Containerized IBM Security Guardium Key Lifecycle Manager
Version 4.1

Documentation
(BETA 1)

IBM Confidential

Deploying IBM Security Key Lifecycle Manager

You can deploy IBM Security Key Lifecycle Manager with the IBM Db2 database or the PostgreSQL database.

Deploying IBM Security Key Lifecycle Manager containers on Kubernetes cluster using Helm charts (Sample provided for PostgreSQL only)

You can deploy IBM Security Key Lifecycle Manager containers on Kubernetes cluster using Helm charts only with PostgreSQL database.

Prerequisites

- Set up a Kubernetes cluster. You can use Version 1.17 or later. For more information, see https://kubernetes.io/docs/setup/.
- Ensure that you have an account on the Docker Hub.
- Install Helm Version 2.0 or later on the system from which you will access the Kubernetes cluster. For more information, see https://helm.sh/docs/intro/install/.
- To obtain the license activation file for IBM Security Key Lifecycle Manager, send us an email at: ibmsklm@in.ibm.com.

Procedure

Complete the following steps on the system on which you installed Helm:

1. Download the k8s-helm.zip file that contains the sample Helm charts for deploying IBM Security Key Lifecycle Manager.
2. Extract the **k8s-helm.zip** file.
3. In the directory where you extracted the files, navigate to **k8s-helm** > **sklm** directory.
4. Open the **values.yaml** file to modify the parameter values as per your requirement.
5. Navigate to **k8s-helm** directory and run the following command:

   ```
   helm install sklm
   ```

   Note: If you are using Helm Version 3.0 or later, use the following command:

   ```
   helm install <name> sklm
   ```

6. Verify the installation by running the following commands:
7. `helm list`
8. `kubectl get pods`

9.
   ```
   kubectl get pv
   kubectl get pvc
   ```

10. Launch the IBM Security Key Lifecycle Manager graphical user interface:

    ```
    https://ip-address:port/ibm/SKLM/login.jsp
    ```

11. On the Configuration page that appears, click the License Agreements link to review the license terms, and then select the **I accept the terms in the License Agreements** check box.
12. Click **Activate License**.
13. Upload the IBM Security Key Lifecycle Manager license activation file and activate the license.
14. Click **Login**.
15. Log in to the IBM Security Key Lifecycle Manager graphical user interface with the Administrator user credentials (sklmadmin).

From the Welcome page, configure the drive types, keys, and certificates that your organization requires, or get started with using the product. See Working with IBM Security Key Lifecycle Manager.

Deploying IBM Security Key Lifecycle Manager with PostgreSQL database using Docker

See this section for instructions on deploying IBM Security Key Lifecycle Manager with PostgreSQL as the database.
Prerequisites

- Ensure that the host system meets the following minimum system requirements:

Resource	Requirement
CPU	4 Cores
Memory	8 GB
Disk space	100 GB
Operating system and Supported architectures	Linux o x86_64 o s390x

- Install Docker engine on the host system. For instructions, see https://docs.docker.com/.
- Ensure that you have an account on the Docker Hub.

- To obtain the license activation file for IBM Security Key Lifecycle Manager, send us an email at: ibmsklm@in.ibm.com.
- Set up the PostgreSQL container by running the following command:

  ```
  docker run -d -v sklmpostgresdbvolume:/var/lib/postgresql/data -e
  POSTGRES_PASSWORD=Example@db2 -e POSTGRES_USER=sklmdb41 -e
  POSTGRES_DB=sklmdb41 -p 5432:5432 postgres
  ```

  Note: The container might take a few minutes to start. You can monitor the progress by using the docker logs command.

Procedure

Complete the following steps on the host system:

1. Log in to Docker Hub.
2. (*Optional*) Create an environment variable list file (for example, sklmenv) with the parameters for the IBM Security Key Lifecycle Manager container:
   - **Parameter list**

Parameter	**Mandatory /Optional**	**Description**
Container name		
name	Mandatory	Specify a name for the container.
Environment variables		
DB_PASSWORD	Mandatory	Password to connect to the database instance where the IBM Security Key Lifecycle Manager database is running
DB_TYPE	Optional	Type of the database. Specify postgres as the value. Default value: db2 **Note**: This parameter is ignored in the subsequent docker run commands when the same value of the sklmAppVolume parameter is used.
DB_USER	Optional	User name of the database. Default value: sklmdb41
DBNAME	Optional	Name of the database. Default value: sklmdb41

DB_PORT	Mandatory	Port number of the database instance where the IBM Security Key Lifecycle Manager database is running
DB_HOST	Mandatory	IP address or fully qualified host name of the system that hosts the database instance where the IBM Security Key Lifecycle Manager database is running. You can use the same system to host the database instance and the application Docker container, or choose a different system for each of them.
LICENSE	Mandatory	Variable to accept license terms. Specify value as "**accept**".
SKLM_SEED	Mandatory	Secret passcode that is unique for a deployment, and must be stored securely. The value must be a random string of 32 or 64 characters that you can generate using an external utility. **Note**: Ensure that the value of this parameter in the subsequent docker run commands is the same as that used in the first docker run command, when the same value of the sklmAppVolume parameter is used.
SKLMADMIN_USERNAME	Optional	User name of the IBM Security Key Lifecycle Manager administrator. You can specify only alphanumeric characters. Default value: sklmadmin **Note**: This parameter is ignored in the subsequent docker run commands when the same value of the sklmAppVolume parameter is used.
SKLMADMIN_PASSWORD	Mandatory	Password for the IBM Security Key Lifecycle Manager administrator user that is specified in the SKLMADMIN_USERNAME parameter. **Note**: This parameter is ignored in the subsequent docker run commands when the same value of the sklmAppVolume parameter is used.

KEY_STORE_PWD	Optional	Password for the IBM Security Key Lifecycle Manager keystore. Default value: SKLMWebAS **Note**: Ensure that the value of this parameter in the subsequent docker run commands is the same as that used in the first docker run command, when the same value of the sklmAppVolume parameter is used.
Port numbers		
9443	Mandatory	Port number for the graphical user interface.
5696	Mandatory	KMIP port
1441	Mandatory	SSL port
3801	Mandatory	TCP port
Persistent storage		
sklmAppVolume	Mandatory	Persistent storage to store the application server configuration and metadata information. Sample value: /opt/ibm/wlp/usr/products

3. Ensure that the PostgreSQL container is running and ready to accept connections.
4. Run the IBM Security Key Lifecycle Manager application Docker container by using the environment list file or specifying the parameters.
   Sample command with environment list file:

   ```
   docker run --name sklm_test -itd -h sklm.com -p 9443:9443 -p
   3801:3801 -p 5696:5696 -p 1441:1441  --env-file=sklmenvp_beta1.txt  -
   v sklmAppVolume_new:/opt/ibm/wlp/usr/products ibmcom/sklm
   ```

   Sample command with parameters:

   ```
   docker run --name sklm -itd -h sklm.com -p 9443:9443 -p 3801:3801 -p
   5696:5696 -p 1441:1441  -e LICENSE=accept -e
   SKLMADMIN_USERNAME=sklmadminuser -e KEY_STORE_PWD=Example@keystore123
   -e SKLMADMIN_PASSWORD=Example@admin123 -e DB_HOST=172.x.x.x -e
   DB_PORT=5432 -e SKLM_SEED=68d95f0081f1dbfc0b06de9b0916df1c -e
   DB_PASSWORD=Example@db2 -e DB_TYPE=postgres -e DB_USER=sklmdb41 -e
   DBNAME=sklmdb41 -v sklmAppVolume:/opt/ibm/wlp/usr/products
   ibmcom/sklm
   ```

   Note: The container might take a few minutes to start. You can monitor the progress by using the docker logs command.

5. Launch the IBM Security Key Lifecycle Manager graphical user interface:

   ```
   https://ip-address:port/ibm/SKLM/login.jsp
   ```

6. On the Configuration page that appears, click the License Agreements link to review the license terms, and then select the **I accept the terms in the License Agreements** check box.
7. Click **Activate License**.
8. Upload the IBM Security Key Lifecycle Manager license activation file and activate the license.
9. Click **Login**.
10. Log in to the IBM Security Key Lifecycle Manager graphical user interface with the Administrator user credentials (sklmadmin).

From the Welcome page, configure the drive types, keys, and certificates that your organization requires, or get started with using the product. See Working with IBM Security Key Lifecycle Manager.

Deploying IBM Security Key Lifecycle Manager with Db2 database using Docker

See this section for instructions on deploying IBM Security Key Lifecycle Manager with IBM Db2 as database.

Prerequisites

- Ensure that the host system meets these minimum system requirements:

Resource	Requirement
CPU	4 Cores
Memory	8 GB
Disk space	100 GB
Operating system and Supported architectures	Linux o x86_64 o s390x

- Install Docker engine on the host system. For instructions, see https://docs.docker.com/.
- Ensure that you have an account on the Docker Hub.
- To obtain the license activation file for IBM Security Key Lifecycle Manager, send us an email at: ibmsklm@in.ibm.com.
- Set up IBM Db2 by using one of the following options:
  - **Obtain the IBM Db2 container and customize it for IBM Security Key Lifecycle Manager**

Note: You can customize IBM Db2 for IBM Security Key Lifecycle Manager only with the **Standard** or **Advanced** edition of IBM Db2. Ensure that you are using the required license key for one of these editions. The file type for the license is **.lic**. For example, db2awse_c_np.lic.

To obtain the IBM Db2 image, go to the IBM Db2 container.
To customize the IBM Db2 container:

1. Download the attached file and extract its content in a directory on the host system.
2. Edit the **Dockerfile.sample** file, as required, and save the file. You can use any text editor.
3. Run the following command from the directory where the **Dockerfile.sample** file is extracted:
4. `docker build -t sklmdb -f Dockerfile.sample --no-cache .`
5. Run the customized IBM Db2 container.
   For example:

   ```
   docker run --name sklmdb --restart=always --detach --
   ipc="" --cap-add=IPC_OWNER -p 50000:50000 -e
   LICENSE=accept -e DB2INSTANCE=sklmdb41 -e
   DB2INST1_PASSWORD=Example@db2 -e DBNAME=sklmdb41 -v
   sklmDb2Volume:/database sklmdb
   ```

   For more information, see https://hub.docker.com/r/ibmcom/db2.

- **Use an existing on-premise or standalone version of IBM Db2**

  You can use an existing version of IBM Db2 and create an empty or blank database.

  Note: Minimum supported version of the standalone IBM Db2 is Version 11.1.4.4 interim fix 1.

- **Note**: The IBM Db2 container might take a few minutes to start. You can monitor the progress by using the docker logs command.
-
- Procedure
-
- Complete the following steps on the host system:
  1. Log in to Docker Hub.
  2. (*Optional*) Create an environment variable list file (for example, sklmenv) with the parameters for the IBM Security Key Lifecycle Manager container:
     - **Parameter list**

Parameter	**Mandatory/ Optional**	**Description**
Container name		
name	Mandatory	Specify a name for the container**.**

Environment variables		
DB_PASSWORD	Mandatory	Password to connect to the database instance where the IBM Security Key Lifecycle Manager database is running.
DB_TYPE	Optional	Type of the database. Default value: db2 Other possible value: postgres **Note**: This parameter is ignored in the subsequent docker run commands when the same value of the sklmAppVolume parameter is used.
DB_USER	Optional	User name of the database. Default value: sklmdb41
DBNAME	Optional	Name of the database. Default value: sklmdb41
DB_PORT	Mandatory	Port number of the database instance where the IBM Security Key Lifecycle Manager database is running
DB_HOST	Mandatory	IP address or fully qualified host name of the system that hosts the database instance where the IBM Security Key Lifecycle Manager database is running. You can use the same system to host the database instance and the application Docker container, or choose a different system for each of them.
LICENSE	Mandatory	Variable to accept license terms. Specify value as "**accept**".
SKLM_SEED	Mandatory	Secret passcode that is unique for a deployment, and must be stored securely. The value is a random string of 32 or 64 characters that you can generate using an external utility. **Note**: Ensure that the value of this parameter in the subsequent docker run commands is the same as that used in the first docker run

		command, when the same value of the sklmAppVolume parameter is used.
SKLMADMIN_USERNAME	Optional	User name of the IBM Security Key Lifecycle Manager administrator. You can specify only alphanumeric characters. Default value: sklmadmin **Note**: This parameter is ignored in the subsequent docker run commands when the same value of the sklmAppVolume parameter is used.
SKLMADMIN_PASSWORD	Mandatory	Password for the IBM Security Key Lifecycle Manager administrator user that is specified in the SKLMADMIN_USERNAME parameter. **Note**: This parameter is ignored in the subsequent docker run commands when the same value of the sklmAppVolume parameter is used.
KEY_STORE_PWD	Optional	Password for the IBM Security Key Lifecycle Manager keystore. Default value: SKLMWebAS **Note**: Ensure that the value of this parameter in the subsequent docker run commands is the same as that used in the first docker run command, when the same value of the sklmAppVolume parameter is used.
Port numbers		
9443	Mandatory	Port number for the graphical user interface.
5696	Mandatory	KMIP port
1441	Mandatory	SSL port
3801	Mandatory	TCP port
Persistent storage		
sklmAppVolume	Mandatory	Persistent storage to store the application server configuration and metadata information.

		Sample value: /opt/ibm/wlp/usr/products

3. Ensure that the IBM Db2 container is running and ready to accept connections.
4. Run the IBM Security Key Lifecycle Manager application Docker container by using the environment list file or specifying the parameters.

   Sample command with environment list file:

   ```
   docker run --name sklmapp -itd -h sklm.com -p 9443:9443 -p
   3801:3801 -p 5696:5696 -p 1441:1441  --env-
   file=sklmenv_beta1.txt -v
   sklmAppVolume_db2:/opt/ibm/wlp/usr/products ibmcom/sklm
   ```

   Sample command with parameters:

   ```
   docker run --name sklm -itd -h sklm.com -p 9443:9443 -p
   3801:3801 -p 5696:5696 -p 1441:1441  -e LICENSE=accept -e
   KEY_STORE_PWD=Example@keystore123 -e
   SKLMADMIN_USERNAME=sklmadminuser -e
   SKLMADMIN_PASSWORD=Example@admin123 -e DB_HOST=172.x.x.x -e
   DB_PORT=50000 -e SKLM_SEED=68d95f0081f1dbfc0b06de9b0916df1c -e
   DB_PASSWORD=Example@db2 -e DB_TYPE=db2 -e DB_USER=sklmdb41 -e
   DBNAME=sklmdb41 -v sklmAppVolume_db2:/opt/ibm/wlp/usr/products
   ibmcom/sklm
   ```

   Note: The container might take a few minutes to start. You can monitor the progress by using the docker logs command.

5. Launch the IBM Security Key Lifecycle Manager graphical user interface:

   ```
   https://ip-address:port/ibm/SKLM/login.jsp
   ```

6. On the Configuration page that appears, click the License Agreements link to review the license terms, and then select the **I accept the terms in the License Agreements** check box.
7. Click **Activate License**.
8. Upload the IBM Security Key Lifecycle Manager license activation file and activate the license.
9. Click **Login**.
10. Log in to the IBM Security Key Lifecycle Manager graphical user interface with the Administrator user credentials (sklmadmin).

From the Welcome page, configure the drive types, keys, and certificates that your organization requires, or get started with using the product. See Working with IBM Security Key Lifecycle Manager.

User management

Users, user roles, and user groups control who has access to the product, which tasks they can perform, and which data they can access.

With support for WebSphere Application Server Liberty, IBM Security Key Lifecycle Manager application container now includes the user management feature.

Use the User Management REST APIs to configure and manage user roles and groups.

Click here to download the User management REST API PDF.

- **User management REST APIs**

Action on	URL	Description
Users	GET /SKLM/rest/v1/ckms /usermanagement/users	Retrieve details for all users in IBM Security Key Lifecycle Manager.
	GET /SKLM/rest/v1/ckms /usermanagement/users /{userName}	Retrieve the role and group details for a specific user.
	DELETE /SKLM/rest/v1/ckms /usermanagement/users /{userName}	Delete all roles and groups associated with a specific user.
	POST /SKLM/rest/v1/ckms /usermanagement/rolesuser	Assign a role to a user.
	DELETE /SKLM/rest/v1/ckms /usermanagement/rolesuser	Delete the assigned role from a user.
	To add a user, see Configuring a basic user registry for Liberty. **Note**: The **server.xml** file is present in the serverConfig directory in the sklmAppVolume volume.	
User Roles	GET /SKLM/rest/v1/ckms /usermanagement/roles	Retrieve list of all user roles.
	GET /SKLM/rest/v1/ckms /usermanagement/roles /{roleName}	Retrieve details such as role description, assigned users, assigned groups for a specific role.
	GET /SKLM/rest/v1/ckms /usermanagement/groups /{groupName}	Retrieve user group details such as assigned roles and assigned users for a user group.

Action on	URL	Description
	POST /SKLM/rest/v1/ckms /usermanagement/roles /{roleName}	Add a user role.
	PUT /SKLM/rest/v1/ckms /usermanagement/roles /{oldRoleName}	Update an existing user role.
	DELETE /SKLM/rest/v1/ckms /usermanagement/roles /{roleName}	Delete an existing user role.
User Groups	GET /SKLM/rest/v1/ckms /usermanagement/groups	Retrieve all the user groups in IBM Security Key Lifecycle Manager.
	POST /SKLM/rest/v1/ckms /usermanagement/groups /{groupName}	Add a user group.
	PUT /SKLM/rest/v1/ckms /usermanagement/groups /{oldGroupName}	Update an existing user group.
	DELETE /SKLM/rest/v1/ckms /usermanagement/groups /{groupName}	Delete an existing user group.
	POST /SKLM/rest/v1/ckms /usermanagement/groupuser	Assign a user to a user group.
	DELETE/SKLM/rest/v1/ckms /usermanagement/groupuser	Delete a user from a user group.
	POST /SKLM/rest/v1/ckms /usermanagement/rolesgroup	Assign a role to a user group.
	DELETE /SKLM/rest/v1/ckms /usermanagement/rolesgroup	Remove a role from a user group.

Restrictions and limitations

This Beta version of the containerized IBM Security Key Lifecycle Manager application has the following limitations:

- The following features are not supported:
  - CLI commands. Alternatively, use REST APIs. Swagger UI is now integrated with IBM Security Key Lifecycle Manager, and you can use it to call any REST API.
  - Multi-Master cluster
  - Replication
  - LDAP

  - HSM
  - Security standards: FIPS, Suite B, SP800-131a, SSL/TLS Cipher suites, and CA-signed Certificate for Liberty
  - User and database password change from the user interface
- No password policy is applicable for the SKLMADMIN_PASSWORD and KEY_STORE_PWD values.
- User to be assigned to the IBM Security Key Lifecycle Manager application must have at least one role assigned to them.
- Server restart is not supported. To restart the server, you must restart the application container.
- After completing the user management changes, you must restart the application container.
- To support the keys rollover feature when using the PostgreSQL database, modify the postgres.conf file that exists in the Persistent storage or volume. In the Resource usage section, replace `max_prepared_transactions = 0` by `max_prepared_transactions = 100` and then restart the PostgreSQL container.
- The User Profile page is not functional.

Known issues

Here is a list of known issues in this Beta version:

- After you restore data from a previously backed-up application container, users and their associations might get corrupted.
- Some backup files might not be displayed on the Backup and Restore page.

License (Terms and Conditions)
By using the IBM Security Key Lifecycle Manager container image, you are agreeing to the terms and conditions given here: Software License Agreement

Feedback and support
For more information, any questions or feedback, send us an email at: ibmsklm@in.ibm.com

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, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785

US

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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

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

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

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

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 http://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.

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

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Product Number:

IBM Confidential