kyndryl™

Kyndryl Resiliency Orchestration

Upgrade Guide

Version 8.4.9.0

DISCLAIMER

Kyndryl believes that the information in this publication is accurate as of its publication date. The information is subject to change without notice.

COPYRIGHT

TRADEMARK INFORMATION

Not all offerings are available in every country in which Kyndryl operates. This program is licensed under the terms of the license agreement accompanying the Program. Please read the “Terms of Use” for this offering before using this program. By using the program, you agree to the terms.

kyndryl™

Revision History

We have updated documentation to reflect changes in terminologies from Master/Slave to Primary/Standby. You will encounter continued references to these former terminologies while we work to implement these deeper changes to code, UI, API, configuration files, and CLI commands.

Document Version	Revision Date	Sections Updated	Supported Product Version
8.2	June 2021	2.6.1 Sample report after using new Schema validator script	8.2.x
	June 2021	Table of tested upgrade versions changed Page 4	
	June 2021	Post-installation SQL query added Page 32	
8.2.1	September 201	Veeam section added	8.2.x
8.2.3	September	Veeam section updated	
8.1.3	September 2021	Backing and Exporting up MariaDB Page 7	
		Multiple minor changes	
8.2.0	September 2021	Multiple minor changes	
8.2.3		Post-install steps added	
8.2.6	December 2021	2.8.2 Post upgrade procedure Page 32	
8.2.6	December 2021	2.3.1 Backup Plan (Updated command of this point - IBM Resiliency Orchestration Server MariaDB Metadata)	
8.2.6	December 2021	2.2 Prerequisite for upgrading to 8.2.6 in Silent and GUI Mode Upgrade (Added bullet point for validation key, page 7	
8.2.6	December 2021	2.10 Known limitation (Added known limitation for cyber component - Cold Capable)	
8.2.6	January 2022	2.8.2 Post upgrade procedures, added step 20, page 37	

Document Version	Revision Date	Sections Updated	Supported Product Version
8.2.6	January 2022	2.2 Prerequisite for upgrading to 8.2.6 in Silent and GUI Mode Upgrade (added bullet point for a subfolder, Page 7)	
8.2.6	January 2022	2.3 Preparing for Upgrade to 8.2.6 (added step 4, Page 8)	
8.2.6	January 2022	2.8.2 Post upgrade procedures (added step 21, Page 37)	
8.2.7	January 2022	RO version updated in the document	8.2.x
8.2.7	January 2022	Section 1 Table updated Page 5	
8.2.7	January 2022	2.10 Known issues, Page 39 While upgrading, from server 1 to server 2, the group creation fails as the solution plugin folders are copied by the installer. Workaround - To avoid this, from the installer backup folder, copy missing folders to <eamsroot>rpd/solutionplugins for the failing solutions. After copying the folder manually, re-create the group.	
8.2.8	February 2022	Removed Known Limitation related to Cold Capable from Section 2.10 Known Limitations, Pages 38 and 39 (Ref JIRA: RO-27605)	8.2.x
8.2.8	February 2022	Updated the tested upgrade version hops table on Page 5	8.2.x
8.2.9	March 2022	Added a bullet in the 2.2 Prerequisite for upgrading to 8.2.9 in the Silent and GUI Mode Upgrade section to describe: Migrating remote agents from Agent Node (RO) to Site Controller.	8.2.x
		Restructured the documentation flow, Removed instances of ‘Silent’ mode and used Console mode, Added import database script details: mysql -u UserName -p Password < dbdumpname.sql, Added the following script:	8.2.x

kyndryl™

Document Version	Revision Date	Sections Updated	Supported Product Version
		DROP USER panaces; GRANT SELECT,INSERT,UPDATE,DELETE,DROP,CREATE,EXECUTE,SHOW VIEW ON panaces.* TO 'panaces'@'localhost' IDENTIFIED BY '<password>' WITH GRANT OPTION; GRANT SELECT,INSERT,UPDATE,DELETE,DROP,CREATE,EXECUTE,SHOW VIEW ON panaces.* TO 'panaces'@'<RO-IP>' IDENTIFIED BY '<password>' WITH GRANT OPTION; FLUSH PRIVILEGES; The updated heading of 2.2 Removed shell script code box from 2.3.2.1 Creating User.sql file Added mysql_upgrade script details Updated heading of 2.4 Updated heading of 2.6.2	
		Removed this Known limitation as this is fixed: 2.8 Known limitation While upgrading, from server 1 to server 2, the group creation fails as the solution plugin folders are copied by the installer. Workaround - To avoid this, from the installer backup folder, copy missing folders to <eamsroot>rpd/solutionplugins for the failing solutions. After copying the folder manually, re-create group.	
		Post upgrade, first bullet to describe the requirement of restarting RO and SC (Section 2.6.1)	
8.2.9.1	April 2022	Added a new step 22 under section 2.6.3 Post upgrade procedures on Page 47. Reference JIRA: RO-40834	8.2.9.x
		Updated the table under section 1 Overview of the Upgrade Procedures on Page 6.	8.2.9.x

kyndryl

Document Version	Revision Date	Sections Updated	Supported Product Version
8.2.9.2	May 2022	Added a new Note in the section “2.3.1 Backup Plan” on Page 12. Reference JIRA: RO-41916	8.2.9.2
		Updated the table under the section 1 Overview of the Upgrade Procedures on Page 8. Reference JIRA: RO-41852	8.2.9.2
8.3.0	June 22	2.6.4 Section added RBR post upgrade mandatory steps page 47 JIRA RO-42673	8.3.0
		Prerequisite for upgrading to the latest version page 9	
		Added a new section “Resiliency File Replicator (RFR) Upgrade” on Page 40.	8.3.0
		Post Upgrade Steps for SRM-based Solution page 49	
8.3.1	July 2022	Updated the section “Resiliency File Replicator (RFR) Upgrade with the Note on Page 40. Reference JIRA: RO-44779	8.3.x
8.3.1	July 2022	Updated the section “1 Overview of the Upgrade Procedures” on Page 6. Reference JIRA: RO-44782	8.3.x
8.3.2	August 2022	Updated the section “1 Overview of the Upgrade Procedures” on Page 6. Reference JIRA: RO-46382, RO-46381, RO-46380	8.3.x
8.3.3	September 2022	The following sections are updated that include log4j steps: • Deleted the section "Execute the Post-Upgrade Scripts". • Deleted the log4j step from the "RFR Upgrade" section. • Deleted the log4j step from "Post Upgrade procedure". Reference JIRA: RO-47638	8.3.x
		Updated the section “1 Overview of the Upgrade Procedures” on Page 6. Reference JIRA: RO-47818	8.3.x

Document Version	Revision Date	Sections Updated	Supported Product Version
		Removed the table (tested upgrade versions) and added Note to explain the one-hop upgrade support	
		Added Purge Now option details in the 2.3.1 Backup Plan section	
8.3.4	October 2022	Updated the section “1 Overview of the Upgrade Procedures” on Page 6. Reference JIRA: RO-49204	8.3.x
8.3.5	November 2022	Updated the section “1 Overview of the Upgrade Procedures” on Page 9. Reference JIRA: RO-50714	8.3.x
		Updated Step 5 on Page 46 in the section “2.7.3 Post Upgrade Procedures”. Reference JIRA: RO-51025	8.3.x
8.3.6	December 2022	Added section 2.7.7 - Post Upgrade steps for Workflow Version Update, on page 51.	8.3.x
		Added a new Note in the section “2.1 Overview” on Page 10. Reference JIRA: RO-48406	8.3.x
		Added a new Note in the section “2.7.3 Post Upgrade Procedures” on Page 45. Reference JIRA: RO-51718	8.3.x
		Added information related to Compressed zip backup 2.4.3 One Tier to One Tier Upgrade: Step 17 2.5.1 Steps for Kyndryl RO Linux SC upgrade to the latest version 2.5.2 Steps for Kyndryl RO Windows SC upgrade to the latest version	8.3.x
		Added the following new sections: 2.7.8 Apply patch in the RO Server 2.7.9 Rollback Steps after applying patch in the RO Server 2.7.10 Apply Script in the RO Server Reference JIRA: RO-52199	8.3.x

Document Version	Revision Date	Sections Updated	Supported Product Version
		Added a new section “Known Issue and Workaround”. Reference JIRA: RO-52512	8.3.x
8.3.7	January 2023	Added 2.9.2 SchemaValidator script execution is failing on Upgrade under Section " Known Issues and Workaround " Reference ADO workItem: 754726	8.3.x
8.3.8	February 2023	Added section 2.7 for RBR specific upgrade procedure	8.3.x
		Added section Post upgrade steps for Tomcat server.xml	
		Added section 3 RBR Procedure to Upgrade VIB and NICRA/SA without impacting the Groups	
8.3.9.0/ 8.3.9.1	March 2023	Section ‘Post Upgrade steps for Workflow Version Update’ renamed as ‘(Optional) Workflow Version in View Workflow Page’ and moved under ‘Known issue and Workaround’, on page 60-61.	8.3.x
		Updated section 3 RBR Procedure to Upgrade VIB and NICRA/SA without impacting the Groups	
		Added the missing property (missing from 8.3.6 version) in the post upgrade procedure: panaces.acp.server.concurrentRequestProcessCount panaces.acp.server.concurrentRequestProcessCountMax	
		2.8.4 step4 Post upgrade added for Thick and thin provisioning	
8.3.10.0	April 2023	Updated - Upgrade Steps for SRM-based Solution with Note	8.3.x
8.3.11.0	May 2023	Added chapter 3 GPL Dependencies	
		Removed information related to ./registerRPDPlugin.sh -d Veeam	
8.4.0.0	June 2013	Added section 2.8 Upgrade script	
		Added section RO users'('panacesuser' & 'tomcatuser') password policies and password lenghths configuration	
		Added section 2.7.10 Script upgrade to support Dataset and Protection Schema	

Document Version	Revision Date	Sections Updated	Supported Product Version
8.4.1.0	July 2023	2.7 section of RBR upgrade updated, 2.8 section added more details	
		Known issue with workaround 2.11.4 section added	
8.4.2.0	August 2023	Updated Post Upgrade section with the following: 2.9.10 Apply the patch after RO and SC upgrade, for existing discovered Oracle DG groups to get the MRP Event. 2.9.11 Support for Custom Replicator Solutions to convert plain text to group credentials.	
		2.9.2.1 Post upgrade procedure Vault configuration: Step 22 added	
		Added section 2.11.5 Upgrade steps for RO Base Version 7.2.SP4	
8.4.3.0	September 2023	Added Step 7 rebranding from IBM to Resiliency and removed old step 4 from 2.9.3 upgrade of RBR NICRA based solution.	
		Added 2.4.3 added section numbers	
		Added 4 jar files to be added in 2.9.2.1 Post upgrade guide step 22 sub step 2.	
		2.9.1.0 step 10 Note added: check if mariadb certificate files 1. ca-cert.pem, 2.server-cert.pem 3.server-key.pem All three are present in "$EAMSROOT/installconfig/mariadbencryption" directory. if not present a SSL connection error will come in logs. Resolution is Copy below 3 files from RO backup folder to "$EAMSROOT/installconfig/mariadbencryption". 1.$EAMSROOT/installconfig/mariadbencryption/ca-cert.pem 2.$EAMSROOT/installconfig/mariadbencryption/server-cert.pem 3.$EAMSROOT/installconfig/mariadbencryption/server-key.pem	

Document Version	Revision Date	Sections Updated	Supported Product Version
8.4.4.0	Oct 23	• prerequisite section 2.2 added Before any upgrade operation the prerequisite is to perform a Cleanup of temporary files. • Added note: Note: MUST INSTALL PATCH list. After upgrade or after fresh install contact the SUPPORT team to determine MANDATORY patch's for your setup.This list depends on your PR/DR environment, this has to be obtained support team for successful completion of your setup. • Added section '2.8 - Upgrading to the latest version of RO Anomaly Detection (ROAD) Tool'	
8.4.5.0	Nov 23	• Upgrade guide script section 2.9.1 and 2.9.2 on supported solution updated • Second point added under prerequisites of section 2.5 Site Controller Upgrade • Added substeps h and I to RBR post upgrade 2.10.3 • 2.2 added Note: From RO 8.4.5.0 onwards RO GUI logger filename has been changed from "PanacesGUI.log' to "PanacesStrutsGUI.log" from "PanacesGUI.log.debug" to "PanacesStrutsGUI.log.debug" respectively.	
8.4.7.0	Jan 24	• Section of Tomcat upgrade 2.3.3 added • 2.11.6 added under 'Known Issue and Workaround' section	
8.4.8.0	Feb 24	• 2.10.2 SchemaValidator.sh script 3 arguments information added • Updated Prerequisite for upgrading to the latest version (Single Hop Upgrade)	
8.4.9.0	Mar 24	Section 2.10.12 Optimal Performance added	

TABLE OF CONTENTS

1 Overview of the Upgrade Procedures

The Kyndryl Resiliency Orchestration Upgrade Guide provides procedures to upgrade the Kyndryl Resiliency Orchestration Application. This guide is intended for administrators responsible for upgrading and configuring the Kyndryl Resiliency Orchestration Application.

The latest version of Kyndryl Resiliency Orchestration version supports a single-hop upgrade. This feature allows you to directly upgrade from 7.2 onwards to the latest version without the need to follow an intermediate upgrade path.

Note:

- For upgrading Kyndryl Resiliency Orchestration to the latest version, you will need to perform requisite platform upgrades. Please refer to the Kyndryl Resiliency Orchestration Installation guide for supported versions of RHEL, MariaDB, and Tomcat, and refer the section 8.1.3 for backing up and upgrading relevant platforms.
- To leverage the single-hop feature of this release, you will need to be at least on 7.2. In case you are using a lower version, then you will need to upgrade to 7.2 before upgrading to the latest version.

Note: The one-hop upgrade is supported for any version starting from RO 7.2 onwards to the latest version.

2 Upgrading Kyndryl Resiliency Orchestration using Simplified Upgrade (Single Hop Upgrade)

2.1 Overview

The Kyndryl Resiliency Orchestration application is enhanced for encrypted communication between the Kyndryl Resiliency Orchestration and the Agents. The Site Controller is enabled to be installed alongside the Kyndryl Resiliency Orchestration.

Ensure that you read, understand, and then follow the procedures in the sequence they are indicated to be performed:

1. Prerequisites section.

2. Preparing for the Upgrade section.
3. Use the installer in GUI or Console mode for the upgrade.
    a. For upgrading via GUI mode, refer to the section Upgrading the Kyndryl Resiliency Orchestration Application software to the latest version.
    b. For upgrading via Console mode, refer to the section **Upgrading the Kyndryl Resiliency Orchestration Application software in Console Mode**.
4. Post-installation steps.

2.2 Prerequisite for upgrading to the latest version

Before you perform the upgrade procedure, ensure the following prerequisites are met.

- Ensure the Agents are upgraded to version 8.3.4 or later.
- For a supported Operating System, refer to the Kyndryl Resiliency Orchestration Install guide.
- For MariaDB, and Apache Tomcat versions, refer to the Kyndryl Resiliency Orchestration Install Guide.
- Ensure that you have admin privileges on the Linux server where Kyndryl Resiliency Orchestration software is currently installed.
- Before any upgrade operation one of the prerequisites is to perform a Cleanup of temporary files.
- Ensure that before the Resiliency Orchestration Server upgrade starts, all the Site Controller services and all agents running on-site Controller are stopped.
- If you are planning to upgrade an existing Kyndryl Resiliency Orchestration server RHEL Operating system or new server hardware, it is recommended that you maintain the same IP for the Kyndryl Resiliency Orchestration application as in the existing installation. If you want to use a different IP, use the procedure mentioned in section **Migrating to new Server with New IP** in the Kyndryl Resiliency Orchestration Installation guide.
- The upgrade should be performed only when all the groups are in "Normal Inactive" or "Normal Reset" state.
- No operations/workflows should be executed during the upgrade process. If NormalCopy/FailOver/ SwitchOver/SwitchBack or any Business Process/Test/Policy is in progress, it should be completed, stopped, or aborted so that the group can be moved to a Normal Inactive state. Use the "Change continuity" option to move the group to "Normal Inactive" or “Normal Reset".

- For upgrading from any one-hop supported version to the latest version, you need to perform 'panaces' database dump which needs to be imported to the target machine. Use the following commands to import the database:

  ```
  mysql -uUserName -p<Password> < dbdumpname.sql
  ```

- The user table needs to be exported from older Kyndryl Resiliency Orchestration RHEL box to the upgraded Kyndryl Resiliency Orchestration RHEL box.

- Validate that there is no subfolder under the following location:

  $EAMSROOT/installconfig/keystore

  If any subfolder is found other than files, move them to a different folder before starting the upgrade process.

  Example: You may find bkp_keystore as a folder under

  /opt/pances/installconfig/keystore

  In this case, use the following command to move the folder:

  ```
  mv /opt/panaces/installconfig/keystore/bkp_keystore /home
  ```

  (Starting from 8.1.2 – to all versions)

- To migrate the Agent Node to Site Controller, execute the following script:

  ```
  $EAMSROOT/bin>./MigrateRemoteAgentCLI.sh
  ```

  As per the recommendation if any remote agent is running on RO (Agent Node), then migrate the remote agents to the configured Site Controller. For the migration steps refer to the following section of the Kyndryl Resiliency Orchestration Installation guide: *Migrating remote agents from Agent Node (RO) to Site Controller*

- For the AIX agent, upgrade it manually. For more information, refer to the Installation Guide.

- **Note**: From RO 8.4.5.0 onwards RO GUI logger filename has been changed from "PanacesGUI.log' to "PanacesStrutsGUI.log" from "PanacesGUI.log.debug" to "PanacesStrutsGUI.log.debug" respectively.

2.3 Preparing for upgrade to the latest

1. Stop the Kyndryl Resiliency Orchestration Server Services by using the following command:

   ```
   sudo $EAMSROOT/bin/panaces stop
   ```

   Note – $EAMSROOT is the path where Kyndryl Resiliency Orchestration software is installed. For example, /opt/panaces.

2. Stop all remote agents before upgrade by using the following command:

   ```
   sudo $EAMSROOT/bin/DRMAgentsStop.sh ALL
   ```

3. Decrypt the metadata and perform a backup of the Kyndryl Resiliency Orchestration Software and configuration files using the stipulated steps in the section Backup Plan below.

   Note – If you back up the metadata without decrypting it first, you will not be able to restore the metadata correctly.

4. Before you start the upgrade process, the tmp folder in the RO server should be cleaned by using the following command:

   ```
   cd /tmp
   rm -rf *
   ```

2.3.1 Backup Plan

The older metadata having encrypted tables cannot be directly imported to the upgraded MariaDB. The metadata needs to be decrypted before importing.

This is a prerequisite command before taking a dump.

```
 $EAMSROOT/bin/enableEncryptionOnTables.sh “dec”
<mysqlpassword>
```

Note: If the upgrade does not happen, then you must enable the encryption by executing the following command:

```
$EAMSROOT/bin/enableEncryptionOnTables.sh “enc”
   <mysqlpassword>
```

Note: Skip this step if you have the RO version below 7.2.4 as the encryption table is not available.

For Example: –

```
     /opt/panaces/bin/enableEncryptionOnTables.sh "dec"
<Password>
```

Take a backup of the following files and directories on a backup server within the network in case a rollback to the prior version is required.

- Kyndryl Resiliency Orchestration Server MariaDB Metadata

```
mysqldump -u <userName> -p --databases panaces pfr --
triggers --routines > <backup_folder_path>/<filename>.sql
```

- Take EAMSROOT, and TOMCAT Home folder backup (replace $EAMSROOT,$TOMCAT_HOME with absolute path)

For Example: –

Note: Assuming $EAMSROOT is configured as /opt/panaces

& $TOMCAT_HOME is configured as /opt/tomcat9

1. *cd /opt*
2. *mkdir backup*
3. *tar -cvzf /opt/backup/panaces.tar.gz panaces*
4. *tar -cvzf /opt/backup/tomcat9.tar.gz tomcat9*
5. *Take a backup of user files, if any*

If Kyndryl Resiliency Orchestration Server is configured with a Linux OS agent, backup the following:

- Agent Binaries
- Custom/Field Specific scripts
- Maria DB

It is recommended to take the DB backup, after purging the logs. To purge the logs, follow these steps:

1. In the RO UI, go to RO Server > Admin page > "Go to Operational History" option > **Purge Now** button.
2. Click the **Purge Now** button. As per your preference, you can edit the retention period and then click the **Purge Now** button.

2.3.2 Backing and Exporting up MariaDB

2.3.2.1 Creating User.sql file

First, you will need to create user.sql file on the current machine to back up the user profiles.

1. Use the following shell script to back up the user profiles.

   Note: You can also find the script in the $EMSROOT/bin folder in the new Kyndryl Resiliency Orchestration build.

2. Execute the below command to run the shell script on the current un-upgraded host machine.

```
./ExportUsers.sh <existing RO host IP address> <mysql_user>
<password> <new RO host IP address> > user.sql
```

For Example: – In case you have Maria DB 10.3 or below and would like to upgrade to 10.5, then execute the below example script.

```
./ExportUsers.sh

<existing RO host ip address> <root> <password> < new RO host
ip address> > user.sql
```

2.3.2.2 Execute export command on target DB

1. Copy the user.sql file created above to the target DB machine.
2. Execute the following export command on the target DB.

```
mysql -u root -p<password> mysql < /tmp/user.sql
```

2.3.3 Perform OS, tomcat, and MariaDB upgrades

2.3.3.1 Apache Tomcat Server Upgrade Steps

1.Download, The applicable version

from official Apache Tomcat site

Format example `apache-tomcat-9.0.xx.tar.gz`

Extract and place the new tomcat folder on the RO Server.

2. Apache-Server-Upgrade.sh script is available at

$EAMSROOT/bin/ location.

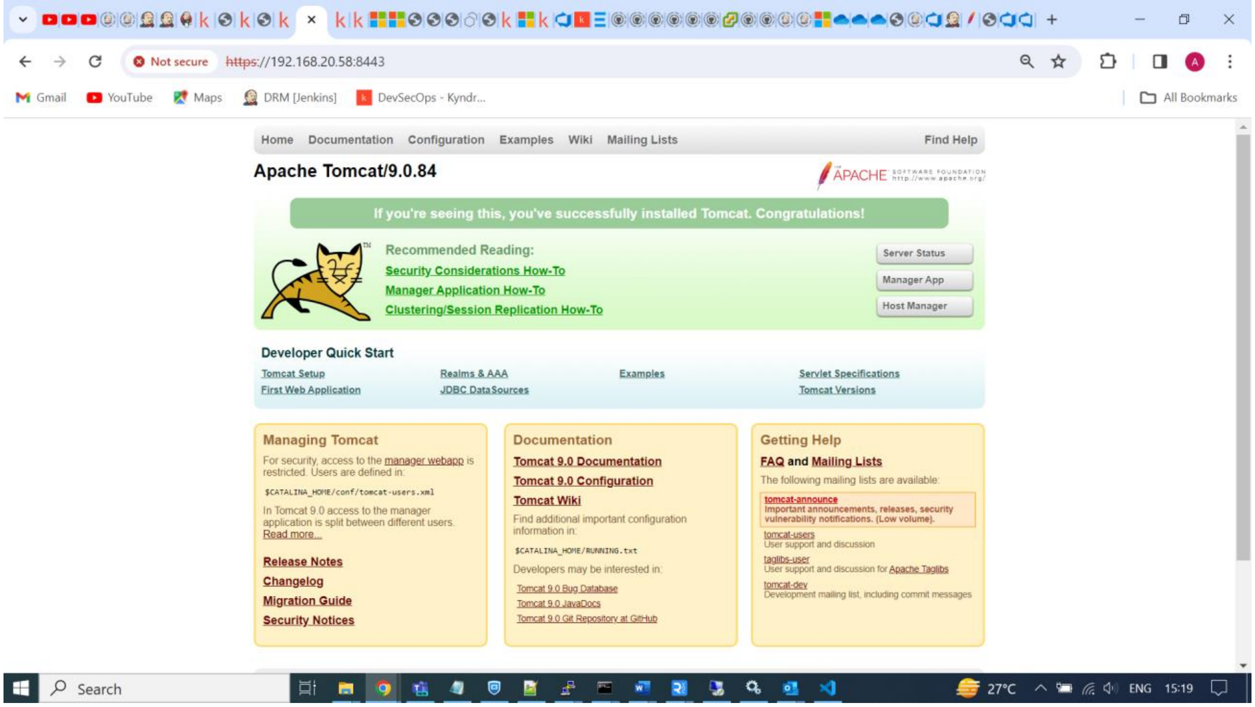
3.Run the Apache-Server-Upgrade script as below by providing the absolute paths of old and new tomcat folders as argument.

CLI : Apache-Server-Upgrade.sh <Current-tomcat-absolute-path> <new-tomcat-absolute-path>

Example *./Apache-Server-Upgrade.sh /opt/apache-tomcat-9.0.71 /opt/apache-tomcat-9.0.84*

4.After completion verify on UI. (on giving IP and url the tomat should come up and display its version)

Sample URL: https://192.168.20.58:8443/



Apache Tomcat/9.0.84

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
Security Considerations How-To
Manager Application How-To
Clustering/Session Replication How-To

Developer Quick Start
Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat
For security, access to the manager webapp is restricted. Users are defined in:
```
$CATALINA_HOME/conf/tomcat-users.xml
```
In Tomcat 9.0 access to the manager application is split between different users. Read more...
Release Notes
Changelog
Migration Guide
Security Notices

Documentation
Tomcat 9.0 Documentation
Tomcat 9.0 Configuration
Tomcat Wiki
Find additional important configuration information in:
```
$CATALINA_HOME/RUNNING.txt
```
Developers may be interested in:
Tomcat 9.0 Bug Database
Tomcat 9.0 JavaDocs
Tomcat 9.0 Git Repository at GitHub

Getting Help
FAQ and Mailing Lists
The following mailing lists are available:
tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).
tomcat-users
User support and discussion
taglibs-user
User support and discussion for Apache Taglibs
tomcat-dev
Development mailing list, including commit messages

2.3.3.2 Work around for the Apache Tomcat hardening:

How to turn it ON and also Turn it OFF :

Use the below validation, *when turned ON*

(`JAVA_OPTS="$JAVA_OPTS -Dorg.apache.catalina.STRICT_SERVLET_COMPLIANCE=true`" when set to true, internally turns on around 10 sub validations), *affects the RO,* *we could explicitly turn it off;*

```
tldValidation="false"
```

at `$TOMCAT_HOME/conf/context.xml`, change the value of these keys to ‘false’, and in case they do not exist, add this string to the file.

```
<Context tldValidation="false">
```

2.3.3.3 Tomcat server Rollback Steps:

1. Update the old tomcat path at TOMCAT_HOME and CATALINA_HOME in *`$EAMSROOT/bin/SecurityUserInjection.sh`* file and in *`$EAMSROOT/bin/panaces_env.`*

2.Execute the *`$EAMSROOT/bin/SecurityUserInjection.sh`*

2.3.3.4 OS, Tomcat, and MariaDB upgrades

1. Prepare the operating system, Tomcat, and MariaDB for the latest version Upgrade.
2. Upgrade the Operating System from the current version to one of the versions mentioned in the Interop guide of the latest version with assistance from IT support.
   a. Refer to the section “Installation of MariaDB” in the Kyndryl Resiliency Orchestration Installation Guide to perform MariaDB installation.
   b. If there is a change in the version of MariaDB, then upgrade to a supported version.
   c. Post Installation of MariaDB, Restore the metadata from backup

   ```
   mysql –u <username> -p <
   <backup_folder_path>/<filename>.sql
   ```

   d. Refer to the section “Installing Apache Tomcat” in the Kyndryl Resiliency Orchestration installation Guide to perform Tomcat installation. Assuming TOMCAT_HOME is /opt/tomcat9.
   e. If you are performing an in-place upgrade, and the MariaDB version has changed, execute the following command to check if panaces DB user can log in successfully:

```
mysql -u <username> -p <password> panaces
```

Workaround: In case the user can’t login, then the recommendation is to execute the following commands:

```
DROP USER panaces;

GRANT
SELECT,INSERT,UPDATE,DELETE,DROP,CREATE,EXECUTE,SHOW
VIEW ON panaces.* TO 'panaces'@'localhost' IDENTIFIED BY
'<password>' WITH GRANT OPTION;

GRANT
SELECT,INSERT,UPDATE,DELETE,DROP,CREATE,EXECUTE,SHOW
VIEW ON panaces.* TO 'panaces'@'<RO-IP>' IDENTIFIED BY
'<password>' WITH GRANT OPTION;

FLUSH PRIVILEGES;
```

2.4 Upgrading to the latest version

This section is applicable for the Kyndryl Resiliency Orchestration Application upgrade.

You can either:

- Host all components on the local host server (One tier mode) or
- Host DB component on a dedicated server and other components on a local host server (Two Tier mode).

In case you are on one-tier mode and would like to upgrade to two-tier mode with Kyndryl Resiliency Orchestration, refer to the topic One Tier Mode to Two Tier Mode Upgrade in GUI mode.

For the Two-tier to Two-tier upgrade, refer to Two Tier Mode to Two-Tier Mode Upgrade in console mode.

For the One-tier to One-tier upgrade, refer to One Tier to One Tier Upgrade in GUI mode.

Note: If currently installed versions of Tomcat/Maria DB are not in the supported list of versions mentioned in the install guide, then they need to be upgraded.

Refer to the Kyndryl Resiliency Orchestration installation guide for supported platform versions.

Refer to the section Preparing for upgrading to the latest version for backing up and upgrading relevant platforms.

2.4.1 One Tier Mode to Two Tier Mode Upgrade in GUI mode

For upgrading from Kyndryl Resiliency Orchestration 8.1/8.1.1/8.1.2 one-tier mode to the latest version of Two-tier mode, perform the following procedures.

1. Take all pertinent backup of the existing one-tier DB.
2. Perform 8.1/8.1.1/8.1.2 one tier to the latest version one tier upgrade.

   Note: Refer to the topic: One Tier to One Tier Upgrade.
3. Perform DB migration from single tier to two tier.

   Note: Refer to the topic **Migrating DB Component from Local Host to Dedicated Server (Split Installation)** in the Kyndryl Resiliency Orchestration Installation guide.

2.4.2 Two Tier Mode to Two Tier Mode Upgrade in the console mode

For upgrading from Kyndryl Resiliency Orchestration 8.1/8.1.1/8.1.2 two-tier mode to the latest version Two tier mode, refer to the topic **Installing the Kyndryl Resiliency Orchestration Server in Console Mode** in the Kyndryl Resiliency Orchestration Installation guide.

While editing the PanacesServerInstaller.properties file, modify the respective properties files for the keywords as shown below. The example provided here is for console/on-demand password mode, which is the recommended mode. If you choose console mode, you will need to provide the various required passwords in the property file in clear text, which is not secure.

To take a backup of the existing Metadata, add the PANACES_BACKUP_DIALOG_BUTTON parameter if it does not exist in the properties file, and then, set the value to 0. If you do not want to take a backup, set the value to 1.

Two additional properties were added for Fully Qualified Domain Name (FQDN) selection – FQDN_SELECTION and LOCAL_HOST_SERVER. Leave the FQDN_SELECTION Value as 0 (default) for the IP address. Please make sure to enter the Local host server IP address in the LOCAL_HOST_SERVER, or else the upgrade will fail.

The following additional properties are added for Two Tier AWS RDS MARIADB support.

1. #Database type
   a. Value - **MARIADB** (Co-hosted MariaDB)

      For Example –

DATABASE_TYPE=MARIADB

b. Value - **AWS_RDS_MARIADB** (AWS RDS MariaDB instance). When the database type of AWS RDS MARIADB is used, the appropriate value for the property Instance URL should be provided as shown in the example below.

For Example –

DATABASE_TYPE=AWS_RDS_MARIADB

INSTANCE_URL=database-1.mariadb.us-east-1.rds.amazonaws.com

2. #SLAVE_MODE_INSTALLATION

   Slave selection will deploy only the application files on the server

   a. Value – No (default) – Leave the value as No for Primary Kyndryl Resiliency Orchestration server deployment

   b. Value = Yes – Set the value as Yes for Standby Kyndryl Resiliency Orchestration server deployment

3. #MASTER_HOST

   This field is applicable for Standby Kyndryl Resiliency Orchestration server installation only. This is the IP address of the Primary Kyndryl Resiliency Orchestration server.

   If slave mode = yes, then Primary Kyndryl Resiliency Orchestration server IP has to be provided.

   If slave mode = no, the Primary Kyndryl Resiliency Orchestration server IP is empty, by default, the current Standby Kyndryl Resiliency Orchestration server IP will be considered as MASTER_HOST.

   a. #RDS_CERT_PATH

      If Internet connectivity is enabled in the EC2 instance, then this field can be left blank. The certificate will be automatically downloaded from AWS RDS and imported into the trust store.

      If internet connectivity is not enabled in the EC2 instance, then download the RDS certificate from https://s3.amazonaws.com/rds-downloads/rds-ca-2019-root.pem and save it in the EC2 instance. Ensure the execute permissions are enabled for the certificate to the current user (user performing the installation). Provide the absolute path of the RDS certificate in the property RDS_CERT_PATH.

Sample PanacesServerInstaller.properties file for Two Tier console mode installation is provided below -

```
#Installer UI property value is console for on demand
passwords and silent for without user interaction.
INSTALLER_UI=console
MODIFY_SYSTEM_FILES=1
USER_INSTALL_DIR=<The Current EAMSROOT Path>

#On demand password property values is Yes for console mode
and No for silent
ON_DEMAND_PASSWORD=Yes

#Number_of_Tiers Selection values are 1 or 2
# Value 1 : Host all components on the local host server
# Value 2 : Host DB component on a dedicated server and
other components on local host server
NUMBER_OF_TIERS=2
DATABASE_PORT=3306
#AWS RDS support only for two tier selection.
#Database type values are MARIADB or AWS_RDS_MARIADB
(Instance URL value #required only DB type as
AWS_RDS_MARIADB)
#RDS cert path is an optional input for AWS_RDS_MARIADB
selection (Path value with certificate file name)
DATABASE_TYPE=MARIADB
INSTANCE_URL=
RDS_CERT_PATH=
#Slave selection will deploy only the application files on
the server
#Slave mode values Yes or No
#Master_host value is required only on slave mode selection
as yes
SLAVE_MODE_INSTALLATION=No
MASTER_HOST=

#MariaDB root password is mandatory.
DATABASE_USER_NAME=<Username>
DATABASE_PASSWORD=
# Fully qualified domain name selection. Values 0 for IP
address and 1 for FQDN /hostname.
# Local host server values are Ip address or FQDN /hostname
FQDN_SELECTION=0
```

```
LOCAL_HOST_SERVER=<IP address>

KEYSTORE_FILE_PATH=$EAMSROOT/installconfig/keystore/sanovi.
keystore
REFRESH_EXISTING_SCHEMA=0
STOP_IBM_RESILIENCY_ORCHESTRATION_AND_UNINSTALL=0

#User management mode Property value is IBM_RO or
THIRD_PARTY
USER_MANAGEMENT_MODE=IBM_RO

THIRD_PARTY_SERVER_TYPE=AD
THIRD_PARTY_SERVER_URL=
THIRD_PARTY_SERVER_DOMAIN=
DIRECTORY_USERNAME=
DIRECTORY_PASSWORD=
SEARCH_BASE_FOR_READING_ROLES=
AD_DEFAULT_ROLES=
LICENSE_ACCEPTED=TRUE
SUPPORT_USER_PASSWORD=
TOMCAT_HOME=<TOMCAT_HOME>
SANOVI_USER_PASSWORD=
USER_INPUT_RESULT_NAT_IP=

#Property value is blank for fresh installation and Upgrade
for upgrade installation.
CHOSEN_INSTALL_MODE=Upgrade

#Add this property if it does not exist in the properties
file to take metadata backup during the upgrade
PANACES_BACKUP_DIALOG_BUTTON=0

#Required properties for Two-tier installation
DATABASE_HOST=<IP of the VM where DB is hosted>
DATABASE_HOST_LOGIN_USER=<Username of the VM where DB is
hosted>
SSH_PRIVATE_KEY_ABSOLUTE_PATH=/home/sanovi/.ssh/id_rsa
```

Note – MODIFY_SYSTEM_FILES=1 modifies the system files, i.e., /etc/hosts, /etc/sysconfig/selinux and /etc/sysctl.conf. The below-listed changes will be done –

```
"IP/Hostname localhost Hostname" in /etc/hosts file

"net.ipv4.tcp_retries2=4"  in /etc/sysctl.conf file

"SELINUX=permissive" in /etc/sysconfig/selinux file
```

2.4.3 One Tier to One Tier Upgrade

There are two modes of upgrade. For GUI mode, refer to <Section 2.4.3.1>

For Console mode, refer to <section 2.4.3.2>.

2.4.3.1 *One Tier to One Tier Upgrade in GUI mode*

Perform the following steps for upgrading the Kyndryl Resiliency Orchestration Server 8.1/8.1.1/8.1.2 One tier to the latest version One tier mode. The commands specified in the following points must be provided at the command prompt.

1. Download the server binaries.

   Note – For download instructions, please refer to the topic **Downloading the Software Package** in the Kyndryl Resiliency Orchestration Installation guide.

2. Log in as a Kyndryl Resiliency Orchestration User and execute the following command, whichever is applicable:

   ```
   sudo sh install.bin (or) ./install.bin
   ```

   > Note:
   > Ensure that you have a free space of approximately 2048 MB in /tmp directory before executing the above command.

3. Kyndryl Resiliency Orchestration Server upgrade starts with the following screen:

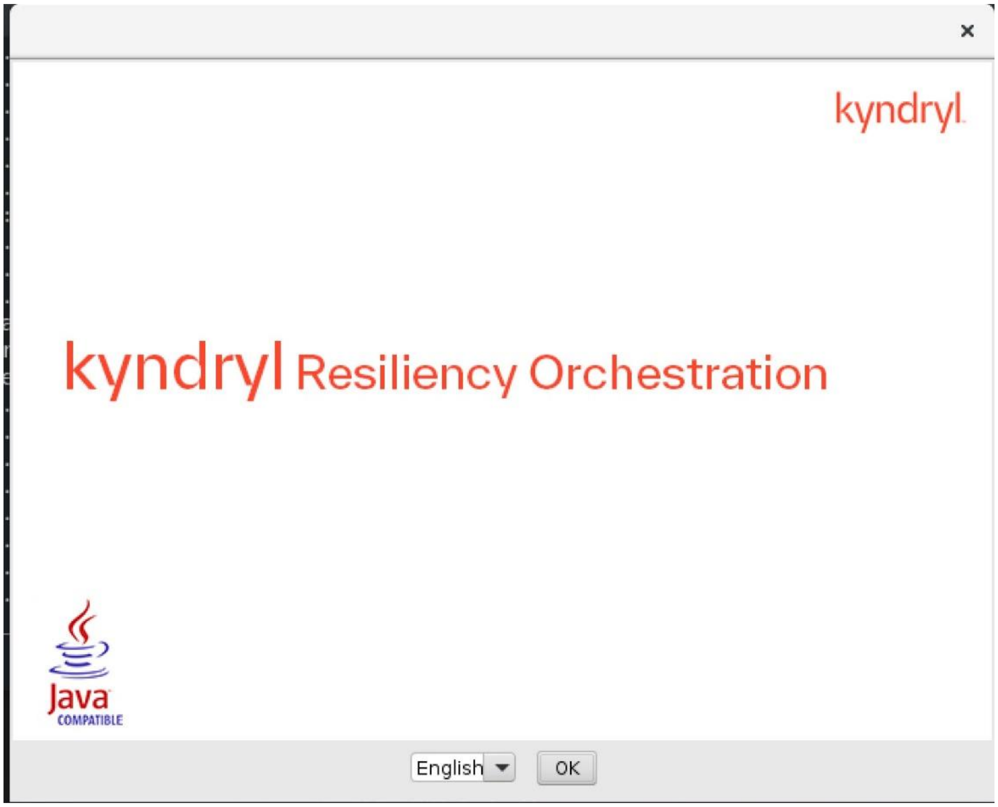
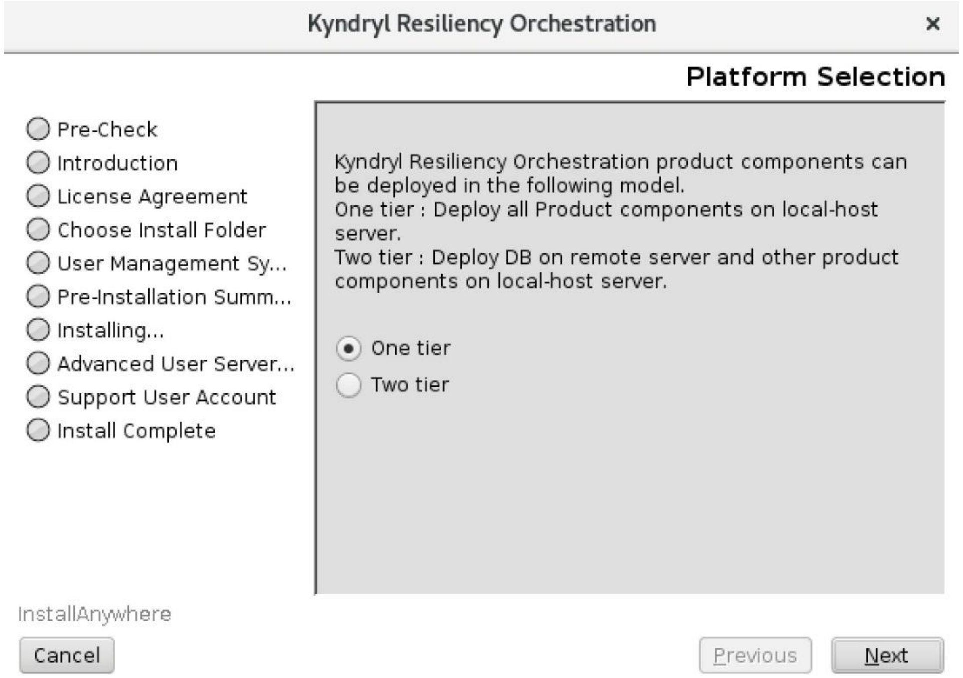


Figure 1: Kyndryl Resiliency Orchestration Installer

4. After displaying the **Kyndryl Resiliency Orchestration Installer** screen, the **Platform Selection** window is displayed.



Kyndryl Resiliency Orchestration

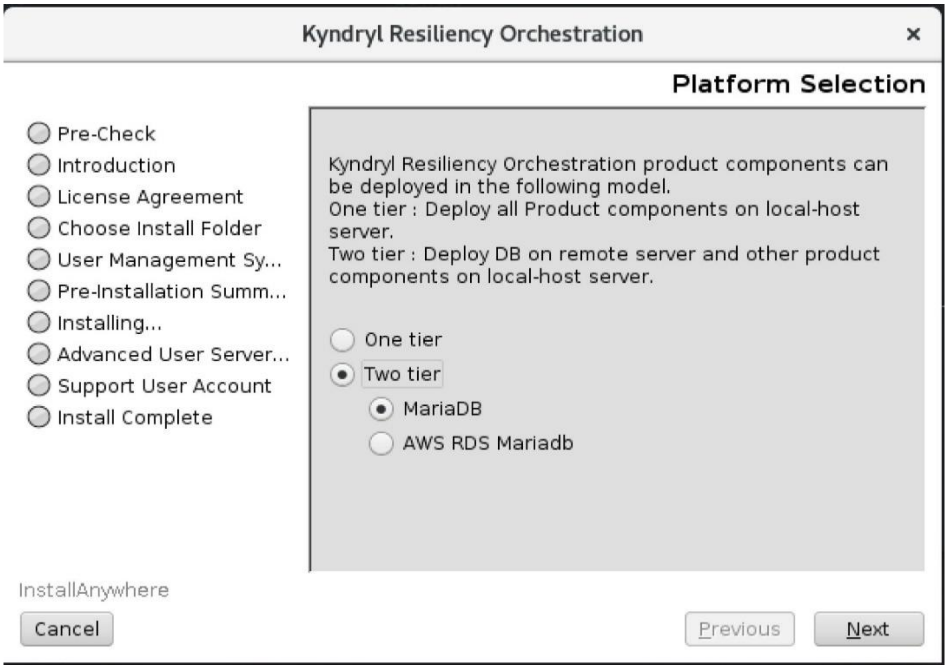
Platform Selection

Kyndryl Resiliency Orchestration product components can be deployed in the following model.
One tier : Deploy all Product components on local-host server.
Two tier : Deploy DB on remote server and other product components on local-host server.

● One tier
○ Two tier

Figure 2: Platform Selection

5. Select the option **One Tier** and then Click **Next.** The **Database Access details for single tier** window are displayed for one tier selection.



Kyndryl Resiliency Orchestration

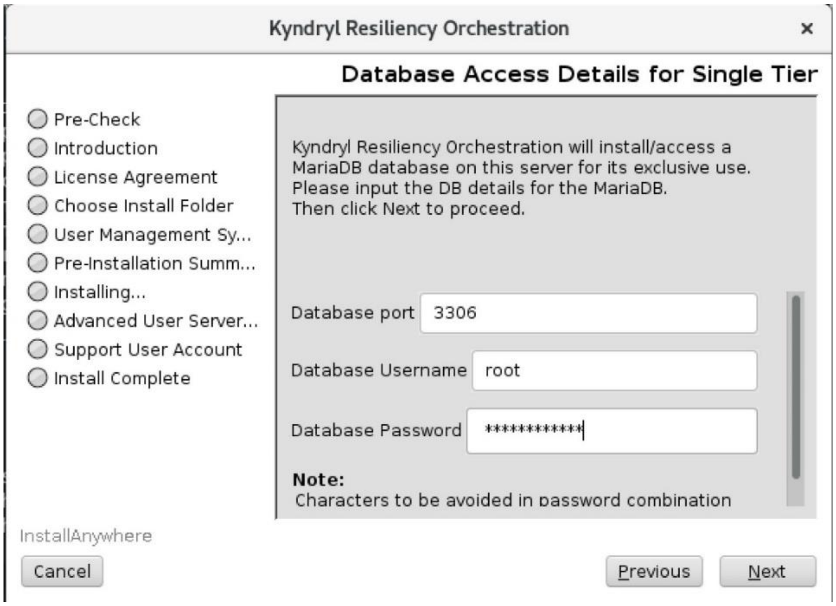
Platform Selection

Kyndryl Resiliency Orchestration product components can be deployed in the following model.
One tier : Deploy all Product components on local-host server.
Two tier : Deploy DB on remote server and other product components on local-host server.

○ One tier
● Two tier
 ● MariaDB
 ○ AWS RDS Mariadb

Figure 3: Database Access Details for Single Tier

6. Enter the **Database port number**, **Database Username,** and **Database Password.**



Database Access Details for Single Tier

Kyndryl Resiliency Orchestration will install/access a MariaDB database on this server for its exclusive use. Please input the DB details for the MariaDB. Then click Next to proceed.

Database port: 3306

Database Username: root

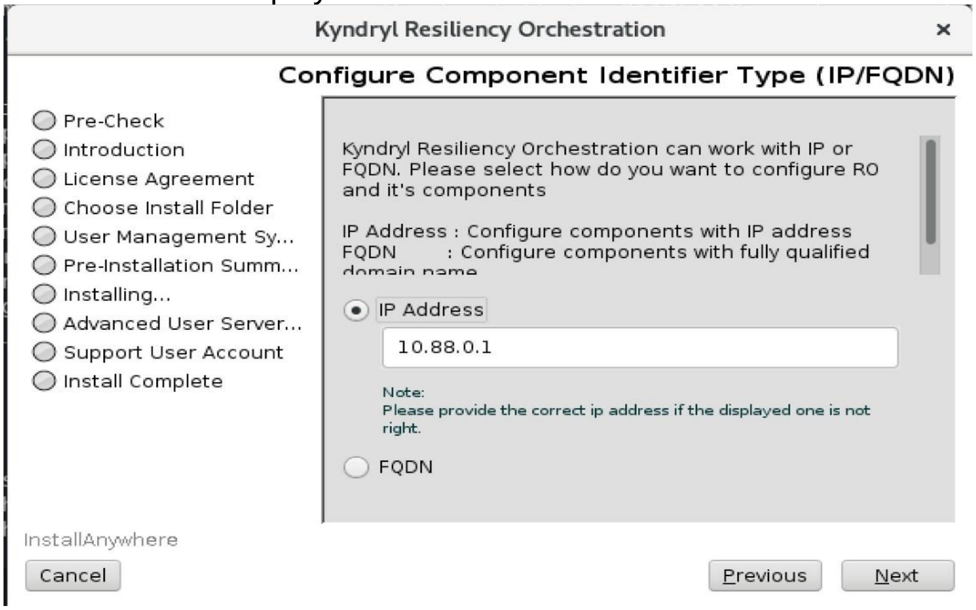
Database Password: ************

Note:
Characters to be avoided in password combination

7. Click **Next**, and the **Configure Component Identifier Type (IP/FQDN)** window is displayed.

   Kyndryl Resiliency Orchestration can work with IP or hostname (which can be also a Fully Qualified Domain Name (FQDN)). Make a selection of either IP address or FQDN in this panel.

   a. If you would like to configure the components using their IP Address, then choose option **IP Address,** and the screen such as the one shown below is displayed.



Configure Component Identifier Type (IP/FQDN)

Kyndryl Resiliency Orchestration can work with IP or FQDN. Please select how do you want to configure RO and it's components

IP Address : Configure components with IP address
FQDN : Configure components with fully qualified domain name

● IP Address

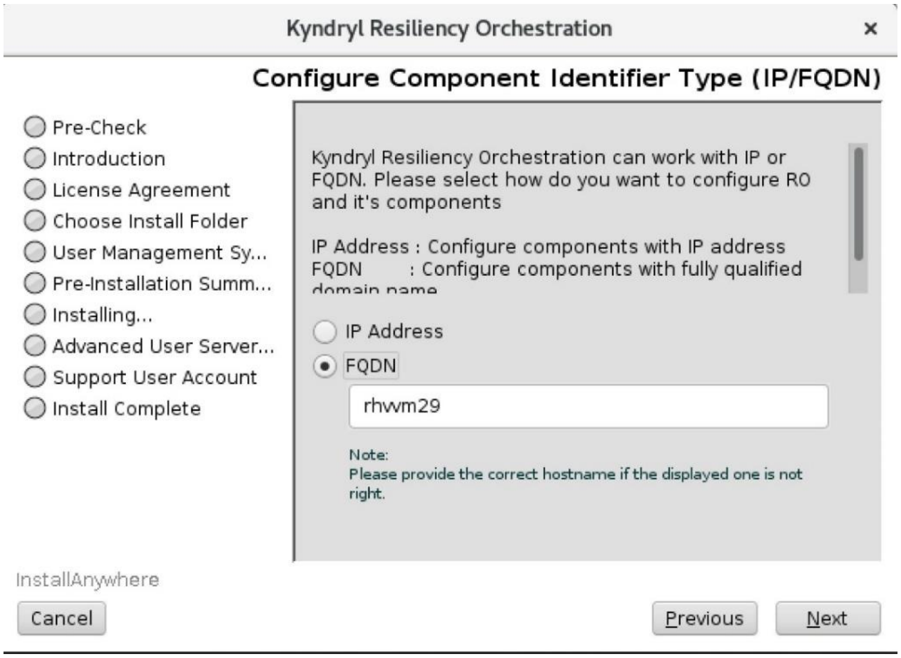
10.88.0.1

Note:
Please provide the correct ip address if the displayed one is not right.

○ FQDN

Figure 4 Configure Component Identifier Type (IP/FQDN)-IP

b. If you would like to configure components using their hostname/FQDN, select option **FQDN** and the panel changes to the one as shown below.



Configure Component Identifier Type (IP/FQDN)

Kyndryl Resiliency Orchestration can work with IP or FQDN. Please select how do you want to configure RO and it's components

IP Address : Configure components with IP address
FQDN : Configure components with fully qualified domain name

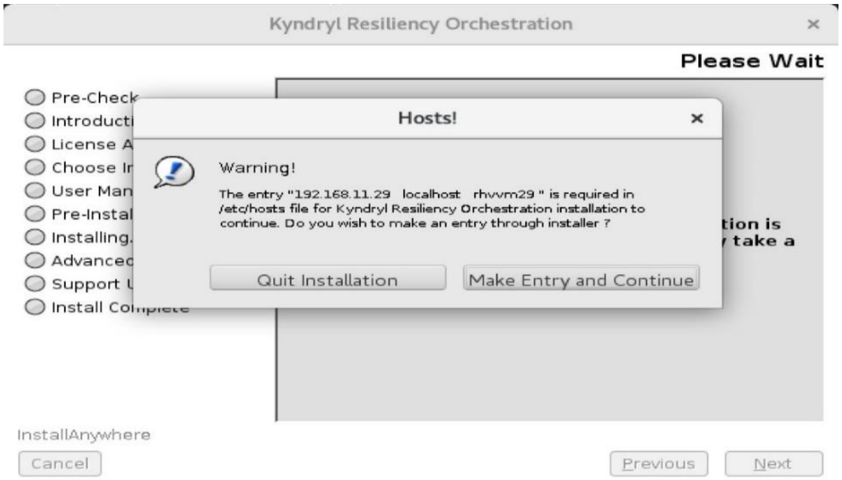
○ IP Address
● FQDN

rhvvm29

Note:
Please provide the correct hostname if the displayed one is not right.

Figure 5: Configure Component Identifier Type (IP/FQDN)-FQDN

8. Enter the IP Address or hostname/FQDN and click **Next**. The **Hosts (on localhost)** warning window is displayed.



Warning!

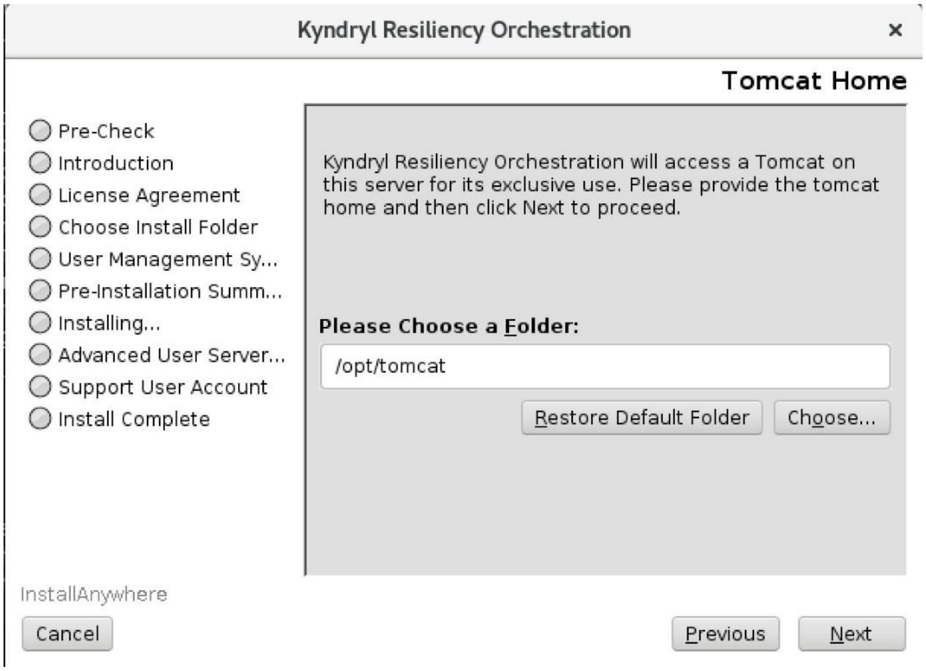
The entry "192.168.11.29 localhost rhvvm29 " is required in /etc/hosts file for Kyndryl Resiliency Orchestration installation to continue. Do you wish to make an entry through installer ?

Figure 6:Local Host entry

Click **Make Entry and Continue** if you wish to make an entry of the local host entry in /etc/hosts through the installer or

Click **Quit Installation** and make the entry of localhost in /etc/hosts manually. Restart at Step 1.

9. The **Tomcat Home** window is displayed.



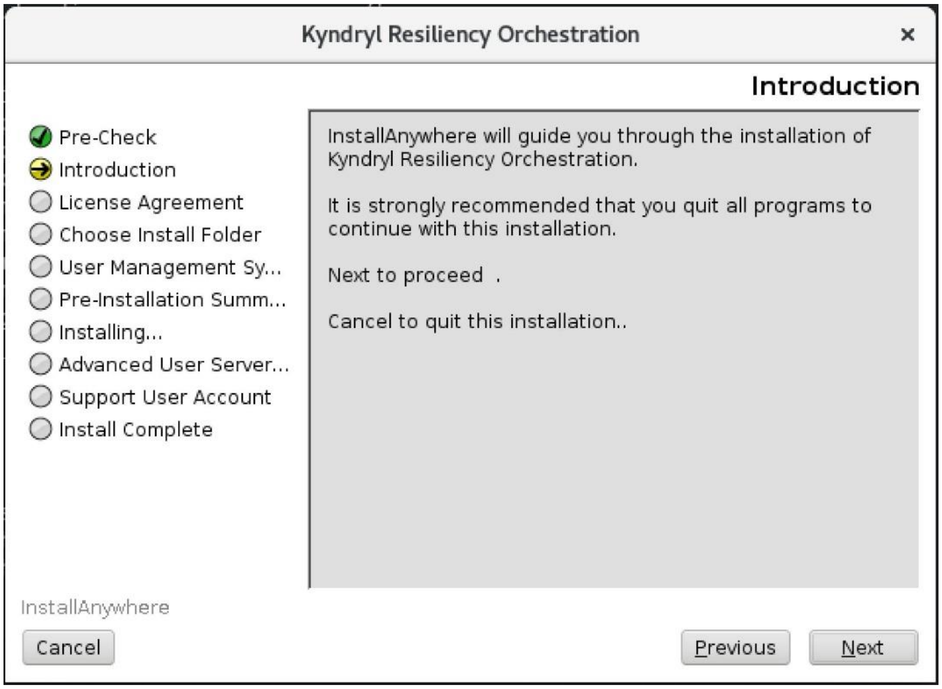
Kyndryl Resiliency Orchestration will access a Tomcat on this server for its exclusive use. Please provide the tomcat home and then click Next to proceed.

Please Choose a Folder: /opt/tomcat

Figure 7:Tomcat Home

10. Click **Choose…** to browse and select the location of Tomcat and then click **Next**. The **Introduction** window is displayed.

Note:
Please close any other running applications before clicking the **Next** button to ensure a clean installation.



InstallAnywhere will guide you through the installation of Kyndryl Resiliency Orchestration.

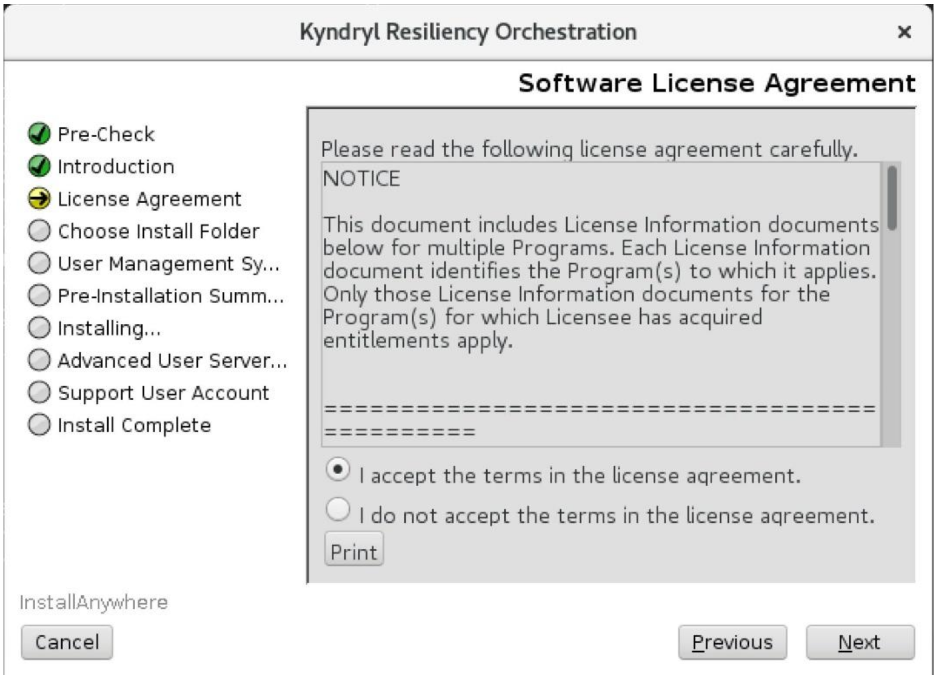
It is strongly recommended that you quit all programs to continue with this installation.

Next to proceed .

Cancel to quit this installation..

Figure 8: Introduction Window

11. Click **Next**. The **License Agreement** window is displayed.



Please read the following license agreement carefully.

NOTICE

This document includes License Information documents below for multiple Programs. Each License Information document identifies the Program(s) to which it applies. Only those License Information documents for the Program(s) for which Licensee has acquired entitlements apply.

==================================== ==========

● I accept the terms in the license agreement.

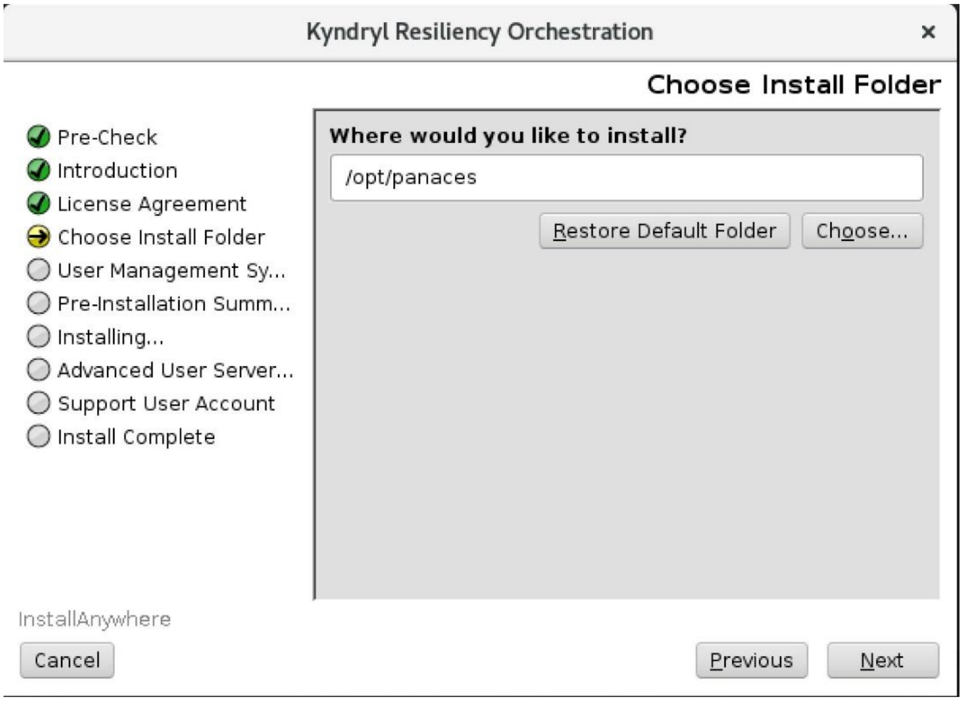
○ I do not accept the terms in the license agreement.

Figure 9: License Agreement

12. Click the appropriate option button after reading the **License Agreement**. The options are:

Option Button	Description
I accept the terms of the license agreement	Click this option button for acceptance of the License Agreement.
I do NOT accept the terms of the license agreement	Click this option button for rejection of the License Agreement. By default, this is selected. The Next button is unavailable with this option.

13. Click **Next** (on acceptance of the **License Agreement** window) to proceed with the installation. The **Choose Install Folder** window is displayed.



Where would you like to install?

/opt/panaces

Figure 10: Choose Install Folder

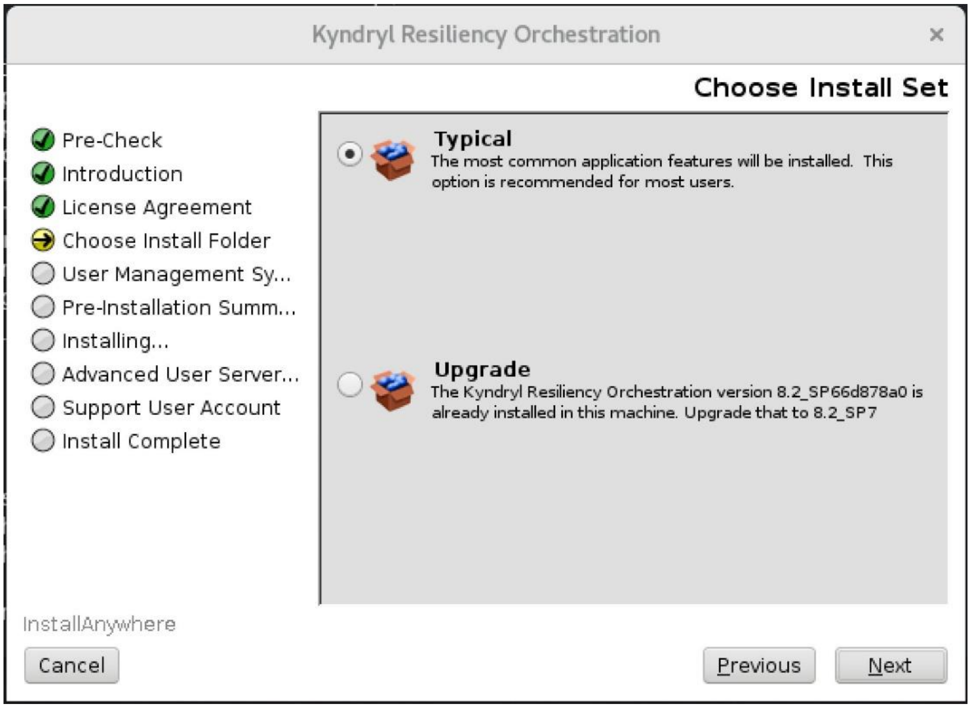
14. Select a path to install the software by clicking **Choose.** Choose the path where the Panaces are currently installed.

> **Note**:
>
> The latest version binaries will be installed in the same path by renaming the existing installation folder by appending the release name. For example, if 8.1.3 is installed in /opt/panaces, the folder will be renamed to /opt/
>
> panaces_8.1_82cace9 contains the old installation, while /opt/panaces will be installed with the latest version.

15. Click **Next** to continue.

Note:

The **Choose Install Set** window is displayed. The **Choose Install Set** screen will be displayed only when the user selects the install location same as the current one. See the sample screen shown in the following figure. For Example, Upgrade from a previous version to the latest version, the screen looks like the below.

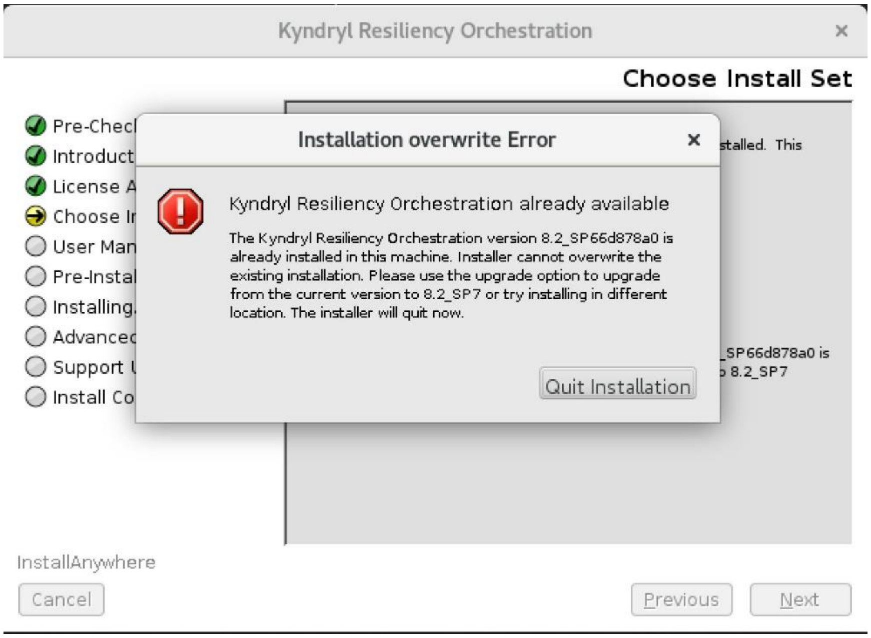


● **Typical**
The most common application features will be installed. This option is recommended for most users.

○ **Upgrade**
The Kyndryl Resiliency Orchestration version 8.2_SP66d878a0 is already installed in this machine. Upgrade that to 8.2_SP7

Figure 11: Choose Install Set

16. If Typical is selected and the current version of Kyndryl Resiliency Orchestration Server already is present in the system, the following error is displayed:



Installation overwrite Error

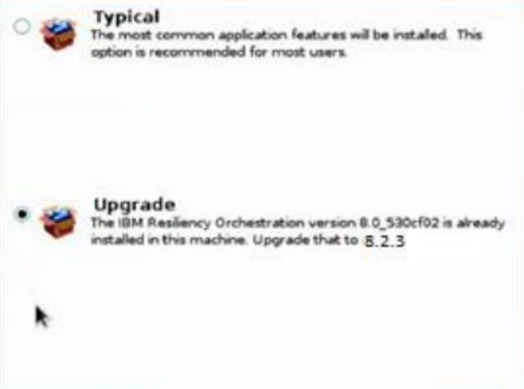
Kyndryl Resiliency Orchestration already available

The Kyndryl Resiliency Orchestration version 8.2_SP66d878a0 is already installed in this machine. Installer cannot overwrite the existing installation. Please use the upgrade option to upgrade from the current version to 8.2_SP7 or try installing in different location. The installer will quit now.

Quit Installation

Click **Cancel** to abort.

17. Click the **Upgrade** icon.



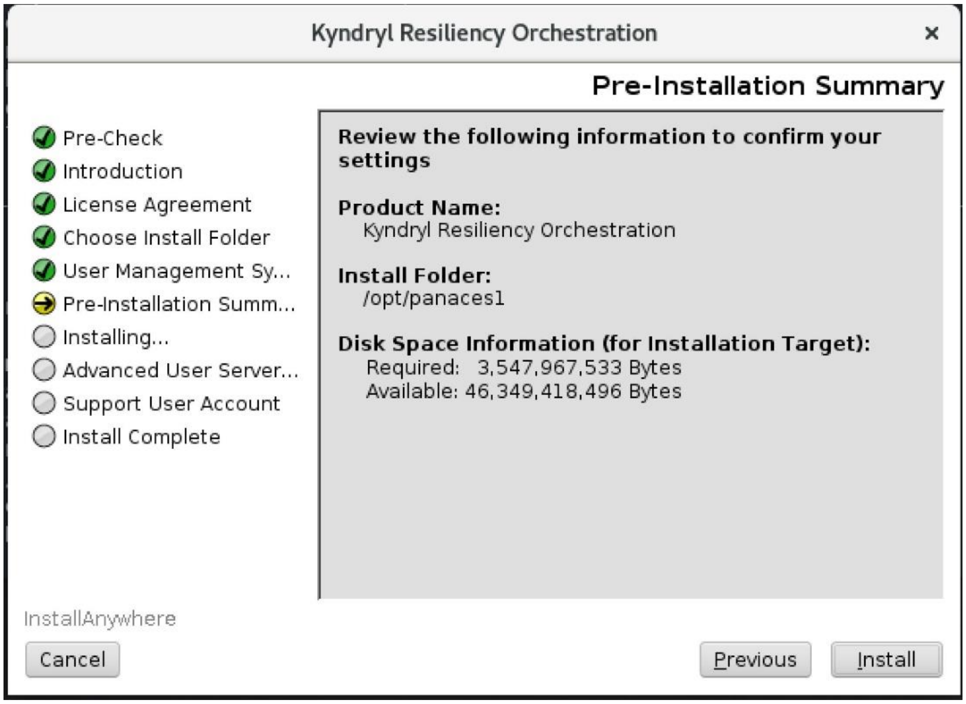
○ Typical
The most common application features will be installed. This option is recommended for most users.

● Upgrade
The IBM Resiliency Orchestration version 8.0_530cf02 is already installed in this machine. Upgrade that to 8.2.3

The RO binaries are installed in the same path by renaming the existing installation folder by appending the release name. For example, if 8.3.0 is installed in */opt/panaces*, the folder is zipped to */opt/panaces_8.3_<revision ID>.zip* containing the old installation, while */opt/panaces* will be installed with the latest version.

18. Click **Next**. The **Please Wait** window is displayed.

19. After Resiliency Orchestration is configured for your system, the Next button is enabled. Click **Next.** The Pre-Installation summary window is displayed.



Kyndryl Resiliency Orchestration ×

Pre-Installation Summary

- ✓ Pre-Check
- ✓ Introduction
- ✓ License Agreement
- ✓ Choose Install Folder
- ✓ User Management Sy...
- ➔ Pre-Installation Summ...
- ○ Installing...
- ○ Advanced User Server...
- ○ Support User Account
- ○ Install Complete

Review the following information to confirm your settings

Product Name:
Kyndryl Resiliency Orchestration

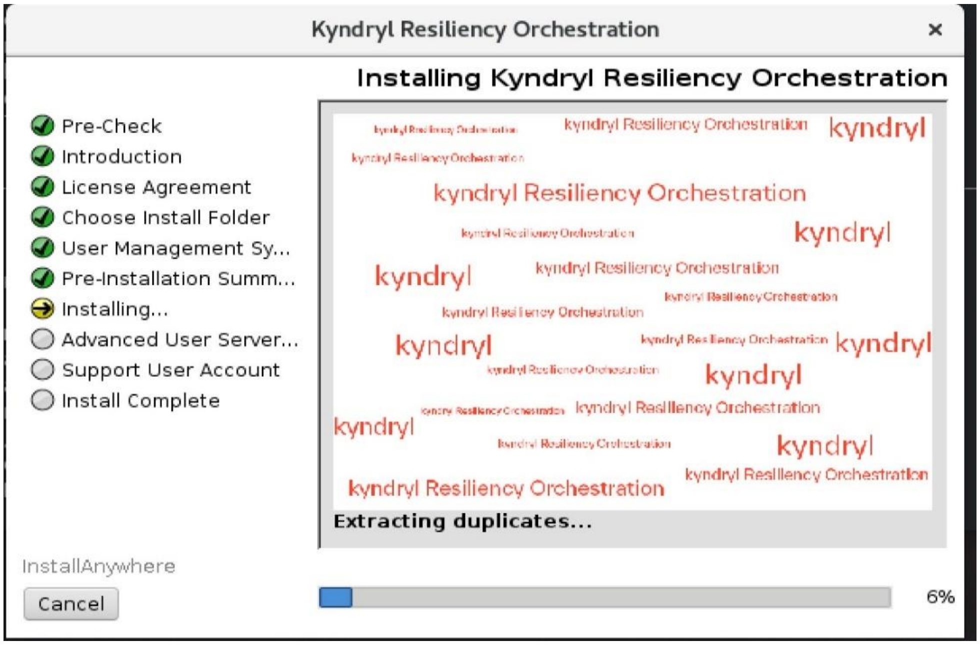
Install Folder:
/opt/panaces1

Disk Space Information (for Installation Target):
Required: 3,547,967,533 Bytes
Available: 46,349,418,496 Bytes

InstallAnywhere

Figure 13: Pre-Installation window

20. Click **Install**. The **Installing Kyndryl Resiliency Orchestration** windows are displayed.



Kyndryl Resiliency Orchestration ×

Installing Kyndryl Resiliency Orchestration

- ✓ Pre-Check
- ✓ Introduction
- ✓ License Agreement
- ✓ Choose Install Folder
- ✓ User Management Sy...
- ✓ Pre-Installation Summ...
- ➔ Installing...
- ○ Advanced User Server...
- ○ Support User Account
- ○ Install Complete

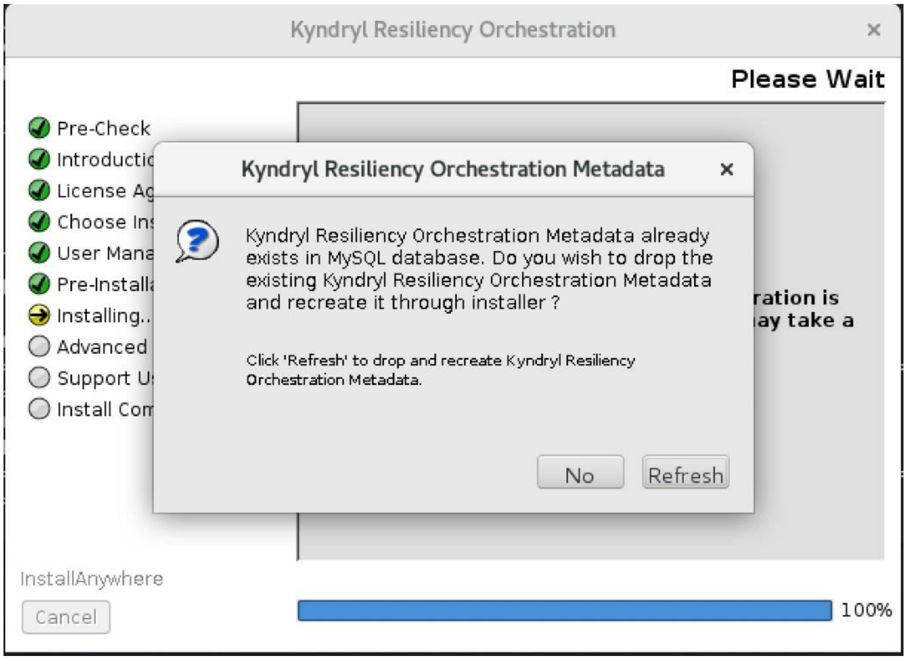
Extracting duplicates...

InstallAnywhere

6%

Figure 14: Installing Kyndryl Resiliency Orchestration window

21. The **Taking Backup of existing metadata** dialog box appears.



Kyndryl Resiliency Orchestration Metadata

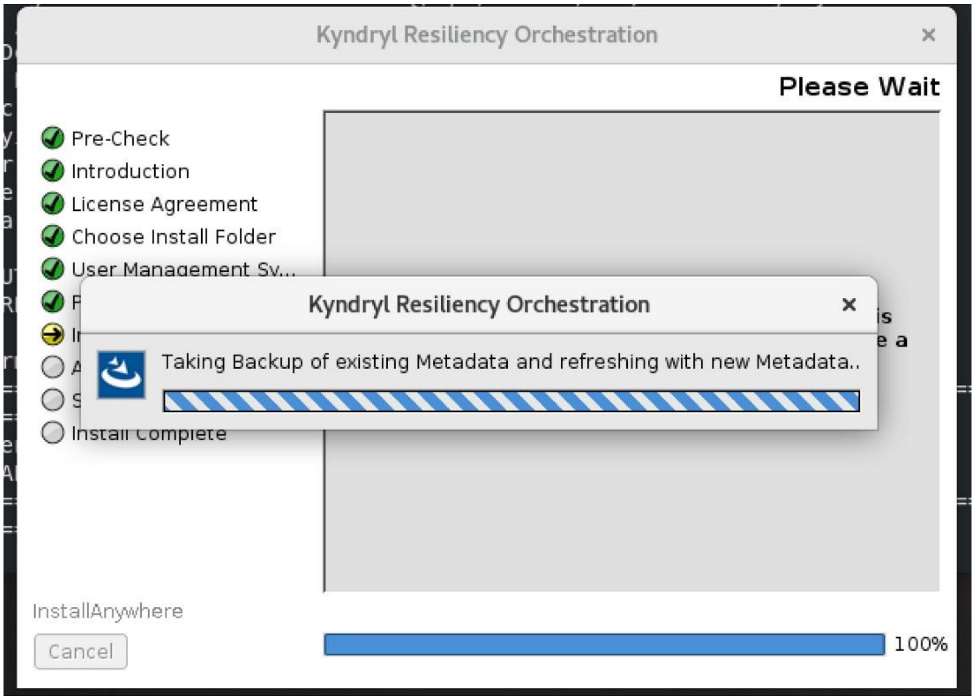
Kyndryl Resiliency Orchestration Metadata already exists in MySQL database. Do you wish to drop the existing Kyndryl Resiliency Orchestration Metadata and recreate it through installer ?

Click 'Refresh' to drop and recreate Kyndryl Resiliency Orchestration Metadata.

Figure 15: Taking Backup of existing metadata option

22. Click **Yes** to take the backup of the metadata or **No** to dismiss.

> **Note:** If **Yes** is selected, the installer will take a backup of the existing metadata before upgrading.



Taking Backup of existing Metadata and refreshing with new Metadata..

Figure 16: Upgrade Progress

23. Post the upgrade, the **Upgrade Complete** window appears as shown below.

Note:
At this stage, the older installation folder is renamed by appending the current release name. Therefore, in case the upgrade is canceled, the older installation folder has to be renamed to its original name by the user as part of the fallback plan. For example, if 8.1.3 is installed in /opt/panaces, the folder will be renamed to /opt/panaces_8.1<*buid_revision_No*>. If the upgrade is canceled, the user has to rename /opt/panaces_8.1<build_revision_No> to /opt/panaces to reinitiate the upgrade or to continue to use the older version of the product.

24. Click **Done** to exit the installer.

Limitation:

Upgrading Kyndryl Resiliency Orchestration (Integrated with AD)) to the latest version of Kyndryl Resiliency Orchestration, through GUI mode and Console mode is not supported Please perform the following workaround procedure if AD integration is needed.

Workaround:

After upgrading the Kyndryl Resiliency Orchestration (without AD integration), import the AD server certificate and configure AD manually by executing DRMChangeUserMgmtMode.sh script as shown in the steps below -

1. `Go to $EAMSROOT/<jdk_folder>/bin`

2. `Import AD certificate using command –`

```
keytool -import -keystore
$EAMSROOT/<jdk_folder>/jre/lib/security/cacerts -alias 'RO-
AD-Server' -file  <AD certificate file>  -storepass
changeit -noprompt
```

```
Example -
```

```
keytool -import -keystore
/opt/panaces_813/jdk1.8.0_261/jre/lib/security/cacerts -
alias 'RO-AD-Server' -file /tmp/ldaps_new.cer -storepass
changeit -noprompt
```

```
3. Go to $EAMSROOT/bin
```

```
4. Execute the command sudo ./DRMChangeUserMgmtMode.sh
```

Refer to **Enabling SSL Security for Active Directory** and **User Authentication and Authorization** sections in *Kyndryl Resiliency Orchestration Administrator's guide* for usage of key tool command and script DRMChangeUserMgmtMode.sh

Step 4 can be skipped in case of an upgrade of Kyndryl Resiliency Orchestration software on the same server and without schema refresh.

2.4.3.2 *One-tier to one-tier upgrade in Console mode*

In the Console mode method, the installation program reads the settings for your configuration from the *PanacesServerInstaller.properties* file that you need to update before the upgrade. The installation program does not display any configuration options during the upgrade process.

Note:
Confirm that the hardware and software configurations required for Kyndryl Resiliency Orchestration installation are available.

2.4.3.2.1 Steps to be Performed for Console Mode Upgrade

To complete the upgrade procedure in Console Mode, complete the following steps:

1. Open the properties file (PanacesServerInstaller.properties) by using the following command:

```
i. cd <Installer path>
```

    ii. `sudo vi PanacesServerInstaller.properties`

    iii. **Note:** For parameter description, please refer to the topic **Installing the Kyndryl Resiliency Orchestration Server in Console Mode** in the Kyndryl Resiliency Orchestration Installation guide.

2. Update the key `"CHOSEN_INSTALL_MODE="` value to `"Upgrade"`
   Example: `CHOSEN_INSTALL_MODE=Upgrade`

3. To take a backup of the existing Metadata, add the PANACES_BACKUP_DIALOG_BUTTON parameter if it does not exist in the properties file, and then, set the value to 0. If you do not want to take a backup, set the value to 1.

    i. **Example**: `PANACES_BACKUP_DIALOG_BUTTON=0`

4. Modify the parameter (`USER_INSTALL_DIR`) in the properties file with the path to the directory where the current version of the software was installed. The new software version will be installed in the same location.

5. Two additional properties are added for Fully Qualified Domain Name (FQDN) selection – FQDN_SELECTION and LOCAL_HOST_SERVER. Leave the FQDN_SELECTION Value as 0 (default) for the IP address. Please make sure to enter the Local host server Ip address in the LOCAL_HOST_SERVER, else upgrade will fail.

6. Some additional properties are added for Two Tier AWS RDS MARIADB support. Refer to section Two Tier Mode to Two Tier Mode Upgrade in console mode for details.

Sample PanacesServerInstaller.properties file for one-tier installation in console mode is provided below -

```
#Installer UI property value is console for on-demand
passwords and silent without user interaction.
INSTALLER_UI=console
MODIFY_SYSTEM_FILES=1
USER_INSTALL_DIR=<The Current EAMSROOT Path>

#On demand password property values are Yes for
console mode and No for silent
ON_DEMAND_PASSWORD=Yes

#Number_of_Tiers Selection values are 1 or 2
# Value 1 : Host all components on the local host
server
# Value 2 : Host DB component on a dedicated server
and other components on local host server
```

```
NUMBER_OF_TIERS=1
DATABASE_PORT=3306


#MariaDB root password is mandatory.
DATABASE_USER_NAME=<Username>
DATABASE_PASSWORD=

# Fully qualified domain name selection. Values 0 for
IP address or 1 for FQDN /hostname.
# Local host server values are Ip address or FQDN
/hostname
FQDN_SELECTION=0
LOCAL_HOST_SERVER=<IP address>

KEYSTORE_FILE_PATH=$EAMSROOT>/installconfig/keystore/s
anovi.keystore
REFRESH_EXISTING_SCHEMA=0
STOP_IBM_RESILIENCY_ORCHESTRATION_AND_UNINSTALL=0

#User management mode Property value is IBM_RO or
THIRD_PARTY
USER_MANAGEMENT_MODE=IBM_RO

THIRD_PARTY_SERVER_TYPE=AD
THIRD_PARTY_SERVER_URL=
THIRD_PARTY_SERVER_DOMAIN=
DIRECTORY_USERNAME=
DIRECTORY_PASSWORD=
SEARCH_BASE_FOR_READING_ROLES=
AD_DEFAULT_ROLES=
LICENSE_ACCEPTED=TRUE
SUPPORT_USER_PASSWORD=
TOMCAT_HOME=<TOMCAT_HOME>
SANOVI_USER_PASSWORD=
USER_INPUT_RESULT_NAT_IP=

#Property value is blank for fresh installation and
Upgrade for upgrade installation.
CHOSEN_INSTALL_MODE=Upgrade
```

Note - Refer *MODIFY_SYSTEM_FILES* for details about this property.

7. Execute the following command to start the installation:

```
sudo /<Installer path>/install.bin -f /<Installer
Path>/PanacesServerInstaller.properties
```

8. After upgrading, follow the steps in the section *Post Upgrade*.

2.5 Site Controller Upgrade

In case you are currently using a lower version of Site Controller (SC), then follow the below steps to upgrade.

Prerequisites:

- Ensure that the version for SC and related OS mentioned in the interop are met.
- Make sure the original TCL/Scripts or any other customized files are restored, once after upgrading (RO/Local Agent/SC) manually from the backup folder.

2.5.1 Steps for Kyndryl RO Linux SC upgrade to the latest version

1. Stop the services.
2. Download the Kyndryl Resiliency Orchestration Linux SC software from the fix/JFrog central.
3. Run the installer.
4. In the PanacesAgentNodeInstaller.properties set CHOSEN_INSTALL_MODE=upgrade
5. Update the $EAMSROOT/installconfig/SiteController.cfg with the new RO value as below.

   For Example: –

   ```
   PANACES_MASTER_SERVER_ADDRESS = <<old IP>>
   PANACES_SLAVE_SERVER_ADDRESS = << old IP >>
   Change it to:
   PANACES_MASTER_SERVER_ADDRESS = <<New IP>>
   PANACES_SLAVE_SERVER_ADDRESS = <<New IP>>
   ```

6. Start the Site Controller services.
7. Post-starting Linux SC should be connected to the Kyndryl Resiliency Orchestration and start the associated agents from the Kyndryl Resiliency Orchestration UI.

Notes:

- For more information on editing PanacesAgentNodeInstaller.properties file, refer to the Installation Guide.
- The RO binaries are installed in the same path by renaming the existing installation folder by appending the release name. For example, if 8.3.0 is installed in */opt/panaces*, the folder is zipped to

/opt/panaces_8.3_<revision ID>.zip containing the old installation, while */opt/panaces* will be installed with the latest version.

2.5.2 Steps for Kyndryl RO Windows SC upgrade to the latest version

Note: For Kyndryl RO Windows SC upgrade, we have certified Windows 2016 SC upgrade from 8.1.3 to the latest version.

1. Stop the services.
2. Download the Kyndryl Resiliency Orchestration Windows SC software from fix central.
3. Run the installer.
4. Select CHOSEN_INSTALL_MODE as an upgrade.
5. Install the Kyndryl Resiliency Orchestration Windows SC software.
6. EAMSROOT should be installed and a backup folder should be created.

   Eg: panaces_SCC_8.0_530cf02
7. Update the $EAMSROOT/installconfig/SiteController.cfg with new RO value as below.

For Example: –

```
 PANACES_MASTER_SERVER_ADDRESS = <<old IP>>
PANACES_SLAVE_SERVER_ADDRESS = << old IP >>
Change it to:
PANACES_MASTER_SERVER_ADDRESS = <<New IP>>
PANACES_SLAVE_SERVER_ADDRESS = << New IP >>
```

1. Restart the services.
2. Post starting Windows, SC should be connected to the Kyndryl Resiliency Orchestration and associated agents need to be started from the Kyndryl Resiliency Orchestration UI.

   Notes:

   - The SC status is displayed as “Connected” on the Site Controller tab at Kyndryl Resiliency Orchestration UI.
   - The RO binaries will be installed in the same path by renaming the existing installation folder by appending the release name. For example, if 8.3.0 is installed in /opt/panaces, the folder will be zipped to /opt/panaces_8.3_<revision ID>.zip containing the old installation, while /opt/panaces will be installed with the latest version.

2.6 Resiliency File Replicator (RFR) Upgrade

Refer to the File Replicator Installation Guide.

2.7 Update Production NICRA and Staging Appliance (RHEL 8.4)

(This upgrade step is applicable only for nicra RHEL version 8.4)

Step 1: Back up the VMDK mapping file.

(Step applicable on Production Nicra)

```
              [root@PR_Nicra ~]# dtcresetport -d
/var/opt/IBMRBRdtc/vmdk_mapping_flle_bkp.txt
```

Step 2: Move the mobility groups on Nicra to NDU mode.

(Step applicable on Production Nicra)

(Note: We should complete the complete nicra upgrade in <20 mins)

```
              [root@PR_Nicra ~]# dtcstartndu
               //After executing the command, please monitor the file
/var/log/messages for the log
              DTC: [INFO / GENMSG]: STARTNDU completed successfully

              // Monitor for 5 mins, for the above trace. If you are still
unable to see the trace, Please stop the NDU and Re-try the NDU process
after ~15 mins.
     [root@PR_Nicra ~]# dtcstopndu    (Command to stop NDU)
     [root@PR_Nicra ~]# dtcstartndu   (Command to re-try start NDU after
15 mins)

// dtcstartndu will pause the replication and we will not see any local
writes (data) from VIB to Nicra until we finish the upgrade.
```

Step 3: Uninstall old rpm in NICRA

(group stops from normal mode)

```
[root@snapshot-source ~]# rpm -e IBM-Resiliency-Block-Replicator-
ADB-3.0.0.0-18651.x86_64
No IBM Resiliency Block Replicator for UNIX* RMD daemons were
running.
in.dtc master IBM Resiliency Block Replicator for UNIX* daemon
has been shutdown
```

```
     throtd IBM Resiliency Block Replicator for UNIX* throttle daemon
     is not running
     Stop IBM IBM Resiliency Block Replicator for UNIX* Agent daemons
     IBM IBM Resiliency Block Replicator for UNIX* Agent has been
     shutdown
     Moving IBMRBRdtc Config files to
     /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
     Moving IBMRBRdtc Shell files to
     /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
     Moving IBMRBRdtc License files to
     /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
     Moving IBMRBRdtc Product usage statistics files to
     /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
     Moving IBMRBRdtc Product usage checksum files to
     /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
     Moving the dtc.conf file to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
     Moving IBMRBRdtc Agent Config files to
     /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
     Moving IBMRBRdtc vmdk_mapping file to
     /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
     service IBMRBRdtc-scan does not support chkconfig
Disabling and removing IBMRBRdtc-start.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-
start.service.
Disabling and removing IBMRBRdtc-stop.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-
stop.service.
Disabling and removing IBMRBRdtc-startdaemons.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-
startdaemons.service.
Disabling and removing IBMRBRdtc-startmaster.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-
startmaster.service.
Disabling and removing IBMRBRdtc-startpmds.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-
startpmds.service.
warning: file /etc/opt/IBMRBRdtc/dtc_pre_failover_pxxx.sh: remove
failed: No such file or directory
warning: file /etc/opt/IBMRBRdtc/dtc_post_failover_sxxx.sh: remove
failed: No such file or directory
warning: file /etc/opt/IBMRBRdtc/dtc_post_failover_pxxx.sh: remove
failed: No such file or directory
warning: file /etc/opt/IBMRBRdtc/DTC.lic.perm: remove failed: No such
file or directory
Removing IBM Resiliency Block Replicator for UNIX* Symbolic Links from
/usr/local/bin
Removing IBM Resiliency Block Replicator for UNIX* device tree:
/dev/dtc
Removing temporary files from /var/opt/IBMRBRdtc
Removing core files from /var/run/IBMRBRdtc
Removing IBM Resiliency Block Replicator for UNIX* master daemon from
/etc/services
Saving current /etc/modprobe.d/ibmrbrdtc.conf to
/etc/modprobe.d/ibmrbrdtc.conf.pre_dtc_remove
Removing IBM Resiliency Block Replicator for UNIX* modifications from
/etc/modprobe.d/ibmrbrdtc.conf
Cleaning up /etc/opt/IBMRBRdtc and /opt/IBMRBRdtc
Cleaning up IBMBR UDEV SUPPORT RULES
[root@snapshot-source ~]#
```

Step 4: Install the new rpm in NICRA

```
[root@snapshot-source ~]# rpm -ivh /opt/BAD/RedHat/7x/x86_64/IBM-
Resiliency-Block-Replicator-ADB-3.0.0.0-18656.x86_64.rpm
Preparing...
################################## [100%]
Updating / installing...
   1:IBM-Resiliency-Block-Replicator-
A################################## [100%]
Creating Symbolic Links in /usr/local/bin
Setting up IBMRBR UDEV SUPPORT
 find and create entry of in.dtc in /etc/services
Restore license file and shell script files from past revs
Restoring previously saved IBMRBRdtc license key file.
Restoring previous Agent config file.
Restoring previous vmdk-mapping config file.
Restoring previously saved IBMRBRdtc device list file.
see if Previous IBM Resiliency Block Replicator for UNIX* Installation
saves exist
Installing our IBMRBRdtc-start.service and IBMRBRdtc-
startdaemons.service files and enabling them to have our scripts
called at boot time
Created symlink from /etc/systemd/system/multi-
user.target.wants/IBMRBRdtc-start.service to
/etc/systemd/system/IBMRBRdtc-start.service.
Created symlink from /etc/systemd/system/multi-
user.target.wants/IBMRBRdtc-startdaemons.service to
/etc/systemd/system/IBMRBRdtc-startdaemons.service.
Installing our IBMRBRdtc-startmaster.service and IBMRBRdtc-
startpmds.service files and enabling them to have our scripts called
at boot time
Created symlink from /etc/systemd/system/multi-
user.target.wants/IBMRBRdtc-startmaster.service to
/etc/systemd/system/IBMRBRdtc-startmaster.service.
Created symlink from /etc/systemd/system/multi-
user.target.wants/IBMRBRdtc-startpmds.service to
/etc/systemd/system/IBMRBRdtc-startpmds.service.
```

```
Removing the old IBMRBRdtc-startdaemons links from the /etc/rc.d
directories
Installing our IBMRBRdtc-stop.service file and enabling it to have our
scripts called at shutdown time
Created symlink from /etc/systemd/system/multi-
user.target.wants/IBMRBRdtc-stop.service to
/etc/systemd/system/IBMRBRdtc-stop.service.
Starting IBM IBM Resiliency Block Replicator for UNIX* daemons
Launching /opt/IBMRBRdtc/bin/in.dtc
```

Step 5: Run "dtcagentset" and retain the config of NICRA

```
[root@snapshot-source ~]# dtcagentset
A previous set of migration group configuration file has been detected
on this system.
Would you like to migrate them into the current environment? [y/n] : y
The migration group configuration file is migrated.
Collector connection information.
  IP address       = 192.168.10.44
  Port number      = 576
  AgentIP address  = 192.168.10.170
  BAB size         = 1547 (MB)
  Transmit Interval= 30 sec
  Listener Port    = 15005
```

Step 6: Update the backup VMDK mapping file.

```
(Step applicable on Production Nicra)
[root@PR_Nicra ~]# dtcresetport -u
/var/opt/IBMRBRdtc/vmdk_mapping_flle_bkp.txt
```

Step 7: Reboot the NICRA VM

```
[root@snapshot-source ~]# reboot
```

Step 8: After Nicra reboot: Stop the NDU mode.

```
(Step applicable on Production Nicra)

[root@PR_Nicra ~]# dtcstopndu

// This command will start the group and resume the
replication.
```

*Repeat the above steps for SA - (can be done before the maintenance window also)

Step 9: RBR Procedure to Upgrade VIB and NICRA/SA without impacting the Groups

Follow the below 7 steps to upgrade VIB and NICRA/SA.

Expand each step to see the details:

Step1 Suspend PRVMS In Vcenter (OR power off the PRVMs)

Login to the Vcenter and suspend the identified Protected VMs (PRVMS). If there are any issues in suspending, then we can choose to Power off the PRVMs.

Step 2 Ensure the group is in a Normal state and zero Data Lag in Groups

The group is in a Normal state itself but the VMDK goes OFFLINE as shown below in the “dtcmonitortty” command output of NICRA

```
2020/05/09 01:14:14 PMD_003 INFO / ESXI_CLIENT_FD: Esxi VMDK's Client FD is:21

2020/05/09 01:14:14 PMD_003 WARNING / GENMSG: Checking leftover bytes from previous pmd shutdown for fd 21

2020/05/09 01:14:14 PMD_003 WARNING / GENMSG: Flushed the queue having 0 bytes of data

2020/05/09 01:14:15 PMD_003 INFO / RFDPHASE2END: Full refresh phase 2 completed for group PMD_003

2020/05/09 01:14:17 PMD_003 INFO / PMDSTART: PMD (Primary Mirror Daemon) started PMD_003

2020/05/09 01:38:30 PMD_003 WARNING / GENMSG: Not enough space in RPO timestamp queue

2020/05/09 01:47:03 (null) WARNING / GENMSG: IBMRBR: VMDK_OFFLINE command received

2020/05/09 01:47:03 (null) WARNING / GENMSG: IBMRBR: VMDK_OFFLINE command received

2020/05/09 01:47:03 (null) WARNING / GENMSG: IBMRBR: VMDK_OFFLINE command received
```

```
2020/05/09 01:47:03 (null) WARNING / GENMSG: IBMRBR: VMDK_OFFLINE
command received




+----------------------------------------RESILIENCY-BLOCK-REPLICATOR--------------------------
--------------+

|            |    State/RFD %  |  Local Read | local Write | Net  Actual | Net  Effect |  Entries
| %BAB used|

+- 01:48:37 +-----------------------------------------------------------------------------------------
+

|LG: 003 Stats |    NORMAL    0% |         0 KB|         0 KB|         0 KB|         0 KB|         0|
0|

|/dev/dtc/lg3/dsk/dtc0     0.00% |      0.00 KB|      0.00 KB|      0.00 KB|      0.00 KB|
0|      0.00|

|/dev/dtc/lg3/dsk/dtc1     0.00% |      0.00 KB|      0.00 KB|      0.00 KB|      0.00 KB|
0|      0.00|

|/dev/dtc/lg3/dsk/dtc2     0.00% |      0.00 KB|      0.00 KB|      0.00 KB|      0.00 KB|
0|      0.00|

|/dev/dtc/lg3/dsk/dtc3     0.00% |      0.00 KB|      0.00 KB|      0.00 KB|      0.00 KB|
0|      0.00|

+-----------------------------------------------------------------------------------------------------+

< Quit : [CTRL +C] >
```

Step 3 Update VIB (or uninstall and install VIB) in the ESXi where NICRA is present.

Login to ESXi and copy the latest VIB to it

Verify the version existing in the ESXi by the below command

```
[root@nestedesxi19:~] esxcli software vib list | grep ibmrbr

ibmrbr 3.0.4.16-1OEM.650.0.0.4598673  IBM CommunitySupported  2020-05-09
```

The recommended procedure is to update the VIB using the single command as below.

```
[root@nestedesxi19:/opt] esxcli software vib update --maintenance-mode -v /opt/ibmrbr-3.0.4.16-1OEM.650.0.0.4598673.x86_64.vib

Installation Result

   Message: Operation finished successfully.

   Reboot Required: false

   VIBs Installed: IBM_bootbank_ibmrbr_3.0.4.16-1OEM.650.0.0.4598673

   VIBs Removed: IBM_bootbank_ibmrbr_3.0.4.13-1OEM.650.0.0.4598673

   VIBs Skipped:
```

OR

If encounter any issues, follow 2 step process i.e. remove and install

```
[root@nestedesxi19:~]  esxcli software vib remove -n ibmrbr --maintenance-mode

Removal Result

   Message: Operation finished successfully.

   Reboot Required: false

   VIBs Installed:

   VIBs Removed: IBM_bootbank_ibmrbr_3.0.4.13-1OEM.650.0.0.4598673

   VIBs Skipped:

[root@nestedesxi19:~]
```

```
[root@nestedesxi19:~] esxcli software vib install -v /opt/ibmrbr-3.0.4.16-1OEM.650.0.0.4598673.x86_64.vib   --no-sig-check
```

```
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: IBM_bootbank_ibmrbr_3.0.4.16-1OEM.650.0.0.4598673
   VIBs Removed:
   VIBs Skipped:
[root@nestedesxi19:~]
```

Step 4 Update NICRA and SAUpdate Production NICRA and Staging Appliance.

(This upgrade steps applicable only for nicra RHEL version 8.4)

Step 4.1 Back up the VMDK mapping file.

```
[root@PR_Nicra ~]# dtcresetport -d > /var/opt/IBMRBRdtc/vmdk_mapping_flle_bkp.txt
```

Step 4.2 Move the mobility groups on Nicra to NDU mode.

(Note: We should complete the complete nicra upgrade in <20 mins)

```
[root@PR_Nicra ~]# dtcstartndu
```

//After executing the command, please monitor the file /var/log/messages for the log

```
DTC: [INFO / GENMSG]: STARTNDU completed successfully
```

// Monitor for 5 mins, for the above trace. If you are still unable to see the trace, Please stop the NDU and Re-try the NDU process after ~15 mins.

```
[root@PR_Nicra ~]# dtcstopndu    (Command to stop NDU)
[root@PR_Nicra ~]# dtcstartndu   (Command to re-try start NDU after 15 mins)
```

// dtcstartndu will pause the replication and we will not see any local writes (data) from VIB to Nicra until we finish the upgrade.

After getting the message:- “**STARTNDU completed successfully”, Kindly review the dtcmonitortty command output. We should make sure the groups are in tracking mode and no local writes are happening in any of the groups.**

Once we confirm this we should go ahead and execute the next steps.

Step 4.3 Uninstall old rpm in NICRA

(group stops from normal mode)

```
[root@snapshot-source ~]# rpm -e IBM-Resiliency-Block-Replicator-ADB-3.0.0.0-18651.x86_64
No IBM Resiliency Block Replicator for UNIX* RMD daemons was running.
in.dtc master IBM Resiliency Block Replicator for UNIX* daemon has been shutdown
throtd IBM Resiliency Block Replicator for UNIX* throttle daemon is not running
Stop IBM IBM Resiliency Block Replicator for UNIX* Agent daemons
IBM IBM Resiliency Block Replicator for UNIX* Agent has been shutdown
Moving IBMRBRdtc Config files to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving IBMRBRdtc Shell files to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving IBMRBRdtc License files to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving IBMRBRdtc Product usage statistics files to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving IBMRBRdtc Product usage checksum files to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving the dtc.conf file to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving IBMRBRdtc Agent Config files to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving IBMRBRdtc vmdk_mapping file to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
service IBMRBRdtc-scan does not support chkconfig
Disabling and removing IBMRBRdtc-start.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-start.service.
Disabling and removing IBMRBRdtc-stop.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-stop.service.
Disabling and removing IBMRBRdtc-startdaemons.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-startdaemons.service.
Disabling and removing IBMRBRdtc-startmaster.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-startmaster.service.
Disabling and removing IBMRBRdtc-startpmds.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-startpmds.service.
warning: file /etc/opt/IBMRBRdtc/dtc_pre_failover_pxxx.sh: remove failed: No such file or directory
warning: file /etc/opt/IBMRBRdtc/dtc_post_failover_sxxx.sh: remove failed: No such file or directory
warning: file /etc/opt/IBMRBRdtc/dtc_post_failover_pxxx.sh: remove failed: No such file or directory
```

```
warning: file /etc/opt/IBMRBRdtc/DTC.lic.perm: remove failed: No such file or
directory
Removing IBM Resiliency Block Replicator for UNIX* Symbolic Links from
/usr/local/bin
Removing IBM Resiliency Block Replicator for UNIX* device tree: /dev/dtc
Removing temporary files from /var/opt/IBMRBRdtc
Removing core files from /var/run/IBMRBRdtc
Removing IBM Resiliency Block Replicator for UNIX* master daemon from
/etc/services
Saving current /etc/modprobe.d/ibmrbrdtc.conf to
/etc/modprobe.d/ibmrbrdtc.conf.pre_dtc_remove
Removing IBM Resiliency Block Replicator for UNIX* modifications from
/etc/modprobe.d/ibmrbrdtc.conf
Cleaning up /etc/opt/IBMRBRdtc and /opt/IBMRBRdtc
Cleaning up IBMBR UDEV SUPPORT RULES
[root@snapshot-source ~]#
```

Step 4.4 Install the new rpm in NICRA

```
[root@snapshot-source ~]# rpm -ivh /opt/BAD/RedHat/7x/x86_64/IBM-
Resiliency-Block-Replicator-ADB-3.0.0.0-18656.x86_64.rpm
Preparing...                          ######################################## [100%]
Updating / installing...
   1:IBM-Resiliency-Block-Replicator-A########################################
[100%]
Creating Symbolic Links in /usr/local/bin
Setting up IBMRBR UDEV SUPPORT
 find and create entry of in.dtc in /etc/services
Restore license file and shell script files from past revs
Restoring previously saved IBMRBRdtc license key file.
Restoring previous Agent config file.
Restoring previous vmdk-mapping config file.
Restoring previously saved IBMRBRdtc device list file.
see if Previous IBM Resiliency Block Replicator for UNIX* Installation saves exist
Installing our IBMRBRdtc-start.service and IBMRBRdtc-startdaemons.service
files and enabling them to have our scripts called at boot time
Created symlink from /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-
start.service to /etc/systemd/system/IBMRBRdtc-start.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-
startdaemons.service to /etc/systemd/system/IBMRBRdtc-startdaemons.service.
Installing our IBMRBRdtc-startmaster.service and IBMRBRdtc-startpmds.service
files and enabling them to have our scripts called at boot time
Created symlink from /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-
startmaster.service to /etc/systemd/system/IBMRBRdtc-startmaster.service.
```

```
Created symlink from /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-startpmds.service to /etc/systemd/system/IBMRBRdtc-startpmds.service.
Removing the old IBMRBRdtc-startdaemons links from the /etc/rc.d directories
Installing our IBMRBRdtc-stop.service file and enabling it to have our scripts called at shutdown time
Created symlink from /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-stop.service to /etc/systemd/system/IBMRBRdtc-stop.service.
Starting IBM IBM Resiliency Block Replicator for UNIX* daemons
Launching /opt/IBMRBRdtc/bin/in.dtc
```

Step 4.5 Run "dtcagentset" and retain the config of NICRA

```
[root@snapshot-source ~]# dtcagentset
A previous set of migration group configuration files has been detected on this system.
Would you like to migrate them into the current environment? [y/n]: y
The migration group configuration file is migrated.
Collector connection information.
  IP address       = 192.168.10.44
  Port number      = 576
  AgentIP address  = 192.168.10.170
  BAB size         = 1547 (MB)
  Transmit Interval= 30 sec
  Listener Port    = 15005
```

Step 4.6 Update the backup VMDK mapping file.

Please remove the existing /var/opt/IBMRBRdtc/vmdk_mapping_flle.txt
By using: rm -rf /var/opt/IBMRBRdtc/vmdk_mapping_flle.txt
Then Execute the below command:

```
[root@PR_Nicra ~]# dtcresetport -u /var/opt/IBMRBRdtc/vmdk_mapping_flle_bkp.txt
```

Step 4.7Reboot the NICRA VM

```
[root@snapshot-source ~]# reboot
```

Step 4.8After Nicra reboot:

```
Stop the NDU mode.
[root@PR_Nicra ~]# dtcstopndu
// This command will start the group and resume the replication.
```

Step 4.9 Check /var/log/messages,

and confirm success on STOPNDU. If a failure message is observed then retry dtcstopndu

Step 4.10 Run the python script

after navigating to the directory /etc/opt/IBMRBRdtc/ and run the python script `"./restore_state.py"`
Kindly check the dtcmonitortty output,
At this stage, All the groups should come back to normal and all groups local rights should start.

Steps to be executed for SA - (can be done before the maintenance window also)

Step 5.1 Uninstall old rpm in SA

```
[root@snapshot-source ~]# rpm -e IBM-Resiliency-Block-Replicator-ADB-3.0.0.0-18651.x86_64
No IBM Resiliency Block Replicator for UNIX* RMD daemons were running.
in.dtc master IBM Resiliency Block Replicator for UNIX* daemon has been shutdown
throtd IBM Resiliency Block Replicator for UNIX* throttle daemon is not running
Stop IBM IBM Resiliency Block Replicator for UNIX* Agent daemons
IBM IBM Resiliency Block Replicator for UNIX* Agent has been shutdown
Moving IBMRBRdtc Config files to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving IBMRBRdtc Shell files to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving IBMRBRdtc License files to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving IBMRBRdtc Product usage statistics files to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving IBMRBRdtc Product usage checksum files to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving the dtc.conf file to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving IBMRBRdtc Agent Config files to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
Moving IBMRBRdtc vmdk_mapping file to /var/opt/IBMRBRdtc/IBMRBRdtc3.0.0.0
service IBMRBRdtc-scan does not support chkconfig
Disabling and removing IBMRBRdtc-start.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-start.service.
Disabling and removing IBMRBRdtc-stop.service
```

```
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-
stop.service.
Disabling and removing IBMRBRdtc-startdaemons.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-
startdaemons.service.
Disabling and removing IBMRBRdtc-startmaster.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-
startmaster.service.
Disabling and removing IBMRBRdtc-startpmds.service
Removed symlink /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-
startpmds.service.
warning: file /etc/opt/IBMRBRdtc/dtc_pre_failover_pxxx.sh: remove failed: No
such file or directory
warning: file /etc/opt/IBMRBRdtc/dtc_post_failover_sxxx.sh: remove failed: No
such file or directory
warning: file /etc/opt/IBMRBRdtc/dtc_post_failover_pxxx.sh: remove failed: No
such file or directory
warning: file /etc/opt/IBMRBRdtc/DTC.lic.perm: remove failed: No such file or
directory
Removing IBM Resiliency Block Replicator for UNIX* Symbolic Links from
/usr/local/bin
Removing IBM Resiliency Block Replicator for UNIX* device tree: /dev/dtc
Removing temporary files from /var/opt/IBMRBRdtc
Removing core files from /var/run/IBMRBRdtc
Removing IBM Resiliency Block Replicator for UNIX* master daemon from
/etc/services
Saving current /etc/modprobe.d/ibmrbrdtc.conf to
/etc/modprobe.d/ibmrbrdtc.conf.pre_dtc_remove
Removing IBM Resiliency Block Replicator for UNIX* modifications from
/etc/modprobe.d/ibmrbrdtc.conf
Cleaning up /etc/opt/IBMRBRdtc and /opt/IBMRBRdtc
Cleaning up IBMBR UDEV SUPPORT RULES
[root@snapshot-source ~]#
```

Step 5.2 Install the new rpm in SA

```
[root@snapshot-source ~]# rpm -ivh /opt/BAD/RedHat/7x/x86_64/IBM-
Resiliency-Block-Replicator-ADB-3.0.0.0-18656.x86_64.rpm
Preparing...                          ######################################## [100%]
Updating / installing...
   1:IBM-Resiliency-Block-Replicator-A########################################
[100%]
Creating Symbolic Links in /usr/local/bin
Setting up IBMRBR UDEV SUPPORT
 find and create entry of in.dtc in /etc/services
```

```
Restore license file and shell script files from past revs
Restoring previously saved IBMRBRdtc license key file.
Restoring previous Agent config file.
Restoring previous vmdk-mapping config file.
Restoring previously saved IBMRBRdtc device list file.
see if Previous IBM Resiliency Block Replicator for UNIX* Installation saves exist
Installing our IBMRBRdtc-start.service and IBMRBRdtc-startdaemons.service files and enabling them to have our scripts called at boot time
Created symlink from /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-start.service to /etc/systemd/system/IBMRBRdtc-start.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-startdaemons.service to /etc/systemd/system/IBMRBRdtc-startdaemons.service.
Installing our IBMRBRdtc-startmaster.service and IBMRBRdtc-startpmds.service files and enabling them to have our scripts called at boot time
Created symlink from /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-startmaster.service to /etc/systemd/system/IBMRBRdtc-startmaster.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-startpmds.service to /etc/systemd/system/IBMRBRdtc-startpmds.service.
Removing the old IBMRBRdtc-startdaemons links from the /etc/rc.d directories
Installing our IBMRBRdtc-stop.service file and enabling it to have our scripts called at shutdown time
Created symlink from /etc/systemd/system/multi-user.target.wants/IBMRBRdtc-stop.service to /etc/systemd/system/IBMRBRdtc-stop.service.
Starting IBM IBM Resiliency Block Replicator for UNIX* daemons
Launching /opt/IBMRBRdtc/bin/in.dtc
```

Step 5.3 Run "dtcagent set" and retain the config of SA

```
[root@snapshot-source ~]# dtcagentset
A previous set of migration group configuration file has been detected on this system.
Would you like to migrate them into the current environment? [y/n] : y
The migration group configuration file is migrated.
Collector connection information.
  IP address       = 192.168.10.44
  Port number      = 576
  AgentIP address  = 192.168.10.170
  BAB size         = 1547 (MB)
  Transmit Interval= 30 sec
  Listener Port    = 15005
```

Step 5.4 Reboot the SA VM

```
[root@snapshot-source ~]# reboot
```

Step6 Start group from DMC. (group goes to tracking mode)

Login to DMC VM.

Initially, the groups will be in “Notstarted” mode as below.

```
 DMC>sendmsg 192.168.10.170 statgroup 3
 DateTime: Sat May  9 02:09:00 2020
 Mode: Not Started
 Percentage Done: 0%
 Status: Not Started
 Read: 0.0 KBps
 Write: 0.0 KBps
 Actual Net: 0.0 KBps
 Effective Net: 0.0 KBps
 Entries: 0
 % in BAB: 0
 Current RPO: 00:00:00
Max RPO: 00:00:00
Current RTT: 0 msec
Time Remaining: 00:00:00
Pending MB: 0 MB
```

Start the group required by running the below command.

```
DMC>command group start
```

After starting the group, it goes to “Tracking” mode as below.

```
DMC>sendmsg 192.168.10.170 statgroup 3

DateTime: Sat May  9 02:11:51 2020

Mode: Tracking

Percentage Done: 0%

Status: Accumulate

Read: 0.0 KBps

Write: 0.0 KBps

Actual Net: 0.0 KBps

Effective Net: 0.0 KBps

Entries: 0

% in BAB: 0

Current RPO: 00:00:00

Max RPO: 00:00:00

Current RTT: 0 msec

Time Remaining: 00:00:00

Pending MB: 0 MB
```

Step 7 Resume the PRVMs-

Start the PRVMs in the Vcenter which were paused/stopped in step 1.

The group is in Tracking mode now and the VMDK comes ONLINE as shown below in the “dtcmonitortty” command output of NICRA.

```
2020/05/09 02:11:24 (null) INFO / GENMSG: IBMBR:Initialized NicraAInitServer() bind
on:5000,for Device:64512,LG:3

2020/05/09 02:11:24 (null) INFO / GENMSG: VAIOD: Dispatch Thread Started for LG:3

2020/05/09 02:11:24 (null) INFO / GENMSG: IBMBR:Initialized NicraAInitServer() bind
on:5001,for Device:64520,LG:3

2020/05/09 02:11:24 (null) INFO / GENMSG: IBMBR:Initialized NicraAInitServer() bind
on:5004,for Device:64528,LG:3

2020/05/09 02:11:24 (null) INFO / GENMSG: IBMBR:Initialized NicraAInitServer() bind
on:5005,for Device:64536,LG:3

2020/05/09 02:11:24 /opt/IBMRBRdtc/bin/dtcset INFO / COMMAND:
/opt/IBMRBRdtc/bin/dtcset -g3 CHUNKDELAY=0 CHUNKSIZE=2048
COMPRESSION=OFF JOURNAL=ON NETMAXKBPS=-1 STATINTERVAL=10
MAXSTATFILESIZE=1024 SYNCMODE=OFF

2020/05/09 02:13:54 (null) INFO / GENMSG: IBMRBR: VMDK_ONLINE command
received

2020/05/09 02:13:54 (null) INFO / GENMSG: IBMRBR: VMDK_ONLINE command
received

2020/05/09 02:13:54 (null) INFO / GENMSG: IBMRBR: VMDK_ONLINE command
received

2020/05/09 02:13:54 (null) INFO / GENMSG: IBMRBR: VMDK_ONLINE command
received
```

```
+-------------------------------------- RESILIENCY-BLOCK-REPLICATOR--------------------------
--------------+

|            |    State/RFD %  |  Local Read | local Write | Net  Actual | Net  Effect |  Entries
| %BAB used|

+- 02:14:35 +--------------------------------------------------------------------------------------------------
+
|LG: 003 Stats |  TRACKING    0% |        0 KB|        0 KB|        0 KB|        0 KB|        0|
0|

|/dev/dtc/lg3/dsk/dtc0     0.00% |      0.00 KB|      0.00 KB|      0.00 KB|      0.00 KB|
0|      0.00|

|/dev/dtc/lg3/dsk/dtc1     0.00% |      0.00 KB|      0.00 KB|      0.00 KB|      0.00 KB|
0|      0.00|

|/dev/dtc/lg3/dsk/dtc2     0.00% |      0.00 KB|      0.00 KB|      0.00 KB|      0.00 KB|
0|      0.00|

|/dev/dtc/lg3/dsk/dtc3     0.00% |      0.00 KB|      0.00 KB|      0.00 KB|      0.00 KB|
0|      0.00|

+-----------------------------------------------------------------------------------------------------------+

< Quit : [CTRL +C] >
```

Step 8 Launch smart refresh from DMC

for the relevant groups (group goes to Normal mode from tracking)

From DMC VM, select the group and run the command to start smart refresh:

```
DMC>command group launchrefresh
```

The group goes to Refresh mode now as shown below in the “dtcmonitortty” command output of NICRA.

```
2020/05/09 02:19:03 PMD_003 WARNING / GENMSG: Flushed the queue having 0
bytes of data

2020/05/09 02:19:03 PMD_003 INFO / ESXI_CLIENT_FD: Esxi VMDK's Client FD is
:12

2020/05/09 02:19:03 PMD_003 WARNING / GENMSG: Checking leftover bytes from
previous pmd shutdown for fd 12

2020/05/09 02:19:03 PMD_003 WARNING / GENMSG: Flushed the queue having 0
bytes of data

2020/05/09 02:19:03 PMD_003 INFO / ESXI_CLIENT_FD: Esxi VMDK's Client FD is
:11
```

```
2020/05/09 02:19:03 PMD_003 WARNING / GENMSG: Checking leftover bytes from previous pmd shutdown for fd 11

2020/05/09 02:19:03 PMD_003 WARNING / GENMSG: Flushed the queue having 0 bytes of data

2020/05/09 02:19:03 PMD_003 INFO / ESXI_CLIENT_FD: Esxi VMDK's Client FD is :13

2020/05/09 02:19:03 PMD_003 WARNING / GENMSG: Checking leftover bytes from previous pmd shutdown for fd 13

2020/05/09 02:19:03 PMD_003 WARNING / GENMSG: Flushed the queue having 0 bytes of data




+-------------------------------------- RESILIENCY-BLOCK-REPLICATOR---------------------------------------+

|            |    State/RFD %  |  Local Read | local Write | Net  Actual | Net  Effect |  Entries | %BAB used|

+- 02:19:46 +--------------------------------------------------------------------------------------------+

|LG: 003 Stats |   REFRESH   16% |         0 KB|         0 KB|   34676.7 KB|     45968 KB|          0|          0|

|/dev/dtc/lg3/dsk/dtc0    20.67% |      0.00 KB|      0.00 KB|  11491.69 KB|  11491.20 KB|          0|       0.00|

|/dev/dtc/lg3/dsk/dtc1    20.57% |      0.00 KB|      0.00 KB|  11693.30 KB|  11494.40 KB|          0|       0.00|

|/dev/dtc/lg3/dsk/dtc2    20.57% |      0.00 KB|      0.00 KB|  11491.69 KB|  11491.20 KB|          0|       0.00|

|/dev/dtc/lg3/dsk/dtc3     2.67% |      0.00 KB|      0.00 KB|      0.00 KB|  11491.20 KB|          0|       0.00|

+----------------------------------------------------------------------------------------------------+
< Quit : [CTRL +C] >
```

This completes the procedure of upgrading the VIB, NICRA, and SA without full Refresh/CBT

Note: We can observe that the Refresh operation gets completed in a few mins itself as It is not a full refresh and there would not be any 2nd phase of Refresh.

```
2020/05/09 02:19:03 PMD_003 WARNING / GENMSG: Checking leftover bytes from previous pmd shutdown for fd 12

2020/05/09 02:19:03 PMD_003 WARNING / GENMSG: Flushed the queue having 0 bytes of data

2020/05/09 02:19:03 PMD_003 INFO / ESXI_CLIENT_FD: Esxi VMDK's Client FD is :11

2020/05/09 02:19:03 PMD_003 WARNING / GENMSG: Checking leftover bytes from previous pmd shutdown for fd 11

2020/05/09 02:19:03 PMD_003 WARNING / GENMSG: Flushed the queue having 0 bytes of data

2020/05/09 02:19:03 PMD_003 INFO / ESXI_CLIENT_FD: Esxi VMDK's Client FD is :13

2020/05/09 02:19:03 PMD_003 WARNING / GENMSG: Checking leftover bytes from previous pmd shutdown for fd 13

2020/05/09 02:19:03 PMD_003 WARNING / GENMSG: Flushed the queue having 0 bytes of data

2020/05/09 02:23:34 PMD_003 INFO / RFDEND: Refresh operation completed for group PMD_003

2020/05/09 02:23:37 PMD_003 INFO / PMDSTART: PMD (Primary Mirror Daemon) started PMD_003
```

```
+-------------------------------------- RESILIENCY-BLOCK-REPLICATOR--------------------------
--------------+

|           |    State/RFD %  |  Local Read | local Write | Net  Actual | Net  Effect |  Entries
| %BAB used|

+- 02:23:36 +----------------------------------------------------------------------------------------
+

|LG: 003 Stats |    NORMAL    0% |        0 KB|        0 KB|        0 KB|        0 KB|        0|
0|

|/dev/dtc/lg3/dsk/dtc0     0.00% |      0.00 KB|      0.00 KB|      0.00 KB|      0.00 KB|
0|      0.00|

|/dev/dtc/lg3/dsk/dtc1     0.00% |      0.00 KB|      0.00 KB|      0.00 KB|      0.00 KB|
0|      0.00|

|/dev/dtc/lg3/dsk/dtc2     0.00% |      0.00 KB|      0.00 KB|      0.00 KB|      0.00 KB|
0|      0.00|

|/dev/dtc/lg3/dsk/dtc3     0.00% |      0.00 KB|      0.00 KB|      0.00 KB|      0.00 KB|
0|      0.00|

+----------------------------------------------------------------------------------------------------+

< Quit : [CTRL +C] >
```

2.8 Upgrading to the latest version of the RO Anomaly Detection tool

Perform the following steps to deploy the new images manually and bring the containers up. This is instead of running the installer.

On the Scanner VM:

1. Login to the scanner VM by using SSH and switch to the root prompt.
2. Create two directories under the $INSTALL_DIR.
   Here, $INSTALL_DIR is /opt/panaces-sally, replace $INSTALL_DIR with the correct installation path.

```
# mkdir -p $INSTALL_DIR/scanner_oct2023
$INSTALL_DIR/scanner/custom
```

Note: Edit the file, skip_file_extns_master_list.py to skip the files that have specific extensions during the scanning and add the file extensions to be skipped during scanning against the VM UUID. Otherwise, this step is optional.

3. Copy the skip_file_extns_master_list.py file into the $INSTALL_DIR/scanner/custom folder.
4. Change the ownership of the folder $INSTALL_DIR/scanner/custom by using the following command:
   ```
   # chown -R 2002:2002 $INSTALL_DIR/scanner/custom
   ```
5. Copy the scanner_oct2023.tar into the folder $INSTALL_DIR/scanner_oct2023.
6. Load the docker image from scanner_oct2023.tar by using the following command.
   ```
   # docker load <
   $INSTALL_DIR/scanner_oct2023/scanner_oct2023.tar
   ```
   Note: New docker image scanner:oct2023 is created in the output of the command: "docker images"
7. Execute the following command to start the new container using a new image:
   ```
   # docker run --name scanner_new_oct2023_1 -u sally:sally --
   tmpfs "/tmp" -d --mount
   type=bind,src=/dev,dst=/scan/dev,readonly=true,bind-
   propagation=shared --mount
   type=bind,src=/monitor,dst=/scan/snapshots,readonly=true,bi
   nd-propagation=shared --mount
   type=bind,src=$INSTALL_DIR/scanner/config1,dst=/scanner/con
   fig --mount
   type=bind,src=$INSTALL_DIR/scanner/custom,dst=/scanner/Scan
   ner/custom --security-opt=no-new-privileges --cpu-
   shares=1024 --network host -e PYTHONUNBUFFERED='1' --pids-
   limit 100 --cpus="2" --memory=3g -e PYTHONUNBUFFERED='1' --
   restart=on-failure:5 scanner:oct2023
   ```

   If there is more than one existing scanner container, then execute the above command by changing the container name and configuration path.
   For example:
   ```
   # docker run --name scanner_new_oct2023_2 -u sally:sally --
   tmpfs "/tmp" -d --mount
   type=bind,src=/dev,dst=/scan/dev,readonly=true,bind-
   propagation=shared --mount
   type=bind,src=/monitor,dst=/scan/snapshots,readonly=true,bi
   nd-propagation=shared --mount
   type=bind,src=$INSTALL_DIR/scanner/config2,dst=/scanner/con
   fig --mount
   ```

```
type=bind,src=$INSTALL_DIR/scanner/custom,dst=/scanner/Scan
ner/custom --security-opt=no-new-privileges --cpu-
shares=1024 --network host -e PYTHONUNBUFFERED='1' --pids-
limit 100 --cpus="2" --memory=3g -e PYTHONUNBUFFERED='1' --
restart=on-failure:5 scanner:oct2023
```

8. Remove the old scanner containers by using the following command:
   ```
   docker rm -f <old container name1> <old container name2>
   ```
   For example:
   ```
   # docker rm -f scanner1 scanner2
   ```

On the Analysis VM:

1. Login to the Analysis VM by using SSH and switch to the root prompt.
2. Create a directory under the $INSTALL_DIR.
   Here, $INSTALL_DIR is /opt/panaces-sally, replace $INSTALL_DIR with the correct installation path.
   ```
   # mkdir -p $INSTALL_DIR/analysis_oct2023
   ```
3. Copy the fe_supervised_oct2023.tar and model_supervised_oct2023.tar into the $INSTALL_DIR/analysis_oct2023 folder.
4. Load the new docker images by using the following command.
   ```
   # docker load <
   $INSTALL_DIR/analysis_oct2023/model_supervised_oct2023.tar
   # docker load <
   $INSTALL_DIR/analysis_oct2023/fe_supervised_oct2023.tar
   ```
   Note: New docker images are created in the output of the command: "docker images"
5. Execute the following command to start the new containers using the new images:
   ```
   # docker run -d --name fe_supervised_oct2023 -v
   $INSTALL_DIR/analysis/fe_supervised/config:/sally-
   supervised-fe/config --cpus="1.0" --cpu-shares=1024 --
   memory=5g -u sally:sally --network host -e
   PYTHONUNBUFFERED='1' --restart=on-failure:5 --tmpfs "/tmp"
   --pids-limit 100 --security-opt=no-new-privileges
   fe_supervised:oct2023

   # docker run -d --name model_supervised_oct2023 -v
   $INSTALL_DIR/analysis/model_supervised/config:/model_superv
   ised/config --cpus="1.0" --cpu-shares=1024 --memory=5g -u
   sally:sally --network host -e PYTHONUNBUFFERED='1' --
   restart=on-failure:5 --tmpfs "/tmp" --pids-limit 100 --
   security-opt=no-new-privileges model_supervised:oct2023
   ```
6. Remove the old scanner containers by using the following command:
   ```
   docker rm -f <old fe supervised container name> <old model
   supervised container name>
   ```

For example:

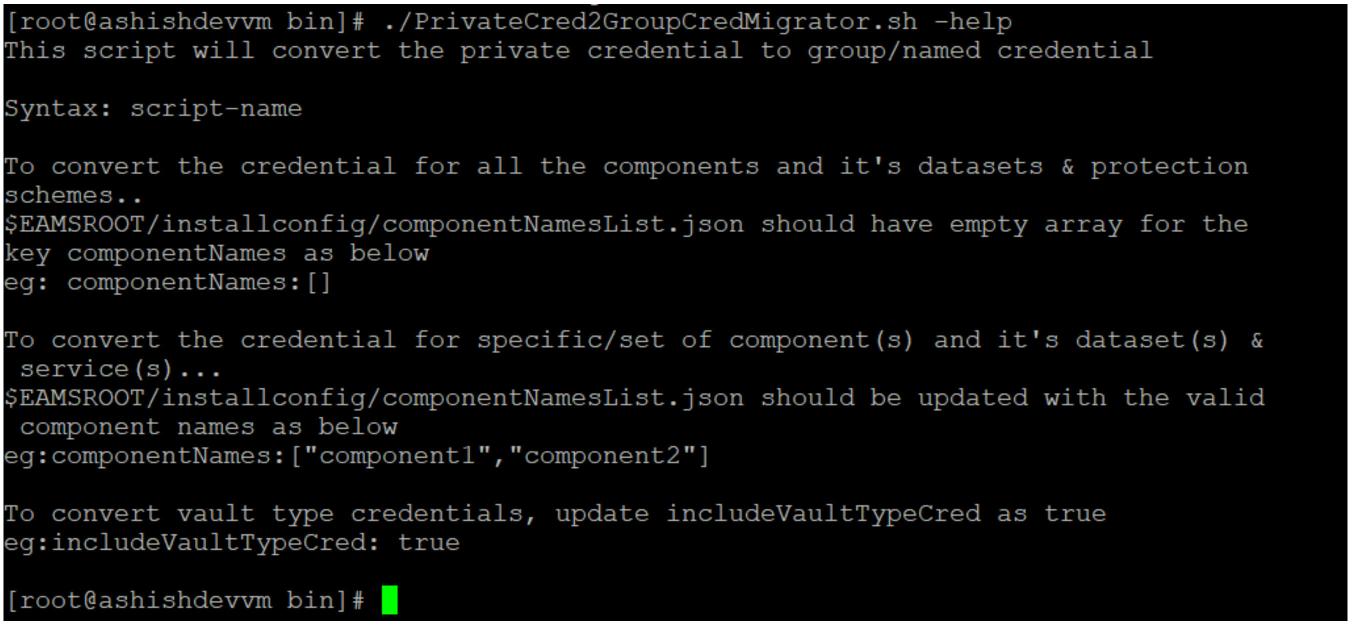
```
# docker rm -f fe_supervised model_supervised
```

2.9 Upgrade script

2.9.1 Script upgrade to support Dataset & Protection schema

Subsystem cred to Private Group cred script upgrade is supported for Dataset (Oracle, MSSQL), PS (DataGuard). Component, Dataset, and protection Schema for nearly all solutions.

For Zerto and VSphere Management service is supported.



```
[root@ashishdevvm bin]# ./PrivateCred2GroupCredMigrator.sh -help
This script will convert the private credential to group/named credential

Syntax: script-name

To convert the credential for all the components and it's datasets & protection
schemes..
$EAMSROOT/installconfig/componentNamesList.json should have empty array for the
key componentNames as below
eg: componentNames:[]

To convert the credential for specific/set of component(s) and it's dataset(s) &
 service(s)...
$EAMSROOT/installconfig/componentNamesList.json should be updated with the valid
 component names as below
eg:componentNames:["component1","component2"]

To convert vault type credentials, update includeVaultTypeCred as true
eg:includeVaultTypeCred: true

[root@ashishdevvm bin]# 
```

[root@ashishdevvm bin]# ./PrivateCred2GroupCredMigrator.sh -help

This script will convert the private credential to a group/named credential

Syntax: script-name

To convert the credential for all the components and its datasets & protection schemes. EAMSROOT/installconfig/componentNamesList.json should have an empty array for the key componentNames as below
eg: componentNames:[]

To convert the credential for a specific/set of component(s) and its dataset(s) & service(s)...
EAMSROOT/installconfig/componentNamesList.json should be updated with the valid component names as below
eg:componentNames:["component1", "component2"]

To convert vault type credentials, update includeVaultTypeCred as true
eg:includeVaultTypeCred: true

2.9.2 AgentCredentialMigration.sh script details

AgentCredentialMigration.sh script is available from RO 8.4.0.0:

This script migrates the Agent Credentials to Group cred (Named Cred). Group cred name has the syntax agent host IP underscore agent id (example 192.x.x.78_107).

Pre-requisites:

1. This script is only applicable for MYSQL and PostgreSQL dataset types.
2. This script has to be executed after a successful RO Upgrade from 8.x.x.x to the latest version.
3. You need to have MySQL, and PostgreSQL dataset discovered in the previous version - else this script will not be applicable for your setup.

Execution Steps:

1. Post successful upgrade to the latest version, go to $EAMSROOT/bin/
2. Execute the following script:

```
sh AgentCredentialMigration.sh
```

3. The logs will be generated at $EAMSROOT/var/log/AgentCredentialMigration.log

2.10 Post upgrade

2.10.1 Prerequisite

Ensure the following prerequisites are met.

- For activeMQ logs to update, post-upgrade, RO and SC should be restarted.

- Note: MUST INSTALL PATCH list. After upgrade or after fresh install contact the SUPPORT team to determine MANDATORY patch's for your setup. This list depends on your PR/DR environment, this has to be obtained from the support team for successful completion of your setup.
- Kyndryl recommends using the same version of Site Controller and Kyndryl Resiliency Orchestration before you proceed with the post-installation steps. Ensure the Site Controller and Kyndryl Resiliency Orchestration are of the same version before you proceed with post-installation steps. For instructions to install Site Controller, refer to sections "Installing Agent Node Server or Site Controller on Linux" or "Installing Agent Node Server or Site Controller in MS Windows" in the Kyndryl Resiliency Orchestration Installation Guide.

  The component that you are going to migrate should be in CIDR range of the Site controller and Site of the Component should be the same.

  Kyndryl supports backward compatibility with two major versions of the agent.

2.10.1.2 Manual steps for post-upgrade

Execute the following steps:

1. Login to RO database using the below command:

```
mysql -u<UserName> -p<Password>
```

2. Execute the following commands:

use panaces;

--To Insert Directory_Server Create & Delete Feature and associate it to Admin

and SuperAdmin.

```
INSERT INTO feature_matrix(fm_package_module, fm_pm_licensable,
fm_feature, fm_feature_licensable, fm_operation,
fm_operation_type, fm_operation_key, fm_operation_auditable,
fm_operation_severity) SELECT
"ADMIN","FALSE","Directory_Server","FALSE","DELETE","CONFIG_DEL","
admin.delete","TRUE","INFO" FROM DUAL WHERE NOT EXISTS ( SELECT
fm_id FROM feature_matrix WHERE fm_feature='Directory_Server' AND
fm_operation='DELETE');

INSERT INTO feature_matrix(fm_package_module, fm_pm_licensable,
fm_feature, fm_feature_licensable, fm_operation,
fm_operation_type, fm_operation_key, fm_operation_auditable,
fm_operation_severity)
```

```
SELECT
"ADMIN","FALSE","Directory_Server","FALSE","CREATE","CONFIG_ADD","
admin.create","TRUE","INFO" FROM DUAL WHERE NOT EXISTS ( SELECT
fm_id FROM feature_matrix WHERE fm_feature='Directory_Server' AND
fm_operation='CREATE');

INSERT INTO category_feature_mapping(cfm_uc_id, cfm_fm_id)

SELECT * FROM (SELECT uc_id,fm_id FROM user_categories,
feature_matrix WHERE (uc_type = "ADMINISTRATOR") AND
(fm_feature='Directory_Server' AND fm_operation IN
('CREATE','DELETE'))) AS tmp

WHERE NOT exists (SELECT cfm_uc_id FROM category_feature_mapping
JOIN user_categories on uc_id=cfm_uc_id JOIN feature_matrix on
fm_id=cfm_fm_id WHERE (uc_type = "ADMINISTRATOR") AND
(fm_feature='Directory_Server' AND fm_operation IN
('CREATE','DELETE')) );

INSERT INTO category_feature_mapping(cfm_uc_id, cfm_fm_id)

SELECT * FROM (SELECT uc_id,fm_id FROM user_categories,
feature_matrix WHERE (uc_type = "SUPER ADMINISTRATOR") AND
(fm_feature='Directory_Server' AND fm_operation IN
('CREATE','DELETE'))) AS tmp

WHERE NOT exists (SELECT cfm_uc_id FROM category_feature_mapping
JOIN user_categories on uc_id=cfm_uc_id JOIN feature_matrix on
fm_id=cfm_fm_id WHERE (uc_type = "SUPER ADMINISTRATOR") AND
(fm_feature='Directory_Server' AND fm_operation IN
('CREATE','DELETE')) );
```

2.10.2 Schema Validation

Post-upgrade, use the following script to verify if the upgraded schema is correct or not. If any differences are found they need to be corrected before proceeding to the next step.

Path: /opt/panaceas/bin

Script: `SchemaValidator.sh`

SchemaValidator.sh script needs 3 arguments and those 3 are as follows:

```
# $EAMSROOT/bin/SchemaValidator.sh
```

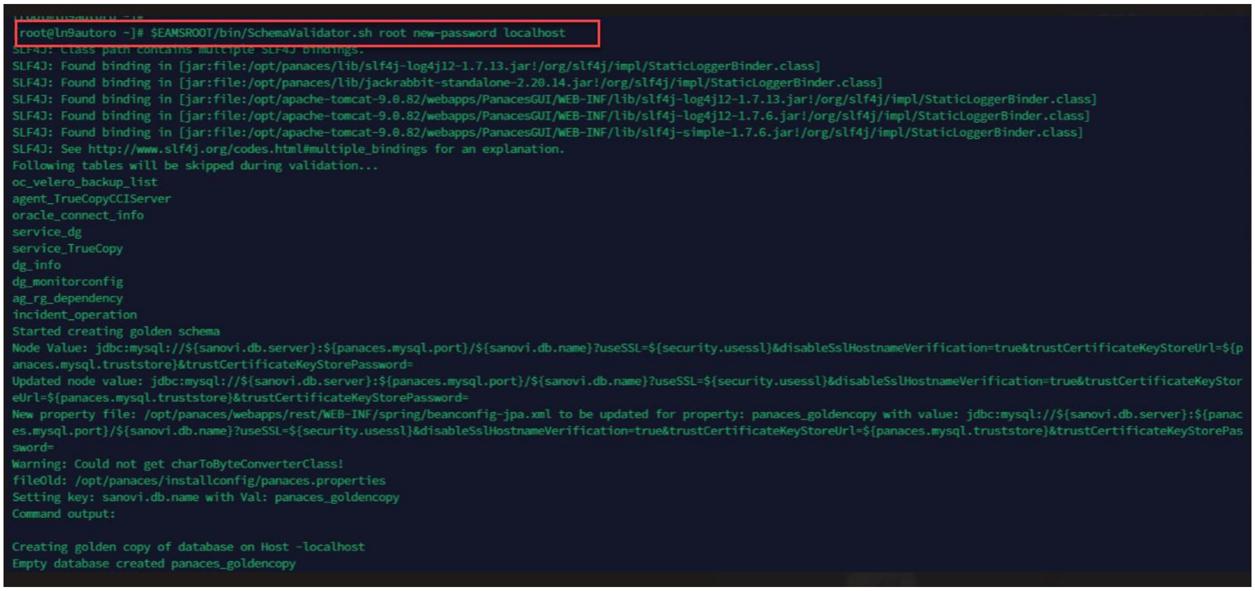
***************Script Usages**********************

SchemaValidator.sh <DB User> <DB Password> <Host where DB is present>

Sample usage example:

```
#$EAMSROOT/bin/SchemaValidator.sh root <rootdb password> localhost
```

Note: Please use "localhost" as last argument. Please DONOT use IP or hostname.



```
root@ln9autoro ~]# $EAMSROOT/bin/SchemaValidator.sh root new-password localhost
SLF4J: Class path contains multiple SLF4J bindings.
SLF4J: Found binding in [jar:file:/opt/panaces/lib/slf4j-log4j12-1.7.13.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/opt/panaces/lib/jackrabbit-standalone-2.20.14.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/opt/apache-tomcat-9.0.82/webapps/PanacesGUI/WEB-INF/lib/slf4j-log4j12-1.7.13.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/opt/apache-tomcat-9.0.82/webapps/PanacesGUI/WEB-INF/lib/slf4j-log4j12-1.7.6.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/opt/apache-tomcat-9.0.82/webapps/PanacesGUI/WEB-INF/lib/slf4j-simple-1.7.6.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
Following tables will be skipped during validation...
oc_velero_backup_list
agent_TrueCopyCCIServer
oracle_connect_info
service_dg
service_TrueCopy
dg_info
dg_monitorconfig
ag_rg_dependency
incident_operation
Started creating golden schema
Node Value: jdbc:mysql://${sanovi.db.server}:${panaces.mysql.port}/${sanovi.db.name}?useSSL=${security.usessl}&disableSslHostnameVerification=true&trustCertificateKeyStoreUrl=${p
anaces.mysql.truststore}&trustCertificateKeyStorePassword=
Updated node value: jdbc:mysql://${sanovi.db.server}:${panaces.mysql.port}/${sanovi.db.name}?useSSL=${security.usessl}&disableSslHostnameVerification=true&trustCertificateKeyStor
eUrl=${panaces.mysql.truststore}&trustCertificateKeyStorePassword=
New property file: /opt/panaces/webapps/rest/WEB-INF/spring/beanconfig-jpa.xml to be updated for property: panaces_goldencopy with value: jdbc:mysql://${sanovi.db.server}:${panac
es.mysql.port}/${sanovi.db.name}?useSSL=${security.usessl}&disableSslHostnameVerification=true&trustCertificateKeyStoreUrl=${panaces.mysql.truststore}&trustCertificateKeyStorePas
sword=
Warning: Could not get charToByteConverterClass!
fileOld: /opt/panaces/installconfig/panaces.properties
Setting key: sanovi.db.name with Val: panaces_goldencopy
Command output:

Creating golden copy of database on Host -localhost
Empty database created panaces_goldencopy
```

2.10.2.1 Sample Report

```
Comparing TABLES(**=golden copy)...........

TABLES matched during comparison: 865

Additional TABLES found in Upgraded Version:

==============================================

No Record Found


TABLES:Missing in Upgraded Version.

===========================================

    BCSSybaseLogPFR_BCOConfig_action

    BCSInformixLogPFR_BCOConfig_action
```

```
TABLES Stats

=================

TABLES in golden copy:                      868

TABLES in upgraded version:                 872

TABLES matched during comparison:           865

TABLES found different during comparison:   0

Additional TABLES found in Upgraded Version: 0

TABLES excluded during comparison:          8 (tables that get
generated after panaces restart, hence ignoring for now. 7 from
Upgraded version & 1 from Golden copy)

Effective TABLES counts for comparison:    865


 Action to be taken by admin/user

===================================

Please refer to post_upgrade_actions.log

This log file will contain queries to create missing artifacts

===================================

Execution Time= 9 minutes

Reverting changes to panaces.properties file.

fileOld: /opt/panaces/installconfig/panaces.properties

Setting key: sanovi.db.name with Val: panaces

Reverting changes to JPA xml file.

Node Value:
jdbc:mysql://${sanovi.db.server}:${panaces.mysql.port}/${sanovi.
db.name}?useSSL=${security.usessl}&disableSslHostnameVerificatio
n=true&trustCertificateKeyStoreUrl=${panaces.mysql.truststore}&t
rustCertificateKeyStorePassword=

Updated node value:
jdbc:mysql://${sanovi.db.server}:${panaces.mysql.port}/${sanovi.
db.name}?useSSL=${security.usessl}&disableSslHostnameVerificatio
n=true&trustCertificateKeyStoreUrl=${panaces.mysql.truststore}&t
rustCertificateKeyStorePassword=
New property file: /opt/panaces/webapps/rest/WEB-
INF/spring/beanconfig-jpa.xml to be updated for property:
panaces with value:
jdbc:mysql://${sanovi.db.server}:${panaces.mysql.port}/${sanovi.
db.name}?useSSL=${security.usessl}&disableSslHostnameVerificatio
n=true&trustCertificateKeyStoreUrl=${panaces.mysql.truststore}&t
rustCertificateKeyStorePassword=

Dropping Golden Database

Database dropped

Command output:

Cleaning Up

The script got executed successfully.
```

2.10.2.2 Post upgrade procedures

Post Upgrade validation for ALTER privilege
Login to mariadb

```
mysql -uroot -p mysql
show grant for 'panaces'@'localhost' ;
```

Validate that, If the ALTER privilege is not listed for 'panaces'@'localhost', then run the following command

```
grant SELECT, INSERT, UPDATE, DELETE, DROP, CREATE, EXECUTE,
ALTER, SHOW VIEW ON panaces.* to 'panaces'@'localhost' ;
```

Perform the following post-upgrade procedures.

1. After the successful upgrade of the Kyndryl Resiliency Orchestration application,
    a. Delete the PanacesServerInstaller.properties file from the downloaded locations.
    b. If you are not able to access the ${EAMSROOT}/bin, log out from the current SSH session, and Log in again to access it.
    c. Before starting the panaces server, ensure to delete the installer-related files in the /tmp path.

Example:

```
rm -rf /tmp/*
rm -rf /tmp/*.data
```

Note: Update the JVM settings as applicable to the customer environment, as the upgrade will set the default as 2048m.

2. Determine if you want to install the Site Controller if you have not done so in an earlier upgrade. For installation instructions, refer to the Kyndryl Resiliency Orchestration Installation Guide under the sections “Installing Agent Node Server or Site Controller on Linux” or” Installing Agent Node Server or Site Controller in MS Windows”, for respective operating systems.
3. If you are planning to install the Site Controller, ensure that you first open Port 42443 on the Kyndryl Resiliency Orchestration Server for the ActiveMQ Broker feature. Additionally, open the 45443 port for the Site Controller component for bidirectional connectivity to the Resiliency Orchestration Server.
4. If you want to use the ActiveMQ Broker feature, you should perform the procedures provided in the Kyndryl Resiliency Orchestration Installation Guide section “Configuring Resiliency Orchestration Server and Site Controller for Secured Communication by Using the ActiveMQ Broker.”
5. Apply Third-party Jars for the Vault and Cisco UCS Director features as applicable.

   Note: Follow Step 2 to Step 5 to apply Third-Party dependencies and Step 6 to Step 7 for the list of Third-Party JS Library files in the section **Post Installation steps for Kyndryl Resiliency Orchestration** in the latest *Kyndryl Resiliency Orchestration Installation guide*.
6. After upgrading to the latest version ensure to run the following script to use the RPD plugins, –

   a. `UpdateRPDPlugins.sh in $EAMSROOT/bin`

      i. **Note** – This script needs to be executed only after the upgrade and not in case of fresh installations.
7. The Server is by default enabled with TLS 1.2 security. To achieve backward compatibility to support older agents, open $EAMSROOT/installconfig/panaces.properties and set `panaces.acp.communicationType = SECURE`

8. If you are planning to enable two-way TLS, please refer to the section Enabling two-way TLSv1.2 authentication in the Kyndryl Resiliency Orchestration Installation Guide.

9. After the upgrade, the default TrustStore and KeyStore passwords should be changed and encrypted. Refer to sections ***Encrypting the custom store password*** and ***Encrypting the custom store passwords for ActiveMQ*** in the Kyndryl Resiliency Orchestration Installation Guide for the encryption procedure.

10. If using a custom MariaDB SSL certificate, the custom path should be updated in /etc/my.cnf and $EAMSROOT/installconfig/panaces.properties files. For the procedure, refer to section 4.5.3 Security Configuration in the Kyndryl Resiliency Orchestration Installation guide.

    Note: Check if mariadb certificate files

    1.ca-cert.pem

    2. server-cert.pem

    3. server-key.pem

    All three are present in "$EAMSROOT/installconfig/mariadbencryption" directory.

    if not present a SSL connection error will come in logs.

    Resolution is

    Copy below 3 files from RO backup folder to "$EAMSROOT/installconfig/mariadbencryption".

    1.$EAMSROOT/installconfig/mariadbencryption/ca-cert.pem

    2.$EAMSROOT/installconfig/mariadbencryption/server-cert.pem

    3.$EAMSROOT/installconfig/mariadbencryption/server-key.pem

11. For the Mimix solution, post-upgrade, to support the SSL mode of communication, make sure to copy the truststore.ks file which gets created while enabling SSL mode to $EAMSROOT/installconfig folder. For the procedure to generate truststore.ks file, refer to the section “Enable SSL Communication” in the IBM iSeries with Mimix Replication solution guide.

12. Run the following script:

    ```
    i.  sudo $EAMSROOT/bin/SecurityUserInjection.sh
    ```

13. Start Resiliency Orchestration Services, and run the following command to perform this task.

```
i.  sudo $EAMSROOT/bin/panaces start
```

14. Verify that the console log shows panaces services have started successfully, run the following command to perform this task.

```
i.  tail -f  $EAMROOT/var/log/console.log
```

15. For upgrading the Agent using low touch upgrade in GUI mode, please refer to the topic Upgrading Agent topic in the Kyndryl Resiliency Orchestration Admin Guide or refer to the online help path Home > Discovery > Subsystem > Agent Upgrade > Agent Upgrade.

    i. For manual upgrade using console mode, please refer to the section Upgrading Resiliency Orchestration Agents in the Kyndryl Resiliency Orchestration Installation Guide.

16. Post upgrade, if there is any workflow with a Listing Action, for example by the name 'action.VerifyApplication.name', edit the workflow, rename the Listing Action to 'Verify Application', save and publish the workflow. The name should then reflect as 'Verify Application'.

    Execute the following 3 steps

    a. Login to mariadb
    b. Execute "use panaces
    c. Execute this query:

    "ALTER TABLE DmcNicrMapping ADD COLUMN

    IF NOT EXISTS natip varchar (255) DEFAULT 'NA';"

17. Please note that the Upgrade script makes a copy of the existing installation folder $EAMSROOT by renaming it as $EAMSROOT_<*OlderVersion*>_<b*uid_revision_No*>, before the upgrade to a new version.

    For example –

    If 8.1.3 is already installed in /opt/panaces, the folder will be renamed to /opt/panaces_8.1_82cace9 which contains the old installation, and the latest version binaries will be installed in /opt/panaces.
    Once the upgrade is complete, make sure to set the specific values of certain properties as per your requirement by referring to the backup version of the properties under $EAMSROOT_<*OlderVersion*>_<*build_revision_No*>.

    Refer to the backup folder for any custom scripts and certificates and apply the same changes after the upgrade.

Example –
/opt/panaces/remote/<IP address>/installconfig/PanacesAgentGeneric.cfg file comes with a default value for property panaces.netapp.communication.type=HTTP

You may need to set it to panaces.netapp.communication.type=HTTPS, if that is your environment's requirement.

For the post-upgrade steps of CR Platform solution, refer to the **Post Upgrade Steps for CR Platform** section in the *Cyber Incident Recovery for Platform User Guide*

18. Post upgrade steps for Cyber Data

    a. For the new Anomaly detection feature of the Cyber data solution, execute the following commands in the same sequence for the feature's events (AnomalyScanClean and AnomalyScanNotClean) and policies to be registered
    for the existing CyberResiliency solution groups –

```
./$EAMSROOT/bin/importDefinitionForTemplate.sh -u -e
$EAMSROOT/templates/typedef/Actifio/BCS-CyberResiliency-
Actifio-CyberAnomalyDetection-events.xml
./$EAMSROOT/bin/AddSignature.sh
./$EAMSROOT/bin/RegisterPoliciesForExistingGroups.sh
$EAMSROOT/templates/typedef/Actifio/BCS-CyberResiliency-
Events-Policy-Association.xml
```

    Note: Make sure the Cyber Resiliency plugin should have registered before running these scripts.
    Restart Panaces Server and recreate a new group

19. Post Upgrade Steps for MariaDB Table Update

    a. Log in to MariaDB as a root user.

    b. Execute the following command for the panaces db.

        i. `use panaces`

    c. Execute this query:

        i.

```
ALTER TABLE DmcNicrMapping ADD COLUMN IF NOT EXISTS
natip varchar(255) DEFAULT 'NA' ;
 ALTER TABLE DmcNicrMapping ADD COLUMN IF NOT EXISTS
isNATSupported bit(1) DEFAULT 'false';
```

20. After you complete the upgrade process, move the Installation logs from the tmp folder to a different location and then clean up the tmp folder again before starting the panaces services, so that you can take a backup of upgrade log files for your future reference.

Example:

```
mv  /tmp/Installation_Log   /home/
cd /tmp
rm -rf *
```

21. In panaces.properties check the values of

1. `panaces.acp.server.concurrentRequestProcessCount`
2. `panaces.acp.server.concurrentRequestProcessCountMax`

   This concurrentRequestProcessCountMax property should be equal to or greater than concurrentRequestProcessCount.

22. Post-upgrade steps to be followed in case of Vault configuration:

    Follow the below steps to mark any connection parameter as sensitive.

```
Step 1)Update the below files,
$EAMSROOT/agents/vault/{vaultType}/config/{vaultType}_config.xml ,
$EAMSROOT/agents/vault/{vaultType}/config/{vaultType}_config_en.xml ,
$EAMSROOT/agents/vault/{vaultType}/config/{vaultType}_config_ja.xml

Use xml element for each connection parameter which is sensitive data.

<Sensitive> true </Sensitive>

Example:

<ConnectionParameter>

            <Parameter>

                 <Name> Application ID</Name>

                 <UniqueId>CYBERARK_APPLICATION_ID</UniqueId>

                 <Description>CyberArk Application ID</Description>

                 <Type>Integer</Type> <!-- Number/Text -->

                                  <Sensitive> true </Sensitive>

            </Parameter>
```

Step 2) **Copy the jar file(javapasswordsdk.jar) to each of the 4 RO directories listed below.**

1. **$EAMSROOT/lib**
2. **$EAMSROOT/agents/vault/CyberArk/lib**
3. **$TOMCAT_HOME/webapps/PanacesGUI/WEB-INF/lib/**
4. **$TOMCAT_HOME/webapps/PanacesGUI/pages/classes/lib/**

step 3) Execute query once for each sensitive= true parameter.

```
UPDATE vault_connection_parameter SET vcp_sensitive=1 where
vcp_uniqueId={UniqueId};
UniqueId can be found in the {vaultType}_config.xml
```

Example:

```
    UPDATE vault_connection_parameter SET vcp_sensitive=1 where
    vcp_uniqueId= '’CYBERARK_APPLICATION_ID’' ;
```

2.9.2.2 RO users'('panacesuser' & 'tomcatuser') password policies and password length configuration

From release 8.4.0.0 onwards, for both fresh installation and upgrade, the OS users 'panacesuser' and 'tomcatuser’ have a password set capability. The password policies can be adopted based on the organization’s technical specifications/security standards.

2.10.3 Post Upgrade Steps for NICRA based RBR Solution

Prerequisite: RBR Solution Groups are already created in the previous version of CRO

After the successful upgrade of CRO to the latest version (8. x to the latest version):

Please follow these Post upgrade steps to reconfigure workflows

1. Login to CRO (Using SSH)
2. Execute the following commands

```
a) sh $EAMSROOT/bin/RBRWorkflowImportUtility.shPreFailoverTestExercise

b) sh $EAMSROOT/bin/RBRWorkflowImportUtility.shPostFailoverTestExercise

c) sh $EAMSROOT/bin/RBRWorkflowImportUtility.sh SwitchOver
```

```
d) sh $EAMSROOT/bin/RBRWorkflowImportUtility.sh SwitchBack
e) sh $EAMSROOT/bin/RBRWorkflowImportUtility.sh StorageVMotion
f) sh $EAMSROOT/bin/RBRWorkflowImportUtility.sh VirtualDiskExpansion
g) sh $EAMSROOT/bin/RBRWorkflowImportUtility.shFailoverTestExercisePrecheck
```

h) **ReName from IBM to Resiliency support from 8.4.3 CRO version**
Post upgrade execute below script to reflect Rebranding Name in CRO UI pages

```
i) sh $EAMSROOT/bin/update_rbr_group_description.sh <dbuserName> <dbPassword>
```

j) Verify the `$EAMSROOT/installconfig/panaces.properties` check the below key and add the "BCSVMReplication"

Example `panaces.compStateChange.flag.enable.list=BCSStatelessApp,BCSVMReplication`

3. Verify the above workflows are imported on all RBR RGs
4. Associate SPBM resource Mapping Policy to existing RGs
   a) Create Test Drill workflow and import AddResourceMappings.xml
   From below Path AddResourceMappings.xml - download to local.
   $EAMSROOT/scripts/VMProtection/VMwareIBMBR/UpdateResourceMapping

   b) Login to RO and configure VmProfileAdd.csv and copy to /tmp
   E.g

```
VmName,ComponentType,Purpose,ProfileName
 rhel_172.16.5.1,Policy,Drill,ResiliencyBlockreplicatorPolicy
 rhel_172.16.5.1,Policy,Recovery,ResiliencyBlockreplicatorPolicy
```

5. Run the Test Drill Workflow
6. Upgrade to RO 8.3.4 onwards BP workflow is available for newly created RG(not for AG). For the pre-existing RG execute the below script

```
sh $EAMSROOT/bin/RBRWorkflowImportUtility.sh StartChecksumRefresh
```

7. Rebranding Name from IBM to Resiliency support from 8.4.3 CRO version
   Post upgrade execute below script to reflect Rebranding Name in CRO UI pages

```
sh $EAMSROOT/bin/update_rbr_group_description.sh <dbuserName>
 <dbPassword>
```

Then verify the existing RBR group details page.

8. **If and only if you are upgrading from any version of RO older than 8.4.3.0** than you need to execute the below steps. From 8.4.3.0 onwards these steps are not required.
   After upgrade download the following workflows as xml file and replace "VMwareIBMBR to "VMReplicationWithRBR" and re-import and publish.

BCO Workflows:

"NormalFullCopy.xml"
"IBRFO.xml"
"IBRFallBack.xml"
"IBRFallBackResync.xml"
"NormalCopy.xml"

Test Workflow:

"PreFailoverTestExercise.xml"
"PostFailoverTestExercise.xml"
"StartAppDR.xml"
"Switchover.xml"
"Switchback.xml"
"FailoverTestExercise.xml"

BP Workflows:

"ProtectNewVirtualDisk.xml"
"UnProtectVirtualDisk.xml"
"IBMBRStorageVMotion.xml"
"VirtualDiskExpansion.xml"
"FailoverTestExercisePrecheck.xml"
"StartChecksumRefresh.xml"
"RediscoverVMDetails.xml"
"IBRvMotion.xml"
"TriggerFullSynchronization.xml"
"Rollback.xml"
"EnableCompression.xml"
"DisableCompression.xml"

2.10.4 Post Upgrade Steps for SRM-based Solution

Perform the pre-upgradation steps as follows:

$EAMSROOT/installconfig/vcenter_vra_mapping.properties file and provide the mapping details in the following format:

1. **Add SRM Port in properties file**
   /opt/panaces/installconfig/vmware_vcenter_service.properties file as shown below:
   Syntax: vi /opt/panaces/installconfig/vmware_vcenter_service.properties

For Example:
192.168.6.159_SRM_PORT = 443
172.168.6.159_SRM_PORT = 443

2. **Mapping of vCenter and VRA in RO**
   Syntax: /opt/panaces/installconfig/vcenter_vra_mapping.properties

3. **Mapping VRA component created to the Vcenter IP**
   Syntax: vi /opt/panaces/installconfig/vcenter_vra_mapping.properties

   For Example:
   192.168.6.158=Linux_192.168.6.160_VRA_PR
   172.168.6.158=Linux_172.168.6.160_VRA_DR

Note:

- To upgrade to RO from Version 8.3.0, the SRM Switchover Workflow Failure path has to be updated manually.
- Ensure you have retained all the above steps performed for post-upgrade before you execute the workflows.

This section explains the following procedures as part of **pre-upgrade and post-upgrade:**

1. **To create a folder**

```
mkdir /opt/panaces/templates/typedef/OtherReplicator
cp /opt/panaces/workflows/samples/VMwareSRM/vSphere-
ReplicationInfo.xml
```

2. **To copy the file**

```
cp $EAMSROOT/workflows/samples/VMwareSRM/vSphere-
ReplicationInfo.xml $EAMSROOT/templates/typedef/OtherReplicator
```

3. **To rename the file**

```
mv $EAMSROOT/templates/typedef/OtherReplicator/vSphere-
ReplicationInfo.xml
$EAMSROOT/templates/typedef/OtherReplicator/OtherReplicator-
RepInfo.xml
```

4. **To verify the file is renamed in the new directory**

```
ls $EAMSROOT/templates/typedef/OtherReplicator/
```

2.10.5 Post upgrade steps for Tomcat server.xml

Follow the steps documented in the Installation Guide, section: “**Installation of Apache Tomcat Server**” (Commenting steps).

2.10.6 Custom Scripts

Custom script report

Use the below script to enlist all custom scripts being used and ensure all are restored back into the upgraded setup.

```
         ListCustomScripts.sh
```

```
       output for ListCustomScripts.sh [root@rhelro201 bin]#
./ListCustomScripts.sh
TOTAL CUSTOM ACTION    ::  115
FILE PRESENT SIZE      ::  112
PRINT SIZE             ::  3
DUPLICATE FILES COUNT ::   0
=================================================================
==================
FOLLOWING CMD(TCL/SH/BAT) FILES ARE NOT PRESENT POST UPGRADE
=================================================================
==================
PATH OF THE CUSTOM ACTION  ::   /opt/test.sh
PATH OF THE CUSTOM
ACTION  ::   scripts\repository\repeatable\vCenter\VMwareVMDisabl
evMotion\VMwareVMDisablevMotion.tcl
PATH OF THE CUSTOM
ACTION  ::   scripts\repository\repeatable\vCenter\VMwareVMEnable
vMotion\VMwareVMEnablevMotion.tcl
=================================================================
==================
Script got executed successfully.
```

2.10.7 Apply Patch in RO Server

Perform the following steps to apply the patch in the RO server post-upgrade:

1. Stop the Panaces Services.

2. Back up the PanacesServer.jar jars from $EAMSROOT/lib directory in the RO Server.

3. Take a backup of Panaces DB by executing the following command.

```
mysqldump --single-transaction --skip-disable-keys -uroot -
p<Password>-  password --databases panaces --triggers --routines >
<backupfolder name>/Panaces_DB.dmp
```

Note: Ensure that enough disk space is present in the backup folder.

4. Copy the PanacesServer.jar files (from the patch) and paste them into the following location

```
$EAMSROOT/lib/
```

5. Copy `BlobEncodeDecodeScript.sh`

files (from the patch) and paste them into the following location:

```
$EAMSROOT/bin/
```

6. Navigate to the $EAMSROOT/bin/ directory and execute the ./SecurityUserInjection.sh file using the following command:

```
./SecurityUserInjection.sh
```

7. Start the Panaces Services.

2.10.8 Rollback Steps after Applying Patch in the RO server

Perform the following steps for rollback steps after applying the patch in the RO server:

1. Stop the Panaces Services.

2. Copy the backed-up "PanacesServer.jar" files before upgrading to $EAMSROOT/lib/

3. Recover panaces DB from backed-up DB during the upgrade.

4. Go to the $EAMSROOT/bin/ directory and execute the **./SecurityUserInjection.sh** file using the following command:

```
./SecurityUserInjection.sh
```

5. Start the Panaces Services.

2.10.9 Apply Script in the RO Server

Perform the following steps to apply the script in the RO Server:

1. Place the script anywhere in the environment (for example, /opt)

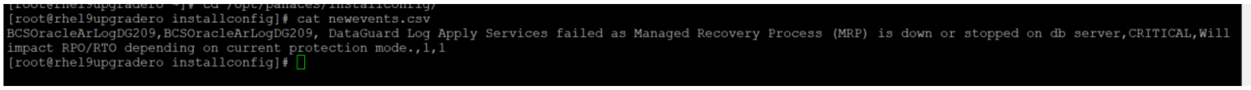
2. In the same location where the script is stored, execute the following command

```
./BlobEncodeDecodeScript.sh
```

2.10.10 Apply the patch after RO and SC upgrade, for existing discovered Oracle DG groups to get the MRP Event.

1. Create the following csv file to generate the BCSOracleArLogDG209 event on the old groups.
2. Create the newevents.csv in this path: *$EAMSROOT/installconfig/newevents.csv* [root@rhel890 Patch]# cat newevents.csv. The content of the csv file must be as follows:

   BCSOracleArLogDG209,BCSOracleArLogDG209, DataGuard Log Apply Services failed as Managed Recovery Process (MRP) is down or stopped on db server,CRITICAL,Will impact RPO/RTO depending on the current protection mode.,1,1



```
[root@rhel9upgradero ~]# cd /opt/panaces/installconfig/
[root@rhel9upgradero installconfig]# cat newevents.csv
BCSOracleArLogDG209,BCSOracleArLogDG209, DataGuard Log Apply Services failed as Managed Recovery Process (MRP) is down or stopped on db server,CRITICAL,Will
impact RPO/RTO depending on current protection mode.,1,1
[root@rhel9upgradero installconfig]# 
```

3. Run the Securityuserinjection script from *$EAMSROOT/bin.*
4. Now run the `./AddEventToExistingGroups.sh` as shown below in the *$EAMSROOT/bin.*

   `./AddEventToExistingGroups.sh -s Oracle-Logs-With-DataGuard.`

5. The following message appears after running the above script:

   Add Event to existing groups

   Adding event BCSOracleArLogDG209 to group oracledg_old

   Added event BCSOracleArLogDG209 to group oracledg_old

   Event BCSOracleArLogDG209 already exists in group oracledg_new

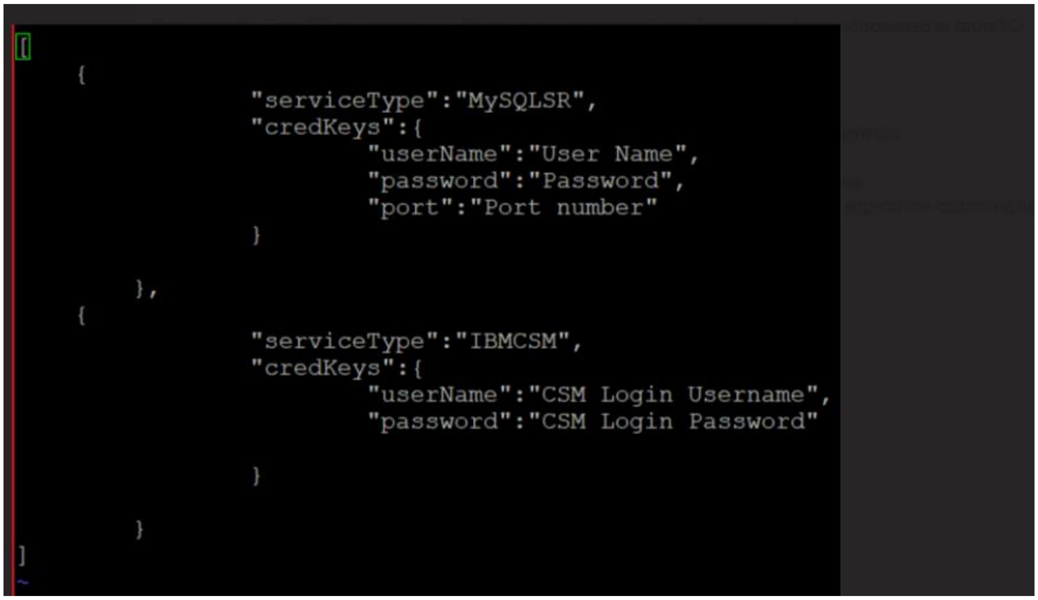
   Scanning to attach default policy

6. Restart SC services(Site controller and Linux OS) and Oracle DataGuardAgent services after running the script, `AddEventToExistingGroups.sh`

2.10.11 Support for Custom Replicator Solutions to convert plain text password to group credentials.

Run the following tool to create Group Credentials for the Custom Replicator protection schemes discovered for any version of RO version earlier then RO 8.3.9.0.

- Navigate to *$EAMSROOT/bin* and select and run the tool as follows: `./CreateGroupCredForCustomReplicators.sh`
- The tool will read the following JSON file: **$EAMSROOT/installconfig/CustomReplicatorGroupCredKeyConfig.json.**
- The script will use the JSON and create respective group credentials for Protection Schemes.
- The JSON also includes Custom Replicator type and keys for credentials.
- A new Custom Replicator Type can be appended to the JSON file in the format shown in the below image:



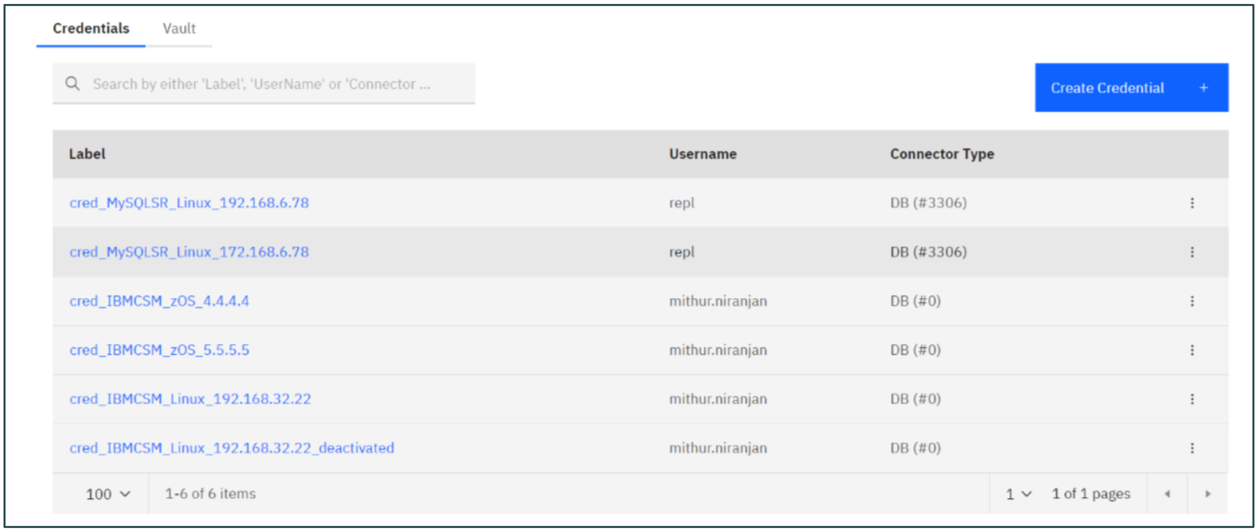
```
[
    {
                "serviceType":"MySQLSR",
                "credKeys":{
                        "userName":"User Name",
                        "password":"Password",
                        "port":"Port number"
                }

        },
    {
                "serviceType":"IBMCSM",
                "credKeys":{
                        "userName":"CSM Login Username",
                        "password":"CSM Login Password"

                }

        }
]
~
```

- After running the tool, the newly created Group credentials can be identified with a name similar to the Custom Replicator name as displayed in the image below:



Label	Username	Connector Type
cred_MySQLSR_Linux_192.168.6.78	repl	DB (#3306)
cred_MySQLSR_Linux_172.168.6.78	repl	DB (#3306)
cred_IBMCSM_zOS_4.4.4.4	mithur.niranjan	DB (#0)
cred_IBMCSM_zOS_5.5.5.5	mithur.niranjan	DB (#0)
cred_IBMCSM_Linux_192.168.32.22	mithur.niranjan	DB (#0)
cred_IBMCSM_Linux_192.168.32.22_deactivated	mithur.niranjan	DB (#0)

2.10.12 Optimal Performance

For the right set of values for max_connections at the DB level, refer to the section Configuring Resiliency Orchestration for Optimal Performance in the Kyndryl Resiliency Orchestration Installation guide.

2.11 Rolling back to the Previous Version

At any time during the upgrade, if there are failures that cannot be corrected within the upgrade window, use the following plan to restore to the earlier version of the Kyndryl Resiliency Orchestration Server installation.

1. Drop the existing databases if they already exist, by using the following commands:

```
mysqladmin –u root -p drop panaces
mysqladmin –u root -p drop pfr
```

2. Restore the MySQL Metadata from the backup.

```
mysql -u root -p < <backup_folder_path>/<filename>.sql
```

3. Restore the Kyndryl Resiliency Orchestration Server software installation directory.

   a. Remove $EAMSROOT with the below command (here assuming $EAMSROOT is /opt/panaces)

```
rm -rf /opt/panaces
rm -rf /opt/tomcat9
```

b. Go to /opt

```
cd /opt/
```

c. Restore binaries

```
tar -xvzf  /opt/backup/panaces.tar.gz
```

d. Restore tomcat9

```
cd /opt
tar –xvzf /opt/backup/tomcat9.tar.gz
```

2.12 Known Issue and Workaround

2.11.1 Vault Configuration is missing post-upgrade

The Vault configuration is missing after the RO server is upgraded from the 8.2.9 version. Test credentials fail for all the components configured with the vault.

Workaround:

Perform the following steps as a workaround:

1. Configure the vault RO post upgrade.
2. Execute the SecurityUserInjection.sh file.
3. Restart Panaces.
4. Perform the Test Credentials procedure.

2.11.2 SchemaValidator script execution is failing on Upgrade

"$EAMSROOT/bin/SchemaValidator.sh" execution is failing on Upgrade RO from 8.3.0 to 8.3.7

Workaround:

If the user executes $EAMSROOT/bin/SchemaValidator.sh with Host IP and receives any access-related issues, follow the below steps:

1. Check if the following GRANT privileges are available if not execute the following commands.

```
 GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP,ALTER, EXECUTE,
SHOW VIEW ON *.* TO '<DB_USER>'@'<HOST_IP>' IDENTIFIED BY PASSWORD
'<DB_PASSWORD>';
```

```
 GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP,ALTER, EXECUTE,
SHOW VIEW ON *.* TO '<DB_USER>'@'<HOST_NAME>' IDENTIFIED BY
PASSWORD'<DB_PASSWORD>';
```

2. After Granting the above privileges to DB_USER the user might receive the below errors.

ERROR 1044 (42000) at line 1433: Access denied for user 'DB_USER'@'HOST_NAME' to database 'panaces_goldencopy'

OR

ERROR 1370 (42000) at line 1433: alter routine command denied to user 'DB_USER'@'HOST_NAME' for routine 'panaces_goldencopy.getWorkflowsC

For these errors, check the grants for <DB_USER> and <HOST_NAME> on panaces_goldencopy database using Following command

```
  SHOW GRANTS FOR `<DB_USER>`@`<HOST_NAME>`;
```

3. Check if the following GRANT privileges are available, if not execute the following commands.

```
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, ALTER,ALTER
ROUTINE,INDEX,CREATE ROUTINE, EXECUTE,TRIGGER, CREATE VIEW,SHOW VIEW
ON `panaces_goldencopy`.* TO `<DB_USER>`@`<HOST_NAME>`;
```

2.11.3 (Optional) Workflow Version in View Workflow Page

Perform the following steps if the workflow version does not display correctly in post-upgrade:

After the upgrade is complete and all RO services are started, execute the following script. This script will update the version of workflows that has been executed so far into a new column viz. asl_version within the action_log table.

It might take several hours to execute based on the number of entries present in the action_log table.

Execute the following command:

```
$EAMSROOT/bin/ActionLogBlobUpgradeUtility.sh
```

The below message displays when the script is failed:

Sample message:

```
Script ran with exit code 1
```

Note: The exit code is always greater than '0' in case of script failures.

The below message displays when the script is a success:

Sample message:

```
Script ran with exit code 0
```

Refer to the following log to know the current state of execution:

```
$EAMSROOT/var/log/ActionLogVersionUpdateBlob.log
```

2.11.4 For low touch agent upgrade, on clock upgrade, there is an error message.

Error Message: 'Error occurred while upgrading agent'

Workaround: This message can be ignored as the upgrade is happening smoothly.

2.11.5 Upgrade steps for RO Base Version 7.2 SP4

Perform the following steps if RO version 7.2 SP4 is used as the Base version for the upgrade:

1. Update the `INSTALLER_UI=console` in the `PanacesServerInstaller.properties` file and proceed with the silent mode upgrade.
2. Pause the upgrade process at this step.

   "SSL check validation"
3. Modify script "$EAMSROOT/bin/TriggerOneHopUpgrade.sh"
   a. Open file "$EAMSROOT/bin/TriggerOneHopUpgrade.sh" using the vi command

b. Update 2 jars name in that CLASSPATH as shown below (line#13)

```
CLASSPATH=<<Older_RO_Version_Backup_Path>>/lib/spring-data-
commons-1.5.2.RELEASE.jar:<<Older_RO_Version_Backup_Path>>

/lib/spring-data-jpa-
1.3.4.RELEASE.jar:$CLASSPATH:$EAMSROOT/lib/onehopupgrade.ja
r:$TOMCAT_HOME/webapps/PanacesGUI/WEB-INF/lib/*
```

Note: <<Older_RO_Version_Backup_Path>> is the path of the older RO version's backup patch. For example, "/opt/panaces_7.2.4.0". If the backup path is not found easily, then search for these 2 jars ("spring-data-commons-1.5.2.RELEASE.jar" and "spring-data-jpa-1.3.4.RELEASE.jar") & take the absolute path of these 2 jars.

4. Then continue with the upgrade process.

2.11.6 For low touch upgrade, agent upgrade page shows wrong upgrade status message and current version even after successful upgrade in the backend for windows platform.

Error Message in RO UI: Unable to get response for this request in configured time.

Workaround: Ignore this error message and reload the page.

3 GPL Dependencies for Kyndryl Resiliency Orchestration

Based on the features, download the GPL-dependent binaries from this link: GPL-dependent binaries (https://sourceforge.net/projects/gnu-utils/files/binaries/) before you install the Kyndryl Resiliency Orchestration.
You must complete the steps mentioned in Installing Third-party Software, in the RO Installation guide.
For more information about the GPL licenses, see the section **GPL License** in the RO Installation guide.