IBM Security Key Lifecycle Manager

An Chen
Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (April 2020)

This edition applies only to the product versions described within.

This document was created or updated on April 1, 2020.
## Contents

**Notices** ................................................................. v
**Trademarks** ............................................................ vi

**Preface** ................................................................. vii
**Authors** ................................................................. vii
**Now you can become a published author, too!** .............................. vii
**Comments welcome** .................................................. viii
**Stay connected to IBM Redbooks** ..................................... viii

**Chapter 1. IBM Security Key Lifecycle Manager Installation and Integration** .......................... 1
  1.1 Installing IBM Security Key Lifecycle Manager ................................................. 2
  1.2 Installing fix pack for IBM Security Key Lifecycle Manager ............................... 10
  1.3 LDAP integration by using WebSphere Integrated Solutions Console ....................... 16
    1.3.1 Add LDAP repository to the federated repository ......................................... 16
    1.3.2 Create the database for LDAP configuration and update data source for WIM .... 21
    1.3.3 Create a database-based repository ............................................................. 23
  1.4 Configuring signed CA certificates for SKLM portal and WebSphere console access 29

**Chapter 2. IBM Security Key Lifecycle Manager Configuration** ......................................... 39
  2.1 Configuring SSL/KMIP certificate for IBM Security Key Lifecycle Manager server .......... 40
    2.1.1 Create a self-signed server certificate ......................................................... 40
    2.1.2 Create a certificate request for a signed CA server certificate ....................... 42
  2.2 Backup and Restore IBM Security Key Lifecycle Manager configuration .................... 46
    2.2.1 Backup IBM Security Key Lifecycle Manager configuration ............................. 47
    2.2.2 Restore IBM Security Key Lifecycle Manager configuration ............................ 48
  2.3 Configuring Replication for IBM Security Key Lifecycle Manager configuration .......... 51
    2.3.1 Configure the master server for replication ............................................... 52
    2.3.2 Configure the clone server for replication .................................................. 54
  2.4 Configuring Multi-Master Cluster ............................................................... 57
    2.4.1 Setting up minimal deployment of a Multi-Master cluster ............................. 58
    2.4.2 HADR takeover scenarios .............................................................................. 63
  2.5 Migrating from an earlier version of IBM Security Key Lifecycle Manager ............... 71
    2.5.1 Inline Migration .............................................................................................. 72
    2.5.2 Cross Migration .............................................................................................. 74

**Related publications** ................................................... 79
**IBM Redbooks** ............................................................. 79
**Online resources** .......................................................... 79
**Help from IBM** ............................................................. 79
Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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 grant 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

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

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

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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.

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

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 actual people or business enterprises 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.
Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, 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 http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

Db2®, IBM®, ProtecTIER®, Redbooks®, Redbooks (logo)®, WebSphere®, Tivoli®

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

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

Other company, product, or service names may be trademarks or service marks of others.
Preface

In this IBM® Redbook we detail the installation, integration, and configuration of IBM Security Key Lifecycle Manager.

Authors

This book was produced remotely, in Australia, by An Chen on behalf of the IBM Redbooks, San Jose Center.

An Chen is an IBM Lab Service storage specialist based in Australia. He joined IBM in 2007 and has more than 10 years of experience in design and delivery storage solutions for Open Systems. His areas of expertise include file and block storage implementation, SAN, ProtecTIER®, performance assessment, disaster recovery and high availability solutions. He holds a Master of Science degree in Internetworking from University of Technology, Sydney.

Thanks to the following people for their contributions to this project:

Connor Fawcett
IBM Manchester Lab

The project was managed by:

Jon Tate
IBM ITSO

Now you can become a published author, too!

Here’s an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks® residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at: ibm.com/redbooks/residencies.html
Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online Contact us review Redbooks form found at:
  ibm.com/redbooks

- Send your comments in an email to:
  redbooks@us.ibm.com

- Mail your comments to:
  IBM Corporation, IBM Redbooks
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:
  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:
  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:
  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

- Stay current on recent Redbooks publications with RSS Feeds:
  http://www.redbooks.ibm.com/rss.html
IBM Security Key Lifecycle Manager Installation and Integration

This chapter describes the tasks associated with initial installation, installing fix packs, integrating with LDAP for centralized authentication and configuring signed CA certificate for secured communication with the IBM Security Key Lifecycle Manager portal and WebSphere® console access.

- Installing IBM Security Key Lifecycle Manager
- Installing fix pack for IBM Security Key Lifecycle Manager
- LDAP integration by using WebSphere Integrated Solutions Console
- Configuring signed CA certificates for SKLM portal and WebSphere console access
1.1 Installing IBM Security Key Lifecycle Manager

Before installing IBM Security Key Lifecycle Manager, make sure that the hardware and operating system meet the prerequisites listed on the knowledge center and ensure the installation guidelines are followed. Refer to the following links for the specific prerequisites and guidelines for each component.

The following section covers the steps to install IBM Security Key Lifecycle version 3.0.1 in graphic mode on a RHEL server.

- Hardware requirements
  https://ibm.biz/BdqdjF
- Operating system requirements
  https://ibm.biz/BdqdjX
- Software requirements
  https://ibm.biz/BdqdjP
- Installation guidelines
  https://ibm.biz/Bdqdjy

The following section covers the steps to install IBM Security Key Lifecycle version 3.0.1 in graphic mode.

Extract the installation package, the launchpad.sh script is extracted to the disk1 directory, as shown in Example 1-1.

**Example 1-1 Extract installation packages**

```
[root@sklm SKLM301]# tar -zxvf SKLM3.0.1_LIN64_1F2_ML.tar.gz
[root@sklm SKLM301]# tar -zxvf SKLM3.0.1_LIN64_2F2_ML.tar.gz
[root@sklm SKLM301]# ls -l
```

```
total 6559017
drwxr-xr-x 1 root root 131072 Dec  5  2018 disk1
drwxr-xr-x 1 root root 131072 Dec  5  2018 disk2
-rwxr-xr-x 1 root root 3675421863 Jun  4  2019 SKLM3.0.1_LIN64_1F2_ML.tar.gz
-rwxr-xr-x 1 root root 3040748415 Jun  4  2019 SKLM3.0.1_LIN64_2F2_ML.tar.gz
```

Run the launchpad.sh script to launch the installation wizard, as shown in Example 1-2.

**Example 1-2 Launch the installation wizard**

```
[root@sklm SKLM301]# ./launchpad.sh
```

Choose the locale for Installation Manager.

1. English
2. French
3. Portuguese
4. Spanish
5. Japanese
6. Korean
7. Simplified Chinese
8. Traditional Chinese
Enter the number that is corresponding to the locale you want to use for the installation (English is selected by default): 1

Locale Selected is English.

Starting IBM Security Key Lifecycle Manager.

No pre-installed IBM Installation Manager found on the system.

Installing IBM Security Key Lifecycle Manager 3.0.1

Select the components to be installed, all components are required for a new installation, as shown in Figure 1-1. Click Next for the prerequisite check, and fix prerequisite issues if there are any.

![Figure 1-1 Components to be installed](image)

Review and accept the terms in the license agreements, as shown in Figure 1-2 on page 4.
Specify the installation path for the Shared Resources Directory and IBM Installation Manager, Figure 1-3 on page 4.
Specify the installation path for the Db2® and WebSphere application, as shown in Figure 1-4.

![Figure 1-4  Db2 and WebSphere application installation path](image)

Confirm the packages to be installed, as shown in Figure 1-5 on page 5.

![Figure 1-5  Confirm packages to be installed](image)
Specify the credentials, and home directory for the Db2 instance owner account as well as the Db2 port, as shown in Figure 1-6.

Figure 1-6   Db2 instance owner account details

Specify the credentials for the WebSphere administrator wasadmin account, the WebSphere instance owner SKLMadmin account, and WebSphere associated ports, as shown in Figure 1-7.
Uncheck the Migrate Encryption Key Manager (EKM) option unless the installation is intended for a migration from EKM, as shown in Figure 1-8 on page 7.
Review the installation summary and click on Install to install IBM Security Key Lifecycle Manager, as shown in Figure 1-9.

![IBM Installation Manager](image)

Figure 1-9  Installation summary information

After a successful installation, select the None option and click Finish to exit the installation wizard, as shown in Figure 1-10.
Figure 1-10  Summary after a successful installation

Logon to the SKLM application portal (https://<ip-address>:port.ibm/SKLM/login.jsp) to check the port configurations are correctly loaded on the dashboard, as shown in Figure 1-11.

Figure 1-11  SKLM dashboard port configuration
Click the question mark at the top right corner and select About to verify the installed software details, as shown in Figure 1-12.

![Figure 1-12   Installed software details](image)

1.2 Installing fix pack for IBM Security Key Lifecycle Manager

The Fix Central website provides fixes and updates for software, hardware, and operating system of your system. IBM Security Key Lifecycle Manager fix packs are published on the Fix Central Website.

The following section covers steps to install fix pack FP003 for IBM Security Key Lifecycle Manager version 3.0.1 in graphic mode on a RHEL server. It is always important to backup the current WebSphere and SKLM configuration before installing the fix pack. The backup and restore operation for SKLM configuration is covered in Chapter 2, “IBM Security Key Lifecycle Manager Configuration” on page 39.

Backup the WebSphere application files as shown in Example 1-3.

**Example 1-3   Backup WebSphere application files**

```
[root@sklm ~]# /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1
ADMU0116I: Tool information is being logged in file
/opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/stopServer.log
ADMU0128I: Starting tool with the KLMProfile profile
ADMU3100I: Reading configuration for server: server1
Realm/Cell Name: <default>
Username: wasadmin
Password: [obscured]
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server server1 stop completed.
```
Create the /sklminstall_linuxfp directory, transfer the fix pack to the folder, extract the package and run the updateSKLM.sh script to launch the update wizard (the script requires executable permission), as shown in Example 1-4.

**Example 1-4  Prepare for the fix pack installation**

```
[root@sklm sklminstall_linuxfp]# ls
3.0.1-ISS-SKLM-FP0003-Linux.tar.gz
[root@sklm sklminstall_linuxfp]# tar -zxvf 3.0.1-ISS-SKLM-FP0003-Linux.tar.gz
[root@sklm sklminstall_linuxfp]# ls -l
-rwxr-xr-x 1 root root 116514653 Jan 14 01:26 3.0.1-ISS-SKLM-FP0003-Linux.tar.gz
-rwxr-xr-x 1 root root 4224 Oct 18 07:54 silent_updateSKLM.sh
drwxr-xr-x 7 root root 234 Oct 18 07:54 sklm
-rwxr-xr-x 1 root root 4934 Oct 18 07:54 SKLM_Uninstall_Linux_Resp.xml
-rwxr-xr-x 1 root root 375 Oct 18 07:54 updateSKLM.xml
[root@sklm sklminstall_linuxfp]# chmod +x updateSKLM.sh
[root@sklm sklminstall_linuxfp]# ./updateSKLM.sh /opt/IBM/InstallationManager
```

The wizard identifies the current installed version and fix pack level, select IBM Security Key Lifecycle Manager v3.0.1 and click Next to continue, as shown in Figure 1-13 on page 12.
Select the fix pack to be installed and click Next to continue, as shown in Figure 1-14.

Review and accept the terms in the license agreement and click Next to continue, as shown in Figure 1-15 on page 13.
Select the features to be installed and click Next to continue, as shown in Figure 1-16.

Type in the password for the wasadmin, SKLMadmin and sklmdb31 accounts, and click Validate Credentials then Next to continue, as shown in Figure 1-17 on page 14.
Figure 1-17   Validate credentials

Confirm the installation details and click Update to install the fix pack, as shown in Figure 1-18.

Figure 1-18   Installation details
After a successful installation, review the installation summary and click Finish to exit the wizard as shown in Figure 1-19 on page 15.

![Figure 1-19 Summary after a successful installation](image)

Logon to the SKLM application portal and click the question mark at the top right corner and select About to verify the installed software details, as shown in Figure 1-20.

![Figure 1-20 Installed software details](image)
1.3 LDAP integration by using WebSphere Integrated Solutions Console

Before you integrate LDAP with IBM Security Key Lifecycle Manager by using WebSphere Integrated Solutions Console, you must run the backup tasks.

You might need to restore the following data to the state as it was before the LDAP configuration steps were run:

- WebSphere Application Server configuration data for IBM Security Key Lifecycle Manager
- IBM Security Key Lifecycle Manager application data

Following the procedures [here](#) to backup IBM Security Key Lifecycle Manager profile (KLMProfile) in WebSphere Application Server.

1.3.1 Add LDAP repository to the federated repository

Log on to the WebSphere Integrated Solutions Console (https://<ip address>:9083.ibm/console/logon.jsp) as wasadmin, as shown in Figure 1-21.

![WebSphere Integrated Solutions Console](#)

Figure 1-21 WebSphere Integrated Solutions Console

Navigate to Security → Global security, in the User account repository section, select Federated repository and click Configure, as shown in Figure 1-22 on page 17.
Click Add repositories to create a new LDAP based repository, as shown in Figure 1-23.

Click New Repository and select LDAP repository, as shown in Figure 1-24 on page 18.
Specify the details for the LDAP repository to be created, such as the repository identifier, directory type, and details of the binding account, as shown in Figure 1-25 on page 19.
Click Ok and specify a base unique distinguished name, click Ok then Save to save the configuration, as shown in Figure 1-26 on page 20.
Verify the LDAP repository has been created and is listed in the realm, as shown in Figure 1-27.

Restart the WebSphere Application Server to make the changes effective, as shown in Example 1-5.
Example 1-5  Restart WebSphere Application Server

[root@sklm ~]# /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1
ADMU0116I: Tool information is being logged in file

/opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/stopServer.log
ADMU0128I: Starting tool with the KLMProfile profile
ADMU3100I: Reading configuration for server: server1
Realm/Cell Name: <default>
Username: wasadmin
Password:  
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server server1 stop completed.

[root@sklm ~]# /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
ADMU0116I: Tool information is being logged in file

/opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/startServer.log
ADMU0128I: Starting tool with the KLMProfile profile
ADMU3100I: Reading configuration for server: server1
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server server1 open for e-business; process id is 26084

Log on to the WebSphere Integrated Solutions Console as wasadmin to check that the AD
users are discoverable, as shown in Figure 1-28 on page 21.

1.3.2  Create the database for LDAP configuration and update data source for
WIM

Create the database for LDAP configuration and connect to the USERDB31 to verify, as
shown in Example 1-6.

Example 1-6  Create database

[root@sklm ~]# su - sklmdb31

Figure 1-28  Verify AD users
Last login: Thu Jan 16 22:33:31 EST 2020 on pts/1
[sklmdb31@sklm ~]$ db2 create database USERDB31 using codeset UTF-8 territory US DB2000001 The CREATE DATABASE command completed successfully.

[sklmdb31@sklm ~]$ db2 connect to userdb31

Database Connection Information

Database server = DB2/LINUXX8664 11.1.2.2
SQL authorization ID = SKLMDB31
Local database alias = USERDB31

[sklmdb31@sklm ~]$ db2 connect reset

Log on to the WebSphere Integrated Solutions Console as wasadmin, select WIM Data Source to update the data source, as shown in Figure 1-29 on page 22.

Figure 1-29  Update WIM data source

Update the database name from SKLMDB31 to USERDB31, as shown in Figure 1-30.
Chapter 1. IBM Security Key Lifecycle Manager Installation and Integration

1.3.3 Create a database-based repository

Create a database-based repository, as shown in Example 1-8.

Example 1-8  Create database-based repository

    [root@sklm ~]# /opt/IBM/WebSphere/AppServer/bin/wsadmin.sh -user wasadmin -password P@ssword123 -lang jython -f /opt/IBM/SKLMV301/bin/LDAPIntegration/createDBRepos.py /opt/IBM/WebSphere/AppServer USERDB31 sklmdb31 P@ssword123 50050

Verify the database-based repository created and listed in the realm, as shown in Figure 1-31.
Remove the groups from the default file based repository, as shown in Example 1-9.

Example 1-9  Remove groups

[root@sklm ~]# /opt/IBM/WebSphere/AppServer/bin/wsadmin.sh -user wasadmin
-password P@ssword123 -lang jython -f
/opt/IBM/SKLMV301/bin/LDAPIntegration/removeGroupsFromDefRepos.py
WASX7209I: Connected to process "server1" on node SKLMNode using SOAP connector;
The type of process is: UnManagedProcess
Removing LTOAdmin Group...
Removed LTOAdmin Group...
Removing LTOAuditor Group...
Removed LTOAuditor Group...
Removing LTOOperator Group...
Removed LTOOperator Group...
Removing klmBackupRestoreGroup ...
Removed klmBackupRestoreGroup ...
Removing klmGUICLIAccessGroup...
Removed klmGUICLIAccessGroup...
Removing klmSecurityOfficerGroup...
Removed  klmSecurityOfficerGroup...
Saving config

Navigate to the Enterprise Applications page and select the sklm_kms resource, as shown in Figure 1-32.
Figure 1-32  Enterprise Applications

Select the Security role to user/group mapping, as shown in Figure 1-33.

Figure 1-33  Security role to user/group mapping

Select the administrator role and click map groups, as shown in Figure 1-34 on page 26.
Select the klmGUICLIACcessGroup and click the left arrow to remove the file based group from the administrator role and save the configuration, as shown in Figure 1-35.

Restart the WebSphere Application Server, as shown in Example 1-5 on page 21.

Add the deleted file based groups to the database-base repository, as shown in Example 1-10.

Example 1-10  Add groups to database-based repository

```
[root@sklm ~]# /opt/IBM/WebSphere/AppServer/bin/wsadmin.sh -user wasadmin -password P@ssword123 -lang jython -f /opt/IBM/SKLVMV301/bin/LDAPIntegration/addGroupsToDBRepos.py
```
WASX7209I: Connected to process "server1" on node SKLMNode using SOAP connector;
The type of process is: UnManagedProcess
Creating LTOAdmin Group...
Created LTOAdmin Group in DB Repos
Creating LTOAuditor Group...
Created LTOAuditor Group in DB Repos
Creating LTOOperator Group...
Created LTOOperator Group in DB Repos
Creating klmBackupRestoreGroup Group...
Created klmBackupRestoreGroup in DB Repos
Creating klmGUICLIAccess Group...
Created klmGUICLIAccessGroup in DB Repos
Creating klmSecurityOfficer Group...
Created klmSecurityOfficerGroup in DB Repos
Saving config

Update the LDAP based repository with the group configuration from the data base repository, as shown in Example 1-11.

Example 1-11  Update the LDAP based repository
[root@sklm ~]# /opt/IBM/WebSphere/AppServer/bin/wsadmin.sh -user wasadmin
-password P@ssword123 -lang jython -f
/opt/IBM/SKLMV301/bin/LDAPIntegration/updateLDAPReposConfig.py ITSO-AD
WASX7209I: Connected to process "server1" on node SKLMNode using SOAP connector;
The type of process is: UnManagedProcess
WASX7303I: The following options are passed to the scripting environment and are available as arguments that are stored in the argv variable: "[ITSO-AD]"
Updating LDAP Repository config
CWWIM5028I  The configuration is saved in a temporary workspace. You must use the "$AdminConfig save" command to save it in the master repository.
Updated LDAP Repository config... with repositoriesForGroups = SKLMDBRepos
Saving config

Map the administrator role to klmGUICLIAccessGroup for integrating IBM Security Key Lifecycle Manager with LDAP user repositories and save the configuration, as shown in Figure 1-36.
Restart the WebSphere Application Server, as shown in Example 1-5 on page 21.

Add LDAP users/groups to IBM Security Key Lifecycle Manager Application Groups to integrate IBM Security Key Lifecycle Manager with the LDAP user repositories, as shown in Example 1-12.

Example 1-12   Add LDAP users/groups to the klmGUICLIAccessGroup

```bash
[root@sklm ~]# /opt/IBM/WebSphere/AppServer/bin/wsadmin.sh -user wasadmin -password P@ssword123 -lang jython -f /opt/IBM/SKLMV301/bin/LDAPIntegration/addLDAPUserToGroup.py 'CN=SecurityAdmins,CN=Users,DC=itso,DC=ibm,DC=com' klmGUICLIAccessGroup
WASX7209I: Connected to process "server1" on node SKLMNode using SOAP connector;
The type of process is: UnManagedProcess
WASX7303I: The following options are passed to the scripting environment and are available as arguments that are stored in the argv variable: "[CN=SecurityAdmins,CN=Users,DC=itso,DC=ibm,DC=com, klmGUICLIAccessGroup]"
Adding user - CN=SecurityAdmins,CN=Users,DC=itso,DC=ibm,DC=com to group - klmGUICLIAccessGroup
CN=SecurityAdmins,CN=Users,DC=itso,DC=ibm,DC=com
Added user - CN=SecurityAdmins,CN=Users,DC=itso,DC=ibm,DC=com to group - klmGUICLIAccessGroup
Saving config
```

For any LDAP users/groups who need IBM Security Key Lifecycle Manager admin access, the user must be made a member of klmSecurityOfficerGroup as well, as shown in Example 1-13.

Example 1-13   Add LDAP users/groups to the klmSecurityOfficerGroup

```bash
[root@sklm ^]# /opt/IBM/WebSphere/AppServer/bin/wsadmin.sh -user wasadmin -password P@ssword123 -lang jython -f /opt/IBM/SKLMV301/bin/LDAPIntegration/addLDAPUserToGroup.py 'CN=SecurityAdmins,CN=Users,DC=itso,DC=ibm,DC=com' klmSecurityOfficerGroup
```

Figure 1-36   Map administrator role to klmGUICLIAccessGroup
WASX7209I: Connected to process "server1" on node SKLMNode using SOAP connector; The type of process is: UnManagedProcess
WASX7303I: The following options are passed to the scripting environment and are available as arguments that are stored in the argv variable: "[CN=SecurityAdmins,CN=Users,DC=itso,DC=ibm,DC=com, klmSecurityOfficerGroup]"
Adding user - CN=SecurityAdmins,CN=Users,DC=itso,DC=ibm,DC=com to group - klmSecurityOfficerGroup
CN=SecurityAdmins,CN=Users,DC=itso,DC=ibm,DC=com
Added user - CN=SecurityAdmins,CN=Users,DC=itso,DC=ibm,DC=com to group - klmSecurityOfficerGroup
Saving config

Logon to the SKLM portal with an LDAP account that is a member of the SecurityAdmins group to verify the configuration, as shown in Figure 1-37 on page 29.

![Figure 1-37 Logon to the SKLM portal with a LDAP account](image)

### 1.4 Configuring signed CA certificates for SKLM portal and WebSphere console access

Before you begin, ensure that you have completed the following tasks:

- Submit a Certificate Signing Request (CSR) for Certificate Authority (CA) approval in a WebSphere Application Server environment
- You have received the certificates from the Certificate Authority

Logon to the IBM WebSphere Integrated Solutions Console (https://<IP address>:9083/ibm/console/logon.jsp), select Security and then SSL certificate and Key management, and select Key Stores and certificates, as shown in Figure 1-38.
Select the NodeDefaultKeyStore resource, as shown in Figure 1-39.

Select Personal certificate request to generate the signing request, as shown in Figure 1-40.
Click New to specify the certificate details, as shown in Figure 1-41 on page 31.

The default location for the signing request is `<WAS HOME>/profiles/KLMProfile/etc`, as shown in Figure 1-42.
Send the request to a signing authority and upload the signed certificate as well as the root certificate of the signing authority to the `<WAS HOME>/profiles/KLMProfile/etc` directory, click Receive from a certificate authority to import the signed certificate, as shown in Figure 1-43 on page 32.

Specify the file name of the signed certificate to import, click Ok and save the configuration as shown in Figure 1-44.
Select the signer certificates to import the root certificate and intermediate certificates, as shown in Figure 1-45 on page 33.

Select Add and specify the details of the root certificate, click Ok and save the configuration, as shown in Figure 1-46.
Select the NodeDefaultKeyStore to verify the certificates are imported correctly, as shown in Figure 1-47 on page 34.

Select the default certificate and click Replace to replace the default with the signed certificate, as shown in Figure 1-48.
Select the certificate from the drop down menu, and click Ok and save the configuration, as shown in Figure 1-49 on page 35.

Restart the WebSphere Application Server and add the signer to the trust stores, as shown in Example 1-14.

Example 1-14 Add new signer certificate to trust store

[root@sklm ~]# /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1 -username wasadmin -password P@ssword123
ADMU0116I: Tool information is being logged in file /opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/stopServer.log
ADMU0128I: Tool information is being logged in file /opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/stopServer.log

[End of Example 1-14]
ADMU3100I: Reading configuration for server: server1
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server server1 stop completed.

[root@sklm ~]# /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
ADMU0116I: Tool information is being logged in file

/opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/startServer.log
ADMU0128I: Starting tool with the KLMProfile profile
ADMU3100I: Reading configuration for server: server1
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server server1 open for e-business; process id is 19702

[root@sklm ~]# /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1 -username wasadmin -password P@ssword123
ADMU0116I: Tool information is being logged in file

/opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/stopServer.log
ADMU0128I: Starting tool with the KLMProfile profile
ADMU3100I: Reading configuration for server: server1

*** SSL SIGNER EXCHANGE PROMPT ***
SSL signer from target host 192.168.48.210 is not found in trust store
/opt/IBM/WebSphere/AppServer/profiles/KLMProfile/etc/trust.p12.
Here is the signer information (verify the digest value matches what is displayed at the server):

Subject DN:    CN=sklm.itso.ibm.com, OU=ITSO, O=IBM, L=SYD, ST=NSW, C=AU
Issuer DN:     CN=itso-DC-CA, DC=itso, DC=ibm, DC=com
Serial number: 4014134136904569007453891124786212800299026
Expires:       Fri Jan 29 18:15:49 EST 2021

Subject DN:    CN=itso-DC-CA, DC=itso, DC=ibm, DC=com
Issuer DN:     CN=itso-DC-CA, DC=itso, DC=ibm, DC=com
Serial number: 9484273844014498998820329267699508084
Expires:       Fri Jan 10 00:21:35 EST 2025

Add signer to the trust store now? (y/n) y
A retry of the request may need to occur if the socket times out while waiting for a prompt response. If the retry is required, note that the prompt will not be redisplayed if (y) is entered, which indicates the signer has already been added to the trust store.
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server server1 stop completed.

[root@sklm ~]# /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
ADMU0116I: Tool information is being logged in file

/opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/startServer.log
ADMU0128I: Starting tool with the KLMProfile profile
ADMU3100I: Reading configuration for server: server1
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server server1 open for e-business; process id is 20182

Open the browser to verify the connection is secured, as shown in Figure 1-50 on page 37.
IBM Security Key Lifecycle Manager Configuration

This chapter describes the tasks associated with creating self-signed or CA signed IBM Security Key Lifecycle Manager server SSL/KMIP certificate, backup/restore and configuring replication for IBM Security Key Lifecycle Manager configuration, configuring IBM Security Key Lifecycle Manager in a Multi-Master cluster and migrating from an earlier version of IBM Security Key Lifecycle Manager.

- Configuring SSL/KMIP certificate for IBM Security Key Lifecycle Manager server
- Backup and Restore IBM Security Key Lifecycle Manager configuration
- Configuring Replication for IBM Security Key Lifecycle Manager configuration
- Configuring Multi-Master Cluster
- Migrating from an earlier version of IBM Security Key Lifecycle Manager
2.1 Configuring SSL/KMIP certificate for IBM Security Key Lifecycle Manager server

After you install IBM Security Key Lifecycle Manager, you must configure secure communication by using SSL.

Logon to the IBM Security Key Lifecycle Manager portal, navigate to Advanced Configuration and select Server Certificates, and click Add to create a server certificate, as shown in Figure 2-1.

2.1.1 Create a self-signed server certificate

Select Create a self-signed certificate, specify the certificate details and validity period, then click Add certificate, as shown in Figure 2-2 on page 41.
Validate the status and expiration date of the created certificate, as shown in Figure 2-3.

Validate the status of the SSL/KMIP configuration from the dashboard, as shown in Figure 2-4 on page 42.
Restart the WebSphere instance to make the change effective, as shown in Figure 2-5.

2.1.2 Create a certificate request for a signed CA server certificate

Select Request certificate from a third-party provider, specify the certificate details and validity period, then click Add certificate, as shown in Figure 2-6 on page 43.
Validate the status and expiration date of the created certificate, as shown in Figure 2-7.

**Note:** The most recently created certificate from the IBM Security Key Lifecycle Manager portal becomes the active certificate for the server, which might break the communication between the configured devices and the server. Plan carefully when there is a need for a new server certificate for other purposes, such as replication.

The server certificate status is shown with a question mark and the certificate request is located in the `/opt/IBM/WebSphere/AppServer/products/sklm/data` directory, as shown in Example 2-1 on page 44.
Example 2-1  Certificate request

```
[root@sklm data]# pwd
/opt/IBM/WebSphere/AppServer/products/sklm/data
[root@sklm data]# ls -al
```
total 4
drwx------  4 root root  75 Feb  5 07:09 .
drwx-r-xr-x 14 root root 312 Jan 13 02:24 ..
-rw-r--r--  1 root root  962 Feb  5 07:09 200205070956-ITSO-SKLM-signed.csr
```
[root@sklm data]# cat 200205070956-ITSO-SKLM-signed.csr
```
-----BEGIN CERTIFICATE REQUEST-----
MIICkDCCAXgCAQAwGzEZMBCGAUExAMQSVRRTyITS0xNLXNpZ251ZDCASIwOQYJKoZIhvcNAQEB
BQADggbEPADCCAQgEBAKueWCEcXwRakTsxJxblcNQ/780aQ46V5hEt3cOh1biY+VY12PcZgRy
+/GCUB0I5fieA6/6HwMuU8Hoio+P+3VQ711TQvveNQ/6+11Z279g4KhNF9GMZenJ6Dej0WnXbE/jr
NE/1UsngN6JrfrP4UV5V8ma71mm91q1XKi+OeefDA9n8BMQnUm1mWcXO8D1818PAGhQpiXVsVbI/8
2B0ZpqXqNSV6uVUmqbd7r7cSxkYQOdiikP5P6W2yTt2rTATfQLeYoC0BYdOpapEkyPaTf/Gah
hBS4al1S9Wve0OBP9c59y6qbjbr7L4osJOEdcyEY/MA1117uhHuZg+Tn38CwEAAB0AWMC4CSqG
```
```
------END CERTIFICATE REQUEST-----
```

Send the certificate request to the trusted certificate authority to issue the certificate, as shown in Example 2-2.

Example 2-2  Signed CA certificate

```
[root@sklm data]# pwd
/opt/IBM/WebSphere/AppServer/products/sklm/data
[root@sklm data]# ls -al
```
total 8
drwx------  4 root root  103 Feb  5 07:31 .
drwxr-xr-x 14 root root  312 Jan 13 02:24 ..
-rw-r--r--  1 root root  962 Feb  5 07:09 200205070956-ITSO-SKLM-signed.csr
```
[root@sklm data]# cat 200205070956-ITSO-SKLM-signed.csr
```
-----BEGIN CERTIFICATE-----
MIIE3jCCA8agAwIBAgITEgAAABm9PUuTn+ZEQwAAAAAGTANBgkqhkiG9w0BAQsFADBVMwEQQYKZCII1zYPQlQQGRBYD29tMRmWSQYKZClmiZPyLQQGRYDaWIjtMRQw
EgYKZCIZmiZPyLQQGRYEAxRzbxETMBEGA1UEAAnMaXZrZby1EQ1DQTAeFw0yMDA0
MDUxMjIwNzEdMDExMjA1NzAyMDAyMBsGCSqGSIG1bD30EBAQUA4CAAwIBAgIigmUo
```
```
------END CERTIFICATE REQUEST-----
```

Send the certificate request to the trusted certificate authority to issue the certificate, as shown in Example 2-2.
Check the pending tasks on the IBM Security Key Lifecycle Manager portal dashboard, click on Third-party certificates pending import, as shown in Figure 2-8.

![Figure 2-8 Pending tasks](image)

Double click on the pending certificate, specify the location of the signed certificate, and select the certificate to import, as shown in Figure 2-9 on page 46.
After importing the signed certificate, validate the status of the server certificate, it should be shown as active, as shown in Figure 2-10.

Restart the WebSphere Application Server, as shown in Example 1-5 on page 21.

### 2.2 Backup and Restore IBM Security Key Lifecycle Manager configuration

IBM Security Key Lifecycle Manager creates cross-platform backup files in a manner that is independent of operating systems and directory structure of the server. You can restore the backup files to an operating system that is different from the one it was backed up from. For
example, you can restore a backup file that is taken on a Linux system and restore it on a
Windows system. Your role must have permissions to back up or to restore files.

2.2.1 Backup IBM Security Key Lifecycle Manager configuration

Logon to the IBM Security Key Lifecycle Manager portal, navigate to Administration and
select Backup and Restore, as shown in Figure 2-11.

![Figure 2-11 Backup and Restore](image1)

Click on Browse to specify the backup repository location, the default location is
/opt/IBM/WebSphere/AppServer/products/sklm/data, and click on Create Backup to specify
the password for the backup file, as shown in Figure 2-12.

![Figure 2-12 Create Backup](image2)
Verify the backup file is created in the default location, and transfer the backup file to the other IBM Security Key Lifecycle Manager servers in your environment, as shown in Example 2-3.

### Example 2-3  Backup jar file

```
[root@sklm data]# pwd
/opt/IBM/WebSphere/AppServer/products/sklm/data
[root@sklm data]# ls -al
```

```
total 56
drwx------  4 root root 155 Feb  5 21:10 .
drwxr-xr-x 14 root root 312 Jan 13 02:24 ..
-rw-r--r--  1 root root 962 Feb  5 07:09 200205070956-ITSO-SKLM-signed.csr
drwx------  2 root root  6 Jan 13 02:20 agent
drwx------  2 root root  8 Feb  6 20:59 restore
-rw-r--r--  1 root root 49151 Feb  5 21:10 sklm_v3.0.1.3_20200205210934-0500_backup.jar
```

The backup files created from the highlighted versions of IBM Security Key Lifecycle Manager in Figure 2-13 can be used for restore on a different supported OS platform.

### Figure 2-13  Cross-platform Restore/Migration

<table>
<thead>
<tr>
<th>Version</th>
<th>Minimum Required Level</th>
<th>In-line Migration</th>
<th>Cross-platform Migration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Key Manager, Version 2.1</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IBM Token Key Lifecycle Manager, Version 1.0</td>
<td>Fix pack 7</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IBM Token Key Lifecycle Manager, Version 2.0</td>
<td>Fix pack 6</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IBM Token Key Lifecycle Manager, Version 2.0</td>
<td>Fix pack 5</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IBM Security Key Lifecycle Manager, Version 2.5</td>
<td>Fix pack 3</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IBM Security Key Lifecycle Manager, Version 2.6</td>
<td>Fix pack 2</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IBM Security Key Lifecycle Manager, Version 2.7</td>
<td>General Availability (GA) version</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IBM Security Key Lifecycle Manager, Version 3.0</td>
<td>3.0 General Availability (GA) version</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Note:** The backup file can only be used for restore on the servers that have the same version of IBM Security Key Lifecycle manager and fix pack installed.

### 2.2.2 Restore IBM Security Key Lifecycle Manager configuration

Logon to the IBM Security Key Lifecycle Manager server where the configuration is being restored to, and make sure the backup file from the primary server is located in the `/opt/IBM/WebSphere/AppServer/products/sklm/data/` directory, as shown in Example 2-4.

### Example 2-4  Backup jar file on the target server

```
[root@sklm1 data]# pwd
/opt/IBM/WebSphere/AppServer/products/sklm/data
[root@sklm1 data]# ls -al
```

```
total 48
drwx------  4 root root  86 Feb  7 09:54 .
drwxr-xr-x 14 root root 312 Feb  6 21:03 ..
drwx------  2 root root  6 Feb  6 20:59 agent
drwx------  2 root root  6 Feb  6 20:59 restore
-rw-r--r--  1 root root 49151 Feb  7 09:54 sklm_v3.0.1.3_20200205210934-0500_backup.jar
```
Logon to the IBM Security Key Lifecycle Manager server portal, navigate to Administration, select Backup and Restore, and the available backup files are listed, as shown in Figure 2-14 on page 49.

![Available backup files](image1)

**Figure 2-14   Available backup files**

Select the backup file, click on Restore From Backup, and enter the password for the backup file to restore, as shown in Figure 2-15.

![Restore from backup](image2)

**Figure 2-15   Restore from backup**

**Note:** Any configurations applied on the secondary server will be lost if you proceed.

The restore process might take some time to complete depending on the size of the configuration, and a confirmation message will be displayed if the backup was restored successful, as shown in Figure 2-16 on page 50.
Figure 2-16  Confirmation of a successfully restoration

Logon to the primary and secondary IBM Security Key Lifecycle Manager portal, and they should have the identical configuration, as shown in Figure 2-17.
2.3 Configuring Replication for IBM Security Key Lifecycle Manager configuration

You can use IBM Security Key Lifecycle Manager to automatically replicate your key materials, configuration files, and other critical information from a primary master server up to 20 secondary clone servers. The automatic replication ensures continuous key and certificate availability to encrypting devices.

The data replication enables cloning of IBM Security Key Lifecycle Manager environments to multiple servers in a manner that is independent of operating systems and directory structure of the server.

The master server is the primary system that is being replicated, and the replication process is triggered only when the new keys, and devices, are added or modified on the master.
server. You can replicate the master server with a maximum of 20 clone servers. Each clone server is identified through an IP address or host name, and a port number. The server uses properties in the ReplicationSKLMConfig.properties file to control the replication process.

You can also use the IBM Security Key Lifecycle Manager replication program to schedule automatic backup operation. You must configure properties only for the master server to back up data at regular intervals.

2.3.1 Configure the master server for replication

Logon to the primary IBM Security Lifecycle Manager portal, navigate to Administration and select Replication, as shown in Figure 2-18.

![Replication configuration](image)

*Figure 2-18 Replication configuration*

Select the Master role on the primary IBM Security Lifecycle Manager server, specify the certificate to be used for the replication configuration, the passphrase for the replication backup files, and the master listen port, as shown in Figure 2-19.
Chapter 2. IBM Security Key Lifecycle Manager Configuration

Click on Add Clone to add a secondary server to replicate to and save the replication configuration, and then click on Start Replication Server, as shown in Figure 2-20.

**Note:** The hostname of the clone server has to be resolvable either via the /etc/hosts file or DNS.
Verify the defined master listen port 1111 is in the listen state on the master server, as shown in Example 2-5.

**Example 2-5  Verify master listen port state**

```
[root@sklm1 ~]# netstat -an|grep tcp |grep -i listen
output omitted...
tcp6       0      0       :::60015                :::*                    LISTEN
tcp6       0      0       :::111                  :::*                    LISTEN
tcp6       0      0       :::80                   :::*                    LISTEN
tcp6       0      0       :::9110                 :::*                    LISTEN
tcp6       0      0       :::22                   :::*                    LISTEN
tcp6       0      0       :::1111                 :::*                    LISTEN
tcp6       0      0       :::441                  :::*                    LISTEN
tcp6       0      0       :::3801                 :::*                    LISTEN
tcp6       0      0       ::1:25                  :::*                    LISTEN
output omitted...
```

### 2.3.2 Configure the clone server for replication

An existing private key must be available in the IBM Security Key Lifecycle Manager keystore of the master and all its clone systems. You must set the alias of this key on the master system in the backup.TLSCertAlias parameter of the ReplicationSKLMConfig.properties configuration file. If the same key is not available on both the master and clone systems, you cannot start communication between the systems to run the replication task.

**Note:** Backup the configuration on the primary server once the initial configuration is complete, and restore the configuration on the clone servers.

Logon to the clone IBM Security Lifecycle Manager portal, navigate to Advanced Configuration and select Server Certificates, and make sure the certificate chosen on the master server for replication is present, as shown in Figure 2-21 on page 54.

![Figure 2-21  Verify certificate for replication](image-url)
Navigate to Administration and select Replication, select the clone role on the clone IBM Security Lifecycle Manager server, specify the master listen port and the clone listen port, as shown in Figure 2-22.

![IBM Security Key Lifecycle Manager](image)

**Figure 2-22 Specify basic properties**

Click on Start Replication Server, and verify that the defined clone listen port 2222 is in the listen state on the clone server, as shown in Example 2-6.

**Example 2-6 Verify clone listen port state**

```bash
[root@sklm2 ~]# netstat -an|grep tcp|grep -i listen
output omitted......
tcp6 0 0 127.0.0.1:9643 :*: LISTEN
tcp6 0 0 :9421 :*: LISTEN
tcp6 0 0 :9070 :*: LISTEN
tcp6 0 0 :2222 :*: LISTEN
tcp6 0 0 :9422 :*: LISTEN
tcp6 0 0 :60015 :*: LISTEN
tcp6 0 0 :111 :*: LISTEN
output omitted......
```

Logon to the master IBM Security Lifecycle Manager portal, navigate to Administration and select Replication, and click Replication Now, as shown in Figure 2-23 on page 56.
The replication process might take some time to complete depending on the size of the configuration, and a confirmation message is displayed once the process is complete, as shown in Figure 2-24.

Logon to the master IBM Security Lifecycle Manager portal, and check the replication status of the clone servers, as shown in Figure 2-25 on page 57.
2.4 Configuring Multi-Master Cluster

Implementation of a high-availability solution requires configuration of IBM Security Key Lifecycle Manager masters in a Multi-Master cluster. All IBM Security Key Lifecycle Manager instances in the cluster point to a single data source that is configured for Db2 high availability disaster recovery (HADR) to ensure real-time availability of latest data to all the masters in the cluster.

You can use IBM Security Key Lifecycle Manager Multi-Master configuration for data transmission to achieve the following objectives:

- Ensures consistent and continuous data availability of IBM Security Key Lifecycle Manager across the organization.
- Avoids a single point of failure by using the high-availability solution.
- Masters can be located in several physical sites, that is, distributed across the network.

For setting up high availability disaster recovery (HADR), the necessary Db2 parameters are configured in IBM Security Key Lifecycle Manager masters with a primary database and a standby database. Figure 2-26 on page 58 shows a simple deployment of IBM Security Key Lifecycle Manager and Db2 HADR for a Multi-Master environment where four instances (masters) of Db2 HADR and N instances of IBM Security Key Lifecycle Manager are configured.
2.4.1 Setting up minimal deployment of a Multi-Master cluster

The following section covers the configuration of the minimal deployment of a Multi-Master cluster, as shown in Figure 2-27.

Deployment prerequisites:

- Both primary and standby Db2 database servers must be installed on the same version of operating system.
The Db2 version that is installed on the IBM Security Key Lifecycle Manager primary and standby master servers must match.

Must use a dedicated network for the Db2 HADR primary and standby connections.

You must ensure that your computer host name is configured correctly before you set up IBM Security Key Lifecycle Manager masters for Multi-Master configuration. You can resolve an IP address to a host name by editing the etc/hosts file.

For Db2 HADR configuration, you must update the etc/hosts file in the primary and standby master servers of the cluster to enable host name to IP address mapping, as shown in Example 2-7.

**Example 2-7 /etc/hosts file on primary master and standby master servers**

<table>
<thead>
<tr>
<th>Primary Master</th>
</tr>
</thead>
<tbody>
<tr>
<td>[root@sklm4-1 ~]# cat /etc/hosts</td>
</tr>
<tr>
<td>127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4</td>
</tr>
<tr>
<td>::1 localhost localhost.localdomain localhost6 localhost6.localdomain6</td>
</tr>
<tr>
<td>192.168.48.221 sklm4-1.itso.ibm.com</td>
</tr>
<tr>
<td>192.168.48.222 sklm4-2.itso.ibm.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standby Master</th>
</tr>
</thead>
<tbody>
<tr>
<td>[root@sklm4-2 ~]# cat /etc/hosts</td>
</tr>
<tr>
<td>127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4</td>
</tr>
<tr>
<td>::1 localhost localhost.localdomain localhost6 localhost6.localdomain6</td>
</tr>
<tr>
<td>192.168.48.221 sklm4-1.itso.ibm.com</td>
</tr>
<tr>
<td>192.168.48.222 sklm4-2.itso.ibm.com</td>
</tr>
</tbody>
</table>

Update the Db2 kernel parameters on primary master and standby master servers if IBM Security Key Lifecycle Manager is installed on a Linux operating system by editing the /etc/sysctl.conf file, as shown in Example 2-8.

**Example 2-8 Db2 kernel parameters**

```
#Example for a computer with 16GB of RAM:
kernl.shmmni=4096
kernl.shmax=17179869184
kernl.shmall=8388608

#kernel.sem=<SEMMSL> <SEMMNS> <SEMOPM> <SEMMNI>
kernel.sem=250 1024000 32 4096
kernl.msgmni=16384
kernl.msgmax=65536
kernl.msgmnb=65536
```

Refer to the [Db2 Knowledge Center](https://www.ibm.com) for more details on setting up kernel parameters.

Logon to the IBM Security Key Lifecycle Manager portal on the primary master server, navigate to Administration, and select Multi-Master, click on Multi-Master then OK to start the Multi-Master configuration, as shown in Figure 2-28 on page 60.
Click on Add Master to add the standby master server, and specify the details in the Basic Properties, as shown in Figure 2-29.

Figure 2-29  Basic Properties
Select the Advanced Properties, select Yes to make the server to be added as a standby master, keep the HADR port and Standby priority index as default, as shown in Figure 2-30.

![Advanced Properties](image)

**Figure 2-30  Advanced Properties**

**Note:** The standby server to be added must be a new installation with no configurations on it.

Click on Check Prerequisites to verify if the standby master server meets the requirement, as shown in Figure 2-31 on page 62.
Figure 2-31  Check Prerequisites

Click Add to add the standby master server, the process might take some time to complete, and a confirmation message will be displayed if the standby server is successfully added, as shown in Figure 2-32.
Verify the HADR status on the master and standby servers, as shown in Example 2-9.

*Example 2-9  HADR status*

```
[sklmd40@sklm4-1 ~]$ db2pd -d sklmdb40 -hadr

Database Member 0 -- Database SKLMDB40 -- Active -- Up 0 days 02:10:46 -- Date 2020-02-21-04.53.09.886158

    HADR_ROLE = PRIMARY
    REPLAY_TYPE = PHYSICAL
    HADR_SYNCMODE = SYNC
    STANDBY_ID = 1
    LOG_STREAM_ID = 0
    HADR_STATE = PEER
    HADR_FLAGS = TCP_PROTOCOL
    PRIMARY_MEMBER_HOST = sklm4-1.itso.ibm.com
    PRIMARY_INSTANCE = sklmdb40
    PRIMARY_MEMBER = 0
    STANDBY_MEMBER_HOST = sklm4-2.itso.ibm.com
    STANDBY_INSTANCE = sklmdb40
    STANDBY_MEMBER = 0
    HADR_CONNECT_STATUS = CONNECTED

output omitted......

[sklmd40@sklm4-2 ~]$ db2pd -d sklmdb40 -hadr

Database Member 0 -- Database SKLMDB40 -- Standby -- Up 0 days 01:37:40 -- Date 2020-02-21-04.53.56.492185

    HADR_ROLE = STANDBY
    REPLAY_TYPE = PHYSICAL
    HADR_SYNCMODE = SYNC
    STANDBY_ID = 0
    LOG_STREAM_ID = 0
    HADR_STATE = PEER
    HADR_FLAGS = TCP_PROTOCOL
    PRIMARY_MEMBER_HOST = sklm4-1.itso.ibm.com
    PRIMARY_INSTANCE = sklmdb40
    PRIMARY_MEMBER = 0
    STANDBY_MEMBER_HOST = sklm4-2.itso.ibm.com
    STANDBY_INSTANCE = sklmdb40
    STANDBY_MEMBER = 0
    HADR_CONNECT_STATUS = CONNECTED

output omitted......
```

2.4.2 HADR takeover scenarios

The following section covers the takeover scenarios as shown in Figure 2-33.
Figure 2-33  HADR take over scenarios

Primary database down
This section describes the primary database down scenario, as shown in Figure 2-34.

Start the Db2 database on the primary server to simulate the database down scenario, as shown in Example 2-10.

Example 2-10  Shutdown primary database

```
[root@sklm4-1 ~]# su - sklmdb40
Last login: Sat Feb 22 18:18:23 EST 2020 on pts/0
[sklmdb40@sklm4-1 ~]$ db2stop force
02/22/2020 19:21:26     0   0   SQL1064N  DB2STOP processing was successful.
SQL1064N  DB2STOP processing was successful.
[sklmdb40@sklm4-1 ~]$
```

Confirm the standby database takes over the primary HADR role, as shown in Example 2-11.

Example 2-11  Standby database takes over primary HADR role

```
[sklmdb40@sklm4-2 ~]$ db2pd -d sklmdb40 -hadr
Database Member 0 -- Database SKLMDB40 -- Active -- Up 0 days 01:13:11 -- Date
2020-02-22-19.32.42.386466

    HADR_ROLE = PRIMARY
    REPLY_TYPE = PHYSICAL
    HADR_SYNCMODE = SYNC
    STANDBY_ID = 1
    LOG_STREAM_ID = 0
    HADR_STATE = DISCONNECTED
    HADR_FLAGS =
```

---

**Table 2-33**

<table>
<thead>
<tr>
<th>Primary Agent</th>
<th>Primary database</th>
<th>Standby Agent</th>
<th>Standby database</th>
<th>Auto takeover</th>
<th>Manual takeover</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>Down</td>
<td>Up</td>
<td>Up</td>
<td>Yes</td>
<td>Not applicable</td>
<td>Restart primary database.</td>
</tr>
<tr>
<td>Down or Unreachable</td>
<td>Down or Unreachable</td>
<td>Up</td>
<td>Yes</td>
<td>Not applicable</td>
<td>See Split cluster scenario</td>
<td></td>
</tr>
<tr>
<td>Down</td>
<td>Down</td>
<td>Up or Down</td>
<td>Down</td>
<td>No</td>
<td>Yes</td>
<td>Takeover manually on the auxiliary standby master server, if exists. Requires manual intervention because both databases are down.</td>
</tr>
</tbody>
</table>

Legend:
- **Host system**
- **Mandatory components in Multi-master cluster for Db2 High Availability (HA – SYNC mode)**
- **Db2 HADR Setup**
- **Connection with single data source configured as Db2 HADR for Multi-Master cluster**

---

**Figure 2-34**  Primary database setup
PRIMARY_MEMBER_HOST = sklm4-2.itso.ibm.com
PRIMARY_INSTANCE = sklmdb40
PRIMARY_MEMBER = 0
STANDBY_MEMBER_HOST = sklm4-1.itso.ibm.com
STANDBY_INSTANCE = sklmdb40
STANDBY_MEMBER = 0
HADR_CONNECT_STATUS = DISCONNECTED

After the standby database takes over the primary HADR role, the Db2 connections are automatically rerouted to the new primary database, as shown in Example 2-12.

Example 2-12 Db2 connections

```
[sklmdb40@sklm4-2 ~]$ db2 list application

<table>
<thead>
<tr>
<th>Auth Id</th>
<th>Application Name</th>
<th>Appl. Name</th>
<th>Application Id</th>
<th>DB Name</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agents</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>------------</td>
<td>----------------------------------------------------</td>
<td>---------</td>
<td>---</td>
</tr>
<tr>
<td>SKLMDB40 db2jcc_applica 17546</td>
<td>192.168.48.221.34758.200223051449</td>
<td>SKLMDB40 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SKLMDB40 db2jcc_applica 17467</td>
<td>192.168.48.221.34688.200223051330</td>
<td>SKLMDB40 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SKLMDB40 db2jcc_applica 17513</td>
<td>192.168.48.222.53102.200223051416</td>
<td>SKLMDB40 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SKLMDB40 db2jcc_applica 17434</td>
<td>192.168.48.221.34608.200223051257</td>
<td>SKLMDB40 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SKLMDB40 db2jcc_applica 17684</td>
<td>192.168.48.221.34952.200223051707</td>
<td>SKLMDB40 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SKLMDB40 db2jcc_applica 17480</td>
<td>192.168.48.222.53040.200223051343</td>
<td>SKLMDB40 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SKLMDB40 db2jcc_applica 17447</td>
<td>192.168.48.221.34644.200223051310</td>
<td>SKLMDB40 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SKLMDB40 db2jcc_applica 17493</td>
<td>192.168.48.222.34734.200223051356</td>
<td>SKLMDB40 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SKLMDB40 db2jcc_applica 17600</td>
<td>192.168.48.222.53006.200223051323</td>
<td>SKLMDB40 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SKLMDB40 db2jcc_applica 17552</td>
<td>192.168.48.221.34772.200223051455</td>
<td>SKLMDB40 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SKLMDB40 db2jcc_applica 17473</td>
<td>192.168.48.222.53022.200223051336</td>
<td>SKLMDB40 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SKLMDB40 db2jcc_applica 17440</td>
<td>192.168.48.221.34624.200223051303</td>
<td>SKLMDB40 1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Restart the Db2 database on the previous primary server as the standby database to return to the normal HADR configuration, as shown in Example 2-13.

Example 2-13 Return to normal HADR configuration

```
[sklmdb40@sklm4-1 ~]$ db2start
02/22/2020 19:50:53 0 0 SQL1063N DB2START processing was successful.
[sklmdb40@sklm4-1 ~]$ db2 start hadr on database SKLMDB40 as standby
[sklmdb40@sklm4-1 ~]$ db2pd -d sklmdb40 -hadr

DatabaseMember0--DatabaseSKLMDB40--Standby--Up0 days 00:00:04--Data
2020-02-22-19.51.42.919779

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HADR_ROLE</td>
<td>STANDBY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REPLAY_TYPE</td>
<td>PHYSICAL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HADR_SYNCMODE</td>
<td>SYNC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>STANDBY_ID</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LOG_STREAM_ID</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HADR_STATE</td>
<td>PEER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Primary server down or connection lost between the primary and standby server

This section describes the split cluster scenario, as shown in Figure 2-35.

![Figure 2-35 Split cluster scenario](image)

**Simulate the server down/unreachable scenario**

Power off the primary server to simulate the down/unreachable scenario, and check the status on the standby server once it takes over, as shown in Example 2-14 on page 66.

```
Example 2-14   HADR status on standby server after take over

[sklmb40@sklm4-2 ~]$ db2pd -d SKLMDB40 -hadr

Database Member 0 -- Database SKLMDB40 -- Active -- Up 0 days 00:37:04 -- Date 2020-02-22-21.31.23.558962

HADR Information:
HADR is not active.
```

**Note:** The standby server temporarily takes over the primary HADR role, then it transitions to an independent Db2 instance.

The ‘Merge this primary master back into the cluster’ option becomes available on the dashboard after the takeover, as shown in Figure 2-36.
Before clicking on the ‘Merge this primary master back into the cluster’ option, check the status of the Db2 connection and HADR status on the primary server, as shown in Example 2-15.

**Example 2-15  Db2 connection and HADR status on primary server**

```
[sklmdb40@sklm4-1 ~]$ db2pd -d SKLMDB40 -hadr
```

Database Member 0 -- Database SKLMDB40 -- Standby -- Up 0 days 00:02:22 -- Date 2020-02-22-21.49.52.827925

```
HADR_ROLE = STANDBY
REPLAY_TYPE = PHYSICAL
HADR_SYNCHMODE = SYNC
STANDBY_ID = 0
LOG_STREAM_ID = 0
HADR_STATE = LOCAL_CATCHUP
HADR_FLAGS =
PRIMARY_MEMBER_HOST = NULL
PRIMARY_INSTANCE = NULL
PRIMARY_MEMBER = NULL
STANDBY_MEMBER_HOST = sklm4-1.itso.ibm.com
STANDBY_INSTANCE = sklmdb40
STANDBY_MEMBER = 0
HADR_CONNECT_STATUS = DISCONNECTED
```

**Note:** After the primary server comes back online, it temporarily has the primary HADR role, then it transitions to the standby HADR role.

Run the sklmTakeoverHADR.sh on the primary server to resume the HADR primary role and check the HADR status, as shown in Example 2-16.
Example 2-16  HADR status after take over

[root@sklm4-1 ~]# /opt/IBM/SKLMV40/agent/sklmTakeoverHADR.sh
/opt/IBM/WebSphere/AppServer sklm4-1.itso.ibm.com 60015
HADR Takeover successful.
[sklmdb40@sklm4-1 ~]$ db2pd -d SKLMDB40 -hadr

Database Member 0 -- Database SKLMDB40 -- Active -- Up 0 days 07:42:26 -- Date 2020-02-23-05.29.56.580203

HADR_ROLE = PRIMARY
REPLAY_TYPE = PHYSICAL
HADR_SYNCHMODE = SYNC
STANDBY_ID = 1
LOG_STREAM_ID = 0
HADR_STATE = DISCONNECTED
HADR_FLAGS =
PRIMARY_MEMBER_HOST = sklm4-1.itso.ibm.com
PRIMARY_INSTANCE = sklmdb40
PRIMARY_MEMBER = 0
STANDBY_MEMBER_HOST = NULL
STANDBY_INSTANCE = NULL
STANDBY_MEMBER = NULL
HADR_CONNECT_STATUS = DISCONNECTED

Note: At this stage, the Db2 database is running as an independent instance, thus the HADR in the above example is shown as disconnected.

Both the primary and secondary server are now running as primary, as shown in Figure 2-37 on page 69
Click the ‘Merge this primary master back into the cluster’ option on the standby server and click OK to proceed, as shown in Figure 2-38 on page 70.
A confirmation message will be displayed if the merge is successful, as shown in Figure 2-39.

Verify the HADR status on the primary and secondary server, as shown in Figure 2-39.

Example 2-17  HADR status after merge

```
[sklmdb40@sklm4-1 ~]$ db2pd -d SKLMDB40 -hadr
```

Database Member 0 -- Database SKLMDB40 -- Active -- Up 0 days 08:01:46 -- Date 2020-02-23-05.49.16.709415

```
HADR_ROLE = PRIMARY
REPLAY_TYPE = PHYSICAL
HADR_SYNCMODE = SYNC
```
2.5 Migrating from an earlier version of IBM Security Key Lifecycle Manager

IBM Security Key Lifecycle Manager does not support a direct upgrade from the existing version (installed on the host system) to the target version (to which you want to upgrade).

There are two methods of data migration:

- Inline migration
  When the host system of the target version is the same as the existing version, use inline migration of data.

- Cross migration
  When the host system of the target version is different than the host system of the existing version, use cross migration of data. IBM Security Key Lifecycle Manager provides sample response files that you can use to cross migrate data.

Supported upgrade paths and migration methods are shown in Figure 2-40 on page 72.
2.5.1 Inline Migration

This section describes the tasks associated with the Inline Migration from IBM Security Key Lifecycle Manager version 3.0.1.3 to 4.0.0.0.

Run the launchpad.sh script to start the installation wizard, follow the installation process described in Chapter 1, “IBM Security Key Lifecycle Manager Installation and Integration” on page 1 until the version 4.0.0.0 installer detects the existing version installed on the machine, change the HTTPS WAS port from 9083 to 9087, click Validate Credentials and then Next to proceed, as shown in Figure 2-41.
Review the installation summary and click Install to install the product, as shown in Figure 2-42 on page 73.
Logon to the IBM Security Key Lifecycle Manager portal to confirm the version and the previous configuration has been migrated, as shown in Figure 2-43 on page 74.

![Configuration and version details](image)

**Figure 2-43  Configuration and version details**

### 2.5.2 Cross Migration

This section describes the tasks associated with the Cross Migration from IBM Security Key Lifecycle Manager version 3.0.0.2 to 4.0.0.0.

Locate the migration utility on the server where IBM Security Key Lifecycle Manager version 4.0.0.0 is installed, as shown in Example 2-18.

**Example 2-18  Migration Utility**

```
[root@sklm utilities]# pwd
/opt/IBM/SKLMV40/migration/utilities
[root@sklm utilities]# ls -l
```

```
total 24
  drwxr-xr-x 2 sklmdb40 root 4096 Feb 23 08:04 ekm21
  drwxr-xr-x 2 sklmdb40 root 4096 Feb 23 08:04 sklmv25
  drwxr-xr-x 2 sklmdb40 root 4096 Feb 23 08:04 sklmv26
  drwxr-xr-x 2 sklmdb40 root 4096 Feb 23 08:04 sklmv27
  drwxr-xr-x 2 sklmdb40 root 4096 Feb 23 08:04 sklmv30
  drwxr-xr-x 2 sklmdb40 root 4096 Feb 23 08:04 sklmv301
```

Transfer the corresponding version of the utility directory to the server where IBM Security Key Lifecycle Manager version 3.0.0.2 is installed, and in this case it is the sklmv30 directory, as shown in Example 2-19.

**Example 2-19  Transfer the utility to the target server**

```
[root@sklm utilities]# pwd
/opt/IBM/SKLMV40/migration/utilities
[root@sklm utilities]# scp -r sklmv30 192.168.48.10:/root/
```
Modify the backup.properties file with the actual WAS_HOME and JAVA_HOME path and correct credentials for the sklmdb30 and wasadmin account, as shown in Example 2-20.

**Example 2-20  Modify the backup.properties file**

```bash
[root@sklm sklmv30]# ls
additional_backup.properties
additional_restore.properties
backup.properties
backupUsersRolesGroups.py
backupV30.bat
backupV30.sh
com.ibm.sklm.server.migrate.sklmv30.jar
com.ibm.sklm.server.migrate.sklmv30.jar.versioned
readme.html
restore.properties
restoreUserRolesGroups.py
restoreV30.bat
restoreV30.sh
```

```
[root@sklm sklmv30]# cat backup.properties
WAS_HOME=/opt/IBM/WebSphere/AppServer
JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0/
BACKUP_PASSWORD=Password123
DB_PASSWORD=Password123
WAS_USER_PWD=Password123
```

Run the backupV30.sh script to generate the cross platform migration file. The migration file is located in the backup directory within the utility directory, as shown in Example 2-21 on page 75.

**Example 2-21  Generate migration file**

```bash
[root@sklm sklmv30]# ./backupV30.sh
CURR_DIR=/root/sklmv30/
Backup completed, please refer to backup.log for more details.
```

```
[root@sklm sklmv30]# ls -l ./backup
total 144
-rw-r--r--. 1 root root   1393 Feb 24 05:43 backupStatus.properties
-rw-r--r--. 1 root root 141140 Feb 24 05:43 sklm_v3.0.0.2_20200224054259-0500_migration_backup.jar
```

Transfer the migration file to the server where IBM Security Key Lifecycle Manager version 4.0.0.0 is installed, as shown in Example 2-22.

**Example 2-22  Transfer the migration file**

```bash
[root@sklm backup]# pwd
/root/sklmv30/backup
[root@sklm backup]# scp sklm_v3.0.0.2_20200224054259-0500_migration_backup.jar root@192.168.48.210:/opt/IBM/WebSphere/AppServer/products/sklm/data/
```

Logon to the IBM Security Key Lifecycle Manager portal where IBM Security Key Lifecycle Manager version 4.0.0.0 is installed, navigate to Administration then Backup and Restore, and click Display Backups to list the available ones as shown in Figure 2-44.
Select the migration file to restore the configuration from the previous version, as shown in Figure 2-45 on page 76.

The restoration process might take some time to complete depending on the size of the configuration, and a confirmation message will be displayed if the backup was restored successfully, as shown in Figure 2-46.
Figure 2-46  Confirmation of a successfully restoration
Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document.

IBM DS8000 Encryption for data at rest, Transparent Cloud Tiering, and Endpoint Security (DS8000 Release 9.0)

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

ibm.com/redbooks

Online resources

These websites are also relevant as further information sources:

IBM Security Key Lifecycle Manager (Knowledge Center)

IBM Security Key Lifecycle Manager Support Matrix

IBM Security Key Lifecycle Manager Dashboard

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services
To determine the spine width of a book, you divide the paper PPI into the number of pages in the book. An example is a 250 page book using Professional opaque 50# smooth which has a PPI of 526. Divided

<table>
<thead>
<tr>
<th>Pages</th>
<th>Spine Width (in.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>0.17”</td>
</tr>
<tr>
<td>90</td>
<td>0.35”-1.49”</td>
</tr>
<tr>
<td>250</td>
<td>0.475”-0.875”</td>
</tr>
<tr>
<td>450</td>
<td>0.5”-1.0”</td>
</tr>
<tr>
<td>789</td>
<td>1.5”-1.998”</td>
</tr>
<tr>
<td>1051</td>
<td>1.998”-2.498”</td>
</tr>
</tbody>
</table>
To determine the spine width of a book, you divide the number of pages by the PPI of the paper. For example, if a book has 250 pages using Plainfield opaque 50# smooth which has a PPI of 526, you would divide 250 by 526 which equals .4752". In this case, you would use the .5" spine. Now select the spine width for the book and hide the others. To add conditional text settings to all files in your book, open the book file with the spine.fm still open and import the Conditional Text Settings (ONLY!) to the book files.