_name`* where *host_name* is the fully qualified host name of the version 7.0 policy server. For example: `master-host=server1.example.ibm.com` 3. Save the files.

Table 2. Configure previous level component to 7.0 policy server on AIX, Linux, or Solaris (continued)

Component	Steps to configure a previous level component with a 7.0 policy server

• Runtime
• Development system
	1. Open the following configuration file:
	`/opt/PolicyDirector/etc/pd.conf`
	2. Change the `master-host` entry in the `[manager]` stanza to the following value:
	`master-host=`*`host_name`*
	
	where *host_name* is the fully qualified host name of the version 7.0 policy server. For example:
	`master-host=server1.example.ibm.com`
	3. Save the file.

Runtime for Java	1. Unconfigure the Runtime for Java. 2. Configure the Runtime for Java for the 7.0 policy server.
Policy Proxy Server	1. Open each of the following configuration files: • `/opt/PolicyDirector/etc/pd.conf` • `/opt/PolicyDirector/etc/pdmgrproxyd.conf` 2. In each file, change the `master-host` entry in the `[manager]` stanza to the following value: `master-host=`*`host_name`* where *host_name* is the fully qualified host name of the version 7.0 policy server. For example: `master-host=server1.example.ibm.com` 3. Save the files.
WebSEAL	1. Open each of the following configuration files: • `/opt/PolicyDirector/etc/pd.conf` • `/opt/pdweb/etc/webseald-`*`instance`*`.conf` 2. In each file, change the `master-host` entry in the `[manager]` stanza to the following value: `master-host=`*`host_name`* where *host_name* is the fully qualified host name of the version 7.0 policy server for the domain to which WebSEAL belongs. For example: `master-host=server1.example.ibm.com` 3. Save the files.

Table 2. Configure previous level component to 7.0 policy server on AIX, Linux, or Solaris (continued)

Component	Steps to configure a previous level component with a 7.0 policy server
SMS CLI	1. Open each of the following configuration files: • `/opt/PolicyDirector/etc/pd.conf` • `/opt/pdsms/etc/pdsmsclicfg.conf` 2. In each file, change the `master-host` entry in the `[manager]` stanza to the following value: `master-host=`*`host_name`* where *host_name* is the fully qualified host name of the version 7.0 policy server. For example: `master-host=server1.example.ibm.com` 3. Save the files.

4. Start all Tivoli Access Manager applications and services:

   ```
   pd_start start
   ```

5. Optional: Confirm that the previous level component can contact the Security Access Manager 7.0 policy server. For example, run a sample **pdadmin** command:

   ```
   pdadmin -a sec_master -p password
   pdadmin sec_master> acl list
   ```

Scenario 1: Two system upgrade with large user base

The key considerations in this scenario involve:

- A primary system that has both the policy server and the primary LDAP server, Tivoli Directory Server.
- Large numbers of Security Access Manager user accounts, such as in the millions.

Rather than affect the active, primary policy server, use the two system upgrade procedure to install a 7.0 policy server on an LDAP server peer. Or, if you do not want to use an LDAP server peer for this purpose, you can introduce an additional server to act as the new registry server. The peer or second server in this scenario is named the `ldap_host2` system.

Security Access Manager 7.0 components require a Tivoli Directory Server 6.3 FP17 client on the same machine. However, Tivoli Directory Server 6.3 FP17 clients can coexist on the same machine with other Tivoli Directory Server clients that are version 6.0 or later.

For example, if you keep the LDAP server at version 6.2, and you have Tivoli Directory Server 6.2 clients, then if you install any Security Access Manager 7.0 component, that machine must also have a 6.3 FP17 client. In this case, you can keep the 6.2 clients and add 6.3 clients on the same machine because of the Tivoli Directory Server coexistence support.

For more information about Tivoli Directory Server 6.3 FP17 server and client coexistence, see: the *Tivoli Directory Server Installation and Configuration Guide* for version 6.3 FP17.

Scenario 1: Conditions

The following conditions apply to this scenario:

1. Service must remain available during migration.
2. The number of Security Access Manager user accounts are in the millions.
3. Must be able to fall back to a previous version in the event of failure with minimal downtime. This condition precludes restoring from tape backup.
4. If necessary, provide more hardware to support the upgrade process.

Scenario 1: Hardware configuration

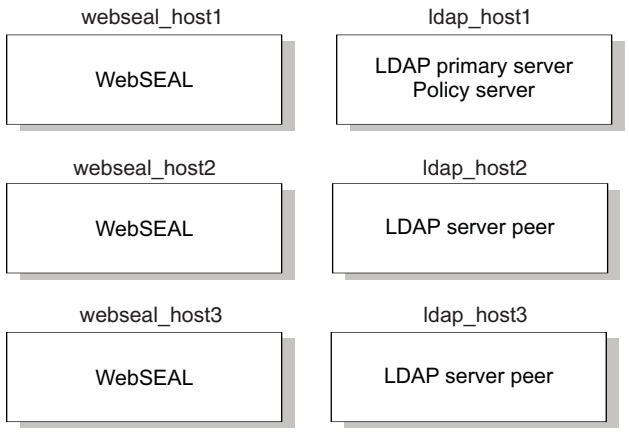

Figure 1. Scenario 1: Hardware configuration

In this scenario:

LDAP primary server
: Indicates the primary LDAP server against which the policy server is configured. This system also provides authentication services for the WebSEAL servers.

LDAP server peers
: Indicates the backup LDAP servers for the policy server. Also provides authentication services for the WebSEAL servers.

Scenario 1: High-level steps

Use the following procedure as a guideline to understand the high-level steps that are required to upgrade your environment. If your environment does not exactly match the following two-system scenario, create a custom upgrade plan with the procedures in this guide.

Procedure

1. Back up the following data:
   - Tivoli Access Manager servers

     See the **pdbackup** utility in the *IBM Security Access Manager for Web Command Reference* for information.

- User registry data

  For Tivoli Directory Server, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17; otherwise, consult the documentation for your supported registry server.

2. Upgrade Tivoli® Directory Server on `ldap_host2`.
   a. Upgrade Tivoli Directory Server. For instructions, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17. Then, return to these high-level steps and continue with step 2b.
   b. Test that Tivoli Directory Server is up and running by using the following command: `idsldapsearch -h ldap_host2 -s base –p port objectclass=*` If the last line from the output from the **ldapsearch** command (`ibm-slapdisconfigurationmode`) is set to `TRUE`, there was a problem during the migration and the server started in configuration mode. Examine the `ibmslapd.log` file for errors. If no specific error is given, try restarting Tivoli Directory Server.
   c. Verify that replication still works by creating a Security Access Manager user on the LDAP primary server (`ldap_host1`) and verify that it is replicated to this LDAP server peer (`ldap_host2`).
3. Upgrade the policy server by following the two system approach. Make `ldap_host2` the new system and `ldap_host1` the original system.

   For instructions on upgrading the policy server for your appropriate platform by following the two system approach, see Chapter 3, "Upgrading the policy server," on page 21.

   After the upgrade is complete, `ldap_host2` hosts Tivoli Directory Server 6.3 FP17 and Security Access Manager policy server, version 7.0. The other servers still have the older versions of the software.

   Note: Maintain the original policy server until the other Security Access Manager components complete upgrade. This approach provides the option of restoring the original version.

   Any policy modification that results in an update on one policy server must also be made on the other one. This means that new ACLs and other policy-related configurations must be completed on both the new and the old policy servers when the two systems are running in parallel.
4. Upgrade the WebSEAL servers (`webseal_host1`, `webseal_host2`, `webseal_host3`).

   The WebSEAL servers are still configured to use the policy server that is on `ldap_host1`. However, because there is compatibility with an earlier version between the 7.0 policy server and previous versions of WebSEAL, you can configure the three WebSEAL servers to use the new policy server.

   This approach offers a low-risk way of moving over to the new policy server. If for some reason a WebSEAL server does not function properly with the new policy server, point it back to the old one. Changing the policy server that WebSEAL uses involves changing the `master-host` entry in the WebSEAL configuration file.

   Another item to consider concerns the user activity on the system during your upgrade. If you plan to upgrade WebSEAL while users are trying to access the system, you must isolate each WebSEAL server before you upgrade it. To do so, change the port on which the WebSEAL server listens or configure your load balancer so that it does not route traffic to the WebSEAL server.

   Apply the following steps to each WebSEAL server in succession:

a. If required, isolate the WebSEAL server from use by changing the listening port or by reconfiguring the load balancer.
b. Upgrade WebSEAL. For instructions, see Chapter 5, "Upgrading WebSEAL," on page 71.
c. If you took measures to isolate the WebSEAL server from use, reverse those measures and restart WebSEAL.

Note: Do not change the WebSEAL configuration file to use the new policy server before you complete step 4b.

5. Retire the original policy server.

   After the WebSEAL servers are upgraded, you have at least one instance of each Security Access Manager component that runs the new version of the software. You can keep this configuration up and running until you feel that the new version is stable. When you are ready to make the switch, retire the original policy server (`ldap_host1`). For information about how to retire the original policy server, see the procedure for your platform in Chapter 3, "Upgrading the policy server," on page 21.

6. Upgrade Tivoli Directory Server.

   Upgrade Tivoli Directory Server on `ldap_host1` and `ldap_host3`. For instructions on upgrading, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17

Scenario 2: No peer or additional servers available

The key feature in this configuration is having little or no redundancy in the servers, where occasional failure outages are preferred over maintaining more servers.

Similar to "Scenario 1: Two system upgrade with large user base" on page 8, this scenario requires the use of existing hardware to the maximum advantage. However, unlike the large user base scenario, there is no redundancy in the servers (no peer or second server) so downtime must be scheduled with the users of the system.

This scenario involves various Security Access Manager components, but does not service as many users as in "Scenario 1: Two system upgrade with large user base" on page 8.

Scenario 2: Conditions

The following conditions apply to this scenario:

1. Service outage for upgrade can be scheduled.
2. The number of Security Access Manager servers is minimal.
3. The number of Security Access Manager user accounts is in the tens of thousands.
4. Must be able to fall back to the previous version in the event of failure.
5. Not willing to purchase more hardware to support migration.

Scenario 2: Hardware configuration

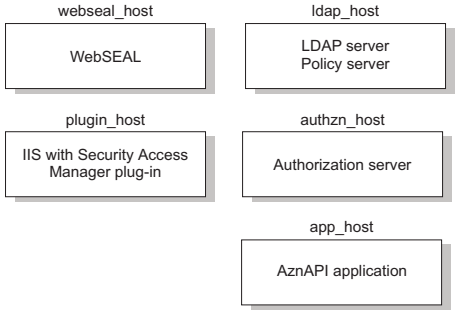

Figure 2. Scenario 2: Hardware configuration

In this scenario:

LDAP primary server
Indicates the primary LDAP server against which the policy server is configured, and there is no backup LDAP server for the policy server. This system also provides authentication services for the WebSEAL servers.

Scenario 2: High-level steps

Use the following procedure as a guideline to understand the high-level steps that are required to upgrade your environment. If your environment does not exactly match the following limited hardware scenario, create a custom upgrade plan with the procedures in this guide.

Procedure

1. Back up the following data:
   - Tivoli Access Manager servers

     See the **pdbackup** utility in the *IBM Security Access Manager for Web Command Reference* for information.
   - User registry data

     For Tivoli Directory Server, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17; otherwise, consult the documentation for your supported registry server.
2. Do one of the following actions:
   - If you scheduled downtime for the upgrade, proceed to step 3 on page 13 without installing a second authorization server.
   - If you want your AznAPI application to have minimal downtime, install a second authorization server to ensure that your AznAPI application continues to make authorization decisions during upgrade. To install the second authorization server, follow these steps:
     a. Install another instance of the authorization server on `app_host`. Use the same software version of the authorization server that is running on `authzn_host`, just running on a different system.
     b. Edit your AznAPI application configuration file on `app_host`:
        1) Comment out the replica entry for the original authorization server.
        2) Add a replica line for the new authorization server.
     c. Restart the AznAPI application on `app_host` and verify that it functions properly.

3. Unconfigure and uninstall the existing Tivoli Access Manager authorization server and runtime packages on `authzn_host`.

   If you have the command-line extension to the Session Management Server installed and configured, unconfigure and uninstall the command-line extension.
4. Install a Security Access Manager, version 7.0, policy server on `authzn_host` for the second policy server in addition to the policy server on `ldap_host`. Use the two system upgrade procedure as instructed for your specific operating system in Chapter 3, "Upgrading the policy server," on page 21. After you complete this step, you have a policy server that runs on `ldap_host` (the original server) and on `authzn_host` (new server).
5. Confirm that the policy server is running on `authzn_host`:

   ```
   pd_start status
   ```
6. Install and configure a Security Access Manager, version 7.0, authorization server on `authzn_host`. For instructions, see the *IBM Security Access Manager for Web Installation Guide*.

   When you use a Tivoli Directory Server registry, set `[ldap] auth-using-compare` to `no` in `ivacld.conf` after you install the authorization server.
7. Upgrade WebSEAL on `webseal_host`.

   For instructions, see Chapter 5, "Upgrading WebSEAL," on page 71. Because there is only one WebSEAL server, there is a time when the WebSEAL service is unavailable.
8. Confirm that the WebSEAL server is running and functioning properly.
9. Upgrade the plug-in for Web Servers on `plugin_host`. For instructions, see Chapter 13, "Upgrading a plug-in for Web servers," on page 177.
10. Upgrade the AznAPI application by completing these procedures:
    - Upgrade the Security Access Manager components such as the development system. See Chapter 9, "Upgrading the development system," on page 129.
    - Install a new version of your AznAPI application that is based on the 7.0 API.

      To deploy a new version of your application, build and test a new version of your code in your 7.0 test environment.

    Complete the build and test activities before the scheduled upgrade of the production servers. To upgrade the production server, complete the following steps on `app_host`:

    a. Stop the AznAPI application.
    b. Unconfigure and uninstall the `aznAPI` application on `app_host`.
    c. Back up your AznAPI application by moving it out of the Security Access Manager directory hierarchy and storing it elsewhere.
    d. Edit `pd.conf` (the configuration file for the Security Access Manager runtime component) and `aznapi.conf` (the configuration file for the authorization API application) to change the `master-host` entry to the value of `authzn_host`. The change directs the IBM Security Access Manager runtime and your application to use the 7.0 policy server that is running on `authzn_host`.
    e. Upgrade Security Access Manager runtime according to the instructions in Chapter 6, "Upgrading the runtime," on page 91.
    f. Copy the newly built 7.0 version of your AznAPI application to the same location where you stored the previous version.

g. Start your AznAPI application.

11. Retire the previous level policy server.

    After success with the version 7.0 Security Access Manager servers in production, you can retire the previous level policy server. For information about retiring the original policy server, see information for your platform in Chapter 3, "Upgrading the policy server," on page 21.

12. Upgrade Tivoli Directory Server.

    For instructions on upgrading, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17.

Scenario 3: Using a registry other than Tivoli Directory Server

This scenario describes the use of Security Access Manager with a registry server other than Tivoli Directory Server. Microsoft Active Directory is chosen for this example.

Scenario 3: Conditions

The following conditions apply to this scenario:

1. The system is on AIX, Linux, or Solaris.
2. Service outage for migration can be scheduled for short interval.
3. The number of Security Access Manager servers is minimal.
4. The number of Security Access Manager user accounts is in the tens of thousands.
5. Must be able to fall back to the previous version in the event of failure.
6. Not willing to purchase more hardware to support migration.
7. Uses a non-IBM user registry server.

Scenario 3: Hardware configuration

Similar to "Scenario 1: Two system upgrade with large user base" on page 8, this scenario requires using the existing hardware to maximum advantage. However, unlike the large user base scenario, there is redundancy only in the WebSEAL servers, so downtime must be scheduled with the users of the system during the policy server upgrade. Scheduled downtime primarily affects policy management, not WebSEAL authentication.

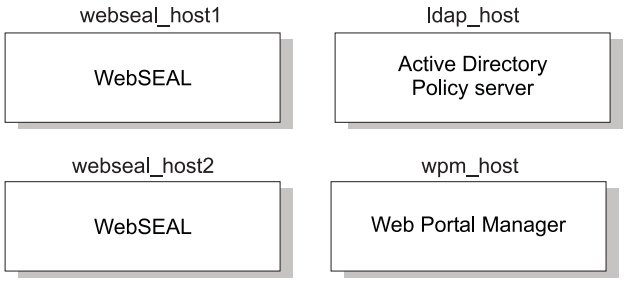

Figure 3. Scenario 3: Hardware configuration

Scenario 3: High-level steps

Use the following procedure as a guideline to understand the high-level steps that are required to upgrade your environment. If your environment does not exactly match the following scenario, create a custom upgrade plan with the procedures in this guide.

Procedure

1. Back up the following data:
   - Tivoli Access Manager servers

     See the **pdbackup** utility in the *IBM Security Access Manager for Web Command Reference* for information.
   - User registry data

     For Tivoli Directory Server, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17; otherwise, consult the documentation for your supported registry server.
2. Upgrade the Web Portal Manager system.

   Because Web Portal Manager does not have its own database to manage (it retrieves its data from Security Access Manager), uninstall the old version and install the latest version. For instructions, see the *IBM Security Access Manager for Web Installation Guide*.
3. Upgrade the policy server by following the single system approach only.

   Note: The two-system approach is supported for LDAP-based and Active Directory registries only.

   You must schedule downtime to upgrade the policy server because there is a time during the upgrade when the policy server is not available.

   An unavailable policy server affects the management of policy information, such as access control lists. The WebSEAL servers continue to provide service.

   For instructions on upgrading the policy server for your appropriate platform by following a single system, see Chapter 3, "Upgrading the policy server," on page 21.
4. Verify that the WebSEAL servers can communicate with the policy server.
5. Upgrade WebSEAL on the servers. To do so, follow these steps:
   a. If you plan to upgrade WebSEAL on a server while users are trying to access the system, you must isolate each WebSEAL server before you upgrade it. To do so, change the port on which the WebSEAL server listens or configure your load balancer so that it does not route traffic to the WebSEAL server.
   b. Upgrade WebSEAL. For instructions, see Chapter 5, "Upgrading WebSEAL," on page 71.
   c. If you took measures to isolate the WebSEAL server, you can reverse those measures and restart WebSEAL.

Chapter 2. Upgrading IBM Tivoli Directory Server

If you have a previous version of IBM Tivoli Directory Server, you can upgrade to IBM Tivoli Directory Server 6.3 FP17 and maintain your existing schema definitions and directory server configuration.

Upgrading from a previous version of IBM Tivoli Directory Server preserves the following established environment settings:

- Data
- Changes that you made to the existing schema definitions
- Directory server configuration

Use the preparation information in this chapter when you are upgrading an existing directory server from a previous version of Tivoli Directory Server on the same physical computer.

This chapter describes:

- "High-level steps for upgrading Tivoli Directory Server"
- "About the client" on page 18
- "Location of migration utilities" on page 18
- "Before you upgrade Tivoli Directory Server" on page 18

After you review and completing the prerequisite tasks, follow the Tivoli Directory Server upgrade procedures:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.IBMDS.doc%2Finstall39.htm&path=8_3_6

If your earlier version of Tivoli Directory Server is on an operating system that is no longer supported for Tivoli Directory Server 6.3 FP17, and you do not want to upgrade the operating system on that computer, follow the Tivoli Directory Server remote migration procedures:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.IBMDS.doc%2Finstall44.htm&path=8_3_6_4

High-level steps for upgrading Tivoli Directory Server

A list of high-level steps provides an outline of required and optional steps during upgrade of Tivoli Directory Server.

About this task

The following list contains the order in which you upgrade software and migrate data. Before you start the upgrade, see "Before you upgrade Tivoli Directory Server" on page 18.

Procedure

1. Prepare the database for migration by backing up and stopping the database.
2. Back up the configuration and schema files for a previous version of Tivoli Directory Server.

© Copyright IBM Corp. 2003, 2012

3. Upgrade the operating system, if necessary.
4. Upgrade DB2 if necessary.
5. If the version of Tivoli Directory Server you are upgrading is **before** 6.2, uninstall Tivoli Directory Server.
6. Install Tivoli Directory Server 6.3 FP17.
7. Migrate schema and configuration files.
8. Migrate your Tivoli Directory Server instance from a previous version of Tivoli Directory Server to a 6.3 FP17 directory server instance.
9. Migrate database instances and the databases.

About the client

If you have only a client that is installed, migration is not necessary.

Clients from release 6.0, 6.1 and 6.2 can coexist with Security Access Manager 7.0 clients and servers.

Location of migration utilities

The upgrade process uses the **migbkup** and **idswmigr** utilities.

These utilities are found on the *IBM Security Access Manager for Web Version 7.0* DVD.

The migration utilities are located in the following directory on the DVD:
platform/tdsV6.3/tools

where *platform* is the operating system.

Before you upgrade Tivoli Directory Server

Before you upgrade Tivoli Directory Server to version 6.3 FP17, consider these steps.

Procedure

1. Upgrade your operating system to the minimum supported level. For information about minimum supported levels, see *IBM Security Access Manager for Web Release Notes*.
2. Be sure that the server you plan to migrate to IBM Tivoli Directory Server 6.3 FP17 can successfully start. (If the server is not a proxy server, be sure that the database is configured.) If the server cannot start successfully, whether it is a proxy server or a full directory server, the upgrade is not supported.

   Note: You must not remove the directory server instance that you want to upgrade. For a full directory server instance, you must not unconfigure the database. If you do either of these actions, upgrade is not supported.
3. Back up the databases and DB2 settings. See the *IBM Tivoli Directory Server Administration Guide* for your IBM Tivoli Directory Server release for information about backing up databases by using DB2 commands, the **dbback** or **idsdbback** command, or the Configuration Tool. Take an offline database backup for each local database on the server. (Do this step now or after step 4 on page 19.)

4. Back up the configuration files and schema files with the **migbkup** utility. See "Location of migration utilities" on page 18 for the location of this utility.

   Type the following at a command prompt:

   - For Windows systems:

     `migbkup.bat instance_home backup_directory`

   - For AIX, Linux, and Solaris systems:

     `migbkup instance_home backup_directory`

   This utility backs up the server configuration file and all standard schema files that are supplied with IBM Tivoli Directory Server from the *install_location*\etc directory to a temporary directory, which is specified by *backup_directory*.

   instance_home is the home directory of the instance.

   backup_directory is the temporary directory where the backed up files are copied.

   The following is a partial list of files of which the command creates backup copies:

   - ibmslapd.conf
   - V3.ibm.at
   - V3.ibm.oc
   - V3.system.at
   - V3.system.oc
   - V3.user.at
   - V3.user.oc
   - V3.modifiedschema

   In addition, for backups on version 6.0, the command backs up the following files:

   - V3.config.at
   - V3.config.oc
   - V3.ldapsyntaxes
   - V3.matchingrules
   - ibmslapdcfg.ksf
   - ibmslapddir.ksf
   - ibmdiradmService.cmd
   - ibmslapdService.cmd

   The command also creates the db2info file.

   If you have more schema files that you used in your previous release, copy them manually to the *backup_directory*. When you migrate the configuration and schema files during instance creation, the files copy to the new directory server instance location for the directory server instance.

5. Be sure that the operating system on which you plan to install Tivoli Directory Server is supported. See *IBM Tivoli Directory Server System Requirements* for information about supported levels. If the operating system is not supported, install a supported version.
6. If your current version of DB2 is a version that is not supported for IBM Tivoli Directory Server, upgrade your DB2 version or fix pack level to a supported level. See *IBM Tivoli Directory Server System Requirements* for information about supported DB2 versions. See

http://www-1.ibm.com/support/docview.wss?uid=swg21200005 for information about upgrading your DB2 version. You might also be required to upgrade the bit-width of the database with DB2 commands.

7. After you review and completing the prerequisite tasks, follow the Tivoli Directory Server upgrade procedures: http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.IBMDS.doc%2Finstall39.htm&path=8_3_6.

Chapter 3. Upgrading the policy server

You can upgrade your policy server to a Security Access Manager, version 7.0, policy server either on the same policy server system or by using two systems: your current policy server system and a second, clean system for the new 7.0 policy server.

The single-system approach is supported for AIX, Linux, and Solaris systems.

The two-system approach is supported for LDAP-based and Active Directory user registries. With this approach, you can maintain your current policy server as it was set up, while you upgrade and test a second, version 7.0, policy server system.

The two-system approach requires more hardware. If you encounter a problem when you upgrade with two systems, you can take the version 7.0 server offline.

AIX, Solaris, and Linux: Upgrade considerations

Before you upgrade the policy server to version 7.0 on AIX, Linux, and Solaris operating systems, review the considerations that are described in this section.

- Before you upgrade to Security Access Manager, version 7.0, back up the following data:
  - All Tivoli Access Manager servers.

    See the **pdbackup** utility in the *IBM Security Access Manager for Web Command Reference* for information.
  - User registry data

    For Tivoli Directory Server, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17; otherwise, consult the documentation for your supported registry server.
- Upgrade your operating system to the minimum supported level. For information about minimum supported levels, see the *IBM Security Access Manager for Web Release Notes*.
- If your earlier version of Tivoli Access Manager runs on an operating system that is not supported by Security Access Manager 7.0, and you do not want to upgrade the operating system on that computer, follow the upgrade instructions for a two system upgrade to migrate the policy server and its data onto a supported platform.
- In Tivoli Directory Server 6.3 FP17, clients can coexist on the same server with a client that is version 6.0, 6.1 or 6.2. The Tivoli Directory Server 6.3 FP17 server requires that the version 6.3 client and the Java client are also installed. In addition, the server can coexist on the same server with another client that is version 6.0, 6.1, or 6.2, or with a version of the 6.3 server.
- You are not required to upgrade all Security Access Manager components in your secure domain to a 7.0 level. However, if you upgrade any Security Access Manager component on a system, you must upgrade all components on that system to the 7.0 level. You must also install Tivoli Directory Server client 6.3 FP17 on that system.
- If Tivoli Directory Server is your registry server and is on *a different workstation* from any Security Access Manager component, you can upgrade the registry server at any time, either before or after the upgrade of the Security Access Manager, version 7.0, component.

© Copyright IBM Corp. 2003, 2012

However, when the server package of Tivoli Directory Server is installed *on the same workstation* as a Security Access Manager, version 7.0, component and if you choose to install the server package of Tivoli Directory Server 6.3 FP17, install the Tivoli Directory Server 6.3 FP17 client and server packages at the same time as you install the Security Access Manager 7.0 component on that workstation.

- The upgrade process does not support changing your configuration, such as your registry type. For example, you cannot upgrade from an LDAP registry to an Active Directory registry.
- The default temporary directory is `/tmp`.
- The default installation paths for AIX, Linux, and Solaris operating systems are in the following directory:
  - `/opt/PolicyDirector`
  - `/var/PolicyDirector`
- If you are upgrading and use a language other than English, remember to upgrade your language package. See the *IBM Security Access Manager for Web Installation Guide* to install the language package. However, when you upgrade the IBM Tivoli Directory Server language packages, you must use the upgrade (**-U**) option for AIX, Linux, and Solaris operating systems.

For the Windows operating system, see "Windows: Upgrade considerations" on page 52.

AIX: Upgrading the policy server

Upgrade the policy server system on AIX by either using a single system or a two-system approach. If you complete an upgrade by following the two system approach, retire the original policy server after you successfully migrate its data and the Tivoli Directory Server client and server to the policy server system.

AIX: Upgrading the policy server on a single system

Security Access Manager supports an upgrade of a policy server on a single AIX system.

Before you begin

Before you upgrade the policy server to version 7.0, back up all data, and review "AIX, Solaris, and Linux: Upgrade considerations" on page 21.

About this task

To upgrade the policy server system on AIX, complete the following instructions.

Note: If you encounter a problem when you migrate the policy server to version 7.0 using this single-system approach, you can restore the system to its previous level. For instructions, see "AIX: Restoring the policy server" on page 183.

Procedure

1. Log in as `root`.
2. Install all of the operating system patches that are required by Security Access Manager, version 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.

Note: The AIX operating system requires at least version 10.1 of the `xlC` file set. Check your current version by using the **lslpp** command and upgrade, if necessary.

3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage®.
4. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```

5. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```

6. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   /opt/PolicyDirector/etc/pdbackup.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

   For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

7. Install the Global Security Kit (GSKit):

   ```
   installp -acgYXd image_path/usr/sys/inst.images GSKit8.gskcrypt64.ppc.rte
   installp -acgYXd image_path/usr/sys/inst.images GSKit8.gskssl64.ppc.rte
   ```

   where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located.

8. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/usr/sys/inst.images/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
9. Install the client packages of Tivoli Directory Server:

   ```
   installp -acgYXd image_path/usr/sys/inst.images packages
   ```

   where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage, and where *packages* are the names of the Tivoli Directory Server client packages:

License package	`idsldap.license63`
Client base package	`idsldap.cltbase63`
Client package (64-bit) (no SSL)	`idsldap.clt64bit63`
Client package (64-bit) (SSL)	`idsldap.clt_max_crypto64bit63`
Java client package	`idsldap.cltjava63`

Note: All client packages require the base client package.

10. Ensure that your registry server is running.
11. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:

       ```
       isamLicense
       ```

       Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

       -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

       -? Help: Displays the syntax of the script file.
    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
12. Upgrade the Security Access Manager license:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.lic
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located, and `PD.lic` is the Security Access Manager license package.
13. Upgrade IBM Security Utilities:

    ```
    installp -acgYXd image_path/usr/sys/inst.images TivSec.Utl
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located, and `TivSec.Utl` is the IBM Security Utilities package.
14. Upgrade Security Access Manager runtime:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.RTE
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located, and `PD.RTE` is the Security Access Manager runtime package.
15. Upgrade the Security Access Manager policy server:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.Mgr
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located, and `PD.Mgr` is the Security Access Manager policy server package.
16. Security Access Manager schema definitions are added automatically during the installation of the server package of Tivoli Directory Server 6.3 FP17. You must update the schema if:
    - You are using a supported LDAP server other than IBM Tivoli Directory Server as your registry server.

- You want to continue using your previous version of IBM Tivoli Directory Server 6.2, and you do not want to upgrade the server to IBM Tivoli Directory Server version 6.3 FP17.

Update the schema with the **ivrgy_tool** as follows:

```
ivrgy_tool -d -h ldap_host -p port -D ldap_admin -w pwd schema
```

For more information about the **ivrgy_tool** utility, see the reference information for "ivrgy_tool" on page 201.

17. Start the policy server daemon (pdmgrd):

```
pd_start start
```

18. Confirm that the policy server is running:

```
pd_start status
```

19. Make sure that you can contact the policy server. For example, log in to the pdadmin interface and run a command:

```
pdadmin -a sec_master -p password
pdadmin sec_master> acl list
```

Results

The upgrade of the policy server on AIX is now complete.

AIX: Upgrading the policy server using two systems

Security Access Manager supports an upgrade of a policy server using a two-system approach for AIX systems.

Before you begin

Before you upgrade the policy server to version 7.0, back up all data, and review "AIX, Solaris, and Linux: Upgrade considerations" on page 21.

About this task

Follow these steps to set up a version 7.0 policy server on a second system while you maintain your original policy server system to continue functioning with minimal downtime.

Note: This two-system approach is supported for LDAP-based registries only.

Procedure

1. Log in as root.
2. Insert the *IBM Security Access Manager for Web for AIX* DVD and mount it on the original policy server.
3. Stop all Tivoli Access Manager applications and services:

```
pd_start stop
```

4. Confirm that all Tivoli Access Manager services and applications are stopped:

```
pd_start status
```

If any Tivoli Access Manager service or application is still running, issue the **kill** command:

```
kill –9 daemon_process_id
```

5. Back up your user registry data.

For Tivoli Directory Server, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17; otherwise, consult the documentation for your supported registry server.

6. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   image_path/usr/sys/inst.images/migrate/migxxto700.lst
   ```

   where *image_path*/usr/sys/inst.images is the directory where the installation images are located and where *xx* is the version of software that you are migrating from. The name of the backup list file would be as follows:

   For 6.1.1

   ```
   mig611to700.lst
   ```

   For 6.1

   ```
   mig61to700.lst
   ```

   For 6.0

   ```
   mig60to700.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the migxxto700.lst_*date.time*.tar default file name.

   For more information about the **pdbackup** utility, see "pdbackup" on page 205.

7. Restart the policy server daemon (pdmgrd) on the original policy server:

   ```
   pd_start start
   ```

8. Copy the archive that is produced by the **pdbackup** utility from the original policy server to the version 7.0 policy server.

   Note: The new version 7.0 policy server must be a clean system. Do not reuse an existing policy server system.

9. On the new system, install all of the operating system patches that are required by Security Access Manager, version 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.

   Note: The AIX operating system requires at least version 10.1 of the xlC file set. Check your current version by using the **lslpp** command and upgrade, if necessary.

10. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

11. Install the Global Security Kit (GSKit) on the new system:

    ```
    installp -acgYXd image_path/usr/sys/inst.images GSKit8.gskcrypt64.ppc.rte
    installp -acgYXd image_path/usr/sys/inst.images GSKit8.gskssl64.ppc.rte
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located.

12. Install the Tivoli Directory Server license files on the new system by running the `idsLicense` script in the *image_path*`/usr/sys/inst.images/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
13. Install the Tivoli Directory Server client packages on the new system:

    ```
    installp -acgYXd image_path/usr/sys/inst.images packages
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are installed and where *packages* are the names of the Tivoli Directory Server client packages:

License package	`idsldap.license63`
Client base package	`idsldap.cltbase63`
Client package (64-bit) (no SSL)	`idsldap.clt64bit63`
Client package (64-bit) (SSL)	`idsldap.clt_max_crypto64bit63`
Java client package	`idsldap.cltjava63`

14. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory.
    b. Run the `isamLicense` script:

       ```
       isamLicense
       ```

       Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

       -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

       -? Help: Displays the syntax of the script file.
    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
15. Install the Security Access Manager license on the new system:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.lic
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located and `PD.lic` is the Security Access Manager license package.
16. Install IBM Security Utilities on the new system:

    ```
    installp -acgYXd image_path/usr/sys/inst.images TivSecUtl
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located and `TivSecUtl` is the IBM Security Utilities package.
17. Install the Security Access Manager runtime on the new system:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.RTE
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located and `PD.RTE` is the Security Access Manager runtime package.
18. Install the Security Access Manager policy server on the new system:

```
installp -acgYXd image_path/usr/sys/inst.images PD.Mgr
```

where *image_path*/usr/sys/inst.images is the directory where the installation images are located and PD.Mgr is the Security Access Manager policy server package.

19. Use the **pdbackup** utility on the new system to extract data to the version 7.0 policy server:

```
/opt/PolicyDirector/bin/pdbackup -action extract -path restore_directory
-file archive_name
```

where:

–path *restore_directory*
Specifies a temporary directory on the version 7.0 policy server system in which you want to extract your archive data.

–file *archive_name*
Specifies the fully qualified path to the archive that came from the original policy server.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

CAUTION:

If there is a configuration problem, do not unconfigure this system. If you unconfigure the system, critical data that is needed by the original policy server will be destroyed. Follow instructions in "AIX: Retiring the original policy server" on page 29 with the new server.

The new system is a clone of the original policy server system. This means that the placement of critical files, such as certificate files, must be identical to the original system. For example, if a certificate file is in the /certs directory on the original policy server, it must be in the /certs directory on the new system.

20. Ensure that the LDAP server used by the original policy server is running.
21. Security Access Manager schema definitions are added automatically during the installation of the server package of Tivoli Directory Server 6.3 FP17. Update the schema if you are using a supported LDAP server other than IBM Tivoli Directory Server as your registry server.

    Update the schema with the **ivrgy_tool** as follows:

    ```
    ivrgy_tool -d -h ldap_host -p port -D ldap_admin -w pwd schema
    ```

    For more information about the **ivrgy_tool** utility, see the reference information for "ivrgy_tool" on page 201.
22. Use the **pdconfig** utility to configure the Security Access Manager runtime on the version 7.0 policy server. When prompted for an LDAP server, specify the name of the LDAP server that is used by the original policy server.
23. Use the **pdconfig** utility to configure the new policy server.
    a. When prompted, if you want to configure the policy for migration purposes, select **yes**.
    b. When prompted, if you want to use this policy server for standby, select **no**.
    c. Enter the *restore_directory* parameter that is specified by the –path option in step 20 on page 35.
24. Confirm that the new policy server is running:

    ```
    pd_start status
    ```

25. Your system is ready. Run **pdadmin** and query both the ACL database and the registry to verify their status. For example:

```
pdadmin –a sec_master -p password
pdadmin sec_master> acl list
pdadmin sec_master> user list s* 10
```

26. If you made updates or changes to your database during the migration process, complete the following steps:
    a. Stop the new policy server daemon (pdmgrd):

    ```
    pd_start stop
    ```

    b. Copy the database files from the original policy server to the version 7.0 policy server. The default location of the files to copy is as follows:

    ```
    /var/PolicyDirector/db
    ```

    c. Start the new policy server daemon (pdmgrd):

    ```
    pd_start start
    ```

Results

The upgrade of the policy server for AIX is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Upgrade other Tivoli Access Manager systems to version 7.0 in the order that is specified in Chapter 1, "Introduction," on page 1).

Ensure that the host name of the new policy server is specified in the configuration files for each Security Access Manager component, including the pd.conf file in the install_path/etc directory, and any AZN application configuration files. To do this, on each system on which you want to use the new policy server, ensure that the master-host value in the [manager] stanza of the configuration file contains the server host name of the new policy server. See the *IBM Security Access Manager for Web Administration Guide* for more information about the master-host key value.

After you update all your Security Access Manager systems, complete the procedure in "AIX: Retiring the original policy server" to retire your original policy server.

AIX: Retiring the original policy server

If you upgraded the policy server by following the two-system approach, retire the original policy server after its data and the Tivoli Directory Server client and server are successfully migrated to the 7.0 policy server system.

About this task

CAUTION:

Do not unconfigure the original policy server or the new policy server at any time during the upgrade process. Unconfiguration of the original policy server or the new policy server will destroy critical data that is needed by the policy server. The destruction of critical data results in a nonworking Security Access Manager environment.

Procedure

1. Stop the original policy server.
2. From the original policy server, enter:

```
/opt/PolicyDirector/sbin/pdmgr_ucf
```

3. Uninstall your previous version of Tivoli Access Manager as described in the documentation for that version of Tivoli Access Manager.

Linux on x86-64: Upgrading the policy server

Upgrade the policy server system for Linux on x86-64 using a single system or two systems. If you complete an upgrade by following the two system approach, retire the original policy server after you successfully migrate its data and the Tivoli Directory Server client and server to the policy server system.

Linux on x86-64: Upgrading the policy server using a single system

Use the following procedure to upgrade your policy server to the Security Access Manager, version 7.0 policy server on a single system.

Before you begin

Before you upgrade the policy server to version 7.0, back up all data, and review "AIX, Solaris, and Linux: Upgrade considerations" on page 21.

About this task

Note: If you encounter a problem when you migrate the policy server to version 7.0 using this single-system approach, you can restore the system to its previous level. For instructions, see "Linux on x86-64: Restoring the policy server" on page 184.

Procedure

1. Log in as `root`.
2. Install all of the operating system patches that are required by Security Access Manager, version 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
4. Change to the following directory:

   ```
   cd image_path/linux_x86/
   ```

   where *image_path* is the directory where the installation images are located.
5. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```
6. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
7. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

–list *fullpath_to_backup_listfile*
Specifies the fully qualified path to the backup list file. For example:
`/opt/PolicyDirector/etc/pdbackup.lst`

–path *path*
Specifies the path where you want the backed up files to be stored.

For example:
`/var/PolicyDirector/pdbackup`

–file *filename*
Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

8. Install the IBM Global Security Kit (GSKit):
```
rpm -i gskcrypt64-8.0.14.26.linux.x86_64.rpm
rpm -i gsksslx64-8.0.14.26.linux.x86_64.rpm
```
9. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_x86/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
10. Install the Tivoli Directory Server client packages:
```
rpm -i packages
```
where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.x86_64.rpm`
Base client package	`idsldap-cltbase63-6.3.0-17.x86_64.rpm`
64-bit client package	`idsldap-clt64bit63-6.3.0-17.x86_64.rpm`
Java client package	`idsldap-cltjava63-6.3.0-17.x86_64.rpm`

11. Ensure that your registry server is running.
12. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:
    ```
    isamLicense
    ```
    Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

    -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

    -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

    -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

    -? Help: Displays the syntax of the script file.

    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

d. Accept the license by pressing **1**.

13. Upgrade the Security Access Manager license:
    ```
    rpm -U PDlic-PD-7.0.0-0.x86_64.rpm
    ```
14. Upgrade IBM Security Utilities:
    ```
    rpm -U TivSecUtl-TivSec-7.0.0-0.x86_64.rpm
    ```
15. Upgrade the Security Access Manager runtime:
    ```
    rpm -U PDRTE-PD-7.0.0-0.x86_64.rpm
    ```
16. Upgrade the Security Access Manager policy server:
    ```
    rpm -U PDMgr-PD-7.0.0-0.x86_64.rpm
    ```
17. If your Tivoli Directory Server version is 6.0 or later, you do not have to do this step.

    Security Access Manager schema definitions are added automatically during the installation of the server package of Tivoli Directory Server 6.3 FP17. Update the schema if you are using a supported LDAP server other than IBM Tivoli Directory Server as your registry server.

    Update the schema with the **ivrgy_tool** as follows:

    ```
    ivrgy_tool -d -h ldap_host -p port -D ldap_admin -w pwd schema
    ```

    For more information about the **ivrgy_tool** utility, see the reference information for "ivrgy_tool" on page 201.
18. Start the policy server daemon (`pdmgrd`):
    ```
    pd_start start
    ```
19. Confirm that the policy server is running:
    ```
    pd_start status
    ```
20. Make sure that you can contact the policy server. For example, log in to the **pdadmin** interface and run a command:
    ```
    pdadmin -a sec_master -p password
    pdadmin sec_master> acl list
    ```

Results

The upgrade of the policy server for Linux on x86-64 is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Note: If necessary, edit the `ldap.conf` files for the policy server and WebSEAL to add the replica entry for an alternative LDAP.

Linux on x86-64: Upgrading the policy server using two systems

Use the following procedure to upgrade your policy server to the Security Access Manager, version 7.0, policy server using two-systems.

Before you begin

Before you upgrade the policy server to version 7.0, back up all data, and review "AIX, Solaris, and Linux: Upgrade considerations" on page 21.

About this task

Follow these steps to set up a version 7.0 policy server on a second system while you allow your original policy server to continue functioning with minimal downtime.

Note: This two-system approach is supported for LDAP-based registries only.

Procedure

1. Log in as `root`.
2. On the original system, access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
3. Stop all Tivoli Access Manager applications and services on the original system:

   ```
   pd_start stop
   ```
4. Confirm that all Tivoli Access Manager services and applications are stopped on the original system:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **`kill`** command:

   ```
   kill –9 daemon_process_id
   ```
5. Back up your user registry data.

   For Tivoli Directory Server, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17; otherwise, consult the documentation for your supported registry server.
6. Use the **`pdbackup`** utility to back up critical Tivoli Access Manager information about the original system:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   image_path/linux_x86/migrate/migxxto700.lst
   ```

   where *image_path* is where the installation images are located and *xx* is the version of software from which you are migrating. The name of the backup list file would be as follows:

   For 6.1.1

   ```
   mig611to700.lst
   ```

   For 6.1

   ```
   mig61to700.lst
   ```

   For 6.0

   ```
   mig60to700.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the `migxxto700.lst_date.time.tar` default file name.

7. Restart the policy server daemon (`pdmgrd`) on the original policy server:
   ```
   pd_start start
   ```
8. Copy the archive that is produced by the **pdbackup** utility from the original policy server to the new 7.0 policy server.

   Note: The new 7.0 policy server must be a clean system. Do not reuse an existing policy server system.
9. On the new system, install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
10. On the new system, access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
11. Change to the following directory:
    ```
    cd image_path/linux_x86/
    ```

    where *image_path* is where the installation images are located.
12. Install the Global Security Kit (GSKit) on the new system:
    ```
    rpm -i gskcrypt64-8.0.14.26.linux.x86_64.rpm
    rpm -i gskssl64-8.0.14.26.linux.x86_64.rpm
    ```
13. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_x86/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
14. Install the Tivoli Directory Server client packages on the new system:
    ```
    rpm -i packages
    ```
    where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.x86_64.rpm`
Base client package	`idsldap-cltbase63-6.3.0-17.x86_64.rpm`
64-bit client package	`idsldap-clt64bit63-6.3.0-17.x86_64.rpm`
Java client package	`idsldap-cltjava63-6.3.0-17.x86_64.rpm`

15. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:
       ```
       isamLicense
       ```

       Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

       -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

       -? Help: Displays the syntax of the script file.

c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

d. Accept the license by pressing **1**.

16. Install the Security Access Manager license on the new system:

```
rpm -i PDlic-PD-7.0.0-0.x86_64.rpm
```

17. Install IBM Security Utilities on the new system:

```
rpm -i TivSecUtl-TivSec-7.0.0-0.x86_64.rpm
```

18. Install the Security Access Manager runtime on the new system:

```
rpm -i PDRTE-PD-7.0.0-0.x86_64.rpm
```

19. Install the Security Access Manager policy server on the new system:

```
rpm -i PDMgr-PD-7.0.0-0.x86_64.rpm
```

20. Use the **pdbackup** utility to extract data to the new 7.0 policy server:

```
/opt/PolicyDirector/bin/pdbackup -action extract -path restore_directory
-file archive_name
```

where:

–path *restore_directory*
Specifies a temporary directory on the new 7.0 policy server in which you want to extract your archive data.

–file *archive_name*
Specifies the fully qualified path to the archive that came from the original policy server.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

CAUTION:

If there is a configuration problem, do not unconfigure the policy server. Unconfiguring the policy server destroys critical data that is needed by the original policy server. Follow instructions in "Linux on x86-64: Retiring the original policy server" on page 36 with the new server.

The new system is a clone of the original policy server system. This means that the placement of critical files, such as certificate files, must be identical to the original system. For example, if a certificate file is in the /certs directory on the original policy server, it must be in the /certs directory on the new system.

21. Ensure that the LDAP server used by the original policy server is running.

22. Security Access Manager schema definitions are added automatically during the installation of the server package of Tivoli Directory Server 6.3 FP17. Update the schema if you are using a supported LDAP server other than IBM Tivoli Directory Server as your registry server.

Update the schema with the **ivrgy_tool** as follows:

```
ivrgy_tool -d -h ldap_host -p port -D ldap_admin -w pwd schema
```

For more information about the **ivrgy_tool** utility, see the reference information for "ivrgy_tool" on page 201.

23. Use the **pdconfig** utility to configure the Security Access Manager runtime on the new 7.0 policy server. When prompted for an LDAP server, specify the name of the LDAP server that is used by the original policy server.

24. Use the **pdconfig** utility to configure the new 7.0 policy server.

a. At the prompt, **Would you like to configure a second policy server to this LDAP server (y/n) [No]?**, specify **yes**.

b. When prompted, if you want to use this policy server for standby, select **no**.
c. Enter the *restore_directory* specified by the –path option in step 20 on page 35.

25. Confirm that the policy server is running:
```
pd_start status
```
26. Your system is ready. Run **pdadmin** and query both the ACL database and the registry to verify their status. For example:
```
pdadmin –a sec_master -p password
pdadmin sec_master> acl list
pdadmin sec_master> user list s* 10
```
27. If you made updates or changes to your database during the migration process, complete the following steps:
a. Stop the new policy server daemon (**pdmgrd**):
```
pd_start stop
```
b. Copy the database files from the original policy server to the version 7.0 policy server. The default location of the files to copy is as follows:
```
/var/PolicyDirector/db
```
c. Start the new policy server daemon (**pdmgrd**):
```
pd_start start
```

Results

The upgrade of the policy server for Linux on x86-64 is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Upgrade other Security Access Manager systems to version 7.0 in the order that is specified in Chapter 1, “Introduction,” on page 1).

Specify the host name of the new policy server in the configuration files for each Security Access Manager component, including the `pd.conf` file in the `install_path/etc` directory, and any AZN application configuration files.

To do this, on each system on which you want to use the new policy server, update the `master-host` value in the `[manager]` stanza of the configuration file to contain the server host name of the new policy server. See the *IBM Security Access Manager for Web Administration Guide* for more information about the master-host key value.

After you update all of your Security Access Manager systems, complete the procedure in “Linux on x86-64: Retiring the original policy server” to retire your original policy server.

Linux on x86-64: Retiring the original policy server

Use the following procedure to retire your previous level policy server on Linux x86-64.

About this task

If you upgraded the policy server using the two system approach, retire the original policy server after its data and the Tivoli Directory Server client and server are successfully migrated to the version 7.0 policy server system.

CAUTION:

Do not unconfigure either the original policy server or the new policy server at any time during the upgrade process. Unconfiguring the original policy server or new policy server during upgrade destroys critical data that is needed by the policy server. The destruction of critical data results in a nonworking Security Access Manager environment.

Procedure

1. Stop the policy server.
2. From the original policy server, enter:
   ```
   /opt/PolicyDirector/sbin/pdmgr_ucf
   ```
3. Uninstall your previous version of Tivoli Access Manager.
   For uninstallation procedures, see the documentation for that version of Tivoli Access Manager.

Linux on System z: Upgrading the policy server

You can upgrade the policy server system for Linux on System z® either by using a single system or two systems. If you complete an upgrade using the two system approach, retire the original policy server after successfully migrating its data and the Tivoli Directory Server client and server to the policy server system.

Linux on System z: Upgrading the policy server using a single system

Use the following procedure to upgrade your policy server to the Security Access Manager, version 7.0, policy server on a single Linux on System z server.

About this task

To upgrade the policy server for Linux on System z, complete the following instructions.

Note: If you encounter a problem when you migrate the policy server to version 7.0 using this single-system approach, you can restore the system to its previous level. For instructions, see "Linux on System z: Restoring the policy server" on page 185.

Procedure

1. Before you upgrade the policy server to 7.0, review "AIX, Solaris, and Linux: Upgrade considerations" on page 21.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Obtain access to the *IBM Security Access Manager for Web for Linux on System z* product images on the System z system. The `.rpm` files are in the `/`*`image_path`*`/linux_s390` directory.
5. Stop all Tivoli Access Manager applications and services:
   ```
   pd_start stop
   ```
6. Confirm that all Tivoli Access Manager services and applications are stopped:
   ```
   pd_start status
   ```

If any Tivoli Access Manager service or application is still running, issue the **kill** command:

```
kill –9 daemon_process_id
```

7. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   /opt/PolicyDirector/etc/pdbackup.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

   For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

8. Install the IBM Global Security Kit (GSKit):

   ```
   rpm -i gskcrypt64-8.0.14.26.linux.s390x.rpm
   rpm -i gskssl64-8.0.14.26.linux.s390x.rpm
   ```

9. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_s390/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
10. Install the client packages of Tivoli Directory Server:

    ```
    rpm -i packages
    ```

    where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.s390.rpm`
Base client package	`idsldap-cltbase63-6.3.0-17.s390.rpm`
64-bit client package	`idsldap-clt64bit63-6.3.0-17.s390.rpm`
Java client package	`idsldap-cltjava63-6.3.0-17.s390x.rpm`

11. Ensure that your registry server is running.
12. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory.
    b. Run the `isamLicense` script:

       ```
       isamLicense
       ```

       Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

-? Help: Displays the syntax of the script file.

c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

d. Accept the license by pressing **1**.

13. Upgrade the Security Access Manager license:

```
rpm -U PDlic-PD-7.0.0-0.s390x.rpm
```

14. Upgrade IBM Security Utilities:

```
rpm -U TivSecUtl-TivSec-7.0.0-0.s390x.rpm
```

15. Upgrade the Security Access Manager runtime:

```
rpm -U PDRTE-PD-7.0.0-0.s390x.rpm
```

16. Upgrade the Security Access Manager policy server:

```
rpm -U PDMgr-PD-7.0.0-0.s390x.rpm
```

17. Security Access Manager schema definitions are added automatically during the installation of the server package of Tivoli Directory Server 6.3 FP17. Update the schema if you are using a supported LDAP server other than IBM Tivoli Directory Server as your registry server.

    Update the schema with the **ivrgy_tool** as follows:

```
ivrgy_tool -d -h ldap_host -p port -D ldap_admin -w pwd schema
```

    For more information about the **ivrgy_tool** utility, see the reference information for "ivrgy_tool" on page 201.

18. Start the policy server daemon (`pdmgrd`):

```
pd_start start
```

19. Confirm that the policy server is running:

```
pd_start status
```

20. Make sure that you can contact the policy server. For example, log in to the **pdadmin** interface and run a command:

```
pdadmin -a sec_master -p password
pdadmin sec_master> acl list
```

Results

The upgrade of the policy server for Linux on System z is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Linux on System z: Upgrading the policy server using two systems

Use the following procedure to upgrade your policy server to the Security Access Manager, version 7.0, policy server on two Linux on System z servers.

About this task

Follow these steps to set up a new 7.0 policy server on a second system while your original policy server continues functioning with minimal downtime.

Note: This two-system approach is supported for LDAP-based registries only.

Procedure

1. Before you upgrade the policy server to 7.0, review "AIX, Solaris, and Linux: Upgrade considerations" on page 21.
2. Log in as `root`.
3. Obtain access to the *IBM Security Access Manager for Web for Linux on System z* product image on the original system.
4. Stop all Tivoli Access Manager applications and services on the original system:

   ```
   pd_start stop
   ```
5. Confirm that all Tivoli Access Manager services and applications are stopped on the original system:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
6. Back up your user registry data.

   For Tivoli Directory Server, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17; otherwise, consult the documentation for your supported registry server.
7. Use the **pdbackup** utility on the original system to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   cd image_path/linux_s390/migrate/migxxto700.lst
   ```

   where *image_path* is where the installation images are located, and *xx* is the version of software that you are migrating from. The name of the backup list file would be as follows:

   For 6.1.1

   ```
   mig611to700.lst
   ```

   For 6.1

   ```
   mig61to700.lst
   ```

   For 6.0

   ```
   mig60to700.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /opt/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the `migxxto700.lstlist_date.time.tar` default file name.

   For more information about the **pdbackup** utility, see "pdbackup" on page 205.
8. Restart the policy server daemon (`pdmgrd`) on the original policy server:

   ```
   pd_start start
   ```
9. Copy the archive that is produced by the **pdbackup** utility from the original policy server to the new 7.0 policy server.

Note: The new 7.0 policy server must be a clean system. Do not reuse an existing policy server system.

10. On the new system, install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
11. Obtain access to the *IBM Security Access Manager for Web for Linux on System z* image on the System z system.
12. Change to the following directory:
    ```
    cd image_path/linux_s390
    ```
    where *image_path* is where the installation images are located.
13. Install the Global Security Kit (GSKit) on the new system:
    ```
    rpm -i gskcrypt64-8.0.14.26.linux.s390x.rpm
    rpm -i gskssl64-8.0.14.26.linux.s390x.rpm
    ```
14. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_s390/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
15. Install the Tivoli Directory Server client packages on the new system:
    ```
    rpm -i packages
    ```
    where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.s390.rpm`
Base client package	`idsldap-cltbase63-6.3.0-17.s390.rpm`
64-bit client package	`idsldap-clt64bit63-6.3.0-17.s390.rpm`
Java client package	`idsldap-cltjava63-6.3.0-17.s390x.rpm`

16. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory.
    b. Run the `isamLicense` script:
       ```
       isamLicense
       ```
       Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

       -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

       -? Help: Displays the syntax of the script file.
    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
17. Install the Security Access Manager license on the new system:
    ```
    rpm -i PDlic-PD-7.0.0-0.s390x.rpm
    ```
18. Install IBM Security Utilities on the new system:
    ```
    rpm -i TivSecUtl-TivSec-7.0.0-0.s390x.rpm
    ```

19. Install the Security Access Manager runtime on the new system:

    ```
    rpm -i PDRTE-PD-7.0.0-0.s390x.rpm
    ```

20. Install the Security Access Manager policy server on the new system:

    ```
    rpm -i PDMgr-PD-7.0.0-0.s390x.rpm
    ```

21. Use the **pdbackup** utility to extract data to the new 7.0 policy server:

    ```
    /opt/PolicyDirector/bin/pdbackup -action extract -path restore_directory
    -file archive_name
    ```

    where:

    –path *restore_directory*
    Specifies a temporary directory on the new 7.0 policy server in which you want to extract your archive data.

    –file *archive_name*
    Specifies the fully qualified path to the archive that came from the original policy server.

    For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

    CAUTION:

    If there is a configuration problem, do not unconfigure this system. If you unconfigure the system, critical data that is needed by the original policy server will be destroyed. Follow instructions in "Linux on System z: Retiring the original policy server" on page 43 with the new server.

    The new system is a clone of the original policy server system. This means that the placement of critical files, such as certificate files, must be identical to the original system. For example, if a certificate file is in the /certs directory on the original policy server, it must be in the /certs directory on the new system.

22. Ensure that the LDAP server used by the original policy server is running.
23. Security Access Manager schema definitions are added automatically during the installation of the server package of Tivoli Directory Server 6.3 FP17. Update the schema if you are using a supported LDAP server other than IBM Tivoli Directory Server as your registry server.

    Update the schema with the **ivrgy_tool** as follows:

    ```
    ivrgy_tool -d -h ldap_host -p port -D ldap_admin -w pwd schema
    ```

    For more information about the **ivrgy_tool** utility, see the reference information for "ivrgy_tool" on page 201.
24. Use the **pdconfig** utility to configure the Security Access Manager runtime on the new 7.0 policy server. When prompted for an LDAP server, specify the name of the LDAP server that is used by the original policy server.
25. Use the **pdconfig** utility to configure the new policy server.
    a. When prompted, if you want to configure the policy for migration purposes, select `yes`.
    b. When prompted, if you want to use this policy server for standby, select `no`.
    c. Enter the *restore_directory* specified by the `–path` option in step 21.
26. Confirm that the new policy server is running on the new system:

    ```
    pd_start status
    ```

27. Your system policy server is ready. Run **pdadmin** and query both the ACL database and the registry to verify their status on the new system. For example:

```
pdadmin –a sec_master -p password
pdadmin sec_master> acl list
pdadmin sec_master> user list s* 10
```

28. If you made updates or changes to your database during the migration process, complete the following steps:
    a. Stop the new policy server daemon (pdmgrd):

       ```
       pd_start stop
       ```

    b. Copy the database files from the original policy server to the new 7.0 policy server. The default location of the files to copy is as follows:

       ```
       /var/PolicyDirector/db
       ```

       After you copy the files, verify that the owning user and owning group are both ivmgr.

    c. Start the new policy server daemon (pdmgrd):

       ```
       pd_start start
       ```

Results

The upgrade of the policy server for Linux on System z is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Upgrade other Security Access Manager systems to 7.0 (in the order that is specified in Chapter 1, “Introduction,” on page 1).

Ensure that the host name of the new policy server is specified in the Security Access Manager configuration files for the components, including the pd.conf file in the install_path/etc directory, and any AZN application configuration files.

To do this, on each system on which you want to use the new policy server, ensure that the master-host value in the [manager] stanza of the configuration file contains the server host name of the new policy server. See the *IBM Security Access Manager for Web Administration Guide* for more information about the master-host key value.

After you update all your Security Access Manager systems, complete the procedure in “Linux on System z: Retiring the original policy server” to retire your original policy server.

Linux on System z: Retiring the original policy server

About this task

If you upgraded the policy server using the two system approach, retire the original policy server after its data and the Tivoli Directory Server client and server are successfully migrated to the 7.0 policy server system.

CAUTION:

Do not unconfigure the original policy server or the new policy server at any time during the upgrade process. Unconfiguration of the original policy server or new policy server will destroy critical data that is needed by the policy server. The destruction of critical data results in a nonworking Security Access Manager environment.

Procedure

1. Stop the policy server.
2. From the original policy server, enter:
   ```
   /opt/PolicyDirector/sbin/pdmgr_ucf
   ```
3. Uninstall your previous version of the Tivoli Access Manager policy server.
   For uninstallation procedures, see the documentation for that version of Tivoli Access Manager.

Solaris: Upgrading the policy server

Upgrade the policy server system on Solaris using a single system or two systems. If you complete an upgrade using the two system approach, retire the original policy server after you successfully migrate its data and the Tivoli Directory Server client and server to the policy server system.

Solaris: Upgrading the policy server using a single system

To upgrade the policy server system on Solaris, complete the following instructions.

About this task

Note: If you encounter a problem during upgrade of the policy server to 7.0 using this single-system approach, you can restore the system to its previous level. For instructions, see "Solaris: Restoring the policy server" on page 186.

Procedure

1. Before you upgrade the policy server to 7.0, review "AIX, Solaris, and Linux: Upgrade considerations" on page 21.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Stop all Tivoli Access Manager applications and services:
   ```
   pd_start stop
   ```
6. Confirm that all Tivoli Access Manager services and applications are stopped:
   ```
   pd_start status
   ```
   If any Tivoli Access Manager service or application is still running, issue the **kill** command:
   ```
   kill –9 daemon_process_id
   ```
7. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

```
/opt/PolicyDirector/bin/pdbackup -action backup
 -list fullpath_to_backup_listfile
-path path -file filename
```

where:

–list *fullpath_to_backup_listfile*
Specifies the fully qualified path to the backup list file. For example:

```
/opt/PolicyDirector/etc/pdbackup.lst
```

–path *path*
Specifies the path where you want the backed up files to be stored.

For example:

```
/var/PolicyDirector/pdbackup
```

–file *filename*
Specifies a file name other than the pdbackup.lst_*date.time*.tar default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

8. Install the IBM Global Security Kit (GSKit):

```
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8cry64
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8ssl64
```

where *image_path* specifies the location of the package. The -G option ensures that the package is added in the current zone only.

9. Install the Tivoli Directory Server license files by running the idsLicense script in the *image_path*/solaris/tdsLicense/license directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
10. Install the client packages of the Tivoli Directory Server:

```
pkgadd -d /image_path/solaris/packages
-a /image_path/solaris/pddefault
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and *packages* are as follows:

License package	idsldap.license63.pkg
Base client package	idsldap.cltbase63.pkg
64-bit client package	idsldap.clt64bit63.pkg
Java client package	idsldap.cltjava63.pkg

11. Ensure that your registry server is running.
12. Run the isamLicense license script by completing the following actions:
    a. In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the isamLicense script:

```
isamLicense
```

Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

-? Help: Displays the syntax of the script file.

c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

d. Accept the license by pressing **1**.

13. Install or upgrade the Security Access Manager license:

    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDlic
    ```

    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDlic is the Security Access Manager license package. The -G option ensures that the package is added in the current zone only.

14. Install or upgrade IBM Security Utilities:

    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G TivSecUtl
    ```

    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and TivSecUtl is the IBM Security Utilities package. The -G option ensures that the package is added in the current zone only.

15. Upgrade Security Access Manager runtime:

    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDRTE
    ```

    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDRTE is the Security Access Manager runtime package. The -G option ensures that the package is added in the current zone only.

16. Upgrade Security Access Manager policy server:

    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDMgr
    ```

    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDMgr is the Security Access Manager policy server package. The -G option ensures that the package is added in the current zone only.

17. Security Access Manager schema definitions are added automatically during the installation of the server package of Tivoli Directory Server 6.3 FP17. Update the schema if you are using a supported LDAP server other than IBM Tivoli Directory Server as your registry server.

    Update the schema with the **ivrgy_tool** as follows:

    ```
    ivrgy_tool -d -h ldap_host -p port -D ldap_admin -w pwd schema
    ```

    For more information about the **ivrgy_tool** utility, see the reference information for "ivrgy_tool" on page 201.

18. Start the policy server daemon (pdmgrd):

    ```
    pd_start start
    ```

19. Confirm that the policy server is running:

    ```
    pd_start status
    ```

20. Make sure that you can contact the policy server. For example, log in to the **pdadmin** interface and run a command:

```
pdadmin -a sec_master -p password
pdadmin sec_master> acl list
```

Results

The upgrade of the policy server on Solaris is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Solaris: Upgrading the policy server using two systems

To upgrade the policy server system on Solaris using two systems, complete the following instructions.

About this task

Follow these steps to set up a new 7.0 policy server on a second system while you allow your original policy server system to continue functioning with minimal downtime.

Note: This two-system approach is supported for LDAP-based registries only.

Procedure

1. Before you upgrade the policy server to 7.0, review "AIX, Solaris, and Linux: Upgrade considerations" on page 21.
2. Log in as `root`.
3. On the original policy server, access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
4. Stop all Tivoli Access Manager applications and services on the original system:

   ```
   pd_start stop
   ```
5. Confirm that all Tivoli Access Manager services and applications are stopped on the original system:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
6. Back up your user registry data.

   For Tivoli Directory Server, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17; otherwise, consult the documentation for your supported registry server.
7. Use the **pdbackup** utility on the original system to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   image_path/solaris/migrate/migxxto700.lst
   ```

   where *xx* is the version of software that you are migrating from. The name of the backup list file would be as follows:

For 6.1.1

`mig611to700.lst`

For 6.1

`mig61to700.lst`

For 6.0

`mig60to700.lst`

–path *path*

Specifies the path where you want the backed up files to be stored.

For example:

`/var/PolicyDirector/pdbackup`

–file *filename*

Specifies a file name other than the `mig`*`xx`*`to700.lst_`*`date.time`*`.tar` default file name.

For more information about the **pdbackup** utility, see "pdbackup" on page 205.

8. Restart the policy server daemon (`pdmgrd`) on the original policy server:

   ```
   pd_start start
   ```

9. Copy the archive that is produced by the **pdbackup** utility from the original policy server to the new 7.0 policy server.

   Note: The new 7.0 policy server must be a clean system. Do not reuse an existing policy server system.

10. On the new system, install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
11. On the new system, access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
12. Change to the `/`*`image_path`*`/solaris` directory.
13. Install the Global Security Kit (GSKit) on the new system:

    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8cry64
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8ssl64
    ```

    where `/`*`image_path`*`/solaris` specifies the location of the installation images, and `/`*`image_path`*`/solaris/pddefault` specifies the location of the installation administration script. The `-G` option ensures that the package is added in the current zone only.
14. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *`image_path`*`/solaris/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
15. Install the Tivoli Directory Server client packages on the new system:

    ```
    pkgadd -d /image_path/solaris/packages
    -a /image_path/solaris/pddefault
    ```

    where `/`*`image_path`*`/solaris` specifies the location of the installation images, `/`*`image_path`*`/solaris/pddefault` specifies the location of the installation administration script, and *packages* are as follows:

License package	`idsldap.license63.pkg`
Base client package	`idsldap.cltbase63.pkg`
64-bit client package	`idsldap.clt64bit63.pkg`
Java client package	`idsldap.cltjava63.pkg`

16. Run the `isamLicense` license script by completing the following actions:

a. In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

b. Run the isamLicense script:

```
isamLicense
```

Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an exit status 0 (SUCCESS) if it is.

-? Help: Displays the syntax of the script file.

c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

d. Accept the license by pressing **1**.

17. Install the Security Access Manager license on the new system:

```
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G  PDlic
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDlic is the Security Access Manager license package. The -G option ensures that the package is added in the current zone only.

18. Install IBM Security Utilities on the new system:

```
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G TivSecUtl
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and TivSecUtl is the IBM Security Utilities package. The -G option ensures that the package is added in the current zone only.

19. Install Security Access Manager runtime on the new system:

```
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDRTE
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDRTE is the Security Access Manager runtime package. The -G option ensures that the package is added in the current zone only.

20. Install Security Access Manager policy server on the new system:

```
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDMgr
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDMgr is the Security Access Manager policy server package. The -G option ensures that the package is added in the current zone only.

21. Use the **pdbackup** utility on the new system to extract data to the new 7.0 policy server:

```
/opt/PolicyDirector/bin/pdbackup -action extract -path restore_directory
-file archive_name
```

where:

–path *restore_directory*
Specifies a temporary directory on the new 7.0 policy server in which you want to extract your archive data.

–file *archive_name*
Specifies the fully qualified path to the archive that came from the original policy server.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

CAUTION:

If there is a configuration problem, do not unconfigure this system. If you unconfigure the system, critical data that is needed by the original policy server will be destroyed. Follow instructions in "Solaris: Retiring the original policy server" on page 51 with the new server.

The new system is a clone of the original policy server system. This means that the placement of critical files, such as certificate files, must be identical to the original system. For example, if a certificate file is in the `/certs` directory on the original policy server, it must be in the `/certs` directory on the new system.

22. Ensure that the LDAP used by the original policy server is running.
23. Security Access Manager schema definitions are added automatically during the installation of the server package of Tivoli Directory Server 6.3 FP17. Update the schema:
    - If you are using a supported LDAP server other than IBM Tivoli Directory Server as your registry server.
    - If you want to continue using your previous version of IBM Tivoli Directory Server 6.2, and you do not want to upgrade the server to IBM Directory Server version 6.3 FP17.

    Update the schema with the **ivrgy_tool** as follows:

    ```
    ivrgy_tool -d -h ldap_host -p port -D ldap_admin -w pwd schema
    ```

    For more information about the **ivrgy_tool** utility, see the reference information for "ivrgy_tool" on page 201.
24. Use the **pdconfig** utility to configure the Security Access Manager runtime on the new 7.0 policy server. When prompted for an LDAP server, specify the name of the LDAP server and LDAP port number that is used by the original policy server.
25. Use the **pdconfig** utility to configure the new 7.0 policy server.
    - When prompted if you want to configure the policy for migration purposes, select `yes`.
    - When prompted if you want to use this policy server for standby, select `no`.
    - Enter the *restore_directory* specified by the `–path` option in step 21 on page 49.
26. Confirm that the policy server is running on the new system:

    ```
    pd_start status
    ```
27. Your new system policy server is ready. Run **pdadmin** and query both the ACL database and the registry to verify their status on the new system. For example:

```
pdadmin –a sec_master -p password
pdadmin sec_master> acl list
pdadmin sec_master> user list s* 10
```

28. If you made updates or changes to your database during the migration process, complete the following steps:
    a. Stop the new policy server daemon (pdmgrd):
       ```
       pd_start stop
       ```
    b. Copy the database files from the original policy server to the new 7.0 policy server. The default location of the files to copy is as follows:
       ```
       /var/PolicyDirector/db
       ```
    c. Start the new policy server daemon (pdmgrd):
       ```
       pd_start start
       ```

Results

The upgrade of the policy server on Solaris is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Upgrade other Security Access Manager systems to 7.0 (in the order that is specified in Chapter 1, "Introduction," on page 1).

Ensure that the host name of the new policy server is specified in the configuration files for the Security Access Manager components, including the pd.conf file in the install_path/etc directory, and any AZN application configuration files.

To do this, on each system on which you want to use the new policy server, ensure that the master-host value in the [manager] stanza of the configuration file contains the server host name of the new policy server. See the *IBM Security Access Manager for Web Administration Guide* for more information about the master-host key value.

After you update all your Security Access Manager systems, complete the procedure in "Solaris: Retiring the original policy server" to retire your original policy server.

Solaris: Retiring the original policy server

Use the following procedure to retire your previous level policy server on Solaris when it is no longer needed in your environment.

About this task

If you upgraded the policy server using the two system approach, retire the original policy server after its data and the Tivoli Directory Server client and server are successfully migrated to the 7.0 policy server system.

CAUTION:

Do not unconfigure the original policy server or the new policy server at any time during the upgrade process. Unconfiguration of the original policy server or new policy server will destroy critical data that is needed by the policy server. The destruction of critical data results in a nonworking Security Access Manager environment.

Procedure

1. Stop the policy server.
2. From the original policy server, enter:
   ```
   /opt/PolicyDirector/sbin/pdmgr_ucf
   ```
3. Uninstall your previous version of Tivoli Access Manager.
   For uninstallation procedures, see the documentation for that version of Tivoli Access Manager.

Windows: Upgrading the policy server

Upgrade the policy server system for Windows following the two-system approach.

After you successfully migrate the policy server data and the Tivoli Directory Server client and server to the policy server system, retire the original policy server. See "Windows: Retiring the original policy server" on page 56.

Windows: Upgrade considerations

Before you upgrade the policy server to 7.0, review the following considerations

- Back up the following data:
  - All Tivoli Access Manager servers.
    See the **pdbackup** utility in the *IBM Security Access Manager for Web Command Reference* for information.
  - User registry data
    For Tivoli Directory Server, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17; otherwise, consult the documentation for your supported registry server.
- Install IBM JRE 1.6 or higher.
- Upgrade your operating system to the minimum supported level. For information about minimum supported levels, see *IBM Security Access Manager for Web Release Notes*.
- For Windows systems, you must follow the upgrade instructions for a two system upgrade to migrate the Policy Server and its data onto a supported platform.
- In Tivoli Directory Server version 6.3 FP17, clients can coexist on the same workstation with a client that is version 6.0, 6.1, or 6.2. The Tivoli Directory Server 6.3 FP17 server requires that the version 6.3 client and the Java client also be installed. In addition, the server can coexist on the same workstation with another client that is version 6.0, 6.1, or 6.2, or with a version of the 6.3 server.
- You are not required to upgrade all Security Access Manager components in your secure domain to a 7.0 level. However, if you upgrade any Security Access Manager component on a system, all components on that same system must also be upgraded to the 7.0 level, and you must install Tivoli Directory Server client 6.3 FP17 on that system.
- If Tivoli Directory Server is your registry server and is on *a different machine* from any Security Access Manager component, you can upgrade the registry server either before or after the upgrade of the Security Access Manager 7.0 component.
  However, when the server package of Tivoli Directory Server is installed *on the same machine* as any Security Access Manager 7.0 component, and if you choose to upgrade the server package of Tivoli Directory Server to 6.3 FP17, you must

upgrade or install the Tivoli Directory Server 6.3 FP17 client and server packages at the same time as you install the Security Access Manager 7.0 component on that machine.

- If you are upgrading and use a language other than English, remember to upgrade your language package. See the *IBM Security Access Manager for Web Installation Guide* to install the language package.
- The upgrade process does not support changing your configuration, such as your registry type. For example, you cannot upgrade from an LDAP registry to an Active Directory registry.
- Log in to the system as a user with administrator privileges.
- The default temporary directory is the value that is specified by the `TMP` environment variable. If the `TMP` variable does not exist, the value that is specified by the `TEMP` environment variable is used. If neither of these variables is set, the `system` directory is the temporary directory.
- The installation path varies and is dependent on the directory that is specified during the installation.

For operating systems other than Windows, see "AIX, Solaris, and Linux: Upgrade considerations" on page 21.

Windows: Upgrading the policy server using two systems

Follow these steps to set up a new 7.0 policy server on a second system while your original policy server system continues functioning with minimal downtime.

Procedure

1. Before you upgrade the policy server to 7.0, review "Windows: Upgrade considerations" on page 52.
2. Log in as a user with administrative privileges.
3. From the original policy server, access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
4. Exit all running programs on the original system. During the upgrade process, you are prompted to restart your Windows system periodically.
5. Stop all Tivoli Access Manager applications and services. For example, on Windows 2008 systems, select **Start** > **Control Panel** > **Administrative Tools**. Double-click the **Services** icon, and stop all Tivoli Access Manager services that are running on the local system, including applications, such as WebSEAL.

   From **Services**, find the **Access Manager Auto-Start Service**. Double-click this service and change the startup type to **Disabled**.
6. Back up your user registry data.

   For Tivoli Directory Server, see Chapter 2, "Upgrading IBM Tivoli Directory Server," on page 17; otherwise, consult the documentation for your supported registry server.
7. Use the **pdbackup** utility on the original system to back up critical Tivoli Access Manager information:

   ```
   "C:\Program Files\Tivoli\Policy Director\bin\pdbackup"
    -action backup -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

image_path\windows\migrate\mig*xx*to700.lst

where *xx* is the version of software from which you are migrating. The name of the backup list file would be as follows:

For 6.1.1

mig611to700.lst

For 6.1

mig61to700.lst

For 6.0

mig60to700.lst

–path *path*

Specifies the path where you want the backed up files to be stored. For example:

```
"C:\Program Files\Tivoli\Policy Director\pdbackup"
```

–file *filename*

Specifies a file name other than the mig*xx*to700.lst_*date.time*.dar default file name.

For more information about the **pdbackup** utility, see "pdbackup" on page 205.

8. Restart the policy server service (pdmgrd) on the original policy server. For example, on Windows 2008 systems, select **Start** > **Control Panel** > **Administrative Tools**. Double-click the **Services** icon, and start the service.
9. Copy the archive file that is produced by the **pdbackup** utility from the original policy server to the system for the 7.0 policy server.

   Note: The system for the 7.0 policy server must be a clean system. Do not reuse an existing policy server system.
10. On the new system, install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
11. On the new system, access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
12. Install Global Security Kit (GSKit) on the new system by completing the following steps:
    a. Change to the \windows\GSKit directory on the drive where the installation images are located.
    b. Enter the following statement:
       ```
       gsk8ssl64
       ```
    c. Follow the online instructions to complete the installation.
13. **LDAP registry servers only:** If you use an LDAP server as your registry, install the Tivoli Directory Server client by completing the following steps:
    a. Run the **install_tds.exe** script in the windows\tds_client64 directory.
    b. Select to install **C Client 6.3** and **Java Client 6.3**.
    c. Follow the online instructions to complete the installation.

    Note: If you are using Active Directory as your registry and Security Access Manager is in your domain, the Tivoli Directory Server client is not required.
14. Install the security utilities on the new system by running the **setup.exe** script in the \windows\TivSecUtl\Disk Images\Disk1\PDLIC\Disk Images\Disk1 directory. Follow the online instructions to complete the installation.

15. Install the following Security Access Manager components on the new systems by running the **setup.exe** script in the `\windows\PolicyDirector\Disk Images\Disk1` directory. Select to install the following components in this sequence:
    - **Security Access Manager license**
    - **Security Access Manager runtime**
    - **Security Access Manager policy server**

    Follow the online instructions to complete the installation.
16. Use the **pdbackup** utility on the new system to extract data to the new 7.0 policy server:

    ```
    C:\Program Files\Tivoli\Policy Director\bin\pdbackup.exe -action extract
    -path restore_directory -file archive_name
    ```

    where:

    –path *restore_directory*
    Specifies a temporary directory on the version 7.0 policy server in which you want to extract your archive data.

    –file *archive_name*
    Specifies the fully qualified path to the archive that came from the original policy server.

    For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

    CAUTION:

    If there is a configuration problem, do not unconfigure this system. Unconfiguring the system would destroy critical data that is needed by the original policy server. Follow instructions in "Windows: Retiring the original policy server" on page 56 with the new server.

    The new system is a clone of the original policy server system. The placement of critical files, such as certificate files, must be identical to the original system. For example, if a certificate file is in the `\certs` directory on the original policy server, it must be in the `\certs` directory on the new system.
17. Ensure that your LDAP server is running. For example, on Windows 2008 systems, select **Start** > **Control Panel** > **Administrative Tools** and then double-click the **Services** icon to verify whether the service is started.
18. If you are using a supported LDAP server other than Tivoli Directory Server as your registry server, update the schema with the **ivrgy_tool** utility:

    ```
    ivrgy_tool -d -h ldap_host -p port -D ldap_admin -w pwd schema
    ```

    For more information about the **ivrgy_tool** utility, see the reference information for "ivrgy_tool" on page 201.

    Note: Installations of the Tivoli Directory Server 6.3 FP17 server package automatically update the Security Access Manager schema definitions.
19. Use the **pdconfig** utility to configure the runtime on the version 7.0 policy server. When prompted for an LDAP server, specify the name of the LDAP server that is used by the original policy server.
20. Use the **pdconfig** utility to configure the new 7.0 policy server. When prompted if you want to configure the policy for migration purposes, select **yes** and enter the *restore_directory* specified by the `–path` option in step 16.

21. Confirm that the policy server is running on the new system. For example, on Windows 2008 systems, select **Start** > **Control Panel** > **Administrative Tools**. Double-click the **Services** icon to verify whether the service is running.
22. Optional: Your new policy server system is ready. To verify the status of the ACL database and registry, run **pdadmin** on the new system to query both the ACL database and the registry. For example:

```
pdadmin –a sec_master -p password
pdadmin sec_master> acl list
pdadmin sec_master> user list s* 10
```

23. Optional: If you made updates or changes to your database during the migration process, complete the following steps:
    a. Stop the policy server daemon; for example, on a Windows 2008 system, complete the following steps:
        1) Click **Start** > **Control Panel** > **Administrative Tools**.
        2) Double-click the **Services** icon and stop the service.
    b. Copy the database files from the original policy server to the version 7.0 policy server. The default location of the files to copy is in the following directory:

```
C:\Program Files \Tivoli\PolicyDirector\db
```

    c. Start the policy server (`pdmgrd`). For example, on a Windows 2008 system:
        1) Click **Start** > **Control Panel** > **Administrative Tools**.
        2) Double-click the **Services** icon and start the service.

Results

The upgrade of the 7.0 policy server on Windows is now complete. You can upgrade other Security Access Manager systems to version 7.0, or update your previous level Tivoli Access Manager components to connect to the new policy server.

What to do next

Check that the host name of the 7.0 policy server is specified in the configuration files of the product components, including the `install_path\etc\pd.conf` file, and any AZN application configuration file.

To check the host name, on each system where you want to use the 7.0 policy server, check that the `master-host` value in the `[manager]` stanza of the configuration file contains the server host name of the 7.0 policy server. See the *IBM Security Access Manager for Web Administration Guide* for more information about the `master-host` key value.

After you update all your Security Access Manager systems, complete the procedure in "Windows: Retiring the original policy server" to retire your original policy server.

Windows: Retiring the original policy server

Retire your previous level policy server on Windows when you no longer need the original policy server.

About this task

After you upgrade the policy server using the two system approach, retire the original policy server after its data and the Tivoli Directory Server client and server are successfully migrated to the 7.0 policy server system.

CAUTION:

Do not unconfigure the original policy server or the new policy server at any time during the upgrade process. Unconfiguration of the original policy server or new policy server during upgrade destroys critical data that is needed by the policy server. The destruction of critical data results in a nonworking Security Access Manager environment.

Procedure

1. Stop the policy server.
2. From the original policy server, run:

   ```
   C:\Program Files\Tivoli\Policy Director\sbin\pdmgr_ucf.exe
   ```
3. Uninstall your previous version of Tivoli Access Manager.

   For uninstallation procedures, see the documentation for that version of Tivoli Access Manager.
4. **For Tivoli Access Manager 6.1.1 upgrades only**: If you start to uninstall, and a message states that the policy server must be unconfigured, complete the following steps:
   a. Click **Start** > **Run**; type `regedit` in the entry field, and then click **OK** to open the registry.
   b. Click **My Computer** > **HKEY_LOCAL_MACHINE** > **Tivoli** > **Policy Director Management Server** > **6.1.1.**
   c. Change the configuration value from `Yes` to `No`.
   d. Resume the uninstallation process.

Chapter 4. Upgrading the authorization server

Security Access Manager supports an upgrade of an authorization server to version 7.0.

Authorization server: Upgrade considerations

Before you upgrade the authorization server to 7.0, review the following considerations:

- Upgrade your operating system to the minimum supported level. For information about minimum supported levels, see *IBM Security Access Manager for Web Release Notes*.
- In Tivoli Directory Server version 6.3 FP17, clients can coexist on the same workstation with a client that is version 6.0, 6.1, or 6.2. The Tivoli Directory Server 6.3 FP17 server requires that the version 6.3 client and the Java client are also installed. In addition, the server can coexist on the same workstation with another client that is version 6.0, 6.1, or 6.2, or with a version of the 6.3 server.
- You are not required to upgrade all Security Access Manager components in your secure domain to a 7.0 level. However, if you upgrade any Security Access Manager component on a system, all components must be upgraded on that system to the 7.0 level, and you must install Tivoli Directory Server client 6.3 FP17 on that system.

  For a list of components that are compatible with Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.
- In general, if Tivoli Directory Server is your registry server and is *a different machine* from any existing Tivoli Access Manager component, you can upgrade the registry server at any time—before or after the upgrade of the Security Access Manager 7.0 component.

  However, when the server package of Tivoli Directory Server is installed *on the same machine* as any existing Tivoli Access Manager component and if you choose to install the server package of Tivoli Directory Server 6.3 FP17, install the Tivoli Directory Server 6.3 FP17 client and server packages at the same time as you install the Security Access Manager 7.0 component on that machine.
- If you are upgrading and use a language other than English, remember to upgrade your language package. See the *IBM Security Access Manager for Web Installation Guide* to install the language package. However, when you upgrade IBM Tivoli Directory Server language packages, you must use the upgrade (**-U**) option for Linux operating systems.

AIX: Upgrading the authorization server

Upgrade your existing authorization server on AIX to the Security Access Manager, version 7.0, authorization server.

About this task

To upgrade an authorization server system on AIX, complete the following instructions:

© Copyright IBM Corp. 2003, 2012

Procedure

1. Before you upgrade the authorization server to 7.0, review the considerations in "Authorization server: Upgrade considerations" on page 59.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.

   Note: The AIX operating system requires version 10.1 or later of the `xlC` file set. Check your current version by using the **`lslpp`** command and upgrade, if necessary.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```
6. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **`kill`** command:

   ```
   kill –9 daemon_process_id
   ```
7. Use the **`pdbackup`** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   /opt/PolicyDirector/etc/pdbackup.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

   For more information about the **`pdbackup`** utility, see "Upgrade utilities," on page 197.
8. Install the Global Security Kit (GSKit):

   ```
   installp -acgYXd image_path/usr/sys/inst.images GSKit8.gskcrypt64.ppc.rte
   installp -acgYXd image_path/usr/sys/inst.images GSKit8.gsksslppc.rte
   ```

   where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located.
9. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/usr/sys/inst.images/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
10. Install the client packages of Tivoli Directory Server:

    ```
    installp -acgYXd image_path/usr/sys/inst.images packages
    ```

where *image_path*/usr/sys/inst.images is the directory where the installation images are located and where *packages* are the names of the Tivoli Directory Server client packages:

License package	idsldap.license63
Client base package	idsldap.cltbase63
Client package (64-bit) (no SSL)	idsldap.clt64bit63
Client package (64-bit) (SSL)	idsldap.clt_max_crypto64bit63
Java client package	idsldap.cltjava63

11. Ensure that your registry server and policy server are running.
12. Run the isamLicense license script by completing the following actions:
    a. In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the isamLicense script:

       ```
       isamLicense
       ```

       Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

       -t Test: Silently tests whether the current license is already installed. Returns an exit status 0 (SUCCESS) if it is.

       -? Help: Displays the syntax of the script file.
    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
13. Upgrade the Security Access Manager license:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.lic
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located and PD.lic is the Security Access Manager license package.
14. Upgrade IBM Security Utilities:

    ```
    installp -acgYXd image_path/usr/sys/inst.images TivSec.Utl
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located and TivSec.Utl is the IBM Security Utilities package.
15. Upgrade the Security Access Manager runtime:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.RTE
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located and PD.RTE is the Security Access Manager runtime package.
16. Upgrade the Security Access Manager authorization server:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.Acld
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located and PD.Acld is the Security Access Manager authorization server.

17. If the two-system upgrade option was used for the policy server, the `master-host` record must be updated to point to the new policy server. Edit the `master-host` entry in each of the following configuration files:
    - Security Access Manager runtime

      `/opt/PolicyDirector/etc/pd.conf`
    - Security Access Manager authorization server

      `/opt/PolicyDirector/etc/ivacld.conf`
18. Start the authorization server daemon (`pdacld`):

    ```
    pd_start start
    ```
19. Confirm that the authorization server is running:

    ```
    pd_start status
    ```
20. Verify that you can contact the upgraded 7.0 policy server. For example, log on to the **pdadmin** interface and run a command:

    ```
    pdadmin -a sec_master -p password
    pdadmin sec_master> acl list
    ```

Results

The upgrade of the authorization server on AIX is now complete.

Linux on x86-64: Upgrading the authorization server

Upgrade your existing authorization server on Linux x86-64 to the Security Access Manager, version 7.0, authorization server.

Procedure

1. Before you upgrade the authorization server to 7.0, review the considerations in "Authorization server: Upgrade considerations" on page 59.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Change to the following directory:

   ```
   cd image_path/linux_x86
   ```

   where *image_path* is where the DVD is mounted.
6. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```
7. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
8. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

–list *fullpath_to_backup_listfile*
Specifies the fully qualified path to the backup list file. For example:
`/opt/PolicyDirector/etc/pdbackup.lst`

–path *path*
Specifies the path where you want the backed up files to be stored.

For example:
`/var/PolicyDirector/pdbackup`

–file *filename*
Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

9. Install or upgrade IBM Global Security Kit (GSKit).

```
rpm -i gskcrypt64-8.0.14.26.linux.x86_64.rpm
rpm -i gsksslб4-8.0.14.26.linux.x86_64.rpm
```

Or, if you have an earlier version of GSKit installed, upgrade to GSKit 8.0.14.26:

```
rpm -U gskcrypt64-8.0.14.26.linux.x86_64.rpm
rpm -U gsksslб4-8.0.14.26.linux.x86_64.rpm
```

10. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_x86/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
11. Install the client packages of Tivoli Directory Server:

```
rpm -i packages
```

where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.x86_64.rpm`
Base client package	`idsldap-cltbase63-6.3.0-17.x86_64.rpm`
64-bit client package	`idsldap-clt64bit63-6.3.0-17.x86_64.rpm`
Java client package	`idsldap-cltjava63-6.3.0-17.x86_64.rpm`

12. Ensure that your registry server and policy server are running.
13. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:

```
isamLicense
```

Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

`-?` Help: Displays the syntax of the script file.

c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

d. Accept the license by pressing **1**.

14. Upgrade the Security Access Manager license:
    ```
    rpm -U PDlic-PD-7.0.0-0.x86_64.rpm
    ```
15. Upgrade IBM Security Utilities:
    ```
    rpm -U TivSecUtl-TivSec-7.0.0-0.x86_64.rpm
    ```
16. Upgrade the Security Access Manager runtime:
    ```
    rpm -U PDRTE-PD-7.0.0-0.x86_64.rpm
    ```
17. Upgrade the Security Access Manager authorization server:
    ```
    rpm -U PDAcld-PD-7.0.0-0.x86_64.rpm
    ```
18. If the two-system upgrade option was used for the policy server, the `master-host` record must be updated to point to the new policy server. Edit the `master-host` entry in each of the following configuration files:
    - Security Access Manager runtime
      `/opt/PolicyDirector/etc/pd.conf`
    - Security Access Manager authorization server
      `/opt/PolicyDirector/etc/ivacld.conf`
19. Start the authorization server daemon (`pdacld`):
    ```
    pd_start start
    ```
20. Confirm that the authorization server is running:
    ```
    pd_start status
    ```
21. Verify that you can contact the upgraded 7.0 policy server. For example, log on to the **pdadmin** interface and run a command:
    ```
    pdadmin -a sec_master -p password
    pdadmin sec_master> acl list
    ```

Results

The upgrade of the authorization server for Linux on x86-64 is now complete.

Linux on System z: Upgrading the authorization server

Upgrade your existing authorization server on Linux on System z to the Security Access Manager, version 7.0, authorization server.

Procedure

1. Before you upgrade the authorization server to 7.0, review the considerations in "Authorization server: Upgrade considerations" on page 59.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage on the System z system.
5. Change to the following directory:
   ```
   cd image_path/linux_s390
   ```

   where *image_path* is where the installation images are located.

6. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```

7. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```

8. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   /opt/PolicyDirector/etc/pdbackup.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

   For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

9. Install or upgrade Global Security Kit (GSKit):

   ```
   rpm -i gskcrypt64-8.0.14.26.linux.s390x.rpm
   rpm -i gskssl64-8.0.14.26.linux.s390x.rpm
   ```

   Or, if you have an earlier version of GSKit installed, upgrade to GSKit 8.0.14.26:

   ```
   rpm -U gskcrypt64-8.0.14.26.linux.s390x.rpm
   rpm -U gskssl64-8.0.14.26.linux.s390x.rpm
   ```

10. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_s390/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
11. Install the client packages of Tivoli Directory Server:

    ```
    rpm -i packages
    ```

    where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.s390.rpm`
Base client package	`idsldap-cltbase63-6.3.0-17.s390.rpm`
64-bit client package	`idsldap-clt64bit63-6.3.0-17.s390.rpm`
Java client package	`idsldap-cltjava63-6.3.0-17.s390x.rpm`

12. Ensure that your registry server and policy server are running.
13. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

b. Run the `isamLicense` script:

```
isamLicense
```

Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

-? Help: Displays the syntax of the script file.

c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

d. Accept the license by pressing **1**.

14. Upgrade the Security Access Manager license:

```
rpm -U PDlic-PD-7.0.0-0.s390x.rpm
```

15. Upgrade the IBM Security Utilities:

```
rpm -U TivSecUtl-TivSec-7.0.0-0.s390x.rpm
```

16. Upgrade Security Access Manager runtime:

```
rpm -U PDRTE-PD-7.0.0-0.s390x.rpm
```

17. Upgrade the Security Access Manager authorization server:

```
rpm -U PDAcld-PD-7.0.0-0.s390x.rpm
```

18. If the two-system upgrade option was used for the policy server, the `master-host` record must be updated to point to the new policy server. Edit the `master-host` entry in each of the following configuration files:
    - Security Access Manager runtime

      `/opt/PolicyDirector/etc/pd.conf`
    - Security Access Manager authorization server

      `/opt/PolicyDirector/etc/ivacld.conf`

19. Start the authorization server daemon (`pdacld`):

```
pd_start start
```

20. Confirm that the authorization server is running:

```
pd_start status
```

21. Verify that you can contact the upgraded 7.0 policy server. For example, log on to the **pdadmin** interface and run a command:

```
pdadmin -a sec_master -p password
pdadmin sec_master> acl list
```

Results

The upgrade of the authorization server for Linux on System z is now complete.

Solaris: Upgrading the authorization server

Upgrade your previous level authorization server on Solaris to a Security Access Manager, version 7.0 authorization server.

Procedure

1. Before you upgrade the authorization server to 7.0, review the considerations in "Authorization server: Upgrade considerations" on page 59.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```
6. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
7. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   /opt/PolicyDirector/etc/pdbackup.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

   For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.
8. Install the Global Security Kit (GSKit):

   ```
   pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8cry64
   pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8ssl64
   ```

   where `/image_path/solaris` specifies the location of the installation images, and `/image_path/solaris/pddefault` specifies the location of the installation administration script. The `-G` option ensures that the package is added in the current zone only.
9. Install the Tivoli Directory Server license files by running the `idsLicense` script in the `image_path/solaris/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
10. Install the client packages of the Tivoli Directory Server:

    ```
    pkgadd -d /image_path/solaris/packages
    -a /image_path/solaris/pddefault
    ```

    where `/image_path/solaris` specifies the location of the installation images, `/image_path/solaris/pddefault` specifies the location of the installation administration script, and *packages* are as follows:

License package	idsldap.license63.pkg
Base client package	idsldap.cltbase63.pkg
64-bit client package	idsldap.clt64bit63.pkg
Java client package	idsldap.cltjava63.pkg

11. Ensure that your registry server and policy server are running.
12. Run the isamLicense license script by completing the following actions:
    a. In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the isamLicense script:
       ```
       isamLicense
       ```
       Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

       -t Test: Silently tests whether the current license is already installed. Returns an exit status 0 (SUCCESS) if it is.

       -? Help: Displays the syntax of the script file.
    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
13. Upgrade the Security Access Manager license:
    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDlic
    ```
    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDlic is the Security Access Manager license package. The -G option ensures that the package is added in the current zone only.
14. Upgrade IBM Security Utilities:
    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G TivSecUtl
    ```
    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and TivSecUtl is the IBM Security Utilities package. The -G option ensures that the package is added in the current zone only.
15. Upgrade Security Access Manager runtime:
    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDRTE
    ```
    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDRTE is the Security Access Manager runtime package. The -G option ensures that the package is added in the current zone only.
16. Upgrade the Security Access Manager authorization server:
    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDAcld
    ```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDAcld is the Security Access Manager authorization server package. The -G option ensures that the package is added in the current zone only.

17. If the two-system upgrade option was used for the policy server, the master-host record must be updated to point to the new policy server. Edit the master-host entry in each of the following configuration files:
    - Security Access Manager runtime

      /opt/PolicyDirector/etc/pd.conf
    - Security Access Manager authorization server

      /opt/PolicyDirector/etc/ivacld.conf
18. Start the authorization server daemon (pdacld):

    ```
    pd_start start
    ```
19. Confirm that the authorization server is running:

    ```
    pd_start status
    ```
20. Verify that you can contact the upgraded 7.0 policy server. For example, log on to the **pdadmin** interface and run a command:

    ```
    pdadmin -a sec_master -p password
    pdadmin sec_master> acl list
    ```

Results

The upgrade of the authorization server for Solaris is now complete.

Windows: Upgrading the authorization server

Upgrade your previous level authorization server on Windows to a Security Access Manager, version 7.0 authorization server.

About this task

The following procedure uses a two-system approach to set up the Security Access Manager 7.0 authorization server.

Procedure

1. Review the considerations in "Authorization server: Upgrade considerations" on page 59.
2. Log in to the existing authorization server system as a user with administrative privileges and complete the following steps:
   a. Stop all Tivoli Access Manager applications and services. For example, on Windows 2008 systems:
      1) Select **Start** > **Control Panel** > **Administrative Tools**.
      2) Double-click the **Services** icon.
      3) Stop all Tivoli Access Manager services that run on the local system, including applications, such as WebSEAL.
   b. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

      ```
      "C:\Program Files\Tivoli\Policy Director\bin\pdbackup" -action backup
      -list fullpath_to_backup_listfile
      -path path -file filename
      ```

      where:

–list *fullpath_to_backup_listfile*
Specifies the fully qualified path to the backup list file. For example:
`"C:\Program Files\Tivoli\Policy Director\etc\pdbackup.lst"`

–path *path*
Specifies the path where you want the backed up files to be stored. For example:
`"C:\Program Files\Tivoli\Policy Director\pdbackup"`

–file *filename*
Specifies a file name other than the `pdbackup.lst_date.time.dar` default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

c. Save the backup `.dar` file on another system.
Saving the backup data on a different system ensures that the archived data is not removed if you decide to uninstall the existing authorization server. Archived data is critical for restoring environments.

d. Start all Tivoli Access Manager applications and services. For example, on Windows 2008 systems:
1) Select **Start** > **Control Panel** > **Administrative Tools**.
2) Double-click the **Services** icon.
3) Start all Tivoli Access Manager services that run on the local system, including applications, such as WebSEAL.

3. On the system that will host the Security Access Manager 7.0 authorization server, complete the following steps:
a. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*®.
b. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
c. Install the Security Access Manager 7.0 authorization server as described in the *IBM Security Access Manager for Web Installation Guide*.
d. Configure the Security Access Manager 7.0 authorization server as described in the *IBM Security Access Manager for Web Installation Guide*.

Results

The backup of your previous authorization server and the setup of the Security Access Manager 7.0 authorization server on Windows is now complete.

What to do next

You can optionally re-create any previous customization on your Security Access Manager 7.0 authorization server system.

When you no longer need your previous level authorization server, unconfigure and uninstall the previous level authorization server as described in the *IBM Security Access Manager for Web Installation Guide*.

Chapter 5. Upgrading WebSEAL

Security Access Manager supports an upgrade of WebSEAL to version 7.0.

WebSEAL upgrade steps are identical for using either LDAP or Active Directory registries.

Note: You must upgrade the policy server before you upgrade WebSEAL. Upgrading only WebSEAL causes a core memory dump when it calls a routine on an old policy server.

WebSEAL: Upgrade considerations

- Upgrade the policy server before you upgrade WebSEAL.
- When WebSEAL is installed, a directory named `html.tivoli` is installed in the `pdweb` directory. The `html.tivoli` directory contains the default versions of the various files that are used in the instances, including files such as the login and error pages. These files are copied to the directories for the individual instances when the instances are created.

  When you upgrade from a previous version of WebSEAL, the files that are provided with the new version of WebSEAL are installed in the `html.tivoli` directory. New instances that are created after the upgrade use these files. Existing instances are not modified. Corresponding files of the same names as the files in the `html.tivoli` directory are not overwritten when the upgrade completes. This is by design to not overwrite any customized file.

  Review your existing files in the existing instances. Consider whether you want to modify them to incorporate the new versions of the files that are contained in the `html.tivoli` directory.
- Upgrade your operating system to the minimum supported level. For information about minimum supported levels, see *IBM Security Access Manager for Web Release Notes*.
- In Tivoli Directory Server, version 6.3 FP17, clients can coexist on the same server with a client that is version 6.0, 6.1, or 6.2. The Tivoli Directory Server 6.3 FP17 server requires that the version 6.3 client and the Java client also are installed. The server can coexist on the same server with another client that is version 6.0, 6.1, or 6.2, or with a version of the 6.3 server.
- You are not required to upgrade all Security Access Manager components in your secure domain to a 7.0 level. However, if you upgrade any Security Access Manager component on a system, all components must be upgraded on that system to the 7.0 level, and you must install Tivoli Directory Server client 6.3 FP17 on that system.

  For a list of components that are compatible with Security Access Manager, version 7.0, see the *IBM Security Access Manager for Web Release Notes*.
- If Tivoli Directory Server is your registry server and is *on a different machine* from any Security Access Manager component, you can upgrade the registry server at any time, either before or after the upgrade of the Security Access Manager 7.0 component.

  However, when the server package of Tivoli Directory Server is installed *on the same machine* as any Security Access Manager 7.0 component and if you choose to install the server package of Tivoli Directory Server 6.3 FP17, install the Tivoli

© Copyright IBM Corp. 2003, 2012

Directory Server 6.3 FP17 client and server packages at the same time as you install the Security Access Manager 7.0 component on that server.

- If there is only one WebSEAL server in your production environment, you must schedule downtime to upgrade the WebSEAL server.
- If there is a WebSEAL instance server in your production environment, follow the instructions in "AIX: Upgrading WebSEAL" on page 73 to upgrade one of the WebSEAL servers to 7.0 while the other continues to provide service.
- If you modified WebSEAL libraries, such as `libcdmf.a` or any CDAS libraries, you must back up these files to preserve your updates. To do so, manually copy the files to another location. After you install the WebSEAL 7.0 package, you can restore the backed up files before you start WebSEAL.
- During the upgrade of a WebSEAL instance to 7.0, existing symbolic links that were created during the initial configuration are retained. When you configure new WebSEAL instances with 7.0, no symbolic links are created. Before 7.0, the configuration process created symbolic links. Starting with 7.0, the configuration process no longer creates symbolic links. For consistency, consider removing symbolic links from WebSEAL instances.
- If you have applications (such as CDAS modules) that are compiled for use with earlier product versions, recompile these applications after you upgrade WebSEAL. This recompilation resolves product library changes and dependencies that can arise from new releases and operating systems. No code changes are required because full compatibility with an earlier version is maintained for the API.
- Windows systems upgrades are supported using a two system upgrade.
- **For AIX systems only**: If you plan to upgrade WebSEAL that runs on AIX, upgrade the operating system to AIX 6.1 or AIX 7.1 before you upgrade WebSEAL.
- **For Windows systems only**:
  - If you plan to upgrade WebSEAL that runs on Windows, your Windows platform must be at one of the following levels before you upgrade WebSEAL:
    - Windows 2008 x86-64 Standard, and Enterprise Edition Server
    - Windows 2008 R2 x86-64 Standard, Datacenter, and Enterprise Edition Server
  - Before you upgrade, stop all Security Access Manager services that run on the local system, including applications such as WebSEAL.

    Also, for each WebSEAL instance, change the startup type for **Security Access Manager Auto-Start Service** > **Auto Trace Runtime** > **Manual**. After upgrade, change the startup type back to **Automatic**.
  - During the upgrade process, if you receive a message that states that files are locked by a process, click **Ignore**. This message does not adversely affect the upgrade process.
- **On AIX, Linux on x86-64, Linux on System z, Solaris, and Windows systems**: Upgrade the session management server before you upgrade WebSEAL and Web Plug-in servers. See Chapter 10, "Upgrading the session management server," on page 141.
- If you use a language other than English, upgrade your language package. See the *IBM Security Access Manager for Web Installation Guide* to install the language package. When you upgrade the IBM Tivoli Directory Server language packages, use the upgrade (**-U**) option for Linux operating systems.

AIX: Upgrading WebSEAL

Upgrade WebSEAL to version 7.0 on AIX. You can also upgrade the Security Access Manager Web Security Application Development Kit (Web Security ADK) and the Security Access Manager Application Development Kit (ADK) at the same time.

About this task

You can follow these steps to complete an in-place upgrade for an existing 64-bit WebSEAL system on AIX.

Note: If you are upgrading a 32-bit environment, you cannot do an in-place upgrade. To upgrade from an existing 32-bit environment, you must complete a new WebSEAL 7.0 installation on the 64-bit server. You can then manually migrate WebSEAL instances from previous versions of WebSEAL to the new environment.

Procedure

1. Before you upgrade WebSEAL to 7.0, review the considerations in "WebSEAL: Upgrade considerations" on page 71.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.

   Note: The AIX operating system requires version 10.1 or higher of the `xlC` file set. Check your current version by using the **`lslpp`** command and upgrade, if necessary.
4. Ensure that the policy server for the secure domain is upgraded to version 7.0. For instructions, see Chapter 3, "Upgrading the policy server," on page 21.
5. Make sure that you can contact the policy server. For example, log in to the **`pdadmin`** interface and run a command:

   ```
   pdadmin -a sec_master -p password
   pdadmin sec_master> acl list
   ```

   If you cannot log in, do not proceed with the WebSEAL upgrade. Resolve the login problem before you continue. If you upgraded the policy server using two systems, step 10a on page 74 might help you resolve your login problem.
6. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
7. Stop WebSEAL and any Tivoli Access Manager service that is running on the system. To stop applications and services, use the **`pd_start`** utility:

   ```
   pdweb stop
   ```
8. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pdweb status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **`kill`** command:

   ```
   kill –9 daemon_process_id
   ```
9. Use the **`pdbackup`** utility in the `install_dir/bin` directory to back up the WebSEAL information for each WebSEAL instance, as follows:
   a. Run the following command:

      ```
      sed "s/<instance>/myInstance/g" install_dir/etc/amwebbackup.lst.template >
      /tmp/amwebbackup_myInstance.lst
      ```

This command creates a file that is called /tmp/amwebbackup_myInstance.lst and substitutes every occurrence of the string <instance> with myInstance in the file. You must use this new file in the **pdbackup** command.

b. Run the **pdbackup** utility to back up the instance information:

```
"/opt/PolicyDirector/bin/pdbackup" -action backup
-list fullpath_to_backup_listfile
-path path -file filename
```

where:

fullpath_to_backup_listfile
Specifies the fully qualified path to the backup list file. For example:

```
/tmp/amwebbackup_myInstance.lst
```

path Specifies the path where you want to store the backup files. For example:

```
/opt/Policy Director/pdbackup
```

filename
Specifies a name for the archive file.

Note: If you have more than one WebSEAL instance, make sure that you repeat this step to back up each instance.
For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

10. Do one of the following options:
    - If you upgraded the policy server on *one* system, skip to step 11.
    - If you upgraded the policy server using *two* systems, complete the following steps for each WebSEAL instance in your environment:
      a. Manually configure WebSEAL to use the new policy server. To do so, edit the webseald-*instance*.conf and pd.conf files and change the master-host entry in the [manager] stanza to the following entry:

         ```
         master-host=host_name
         ```

         where *host_name* is the fully qualified host name of the version 7.0 policy server for the domain to which WebSEAL belongs. For example:

         ```
         master-host=server1.example.ibm.com
         ```

      b. Start the WebSEAL instance server:

         ```
         pdweb start instance
         ```

      c. Examine the WebSEAL server log to verify that it does not contain any errors that indicate a communication problem with the new policy server.
      d. Stop WebSEAL:

         ```
         pdweb stop instance
         ```

11. Upgrade WebSEAL using a native installation utility, such as **installp**. Follow these steps:
    a. Install the Global Security Kit (GSKit):

       ```
       installp -acgYXd image_path/usr/sys/inst.images GSKit8.gskcrypt64.ppc.rte
       installp -acgYXd image_path/usr/sys/inst.images GSKit8.gskssl64.ppc.rte
       ```

       where *image_path*/usr/sys/inst.images is the directory where the installation images are located.
    b. Install the Tivoli Directory Server license files by running the idsLicense script in the *image_path*/usr/sys/inst.images/tdsLicense/license

directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

c. Install the client packages of Tivoli Directory Server:

```
installp -acgYXd image_path/usr/sys/inst.images packages
```

where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and *packages* are the names of the Tivoli Directory Server client packages:

License package	idsldap.license63
Client base package	idsldap.cltbase63
Client package (64-bit) (no SSL)	idsldap.clt64bit63
Client package (64-bit) (SSL)	idsldap.clt_max_crypto64bit63
Java Client package	idsldap.cltjava63

d. Ensure that your registry server is running.

e. Run the isamLicense license script by completing the following actions:

1) In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

2) Run the isamLicense script:

```
isamLicense
```

Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an exit status 0 (SUCCESS) if it is.

-? Help: Displays the syntax of the script file.

3) Read the license by pressing press **Enter** on each page to view the complete license agreement.

4) Accept the license by pressing **1**.

f. Install or upgrade the Security Access Manager license:

```
installp -acgYXd image_path/usr/sys/inst.images PD.lic
```

where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and PD.lic is the Security Access Manager license package.

g. Install or upgrade IBM Security Utilities:

```
installp -acgYXd image_path/usr/sys/inst.images TivSec.Utl
```

where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and TivSec.Utl is the IBM Security Utilities package.

h. Upgrade the Security Access Manager runtime:

```
installp -acgYXd image_path/usr/sys/inst.images PD.RTE
```

where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and PD.RTE is the Security Access Manager runtime package.

i. Ensure that Security Access Manager runtime is working, and that you can contact the policy server. For example, log in to the **pdadmin** interface and run a command:

```
pdadmin -a sec_master -p password
pdadmin sec_master> acl list
```

j. Upgrade the Security Access Manager Web Security runtime:

```
installp -acgYXd image_path/usr/sys/inst.images PDWeb.RTE
```

where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and PDWeb.Web is the Security Access Manager Web Security runtime package.

k. Upgrade Security Access Manager WebSEAL:

```
installp -acgYXd image_path/usr/sys/inst.images PDWeb.Web
```

where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and PDWeb.Web is the Security Access Manager WebSEAL package.

12. If you modified WebSEAL libraries, such as libcdmf.a or any CDAS libraries and if you manually copied the files to another location to preserve your updates before upgrade, after you install the WebSEAL 7.0 package, then move back the copied files before you start WebSEAL.
13. Upgrade WebSEAL instances.
    a. For the WebSEAL instance server, start the server manually in the foreground. This command causes WebSEAL to migrate the configuration files.

    ```
    /opt/pdweb/bin/webseald -config etc/webseald-instance.conf -foreground
    ```

    Where *instance* is the name of the instance you want to upgrade.

    Note: Ignore any messages that are displayed. The messages are not errors. For example, you might encounter stanza messages.

    b. Confirm that the WebSEAL instance server started successfully. To do so, use a browser to access the WebSEAL URL (https://*instance_servername*) and log in to WebSEAL.

    Note: The splash screen might still display a previous version number. This issue is a known limitation and can be ignored.

    c. Press the **Ctrl+C** keys to stop the WebSEAL (webseald) process that runs in the foreground.

    d. Start the WebSEAL instance server:

    ```
    pdweb start instance
    ```

    e. Repeat these steps for each instance.

    The upgrade of WebSEAL on AIX is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.
14. Optional: To upgrade the Security Access Manager Web Security Application Development Kit (Web Security ADK) on your WebSEAL system, enter:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.AuthADK PDWeb.ADK
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located, PD.AuthADK is the Security Access Manager Application

Development Kit (Security Access Manager ADK), and `PDWeb.ADK` is the Security Access Manager Web Security Application Development Kit package.

Note: The Web Security ADK has a dependency on the Security Access Manager ADK component. Both ADK packages are included on the *IBM Security Access Manager Web Security for AIX* DVD.

Results

You do not need to run **pdconfig** to configure components. Your custom configuration settings in the WebSEAL configuration files are preserved and automatically updated with version 7.0 stanzas and parameters.

Linux on x86-64: Upgrading WebSEAL

Upgrade WebSEAL to version 7.0 on Linux x86-64. You can also upgrade the Security Access Manager Web Security Application Development Kit (Web Security ADK) and the Security Access Manager Application Development Kit (ADK) at the same time.

About this task

You can follow these steps to complete an in-place upgrade for an existing 64-bit WebSEAL system for Linux on x86-64.

Note: If you are upgrading a 32-bit environment, you cannot do an in-place upgrade. To upgrade from an existing 32-bit environment, you must complete a new WebSEAL 7.0 installation on the 64-bit server. You can then manually migrate WebSEAL instances from previous versions of WebSEAL to the new environment.

Procedure

1. Before you upgrade WebSEAL to 7.0, review the considerations in "WebSEAL: Upgrade considerations" on page 71.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Ensure that the policy server for the secure domain is upgraded to version 7.0. For instructions, see Chapter 3, "Upgrading the policy server," on page 21.
5. Make sure that you can contact the policy server. For example, log in to the **pdadmin** interface and run a command:

   ```
   pdadmin -a sec_master -p password
   pdadmin sec_master> acl list
   ```

   If you cannot log in, do not proceed with the WebSEAL upgrade. Resolve the login problem before you continue. If you upgraded the policy server using two systems, step 10a on page 78 might help you resolve your login problem.
6. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
7. Change to the following directory:

   ```
   cd image_path/linux_x86
   ```

   where *image_path*`/linux_x86` is the location of the installation images.

8. Stop WebSEAL and any Tivoli Access Manager service that is running on the system. To stop applications and services, use the **pdweb** utility:

   ```
   pdweb stop
   ```

9. Use the **pdbackup** utility in the `install_dir/bin` directory to back up the WebSEAL information for each WebSEAL instance, as follows:

   a. Run the following command:

      ```
      sed "s/<instance>/myInstance/g" install_dir/etc/amwebbackup.lst.template >
      /tmp/amwebbackup_myInstance.lst
      ```

      This command creates a file that is called `/tmp/amwebbackup_myInstance.lst` and substitutes every occurrence of the string `<instance>` with `myInstance` in the file. You must use this new file in the **pdbackup** command.

   b. Run the **pdbackup** utility to back up the instance information:

      ```
      "/opt/PolicyDirector/bin/pdbackup" -action backup
      -list fullpath_to_backup_listfile
      -path path -file filename
      ```

      where:

      fullpath_to_backup_listfile
      Specifies the fully qualified path to the backup list file. For example:

      ```
      /tmp/amwebbackup_myInstance.lst
      ```

      path Specifies the path where you want to store the backup files. For example:

      ```
      /opt/Policy Director/pdbackup
      ```

      filename
      Specifies a name for the archive file.

   Note: If you have more than one WebSEAL instance, make sure that you repeat this step to back up each instance.
   For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

10. Do one of the following tasks:
    - If you upgraded the policy server on *one* system, skip to step 11 on page 79.
    - If you upgraded the policy server using *two* systems, complete the following steps for each WebSEAL instance in your environment:

      a. Manually configure WebSEAL to use the new policy server. To do so, edit the `webseald-instance.conf` and `pd.conf` files and change the `master-host` entry in the `[manager]` stanza to the following options:

         ```
         master-host=host_name
         ```

         where *host_name* is the fully qualified host name of the version 7.0 policy server for the domain to which WebSEAL belongs. For example:

         ```
         master-host=server1.example.ibm.com
         ```

         For the location of the `webseald-instance.conf` file, see the WebSEAL configuration file section of the *IBM Security Access Manager for Web WebSEAL Administration Guide*.

      b. Start the WebSEAL instance server:

         ```
         pdweb start instance
         ```

c. Examine the WebSEAL server log to verify that it does not contain any errors that indicate a communication problem with the new policy server.

d. Stop WebSEAL:

```
pdweb stop instance
```

11. Upgrade WebSEAL using a native installation utility, such as **rpm**. Follow these steps:

a. Install the IBM Global Security Kit (GSKit).

```
rpm -i gskcrypt64-8.0.14.26.linux.x86_64.rpm
rpm -i gskssl64-8.0.14.26.linux.x86_64.rpm
```

b. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_x86/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

c. Install the Tivoli Directory Server client packages:

```
rpm -i packages
```

where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.x86_64.rpm`
Base client package	`idsldap-cltbase63-6.3.0-17.x86_64.rpm`
64-bit client package	`idsldap-clt64bit63-6.3.0-17.x86_64.rpm`
Java client package	`idsldap-cltjava63-6.3.0-17.x86_64.rpm`

d. Ensure that your registry server is running.

e. Run the `isamLicense` license script by completing the following actions:

1) In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

2) Run the `isamLicense` script:

```
isamLicense
```

Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

-? Help: Displays the syntax of the script file.

3) Read the license by pressing press **Enter** on each page to view the complete license agreement.

4) Accept the license by pressing **1**.

f. Upgrade the Security Access Manager license

```
rpm -U PDlic-PD-7.0.0-0.x86_64.rpm
```

g. Upgrade the IBM Security Utilities:

```
rpm -u TivSecUtl-TivSec-7.0.0-0.x86_64.rpm
```

h. Upgrade the Security Access Manager runtime:

```
rpm -U PDRTE-PD-7.0.0-0.x86_64.rpm
```

i. Ensure that the Security Access Manager runtime is working, and that you can contact the policy server. For example, log in to the **pdadmin** interface and run a command:

```
pdadmin -a sec_master -p password
pdadmin sec_master> acl list
```

j. Upgrade the Security Access Manager Web Security runtime:

```
rpm -U PDWebRTE-PD-7.0.0-0.x86_64.rpm
```

k. Upgrade Security Access Manager WebSEAL:

```
rpm -U PDWeb-PD-7.0.0-0.x86_64.rpm
```

12. If you modified WebSEAL libraries, such as `libcdmf.so` or any CDAS libraries and if you manually copied the files to another location to preserve your updates before upgrade, after you install the WebSEAL 7.0 package, then move back the copied files before you start WebSEAL.
13. Upgrade WebSEAL instance servers:
    a. For the WebSEAL instance server, start the server manually in the foreground. This command causes WebSEAL to migrate the configuration files.

    ```
    /opt/pdweb/bin/webseald -config etc/webseald-instance.conf -foreground
    ```

    where *instance* is the name of the instance you must configure.

    Note: Ignore any messages that are displayed. These messages are not errors. For example, you might encounter stanza messages.

    b. Confirm that WebSEAL instance server started successfully. To do so, use a browser to access the WebSEAL URL (`https://instance_servername`) and log in to WebSEAL.

    Note: The splash screen that displays might show a previous version number. This response is a known limitation and can be ignored.

    c. Press the **Ctrl+C** keys to stop the WebSEAL (`webseald`) process that runs in the foreground.
    d. Start the WebSEAL instance server:

    ```
    pdweb start instance
    ```

    e. Repeat these steps for each instance.

    The upgrade of WebSEAL for Linux on x86-64 is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.
14. Optional: To upgrade the Web Security Application Development Kit (Web Security ADK) on your version 7.0 WebSEAL system, enter:

    ```
    rpm -U PDADK-PD-7.0.0-0.x86_64.rpm PDWebADK-PD-7.0.0-0.x86_64.rpm
    ```

    Note: The Web Security Application Development Kit has a dependency on the Security Access Manager Application Development Kit component. Both Application Development Kit packages are included on the *IBM Security Access Manager Web Security for Linux on x86_64* DVD.

Results

You do not need to run **pdconfig** to configure components. Your custom configuration settings in the WebSEAL configuration files are preserved and automatically updated with version 7.0 stanzas and parameters.

Linux on System z: Upgrading WebSEAL

Upgrade WebSEAL for Linux on System z to version 7.0. You can also upgrade the Security Access Manager Web Security Application Development Kit (Web Security ADK) and the Security Access Manager Application Development Kit (ADK) at the same time.

About this task

You can follow these steps to complete an in-place upgrade for an existing 64-bit WebSEAL system on System z.

Note: If you are upgrading a 32-bit environment, you cannot do an in-place upgrade. To upgrade from an existing 32-bit environment, you must complete a new WebSEAL 7.0 installation on the 64-bit server. You can then manually migrate WebSEAL instances from previous versions of WebSEAL to the new environment.

Procedure

1. Before you upgrade WebSEAL to 7.0, review the considerations in "WebSEAL: Upgrade considerations" on page 71.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Ensure that the policy server for the secure domain is upgraded to version 7.0. For instructions, see Chapter 3, "Upgrading the policy server," on page 21.
5. Make sure that you can contact the policy server. For example, log in to the **pdadmin** interface and run a command:

   ```
   pdadmin -a sec_master -p password
   pdadmin sec_master> acl list
   ```

   If you cannot log in, do not proceed with the WebSEAL upgrade. Resolve the login problem before you continue. If you upgraded the policy server using two systems, step 10a on page 82 might help you resolve your login problem.
6. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage on the System z system.
7. Change to the following directory:

   ```
   cd image_path/linux_s390
   ```

   Where *image_path* is where the installation images are located.
8. Stop WebSEAL and any Tivoli Access Manager service that is running on the system. To stop applications and services, use the **pdweb** utility:

   ```
   pdweb stop
   ```
9. Use the **pdbackup** utility in the *install_dir*`/bin` directory to back up the WebSEAL information for each WebSEAL instance, as follows:
   a. Run the following command:

      ```
      sed "s/<instance>/myInstance/g" install_dir/etc/amwebbackup.lst.template >
      /tmp/amwebbackup_myInstance.lst
      ```

      where:

      install_dir
      The WebSEAL runtime installation directory.

This command creates a file that is called /tmp/amwebbackup_myInstance.lst and substitutes every occurrence of the string <instance> with myInstance in the file. You must use this new file in the **pdbackup** command.

b. Run the **pdbackup** utility to back up the instance information:

```
"/opt/PolicyDirector/bin/pdbackup" -action backup
-list fullpath_to_backup_listfile
-path path -file filename
```

where:

fullpath_to_backup_listfile
Specifies the fully qualified path to the backup list file. For example:

```
/tmp/amwebbackup_myInstance.lst
```

path Specifies the path where you want to store the backup files. For example:

```
/opt/Policy Director/pdbackup
```

filename
Specifies a name for the archive file.

Note: If you have more than one WebSEAL instance, make sure that you repeat this step for each instance.
For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

10. Do one of the following tasks
    - If you upgraded the policy server on *one* system, skip to step 11.
    - If you upgraded the policy server using *two* systems, complete the following steps for each WebSEAL instance in your environment:
      a. Manually configure WebSEAL to use the new policy server. To do so, edit the webseald-*instance*.conf (such as webseald-default.conf) and pd.conf files and change the master-host entry in the [manager] stanza to the following options:

         ```
         master-host=host_name
         ```

         where *host_name* is the fully qualified host name of the version 7.0 policy server for the domain to which WebSEAL belongs. For example:

         ```
         master-host=server1.example.ibm.com
         ```

      b. Start the WebSEAL instance server:

         ```
         pdweb start instance
         ```

      c. Examine the WebSEAL server log to verify that it does not contain any errors that indicate a communication problem with the new policy server.

      d. Stop WebSEAL:

         ```
         pdweb stop instance
         ```

11. Upgrade WebSEAL with a native installation utility, such as **rpm**. Follow these steps:
    a. Install IBM Global Security Kit (GSKit).

       ```
       rpm -i gskcrypt64-8.0.14.26.linux.s390x.rpm
       rpm -i gskssl64-8.0.14.26.linux.s390x.rpm
       ```

b. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_s390/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

c. Install the client packages of Tivoli Directory Server:

```
rpm -i packages
```

where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.s390.rpm`
Base client package	`idsldap-cltbase63-6.3.0-17.s390.rpm`
64-bit client package	`idsldap-clt64bit63-6.3.0-17.s390.rpm`
Java client package	`idsldap-cltjava63-6.3.0-17.s390x.rpm`

d. Ensure that your registry server is running.

e. Run the `isamLicense` license script by completing the following actions:

1) In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

2) Run the `isamLicense` script:

```
isamLicense
```

Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

-? Help: Displays the syntax of the script file.

3) Read the license by pressing press **Enter** on each page to view the complete license agreement.

4) Accept the license by pressing **1**.

f. Upgrade the Security Access Manager license:

```
rpm -U PDlic-PD-7.0.0-0.s390x.rpm
```

g. Upgrade the IBM Security Utilities

```
rpm -U TivSecUtl-TivSec-7.0.0-0.s390x.rpm
```

h. Upgrade the Security Access Manager runtime:

```
rpm -U PDRTE-PD-7.0.0-0.s390x.rpm
```

i. Ensure that the Security Access Manager runtime is working, and that you can contact the policy server. For example, log in to the **pdadmin** interface and run a command:

```
pdadmin -a sec_master -p packages
pdadmin sec_master> acl list
```

j. Upgrade the Security Access Manager Web Security runtime:

```
rpm -U PDWebRTE-PD-7.0.0-0.s390x.rpm
```

k. Upgrade Security Access Manager WebSEAL:

```
rpm -U PDWeb-PD-7.0.0-0.s390x.rpm
```

12. If you modified WebSEAL libraries, such as `libcdmf.so` or any CDAS libraries and if you manually copied the files to another location to preserve your updates before upgrade, after you install the WebSEAL 7.0 package, then move back the copied files before you start WebSEAL.
13. Upgrade each WebSEAL instance server:
    a. For each WebSEAL instance server, start the server manually in the foreground. This command causes WebSEAL to migrate the configuration files.

       ```
       /opt/pdweb/bin/webseald -config etc/webseald-instance.conf -foreground
       ```

       where *instance* is the name of the instance you need to configure.

       Note: Ignore any messages that are displayed. These messages are not errors. For example, you might encounter stanza messages.
    b. Confirm that WebSEAL instance server started successfully. To do so, use a browser to access the WebSEAL URL (`https://instance_servername`) and log in to WebSEAL.

       Note: The splash screen that displays might still show a previous version number. This issue is a known limitation and can be ignored.
    c. Press the **Ctrl** > **C** keys to stop the WebSEAL (`webseald`) process that runs in the foreground.
    d. Start the WebSEAL instance server:

       ```
       pdweb start instance
       ```
    e. Repeat these steps for each instance.

    The upgrade of WebSEAL for Linux on System z is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.
14. Optional: To upgrade the Web Security Application Development Kit (Web Security ADK) on your version 7.0 WebSEAL system, enter the following command:

    ```
    rpm -U PDAuthADK-PD-7.0.0-0.s390x.rpm PDWebADK-PD-7.0.0-0.s390x.rpm
    ```

    where `PDAuthADK` is the Security Access Manager Application Development Kit (Access Manager ADK), and `PDWebADK` is the Web Security Application Development Kit package.

    Note: The Web Security ADK has a dependency on the Security Access Manager ADK component. Both ADK packages are included on the *IBM Security Access Manager Web Security for Linux on System z* installation image.

Results

You do not need to run **pdconfig** to configure components. Your custom configuration settings in the WebSEAL configuration files are preserved and automatically updated with version 7.0 stanzas and parameters.

Solaris: Upgrading WebSEAL

Upgrade WebSEAL on Solaris to version 7.0. You can also upgrade the Security Access Manager Web Security Application Development Kit (Web Security ADK) and the Security Access Manager Application Development Kit (ADK) at the same time.

About this task

You can follow these steps to complete an in-place upgrade for an existing 64-bit WebSEAL system on Solaris.

Note: If you are upgrading a 32-bit environment, you cannot do an in-place upgrade. To upgrade from an existing 32-bit environment, you must complete a new WebSEAL 7.0 installation on the 64-bit server. You can then manually migrate WebSEAL instances from previous versions of WebSEAL to the new environment.

Procedure

1. Before you upgrade WebSEAL to 7.0, review the considerations in "WebSEAL: Upgrade considerations" on page 71.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Ensure that the policy server for the secure domain is upgraded to version 7.0. For instructions, see Chapter 3, "Upgrading the policy server," on page 21.
5. Make sure that you can contact the policy server. For example, log in to the **pdadmin** interface and run a command:

   ```
   pdadmin -a sec_master -p password
   pdadmin sec_master> acl list
   ```

   If you cannot log in, do not proceed with the WebSEAL upgrade. Resolve the login problem before you continue. If you upgraded the policy server using two systems, step 9a on page 86 might help you resolve your login problem.
6. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
7. Stop WebSEAL and any Tivoli Access Manager service that is running on the system. To stop applications and services, use the **pd_start** utility:

   ```
   pdweb stop
   ```

8. Use the **pdbackup** utility in the `install_dir/bin` directory to back up the WebSEAL information for each WebSEAL instance, as follows:
   a. Run the following command:

      ```
      sed "s/<instance>/myInstance/g" install_dir/etc/amwebbackup.lst.template >
      /tmp/amwebbackup_myInstance.lst
      ```

      This command creates a file that is called `/tmp/amwebbackup_myInstance.lst` and substitutes every occurrence of the string `<instance>` with `myInstance` in the file. You must use this new file in the **pdbackup** command.
   b. Run the **pdbackup** utility to back up the instance information:

      ```
      "/opt/PolicyDirector/bin/pdbackup" -action backup
      -list fullpath_to_backup_listfile
      -path path -file filename
      ```

      where:

      fullpath_to_backup_listfile
      Specifies the fully qualified path to the backup list file. For example:

      ```
      /tmp/amwebbackup_myInstance.lst
      ```

path Specifies the path where you want to store the backup files. For example:

```
/opt/Policy Director/pdbackup
```

filename
Specifies a name for the archive file.

Note: If you have more than one WebSEAL instance, make sure that you repeat this step to back up each instance.
For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

9. Do one of the following
   - If you upgraded the policy server on *one* system, skip to step 10.
   - If you upgraded the policy server using *two* systems, complete the following steps for each WebSEAL instance in your environment:
     a. Manually configure WebSEAL to use the new policy server. To do so, edit the `webseald-instance.conf` and `pd.conf` files and change the `master-host` entry in the `[manager]` stanza to the following options:

        ```
        master-host=host_name
        ```

        where *host_name* is the fully qualified host name of the version 7.0 policy server for the domain to which WebSEAL belongs. For example:

        ```
        master-host=server1.example.ibm.com
        ```

     b. Start the WebSEAL instance server:

        ```
        pdweb start instance
        ```

     c. Examine the WebSEAL server log to verify that it does not contain any errors that indicate a communication problem with the new policy server.
     d. Stop WebSEAL:

        ```
        pdweb stop instance
        ```

10. Upgrade WebSEAL with a command-line installation utility, such as **pkgadd**. Follow these steps:
    a. Change to the `/image_path/solaris` directory.
    b. Install the Global Security Kit (GSKit):

       ```
       pkgadd -d /image_path/solaris
       -a /image_path/solaris/pddefault -G gsk8cry64
       -a /image_path/solaris/pddefault -G gsk8ssl64
       ```

       where `/image_path/solaris` specifies the location of the installation images, and `/image_path/solaris/pddefault` specifies the location of the installation administration script. The `-G` option ensures that the package is added in the current zone only.

       Note: During installation, you are asked if you want to use `/opt` as the `root` directory. If space permits, use `/opt` as the `root` installation directory. To accept `/opt` as the `root` directory, press **Enter**.

    c. Install the Tivoli Directory Server license files by running the `idsLicense` script in the `image_path/solaris/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    d. Install the Tivoli Directory Server client packages:

       ```
       pkgadd -d /image_path/solaris/packages
       -a /image_path/solaris/pddefault
       ```

where /*image_path*/solaris specifies the location of the package, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and *packages* are as follows:

License package	idsldap.license63.pkg
Base client package	idsldap.cltbase63.pkg
64-bit client package	idsldap.clt64bit63.pkg
Java client package	idsldap.cltjava63.pkg

e. Ensure that your registry server is running.

f. Run the isamLicense license script by completing the following actions:

1) In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

2) Run the isamLicense script:

```
isamLicense
```

Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an exit status 0 (SUCCESS) if it is.

-? Help: Displays the syntax of the script file.

3) Read the license by pressing press **Enter** on each page to view the complete license agree

4) Accept the license by pressing **1**.

g. Upgrade the Security Access Manager license:

```
pkgadd -d /image_path/solaris
-a /image_path/solaris/pddefault -G PDlic
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDlic is the Security Access Manager license package. The -G option ensures that the package is added in the current zone only.

h. Install or upgrade IBM Security Utilities:

```
pkgadd -d /image_path/solaris
-a /image_path/solaris/pddefault -G TivSecUtl
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and TivSecUtl is the IBM Security Utilities package. The -G option ensures that the package is added in the current zone only.

i. Upgrade the Security Access Manager runtime:

```
pkgadd -d /image_path/solaris
-a /image_path/solaris/pddefault -G PDRTE
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDRTE is the IBM Security Utilities package. The -G option ensures that the package is added in the current zone only.

j. Ensure that Security Access Manager runtime is working, and that you can contact the policy server. For example, log in to the **pdadmin** interface and run a command:

```
pdadmin -a sec_master -p password
pdadmin sec_master> acl list
```

k. Upgrade Security Access Manager Web Security Runtime:

```
pkgadd -d /image_path/solaris
-a /image_path/solaris/pddefault -G PDWebRTE
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDWebRTE is the Security Access Manager Web Security runtime package. The -G option ensures that the package is added in the current zone only.

l. Upgrade Security Access Manager WebSEAL:

```
pkgadd -d /image_path/solaris
-a /image_path/solaris/pddefault -G PDWeb
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDWeb is the Security Access Manager WebSEAL package. The -G option ensures that the package is added in the current zone only.

11. If you modified WebSEAL libraries, such as libcdmf.so or any CDAS libraries and if you manually copied the files to another location to preserve your updates before upgrade, after you install the WebSEAL 7.0 package, then move back the copied files before you start WebSEAL.
12. Upgrade each WebSEAL instance server:
    a. For the WebSEAL instance server, start the server manually in the foreground. This command causes WebSEAL to migrate the configuration files.

    ```
    /opt/pdweb/bin/webseald -config etc/webseald-instance.conf -foreground
    ```

    where *instance* is the name of the instance you need to configure.

    Note: Ignore any messages that display. These messages are not errors. For example, you might encounter stanza messages.

    b. Confirm that WebSEAL instance server started successfully. To do so, use a browser to access the WebSEAL URL (https://*instance_servername*) and log in to WebSEAL.

    Note: The splash screen that displays might show a previous version number. This issue is a known limitation and can be ignored.

    c. Press the **Ctrl** > **C** keys to stop the WebSEAL (webseald) process that runs in the foreground.
    d. Start the WebSEAL instance server:

    ```
    pdweb start instance
    ```

    e. Repeat these steps for each instance.

The upgrade of WebSEAL on Solaris is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

13. Optional: To upgrade the Security Access Manager Web Security Application Development Kit (Web Security ADK) on your version 7.0 WebSEAL system, enter:

    ```
    pkgadd -d /image_path/solaris
    -a /image_path/solaris/pddefault -G PDAuthADK PDWebADK
    ```

    where `/image_path/solaris` specifies the location of the installation images, `/image_path/solaris/pddefault` specifies the location of the installation administration script, `PDauthADK` is the Security Access Manager Application Development Kit (Access Manager ADK) package, and `PDWebADK` is the Security Access Manager Web Security ADK package. The `-G` option ensures that the package is added in the current zone only.

    Note: The Web Security ADK has a dependency on the Security Access Manager ADK component. Both ADK packages are included in the product installation image.

Results

You do not need to run **pdconfig** to configure components. Your custom configuration settings in the WebSEAL configuration files are preserved and automatically updated with version 7.0 stanzas and parameters.

Windows: Upgrading WebSEAL

Upgrade WebSEAL on Windows to version 7.0. You can upgrade the Security Access Manager Web Security Application Development Kit (Web Security ADK) and the Security Access Manager Application Development Kit (ADK) at the same time.

About this task

There is no automated upgrade process for existing WebSEAL systems on Windows. This procedure describes how to manually upgrade to a new WebSEAL version 7.0 system.

Note: Windows upgrades are supported on a two-system upgrade approach only.

Procedure

1. Before you upgrade WebSEAL to 7.0, review the considerations in "WebSEAL: Upgrade considerations" on page 71.
2. On the new system for version 7.0, log in as a user with administrator privileges.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Ensure that the policy server for the secure domain is upgraded to version 7.0. For instructions, see Chapter 3, "Upgrading the policy server," on page 21.
5. On the system that is to host WebSEAL version 7.0, complete the following steps to install the 7.0 WebSEAL server:
   a. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

b. Install Global Security Kit (GSKit) by changing to the `\windows\GSKit` directory of the installation image and enter:

   ```
   gsk8ssl64
   ```

   Follow the online instructions to complete the installation.

c. **LDAP server registries only:** If you use an LDAP server as your registry, install the Tivoli Directory Server client by completing the following steps:

   1) Run the **install_tds.exe** script in the `windows\tds_client64` directory.
   2) Select to install **C Client 6.3** and **Java Client 6.3**.
   3) Follow the online instructions to complete the installation.

   Note: If you use Active Directory as your registry, and the Security Access Manager systems in your domain are Windows based, the Tivoli Directory Server client is not required.

d. Upgrade the security utilities by running the **setup.exe** script in the `\windows\TivSecUtl\Disk Images\Disk1` directory. Select to install **IBM Security Utilities**, and follow the online instructions to complete the installation.

e. Install components by running the **setup.exe** file in the `\windows\PolicyDirector\Disk Images\Disk1` directory. Select to install the following components in this sequence:

   - **Security Access Manager license**
   - **Security Access Manager runtime**
   - **Security Access Manager Web Security runtime**
   - **Security Access Manager WebSEAL**

   Follow the online instructions to complete the installation.

f. Configure the Web Security runtime environment.

g. Create and configure the WebSEAL instances for your environment. You can manually migrate WebSEAL instances from previous versions of WebSEAL. For each instance from a previous version, create a WebSEAL instance in the WebSEAL version 7.0 environment and then re-create the configuration of the legacy instance. This configuration includes the junction definitions and WebSEAL configuration files.

h. Ensure that Security Access Manager runtime is working, and that you can contact the 7.0 policy server. For example, log in to the **pdadmin** interface and run a command:

   ```
   pdadmin -a sec_master -p password
   pdadmin sec_master> acl list
   ```

6. Optional: To upgrade the Web Security Application Development Kit (Web Security ADK) on your version 7.0 WebSEAL system, run the **setup.exe** file in the `\windows\PolicyDirector\Disk Images\Disk1` directory. Select to install the **Security Access Manager Application Development Kit** followed by the **Web Security Application Development Kit**. Follow the online instructions to complete the installation.

   Note: The Web Security ADK has a dependency on the Security Access Manager ADK component. Both ADK packages are included in the product installation image.

Results

WebSEAL version 7.0 is installed and configured on the new server.

Chapter 6. Upgrading the runtime

Security Access Manager supports an upgrade of Security Access Manager runtime system to version 7.0.

Security Access Manager Runtime: Upgrade considerations

Before you upgrade Security Access Manager runtime to 7.0, review the following considerations:

- Upgrade your operating system to the minimum supported level. For information about minimum supported levels, see *IBM Security Access Manager for Web Release Notes*.
- In Tivoli Directory Server, version 6.3 FP17, clients can coexist on the same workstation with a client that is version 6.0, 6.1, and 6.2. The Tivoli Directory Server, version 6.3 FP17, server requires that the version 6.3 client and the Java client are also installed. In addition, the server can coexist on the same workstation with another client that is version 6.3, or with a version of the 6.3 server.
- You are not required to upgrade all Security Access Manager components in your secure domain to a 7.0 level. However, if you upgrade any Security Access Manager component on a system, all components must be upgraded on that system to the 7.0 level, and you must install Tivoli Directory Server client 6.3 FP17 on that system.

  For a list of components that are compatible with Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.
- If Tivoli Directory Server is your registry server and is *on a different machine* from any Security Access Manager component, you can upgrade the registry server at any time, either before or after the upgrade of the Security Access Manager 7.0 component.

  However, when the server package of Tivoli Directory Server is installed *on the same machine* as any Security Access Manager 7.0 component and if you choose to install the server package of Tivoli Directory Server 6.3 FP17, install the Tivoli Directory Server 6.3 FP17 client and server packages at the same time as you install the Security Access Manager 7.0 component on that machine.
- Windows systems upgrades are supported using a two system upgrade.
- If you use a language other than English, upgrade your language package. See the *IBM Security Access Manager for Web Installation Guide* to install the language package. When you upgrade the IBM Tivoli Directory Server language packages, use the upgrade (**-U**) option for Linux operating systems.

AIX: Upgrading the runtime

Upgrade your existing runtime to the Security Access Manager, version 7.0, on AIX.

Procedure

1. Before you upgrade the runtime to 7.0, review the considerations in "Security Access Manager Runtime: Upgrade considerations."
2. Log in as `root`.

© Copyright IBM Corp. 2003, 2012

3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.

   Note: The AIX operating system requires version 10.1 or later of the `xlC` file set. Check your current version by using the **lslpp** command and upgrade, if necessary.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```
6. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
7. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   /opt/PolicyDirector/etc/pdbackup.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

   For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.
8. Install the Global Security Kit (GSKit):

   ```
   installp -acgYXd image_path/usr/sys/inst.images GSKit8.gskcrypt64.ppc.rte
   installp -acgYXd image_path/usr/sys/inst.images GSKit8.gskssl64.ppc.rte
   ```

   where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located.
9. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/usr/sys/inst.images/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
10. Install the client packages of Tivoli Directory Server:

    ```
    installp -acgYXd image_path/usr/sys/inst.images packages
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located, and where *packages* are the names of the Tivoli Directory Server client packages:

License package	`idsldap.license63`
Client base package	`idsldap.cltbase63`

Client package (64-bit) (no SSL)	idsldap.clt64bit63
Client package (64-bit) (SSL)	idsldap.clt_max_crypto64bit63
Client package (64-bit) (SSL)	idsldap.cltjava63

11. Ensure that your registry server is running.
12. Run the isamLicense license script by completing the following actions:
    a. In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the isamLicense script:

       ```
       isamLicense
       ```

       Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

       -t Test: Silently tests whether the current license is already installed. Returns an exit status 0 (SUCCESS) if it is.

       -? Help: Displays the syntax of the script file.
    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
13. Upgrade the Security Access Manager license:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.lic
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and PD.lic is the Security Access Manager license package.
14. Upgrade IBM Security Utilities:

    ```
    installp -acgYXd image_path/usr/sys/inst.images TivSec.Utl
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and TivSec.Utl is the IBM Security Utilities package.
15. Upgrade Security Access Manager runtime:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.RTE
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and PD.RTE is the Security Access Manager runtime package.
16. If the two-system upgrade option was used for the policy server, the master-host record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.
    Edit the master-host entry in the following Security Access Manager runtime configuration file: /opt/PolicyDirector/etc/pd.conf
17. Verify that you can contact the upgraded 7.0 policy server. For example, log on to the **pdadmin** interface and run a command:

```
pdadmin -a sec_master -p password
pdadmin sec_master> acl list
```

Results

The upgrade of an Security Access Manager runtime system on AIX is now complete.

Linux on x86-64: Upgrading the runtime

Upgrade your existing runtime to the Security Access Manager, version 7.0, on Linux x86-64.

Procedure

1. Before you upgrade the runtime to 7.0, review the considerations in "Security Access Manager Runtime: Upgrade considerations" on page 91.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Change to the following directory:

   ```
   cd image_path/linux_x86
   ```

   where *image_path* is where the installation images are located.
6. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```
7. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
8. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   /opt/PolicyDirector/etc/pdbackup.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

   For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

9. UpgradeIBM Global Security Kit (GSKit):

   ```
   rpm -U gskcrypt64-8.0.14.26.linux.x86_64.rpm
   rpm -U gskssl64-8.0.14.26.linux.x86_64.rpm
   ```

10. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_x86/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
11. Install the client packages of Tivoli Directory Server:

    ```
    rpm -i packages
    ```

    where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.x86_64.rpm`
Base client package	`rpm -i idsldap-cltbase63-6.3.0-17.x86_64.rpm`
64-bit client package	`rpm -i idsldap-clt64bit63-6.3.0-17.x86_64.rpm`
Java client package	`rpm -i idsldap-cltjava63-6.3.0-17.x86_64.rpm`

12. Ensure that your registry server is running.
13. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:

       ```
       isamLicense
       ```

       Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

       -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

       -? Help: Displays the syntax of the script file.

    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
14. Upgrade the Security Access Manager license:

    ```
    rpm -U PDlic-PD-7.0.0-0.x86_64.rpm
    ```

15. Upgrade IBM Security Utilities

    ```
    rpm -U TivSecUtl-TivSec-7.0.0-0.x86_64.rpm
    ```

16. Upgrade Security Access Manager runtime:

    ```
    rpm -U PDRTE-PD-7.0.0-0.x86_64.rpm
    ```

17. If the two-system upgrade option was used for the policy server, the `master-host` record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

Edit the `master-host` entry in the following Security Access Manager Runtime configuration file: `/opt/PolicyDirector/etc/pd.conf`

18. Verify that you can contact the upgraded 7.0 policy server. For example, log on to the **pdadmin** interface and run a command:

```
pdadmin -a sec_master -p password
pdadmin sec_master> acl list
```

Results

The upgrade of an Security Access Manager runtime system for Linux on x86_64 is now complete.

Linux on System z: Upgrading the runtime

Upgrade your existing runtime to the Security Access Manager, version 7.0, on Linux on System z.

Procedure

1. Before you upgrade the runtime to 7.0, review the considerations in "Security Access Manager Runtime: Upgrade considerations" on page 91.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage on the System z system.
5. Change to the following directory:

   ```
   cd image_path/linux_s390
   ```

   where *image_path* is the location of the installation images. The `.rpm` files are in the `/image_path/linux_s390` directory.
6. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```
7. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
8. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   /opt/PolicyDirector/etc/pdbackup.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

–file *filename*

Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

9. Upgrade IBM Global Security Kit (GSKit):

```
rpm -U gskcrypt64-8.0.14.26.linux.s390x.rpm
rpm -U gsksslx64-8.0.14.26.linux.s390x.rpm
```

10. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_s390/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
11. Install the client packages of Tivoli Directory Server:

```
rpm -i packages
```

where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.s390.rpm`
Base client package	`idsldap-cltbase63-6.3.0-17.s390.rpm`
64-bit client package	`idsldap-clt64bit63-6.3.0-17.s390.rpm`
Java client package	`idsldap-cltjava63-6.3.0-17.s390x.rpm`

12. Ensure that your registry server is running.
13. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:

```
isamLicense
```

Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

-? Help: Displays the syntax of the script file.

    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
14. Upgrade the Security Access Manager license

```
rpm -U PDlic-PD-7.0.0-0.s390x.rpm
```

15. Upgrade IBM Security Utilities

```
rpm -U TivSecUtl-TivSec-7.0.0-0.s390x.rpm
```

16. Upgrade the Security Access Manager runtime:

```
rpm -U PDRTE-PD-7.0.0-0.s390x.rpm
```

17. If the two-system upgrade option was used for the policy server, the `master-host` record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.
    Edit the `master-host` entry in the following the Security Access Manager runtime configuration file: `/opt/PolicyServer/etc/pd.conf`
18. Verify that you can contact the upgraded 7.0 policy server. For example, log on to the **pdadmin** interface and run a command:

    ```
    pdadmin -a sec_master -p password
    pdadmin sec_master> acl list
    ```

Results

The upgrade of a Security Access Manager runtime system for Linux on System z is now complete.

Solaris: Upgrading the runtime

Upgrade your existing runtime to Security Access Manager, version 7.0, on Solaris.

Procedure

1. Before you upgrade the runtime to 7.0, review the considerations in "Security Access Manager Runtime: Upgrade considerations" on page 91.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```
6. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
7. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:
   `/opt/PolicyDirector/etc/pdbackup.lst`

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:
   `/var/PolicyDirector/pdbackup`

–file *filename*
Specifies a file name other than the pdbackup.lst_*date.time*.tar default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

8. Install the Global Security Kit (GSKit):

```
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8cry64
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8ssl64
```

where /*image_path*/solaris specifies the location of the installation images, and /*image_path*/solaris/pddefault specifies the location of the installation administration script. The -G option ensures that the package is added in the current zone only.

9. Install the Tivoli Directory Server license files by running the idsLicense script in the *image_path*/solaris/tdsLicense/license directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
10. Install the Tivoli Directory Server client packages:

```
pkgadd -d /image_path/solaris/packages
-a /image_path/solaris/pddefault
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and *packages* are as follows:

License package	idsldap.license63.pkg
Base client package	idsldap.cltbase63.pkg
64-bit client package	idsldap.clt64bit63.pkg
Java client package	idsldap.cltjava63.pkg

11. Ensure that your registry server is running.
12. Run the isamLicense license script by completing the following actions:
    a. In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the isamLicense script:

```
isamLicense
```

Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an exit status 0 (SUCCESS) if it is.

-? Help: Displays the syntax of the script file.

    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
13. Upgrade the Security Access Manager license:

```
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDlic
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDlic is the Security Access Manager license package. The -G option ensures that the package is added in the current zone only.

14. Upgrade IBM Security Utilities:

```
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G TivSecUtl
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and TivSecUtl is the IBM Security Utilities package. The -G option ensures that the package is added in the current zone only.

15. Upgrade the Security Access Manager runtime:

```
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDRTE
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDRTE is the Security Access Manager runtime package. The -G option ensures that the package is added in the current zone only.

16. If the two-system upgrade option was used for the policy server, the master-host record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.
    Edit the master-host entry in the following Security Access Manager runtime configuration file: /opt/PolicyDirector/etc/pd.conf

17. Verify that you can contact the upgraded 7.0 policy server. For example, log on to the **pdadmin** interface and run a command:

```
pdadmin -a sec_master -p password
pdadmin sec_master> acl list
```

Results

The upgrade of an Security Access Manager runtime system on Solaris is now complete.

Windows: Upgrading the runtime

Upgrade your existing runtime to the Security Access Manager, version 7.0, on Windows.

About this task

The following procedure uses a two-system approach to set up the Security Access Manager 7.0 runtime system.

Procedure

1. Review the considerations in "Security Access Manager Runtime: Upgrade considerations" on page 91.
2. Log in to the previous level system as a user with administrative privileges and complete the following steps:
   a. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

```
"C:\Program Files\Tivoli\Policy Director\bin\pdbackup" -action backup
 -list fullpath_to_backup_listfile
-path path -file filename
```

where:

–list *fullpath_to_backup_listfile*
Specifies the fully qualified path to the backup list file. For example:

```
"C:\Program Files\Tivoli\Policy Director\etc\pdbackup.lst"
```

–path *path*
Specifies the path where you want the backed up files to be stored.

For example:

```
"C:\Program Files\Tivoli\Policy Director\pdbackup"
```

–file *filename*
Specifies a file name other than the `pdbackup.lst_date.time.dar` default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

b. Save the backup `.dar` file on another system.

Saving the backup data on a different system ensures that the archived data is not removed whether you decide to uninstall the existing runtime. Archived data is critical for restoring environments.

3. On the system that will host the Security Access Manager 7.0 runtime, complete the following steps:
   a. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
   b. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
   c. Install the Security Access Manager 7.0 runtime as described in the *IBM Security Access Manager for Web Installation Guide*.
   d. Configure the Security Access Manager 7.0 runtime as described in the *IBM Security Access Manager for Web Installation Guide*.

Results

The backup of your previous runtime and the setup of a Security Access Manager 7.0 runtime system on Windows is now complete.

What to do next

When you no longer need your previous level runtime, unconfigure and uninstall the previous level runtime as described in the *IBM Security Access Manager for Web Installation Guide*.

Chapter 7. Upgrading the runtime for Java

Security Access Manager supports an upgrade of an IBM Security Access Manager Runtime for Java system to version 7.0.

Note: For Security Access Manager 6.0, the runtime for Java component is renamed to IBM Security Access Manager Runtime for Java. IBM Security Access Manager Runtime for Java requires the Java virtual machine (JVM) it is deployed into to be IBM Java Runtime 1.6.0 SR10.

Security Access Manager Runtime for Java: Upgrade considerations

Before you upgrade IBM Security Access Manager Runtime for Java to 7.0, review the following considerations:

- Upgrade your operating system to the minimum supported level. For information about minimum supported levels, see *IBM Security Access Manager for Web Release Notes*.
- IBM Security Access Manager Runtime for Java requires the JVM it is deployed into to be IBM Java Runtime 1.6.0 SR10.
- If the previous version of JVM that you configured is not IBM Java Runtime 1.6.0 SR10, you must deploy a new IBM Security Access Manager Runtime for Java 7.0 into a copy of IBM Java Runtime 1.6.0 SR10.
- You are not required to upgrade all Security Access Manager components in your secure domain to a 7.0 level. However, if you upgrade any Security Access Manager component on a system, all components must be upgraded on that system to the 7.0 level, and you must install Tivoli Directory Server client 6.3 FP17 on that system.

  For a list of components that are compatible with Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.
- Windows systems upgrades are supported using a two system upgrade.
- If you use a language other than English, remember to upgrade your language package. See the *IBM Security Access Manager for Web Installation Guide* to install the language package. When you upgrade the IBM Tivoli Directory Server language packages, use the upgrade (**-U**) option for AIX, Linux, and Solaris operating systems.

AIX: Upgrading the runtime for Java

Upgrade your existing runtime for Java to IBM Security Access Manager Runtime for Java, version 7.0, on AIX.

Procedure

1. Before you upgrade the runtime for Java to IBM Security Access Manager Runtime for Java 7.0, review the considerations in "Security Access Manager Runtime for Java: Upgrade considerations."
2. Log on as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.

© Copyright IBM Corp. 2003, 2012

Note: The AIX operating system requires version 10.1 or later of the `xlC` file set. Check your current version by using the **lslpp** command and upgrade, if necessary.

4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Install the IBM Java Runtime package:

   ```
   installp -acgYXd image_path/usr/sys/inst.images packages
   ```

   where *image_path* is the directory where the DVD is mounted or the files are located, and *packages* are as follows:

   Java6_64.samples
   Specifies the IBM Java Runtime sample files package.

   Java6_64.sdk
   Specifies the IBM Java Runtime software development kit (SDK) extensions package.

   Java6_64.source
   Specifies the IBM Java Runtime source files package.
6. After the installation completes successfully, do one of the following tasks:
   - Set the PATH environmental variable. For example:

     ```
     export PATH=/usr/java6_64/bin:$PATH
     ```

     Note: To verify whether the JRE is already in the path, use the **java –version** command.
   - Set the `JAVA_HOME` environmental variable to the path where you installed IBM Java Runtime. For example, using **ksh**, enter the following to define `JAVA_HOME`:

     ```
     export JAVA_HOME=/usr/java6_64/
     ```
7. If Security Access Manager runtime is not installed, skip to step 8 on page 105. If Security Access Manager runtime is installed, do the following steps:
   a. Stop all Security Access Manager applications and services:

      ```
      pd_start stop
      ```
   b. Confirm that all Security Access Manager services and applications are stopped:

      ```
      pd_start status
      ```

      If any Security Access Manager service or application is still running, issue the **kill** command:

      ```
      kill –9 daemon_process_id
      ```
   c. Use the **pdbackup** utility to back up critical Security Access Manager information:

      ```
      /opt/PolicyDirector/bin/pdbackup -action backup
        -list fullpath_to_backup_listfile
      -path path -file filename
      ```

      where:

      –list *fullpath_to_backup_listfile*
      Specifies the fully qualified path to the backup list file. For example:

      ```
      /opt/PolicyDirector/etc/pdbackup.lst
      ```

      –path *path*
      Specifies the path where you want the backed up files to be stored.

For example:

```
/var/PolicyDirector/pdbackup
```

–file *filename*
Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

8. Ensure that your registry server and policy server are running.
9. Run the `isamLicense` license script by completing the following actions:
   a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
   b. Run the `isamLicense` script:

      ```
      isamLicense
      ```

      Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

      -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

      -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

      -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

      -? Help: Displays the syntax of the script file.
   c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
   d. Accept the license by pressing **1**.
10. Upgrade the Security Access Manager license:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.lic
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located and `PD.lic` is the Security Access Manager license package.
11. If the IBM Security Access Manager Runtime for Java is configured into the JVM for IBM WebSphere Application Server, stop the WebSphere Application Server and the IBM HTTP Server.
12. Upgrade IBM Security Access Manager Runtime for Java:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PDJ.rte
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located and `PDJ.rte` is the IBM Security Access Manager Runtime for Java package.
13. If the two-system upgrade option was used for the policy server, update the `PD.properties` file in each configured Java virtual machine (JVM) to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.
14. If the IBM Security Access Manager Runtime for Java is configured into the JVM for IBM WebSphere Application Server, restart the WebSphere Application Server and the IBM HTTP Server.

Results

The upgrade of an IBM Security Access Manager Runtime for Java system on AIX is now complete.

Linux on x86-64: Upgrading the runtime for Java

Upgrade your existing runtime for Java to IBM Security Access Manager Runtime for Java, version 7.0, on Linux x86-64.

Procedure

1. Before you upgrade the runtime for Java to IBM Security Access Manager Runtime for Java 7.0, review the considerations in "Security Access Manager Runtime for Java: Upgrade considerations" on page 103.
2. Log on as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Change to the *image_path*`/linux_x86` directory where *image_path* is the directory where the installation images are installed:

   ```
   cd image_path/linux_x86
   ```
6. Install the IBM Java Runtime package:

   ```
   rpm -ihv ibm-java-x86_64-sdk-6.0-10.0.x86_64.rpm
   ```
7. Set the PATH environment variable:

   ```
   export PATH=jre_path:$PATH
   ```

   For example, to ensure that the IBM Java Runtime is accessible through the PATH system variable, enter the following command:

   ```
   export PATH=/opt/ibm/java-x86_64-60/jre/bin:$PATH
   ```

   Note: To verify whether the JRE is already in the path, use the **java –version** command.
8. If Security Access Manager runtime is not installed, skip to step 9 on page 107. If Security Access Manager runtime is installed, do the following:
   a. Stop all Security Access Manager applications and services:

      ```
      pd_start stop
      ```
   b. Confirm that all Security Access Manager services and applications are stopped:

      ```
      pd_start status
      ```

      If any Security Access Manager service or application is still running, issue the **kill** command:

      ```
      kill –9 daemon_process_id
      ```
   c. Use the **pdbackup** utility to back up critical Security Access Manager information:

      ```
      /opt/PolicyDirector/bin/pdbackup -action backup
        -list fullpath_to_backup_listfile
      -path path -file filename
      ```

      where:

–list *fullpath_to_backup_listfile*
Specifies the fully qualified path to the backup list file. For example:

```
/opt/PolicyDirector/etc/pdbackup.lst
```

–path *path*
Specifies the path where you want the backed up files to be stored.

For example:

```
/var/PolicyDirector/pdbackup
```

–file *filename*
Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

9. Ensure that your registry server is running.
10. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:

    ```
    isamLicense
    ```

    Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

    -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

    -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

    -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

    -? Help: Displays the syntax of the script file.

    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
11. Upgrade the Security Access Manager license

    ```
    rpm -U PDlic-PD-7.0.0-0.x86_64.rpm
    ```
12. If the IBM Security Access Manager Runtime for Java is configured into the JVM for IBM WebSphere Application Server, stop the WebSphere Application Server and the IBM HTTP Server.
13. Upgrade IBM Security Access Manager Runtime for Java:

    ```
    rpm -U PDJrte-PD-7.0.0-0.x86_64.rpm
    ```
14. If the two-system upgrade option was used for the policy server, update the `PD.properties` file in each configured Java virtual machine (JVM) to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

15. If the IBM Security Access Manager runtime for Java is configured into the JVM for IBM WebSphere Application Server, restart the WebSphere Application Server and the IBM HTTP Server.

Results

The upgrade of an IBM Security Access Manager Runtime for Java system for Linux on x86-64 is now complete.

Linux on System z: Upgrading the runtime for Java

Upgrade your existing runtime for Java to IBM Security Access Manager Runtime for Java, version 7.0, on Linux on System z.

Procedure

1. Before you upgrade the runtime for Java to IBM Security Access Manager Runtime for Java 7.0, review the considerations in "Security Access Manager Runtime for Java: Upgrade considerations" on page 103.
2. Log on as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage on the System z system.
5. Change to the *image_path*`/linux_s390` directory where *image_path* is the mount point for your DVD or installation image file location. The `.rpm` files are in the /*image_path*`/linux_s390` directory.
6. Install the IBM Java Runtime package:
   ```
   rpm -ihv ibm-java-s390x-sdk-6.0-10.0.s390x.rpm
   ```
7. Set the PATH environment variable;
   ```
   export PATH=/opt/ibm/java-x86_64-60/jre/bin:$PATH
   ```

   Note: To verify whether the JRE is already in the path, use the **java –version** command.
8. If Security Access Manager runtime is not installed, skip to step 9 on page 109. If Security Access Manager runtime is installed, do the following steps:
   a. Stop all Security Access Manager applications and services:
      ```
      pd_start stop
      ```
   b. Confirm that all Security Access Manager services and applications are stopped:
      ```
      pd_start status
      ```
      If any Security Access Manager service or application is still running, issue the **kill** command:
      ```
      kill –9 daemon_process_id
      ```
   c. Use the **pdbackup** utility to back up critical Security Access Manager information:
      ```
      /opt/PolicyDirector/bin/pdbackup -action backup
        -list fullpath_to_backup_listfile
      -path path -file filename
      ```
      where:

–list *fullpath_to_backup_listfile*
Specifies the fully qualified path to the backup list file. For example:

```
/opt/PolicyDirector/etc/pdbackup.lst
```

–path *path*
Specifies the path where you want the backed up files to be stored.

For example:

```
/var/PolicyDirector/pdbackup
```

–file *filename*
Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

9. Ensure that your registry server is running.
10. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:

    ```
    isamLicense
    ```

    Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

    -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

    -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

    -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

    -? Help: Displays the syntax of the script file.

    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
11. Upgrade Security Access Manager license:

    ```
    rpm -U PDlic-PD-7.0.0-0.s390x.rpm
    ```

12. If the IBM Security Access Manager runtime for Java is configured into the JVM for IBM WebSphere Application Server, stop the WebSphere Application Server and the IBM HTTP Server.
13. Upgrade IBM Security Access Manager Runtime for Java:

    ```
    rpm -U PDJrte-PD-7.0.0-0.s390x.rpm
    ```

    The **rpm** command using the **–U** flag runs a script to automatically upgrade the IBM Security Access Manager Runtime for Java in the Java Runtime Environment where it is installed. If unsuccessful, a message displays with instructions to run the **pdjrteupg** utility manually. In this case, the utility must be run using the **–p** flag. For example:

    ```
    /opt/PolicyDirector/sbin # ./pdjrteupg -p
    ```

14. If the two-system upgrade option was used for the policy server, update the `PD.properties` file in each configured Java virtual machine (JVM) to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.
15. If the IBM Security Access Manager runtime for Java is configured into the JVM for IBM WebSphere Application Server, restart the WebSphere Application Server and the IBM HTTP Server.

Results

The upgrade of an IBM Security Access Manager Runtime for Java system for Linux on System z is now complete.

Solaris: Upgrading the runtime for Java

Upgrade your existing runtime for Java to IBM Security Access Manager Runtime for Java, version 7.0, on Solaris.

Procedure

1. Before you upgrade the runtime for Java to IBM Security Access Manager Runtime for Java 7.0, review the considerations in "Security Access Manager Runtime for Java: Upgrade considerations" on page 103.
2. Log on as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Install the IBM Java Runtime package:
   a. Enter: `mkdir p /opt/ibm/solaris`
   b. Extract the file:
      path_to_IBM_Java_package`/sol6460sr10hybrid-20111110_01-sdk.tar.Z`

      to the `/opt/ibm/solaris` directory.
6. After the installation completes successfully, do one of the following tasks:

   Note: The upgrade program expects the JRE to be installed in the default location, which is used in the following example.
   - Set the PATH environmental variable.
     `export PATH=/`*`java_path`*`:$PATH`

     For example:
     `export PATH=/opt/ibm/solaris/jre/bin:$PATH`

     Note: To verify whether the JRE is already in the path, use the **`java –version`** command.
   - If you used an installation path other than the default, set the `JAVA_HOME` environmental variable to the path where you installed IBM Java Runtime. For example, using the Korn shell, enter the following to define `JAVA_HOME`:
     `export JAVA_HOME=/opt/ibm/solaris`

7. If Security Access Manager runtime is not installed, skip to step 8. If Security Access Manager runtime is installed, do the following steps:
   a. Stop all Security Access Manager applications and services:
      ```
      pd_start stop
      ```
   b. Confirm that all Security Access Manager services and applications are stopped:
      ```
      pd_start status
      ```
      If any Security Access Manager service or application is still running, issue the **kill** command:
      ```
      kill –9 daemon_process_id
      ```
   c. Use the **pdbackup** utility to back up critical Security Access Manager information:
      ```
      /opt/PolicyDirector/bin/pdbackup -action backup
        -list fullpath_to_backup_listfile
      -path path -file filename
      ```
      where:

      –list *fullpath_to_backup_listfile*
      Specifies the fully qualified path to the backup list file. For example:
      ```
      /opt/PolicyDirector/etc/pdbackup.lst
      ```

      –path *path*
      Specifies the path where you want the backed up files to be stored.

      For example:
      ```
      /var/PolicyDirector/pdbackup
      ```

      –file *filename*
      Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

      For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.
8. Ensure that your registry server is running.
9. Run the `isamLicense` license script by completing the following actions:
   a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
   b. Run the `isamLicense` script:
      ```
      isamLicense
      ```

      Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

      -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

      -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

      -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

      -? Help: Displays the syntax of the script file.

c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

d. Accept the license by pressing **1**.

10. Upgrade the Security Access Manager license:

    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDlic
    ```

    where /*image_path*/solaris specifies the location of the installation image, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDlic is the Security Access Manager license package. The -G option ensures that the package is added in the current zone only.

11. If the IBM Security Access Manager runtime for Java is configured into the JVM for IBM WebSphere Application Server, stop the WebSphere Application Server and the IBM HTTP Server.

12. Upgrade IBM Security Access Manager Runtime for Java:

    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDJrte
    ```

    where /*image_path*/solaris specifies the installation image location, /*image_path*/solaris/pddefault specifies the installation administration script location, and PDJrte is the IBM Security Access Manager Runtime for Java package. The -G option ensures that the package is added in the current zone only.

13. If the two-system upgrade option was used for the policy server, update the PD.properties file in each configured Java virtual machine (JVM) to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

14. If the IBM Security Access Manager Runtime for Java is configured into the JVM for IBM WebSphere Application Server, restart the WebSphere Application Server and the IBM HTTP Server.

Results

The upgrade of an IBM Security Access Manager Runtime for Java system on Solaris is now complete.

Windows: Upgrading the runtime for Java

Upgrade your existing runtime for Java to IBM Security Access Manager Runtime for Java, version 7.0, on Windows.

Before you begin

You must install Security Access Manager runtime on a system before you install IBM runtime for Java. See “Windows: Upgrading the runtime” on page 100.

About this task

The following procedure uses a two-system approach to set up the Security Access Manager 7.0 runtime for Java.

Procedure

1. Review the considerations in “Security Access Manager Runtime for Java: Upgrade considerations” on page 103.

2. Log in to the existing runtime for Java system as a user with administrative privileges and complete the following steps:
   a. Use the **pdbackup** utility to back up critical Security Access Manager information:

      ```
      "C:\Program Files\Tivoli\PolicyDirector\bin\pdbackup"
        -action backup -list fullpath_to_backup_listfile
        -path path -file filename
      ```

      where:

      –list *fullpath_to_backup_listfile*
      Specifies the fully qualified path to the backup list file. For example:

      ```
      "C:\Program Files\Tivoli\Policy Director\etc\pdbackup.lst"
      ```

      –path *path*
      Specifies the path where you want the backed up files to be stored.

      For example:

      ```
      "C:\Program Files\Tivoli\Policy Director\pdbackup"
      ```

      –file *filename*
      Specifies a file name other than the `pdbackup.lst_date.time.dar` default file name.

      For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.
   b. Save the backup `.dar` file on another system.

      Saving the backup data on a different system ensures that the archived data is not removed if you decide to uninstall the existing runtime for Java. Archived data is critical for restoring environments.
3. On the system that will host the Security Access Manager 7.0 runtime for Java, complete the following steps:
   a. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
   b. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
   c. Install the Security Access Manager 7.0 runtime for Java as described in the *IBM Security Access Manager for Web Installation Guide*.
   d. Configure the Security Access Manager 7.0 runtime for Java as described in the *IBM Security Access Manager for Web Installation Guide*.

Results

The backup of your previous runtime for Java and the setup of an IBM Security Access Manager Runtime for Java system on Windows is now complete.

What to do next

When you no longer need your previous level IBM runtime for Java, unconfigure and uninstall the previous version as described in the *IBM Security Access Manager for Web Installation Guide*.

Chapter 8. Upgrading the policy proxy server

Security Access Manager supports an upgrade of the policy proxy server to 7.0.

Policy proxy server: Upgrade considerations

Before you upgrade the policy proxy server system to 7.0, review the following considerations:

- Upgrade your operating system to the minimum supported level. For information about minimum supported levels, see *IBM Security Access Manager for Web Release Notes*.
- In Tivoli Directory Server version 6.3 FP17, clients can coexist on the same workstation with a client that is version 6.0, 6.1, and 6.2. The Tivoli Directory Server 6.3 FP17 server requires that the version 6.3 client and the Java client are also installed. In addition, the server can coexist on the same workstation with another client that is version 6.0, 6.1, or 6.2 or with a version of the 6.3 server.
- You are not required to upgrade all Security Access Manager components in your secure domain to a 7.0 level. However, if you upgrade any Security Access Manager component on a system, all components must be upgraded on that system to the 7.0 level, and you must install Tivoli Directory Server client 6.3 FP17 on that system.

  For a list of components that are compatible with Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.
- If Tivoli Directory Server is your registry server and is *on a different machine* from any Security Access Manager component, you can upgrade the registry server at any time, either before or after the upgrade of the Security Access Manager 7.0 component.

  However, when the server package of Tivoli Directory Server is installed *on the same machine* as any Security Access Manager 7.0 component and if you choose to install the server package of Tivoli Directory Server 6.3 FP17, install the Tivoli Directory Server 6.3 FP17 client and server packages at the same time as you install the Security Access Manager 7.0 component on that machine.
- Windows systems upgrades are supported using a two system upgrade.
- If you use a language other than English, upgrade your language package. See the *IBM Security Access Manager for Web Installation Guide* to install the language package. When you upgrade the IBM Tivoli Directory Server language packages, use the upgrade (**-U**) option for Linux operating systems.

AIX: Upgrading the policy proxy server

Upgrade your existing policy proxy server to the Security Access Manager, version 7.0, level on AIX.

Procedure

1. Before you upgrade the policy proxy server system to 7.0, review the considerations in "Policy proxy server: Upgrade considerations."
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.

© Copyright IBM Corp. 2003, 2012

Note: The AIX operating system requires version 10.1 or higher of the `xlC` file set. Check your current version by using the **lslpp** command and upgrade, if necessary.

4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```

6. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```

7. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   /opt/PolicyDirector/etc/pdbackup.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

   For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

8. Install the Global Security Kit (GSKit):

   ```
   installp -acgYXd image_path/usr/sys/inst.images GSKit8.gskcrypt64.ppc.rte
   installp -acgYXd image_path/usr/sys/inst.images GSKit8.gsksslppc.rte
   ```

   where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located.

9. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/usr/sys/inst.images/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
10. Install the Tivoli Directory Server client packages:

    ```
    installp -acgYXd image_path/usr/sys/inst.images packages
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located, and where *packages* are the names of the Tivoli Directory Server client packages:

License package	`idsldap.license63`
Client base package	`idsldap.cltbase63`
Client package (64-bit) (no SSL)	`idsldap.clt64bit63`
Client package (64-bit) (SSL)	`idsldap.clt_max_crypto64bit63`
Java Client package	`idsldap.cltjava63`

11. Ensure that your registry server is running.
12. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:

       ```
       isamLicense
       ```

       Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

       -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

       -? Help: Displays the syntax of the script file.
    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
13. Upgrade Security Access Manager license:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.lic
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located, and `PD.lic` is the Security Access Manager license package.
14. Upgrade IBM Security Utilities:

    ```
    installp -acgYXd image_path/usr/sys/inst.images TivSec.Utl
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located, and `TivSec.Utl` is the IBM Security Utilities package.
15. Upgrade Security Access Manager runtime:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.RTE
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located, and `PD.RTE` is the Security Access Manager runtime package.
16. Upgrade Security Access Manager policy proxy server:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.MgrPrxy
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located, and `PD.MgrPrxy` is the Security Access Manager policy proxy server package.
17. If the two-system upgrade option was used for the policy server, the `master-host` record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.
    Edit the `master-host` entry in each of the following configuration files:
    - Security Access Manager runtime

      ```
      /opt/PolicyDirector/etc/pd.conf
      ```

- Security Access Manager policy proxy server

  `/opt/PolicyDirector/etc/pdmgrpxoxyd.conf`

18. Start the policy proxy server daemon (`pdmgrproxyd`):

    ```
    pd_start start
    ```

19. Ensure that policy proxy server is running:

    ```
    pd_start status
    ```

20. Verify that you can contact the upgraded 7.0 policy server. For example, log on to the **pdadmin** interface and run a command:

    ```
    pdadmin -a sec_master -p password
    pdadmin sec_master> acl list
    ```

Results

The upgrade of the policy proxy server on AIX is now complete.

Linux on x86-64: Upgrading policy proxy servers

Upgrade your existing policy proxy server to the Security Access Manager, version 7.0, level on Linux x86-64.

Before you begin

Before you upgrade the policy proxy server system to 7.0, review the considerations in "Policy proxy server: Upgrade considerations" on page 115.

Procedure

1. Log in as **root**.
2. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
4. Change to the following directory:

   ```
   cd image_path/linux_x86
   ```

   where *image_path*`/linux_x86` is the directory where the installation images are located.
5. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```

6. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```

7. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

```
/opt/PolicyDirector/etc/pdbackup.lst
```

–path *path*
Specifies the path where you want the backed up files to be stored.

For example:

```
/var/PolicyDirector/pdbackup
```

–file *filename*
Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

8. Upgrade Global Security Kit (GSKit):

```
rpm -U gskcrypt64-8.0.14.26.linux.x86_64.rpm
rpm -U gsksslb64-8.0.14.26.linux.x86_64.rpm
```

9. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_x86/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
10. Install the Tivoli Directory Server client packages:

```
rpm -i packages
```

where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.x86_64.rpm`
Base client package	`idsldap-cltbase63-6.3.0-17.x86_64.rpm`
64-bit client package	`idsldap-clt64bit63-6.3.0-17.x86_64.rpm`
Java client package	`idsldap-cltjava63-6.3.0-17.x86_64.rpm`

11. Ensure that your registry server and policy server are running.
12. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:

```
isamLicense
```

Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

-? Help: Displays the syntax of the script file.

    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
13. Upgrade the Security Access Manager license:

```
rpm -U PDlic-PD-7.0.0-0.x86_64.rpm
```

14. Upgrade IBM Security Utilities:
```
rpm -U TivSecUtl-TivSec-7.0.0-0.x86_64.rpm
```
15. Upgrade the Security Access Manager runtime:
```
rpm -U PDRTE-PD-7.0.0-0.x86_64.rpm
```
16. Upgrade the Security Access Manager policy proxy server:
```
rpm -U PDMgrPrxy-PD-7.0.0-0.x86_64.rpm
```
17. If the two-system upgrade option was used for the policy server, the `master-host` record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.
    Edit the `master-host` entry in each of the following configuration files:
    - Security Access Manager runtime
      `/opt/PolicyDirector/etc/pd.conf`
    - Security Access Manager policy proxy server
      `/opt/PolicyDirector/etc/pdmgrproxyd.conf`
18. Start the policy proxy server daemon (`pdmgrproxyd`):
```
pd_start start
```
19. Confirm that the policy proxy server is running:
```
pd_start status
```
20. Verify that you can contact the upgraded 7.0 policy server. For example, log on to the **pdadmin** interface and run a command:
```
pdadmin -a sec_master -p password
pdadmin sec_master> acl list
```

Results

The upgrade of the policy proxy server for Linux on x86-64 is now complete.

Linux on System z: Upgrading policy proxy servers

Upgrade your existing policy proxy server to the Security Access Manager, version 7.0, level on Linux on System z.

Before you begin

Before you upgrade the policy proxy server system to 7.0, review the considerations in "Policy proxy server: Upgrade considerations" on page 115.

Procedure

1. Log in as **root**.
2. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
3. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage on the System z system.
4. Change to the following directory:
```
cd image_path/linux_s390
```

where *image_path* is the directory where the installation images are located. The `.rpm` files are in the `/`*`image_path`*`/linux_s390` directory.

5. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```

6. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```

7. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   /opt/PolicyDirector/etc/pdbackup.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the `pdbackup.lst_`*`date.time`*`.tar` default file name.

   For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

8. Upgrade IBM Global Security Kit (GSKit):

   ```
   rpm -U gskcrypt64-8.0.14.26.linux.s390x.rpm
   rpm -U gskssl64-8.0.14.26.linux.s390x.rpm
   ```

9. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_s390/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

10. Install the client packages of Tivoli Directory Server:

    ```
    rpm -i packages
    ```

    where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.s390.rpm`
Base client package	`idsldap-cltbase63-6.3.0-17.s390.rpm`
64-bit client package	`idsldap-clt64bit63-6.3.0-17.s390x.rpm`
Java client package	`idsldap-cltjava63-6.3.0-17.s390x.rpm`

11. Ensure that your registry server and policy server are running.

12. Run the `isamLicense` license script by completing the following actions:

    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

    b. Run the `isamLicense` script:

       ```
       isamLicense
       ```

Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

-? Help: Displays the syntax of the script file.

c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

d. Accept the license by pressing **1**.

13. Upgrade the Security Access Manager license:
    ```
    rpm -U PDlic-PD-7.0.0-0.s390x.rpm
    ```
14. Upgrade IBM Security Utilities:
    ```
    rpm -U TivSecUtil-TivSec-7.0.0-0.s390x.rpm
    ```
15. Upgrade the Security Access Manager runtime:
    ```
    rpm -U PDRTE-PD-7.0.0-0.s390x.rpm
    ```
16. Upgrade the Security Access Manager policy proxy server:
    ```
    rpm -U PDMgrPrxy-PD-7.0.0-0.s390x.rpm
    ```
17. If the two-system upgrade option was used for the policy server, the `master-host` record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

    Edit the `master-host` entry in each of the following configuration files:

    - Security Access Manager runtime
      `/opt/PolicyDirector/etc/pd.conf`
    - Security Access Manager policy proxy server
      `/opt/PolicyDirector/etc/pdmgrproxyd.conf`
18. Start the policy proxy server daemon (`pdmgrproxyd`):
    ```
    pd_start start
    ```
19. Confirm that the policy proxy server is running:
    ```
    pd_start status
    ```
20. Verify that you can contact the upgraded 7.0 policy server. For example, log on to the **pdadmin** interface and run a command:
    ```
    pdadmin -a sec_master -p password
    pdadmin sec_master> acl list
    ```

Results

The upgrade of the policy proxy server for Linux on System z is now complete.

Solaris: Upgrading the policy proxy server

Upgrade your existing policy proxy server to the Security Access Manager, version 7.0, level on Solaris.

Procedure

1. Before you upgrade the policy proxy server system to 7.0, review the considerations in "Policy proxy server: Upgrade considerations" on page 115.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```
6. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
7. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   /opt/PolicyDirector/etc/pdbackup.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

   For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.
8. Install the Global Security Kit (GSKit):

   ```
   pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8cry64
   pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8ssl64
   ```

   where `/image_path/solaris` specifies the location of the package and `/image_path/solaris/pddefault` specifies the location of the installation administration script. The `-G` option ensures that the package is added in the current zone only.

   Note: During installation, you are asked if you want to use `/opt` as the `root` directory. If space permits, use `/opt` as the `root` installation directory. To accept `/opt` as the `root` directory, press **Enter**.
9. Install the Tivoli Directory Server license files by running the `idsLicense` script in the `image_path/solaris/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
10. Install the Tivoli Directory Server client packages of the:

```
pkgadd -d /image_path/solaris/packages
-a /packages/solaris/pddefault
```

where /*image_path*/solaris specifies the location of the package, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and where *packages* are as follows:

License package	idsldap.license63.pkg
Base client package	idsldap.cltbase63.pkg
64-bit client package	idsldap.clt64bit63.pkg
Java client package	idsldap.cltjava63.pkg

11. Ensure that your registry server and policy server are running.
12. Run the isamLicense license script by completing the following actions:
    a. In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the isamLicense script:
       ```
       isamLicense
       ```
       Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:
       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.
       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.
       -t Test: Silently tests whether the current license is already installed. Returns an exit status 0 (SUCCESS) if it is.
       -? Help: Displays the syntax of the script file.
    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
13. Install or upgrade the Security Access Manager license:
    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDlic
    ```
    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDlic is the Security Access Manager license package. The -G option ensures that the package is added in the current zone only.
14. Install or upgrade IBM Security Utilities:
    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G TivSecUtl
    ```
    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and TivSecUtl is the IBM Security Utilities package. The -G option ensures that the package is added in the current zone only.
15. Upgrade the Security Access Manager runtime:
    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDRTE
    ```
    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation

administration script, and PDRTE is the Security Access Manager runtime package. The -G option ensures that the package is added in the current zone only.

16. Upgrade the Security Access Manager policy proxy server:

    ```
    pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G PDMgrPrxy
    ```

    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDMgrPrxy is the Security Access Manager policy proxy server package. The -G option ensures that the package is added in the current zone only.

17. If the two-system upgrade option was used for the policy server, the master-host record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

    Edit the master-host entry in each of the following configuration files:

    - Security Access Manager runtime

      /opt/PolicyDirector/etc/pd.conf

    - Security Access Manager policy proxy server

      /opt/PolicyDirector/etc/pdmgrproxyd.conf

18. Start the policy proxy server daemon (pdmgrproxyd):

    ```
    pd_start start
    ```

19. Confirm that the policy proxy server is running:

    ```
    pd_start status
    ```

20. Verify that you can contact the upgraded 7.0 policy server. For example, log on to the **pdadmin** interface and run a command:

    ```
    pdadmin -a sec_master -p password
    pdadmin sec_master> acl list
    ```

Results

The upgrade of the policy proxy server on Solaris is now complete.

Windows: Upgrading the policy proxy server

Upgrade your existing policy proxy server to the Security Access Manager, version 7.0, level on Windows.

About this task

The following procedure uses a two-system approach to set up the Security Access Manager 7.0 policy proxy server.

Procedure

1. Review the considerations in "Policy proxy server: Upgrade considerations" on page 115.
2. Log in to the existing policy proxy server system as a user with administrative privileges and complete the following steps:
   a. Stop all Tivoli Access Manager applications and services. For example, on Windows 2008 systems:
      1) Select **Start** > **Control Panel** > **Administrative Tools**.
      2) Double-click the **Services** icon.

3) Stop all Tivoli Access Manager services that run on the local system, including applications, such as WebSEAL.

b. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

```
"C:\Program Files\Tivoli\Policy Director\bin\pdbackup" -action backup
-list fullpath_to_backup_listfile
-path path -file filename
```

where:

–list *fullpath_to_backup_listfile*
Specifies the fully qualified path to the backup list file. For example:

```
"C:\Program Files\Tivoli\Policy Director\etc\pdbackup.lst"
```

–path *path*
Specifies the path where you want the backed up files to be stored. For example:

```
"C:\Program Files\Tivoli\Policy Director\pdbackup"
```

–file *filename*
Specifies a file name other than the `pdbackup.lst_date.time.dar` default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

c. Save the backup `.dar` file on another system.

Saving the backup data on a different system ensures that the archived data is not removed if you decide to uninstall the existing policy proxy server. Archived data is critical for restoring environments.

d. Start all Tivoli Access Manager applications and services. For example, on Windows 2008 systems:

1) Select **Start** > **Control Panel** > **Administrative Tools**.
2) Double-click the **Services** icon.
3) Start all Tivoli Access Manager services that run on the local system, including applications, such as WebSEAL.

3. On the system that will host the Security Access Manager 7.0 policy proxy server, complete the following steps:

a. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.

b. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.

c. Install the Security Access Manager 7.0 policy proxy server as described in the *IBM Security Access Manager for Web Installation Guide*.

d. Configure the Security Access Manager 7.0 policy proxy server as described in the *IBM Security Access Manager for Web Installation Guide*.

Results

The backup of your previous policy proxy server and the setup of the Security Access Manager 7.0 policy proxy server on Windows is now complete.

What to do next

You can optionally recreate any previous customization on your Security Access Manager 7.0 policy proxy server system.

When you no longer need your previous level policy proxy server, unconfigure and uninstall the previous level policy proxy server as described in the *IBM Security Access Manager for Web Installation Guide*.

Chapter 9. Upgrading the development system

Security Access Manager supports an upgrade of a development (ADK) system to version 7.0.

Development ADK: Upgrade considerations

Before you upgrade the development ADK system to 7.0, review the following considerations:

- Ensure that you have IBM JRE 1.5 or higher installed on your system.
- Upgrade your operating system to the minimum supported level. For information about minimum supported levels, see *IBM Security Access Manager for Web Release Notes*.
- In Tivoli Directory Server, version 6.3 FP17, clients can coexist on the same workstation with a client that is version 6.0, 6.1, or 6.2. The Tivoli Directory Server 6.3 FP17 server requires that the version 6.3 client and the Java client also be installed. In addition, the server can coexist on the same workstation with another client that is version 6.0, 6.1, or 6.2, or with a version of the 6.3 server.
- You are not required to upgrade all Security Access Manager components in your secure domain to a 7.0 level. However, if you upgrade any Security Access Manager component on a system, all components must be upgraded on that system to the 7.0 level, and you must install Tivoli Directory Server client 6.3 FP17 on that system.

  For a list of components that are compatible with Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.
- In general, if Tivoli Directory Server is your registry server and is *on a different machine* from any Security Access Manager component, you can upgrade the registry server at any time, either before or after the upgrade of the Security Access Manager 7.0 component.

  However, when the server package of Tivoli Directory Server is installed *on the same machine* as any Security Access Manager 7.0 component and if you choose to install the server package of Tivoli Directory Server 6.3 FP17, install the Tivoli Directory Server 6.3 FP17 client and server packages at the same time as you install the Security Access Manager 7.0 component on that machine.
- Windows systems upgrades are supported using a two system upgrade.
- If you use a language other than English, upgrade your language package. See the *IBM Security Access Manager for Web Installation Guide* to install the language package. When you upgrade the IBM Tivoli Directory Server language packages, use the upgrade (**-U**) option for Linux operating systems.

AIX: Upgrading the development system

Upgrade your existing development system to the Security Access Manager, version 7.0, development system on AIX.

Procedure

1. Before you upgrade the development system to 7.0, review the considerations in "Development ADK: Upgrade considerations."
2. Log in as **root**.

© Copyright IBM Corp. 2003, 2012

3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*. The AIX operating system requires version 10.1 or later of the `xlC` file set. Check your current version by using the **lslpp** command and upgrade, if necessary.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```
6. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
7. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup
    -action backup -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   /opt/PolicyDirector/etc/pdbackup.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

   For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.
8. Install the Global Security Kit (GSKit):

   ```
   installp -acgYXd image_path/usr/sys/inst.images GSKit8.gskcrypt64.ppc.rte
   installp -acgYXd image_path/usr/sys/inst.images GSKit8.gsksslppc.rte
   ```

   where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located.
9. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/usr/sys/inst.images/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
10. Install the client packages of Tivoli Directory Server:

    ```
    installp -acgYXd image_path/usr/sys/inst.images packages
    ```

    where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located and where *packages* are the names of the Tivoli Directory Server client packages:

License package	`idsldap.license63`
Client base package	`idsldap.cltbase63`
Client package (64-bit) (no SSL)	`idsldap.clt64bit63`

Client package (64-bit) (SSL)	idsldap.clt_max_crypto64bit63
Java Client package	idsldap.cltjava63

11. Ensure that your registry server and policy server are running.
12. Run the isamLicense license script by completing the following actions:
    a. In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the isamLicense script:

       ```
       isamLicense
       ```

       Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

       -t Test: Silently tests whether the current license is already installed. Returns an exit status 0 (SUCCESS) if it is.

       -? Help: Displays the syntax of the script file.
    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
13. Install or upgrade Security Access Manager license:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.lic
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and PD.lic is the Security Access Manager license package.
14. Install or upgrade IBM Security Utilities:

    ```
    installp -acgYXd image_path/usr/sys/inst.images TivSec.Utl
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and TivSec.Utl is the IBM Security Utilities package.
15. Upgrade Security Access Manager runtime:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.RTE
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and PD.RTE is the Security Access Manager runtime package.
16. Upgrade Security Access Manager Application Development Kit:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.AuthADK
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and PD.AuthADK is the Security Access Manager Application Development Kit.
17. If the two-system upgrade option was used for the policy server, the master-host record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

Edit the `master-host` entry in the following Security Access Manager runtime configuration file: `/opt/PolicyDirector/etc/pd.conf`

Results

The upgrade of a development system on AIX is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Linux on x86-64: Upgrading the development ADK

Upgrade your existing development system to the Security Access Manager, version 7.0, development system on Linux x86-64.

Procedure

1. Before you upgrade the development system to 7.0, review the considerations in "Development ADK: Upgrade considerations" on page 129.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Change to the following directory:
   ```
   cd image_path/linux_x86
   ```
   where *image_path* is where the installation images are located.
6. Stop all Tivoli Access Manager applications and services:
   ```
   pd_start stop
   ```
7. Confirm that all Tivoli Access Manager services and applications are stopped:
   ```
   pd_start status
   ```
   If any Tivoli Access Manager service or application is still running, issue the **kill** command:
   ```
   kill –9 daemon_process_id
   ```
8. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:
   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```
   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:
   `/opt/PolicyDirector/etc/pdbackup.lst`

   –path *path*
   Specifies the path where you want the backed up files to be stored.
   For example:
   `/var/PolicyDirector/pdbackup`

   –file *filename*
   Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

9. Upgrade the IBM Global Security Kit (GSKit).

   ```
   rpm -U gskcrypt64-8.0.14.26.linux.x86_64.rpm
   rpm -U gskssl64-8.0.14.26.linux.x86_64.rpm
   ```

10. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_x86/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
11. Install the client packages of Tivoli Directory Server:

    ```
    rpm -i packages
    ```

    where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.x86_64.rpm`
Base client package	`idsldap-cltbase63-6.3.0-17.x86_64.rpm`
64-bit client package	`idsldap-clt64bit63-6.3.0-17.x86_64.rpm`
Java client package	`idsldap-cltjava63-6.3.0-17.x86_64.rpm`

12. Ensure that your registry server and policy server are running.
13. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:

       ```
       isamLicense
       ```

       Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

       -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

       -? Help: Displays the syntax of the script file.

    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
14. Upgrade the Security Access Manager license:

    ```
    rpm -U PDlic-PD-7.0.0-0.x86_64.rpm
    ```

15. Upgrade IBM Security Utilities:

    ```
    rpm -U TivSecUtl-TivSec-7.0.0-0.x86_64.rpm
    ```

16. Upgrade Security Access Manager runtime:

    ```
    rpm -U PDRTE-PD-7.0.0-0.x86_64.rpm
    ```

17. Upgrade Security Access Manager Application Development Kit:

    ```
    rpm -U PDAuthADK-PD-7.0.0-0.x86_64.rpm
    ```

18. If the two-system upgrade option was used for the policy server, the `master-host` record must be updated to point to the new policy server.

Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

Edit the `master-host` entry in the following Security Access Manager runtime configuration file: `/opt/PolicyDirector/etc/pd.conf`

Results

The upgrade of a development system for Linux on x86-64 is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Linux on System z: Upgrading the development system

Upgrade your existing development system to the Security Access Manager, version 7.0, development system on Linux on System z.

Procedure

1. Before you upgrade the development system to 7.0, review the considerations in "Development ADK: Upgrade considerations" on page 129.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage on the System z system.
5. Change to the following directory:

   ```
   cd image_path/linux_s390
   ```

   where *image_path* is where the DVD is mounted. The `.rpm` files are in the `/image_path/linux_s390` directory.
6. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```
7. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
8. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:

   ```
   /opt/PolicyDirector/etc/pdbackup.lst
   ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

–file *filename*
Specifies a file name other than the pdbackup.lst_*date.time*.tar default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

9. Install or upgrade IBM Global Security Kit (GSKit).
```
rpm -U gskcrypt64-8.0.14.26.linux.s390x.rpm
rpm -U gsksslk64-8.0.14.26.linux.s390x.rpm
```
10. Install the Tivoli Directory Server license files by running the idsLicense script in the *image_path*/linux_s390/tdsLicense/license directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
11. Install the client packages of Tivoli Directory Server:
```
rpm -i packages
```
where *packages* are as follows:

License package	idsldap-license63-6.3.0-17.s390.rpm
Base client package	idsldap-cltbase63-6.3.0-17.s390.rpm
64-bit client package	idsldap-clt64bit63-6.3.0-17.s390x.rpm
Java client package	idsldap-cltjava63-6.3.0-17.s390.rpm

12. Ensure that your registry server is running.
13. Run the isamLicense license script by completing the following actions:
    a. In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the isamLicense script:
```
isamLicense
```
    Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:

    -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

    -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

    -t Test: Silently tests whether the current license is already installed. Returns an exit status 0 (SUCCESS) if it is.

    -? Help: Displays the syntax of the script file.

    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
14. Upgrade Security Access Manager license:
```
rpm -U PDlic-PD-7.0.0-0.s390x.rpm
```
15. Upgrade IBM Security Utilities:
```
rpm -U TivSecUtl-TivSec-7.0.0-0.s390x.rpm
```
16. Upgrade Security Access Manager runtime:
```
rpm -U PDRTE-PD-7.0.0-0.s390x.rpm
```
17. Upgrade Security Access Manager Application Development Kit:

```
rpm -U PDAuthADK-PD-7.0.0-0.s390x.rpm
```

18. If the two-system upgrade option was used for the policy server, the `master-host` record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

    Edit the `master-host` entry in the following Security Access Manager runtime configuration file: `/opt/PolicyDirector/etc/pd.conf`

Results

The upgrade of a development system for Linux on System z is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Solaris: Upgrading the development system

Upgrade your existing development system to the Security Access Manager, version 7.0, development system on Solaris.

Procedure

1. Before you upgrade the development system to 7.0, review the considerations in "Development ADK: Upgrade considerations" on page 129.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```

6. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```

7. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the backup list file. For example:
   `/opt/PolicyDirector/etc/pdbackup.lst`

   –path *path*
   Specifies the path where you want the backed up files to be stored.
   For example:
   `/var/PolicyDirector/pdbackup`

   –file *filename*
   Specifies a file name other than the `pdbackup.lst_date.time.tar` default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

8. Install the Global Security Kit (GSKit):

   ```
   pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8cry64
   pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8ssl64
   ```

   where /*image_path*/solaris specifies the location of the installation images, and /*image_path*/solaris/pddefault specifies the location of the installation administration script. The -G option ensures that the package is added in the current zone only.

9. Install the Tivoli Directory Server license files by running the idsLicense script in the *image_path*/solaris/tdsLicense/license directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

10. Install the Tivoli Directory Server client packages:

    ```
    pkgadd -d /image_path/solaris/packages
    -a /image_path/solaris/pddefault
    ```

    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and *packages* are as follows:

License package	idsldap.license63.pkg
Base client package	idsldap.cltbase63.pkg
64-bit client package	idsldap.clt64bit63.pkg
Java client package	idsldap.cltjava63.pkg

11. Ensure that your registry server and policy server are running.

12. Run the isamLicense license script by completing the following actions:

    a. In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.

    b. Run the isamLicense script:

       ```
       isamLicense
       ```

       Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

       -t Test: Silently tests whether the current license is already installed. Returns an exit status 0 (SUCCESS) if it is.

       -? Help: Displays the syntax of the script file.

    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

    d. Accept the license by pressing **1**.

13. Install or upgrade the Security Access Manager license:

    ```
    pkgadd -d /image_path/solaris
    -a /image_path/solaris/pddefault -G PDlic
    ```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDlic is the Security Access Manager license package. The -G option ensures that the package is added in the current zone only.

14. Upgrade IBM Security Utilities:

    ```
    pkgadd -d /image_path/solaris
    -a /image_path/solaris/pddefault -G TivSecUtl
    ```

    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and TivSecUtl is the IBM Security Utilities package. The -G option ensures that the package is added in the current zone only.

15. Upgrade Security Access Manager runtime:

    ```
    pkgadd -d /image_path/solaris
    -a /image_path/solaris/pddefault -G PDRTE
    ```

    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDRTE is the Security Access Manager runtime package. The -G option ensures that the package is added in the current zone only.

16. Upgrade Security Access Manager Application Development Kit:

    ```
    pkgadd -d /image_path/solaris
    -a /image_path/solaris/pddefault -G PDAuthADK
    ```

    where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDAuthADK is the Security Access Manager Application Development Kit package. The -G option ensures that the package is added in the current zone only.

17. If the two-system upgrade option was used for the policy server the master-host record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

    Edit the master-host entry in the following Security Access Manager runtime configuration file: /opt/PolicyDirector/etc/pd.conf

Results

The upgrade of a development system on Solaris is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Windows: Upgrading the development system

Upgrade your existing development system to the Security Access Manager, version 7.0, development system on Windows.

About this task

The following procedure uses a two-system approach to set up the Security Access Manager 7.0 development system.

Procedure

1. Review the considerations in "Development ADK: Upgrade considerations" on page 129.
2. Log in to the existing development system as a user with administrative privileges and complete the following steps:
   a. Stop all Tivoli Access Manager applications and services. For example, on Windows 2008 systems:
      1) Select **Start** > **Control Panel** > **Administrative Tools**.
      2) Double-click the **Services** icon.
      3) Stop all Tivoli Access Manager services that run on the local system, including applications, such as WebSEAL.
   b. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

      ```
      "C:\Program Files\Tivoli\Policy Director\bin\pdbackup" -action backup
      -list fullpath_to_backup_listfile
      -path path -file filename
      ```

      where:

      –list *fullpath_to_backup_listfile*
      Specifies the fully qualified path to the backup list file. For example:

      ```
      "C:\Program Files\Tivoli\Policy Director\etc\pdbackup.lst"
      ```

      –path *path*
      Specifies the path where you want the backed up files to be stored. For example:

      ```
      "C:\Program Files\Tivoli\Policy Director\pdbackup"
      ```

      –file *filename*
      Specifies a file name other than the `pdbackup.lst_date.time.dar` default file name.

      For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.
   c. Save the backup `.dar` file on another system.

      Saving the backup data on a different system ensures that the archived data is not removed if you decide to uninstall the existing development system. Archived data is critical for restoring environments.
   d. Start all Tivoli Access Manager applications and services. For example, on Windows 2008 systems:
      1) Select **Start** > **Control Panel** > **Administrative Tools**.
      2) Double-click the **Services** icon.
      3) Start all Tivoli Access Manager services that run on the local system, including applications, such as WebSEAL.
3. On the system that will host the Security Access Manager 7.0 development system, complete the following steps:
   a. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
   b. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
   c. Install the Security Access Manager 7.0 development system as described in the *IBM Security Access Manager for Web Installation Guide*.

d. Configure the Security Access Manager 7.0 development system as described in the *IBM Security Access Manager for Web Installation Guide*.

Results

The backup of your previous development system and the setup of the Security Access Manager 7.0 development system on Windows is now complete.

Perform any necessary application-specific tasks before you start Security Access Manager applications.

What to do next

You can optionally re-create any previous customization on your Security Access Manager 7.0 development system.

When you no longer need your previous level development system, unconfigure and uninstall the previous level development system as described in the *IBM Security Access Manager for Web Installation Guide*.

Chapter 10. Upgrading the session management server

This chapter provides information about upgrading a Security Access Manager session management server (SMS) system from version 6.0, 6.1, or 6.1.1 to version 7.0.

To upgrade a session management server, extract the session management server instance configuration of the existing version, edit it as required, and then apply the updated configuration to the Security Access Manager 7.0 session management server instance.

For AIX, Linux and Solaris systems, Security Access Manager supports an upgrade of the session management server to 7.0 on existing application server systems, or on a new set of application server systems.

For Windows systems, Security Access Manager supports an upgrade of the session management server on a new set of application server systems.

Session Management Server: Upgrade considerations

Before you upgrade and migrate data for Session Management Server, review these considerations.

- If your current version of WebSphere Application Server is not supported for Security Access Manager, upgrade your WebSphere Application Server version to a supported level. See the *IBM Security Access Manager for Web Release Notes* for information about supported WebSphere Application Server versions. For upgrade instructions, see the WebSphere Application Server documentation.
- Security Access Manager 7.0 session management server runs on WebSphere Application Server 7.0 or 8.0 only, and WebSphere eXtreme Scale 8.5.
- Upgrade your operating system to the minimum supported level. For information about minimum supported levels, see the *IBM Security Access Manager for Web Release Notes*.
- Windows upgrades are supported on a two-system upgrade approach only.
- If you upgrade from SMS 6.1.1, you can upgrade the session management server either:
  - Before or after the Web security servers (WebSEAL and the Plug-in for Web Servers) upgrade.
  - Before or after the policy server and authorization servers upgrades.
- If you upgrade from SMS 6.0, the session management server must be upgraded before the Web security servers (WebSEAL or Plug-in for Web Servers).
- If you are upgrading from a 32-bit SMS 6.0 environment, you must upgrade to SMS 6.1 or SMS 6.1.1 before you can extract the existing configuration.
- The Security Access Manager WebSEAL and Web Plug-in servers for versions 6.1 and 6.1.1 run against Security Access Manager session management server 6.1 and 6.1.1 only. Security Access Manager WebSEAL and Web Plug-in servers for version 6.0 run against session management server 6.0, 6.1, or 6.1.1.
- User sessions are not retained across the upgrade. Some downtime is necessary. To reduce downtime, reconfigure WebSEAL or Plug-in for Web Servers instances to disable session management server at the start of the process. This

© Copyright IBM Corp. 2003, 2012

reconfiguration allows the servers to continue processing user sessions during upgrade. During processing, functions could be reduced.
- You are not required to modify the login history database during upgrade.

Upgrade scenarios

This section lists three upgrade scenarios: a single server upgrade, a side-by-side cluster upgrade, and an in-place cluster upgrade. The basic processes for these scenarios are documented below, ignoring operating system specifics.

The other viable option is to upgrade by installing a separate version of WebSphere Application Server on the same set of workstations. This works the same way as the 'side by side' cluster upgrade below.

Single server upgrade from version 6.1.1

About this task

Single server upgrades are supported on AIX, Linux, and Solaris systems.

Procedure

1. Log in as `root`.
2. Source the **setupCmdLine** script for the WebSphere Application Server profile.
3. Insert and mount the Session Management Server installation DVD. For more details on specific operating system tasks, see "Upgrading the session management server" on page 148.
4. Install the 7.0 packages on the target system.
5. Run the extract command:
   ```
   smscfg -action extract -instance oldinstance -record sms_upgrade.rsp
   ```
6. Check the values in the recorded response file to ensure that they are correct for the 7.0 installation.
7. Deploy the 7.0 instance:
   ```
   smscfg -action deploy -instance newinstance
   ```
8. Configure the 7.0 instance:
   ```
   smscfg -action config -instance newinstance -rsp_file sms_upgrade.rsp
   ```
9. If possible, test the 7.0 instance with a single Web security server instance.
10. Stop the Web security server processes on all WebSEAL or Web Plug-in systems.
11. On each Web security server system:
    a. Update the Web security server configuration to specify the new Session Management Server URL (replace *oldinstance* with *newinstance*).
    b. Start the Web security server processes (`pdweb start / pdwebpi_start`).
12. Unconfigure the 6.1.1 instance:
    ```
    smscfg -action unconfig -instance oldinstance
    ```
13. Undeploy the 6.1.1 instance:
    ```
    smscfg -action undeploy -instance oldinstance
    ```

Results

The Session Management Server console module can be upgraded before or after this process. To upgrade the console module, complete the following steps:

1. Log in as root.
2. Ensure the Session Management Server 7.0 packages are installed on the system.
3. Source the **setupCmdLine** script for the WebSphere Application Server profile.
4. Uninstall the Session Management Server console module:
   ```
   smscfg -action undeploy -instance ISC
   ```
5. Install the updated Session Management Server console module version 7.0:
   ```
   smscfg -action deploy -instance ISC
   ```

The Session Management Server CLI must be reconfigured to point to the new Session Management Server instance:

```
pdsmsclicfg -action config -instances newinstance
```

Single server upgrade from version 6.1

About this task

Single server upgrades are supported on AIX, Linux, and Solaris systems.

Procedure

1. Log in as root.
2. Source the **setupCmdLine** script for the WebSphere Application Server profile.
3. Insert and mount the Session Management Server installation DVD. For more details on specific operating system tasks, see "Upgrading the session management server" on page 148.
4. Install the 7.0 packages on the target system.
5. Run the extract command:
   ```
   smscfg -action extract -instance oldinstance -record sms_upgrade.rsp
   ```
6. Check the values in the recorded response file to ensure that they are correct for the 7.0 installation.
7. Deploy the 7.0 instance:
   ```
   smscfg -action deploy -instance newinstance
   ```
8. Configure the 7.0 instance:
   ```
   smscfg -action config -instance newinstance -rsp_file sms_upgrade.rsp
   ```
9. If possible, test the 7.0 instance with a single Web security server instance.
10. Stop the Web security server processes on all WebSEAL or Web Plug-in server.
11. On each Web security server system:
    a. Update the Web security server configuration to specify the new Session Management Server URL (replace *oldinstance* with *newinstance*).
    b. Start the Web security server processes (`pdweb start` / `pdwebpi_start`).
12. Unconfigure the 6.1 instance:
    ```
    smscfg -action unconfig -instance oldinstance
    ```
13. Undeploy the 6.1 instance:
    ```
    smscfg -action undeploy -instance oldinstance
    ```

Results

You can upgrade the Session Management Server console module either before or after this process by completing the following steps:

1. Log in as root.

2. Ensure the Session Management Server 7.0 packages are installed on the system.
3. Source the **setupCmdLine** script for the WebSphere Application Server profile.
4. Uninstall the Session Management Server console module:
   ```
   smscfg -action undeploy -instance ISC
   ```
5. Install the updated Session Management Server console module version:
   ```
   smscfg -action deploy -instance ISC
   ```

The Session Management Server CLI must be reconfigured to point to the new Session Management Server instance:

```
pdsmsclicfg -action config -instances newinstance
```

Single server upgrade from version 6.0

About this task

Single server upgrades are supported on AIX, Linux, and Solaris systems.

Procedure

1. Log in as `root`.
2. Source the **setupCmdLine** script for the WebSphere Application Server profile.
3. Insert and mount the Session Management Server installation DVD. For more details on specific operating system tasks, see "Upgrading the session management server" on page 148.
4. Install the 6.1.1 packages on the target system.
5. Run the extract command:
   ```
   smscfg -action extract -instance TAM60_SMS -record sms_upgrade.rsp
   ```
6. Check the values in the recorded response file to ensure that they are correct for the 7.0 installation.
7. Unconfigure the Session Management Server 6.0 instance:
   ```
   smscfg -action unconfig -instance TAM60_SMS
   ```
8. Uninstall the Session Management Server 6.0 instance by uninstalling the **DSess** > **DSessConfig** applications:
   a. Open the WebSphere Application Server administrative console.
      For example, enter this URL from a supported Web browser:
      ```
      http://host_name:9060/ibm/console
      ```
      where *host_name* specifies the name or IP address of the system where the IBM WebSphere Application Server is installed.
   b. Log in to the console with a valid user ID and, if applicable, password.
   c. Click **Applications** > **Enterprise Applications** in the console navigation tree.
   d. Select the **DSess** > **DSessConfig** applications.
   e. Click **Uninstall**.
   f. Save the changes.
9. If the Web Portal Manager is installed, unconfigure it:
   ```
   amwpmcfg -action unconfig -interactive
   ```
10. Upgrade to WebSphere Application Server 7.0 or 8.0 and install the required WebSphere Application Server fix pack levels.
11. Install the 7.0 packages on the target system.
12. Deploy the 7.0 instance:

```
smscfg -action deploy -instance newinstance
```

13. Configure the 7.0 instance:
    ```
    smscfg -action config -instance newinstance -rsp_file sms_upgrade.rsp
    ```
14. If possible, test the 7.0 instance with a single Web security server instance.
15. Stop the Web security server processes on all WebSEAL or Web Plug-in machines.
16. On each Web security server system:
    a. Update the Web security server configuration to specify the new Session Management Server URL (replace *oldinstance* with *newinstance*).
    b. Start the Web security server processes (`pdweb start` or `pdwebpi_start`).

Side-by-side cluster upgrade from SMS 6.0, 6.1, or 6.1.1

About this task

This scenario assumes the cluster for 7.0 is already configured, and has the appropriate WebSphere Application Server fix packs installed.

Procedure

1. Log in to the 6.0, 6.1, or 6.1.1 deployment manager server as root.
2. If you upgrade from Session Management Server 6.0:
   a. Insert and mount the Session Management Server installation DVD.
   b. Install the Session Management Server 7.0 packages.
3. Source the **setupCmdLine** script from the deployment manager profile.
4. Extract the 6.0, 6.1, or 6.1.1 configuration:
   ```
   smscfg -action extract -instance instance -record sms_upgrade.rsp
   ```
5. Check the values in the recorded response file to ensure that they are correct for the new environment.
6. For each server in the 7.0 environment, including the deployment manager:
   a. Log in as `root`.
   b. Insert and mount the WebSphere eXtreme Scale installation DVD.
   c. Stop all WebSphere Application Server processes in all WebSphere Application Server profiles that will host the 7.0 Session Management Server instance.
   d. Run the WebSphere eXtreme Scale 8.5 installer, ensuring the path for the correct WebSphere Application Server installation is specified and that all appropriate profiles are augmented. Both the client and server components must be installed, but none of the optional components are required.
   e. Start all WebSphere Application Server processes that were stopped previously.
7. Log in to the deployment manager server for the 7.0 installation as `root`.
8. Transfer the recorded response file from the 6.1 or 6.1.1 deployment manager server.
9. Source the **setupCmdLine** script from the deployment manager profile.
10. Insert and mount the Session Management Server installation DVD.
11. Install the Session Management Server 7.0 packages.
12. Deploy the Session Management Server 7.0 instance:
    ```
    smscfg -action deploy -instance instance
    ```
13. Configure the Session Management Server 7.0 instance:

```
smscfg -action config -instance instance -rsp_file sms_upgrade.rsp
```

14. If required, install the Session Management Server console module:
    ```
    smscfg -action deploy -instance ISC
    ```
15. Stop the Web security servers on all systems (`pdweb stop` or `pdwebpi_start stop`).
16. Update the Web security server configuration to specify the new Session Management Server URLs.
17. Start the Web security servers on all systems (`pdweb start` or `pdwebpi_start`).
18. Log in to the 6.0, 6.1, or 6.1.1 deployment manager systems as root.
19. Source the **setupCmdLine** script from the deployment manager profile.
20. Unconfigure the old Session Management Server instance:
    ```
    smscfg -action unconfig -instance instance
    ```
21. Uninstall the Session Management Server 6.0 instance by uninstalling the **DSess** > **DSessConfig** applications:
    a. Open the WebSphere Application Server administrative console.
       For example, enter this URL from a supported Web browser:
       ```
       http://host name:9060/ibm/console
       ```
       where *host name* specifies the name or IP address of the system where the IBM WebSphere Application Server is installed.
    b. Log in to the console with a valid user ID and, if applicable, password.
    c. Click **Applications** > **Enterprise Applications** in the console navigation tree.
    d. Select the **DSess** > **DSessConfig** applications.
    e. Click **Uninstall**.
    f. Save the changes.
22. If the Session Management Server console module was installed, uninstall it:
    ```
    smscfg -action undeploy -instance ISC
    ```
23. Remove the old Session Management Server packages from the system.
24. For each system in the Session Management Server 6.1 or 6.1.1 environment:
    a. Log in as `root`.
    b. Source the **setupCmdLine** script from any profile.
    c. Shut down all WebSphere Application Server processes.
    d. Uninstall ObjectGrid 6.1 or 6.1.1:
       ```
       cd $WAS_HOME/uninstall_objectgrid ; java -cp og_install.jar run
       ```
    e. Start WebSphere Application Server processes as necessary.

Results

The Session Management Server CLI must also be reconfigured to point to the new Session Management Server instance:

```
pdsmsclicfg -action config -instances newinstance
```

In-place cluster upgrade from version 6.0, 6.1, or 6.1.1

About this task

Attention: This upgrade scenario involves significant downtime of Session Management Server. The scenario does not provide a fail-safe way to go back to 6.1 or 6.1.1 should anything goes wrong during installation of the 7.0 instance.

Procedure

1. Stop all Web security servers with either `pdweb stop` or `pdwebpi_start stop`.
2. Log in to the deployment manager workstation as root.
3. Source the **setupCmdLine** script for the deployment manager profile.
4. Insert and mount the Session Management Server 7.0 installation DVD.
5. Upgrade the Session Management Server packages to version 7.0.
6. Extract the existing Session Management Server configuration:

   ```
   smscfg -action extract -instance instance -record sms_upgrade.rsp
   ```

   where *instance* is `TAM60_SMS` for Session Management Server 6.0.
7. Check that the details in the recorded response file are correct and still apply in the new environment.
8. Unconfigure the Session Management Server 6.1 or 6.1.1 instance:

   ```
   smscfg -action unconfig -instance instance
   ```
9. Undeploy the Session Management Server 6.1 or 6.1.1 instance:

   ```
   smscfg -action undeploy -instance instance
   ```
10. If you upgrade from Session Management Server 6.1 or 6.1.1, and the Session Management Server console module is installed, uninstall it:

    ```
    smscfg -action undeploy -instance ISC
    ```
11. If you upgrade from Session Management Server 6.0, uninstall the Web Portal Manager, if installed.
12. Stop all WebSphere Application Server processes.
13. If you upgrade from Session Management Server 6.1 or 6.1.1, uninstall ObjectGrid 6.1 or 6.1.1:

    ```
    cd $WAS_HOME/uninstall_objectgrid ; java -cp og_install.jar run
    ```
14. If you upgrade from Session Management Server 6.0, install WebSphere Application Server 7.0 or 8.0.
15. Install any WebSphere Application Server fix packs required to run SMS 7.0.
16. Insert and mount the WebSphere eXtreme Scale 8.5 installation DVD.
17. Install WebSphere eXtreme Scale 8.5 from the DVD. Both the client and server components must be installed, but none of the optional components are required.
18. Restart all WebSphere Application Server processes.
19. For all other WebSphere Application Server workstation in the Session Management Server cluster:
    a. Log in as `root`.
    b. Source the **setupCmdLine** script from the managed node profile.
    c. Stop all WebSphere Application Server processes.
    d. If you upgrade from Session Management Server 6.1 or 6.1.1, uninstall ObjectGrid 6.1 or 6.1.1:

       ```
       cd $WAS_HOME/uninstall_objectgrid ; java -cp og_install.jar run
       ```
    e. Install any WebSphere Application Server fix packs required to run Session Management Server 7.0.
    f. Insert and mount the WebSphere eXtreme Scale installation DVD.
    g. Install WebSphere eXtreme Scale 8.5 from the DVD. Both the client and server components must be installed, but none of the optional components are required.
    h. Restart all WebSphere Application Server processes.

20. Log in to the deployment manager workstation as root.
21. Source the **setupCmdLine** script from the deployment manager profile.
22. Deploy the Session Management Server 7.0 instance:
    `smscfg -action deploy -instance instance`
23. Configure the Session Management Server 7.0 instance:
    `smscfg -action config -instance instance -rsp_file sms_upgrade.rsp`
24. Restart all Web security servers. No changes to the Web security server configuration are required.

Results

You can upgrade the Session Management Server CLI either before or after the rest of this process. No configuration changes are required.

Upgrading the session management server

Security Access Manager supports an upgrade of the session management server to 7.0 on new and existing application server systems.

AIX: Upgrading the session management server

Upgrade your existing session management server to the Security Access Manager, version 7.0, session management server on AIX.

Procedure

1. Before you upgrade, read "Session Management Server: Upgrade considerations" on page 141.
2. Log in as `root`.
3. Ensure that all necessary operating system patches are installed. Also, review the most-recent release information, including system requirements, disk space requirements, and known defects and limitations. See the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
4. Ensure that the registry server and policy server are up and running (in normal mode).
5. If you are upgrading on an existing system, upgrade WebSphere Application Server to 7.0 or 8.0. See the WebSphere documentation for upgrade instructions: http://www-306.ibm.com/software/webservers/appserv/was/library/:
6. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
7. Run the `isamLicense` license script by completing the following actions:
   a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
   b. Run the `isamLicense` script:
      `isamLicense`

      Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

      -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

-? Help: Displays the syntax of the script file.

c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

d. Accept the license by pressing **1**.

8. Install the following Security Access Manager packages:

```
installp -acgYXd image_path/usr/sys/inst.images packages
```

where *image_path* is the directory where the installation images are located, and where *packages* are as follows:

PD.lic
Specifies the Security Access Manager license package.

PD.SMS.SMS
Specifies the Security Access Manager Session Management Server package.

9. Before you run **smscfg**, run the WebSphere **setupCmdLine.bat** or **setupCmdLine.sh** script for the deployment manager file, depending on your operating system.

10. Deploy the instance:

```
smscfg -action deploy -instance new_instance
```

where *new_instance* is the name of the new instance. The new instance name that you specify must be short and use ASCII characters only.

11. Extract the Security Access Manager 6.0, 6.1, or 6.1.1 session management server configuration information into a response file:

```
smscfg -action extract -instance TAM60_SMS -record sms_upgrade.rsp
```

Where *TAM60_SMS* is the name of the existing configuration file, and *sms_upgrade.rsp* is the name of the response file. The response file is created in the same directory from which **smscfg** is invoked.

12. Edit the configuration settings in the response file to ensure compatibility with Security Access Manager 7.0 session management server. Required changes might include updated values for the following configuration options:

- **WebSphere Application Server deployment targets**: These settings identify new server or cluster names. If you are deploying to a new set of application servers, and the new server or cluster names are different, you must update the names in the response file:
  - `clustered`
  - `was_cluster`
  - `was_node`
  - `was_server`

  Note: The response file can also include various file paths and passwords for your environment. For example, `trust_store` *`file_path`*.
- **Security Access Manager environment server settings**: These settings identify the existing Security Access Manager policy and authorization servers that are used by the session management server.

- `policysvr_host`
- `policysvr_port`
- `authzsvr`

These settings are examples only. You must decide which settings must be updated for your particular scenario. See the *IBM Security Access Manager for Web Shared Session Management Administration Guide* for a complete list of configuration settings.

13. Apply the updated configuration information to the existing session management server instance:

```
smscfg -action config -instance new_instance -rsp_file sms_upgrade.rsp
```

Where *sms_upgrade.rsp* is the name of the response file.

14. If you are upgrading on an existing system, update the configuration of the Web server to use the new session management server instance:
    a. Stop the server:
       - WebSEAL:

         ```
         pdweb stop
         ```

       - Plug-in for Web Servers:

         ```
         pdwebpi_start stop
         ```

    b. Change the value for `dsess-url` in the `webseald.conf` and `pdwebpi.conf` files to the new session management server web service URL. The new URL is:

       ```
       http://server:port/new_instance/services/DSess
       ```

       where:
       - *server:port* describes either the application server that hosts the Session Management Server instance, or the load balancing proxy in front of the application server.
       - *new_instance* is the instance name that is specified in step 10 on page 149.

    c. Start the server.

15. Unconfigure the previous version of session management server instance:

```
smscfg -action unconfigure -instance TAM60_SMS -admin_id sec_master
-admin_pwd sec_master_password -remove_last_login_db no -interactive no
```

Where *TAM60_SMS* is the name of the existing configuration file, and *sec_master_password* is the master password.

16. Remove the instance by uninstalling the `DSess` and `DSessConfig` applications that use the WebSphere Administration Console:
    a. Click **Applications** > **Enterprise Applications** in the administrative console navigation tree to access the Enterprise Applications page.
    b. Uninstall the applications:
       1) Select the **DSess** > **DSessConfig** applications.
       2) Click **Uninstall**.
    c. Save changes that are made to the administrative configuration.

Results

The upgrade of the Session Management Server on AIX is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Linux on x86-64: Upgrading the session management server

Upgrade your existing session management server to the Security Access Manager, version 7.0, session management server on Linux x86-64.

Procedure

1. Before you upgrade, read "Session Management Server: Upgrade considerations" on page 141.
2. Log in as `root`.
3. Ensure that all necessary operating system patches are installed. Also, review the most-recent release information, including system requirements, disk space requirements, and known defects and limitations. See the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
4. Ensure that the registry server and policy server are up and running (in normal mode).
5. If you are upgrading on an existing system, upgrade WebSphere Application Server to 7.0 or 8.0. See the WebSphere documentation for upgrade instructions: http://www-306.ibm.com/software/webservers/appserv/was/library/.
6. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
7. Run the `isamLicense` license script by completing the following actions:
   a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
   b. Run the `isamLicense` script:
      ```
      isamLicense
      ```
      Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:
      - **`-q`** Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.
      - **`-f`** Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.
      - **`-t`** Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.
      - **`-?`** Help: Displays the syntax of the script file.
   c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
   d. Accept the license by pressing **1**.
8. Change to the following directory:
   ```
   cd image_path/linux_x86
   ```
   where *image_path* is where the installation images are located.

9. Install the following Security Access Manager packages:

   ```
   rpm -ihv packages
   ```

   where *packages* are as follows:

   PDlic-PD-7.0.0-0.x86_64.rpm
   Specifies the Access Manager license package.

   PDSMS-PD-7.0.0-0.x86_64.rpm
   Specifies the Access Manager Session Management Server package.

10. Before you run**smscfg**, run the WebSphere **setupCmdLine.bat** or **setupCmdLine.sh** script for the deployment manager file, depending on your operating system.
11. Deploy the instance:

    ```
    smscfg -action deploy -instance new_instance
    ```

    where *new_instance* is the name of the new instance. The new instance name that you specify must be short and use ASCII characters only.
12. Extract the existing Security Access Manager session management server configuration information into a response file:

    ```
    smscfg -action extract -instance TAM60_SMS -record sms_upgrade.rsp
    ```

    Where *TAM60_SMS* specifies the existing product version, and *sms_upgrade.rsp* is the name of the response file. The response file is created in the same directory from which **smscfg** is called.
13. Edit the configuration settings in the response file to ensure compatibility with Security Access Manager 7.0 session management server. Required changes might include updated values for the following configuration options:
    - **WebSphere Application Server deployment targets**: These settings identify new server or cluster names. If you are deploying to a new set of application servers, and the new server or cluster names are different, update the names in the response file:
      - `clustered`
      - `was_cluster`
      - `was_node`
      - `was_server`

      Note: The response file can also include various file paths and passwords for your environment. For example, `trust_store` *`file_path`*.
    - **Security Access Manager environment server settings**: These settings identify the Security Access Manager policy and authorization servers that are used by the session management server.
      - `policysvr_host`
      - `policysvr_port`
      - `authzsvr`

    These settings are examples only. You must decide which settings to update for your particular scenario. See the *IBM Security Access Manager for Web Shared Session Management Administration Guide* for a complete list of configuration settings.
14. Apply the updated configuration information to the session management server instance:

    ```
    smscfg -action config -instance new_instance -rsp_file sms_upgrade.rsp
    ```

Where *sms_upgrade.rsp* is the name of the response file.

15. If you are upgrading an existing application server system, update the configuration of the Web server to use the new session management server instance:
    a. Stop the server:
       - WebSEAL:

         ```
         pdweb stop
         ```

       - Plug-in for Web Servers:

         ```
         pdwebpi_start stop
         ```

    b. Change the value for `dsess-url` in the `webseald.conf` and `pdwebpi.conf` files to the new session management server web service URL. The new URL is:

       ```
       http://server:port/new_instance/services/DSess
       ```

       where:
       - *server:port* describes either the application server that hosts the SMS instance, or the load balancing proxy in front of the application server.
       - *new_instance* is the instance name that is specified in step 10 on page 149.

    c. Start the server.
16. Remove the previous session management server instance:

    ```
    smscfg -action unconfigure -instance TAM60_SMS -admin_id sec_master
    -admin_pwd sec_master_password -remove_last_login_db no -interactive no
    ```

    where *60* is the previous version number.
17. Remove the instance by uninstalling the `DSess` and `DSessConfig` applications that use the administrative console:
    a. Click **Applications** > **Enterprise Applications** in the administrative console navigation tree to access the Enterprise Applications page.
    b. Uninstall the applications:
       1) Select the **DSess** > **DSessConfig** applications.
       2) Click **Uninstall**.
    c. Save changes that are made to the administrative configuration.

Results

The upgrade of the Session Management Server on Linux on x86-64 is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Linux on System z: Upgrading the session management server

Upgrade your existing session management server to the Security Access Manager, version 7.0, session management server on Linux on System z.

Procedure

1. Before you upgrade, read "Session Management Server: Upgrade considerations" on page 141
2. Log in as `root`.

3. Ensure that all necessary operating system patches are installed. Also, review the most-recent release information, including system requirements, disk space requirements, and known defects and limitations. See the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
4. Ensure that the registry server and policy server are up and running (in normal mode).
5. Upgrade WebSphere Application Server to 7.0 or 8.0. See the WebSphere documentation for upgrade instructions: http://www-306.ibm.com/software/webservers/appserv/was/library/.
6. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage on the System z system.
7. Run the `isamLicense` license script by completing the following actions:
   a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
   b. Run the `isamLicense` script:
      ```
      isamLicense
      ```
      Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:
      -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.
      -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.
      -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.
      -? Help: Displays the syntax of the script file.
   c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
   d. Accept the license by pressing **1**.
8. Change to the following directory:
   ```
   cd image_path/linux_s390
   ```
   where *image_path* is where the installation images are located.
9. Install the following Security Access Manager packages:
   ```
   rpm -ihv packages
   ```
   where *packages* are as follows:
   PDlic-PD-7.0.0-0.s390x.rpm
   Specifies the Security Access Manager license package.
   PDSMS-PD-7.0.0-0.s390x.rpm
   Specifies the Security Access Manager Session Management Server package.
10. Before you run **smscfg**, run the WebSphere **setupCmdLine.bat** or **setupCmdLine.sh** script for the deployment manager file, depending on your operating system.
11. Deploy the instance:
    ```
    smscfg -action deploy -instance new_instance
    ```

where *new_instance* is the name of the new instance. The new instance name that you specify must be short and use ASCII characters only.

12. Extract the existing Security Access Manager session management server configuration information into a response file:

    ```
    smscfg -action extract -instance TAM60_SMS -record sms_upgrade.rsp
    ```

    Where *60* is the existing version, and *sms_upgrade.rsp* is the name of the response file. The response file is created in the same directory from which **smscfg** is called.

13. Edit the configuration settings in the response file to ensure compatibility with Security Access Manager 7.0 session management server. Required changes might include updated values for the following configuration options:

    - **WebSphere Application Server deployment targets**: These settings identify new server or cluster names. If you are deploying to a new set of application servers, and the new server or cluster names are different, you must update the names in the response file:
      - `clustered`
      - `was_cluster`
      - `was_node`
      - `was_server`

      Note: The response file can also include various file paths and passwords for your environment. For example, `trust_store` *`file_path`*.
    - **Security Access Manager environment server settings**: These settings identify the Security Access Manager policy and authorization servers that are used by the session management server.
      - `policysvr_host`
      - `policysvr_port`
      - `authzsvr`

    These settings are examples only. You must decide which settings must be updated for your particular scenario. See the *IBM Security Access Manager for Web Shared Session Management Administration Guide* for a complete list of configuration settings.

14. Apply the updated configuration information to the session management server 7.0 instance:

    ```
    smscfg -action config -instance new_instance -rsp_file sms_upgrade.rsp
    ```

    Where *sms_upgrade.rsp* is the name of the response file.

15. If you are upgrading on an existing application server system, update the configuration of the Web server to use the new session management server 7.0 instance:

    a. Stop the server:
       - WebSEAL:

         ```
         pdweb stop
         ```
       - Plug-in for Web Servers:

         ```
         pdwebpi_start stop
         ```

    b. Change the value for `dsess-url` in the `webseald.conf` and `pdwebpi.conf` files to the new session management server web service URL. The new URL is:

       `http://`*`server:port`*`/`*`new_instance`*`/services/DSess`

where:

- *server:port* describes either the application server that hosts the SMS instance, or the load balancing proxy in front of the application server.
- *new_instance* is the instance name that is specified in step 10 on page 149.

c. Start the server.

16. Remove the previous session management server instance:

```
smscfg -action unconfigure -instance TAM60_SMS -admin_id sec_master
-admin_pwd sec_master_password -remove_last_login_db no -interactive no
```

where *60* is the previous version.

17. Remove the instance by uninstalling the `DSess` and `DSessConfig` applications that use the administrative console:
    a. Click **Applications** > **Enterprise Applications** in the administrative console navigation tree to access the Enterprise Applications page.
    b. Uninstall the applications:
        1) Select the **DSess** > **DSessConfig** applications.
        2) Click **Uninstall**.
    c. Save changes that are made to the administrative configuration.

Results

The upgrade of the Session Management Server on Linux on System z is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Solaris: Upgrading the session management server

Upgrade your existing session management server to the Security Access Manager, version 7.0, session management server on Solaris.

Procedure

1. Before you upgrade, read "Session Management Server: Upgrade considerations" on page 141
2. Log in as `root`.
3. Ensure that all necessary operating system patches are installed. Also, review the most-recent release information, including system requirements, disk space requirements, and known defects and limitations. See the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
4. Ensure that the registry server and policy server are up and running (in normal mode).
5. Upgrade WebSphere Application Server to 7.0 or 8.0. See the WebSphere documentation for upgrade instructions. http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welc6topmigrating.html
6. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
7. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:

```
isamLicense
```

Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

-? Help: Displays the syntax of the script file.

c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

d. Accept the license by pressing **1**.

8. Install the following Security Access Manager packages:

```
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G packages
```

where `/image_path/solaris` is where the installation images are located, `/image_path/solaris/pddefault` specifies the location of the installation administration script, and *packages* are as follows:

PDlic Specifies the Security Access Manager license package.

PDSMS
Specifies the Security Access Manager Session Management Server package.

When the installation process is complete for each package, the following message is displayed:

```
Installation of package successful.
```

The `-G` option ensures that each package is added in the current zone only.

9. Before you run **smscfg**, run the WebSphere **setupCmdLine.bat** or **setupCmdLine.sh** script for the deployment manager file, depending on your operating system.

10. Deploy the instance:

```
smscfg -action deploy -instance new_instance
```

where *new_instance* is the name of the new instance. The new instance name that you specify must be short and use ASCII characters only.

11. Extract the existing Security Access Manager session management server configuration information into a response file:

```
smscfg -action extract -instance TAM60_SMS -record sms_upgrade.rsp
```

Where *60* is the existing version, and *sms_upgrade.rsp* is the name of the response file. The response file is created in the same directory from which **smscfg** is started.

12. Edit the configuration settings in the response file to ensure compatibility with Security Access Manager 7.0 session management server. Required changes might include updated values for the following configuration options:

- **WebSphere Application Server deployment targets**: These settings identify new server or cluster names. If you are deploying to a new set of application servers, and the new server or cluster names are different, you must update the names in the response file:
  - `clustered`
  - `was_cluster`
  - `was_node`
  - `was_server`

  Note: The response file can also include various file paths and passwords for your environment. For example, `trust_store` *`file_path`*.
- **Security Access Manager environment server settings**: These settings identify the Security Access Manager policy and authorization servers that are used by the session management server.
  - `policysvr_host`
  - `policysvr_port`
  - `authzsvr`

These settings are examples only. You must decide which settings must to be updated for your particular scenario. See the *IBM Security Access Manager for Web Shared Session Management Administration Guide* for a complete list of configuration settings.

13. Apply the updated configuration information to the session management server 7.0 instance:

```
smscfg -action config -instance new_instance -rsp_file sms_upgrade.rsp
```

Where *sms_upgrade.rsp* is the name of the response file.

14. If you are upgrading on an existing application server, update the configuration of the Web server to use the new session management server 7.0 instance:
    a. Stop the server:
       - WebSEAL:

         ```
         pdweb stop
         ```
       - Plug-in for Web Servers:

         ```
         pdwebpi_start stop
         ```

    b. Change the value for `dsess-url` in the `webseald.conf` and `pdwebpi.conf` files to the new session management server web service URL. The new URL is:

       ```
       http://server:port/new_instance/services/DSess
       ```

       where:
       - *server:port* describes either the application server that hosts the SMS instance, or the load balancing proxy in front of the application server.
       - *new_instance* is the instance name that is specified in step 10 on page 149.

    c. Start the server.
15. Remove the existing session management server instance:

```
smscfg -action unconfigure -instance TAM60_SMS -admin_id sec_master
-admin_pwd sec_master_password -remove_last_login_db no -interactive no
```

where *60* is the previous version.

16. Remove the instance by uninstalling the `DSess` and `DSessConfig` applications that use the administrative console:
    a. Click **Applications** > **Enterprise Applications** in the administrative console navigation tree to access the Enterprise Applications page.
    b. Uninstall the applications:
        1) Select the **DSess** > **DSessConfig** applications.
        2) Click **Uninstall**.
    c. Save changes that are made to the administrative configuration.

Results

The upgrade of the Session Management Server on Solaris is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Windows: Upgrading the session management server

Upgrade your existing session management server to the Security Access Manager, version 7.0, session management server on Windows.

About this task

Note: Windows upgrades are supported on a two-system upgrade approach only.

Procedure

1. Before you upgrade, read "Session Management Server: Upgrade considerations" on page 141.
2. Log in as an administrator.
3. Ensure that all necessary operating system patches are installed. Also, review the most-recent release information, including system requirements, disk space requirements, and known defects and limitations. See the *IBM Security Access Manager for Web Release Notes* or Technotes in the support knowledge database.
4. Ensure that the registry server and policy server are up and running (in normal mode).
5. Upgrade WebSphere Application Server to 7.0 or 8.0. See the WebSphere documentation for upgrade instructions: http://www-306.ibm.com/software/webservers/appserv/was/library/.
6. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
7. Install the Security Access Manager Session Management Server package. To do so, run the **setup.exe** program in the following directory:

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Follow the online instructions and select to install the following packages:
   - Security Access Manager License
   - Security Access Manager Session Management Server
8. Before you run **smscfg**, run the WebSphere **setupCmdLine.bat** or **setupCmdLine.sh** script for the deployment manager file, depending on your operating system.
9. Deploy the instance:

   ```
   smscfg -action deploy -instance new_instance
   ```

where *new_instance* is the name of the new instance. The new instance name that you specify must be short and use ASCII characters only.

10. Extract the existing Security Access Manager session management server configuration information into a response file:

    ```
    smscfg -action extract -instance TAM60_SMS -record sms_upgrade.rsp
    ```

    Where *60* is the previous version, and *sms_upgrade.rsp* is the name of the response file. The response file is created in the same directory from which **smscfg** is started.

11. **WebSphere Application Server deployment targets**: These settings identify new server or cluster names. If you are deploying to a new set of application servers, and the new server or cluster names are different, you will must update the names in the response file:
    - `clustered`
    - `was_cluster`
    - `was_node`
    - `was_server`

    Note: The response file can also include various file paths and passwords for your environment. For example, `trust_store` *`file_path`*.

12. **Security Access Manager environment server settings**: These settings identify the Security Access Manager policy and authorization servers that are used by the session management server.
    - `policysvr_host`
    - `policysvr_port`
    - `authzsvr`

13. Apply the updated configuration information to the session management server 7.0 instance:

    ```
    smscfg -action config -instance new_instance -rsp_file sms_upgrade.rsp
    ```

    Where *sms_upgrade.rsp* is the name of the response file.

14. Remove the previous session management server instance:

    ```
    smscfg -action unconfigure -instance TAM60_SMS -admin_id sec_master
    -admin_pwd sec_master_password -remove_last_login_db no -interactive no
    ```

    where *60* is the previous version.

15. Remove the instance by uninstalling the `DSess` and `DSessConfig` applications that use the administrative console:
    a. Click **Applications** > **Enterprise Applications** in the administrative console navigation tree to access the Enterprise Applications page.
    b. Uninstall the applications:
       1) Select the **DSess** > **DSessConfig** applications.
       2) Click **Uninstall**.
    c. Save changes that are made to the administrative configuration.

Results

The upgrade of the Session Management Server on Windows is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Chapter 11. Upgrading the session management command line

Security Access Manager supports an upgrade of the session management command line to version 7.0.

Session management command line: Upgrade considerations

Before you upgrade the Security Access Manager session management command-line interface, you must complete the following tasks (as required).

- Upgrade your operating system to the minimum supported level. For information about minimum supported levels, see *IBM Security Access Manager for Web Release Notes*.
- In Tivoli Directory Server version 6.3 FP17, clients can coexist on the same workstation with a client that is version 6.0, 6.1, or 6.2. The Tivoli Directory Server 6.3 FP17 server requires that the version 6.3 client and the Java client are also installed. In addition, the server can coexist on the same workstation with another client that is version 6.0, 6.1, or 6.2, or with a version of the 6.3 server.
- You are not required to upgrade all Security Access Manager components in your secure domain to a 7.0 level. However, if you upgrade any Security Access Manager component on a system, all components must be upgraded on that system to the 7.0 level, and you must install Tivoli Directory Server client 6.3 FP17 on that system.

  For a list of components that are compatible with Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.
- If Tivoli Directory Server is your registry server and is *on a different machine* from any Security Access Manager component, you can upgrade the registry server at any time, either before or after the upgrade of the Security Access Manager 7.0 component.

  However, when the server package of Tivoli Directory Server is installed *on the same machine* as any Security Access Manager 7.0 component and if you choose to install the server package of Tivoli Directory Server 6.3 FP17, install the Tivoli Directory Server 6.3 FP17 client and server packages at the same time as you install the Security Access Manager 7.0 component on that machine.
- Windows systems upgrades are supported using a two system upgrade.
- If you use a language other than English, upgrade your language package. See the *IBM Security Access Manager for Web Installation Guide* to install the language package. When you upgrade the IBM Tivoli Directory Server language packages, use the upgrade (**-U**) option for Linux operating systems.

AIX: Upgrading the session management command line

Upgrade your existing session management command line to the Security Access Manager, version 7.0, session management command line on AIX.

Procedure

1. Before you upgrade the command-line system to 7.0, review the considerations in "Session management command line: Upgrade considerations."
2. Log in as `root`.

© Copyright IBM Corp. 2003, 2012

3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.

   Note: The AIX operating system requires version 10.1 or later of the `xlC` file set. Check your current version by using the **lslpp** command and upgrade, if necessary.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```
6. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
7. Use the **pdbackup** utility to back up critical information:

   ```
   /opt/PolicyDirector/bin/pdbackup-action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Specifies the fully qualified path to the list file. There are two backup list files to back up: the Tivoli Access Manager backup list file and the Session Management Server Command Line backup list file. For example:
   - The Tivoli Access Manager backup list file:

     ```
     /opt/PolicyDirector/etc/pdbackup.lst
     ```
   - The Session Management Server Command Line backup list file:

     ```
     /opt/pdsms/etc/pdinfo-pdsmscli.lst
     ```

   –path *path*
   Specifies the path where you want the backed up files to be stored.

   For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the *list_date.time*`.tar` default file name.

   For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.
8. Install the Global Security Kit (GSKit):

   ```
   installp -acgYXd image_path/usr/sys/inst.images GSKit8.gskcrypt64.ppc.rte
   installp -acgYXd image_path/usr/sys/inst.images GSKit8.gskssl64.ppc.rte
   ```

   where *image_path*`/usr/sys/inst.images` is the directory where the installation images are located.
9. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/usr/sys/inst.images/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
10. Install the Tivoli Directory Server client packages:

    ```
    installp -acgYXd image_path/usr/sys/inst.images packages
    ```

where *image_path*/usr/sys/inst.images is the directory where the installation images are located and where *packages* are the names of the Tivoli Directory Server client packages:

License package	idsldap.license63
Client base package	idsldap.cltbase63
Client package (64-bit) (no SSL)	idsldap.clt64bit63
Client package (64-bit) (SSL)	idsldap.clt_max_crypto64bit63
Java Client package	idsldap.cltjava63

11. Ensure that your registry server is running.
12. Run the isamLicense license script by completing the following actions:
    a. In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the isamLicense script:

       ```
       isamLicense
       ```

       Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:

       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

       -t Test: Silently tests whether the current license is already installed. Returns an exit status 0 (SUCCESS) if it is.

       -? Help: Displays the syntax of the script file.
    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
13. Upgrade the Security Access Manager license:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.lic
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located.
14. Upgrade IBM Security Utilities:

    ```
    installp -acgYXd image_path/usr/sys/inst.images TivSec.Utl
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located.
15. Upgrade the Security Access Manager runtime:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.RTE
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and PD.RTE is the Security Access Manager runtime package.
16. Upgrade the Security Access Manager authorization server package:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.Acld
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and PD.Acld is the Security Access Manager authorization server package.

17. Upgrade the Security Access Manager Session Management Command Line package:

    ```
    installp -acgYXd image_path/usr/sys/inst.images PD.SMSCLI
    ```

    where *image_path*/usr/sys/inst.images is the directory where the installation images are located, and PD.SMSCLI is the Security Access Manager Session Management Command Line package.
18. If the two-system upgrade option was used for the policy server, the master-host record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

    Edit the master-host entry in the following configuration files:

    - /opt/PolicyDirector/etc/pd.conf
    - /opt/PolicyDirector/etc/ivacld.conf

Results

The upgrade of the session management command line on AIX is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Linux on x86-64: Upgrading the session management command line

Upgrade your existing session management command line to the Security Access Manager, version 7.0, session management command line on Linux x86-64.

Procedure

1. Before you upgrade the session management command line to 7.0, review the considerations in "Session management command line: Upgrade considerations" on page 161.
2. Log in as root.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Change to the following directory:

    ```
    cd image_path/linux_x86
    ```

    where *image_path* is where the installation images are located.
6. Stop all Tivoli Access Manager applications and services:

    ```
    pd_start stop
    ```
7. Confirm that all Tivoli Access Manager services and applications are stopped:

    ```
    pd_start status
    ```

    If any Tivoli Access Manager service or application is still running, issue the **kill** command:

    ```
    kill –9 daemon_process_id
    ```
8. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

    ```
    /opt/PolicyDirector/bin/pdbackup -action backup
     -list fullpath_to_backup_listfile
    -path path -file filename
    ```

where:

–list *fullpath_to_backup_listfile*
Where *fullpath_to_backup_listfile* specifies the fully qualified path to the list file. There are two backup list files to back up: the Tivoli Access Manager backup list file and the Session Management Server Command Line backup list file. For example:

- The Tivoli Access Manager backup list file:
  `/opt/PolicyDirector/etc/pdbackup.lst`
- The Session Management Server Command Line backup list file:
  `/opt/pdsms/etc/pdinfo-pdsmscli.lst`

–path *path*
Specifies the path where you want the backed up files to be stored. For example:
`/var/PolicyDirector/pdbackup`

–file *filename*
Specifies a file name other than the *list_date.time*.tar default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

9. Upgrade the IBM Global Security Kit (GSKit):
```
rpm -U gskcrypt64-8.0.14.26.linux.x86_64
rpm -U gskssl64-8.0.14.26.linux.x86_64
```
10. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_x86/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
11. Install the Tivoli Directory Server client packages:
```
rpm -i packages
```
where *packages* are as follows:

License package	`idsldap-license63-6.3.0-17.x86_64.rpm`
Base client package	`idsldap-cltbase63-6.3.0-17.x86_64.rpm`
64-bit client package	`idsldap-clt64bit63-6.3.0-17.x86_64.rpm`
Java client package	`idsldap-cltjava63-6.3.0-17.x86_64.rpm`

12. Ensure that your registry server is running.
13. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:
```
isamLicense
```
Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

-q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

-f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

-t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

-? Help: Displays the syntax of the script file.

c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

d. Accept the license by pressing **1**.

14. Upgrade the Security Access Manager license:

    ```
    rpm -U PDlic-PD-7.0.0-0.x86_64.rpm
    ```

    where `PDlic-PD-7.0.0-0.x86_64.rpm` is the Security Access Manager license package.

15. Upgrade IBM Security Utilities:

    ```
    rpm -U TivSecUtl-TivSec-7.0.0-0.x86_64.rpm
    ```

    where `TivSecUtil-TivSec-7.0.0-0.x86_64.rpm` is the IBM Security Utilities package.

16. Upgrade the Security Access Manager runtime:

    ```
    rpm -U PDRTE-PD-7.0.0-0.x86_64.rpm
    ```

    where `PDRTE-PD-7.0.0-0.x86_64.rpm` is the Security Access Manager runtime package.

17. Upgrade Security Access Manager authorization server package:

    ```
    rpm -U PDAcld-PD-7.0.0-0.x86_64.rpm
    ```

18. Upgrade the Security Access Manager Session Management Command Line package:

    ```
    rpm -U PDSMS-CLI-7.0.0-0.x86_64.rpm
    ```

19. If the two-system upgrade option was used for the policy server, the `master-host` record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

    Edit the `master-host` entry in the following configuration files:

    - `/opt/PolicyDirector/etc/pd.conf`
    - `/opt/PolicyDirector/etc/ivacld.conf`

Results

The upgrade of a development system for Linux on x86-64 is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Linux on System z: Upgrading the session management command line

Upgrade your existing session management command line to the Security Access Manager, version 7.0, session management command line on Linux on System z.

Procedure

1. Before you upgrade the session management command line to 7.0, review the considerations in "Session management command line: Upgrade considerations" on page 161.
2. Log in as `root`.

3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage on the System z system.
5. Change to the following directory:

   ```
   cd image_path/linux_s390
   ```

   Where *image_path* is where the installation images are located. The `.rpm` files are in the `/image_path/linux_s390` directory.
6. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```
7. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```
8. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Where *fullpath_to_backup_listfile* specifies the fully qualified path to the list file. There are two backup list files to back up: the Tivoli Access Manager backup list file, and the Session Management Server Command Line backup list file. For example:
   - The Tivoli Access Manager backup list file:

     ```
     /opt/PolicyDirector/etc/pdbackup.lst
     ```
   - The Session Management Server Command Line backup list file:

     ```
     /opt/pdsms/etc/pdinfo-pdsmscli.lst
     ```

   –path *path*
   Specifies the path where you want the backed up files to be stored. For example:

   ```
   /var/PolicyDirector/pdbackup
   ```

   –file *filename*
   Specifies a file name other than the *list_date.time*`.tar` default file name.

   For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.
9. Upgrade the IBM Global Security Kit (GSKit):

   ```
   rpm -U gskcrypt64-8.0.14.26.linux.s390x.rpm
   rpm -U gskssl64-8.0.14.26.linux.s390x.rpm
   ```
10. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/linux_s390/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
11. Install the Tivoli Directory Server client packages:

    ```
    rpm -i packages
    ```

    where *packages* are as follows:

License package	idsldap-license63-6.3.0-17.s390.rpm
Base client package	idsldap-cltbase63-6.3.0-17.s390.rpm
64-bit client package	idsldap-clt64bit63-6.3.0-17.s390x.rpm
Java client package	idsldap-cltjava63-6.3.0-17.s390.rpm

12. Ensure that your registry server is running.
13. Run the isamLicense license script by completing the following actions:
    a. In a command window, change to the *image_path*/scripts directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the isamLicense script:
       ```
       isamLicense
       ```
       Note: When you accept the license, you agree to its terms and conditions. The isamLicense script has the following optional options:
       -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.
       -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.
       -t Test: Silently tests whether the current license is already installed. Returns an exit status 0 (SUCCESS) if it is.
       -? Help: Displays the syntax of the script file.
    c. Read the license by pressing press **Enter** on each page to view the complete license agreement.
    d. Accept the license by pressing **1**.
14. Upgrade the Security Access Manager license:
    ```
    rpm -U PDlic-PD-7.0.0-0.s390x.rpm
    ```
    where PDlic-PD-7.0.0-0.s390x.rpm is the Security Access Manager license package.
15. Upgrade IBM Security Utilities:
    ```
    rpm -U TivSecUtl-TivSec-7.0.0-0.s390x.rpm
    ```
    where TivSecUtil-TivSec-7.0.0-0.s390x.rpm is the IBM Security Utilities package.
16. Upgrade the Security Access Manager runtime:
    ```
    rpm -U PDRTE-PD-7.0.0-0.s390x.rpm
    ```
    where PDRTE-PD-7.0.0-0.s390x.rpm is the Security Access Manager runtime package.
17. Upgrade the Security Access Manager authorization server package:
    ```
    rpm -U PDAcld-PD-7.0.0-0.s390x.rpm
    ```
    where PDAcld-PD-7.0.0-0.s390x.rpm is the Security Access Manager runtime package.
18. Upgrade the Security Access Manager Session Management Command Line package:
    ```
    rpm -U PDSMS-CLI-7.0.0-0.s390x.rpm
    ```
    where PDSMS-CLI-7.0.0-0.s390x.rpm is the Security Access Manager Session Management Command Line package.

19. If the two-system upgrade option was used for the policy server, the `master-host` record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

    Edit the `master-host` entry in the following configuration files:

    - `/opt/PolicyDirector/etc/pd.conf`
    - `/opt/PolicyDirector/etc/ivacld.conf`

Results

The upgrade of a session management command line for Linux on System z is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Solaris: Upgrading the session management command line

Upgrade your existing session management command line to the Security Access Manager, version 7.0, session management command line on Solaris.

Procedure

1. Before you upgrade the session management command line to 7.0, review the considerations in "Session management command line: Upgrade considerations" on page 161.
2. Log in as `root`.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Stop all Tivoli Access Manager applications and services:

   ```
   pd_start stop
   ```

6. Confirm that all Tivoli Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Tivoli Access Manager service or application is still running, issue the **`kill`** command:

   ```
   kill –9 daemon_process_id
   ```

7. Use the **`pdbackup`** utility to back up critical Tivoli Access Manager information:

   ```
   /opt/PolicyDirector/bin/pdbackup -action backup
    -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Where *fullpath_to_backup_listfile* specifies the fully qualified path to the list file. There are two backup list files to back up: the Security Access Manager backup list file and the Session Management Server Command Line backup list file. For example:

   - The Security Access Manager backup list file:

     ```
     /opt/PolicyDirector/etc/pdbackup.lst
     ```

   - The Session Management Server Command Line backup list file:

     ```
     /opt/pdsms/etc/pdinfo-pdsmscli.lst
     ```

–path *path*
Specifies the path where you want the backed up files to be stored. For example:
`/var/PolicyDirector/pdbackup`

–file *filename*
Specifies a file name other than the `pdbackup.lst`*`list_date.time`*`.tar` default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

8. Install the Global Security Kit (GSKit):
```
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8cry64
pkgadd -d /image_path/solaris -a /image_path/solaris/pddefault -G gsk8ssl64
```
where /*image_path*`/solaris` specifies the location of the installation images, and /*image_path*`/solaris/pddefault` specifies the location of the installation administration script. The `-G` option ensures that the package is added in the current zone only.
9. Install the Tivoli Directory Server license files by running the `idsLicense` script in the *image_path*`/solaris/tdsLicense/license` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
10. Install the Tivoli Directory Server client packages:
```
pkgadd -d /image_path>/solaris/packages
-a /image_path/solaris/pddefault
```
where /*image_path*`/solaris` specifies the location of the installation images, /*image_path*`/solaris/pddefault` specifies the location of the installation administration script, and *packages* are as follows:

License package	`idsldap.license63.pkg`
Base client package	`idsldap.cltbase63.pkg`
64-bit client package	`idsldap.clt64bit63.pkg`
Java client package	`idsldap.cltjava63.pkg`

11. Ensure that your registry server is running.
12. Run the `isamLicense` license script by completing the following actions:
    a. In a command window, change to the *image_path*`/scripts` directory, where *image_path* is the path to the DVD image, or where you downloaded the archive file from Passport Advantage.
    b. Run the `isamLicense` script:
    ```
    isamLicense
    ```
    Note: When you accept the license, you agree to its terms and conditions. The `isamLicense` script has the following optional options:

    -q Quiet: Runs the script without displaying the license. When you use this option, you automatically accept the license without viewing it.

    -f Force: Forces the license to be displayed and prompts you to accept it even if the license is already installed.

    -t Test: Silently tests whether the current license is already installed. Returns an `exit status 0 (SUCCESS)` if it is.

    -? Help: Displays the syntax of the script file.

c. Read the license by pressing press **Enter** on each page to view the complete license agreement.

d. Accept the license by pressing **1**.

13. Upgrade the Security Access Manager license:

```
pkgadd -d /image_path/solaris
-a /image_path/solaris/pddefault -G PDlic
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDlic is the Security Access Manager license package. The -G option ensures that the package is added in the current zone only.

14. Upgrade IBM Security Utilities:

```
pkgadd -d /image_path/solaris
-a /image_path/solaris/pddefault -G TivSecUtl
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and TivSecUtl is the IBM Security Utilities package. The -G option ensures that the package is added in the current zone only.

15. Upgrade the Security Access Manager runtime:

```
pkgadd -d /image_path/solaris
-a /image_path/solaris/pddefault -G PDRTE
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDRTE is the Security Access Manager runtime package. The -G option ensures that the package is added in the current zone only.

16. Upgrade the Security Access Manager authorization server package:

```
pkgadd -d /image_path/solaris
-a /image_path/solaris/pddefault -G PDAcld
```

where /*image_path*/solaris specifies the location of the installation images, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDAcld is the Security Access Manager authorization server package. The -G option ensures that the package is added in the current zone only.

17. Upgrade the session management command-line package:

```
pkgadd -d /image_path/solaris
-a /image_path/solaris/pddefault -G PDSMSCLI
```

where /*image_path*/solaris specifies the location of the package, /*image_path*/solaris/pddefault specifies the location of the installation administration script, and PDSMSCLI is the session management command-line package. The -G option ensures that the package is added in the current zone only.

18. If the two-system upgrade option was used for the policy server, the master-host record must be updated to point to the new policy server.

    Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

    Edit the master-host entry in the following configuration files:

    - /opt/PolicyDirector/etc/pd.conf
    - /opt/PolicyDirector/etc/ivacld.conf

Results

The upgrade of a session management command-line system on Solaris is now complete. Perform any necessary application-specific tasks before you start Security Access Manager applications.

Windows: Upgrading the session management command line

Upgrade your existing session management command line to the Security Access Manager, version 7.0, session management command line on Windows.

About this task

Note: Windows upgrades are supported on a two-system upgrade approach only.

Procedure

1. Before you upgrade the session management command line to 7.0, review the considerations in "Session management command line: Upgrade considerations" on page 161.
2. Log in as a user with administrative privileges.
3. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
4. Access the product DVD or extract the files from the archive file that you downloaded from Passport Advantage.
5. Exit all running programs. During the upgrade process, you are prompted to restart your Windows system periodically.
6. Stop all Tivoli Access Manager applications and services. For example, on Windows 2008 systems, select **Start** > **Control Panel** > **Administrative Tools**. Double-click the **Services** icon, and stop all Tivoli Access Manager services that run on the local system, including applications, such as WebSEAL.

   From **Services**, find the **Access Manager Auto-Start Service**. Double-click this service and change the startup type to **Disabled**.
7. Use the **pdbackup** utility to back up critical Tivoli Access Manager information:

   ```
   "C:\Program Files\bin\pdbackup"
    -action backup -list fullpath_to_backup_listfile
   -path path -file filename
   ```

   where:

   –list *fullpath_to_backup_listfile*
   Where *fullpath_to_backup_listfile* specifies the fully qualified path to the list file. There are two backup list files to back up: the Tivoli Access Manager backup list file and the Session Management Server Command Line backup list file. For example:

   - The Tivoli Access Manager backup list file:

     ```
     "C:\Program Files\Tivoli\Policy Director\etc\pdbackup.lst"
     ```

   - The Session Management Server Command Line backup list file:

     ```
     "C:\Program Files\Tivoli\pdsms\etc\pdinfo-pdsmscli.lst"
     ```

   –path *path*
   Specifies the path where you want the backed up files to be stored. For example:

   ```
   "C:\Program Files\Tivoli\Policy Director\pdbackup"
   ```

–file *filename*
Specifies a file name other than the *list_date.time*.dar default file name.

For more information about the **pdbackup** utility, see "Upgrade utilities," on page 197.

8. Install the Global Security Kit (GSKit). To do so, change to the \windows\GSKit directory on the drive where the installation images are located and enter:
   gsk8ssl64
   Follow online instructions to complete installation.
9. If you are using an LDAP server as your registry, install the Tivoli Directory Server client by running the **install_tds.exe** file in windows\tds_client64. Select to install **C Client 6.3** and **Java Client 6.3** and follow the online instructions to complete the installation.

   Note: If you are using Active Directory as your registry, and the Security Access Manager systems in your domain are Windows, the Tivoli Directory Server client is not required.
10. Install the security utilities by running the **setup.exe** script in the \windows\TivSecUtl\Disk Images\Disk1 directory. Follow the online instructions to complete the installation.
11. Install the components by running the **setup.exe** script in the \windows\PolicyDirector\Disk Images\Disk1 directory. Select to install the following components in this sequence:
    - **Security Access Manager license**
    - **Security Access Manager runtime**
    - **Security Access Manager authorization server**
    - **Security Access Manager Session Management Command Line**

    Follow online instructions to complete installation.
12. Start all Security Access Manager applications and services. For example, on Windows 2008 systems, select **Start** > **Control Panel** > **Administrative Tools**, and then double-click the **Services** icon. Start all Security Access Manager services that run on the local system, including applications, such as WebSEAL.

    From **Services**, find the **Security Access Manager Auto-Start Service**. Double-click this service and change the startup type to **Automatic**.

Results

The upgrade of a development system on Windows is now complete.

Chapter 12. Upgrading the session management Web interface

The Session Management Server console replaced the session management Web interface in Tivoli Access Manager 6.1. There is no upgrade path for the session management Web interface.

The Session Management Server console is a graphical user interface that is on the WebSphere Application Server, and is installed as an extension to the administrative console.

See the *IBM Security Access Manager for Web Installation Guide* and *IBM Security Access Manager for Web Shared Session Management Administration Guide* for more information about the Session Management Server console.

© Copyright IBM Corp. 2003, 2012

Chapter 13. Upgrading a plug-in for Web servers

Before you begin

Decide what type of upgrade you want to complete:

- An in-place upgrade on a supported existing system.
- A two-system upgrade.

You can complete an in-place upgrade only if you are upgrading one of the following existing environments:

- Tivoli Access Manager Plug-in for Web Servers 6.1.1 for 64-bit Apache on Linux on System x.
- Tivoli Access Manager Plug-in for Web Servers 6.1.1 for 64-bit Apache on System z.

All other configurations require the two-system upgrade approach. That is, you have an *original* Plug-in for Web Server system that you want to upgrade and a new *target* system to host the upgraded environment. The two system upgrade approach involves the following high-level steps:

1. Complete a new Plug-in for Web Servers 7.0 installation on the 64-bit server.
2. Manually migrate the legacy Plug-in for Web Servers configuration to the new environment.

About this task

Follow these instructions to complete an upgrade on a Plug-in for Web Server environment. Each step applies to both upgrade types unless stated otherwise.

Complete each step on the target system that is to host Plug-in for Web Server version 7.0 environment unless stated otherwise.

Attention: Upgrade the session management server before you upgrade WebSEAL and Web Plug-in servers. See Chapter 10, “Upgrading the session management server,” on page 141.

Procedure

1. Log in as `root` or as an administrative user.
2. Install all of the operating system patches that are required by Security Access Manager 7.0. For required operating system patches, see the *IBM Security Access Manager for Web Release Notes*.
3. On the Security Access Manager policy server host, complete the following steps:
   a. Ensure that the policy server for the secure domain is upgraded to version 7.0. For instructions, see Chapter 3, “Upgrading the policy server,” on page 21.
   b. Confirm that the policy server is running:
      ```
      pd_start status
      ```
   c. Make sure that you can contact the policy server. For example, log on to the **pdadmin** interface and run the following commands:

© Copyright IBM Corp. 2003, 2012

```
pdadmin -a sec_master -p password
pdadmin sec_master> acl list
```

If you cannot log in, do not proceed with the upgrade of the Web Server plug-in. Resolve the login problem before you continue.

4. If you are completing an in-place upgrade, skip to 5. If you are completing a two-system upgrade, stop the Web server and any Security Access Manager services that are running on the original system.
   - On AIX, Linux, and Solaris operating systems, enter the following command:

     ```
     pd_start stop
     ```
   - On Windows, use the Control Panel:

     For example, on Windows 2008 systems: Select **Start** > **Control Panel** > **Administrative Tools**. Double-click the **Services** icon, and stop the services.
5. Install Plug-in for Web version 7.0 and other prerequisite components on the target system. For installation instructions, see the *IBM Security Access Manager for Web Installation Guide*. The prerequisite components include:
   - Global Security Kit
   - IBM Tivoli Directory Server (depending on the user registry used)
   - IBM Security Utilities
   - Security Access Manager license
   - Security Access Manager runtime
   - Security Access Manager Web Security runtime
   - Security Access Manager Plug-in for Web Servers
   - One of the following plug-ins, depending on the Web server used:
     - Security Access Manager Plug-in for Apache Web Server
     - Security Access Manager Plug-in for HTTP Server
     - Security Access Manager Plug-in for Internet Information Services
6. (*In-place upgrade only*) If you used the two-system upgrade option for the policy server, the `master-host` record on the original Plug-in for Web Server system must be updated to point to the new policy server.

   Note: The two-system upgrade option can be used only if the registry server is an LDAP server.

   Edit the `master-host` entry in each of the following configuration files:
   - Security Access Manager Runtime

     install_path`/etc/pd.conf`
   - Security Access Manager Plug-in for Web Servers

     install_path`/etc/pdwebpi.conf`
7. (*In-place upgrade only*) If you are performing an in-place upgrade, you must manually update the path of the Web Plug-in library (`pdwebpi_module`) in your Apache `httpd.conf` file. Replace the existing library path:

   ```
   LoadModule pdwebpi_module /opt/pdwebpi/lib/libpdwpi-apache22-lib64.so
   ```

   with the new path:

   ```
   LoadModule pdwebpi_module /opt/pdwebpi/lib/libpdwpi-apache22.so
   ```

   Note: You must restart the Web Server for this change to take effect.
8. (*Two-system upgrade only*) Use the **pdconfig** utility to configure the new Plug-in for Web Server version 7.0 environment as described in the *IBM Security*

Access Manager for Web Installation Guide. You must manually migrate the configuration from your original system to this new environment.

9. (*In-place upgrade only*) Start the Web Server plug-in process:
   - On AIX, Linux, or Solaris, enter:

     ```
     pd_start start
     ```
   - On Windows:

     For example, on Windows 2008 systems, select **Start** > **Control Panel** > **Administrative Tools**. Double-click the **Services** icon, and start the service.
10. Verify that you can contact the upgraded 7.0 policy server. For example, log on to the **pdadmin** interface and run a command:

    ```
    pdadmin -a sec_master -p password
    pdadmin sec_master> acl list
    ```

Results

If you completed an in-place upgrade, the existing system is upgraded to a configured Plug-in for Web Server version 7.0 installation. You do not need to run **pdconfig** to configure components.

If you completed a two-system upgrade, Plug-in for Web Server version 7.0 is installed and configured on the new server.

Chapter 14. Upgrading Web Portal Manager

Upgrade of a previous Web Portal Manager system is not supported. You must install Web Portal Manager 7.0.

For instructions on installing Web Portal Manager, see the *IBM Security Access Manager for Web Installation Guide*.

If your current version of WebSphere Application Server is not supported for Security Access Manager 7.0, upgrade your WebSphere Application Server version to a supported level. See the *IBM Security Access Manager for Web Release Notes* for information about supported WebSphere Application Server versions. For upgrade instructions, see the WebSphere Application Server documentation.

© Copyright IBM Corp. 2003, 2012

Chapter 15. Restoring a system to its prior level

If problems occur when you upgrade to Security Access Manager 7.0 from a previous version, this section describes how to restore these types of Security Access Manager systems:

- Policy server
- WebSEAL

Restoring the policy server

If problems occur when you upgrade to Security Access Manager 7.0 from a previous version, you can restore the policy server to a previous version.

AIX: Restoring the policy server

Restore your policy server to a prior level if you encounter a problem when you migrate to the Security Access Manager, version 7.0, policy server on AIX.

About this task

If you encounter a problem when you migrate to Security Access Manager 7.0, you can restore the policy server to its prior Tivoli Access Manager level.

Notes:

- If you encounter a problem during the backup of existing data, contact IBM Support for assistance before you continue with the upgrade process.
- For supported operating system information, required patches and fix pack information for Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.

Procedure

1. Stop all Security Access Manager applications and services:

   ```
   pd_start stop
   ```

2. Confirm that all Security Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Security Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```

   CAUTION:

   If your backup file is in the `opt` or `var` directory, move it out of the directory or it will be deleted when you complete step 3.

3. Remove, but do *not* unconfigure, the Security Access Manager policy server component and prerequisite packages. From the command line:

   a. Enter: `rm –rf /opt/PolicyDirector/.configure/*`

   b. Enter: `rm /opt/PolicyDirector/etc/pd.conf`

   c. Enter: `installp -u -g packages`

© Copyright IBM Corp. 2003, 2012

Note: Use the **–g** option only if you want dependent software for the specified package removed.

where *packages* can be any of the following packages:
- `PD.Mgr` for the Security Access Manager policy server
- `PD.RTE` for the Security Access Manager runtime
- `PD.lic` for the Security Access Manager license
- `TivSec.Utl` for the IBM Security Utilities

4. **For single system upgrade only:** Use your previous Tivoli Access Manager 6.x version DVD or product image, and install the policy server system, which includes the prerequisite components such as the Global Security Kit, Tivoli Directory Server client, and Tivoli Access Manager runtime. For instructions, see the *Tivoli Access Manager Installation Guide* for your particular version.
5. **For single system upgrade only:** Apply any Tivoli Access Manager fix pack that was on the system before the upgrade to version 7.0.
6. On the original system, restore your previous data by completing the following tasks:
   a. Restore your Tivoli Access Manager data with the **pdbackup** `-action restore -file` *filename* utility, where *filename* is the archive file that is created during the **pdbackup** `-action backup` of your original data.

      For more information, see "pdbackup" on page 205.
   b. Restore your user registry data. See the documentation for your user registry for information about restoring the registry to a previous level.
7. Start the policy server daemon (`pdmgrd`):

   ```
   pd_start start
   ```

Linux on x86-64: Restoring the policy server

Restore your policy server to a prior level if you encounter a problem when you migrate to the Security Access Manager, version 7.0, policy server on Linux on x86-64.

About this task

If you encounter a problem when you migrate to Security Access Manager 7.0, you can restore the policy server to its prior Tivoli Access Manager level.

Notes:
- If you encounter a problem during the backup of existing data, contact IBM Support for assistance before you continue with the upgrade process.
- For supported operating system information, required patches and fix pack information for Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.

Procedure

1. Stop all Security Access Manager applications and services:

   ```
   pd_start stop
   ```
2. Confirm that all Security Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Security Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```

CAUTION:

If your backup file is in the `opt` or `var` directory, move it out of the directory or it will be deleted when you complete step 3.

3. Remove, but do *not* unconfigure, the Security Access Manager policy director component and prerequisite packages. From the command line:
   a. Enter: `rm –rf /opt/PolicyDirector/.configure/*`
   b. Enter: `rm /opt/PolicyDirector/etc/pd.conf`
   c. Enter: `rpm -e packages`

      where *packages* can be any of the following packages:
      - `PDMgr-PD-7.0.0-0` for the Security Access Manager policy server
      - `PDRTE-PD-7.0.0-0` for the Security Access Manager runtime
      - `PDlic-PD-7.0.0-0` for the Security Access Manager license
      - `TivSecUtl-TivSec-7.0.0-0` for the IBM Security Utilities
4. **For single system upgrade only:** Use your previous Tivoli Access Manager 6.x version DVDs and install the prerequisite components for the policy server, such as the Global Security Kit, Tivoli Directory Server client, and Tivoli Access Manager runtime. For instructions, see the *Tivoli Access Manager Installation Guide* for your particular version.
5. **For single system upgrade only:** Apply any Tivoli Access Manager fix pack that was on the system before the upgrade to version 7.0.
6. On the original system, restore your previous data by completing the following tasks:
   a. Restore your Tivoli Access Manager data with the **`pdbackup -action restore -file filename`** utility, where *filename* is the archive file that is created during the **`pdbackup -action backup`** of your original data.

      For more information, see “pdbackup” on page 205.
   b. Restore your user registry data. See the documentation for your user registry for information about restoring the registry to a previous level.
7. Start the policy server daemon (`pdmgrd`):

   ```
   pd_start start
   ```

Linux on System z: Restoring the policy server

Restore your policy server to a prior level if you encounter a problem when you migrate to the Security Access Manager, version 7.0, policy server on Linux on System z.

About this task

If you encounter a problem when you migrate to Security Access Manager 7.0, you can restore the policy server to its prior Tivoli Access Manager level.

Notes:

- If you encounter a problem during the backup of existing data, contact IBM Support for assistance before you continue with the upgrade process.
- For supported operating system information, required patches and fix pack information for Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.

Procedure

1. Stop all Security Access Manager applications and services:

   ```
   pd_start stop
   ```

2. Confirm that all Security Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Security Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```

   CAUTION:

   If your backup file is in the opt or var directory, move it out of the directory or it will be deleted when you complete step 3.

3. Remove, but do *not* unconfigure, the Security Access Manager component and prerequisite packages. From the command line:
   a. Enter: `rm –rf /opt/PolicyDirector/.configure/*`
   b. Enter: `rm /opt/PolicyDirector/etc/pd.conf`
   c. Enter: `rpm -e --noscripts` *packages* where *packages* can be any of the following packages:
      - `PDMgr-PD-7.0.0-0` for the Security Access Manager policy server
      - `PDRTE-PD-7.0.0-0` for the Security Access Manager runtime
      - `PDlic-PD-7.0.0-0` for the Security Access Manager license
      - `TivSecUtl-TivSec-7.0.0-0` for the IBM Security Utilities
4. **For single system upgrade only:** Use your previous Tivoli Access Manager 6.x version DVDs and install the policy server system, which includes the prerequisite components such as the Global Security Kit, Tivoli Directory Server client, and Tivoli Access Manager runtime. For instructions, see the *Tivoli Access Manager Installation Guide* for your particular version.
5. **For single system upgrade only:** Apply any Tivoli Access Manager fix pack that was on the system before the upgrade to version 7.0.
6. On the original system, restore your previous data by completing the following tasks:
   a. Restore your Tivoli Access Manager data with the **pdbackup** `-action restore -file` *filename* utility, where *filename* is the archive file that is created during the **pdbackup** `-action backup` of your original data.

      For more information, see “pdbackup” on page 205.
   b. Restore your user registry data. See the documentation for your user registry for information about restoring the registry to a previous level.
7. Start the policy server daemon (`pdmgrd`):

   ```
   pd_start start
   ```

Solaris: Restoring the policy server

Restore your policy server to a prior level if you encounter a problem when you migrate to the Security Access Manager, version 7.0, policy server on Solaris.

About this task

If you encounter a problem when you migrate to Security Access Manager, version 7.0, you might need to restore the system to its prior Tivoli Access Manager level.

Notes:

- If you encounter a problem during the backup of existing data, contact IBM Support for assistance before you continue with the upgrade process.
- For supported operating system information, required patches and fix pack information for Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.

Procedure

1. Stop all Security Access Manager applications and services:

   ```
   pd_start stop
   ```

2. Confirm that all Security Access Manager services and applications are stopped:

   ```
   pd_start status
   ```

   If any Security Access Manager service or application is still running, issue the **kill** command:

   ```
   kill –9 daemon_process_id
   ```

   CAUTION:

   If your backup file is in the opt or var directory, move it out of the directory or it will be deleted when you complete step 3.

3. Remove, but do *not* unconfigure, the Security Access Manager policy server component and prerequisite packages. To do so, from the command line:
   a. Enter: `rm –rf /opt/PolicyDirector/.configure/*`
   b. Enter: `rm /opt/PolicyDirector/etc/pd.conf`
   c. Enter: `pkgrm packages` where *packages* can be any of the following packages:
      - `PDMgr` for the Security Access Manager policy server
      - `PDRTE` for the Security Access Manager runtime
      - `PDlic` for the Security Access Manager license
      - `TivSecUtl` for the IBM Security Utilities

   Note: When prompted to confirm the removal of these components, enter `y`.

4. **For single system upgrade only:** Use your previous Tivoli Access Manager 6.x version DVDs and install the policy server system, which includes the prerequisite components such as the Global Security Kit, Tivoli Directory Server client, and Tivoli Access Manager runtime. For instructions, see the *Tivoli Access Manager Installation Guide* for your particular version.
5. **For single system upgrade only:** Apply any Tivoli Access Manager fix pack that was on the system before the upgrade to version 7.0.
6. On the original system, restore your previous data by completing the following tasks:
   a. Restore your Tivoli Access Manager data with the **pdbackup** `-action restore -file filename` utility, where *filename* is the archive file that is created during the **pdbackup** `-action backup` of your original data.

      For more information, see “pdbackup” on page 205.

   b. Restore your user registry data. See the documentation for your user registry for information about restoring the registry to a previous level.
7. Start the policy server daemon (`pdmgrd`):

   ```
   pd_start start
   ```

Windows: Restoring the policy server

Restore your policy server to a prior level if you encounter a problem when you migrate to the Security Access Manager, version 7.0, policy server on Windows.

About this task

If you have an issue with the version 7.0 policy server during the Windows two-system upgrade, *retire* the 7.0 policy server and return to your original policy server. See "Windows: Retiring the original policy server" on page 56.

If you have issues with your original Tivoli Access Manager policy server, restore it to a working state by following this procedure. This procedure *restores* the policy server to its previous level.

Procedure

1. Stop all Security Access Manager applications and services. For example, on Windows 2008 systems:
   a. Select **Start** > **Control Panel** > **Administrative Tools**
   b. Double-click the **Services** icon.
   c. Stop all Security Access Manager services that run on the local system, including applications, such as WebSEAL.
   d. From **Services**, double-click **Security Access Manager**.
   e. Change the startup type to **Disabled**.

   CAUTION:

   If your backup file is in the Security Access Manager installation directory, move it out of the directory now because step 2 deletes it.
2. **Do not** unconfigure the Security Access Manager policy server. Take the following steps to remove it and its components and prerequisite packages:
   a. Select **Start** > **Run**.
   b. Type `regedit` in the entry field.
   c. Click **OK** to open the registry.
   d. Click **My Computer** > **HKEY_LOCAL_MACHINE** > **Tivoli** > **Policy Director Runtime** > **6.x**.
   e. Change the configuration value from `Yes` to `No`.
   f. Click **My Computer** > **HKEY_LOCAL_MACHINE** > **Tivoli** > **Policy Director Management Server** > **6.x.**.
   g. Change the configuration value from `Yes` to `No`.
   h. Delete the `pd.conf` file from the *`install_path`*`\etc` directory. For example:
      `C:\Program Files\Tivoli\Policy Director\etc\pd.conf`
   i. Log on as a Windows user with administrator privilege.
   j. Remove the following components:
      - Security Access Manager policy server
      - Security Access Manager runtime
      - Security Access Manager license
      - IBM Security Utilities

      For example, on Windows 2008, click **StartControl Panel** and double-click the **Add/Remove Programs** icon.
   k. Select each component from the list and continue the process until all the components are removed.
   l. Click **OK** to exit the program.
3. Restore your previous data by completing the following tasks:

a. Restore your Tivoli Access Manager data with the **pdbackup** `-action restore -file` *`filename`* utility, where *filename* is the archive file that is created during the **pdbackup** `-action backup` of your original data.

   For more information, see "pdbackup" on page 205.

   Note: The **pdbackup** utility requires user input on Tivoli Access Manager 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

b. Restore your user registry data. See the documentation for your user registry for information about restoring the registry to a previous level.

4. Start all Tivoli Access Manager applications and services. For example, on Windows 2008 systems:
   a. Select **Start** > **Control Panel** > **Administrative Tools**.
   b. Double-click the **Services** icon.
   c. Start all Tivoli Access Manager services that run on the local system, including applications, such as WebSEAL.
   d. From **Services**, double-click **Tivoli Access Manager Auto-Start Service**.
   e. Change the startup type to **Automatic**.

Restoring WebSEAL

Use this procedure to restore WebSEAL to a previous version.

AIX: Restoring WebSEAL

Restore WebSEAL to a previous level if you encounter a problem when you migrate WebSEAL to version 7.0 on AIX.

About this task

If you encounter a problem when you migrate WebSEAL to Security Access Manager 7.0, you might need to restore the system to its prior level. These steps apply to LDAP, and Active Directory registries for all supported upgrade versions of Security Access Manager.

Notes:

- If you encounter a problem during the backup of existing data, contact IBM Support for assistance before you continue with the upgrade process.
- For supported operating system information, required patches and fix pack information for Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.

Procedure

1. Stop all Security Access Manager applications and services:
   ```
   pd_start stop
   ```
2. Remove, but do *not* unconfigure, the Security Access Manager WebSEAL component and prerequisite packages. To do so, from the command line:

a. Enter: `rm –rf /opt/PolicyDirector/.configure/*`
b. Enter: `rm /opt/PolicyDirector/etc/pd.conf`
c. Enter: `rm -rf /opt/pdweb/.configure`
d. Enter: `installp -u -g` *packages*

   Note: Use the **–g** option only if you want dependent software for the specified package removed.

   where *packages* are the following options:
   - Security Access Manager WebSEAL (`PDWeb.Web`)
   - Security Access Manager Web Security runtime (`PDWeb.RTE`)
   - Security Access Manager runtime (`PD.RTE`)
   - Security Access Manager license (`PD.lic`)
   - IBM Security Utilities (`TivSec.Utl`)

3. **For single system upgrade only:** Use your previous Tivoli Access Manager version DVDs and install the prerequisite components for WebSEAL, such as the Global Security Kit, Tivoli Directory Server client, and Tivoli Access Manager runtime.
4. Use the **pdbackup** `–action restore` option to restore the base files that you backed up before upgrade.

   On AIX, the default backup file name is *list_file_ddmmmyyyy.hh_mm*`.tar`. For example, for Tivoli Access Manager runtime:

   ```
   /opt/PolicyDirector/bin/pdbackup –action restore –file
   /var/PolicyDirector/pdbackup/61to70rtebackup.lst_17oct2012.10_27.tar
   ```
5. Use **pdadmin** to verify that your previous version of the runtime environment is restored successfully. For example:

   ```
   pdadmin -a sec_master -p password
   pdadmin sec_master> acl list
   ```
6. Install the previous version of Tivoli Access Manager WebSEAL and WebSEAL instance servers (`PDWeb.Web`).
7. Use the **pdbackup** `–action restore` option to restore the WebSEAL files that you backed up before upgrade.

   On AIX, Linux, and Solaris operating systems, the default backup file name is *list_file_ddmmmyyyy.hh_mm*`.tar`. For example, for default WebSEAL and WebSEAL instance files:

   ```
   /opt/PolicyDirector/bin/pdbackup –action restore –file
   /var/PolicyDirector/pdbackup/61to70websealbackup.lst_17oct2012.11_48.tar
   ```
8. Start WebSEAL and the WebSEAL instances. For example, to start the default WebSEAL:

   ```
   pdweb start instance
   ```

   Or, to start a WebSEAL instance:

   ```
   pdweb start instance-name
   ```

Results

The restoration of your previous WebSEAL version is complete.

Linux on x86-64: Restoring WebSEAL

Restore WebSEAL to a previous level if you encounter a problem when you migrate WebSEAL to version 7.0 on Linux x86-64.

About this task

If you encounter a problem when you migrate WebSEAL to Security Access Manager 7.0, you might need to restore the system to its prior level. These steps apply to LDAP, and Active Directory registries for all supported upgrade versions of Security Access Manager.

Notes:

- If you encounter a problem during the backup of existing data, contact IBM Support for assistance before you continue with the upgrade process.
- For supported operating system information, required patches and fix pack information for Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.

Procedure

1. Stop all Security Access Manager applications and services:

   ```
   pd_start stop
   ```

2. Remove, but do *not* unconfigure, the Security Access Manager WebSEAL component and prerequisite packages. To do so, from the command line:
   a. Enter: `rm –rf /opt/PolicyDirector/.configure/*`
   b. Enter: `rm /opt/PolicyDirector/etc/pd.conf`
   c. Enter: `rm -rf /opt/pdweb/.configure/*`
   d. Enter: `rpm -e packages` where *packages* are the following options:
      - Security Access Manager WebSEAL (`PDWeb-PD-7.0.0-0`)
      - Security Access Manager Web Security runtime (`PDWebRTE-PD-7.0.0-0`)
      - Security Access Manager runtime (`PDRTE-PD-7.0.0-0`)
      - Security Access Manager license (`PDlic-PD-7.0.0-0`)
      - IBM Security Utilities (`TivSecUtl-TivSec-7.0.0-0`)
3. **For single system upgrade only:** Use your previous version DVDs and install the prerequisite components for WebSEAL, such as the Global Security Kit, Tivoli Directory Server client, and Tivoli Access Manager runtime.
4. On the original system, use the **pdbackup** `–action restore` option to restore the files that you backed up before upgrade.

   On AIX, Linux, and Solaris operating systems, the default backup file name is *list_file_ddmmmyyyy.hh_mm*`.tar`. For example, for Tivoli Access Manager runtime:

   ```
   /opt/PolicyDirector/bin/pdbackup –action restore –file
   /var/PolicyDirector/pdbackup/61to70rtebackup.lst_17oct2012.10_27.tar
   ```

5. Use **pdadmin** to verify that your previous version of the runtime environment is restored successfully. For example:

   ```
   pdadmin -a sec_master -p password
   pdadmin sec_master> acl list
   ```

6. Install the previous version of Tivoli Access Manager WebSEAL and WebSEAL instance servers (`PDWeb`).
7. Use the **pdbackup** `–action restore` option to restore the WebSEAL files that you backed up before upgrade.

   On AIX, Linux, and Solaris operating systems, the default backup file name is *list_file_ddmmmyyyy.hh_mm*`.tar`. For example, for default WebSEAL and WebSEAL instance files:

   ```
   /opt/PolicyDirector/bin/pdbackup –action restore –file
   /var/PolicyDirector/pdbackup/61to70websealbackup.lst_17oct2012.11_48.tar
   ```

8. Start WebSEAL and the WebSEAL instances. For example, to start the default WebSEAL:

   ```
   pdweb start instance
   ```

   Or, to start a WebSEAL instance:

   ```
   pdweb start instance-name
   ```

Results

The restoration of your previous WebSEAL version is complete.

Linux on System z: Restoring WebSEAL

Restore WebSEAL to a previous level if you encounter a problem when you migrate WebSEAL to version 7.0 on Linux on System z.

About this task

If you encounter a problem when you migrate WebSEAL to Security Access Manager 7.0, you might need to restore the system to its prior level. These steps apply to LDAP, and Active Directory registries for all supported upgrade versions of Security Access Manager.

Notes:

- If you encounter a problem during the backup of existing data, contact IBM Support for assistance before you continue with the upgrade process.
- For supported operating system information, required patches and fix pack information for Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.

Procedure

1. Stop all Security Access Manager applications and services:

   ```
   pd_start stop
   ```

2. Remove, but do *not* unconfigure, the Security Access Manager WebSEAL component and prerequisite packages. To do so, from the command line:
   a. Enter: `rm –rf /opt/PolicyDirector/.configure/*`
   b. Enter: `rm /opt/PolicyDirector/etc/pd.conf`
   c. Enter: `rm -rf /opt/pdweb/.configure/*`
   d. Enter: `rpm -e --noscripts packages` where *packages* are the following options:
      - Security Access Manager WebSEAL (`PDWeb-PD-7.0.0-0`)
      - Security Access Manager Web Security runtime (`PDWebRTE-PD-7.0.0-0`)
      - Security Access Manager runtime (`PDRTE-PD-7.0.0-0`)
      - Security Access Manager license (`PDlic-PD-7.0.0-0`)
      - IBM Security Utilities (`TivSecUtl-TivSec-7.0.0-0`)
3. **For single system upgrade only:** Use your previous Tivoli Access Manager version DVDs and install the prerequisite components for WebSEAL, such as the Global Security Kit, Tivoli Directory Server client, and Tivoli Access Manager runtime.
4. Use the **`pdbackup`** `–action restore` option to restore the base files that you backed up before upgrade.

On AIX, Linux, and Solaris operating systems, the default backup file name is *list_file_ddmmmyyyy.hh_mm*.tar. For example, for Tivoli Access Manager runtime:

```
/opt/PolicyDirector/bin/pdbackup –action restore –file
/var/PolicyDirector/pdbackup/61to70rtebackup.lst_17oct2012.10_27.tar
```

5. Use **pdadmin** to verify that your previous version of the runtime environment is restored successfully. For example:

   ```
   pdadmin -a sec_master -p password
   pdadmin sec_master> acl list
   ```

6. Install the previous version of Tivoli Access Manager WebSEAL and WebSEAL instance servers (PDWeb).
7. Use the **pdbackup** –action restore option to restore the WebSEAL files that you backed up before upgrade.

   On AIX, Linux, and Solaris operating systems, the default backup file name is *list_file_ddmmmyyyy.hh_mm*.tar. For example, for default WebSEAL and WebSEAL instance files:

   ```
   /opt/PolicyDirector/bin/pdbackup –action restore –file
   /rev/PolicyDirector/pdbackup/61to70websealbackup.lst_17oct2012.11_48.tar
   ```

8. Start WebSEAL and the WebSEAL instances. For example, to start the default WebSEAL:

   ```
   pdweb start instance
   ```

   Or, to start a WebSEAL instance:

   ```
   pdweb start instance-name
   ```

Results

The restoration of your previous WebSEAL version is complete.

Solaris: Restoring WebSEAL

Restore WebSEAL to a previous level if you encounter a problem when you migrate WebSEAL to version 7.0 on Solaris.

About this task

If you encounter a problem when you migrate WebSEAL to Security Access Manager 7.0, you might need to restore the system to its prior level. These steps apply to LDAP, and Active Directory registries for all supported upgrade versions of Security Access Manager.

Notes:

- If you encounter a problem during the backup of existing data, contact IBM Support for assistance before you continue with the upgrade process.
- For supported operating system information, required patches and fix pack information for Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.

Procedure

1. Stop all Security Access Manager applications and services:

   ```
   pd_start stop
   ```

2. Remove, but do *not* unconfigure, the Security Access Manager WebSEAL component and prerequisite packages. To do so, from the command line:

a. Enter: `rm –rf /opt/PolicyDirector/.configure/*`
b. Enter: `rm /opt/PolicyDirector/etc/pd.conf`
c. Enter: `rm -rf /opt/pdweb/.configure`
d. Enter: `pkgrm` *packages* where *packages* are the following options:
   - Security Access Manager WebSEAL (`PDWeb`)
   - Security Access ManagerWeb Security runtime (`PDWebRTE`)
   - Security Access Manager runtime (`PDRTE`)
   - Security Access Manager license (`PDlic`)
   - IBM Security Utilities (`TivSecUtl`)

   Note: When prompted to confirm the removal of these components, enter `y`.

3. **For single system upgrade only:** Use your previous version DVDs and install the prerequisite components for WebSEAL, such as the Global Security Kit, Tivoli Directory Server client, and Tivoli Access Manager runtime (`PDRTE`).
4. Use the **pdbackup** `–action restore` option to restore the base files that you backed up before upgrade.

   On AIX, Linux, and Solaris operating systems, the default backup file name is *list_file_ddmmmyyyy.hh_mm*`.tar`. For example, for Tivoli Access Manager runtime:

   ```
   /opt/PolicyDirector/bin/pdbackup –action restore –file
   /var/PolicyDirector/pdbackup/61to70rtebackup.lst_17oct2012.10_27.tar
   ```
5. Use **pdadmin** to verify that your previous version of the runtime environment is restored successfully. For example:

   ```
   pdadmin -a sec_master -p password
   pdadmin sec_master> acl list
   ```
6. Install the previous version of Tivoli Access Manager WebSEAL (`PDWeb`) and WebSEAL instance servers (`PDWeb.Web`).
7. Use the **pdbackup** `–action restore` option to restore the WebSEAL files that you backed up before upgrade.

   On Solaris, the default backup file name is *list_file_ddmmmyyyy.hh_mm*`.tar`. For example, for default WebSEAL and WebSEAL instance files:

   ```
   /opt/PolicyDirector/bin/pdbackup –action restore –file
   /var/PolicyDirector/pdbackup/61to70websealbackup.lst_17oct2012.10_27.tar
   ```
8. Start WebSEAL and the WebSEAL instances. For example, to start the default WebSEAL:

   ```
   pdweb start instance
   ```

   Or, to start a WebSEAL instance:

   ```
   pdweb start instance-name
   ```

Results

The restoration of your previous WebSEAL version is complete.

Windows: Restoring WebSEAL

Restore WebSEAL to a previous level if you encounter a problem when you migrate WebSEAL to version 7.0 on Windows.

About this task

If you encounter a problem when you migrate WebSEAL to Security Access Manager 7.0, you might need to restore the system to its prior level. These steps apply to LDAP, and Active Directory registries for all supported upgrade versions of Security Access Manager.

Notes:

- Stop all Security Access Manager applications and services. For example, on Windows 2008 systems, select **Start → Control Panel → Administrative Tools**. Double-click the **Services** icon, and stop all Security Access Manager services that run on the local system, including applications.
- If you encounter a problem during the backup of existing data, contact Support for assistance before you continue with the upgrade process.
- For supported operating system information, required patches and fix pack information for Security Access Manager 7.0, see the *IBM Security Access Manager for Web Release Notes*.

Procedure

1. Remove, but do *not* unconfigure, the Security Access Manager WebSEAL 7.0 component and prerequisite packages.
   - Security Access Manager WebSEAL
   - Security Access Manager Web Security runtime
   - Security Access Manager runtime
   - IBM Security Utilities
   - Security Access Manager license

   Follow these steps:
   a. Select **Start** > **Run**, type `regedit` in the entry field, and then click **OK** to open the registry.
   b. Click **My Computer** > **HKEY_LOCAL_MACHINE** > **Tivoli** > **Policy Director Runtime** > **7.0**.
   c. Change the configuration value from `Yes` to `No`.
   d. Click **My Computer** > **HKEY_LOCAL_MACHINE** > **Tivoli** > **Access Manager WebSEAL** > **7.0**.
   e. Change the configuration value from `Yes` to `No`.
   f. Delete the `pd.conf` file from the *`install_path`*`\etc` directory. For example:
      ```
      C:\Program Files\Tivoli\Policy Director\etc\pd.conf
      ```
   g. Log in as a Windows user with administrator privilege.
   h. Remove the components. For example, for Windows 2008, click **Start** > **Control Panel** and double-click the **Add/Remove Programs** icon.
   i. Select another component from the list and continue the process until all the components are removed.
   j. Click **OK** to exit the program.
2. **For single system upgrade only:** Use your previous version DVDs and install the prerequisite components for WebSEAL, such as the Global Security Kit, Tivoli Directory Server client, and Tivoli Access Manager runtime.

   Install by running the **`setup.exe`** script in the `\windows\PolicyDirector\Disk Images\Disk1` directory. Select the components, and then follow the online instructions to complete the installation in order.

3. Use the **pdbackup** –action restore option to restore the base files that you backed up before upgrade.

   On Windows operating systems, the default backup file name is *list_file_ddmmmyyyy.hh_mm*.dar. For example, for Tivoli Access Manager runtime:

   ```
   C:\Program Files\Tivoli\Policy Director\bin\pdbackup –action restore –file
   C:\Program Files\Tivoli\Policy
   Director\pdbackup\61to70rtebackup.lst_17oct2012.10_27.dar
   ```

4. Use **pdadmin** to verify that your previous version of the runtime environment is restored successfully. For example:

   ```
   pdadmin -a sec_master -p password
   pdadmin sec_master> acl list
   ```

5. Install by running the **setup.exe** script in the \windows\PolicyDirector\Disk Images\Disk1 directory. Select to install the following components:

   - **Tivoli Access Manager WebSEAL**
   - WebSEAL instance servers

   Follow the online instructions to complete the installation.

6. Use the **pdbackup** –action restore option to restore the Tivoli Access Manager WebSEAL component from the dir file that you backed up before upgrade.

   On Windows operating systems, the default backup file name is *list_file_ddmmmyyyy.hh_mm*.dar. For example, for Tivoli Access Manager WebSEAL:

   ```
   pdbackup60 –action restore –file
   C:\Program Files\Tivoli\Policy
   Director\pdbackup\61to70websealbackup.lst_17oct2012.10_27.dar
   ```

7. Start WebSEAL and the WebSEAL instances. For example, on Windows 2008 systems, select **Start** > **Control Panel** > **Administrative Tools**. Double-click the **Services** icon, and start the services.

Results

The restoration of your previous WebSEAL version is complete.

Appendix. Upgrade utilities

Reading syntax statements

The reference documentation uses the following special characters to define syntax:

[ ] Identifies optional parameters. Parameters 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 parameters in a single use of the command.

{ } Delimits a set of mutually exclusive parameters when one of the parameters is required. If the parameters are optional, they are enclosed in brackets ([ ]).

\ Indicates that the command line wraps to the next line. It is a continuation character.

The parameters 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.

adschema_update

Modifies the Microsoft Active Directory schema to work with the current version of Security Access Manager.

Syntax

adschema_update [–f *schema_file*] –u *active_directory_administrator_id* [–o [g[ui]]] –p *active_directory_administrator_pwd* [–r *response_file*]

Description

Use the **adschema_update** utility to modify the Microsoft Active Directory schema for the current version of Security Access Manager.

Run this utility on the Active Directory domain controller against which the policy server is configured after you upgrade to IBM Security Access Manager for Web, version 7.0.

Parameters

–f *schema_file*
Specifies the name of the Active Directory schema file. By default, the `adschema.def` file is in *installation_directory*`\etc` directory. (Optional)

–o [g[ui]]

–o Specifies to output messages to STDERR. (Optional)

–o g Specifies to display messages in a pop-up message box (GUI). (Optional)

© Copyright IBM Corp. 2003, 2012

–o gui Specifies to display messages in a pop-up message box (GUI). (Optional)

–p *active_directory_administrator_pwd*
Specifies the password for the Active Directory administrator.

–r *response_file*
Specifies the fully qualified path and file name of the response file to use during silent configuration. There is no default response file name. The response file contains stanzas and *key=value* pairs. For information about using response files, see the "Using response files" appendix in the *IBM Security Access Manager for Web Command Reference*. (Optional)

–u *active_directory_administrator_id*
Specifies the Active Directory administrator ID.

Availability

This utility is in the following default installation directory:

```
c:\Program Files\Tivoli\Policy Director\sbin
```

Note: Run this utility on the system where the Security Access Manager policy server is installed and configured.

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.

idsimigr

Migrates the schema and configuration files from an earlier release of Tivoli Directory Server to version 6.3 and creates a directory server instance with the migrated information.

Syntax

idsimigr [–I *instancename*] [-t *dbinstance*] [-u *backupdir*] [-e *encryptseed*] [-g *encryptsalt*] [-p *port*] [-s *secureport*] [-a *admport*] [-c *admsecureport*] [-i *ipaddress*] [-r *description*] [-b *outputfile*] [-d *debuglevel*] [-l *instlocation*] [–q] [-n] | [-v] | [-?]

Description

The **idsimigr** migration utility migrates the schema and configuration files from an earlier release to IBM Tivoli Directory Server 6.3 versions of these files. The utility creates a directory server instance with the migrated information.

This directory server instance is the upgraded version of your previous server. If required, can use the Instance Administration tool, specifying that you want to migrate from a previous release.

For more information about Instance Administration tool, see the *IBM Tivoli Directory Server: Installation and Configuration Guide*.

Attention: When you create a directory server instance, be aware of the information that follows.

1. If you want to use replication, use a distributed directory, or import and export LDIF data between server instances, you must cryptographically synchronize the server instances to obtain the best performance.

   If you are creating a directory server instance that must be cryptographically synchronized with an existing directory server instance, you must synchronize the server instances ***before*** you do any of the following actions:

   - Start the second server instance
   - Run the **idsbulkload** command from the second server instance
   - Run the **idsldif2db** command from the second server instance

   You can synchronize the server instances by ensuring that the encryption salt value for the server instance you are creating is the same as that of the existing server instance. You can obtain the destination server's salt value by searching for the `ibm-slapdCryptoSalt` attribute value (using the **idsldapsearch** utility) in the destination server's `cn=crypto,cn=localhost` entry.
2. After you create a directory server instance and configure the database, use the **idsdbback** utility to create a backup of the directory server instance.

   The configuration and directory key stash files are archived along with the associated configuration and directory data. You can then use the **idsdbrestore** utility to restore the key stash files if necessary. You can also use the **idsdbback** utility after you load data into the database. See the *IBM Tivoli Directory Server: Installation and Configuration Guide* for information about backing up the database.

Parameters

-? Displays usage help for the command.

-a *admport*
: Specifies the port on which the administration daemon for the directory server instance listens.

  Note: If you have two or more directory server instances that listen on the same IP address (or set of IP addresses), be sure that those directory server instances do not use any of the same port numbers.

-b *outputfile*
: Specifies the full path of a file to redirect output into. If used with the **-q** option, only errors are written to the file. If debugging is turned on, debugging information is also sent to the file.

-c *admsecureport*
: Specifies the secure port on which the administration daemon for the directory server instance listens. Specify a positive number that is greater than 0 and less than or equal to 65535. The port that is specified must not conflict with ports used by another directory server instance that is bound to a particular host name or IP address.

-d *debuglevel*
: Sets the LDAP debugging level to *debuglevel*. This option causes the utility to generate debug output to stdout. The *debuglevel* is a bit mask that controls which output is generated with values up to 65535. This parameter is for use by IBM service personnel.

-e *encryptseed*
: Specifies the seed to be used to create the key stash files for the directory

server instance. This option is required if you use the **-n** option. If it is not specified, you are prompted for an encryption seed.

The encryption seed must contain only printable ISO-8859-1 ASCII characters with values in the range of 33 to 126, and must be a minimum of 12 and a maximum of 1016 characters in length. For information about the characters that can be used.

This encryption seed is used to generate a set of Advanced Encryption Standard (AES) secret key values. These values are stored in a directory stash file and used to encrypt and decrypt directory stored password and secret key attributes. There is one encryption seed string for each directory server instance.

Record the encryption seed in a secure location; you might need it if you export data to an LDIF file (the **idsdb2ldif** command) or regenerate the key stash file (the **idsgendirksf** command.)

-g *encryptsalt*
Specifies the encryption salt value. Providing an encryption salt value is useful if you want to use replication, use a distributed directory, or import and export LDIF data between server instances.

You can obtain better performance if the two directory server instances have the same encryption salt value. Therefore, if the directory server instance you are migrating will be used in one of these ways, set the encryption salt value to the encryption salt value of the directory server instances with which it will be involved in these activities.

If you do not specify an encryption salt, the command randomly generates one.

The encryption salt must have exactly 12 characters and can contain only printable ISO-8859-1 ASCII characters in the range from 33 to 126 inclusive.

-i *ipaddress*
Specifies the IP address that the directory server instance binds to. If more than one IP address is specified, a comma separator is required with no spaces. Spaces are allowed only if the entire argument is enclosed in quotation marks (“). Use the key word "all" to specify that you want to use all available IP addresses. If you do not specify the **-i** option, all available IP addresses is the default setting.

-I *instancename*
Specifies the name of the directory server instance to be created or migrated. The instance name must be an existing user ID on the computer and must be no greater than 8 characters in length. If there is no corresponding user ID for the directory server instance name, the command fails.

-l *instlocation*
Specifies the location in which to store the configuration files and logs for the directory server instance. On Windows systems, this option is required and a drive letter must be specified. The location must have at least 30 MB of free disk space. Additional disk space must be available to accommodate growth as directory server log files increase in size.

-n Specifies that you want the command to run without prompting. All output is generated except for messages that require user interaction.

-p *port* Specifies the port on which the directory server instance listens. Specify a positive number that is greater than 0 and less than or equal to 65535. The

port that is specified must not cause a conflict with ports that are used by any other directory server instance that is bound to a particular hostname or IP address.

-q Specifies to run in quiet mode. All output is suppressed except error messages. If the **-d** option is also specified, trace output is not suppressed.

-r *description*
Specifies a description of the directory server instance.

-s *secureport*
Specifies the secure port that the directory server instance listens on. Specify a positive number that is greater than 0 and less than or equal to 65535. The port that is specified must not cause a conflict with ports that are used by any other directory server instance that is bound to a particular host name or IP address.

-t *dbinstance*
Specifies the DB2 database instance name. The database instance name is also the DB2 instance owner ID. By default, the database instance name is assumed to be the same as the directory server instance owner ID.

-u *backupdir*
Specifies the name of the directory in which the schema and configuration files to be migrated were saved.

If all the necessary files are not found in the specified directory, the command fails. These files include the server configuration file and the following schema files: `V3.ibm.at`, `V3.ibm.oc`, `V3.system.at`, `V3.system.oc`, `V3.user.at`, `V3.user.oc`, and `V3.modifiedschema`.

-v Prints version information about the command.

Examples

The following example assumes that you want to migrate from IBM Tivoli Directory Server 6.1 to IBM Tivoli Directory Server 6.3 and:

- You saved the configuration and schema files in a directory named `/tmp/ITDS61`.
- You want to create an instance that is called **myinst** with an encryption seed of **my_secret_key!** and an encryption salt of **mysecretsalt**.

Use the following command to migrate from IBM Tivoli Directory Server 6.1 to IBM Tivoli Directory Server 6.3:

```
idsimigr –I myinst –u /tmp/ITDS61 –e my_secret_key! -g mysecretsalt
```

On Windows, you must specify a location for the directory server instance using the **-l** option. The following example creates a `C:\idsslapd-myinst` directory for the directory server instance that is being migrated.

```
idsimigr –I myinst –u c:\temp –l c: -e my_secret_key!
```

ivrgy_tool

Updates the Security Access Manager schema on an LDAP server. It also applies the required access control lists (ACLs) to suffixes added to the LDAP server after policy server configuration.

This utility is not supported with the Active Directory Lightweight Directory Service (AD LDS) user registry. See the *IBM Security Access Manager for Web Installation Guide* for information about updating the AD LDS schema for use with Security Access Manager.

Syntax

Using `add-acls`:

`ivrgy_tool` –h *host_name* [–p *port*] [–D *admin_dn*] [F] [–g *name*] –w *admin_password* [–d] [–r *response_file*] `add-acls` *domain_name*

Using `add-acls` with SSL communication:

`ivrgy_tool` –h *host_name* [–p *port*] [–D *admin_dn*] [F] [–g *name*] –w *admin_password* [–d] –Z –K *keyfile* –P *keyfile_password* [–N *keyfile_label*] [–r *response_file*] `add-acls` *domain_name*

Using `schema`:

`ivrgy_tool` –h *host_name* [–p *port*] [–D *admin_dn*] –w *admin_password* [–d] [–r *response_file*] `schema`

Using `schema` with SSL communication:

`ivrgy_tool` –h *host_name* [–p *port*] [–D *admin_dn*] –w *admin_password* [–d] –Z –K *keyfile* –P *keyfile_password* [–N *keyfile_label*] [–r *response_file*] `schema`

Description

You can perform the following actions with the **`ivrgy_tool`** and `add-acls` parameter:

- Apply the required ACLs to suffixes that were added to the LDAP server after the policy server was configured.
- Apply ACLs to the servers in a Tivoli Directory Server proxy environment.
- Set the necessary ACLs on servers so that Security Access Manager manages the partition suffix.

In a proxy environment, the server enforces access control. When the ACLs exist on the top-level object of a partition split, you must create the correct ACLs on each server.

With the **`ivrgy_tool`** and `schema` parameter, you can update the Security Access Manager schema on a supported LDAP server.

The schema is defined in a set of files specific to the type of LDAP server. These files are installed during IBM Security Access Manager runtime installation. These files provide input to the automatic schema update process when you configure the policy server.

Typically, the schema is updated when the policy server is configured. When you migrate an existing installation of Security Access Manager, you must upgrade the schema on the LDAP server to the current version with the **`ivrgy_tool`** utility.

The following files contain the LDAP schema:

`secschema.def`
Used for Tivoli Directory Server.

`nsschema.def`
Used for Sun Java System Directory Server.

novschema.def
Used for Novell eDirectory Server.

An administrator can apply and update the schema with one of these files as the LDAP Data Interchange Format (LDIF) input to the **ldapmodify** utility. The **ldapmodify** tool is a Tivoli Directory Server utility.

When an LDAP server is not supported by Security Access Manager, you cannot use the **ivrgy_tool** utility to update the schema. In these cases, an administrator must manually update the schema on the generic LDAP server.

When manually updating the schema, administrators must use the LDIF definitions that are defined in the `nsschema.def` schema file as the basis for the schema definitions. Administrators must modify the definitions in the schema file to meet the requirements of their generic LDAP server.

Parameters

–d Runs in verbose output mode for debugging purposes. (Optional)

–D *admin_dn*
Specifies the distinguished name of the LDAP administrator. The format for a distinguished name is like `cn=root`. (Optional)

–F Forces the addition of ACLs even if the domain is not defined on this server. This parameter is valid only with the `add-acls` command. The default value is not to force the addition of ACLs. (Optional)

–g *name*
Specifies Daemon type [`acld-server` or `remote-acl-user`]. The default value is `acld-server`. (Optional)

–h *host_name*
Specifies the IP address or host name of the LDAP server. Valid values include any valid IP host name. For example:

```
host = libra
host = libra.example.ibm.com
```

When used in a Tivoli Directory Server proxy environment, the value is the server IP address or host name where you want to set the ACLs.

–K *keyfile*
Specifies the fully qualified path and file name of the SSL key database. This parameter is required only when the `–Z` parameter is specified. Use the SSL key file to handle certificates in LDAP communication. The file type can be anything, but the extension, as shown in the following example for the policy server, is typically `.kdb`.

Policy server on Windows

```
C:\Program Files\Tivoli\Policy Director\keytab\ivmgrd.kdb
```

Policy server on AIX, Linux, or Solaris

```
/opt/PolicyDirector/keytab/ivmgrd.kdb
```

–N *key_name*
Specifies the private key name for the keyfile.

–p *port*
Specifies the port number of the LDAP server. Use the LDAP server-configured port number. The default port number is `636` if Secure

Sockets Layer (SSL) is used and 389 if SSL is not used. If not specified, the default LDAP port is used. (Optional)

In a Tivoli Directory Server proxy environment, the value is the port number of the server.

–P *keyfile_password*
Specifies the password for the SSL key database. This parameter is required only if the –Z parameter is specified.

–r *response_file*
Specifies the fully qualified path and file name of the response file for silent configuration. A response file can be used for configuration. There is no default response file name. The response file contains stanzas and *key=value* pairs. For information about using response files, see the "Using response files" appendix in the *IBM Security Access Manager for Web Command Reference*. (Optional)

–R Removes from registry for the `uninstall` command. The default value is `false`. (Optional)

–s *suffix*
Specifies the LDAP suffix under which to create the Management Domain.

–S *name*
Specifies the Security Master Principal Name. The default is `sec_master`. (Optional)

–v *version*
Specifies the data model version to use for the `install` command. The default value is `6`. (Optional)

–w *admin_password*
Specifies the password of the LDAP administrator.

–Z Specifies to use SSL for a secure LDAP connection. (Optional)

add-acls *domain_name*
Indicates that the required access control lists (ACLs) must be applied to all suffixes that are defined on the LDAP server for the specified domain. When the policy server is configured, the management domain is created with the default name of `Default`. When you use the `add-acls` parameters in a Tivoli Directory Server proxy environment, always apply the ACLs to the management domain at a minimum.

This option is useful for adding access control to suffixes that are added to the LDAP server after the policy server is configured.

schema Updates the Security Access Manager schema. Use this parameter when you are using:

- A version of Tivoli Directory Server earlier than version 6.0, such as Tivoli Directory Server version 5.2.
- An LDAP server other than Tivoli Directory Server. For example, you are using Novell eDirectory Server.

Return codes

0 The utility completed successfully.

1 The utility failed. When a utility fails, a description of the error and an error is provided.

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
  ```

pdconfig

Configures and unconfigures Security Access Manager components.

Syntax

pdconfig

Note: Before you run the **pdconfig** utility, you must set the PATH environment variable to include the directory that contains the Java executable file. For example, you might specify the directory where you installed the IBM Java Runtime. See the topics about installing IBM Java Runtime in the *IBM Security Access Manager for Web Installation Guide* for information about setting this environment variable.

Description

When you configure Security Access Manager with the **pdconfig** utility, you are prompted for several options. Use the *IBM Security Access Manager for Web Installation Guide* for option descriptions to help you provide correct values.

When a message displays that indicates a package was successfully configured, press **Enter** to configure another package, or select the **x** (Exit) option twice to close the configuration utility.

If you must comply with security standards such as FIPS 140-2, NIST SP800-131a or NSA Suite B, the **pdconfig** utility prompts you to do the following steps:

1. Stop the configuration process.
2. Update the `pd.conf` file to set `ssl-compliance` to the required compliance type.
3. Restart the configuration process.

If you configure the Security Access Manager security standard in the `ssl-compliance` option to Suite B, NIST SP800-131, or FIPS, and not the default of "`none`," then during Web Portal Manager configuration, you must also configure WebSphere Application Server to enable the same security standard. If the security standard settings do not match, Web Portal Manager configuration fails. To enable the same security setting in WebSphere Application Server, see http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html

Note:

Parameters

None.

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.

pdjrtecfg

Configures or unconfigures IBM Security Access Manager Runtime for Java.

Syntax

Configure in full mode

pdjrtecfg –action config –host *policy_server_host* [–port *policy_server_port*] [–java_home *jre_home*] [–domain *domain_name*] [–config_type full] [–enable_tcd [–tcd *path*]][–cfgfiles_path *path_to_config_files* [–alt_config]]

Configure in stand-alone mode

pdjrtecfg –action config –config_type standalone [–cfgfiles_path *path_to_config_files* [–alt_config]]

Configure in interactive mode

pdjrtecfg –action config –interactive

Configure with a response file

pdjrtecfg –action config –rspfile *response_file*

pdjrtecfg –action name

pdjrtecfg –action status [–java_home *jre_home*]

pdjrtecfg –action unconfig [–java_home {*jre_home*|all}]

pdjrtecfg –action unconfig –interactive

pdjrtecfg –operations

pdjrtecfg –help [*options*]

pdjrtecfg –usage

pdjrtecfg –?

Description

The IBM Security Access Manager Runtime for Java component enables Java applications to manage and use Security Access Manager security.

The **pdjrtecfg** utility adds or updates Security Access Manager `.jar` files in the *jre_home*\lib\ext directory and backs up the existing files. The utility does not modify any other `.jar` files in this directory.

More than one Java runtime can exist on the same computer. Use the **pdjrtecfg** utility to configure IBM Security Access Manager Runtime for Java independently to each JRE.

WebSphere Application Server, version 8, does not permit modification to its JRE, so you must configure IBM Security Access Manager Runtime for Java to a location outside of the WebSphere JRE. With WebSphere Application Server, version 8, the IBM Security Access Manager Runtime for Java configuration files and `.jar` files are in the *WAS_Home*`/tivoli/tam` directory.

You can configure IBM Security Access Manager Runtime for Java into WebSphere Application Server, version 8, either the following ways:

- On the command line with **pdjrtecfg**. This option requires two more configuration options:
  - **-cfgfiles_path**
  - **-alt_config**
- Interactively with either **pdconfig** or **pdjrtecfg -action config -interactive**.

  When **pdjrtecfg** runs with **-interactive**, the utility detects WebSphere Application Server, version 8, and automatically provides the **-cfgfiles_path** and **-alt_config** options.

Note: Use only the **pdjrtecfg** utility and not the `PDJrteCfg` Java class directly.

Parameters

–? Shows the syntax for this utility. (Optional)

–action {config|name|status|unconfig}
Specifies the action that is one of the following values:

config Configures the IBM Security Access Manager Runtime for Java component.

name Retrieves the IBM Security Access Manager Runtime for Java component package name and returns the name value to the **pdconfig** utility. Only **pdconfig** uses this parameter. Do not use this parameter from the command line.

status Determines and returns the IBM Security Access Manager Runtime for Java component configuration status information to the **pdconfig** utility. Only **pdconfig** uses this parameter. Do not use this parameter from the command line.

unconfig
Unconfigures the IBM Security Access Manager Runtime for Java component.

–alt_config
Specifies either to add the `PD.jar` to a specified directory or to update an existing file. The `–cfgfiles_path` *path_to_config_files* option specifies a directory instead of using the default `JRE lib/ext/` directory. (Optional)

You must set the `–cfgfiles_path` parameter to use `–alt_config`.

The `–alt_config` option supports the WebSphere Application Server, version 8, restriction which does not permit modification of any files under the WebSphere Application Server JRE directory.

WebSphere Application Server, version 8, adds the *WAS_HOME*`/tivoli/tam` directory to its `java.ext.dirs` property for use with Security Access

Manager. To use the new directory, you must specify *WAS_HOME*/tivoli/tam for the –cfgfiles_path *path_to_config_files* parameter along with –alt_config so that PD.jar is available to the WebSphere Application Server JVM.

–cfgfiles_path *path_to_config_files*
Specifies an alternative location for the PolicyDirector directory that contains the IBM Security Access Manager Runtime for Java configuration files. Typically, the PolicyDirector directory is at the root of the JRE directory that is being configured. (See -java_home.) (Optional)

If you use this option, then applications that use the PD.jar API in this Java Runtime must set the Java System property, pd.cfg.home with the same *path_to_config_files* value.

This option supports the WebSphere Application Server, version 8, restriction which does not permit the modification of any files under the WebSphere Application Server JRE directory.

WebSphere Application Server, version 8, stores Security Access Manager configuration files in a unique directory: *WAS_HOME*/tivoli/tam/PolicyDirector. WebSphere Application Server version 8 also requires the –alt_config parameter.

The /opt/IBM/WebSphere/AppServer/tivoli/tam directory contains the PD.jar file. The PolicyDirector subdirectory contains the PD.properties file.

For example, if you install WebSphere Application Server, version 8, at a location such as /opt/IBM/WebSphere/AppServer, the value for the –cfgfiles_path variable, *path_to_config_files*, is /opt/IBM/WebSphere/AppServer/tivoli/tam. No other location can be used.

–config_type {**full**|**standalone**}
Specifies the configuration mode. The default value is full. (Optional)

full Completes all the required configuration steps, which include the generation of the server-side certificate for the policy server.

standalone
Completes all the required configuration steps, except for the generation of the server-side certificate for the policy server. With this configuration, you can use the Security Access Manager Java APIs without requiring a policy server. Typically, this configuration is used to configure a Security Access Manager development environment.

–domain *domain_name*
Specifies the local domain name for the Java runtime. A local domain is a Security Access Manager secure domain that is used by programs when no explicit domain is specified. If you do not specify this parameter, the local domain defaults to the management domain. (Optional)

–enable_tcd [**–tcd** *path*]
Enables Tivoli Common Directory (TCD) logging, if it is not already enabled. It also specifies the fully qualified path location for common logging. When TCD is enabled, all Security Access Manager message log files are placed in this common location. (Optional)

–help [*options*]
Provides online help for one or more utility options. It shows descriptions

of the valid command-line options. Alternatively, it provides online help about a specific command-line parameter. (Optional)

–host *policy_server_host*
Specifies the Security Access Manager policy server host name. Valid values include any valid IP host name. Examples:

```
host = libra
host = libra.example.ibm.com
```

–interactive
Specifies the interactive mode in which the user is prompted for configuration information for the IBM Security Access Manager Runtime for Java component. If not specified, the configuration program runs in non-interactive (silent) mode. (Optional)

–java_home *jre_path*
Specifies the fully qualified path to the Java runtime, such as the directory that ends in `JRE`. If you do not specify this parameter, the home directory for the JRE in the PATH statement is used. If the home directory for the JRE is not in the PATH statement, this utility fails. (Optional)

During unconfiguration, you can specify the `all` parameter that unconfigures all configured JREs.

–operations
Prints all the valid command-line options. (Optional)

–port *policy_server_port*
Specifies the Security Access Manager policy server port number. The default value is `7135`. (Optional)

–rspfile *response_file*
Specifies the fully qualified path and file name of the silent configuration response file. You can use a response file for configuration. There is no default response file name. (Optional)

The response file contains *parameter=value* pairs. The following rules apply to response files:

- All slashes in the java_home parameter path must be either:
  - Escaped with a second back slash (`\`)
  - A single front slash (`/`)

  For example:

  ```
  java_home=c:\\Program Files\\IBM\\Java60
  ```

  or

  ```
  java_home=c:/Program Files/IBM/Java60
  ```
- The path must not include quotation marks.

–usage Shows the syntax for this utility. (Optional)

Availability

This utility 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 you select an installation directory other than the default, 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.

Examples

- The following example configures the IBM Security Access Manager Runtime for Java component:

```
pdjrtecfg -action config -host sys123.acme.com -port 7135
-java_home "C:\Program Files\IBM\Java60\jre"
```

- The following example unconfigures the IBM Security Access Manager Runtime for Java component:

```
pdjrtecfg -action unconfig -java_home "C:\Program Files\IBM\Java60\jre"
```

- The following example uses command-line configuration of WebSphere Application Server, version 8, for the Security Access Manager Java API:

```
# pdjrtecfg -action config -host mypolicyserverhostname \
   -java_home /opt/IBM/WebSphere/AppServer/java/jre \
   -cfgfiles_path /opt/IBM/WebSphere/AppServer/tivoli/tam \
   -alt_config -config_type full -port 7135
```

pdsmsclicfg

Configures the command-line administration utility for the session management server.

Syntax

pdsmsclicfg –action config [–rspfile *response_file*] [–interactive {yes|no}] [–sam_integration {yes|no}] [–aznapi_app_config_file *path_name*] [–webservice_location *host*:*port*[,*host*:*port*...]] [–instances *name1*,*name2*] [-ssl_enable {yes|no}] [–sslkeyfile *path*] [–sslkeyfile_stash *path*] [–sslkeyfile_label *label*]

pdsmsclicfg –action unconfig

pdsmsclicfg –action name

pdsmsclicfg –action version

pdsmsclicfg –action upgrade

Description

The **pdsmsclicfg** utility configures or unconfigures the session management server command-line administration utility. A log of the configuration progress is written to the `msg_pdsmsclicfg.log` log file. The log file is in the:

- `/var/pdsms/log` directory on AIX, Linux, and Solaris operating systems.

- *installation_directory*\log directory on Windows operating systems.

This utility can be run in one of the following ways:

- Interactively – the user is prompted to provide configuration information.
- Silently – the utility accepts input from a response file or the command line.

Integration with Security Access Manager can be enabled during configuration. The program prompts the user to specify the path to the configuration file for a configured **aznapi** application. The program prompts the user to specify the location of the web service. The location of the web service is defined by a host name and port that are separated by a semicolon.

The user can specify multiple locations, when each location is separated by a comma. If this web service uses a secure connection, the program prompts the user for the SSL options. You must also specify the session management server instance.

The configuration information is saved to /opt/pdsms/etc/pdsmsclicfg.conf. The presence of this configuration file is used to determine the configuration status of the utility.

The command-line executable program on Windows is pdsmsclicfg-cl.exe.

Parameters

–action {config|unconfig|upgrade|name|version}
Specifies an action that is one of the following values:

config Configures the command-line administration utility.

unconfig
Fully unconfigures the command-line administration utility. No other parameters are required.

name Displays the translated "Session Management Command Line" name. No other options are required.

upgrade
Configures an upgrade from a previous version.

version
Displays the version number for the currently installed SMS CLI package.

–rspfile *response_file*
Specifies the fully qualified path and file name of the response file to use during silent configuration. A response file can be used for configuration. There is no default response file name. The response file contains stanzas and *key=value* pairs. For information about using response files, see the "Using response files" appendix in the *IBM Security Access Manager for Web Command Reference*. (Optional)

–interactive {yes|no}
Indicates whether the configuration is interactive. The default value is yes. (Optional)

–sam_integration {yes|no}
Specifies whether integration with the Security Access Manager administration framework is required. The default value is no. (Optional)

–aznapi_app_config_file *path_name*
Specifies the fully qualified name of the configuration file for the hosting authorization server. Only required if Security Access Manager integration is enabled. (Optional)

–webservice_location *host*:*port*
Specifies the location of the session management server Administration web service. The location is the name of the hosting server and the port on which the web service is located. Multiple locations can be specified. When you specify multiple locations, separate the locations with commas. (Optional)

–instances *name1*,*name2*
The session management server instances which are to be administered. The instance names must be separated by a comma. The default value is `DSess`. (Optional)

-ssl_enable {yes|no}
Indicates whether SSL communication with the web server must be enabled. (Optional)

–sslkeyfile *path*
Specifies the fully qualified name of the SSL key file to use during communication with the session management server web service. Use this parameter only when the `-ssl_enable` parameter is set to `yes`. (Optional)

–sslkeyfile_label *label*
Specifies the SSL key file label of the certificate to be used. Use this parameter only when the `-ssl_enable` parameter is set to `yes`. (Optional)

–sslkeyfile_stash *path*
Specifies the fully qualified name of the stash file that contains the password for the SSL key file. Use this parameter only when the `-ssl_enable` parameter is set to `yes`. (Optional)

Availability

This utility is in one of the following default installation directories:

- On AIX, Linux, and Solaris operating systems:
  `/opt/pdsms/bin`
- On Windows operating systems:
  `c:\Program Files\Tivoli\PDSMS\bin`

To start the command line under Windows, use **pdsmsclicfg-cl.exe**. The **pdsmsclicfg** command starts the wizard.

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.

non-zero
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.

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.

© Copyright IBM Corp. 2003, 2012

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

© Copyright IBM Corp. 2003, 2012

P

R

S

T

U

W

Printed in USA

SC23-6503-02